

# Unleashed 200.8 Online Help

Supporting Release 200.8

# Copyright, Trademark and Proprietary Rights Information

© 2020 CommScope, Inc. All rights reserved.

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

## Export Restrictions

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

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

## Disclaimer

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

## Limitation of Liability

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

## Trademarks

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

# Contents

---

<b>Preface.....</b>	<b>7</b>
Document Conventions.....	7
Notes, Cautions, and Safety Warnings.....	7
Command Syntax Conventions.....	7
Document Feedback.....	8
Ruckus Product Documentation Resources.....	8
Online Training Resources.....	8
Contacting Ruckus Customer Services and Support.....	9
What Support Do I Need?.....	9
Open a Case.....	9
Self-Service Resources.....	9
<b>Introducing Ruckus Unleashed.....</b>	<b>11</b>
Introducing the Ruckus Unleashed Platform.....	11
Unleashed Network Overview.....	11
Unleashed Feature Parity with ZoneDirector.....	12
Unleashed Limitations and Deviations from ZoneDirector.....	13
Unleashed-Only Features.....	14
Unleashed Access Point Physical Features.....	14
C110.....	14
E510.....	19
H320.....	23
H510.....	28
M510.....	32
R320.....	40
R510.....	45
R610.....	49
R710.....	53
R720.....	57
R750.....	62
T310 Family.....	66
T610 and T610s.....	70
T710 and T710s.....	75
<b>Setting Up an Unleashed Wi-Fi Network.....</b>	<b>81</b>
Overview of the Setup Process.....	81
Step 1: Unpack and Install the Unleashed Master AP.....	82
Step 2: Configure Your Unleashed Network.....	82
Step 2a: Setup Using the Unleashed Mobile App.....	82
Step 2b: Setup Using a Web Browser.....	85
Step 2c: Setup Using the Command Line Interface.....	97
Step 3: Customize Your Wireless LANs.....	100
Step 4: Deploy Additional Unleashed Member Access Points.....	102
<b>Using the Admin Interface.....</b>	<b>103</b>
Unleashed Administration Interface Overview.....	103
Navigating the Dashboard.....	103
Using the Dashboard Components.....	104

Internet.....	104
Wi-Fi Networks.....	104
Clients.....	105
Access Points.....	106
Switches.....	107
Admin & Services.....	108
<b>WLAN Configuration.....</b>	<b>109</b>
WLAN Configuration Overview.....	109
WLAN Usage Types.....	109
Creating a New WLAN.....	110
802.1X EAP WLANs.....	112
802.1X WLAN Survivability.....	112
Guest WLANs.....	115
Deploying a Guest WLAN.....	115
Hotspot WLANs.....	175
Configuring Global WLAN Settings.....	176
Editing an Existing WLAN.....	177
Deleting a WLAN.....	179
Temporarily Disabling a WLAN.....	179
<b>Advanced WLAN Configuration.....</b>	<b>181</b>
Advanced WLAN Configuration Overview.....	181
Configuring Advanced WLAN Options.....	181
Zero-IT and DPSK Settings.....	183
Zero-IT.....	183
Dynamic PSK.....	184
Enabling Zero-IT for a WLAN.....	185
Enabling DPSK for a WLAN.....	185
WLAN Priority Settings.....	189
Access Control Settings.....	190
Application Policies.....	191
Creating an Application Control Policy.....	192
Radio Control Settings.....	194
Other Advanced WLAN Settings.....	195
Configuring Client Isolation Whitelists.....	196
Bypass Apple CNA.....	197
<b>Access Point Configuration.....</b>	<b>199</b>
Access Point Configuration Overview.....	199
Show Mesh Topology.....	200
Show Client Info.....	201
Show Events and Alarms.....	203
Configuring Global AP Settings.....	204
Radio B/G/N (2.4G).....	204
Radio A/N/AC (5G).....	205
Others.....	206
Monitoring an Individual AP.....	210
Show Client Info.....	211
Show System Overview.....	212
Show WLANs Info.....	214
Configuring an Individual AP.....	214

Renaming an AP.....	217
Working with AP Groups.....	218
Modifying the System Default AP Group.....	219
Creating a New AP Group.....	223
Modifying Model Specific Controls.....	225
Configuring AP Ethernet Ports.....	227
Restarting an AP.....	232
Removing an AP.....	233
<b>ICX Switch Management.....</b>	<b>235</b>
ICX Switch Management Overview.....	235
Requirements.....	235
Preparing an ICX Switch for Unleashed Management.....	236
Approving a New Switch to Join Unleashed.....	239
Monitoring Connected ICX Switches.....	242
Managing Switch Ports.....	243
Backup and Restore Switch Configuration.....	246
Upgrading ICX Switch Firmware.....	249
<b>Working with Clients.....</b>	<b>253</b>
Client Management Overview.....	253
Viewing the Clients List.....	253
Renaming a Client.....	255
Deleting a Client.....	257
Permanently Blocking a Client Device.....	257
Marking a Client as a Favorite.....	258
Running a SpeedFlex Performance Test on a Wireless Client.....	259
Client Connection Troubleshooting.....	263
Adding User Accounts to the Internal User Database.....	265
Authenticating Clients Using an External Database.....	265
<b>Configuring Admin &amp; Services Settings.....</b>	<b>267</b>
Admin & Services Overview.....	267
System Settings.....	267
System Info Settings.....	268
IP Settings.....	274
Configuring the System Time.....	285
Setting the Country Code.....	286
Configuring User Roles.....	288
Adding New Users to the Local Database.....	290
Changing an Existing User Account.....	292
Deleting a User Record.....	292
Mesh Networking.....	293
Enabling Log Delivery to Remote Syslog Server.....	302
Services.....	303
AAA Servers.....	304
Access Control.....	308
Application Recognition and Control.....	313
Bonjour Gateway.....	319
Dynamic PSK.....	322
Guest Access Services.....	325
Hotspot Services.....	326

Radio Control.....	329
WIPS.....	337
URL Filtering.....	342
Administration Settings.....	348
Preferences.....	348
Backup and Restore.....	350
Upgrade.....	353
Registration.....	360
Diagnostics.....	364
Working with SSL Certificates.....	373
Testing Network Connectivity.....	379
Network Management.....	380
Enabling Mobile App Remote Management.....	385
<b>Unleashed Access Point Power Supply Considerations.....</b>	<b>389</b>
AP Power Warnings.....	389
Power Limitations by PoE Mode and AP Model.....	391
R750.....	391
R720 .....	391
R710.....	391
R610 .....	391
T610 .....	392
M510 .....	392

# Preface

- Document Conventions..... 7
- Command Syntax Conventions..... 7
- Document Feedback..... 8
- Ruckus Product Documentation Resources..... 8
- Online Training Resources..... 8
- Contacting Ruckus Customer Services and Support..... 9

## Document Conventions

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

**TABLE 1** Text Conventions

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

## Notes, Cautions, and Safety Warnings

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

### NOTE

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

### ATTENTION

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



### CAUTION

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



### DANGER

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

## Command Syntax Conventions

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

Convention	Description
<b>bold text</b>	Identifies command names, keywords, and command options.

## Preface

Document Feedback

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

## Document Feedback

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

You can email your comments to Ruckus at [#Ruckus-Docs@commscope.com](mailto:#Ruckus-Docs@commscope.com).

When contacting us, include the following information:

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

For example:

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

## Ruckus Product Documentation Resources

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

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

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

## Online Training Resources

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



# Contacting Ruckus Customer Services and Support

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

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

## What Support Do I Need?

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

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

## Open a Case

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

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

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

## Self-Service Resources

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

- Technical Documentation—<https://support.ruckuswireless.com/documents>
- Community Forums—<https://forums.ruckuswireless.com/ruckuswireless/categories>
- Knowledge Base Articles—<https://support.ruckuswireless.com/answers>
- Software Downloads and Release Notes—[https://support.ruckuswireless.com/#products\\_grid](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](https://support.ruckuswireless.com/case_management).



# Introducing Ruckus Unleashed

---

- [Introducing the Ruckus Unleashed Platform.....](#) 11
- [Unleashed Network Overview.....](#) 11
- [Unleashed Feature Parity with ZoneDirector.....](#) 12
- [Unleashed Limitations and Deviations from ZoneDirector.....](#) 13
- [Unleashed-Only Features.....](#) 14
- [Unleashed Access Point Physical Features.....](#) 14

## Introducing the Ruckus Unleashed Platform

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.

Unleashed provides a controller-less 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 (e.g., ZoneDirector or SmartZone controller).

Unleashed access points 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 a 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 up front and recurring costs, and the simplified web interface also makes deploying Unleashed very easy.

With the Ruckus Unleashed platform, customers can deploy up to 128 APs without the need to purchase and install 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, Bonjour Gateway/Bonjour Fencing, and one-step firmware upgrades of the entire network from a single interface.

## Unleashed Network Overview

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

### NOTE

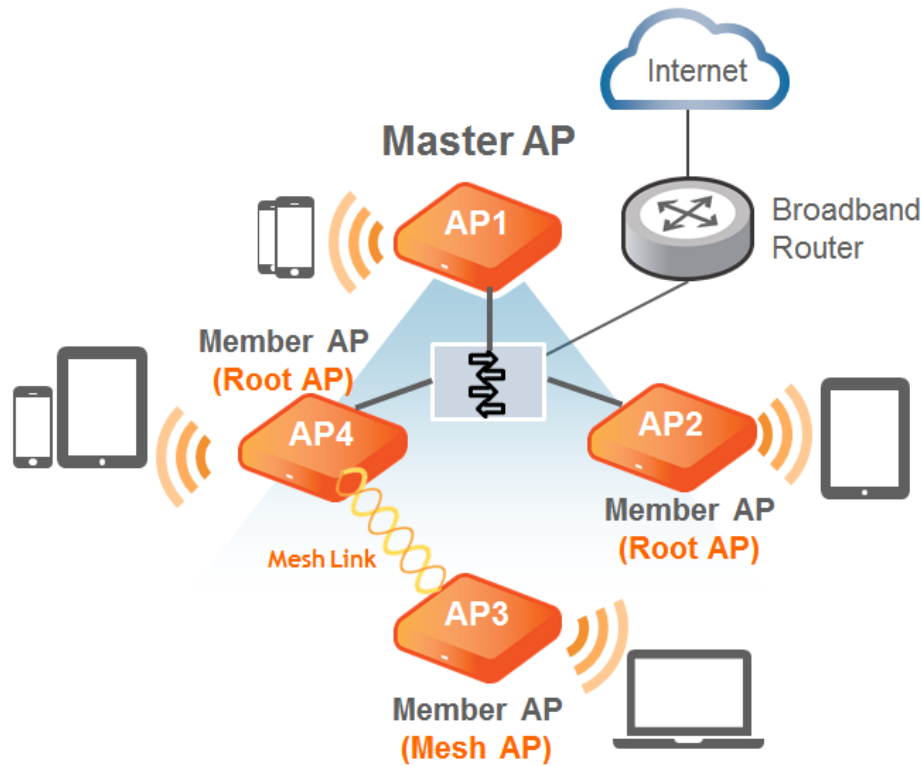
Beginning with release 200.8, the maximum capacity limit has been increased from 50 APs and 1,024 clients to 128 APs and 2,048 clients per Unleashed network in bridge mode (gateway mode supports up to 50 APs and 1,024 clients).

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

An Unleashed member AP joins a Master AP in the same subnet automatically. Unleashed member APs will not attempt to join a ZoneDirector or SmartZone controller on the network. If the Master AP is offline, one of the member APs will assume the role of Unleashed Master and take over control of the Unleashed network.

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

FIGURE 1 Basic Unleashed Network topology



## Unleashed Feature Parity with ZoneDirector

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

- Smart Mesh
- One-step firmware upgrades of the entire network from a single interface
- Layer 2 roaming
- 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/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
  - HTTP/HTTPS Redirect
  - Up to 1,024 local users supported (on the internal database)
  - Up to 1,024 client devices supported (depending on encryption/auth method)
  - Self-Service Guest Pass
  - Client Load Balancing
  - Band Steering
  - Client Isolation
  - Client Fingerprinting and Device Access Policies
- DHCP server (configured manually from Unleashed Network Master AP)
- SNMP Management
- Syslog Delivery to External Syslog Server
- Management IP Interface
- Multi-Language support
- WLAN Prioritization
- Dynamic VLANs
- Enable/Disable WLANs on a per-radio basis
- AP Groups

## Unleashed Limitations and Deviations from ZoneDirector

While many ZoneDirector features are included, 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:

- No layer 3 roaming. All APs must be in the same subnet.
- Tunneled WLANs are not supported.

- IPv6 is not supported.
- No interface to communicate with SmartCell Insight, SPoT, or the ZoneDirector Remote Control mobile app.
- No North Bound Interface to pass client authentication responsibility to an external entity.
- No WLAN Groups.

## Unleashed-Only Features

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

- The Unleashed platform does not require an external controller - all controller functions are performed through a single "Unleashed Master AP" web interface. The Unleashed Master AP serves the same functions as a ZoneDirector controller would perform on the network; i.e., all control functions are performed through the controller and pushed to the other APs on the network.
- An Unleashed Member AP automatically takes over all AP control functions if the Master AP is offline.
- Preferred Master: Admins can configure an AP to serve as the "preferred" Unleashed 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 Unleashed Master role.
- The Unleashed 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 Unleashed Master AP can be configured as a gateway router, performing all NAT and DHCP functions as well as serving as the Unleashed network controller and serving wireless clients.

### NOTE

When gateway mode is enabled, Unleashed supports a maximum 50 APs and 1,024 concurrent clients due to the additional resource demands placed on the Master AP when in gateway mode.

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

## Unleashed Access Point Physical Features

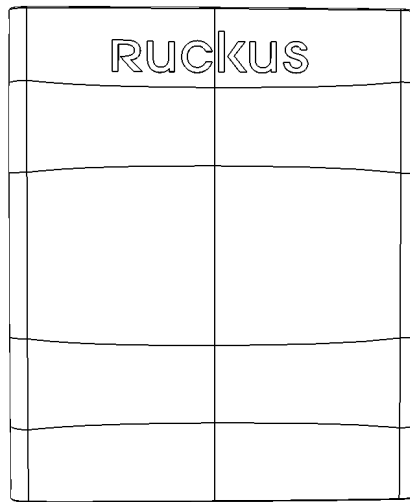
This section describes the physical features of the Unleashed Access Points currently available.

### 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 2** C110 Access Point








### Rear Panel

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

**TABLE 2** Front Panel LEDs

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

**TABLE 2** 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 2** 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 2** 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 2** Front Panel LEDs (continued)

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

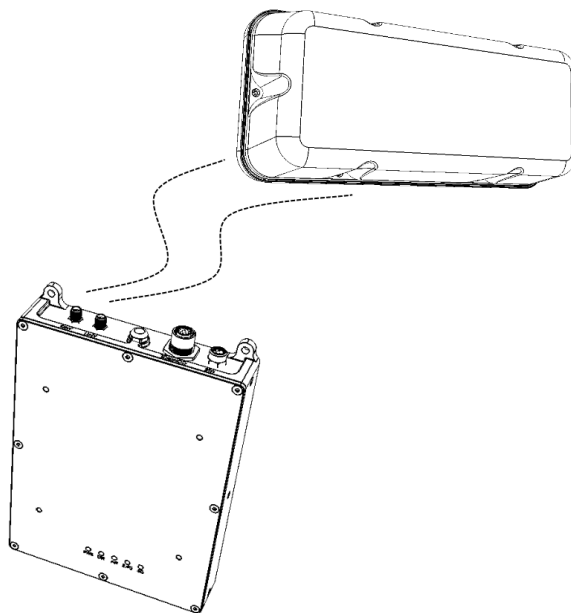
## E510

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 3** E510 Access Point



### Front Panel

The E510 AP features five LEDs on its front panel.

**TABLE 3** 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 3** 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 3** 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 3** Front Panel LEDs (continued)

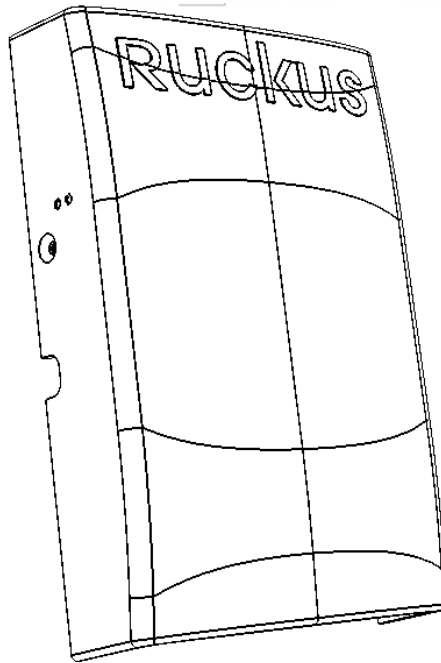
LED	Status	Description
5G	 5G Amber (solid)	Radio is up, no clients are connected to the 5 GHz radio.
5G	 5G Solid Green	Radio is up, at least one client is connected to the 5 GHz radio.
5G	 5G Flashing Green	Radio is up, at least one downstream Mesh AP is connected to the 5G radio.

## 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 4** H320 Access Point



### Rear Panel






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

**TABLE 4** Front Panel LEDs




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



**TABLE 4** 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 4** 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 4** 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 4** Front Panel LEDs (continued)

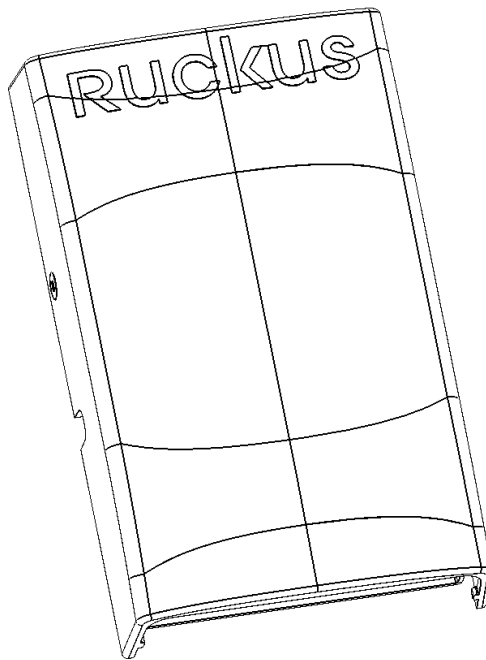
LED	Status	Description
5G	 <p>5G Flashing Green</p>	Radio is up, at least one downstream Mesh AP is connected to the 5G radio.

## 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.

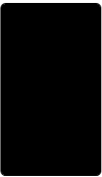
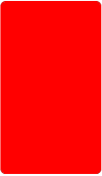
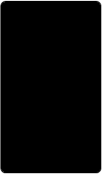
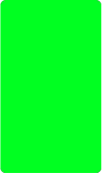
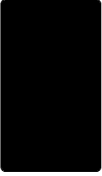
**FIGURE 5** H510 Access Point








### Rear Panel

The H510 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.
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 5** 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 5** 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 5** Front Panel LEDs (continued)

LED	Status	Description
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.
5G	 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.

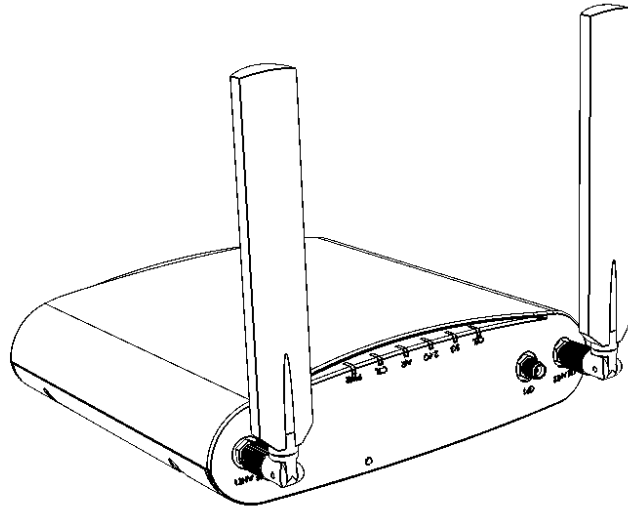
**NOTE**

Because the M510 supports LTE backhaul, it requires special setup procedures different from other Unleashed APs. For information, see [M510 Configuration](#) on page 38.

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




**FIGURE 6** M510 Access Point








**Front Panel**

The M510 AP features six LEDs on its front panel.

**TABLE 6** Front Panel LEDs

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

**TABLE 6** 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 6** 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 6** 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 6** 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.
CEL	 5G Solid Green	<ul style="list-style-type: none"> <li>• Off: No cellular connection.</li> <li>• Amber: 3G connection.</li> <li>• Green: 4G/LTE connection.</li> </ul>

**NOTE**

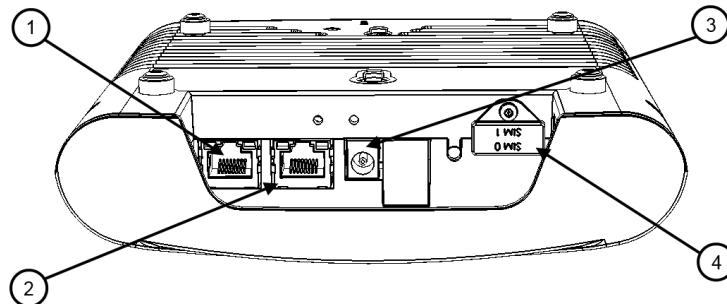
CEL LED will remain in "Off" status until the Unleashed M510 is provisioned.

**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 7** M510 bottom panel



**TABLE 7** M510 bottom panel elements

No.	Label	Description
1	ETH 0 WAN / PoE	10/100/1000 Mbps RJ-45 Ethernet port with PoE support
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.  <b>NOTE</b> The orientation of the SIM cards is reversed, refer to the <i>M510 Quick Setup Guide</i> for details on SIM card insertion.

## Ethernet Port LEDs

**TABLE 8** 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 8** Ethernet (Primary) with Cellular failover

Gateway Mode

**WAN Selection**

\* WAN connection: Ethernet (Primary) with cellular

\* WAN Recovery Timer: 60 seconds (10-300)

---

**Cellular Radio Settings**

APN for SIM 0: defaultapn

APN for SIM 1: defaultapn

---

**WAN IP Address for Ethernet**

Manual  DHCP

\* IP Address: 172.18.165.7

\* Netmask: 255.255.255.0

\* Gateway: 172.18.165.254

\* Primary DNS Server: 10.10.10.10

Secondary DNS Server: 10.10.10.106

\* This image shows the WAN port and SIM slots

---

**LAN & WLAN IP Address**

\* Router IP: 192.168.10.1

\* Netmask: 255.255.255.0

---

**LAN & WLAN Client IP Addresses**

\* Starting IP: 192.168.10.2

\* Ending IP: 192.168.10.102

Number of IPs: 101

Lease Time: Twelve hours

Back
Next

FIGURE 9 Cellular only

1 System 2 IP setting 3 Wireless LAN 4 Administrator 5 Review

Gateway Mode

WAN Selection

\* WAN connection Cellular only

Cellular Radio Settings

APN for SIM 0 internet

APN for SIM 1 internet

LAN & WLAN Client IP Addresses

\* Starting IP 10.10.0.10

\* Ending IP 10.10.0.30

Number of IPs 21

Lease Time Twelve hours

LAN & WLAN IP Address

\* Router IP 10.10.0.1

\* Netmask 255.255.0.0

Back Next

\* This image shows the WAN port and SIM slots

**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.

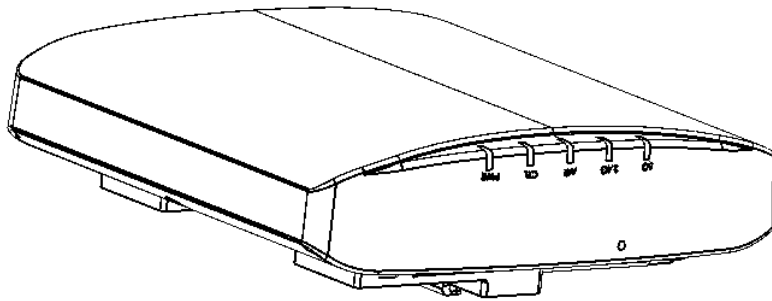
## R320

The Unleashed 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 the Ruckus Unleashed R320 802.11ac Access Point.






**FIGURE 10** R320 Access Point








### Front Panel

The R320 AP features five 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.
PWR	 PWR Flashing Green	System started, no routable IP address detected.

**TABLE 9** 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 9** 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 9** Front Panel LEDs (continued)

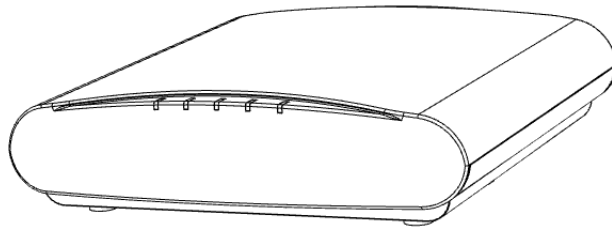
LED	Status	Description
2.4G	 2.4G Solid Green	Radio is up, at least one client is connected to the 2.4 GHz radio.
5G	 5G Off	Radio is down.
5G	 5G Amber (solid)	Radio is up, no clients are connected to the 5 GHz radio.
5G	 5G Solid Green	Radio is up, at least one client is connected to the 5 GHz radio.
5G	 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 11** R510 Access Point








### Front Panel

The R510 AP features five LEDs on its front panel.

**TABLE 10** Front Panel LEDs

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

**TABLE 10** 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 10** 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 10** 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 10** Front Panel LEDs (continued)

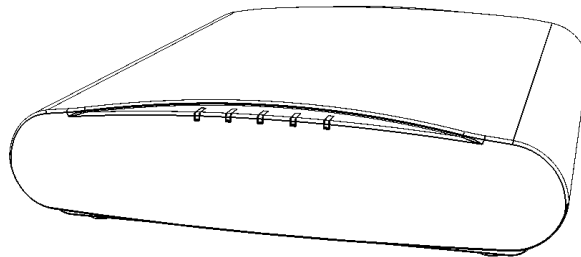
LED	Status	Description
5G	 <p>5G Flashing Green</p>	Radio is up, at least one downstream Mesh AP is connected to the 5G radio.

## 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 12** R610 Access Point




### Front Panel

The R610 AP features five LEDs on its front panel.

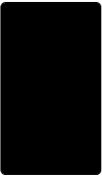
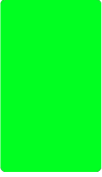
**TABLE 11** Front Panel LEDs

LED	Status	Description
PWR	 <p>PWR Off</p>	No power connected.

**TABLE 11** Front Panel LEDs (continued)

LED	Status	Description
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.
CTL	 CTL Flashing Green (slow, every 2 seconds)	Network problem. Cannot contact Unleashed Master.

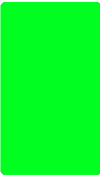

**TABLE 11** Front Panel LEDs (continued)

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 11** Front Panel LEDs (continued)

LED	Status	Description
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.
5G	 5G Amber (solid)	Radio is up, no clients are connected to the 5 GHz radio.

**TABLE 11** Front Panel LEDs (continued)

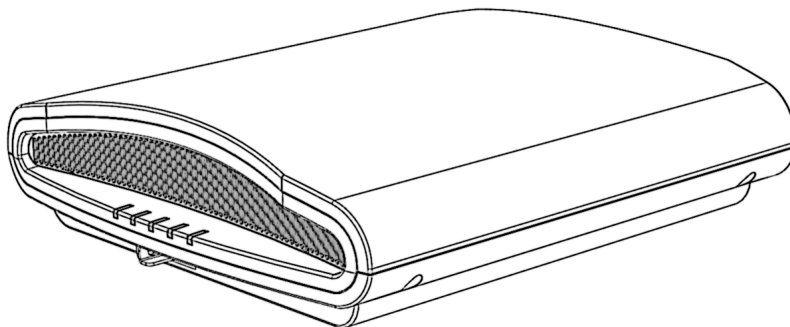
LED	Status	Description
5G	 5G Solid Green	Radio is up, at least one client is connected to the 5 GHz radio.
5G	 5G Flashing Green	Radio is up, at least one downstream Mesh AP is connected to the 5G radio.

## 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 13** R710 Access Point




### Front Panel

The R710 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.
PWR	 PWR Solid Green	Routable IP address received.
CTL	 CTL Off	Unleashed Member AP.

**TABLE 12** 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 12** 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 12** Front Panel LEDs (continued)

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

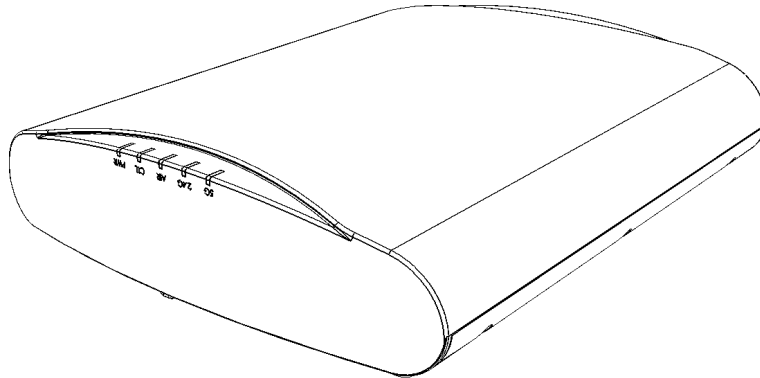
## R720

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 Ethernet port, and one 100/1000/2500 Ethernet port that supports 802.3af and 802.3at Power Over Ethernet (PoE), and a USB port for IoT applications.

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




**FIGURE 14** R720 Access Point



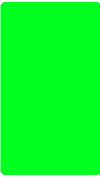



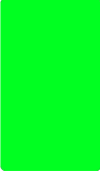
**Front Panel**

The R720 AP features five LEDs on its front panel.






**TABLE 13** 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 13** 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 13** 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 13** Front Panel LEDs (continued)

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

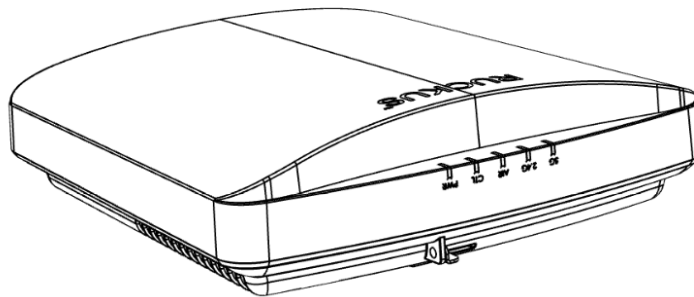
## R750

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 onboard IoT management chip for applications such as ZigBee, BLE (Bluetooth Low Energy) or LTE dongles, and a 2.5 GbE port that supports 802.3af, 802.3at and 802.3bt (40W) PoE, and one 1 GbE port (non-PoE).

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


**FIGURE 15** Unleashed R750 Access Point



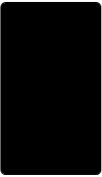
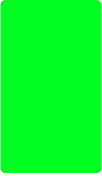
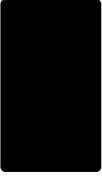
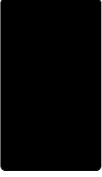
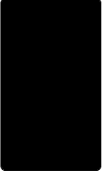
### Front Panel

The R750 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.

**TABLE 14** 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 14** 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 14** 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 14** Front Panel LEDs (continued)

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

## T310 Family

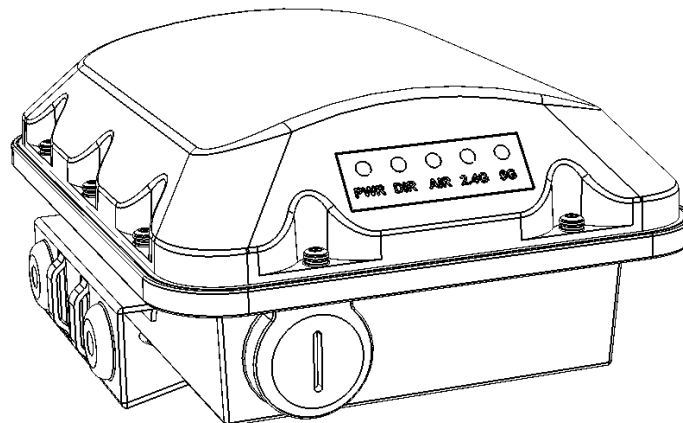
The Unleashed T310 family provides 802.11ac "Wave 2" features, including MU-MIMO, in an outdoor access point.

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


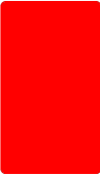

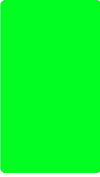

**FIGURE 16** T310d Outdoor Access Point




### Front Panel

The T310 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.
PWR	 PWR Solid Green	Routable IP address received.
CTL	 CTL Off	Unleashed Member AP.




**TABLE 15** 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 15** 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 15** Front Panel LEDs (continued)

LED	Status	Description
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.
5G	 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.

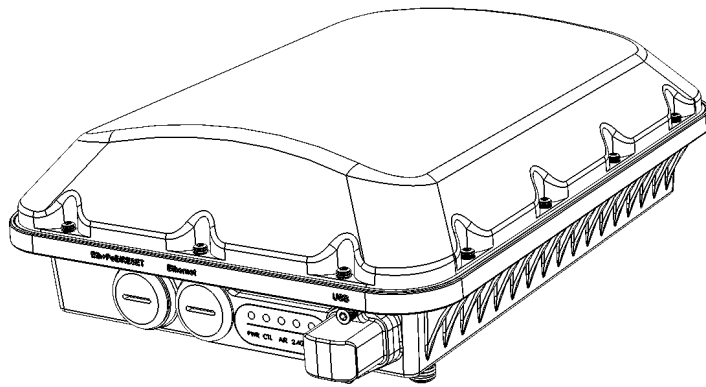
The T610 also includes a USB port for BLE Smart Beacon, Zigbee or other IoT devices.

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 17** Unleashed T610/T610s Outdoor Access Point



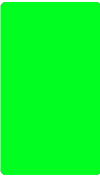



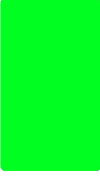
### Front Panel

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

**TABLE 16** 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 16** 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 16** 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 16** Front Panel LEDs (continued)

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

## T710 and T710s

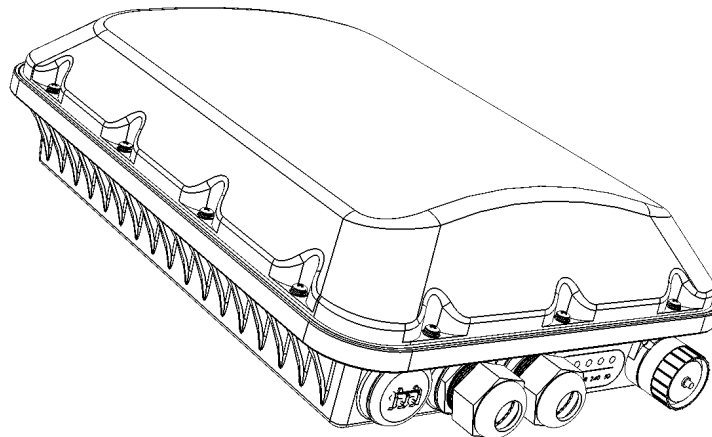
The Unleashed T710 is the first outdoor Ruckus Unleashed 802.11ac Wave 2 access point.

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 18** Unleashed T710/T710s Outdoor Access Point



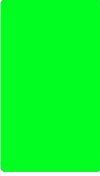
### Front Panel

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

**TABLE 17** Front Panel LEDs

LED	Status	Description
PWR	 PWR Off	No power connected.

**TABLE 17** Front Panel LEDs (continued)

LED	Status	Description
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.
CTL	 CTL Flashing Green (slow, every 2 seconds)	Network problem. Cannot contact Unleashed Master.



**TABLE 17** 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 17** Front Panel LEDs (continued)

LED	Status	Description
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.
5G	 5G Amber (solid)	Radio is up, no clients are connected to the 5 GHz radio.

**TABLE 17** Front Panel LEDs (continued)

LED	Status	Description
5G	 <p data-bbox="469 527 488 543">5G</p> <p data-bbox="428 573 529 590">Solid Green</p>	Radio is up, at least one client is connected to the 5 GHz radio.
5G	 <p data-bbox="469 827 488 844">5G</p> <p data-bbox="415 873 540 890">Flashing Green</p>	Radio is up, at least one downstream Mesh AP is connected to the 5G radio.





# Setting Up an Unleashed Wi-Fi Network

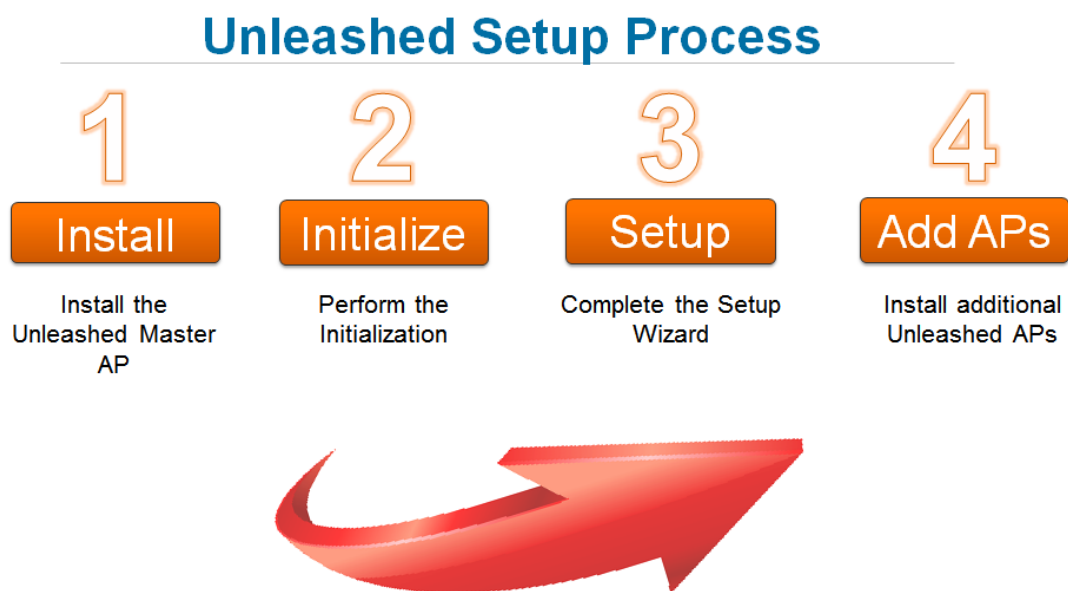
- Overview of the Setup Process.....81
- Step 1: Unpack and Install the Unleashed Master AP..... 82
- Step 2: Configure Your Unleashed Network..... 82
- Step 3: Customize Your Wireless LANs..... 100
- Step 4: Deploy Additional Unleashed Member Access Points.....102

## Overview of the Setup Process

The following section describes the steps required for setup and configuration of a Ruckus Unleashed wireless network.

1. [Step 1: Unpack and Install the Unleashed Master AP](#) on page 82
2. [Step 2: Configure Your Unleashed Network](#) on page 82
3. [Step 3: Customize Your Wireless LANs](#) on page 100
4. [Step 4: Deploy Additional Unleashed Member Access Points](#) on page 102
5. Begin Using Your Ruckus Unleashed Network!

**FIGURE 19** 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 Unleashed Mobile App

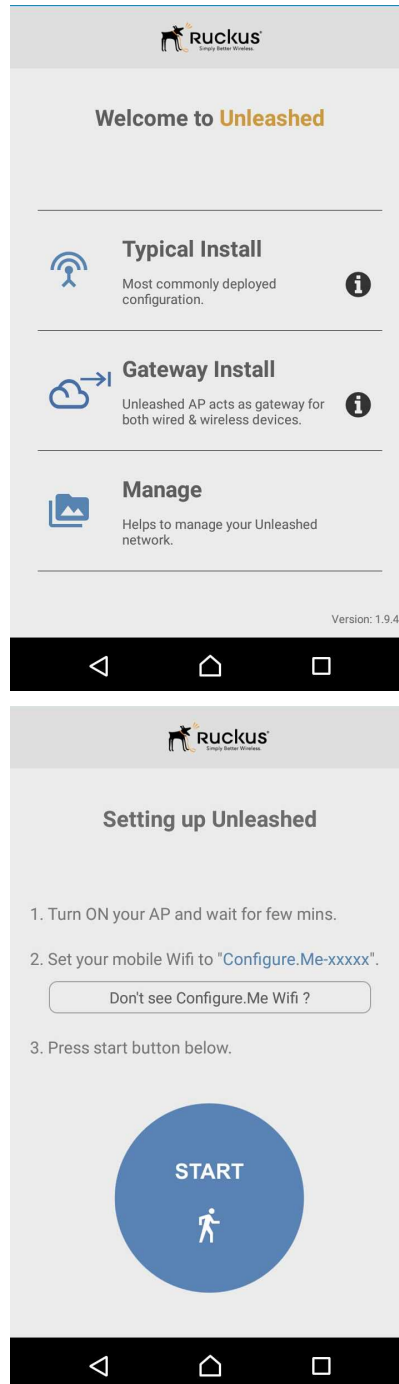
To perform setup using the Unleashed Mobile App, download the iOS or Android app from the app store.

As soon as the Unleashed 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.

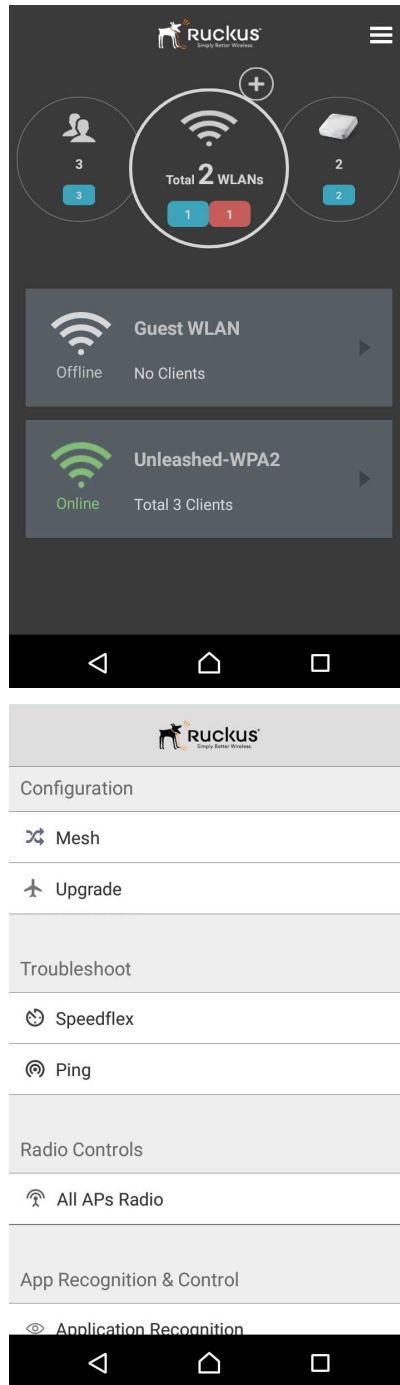
2. Launch the app, and follow the on-screen instructions to configure your Unleashed network(s).

**FIGURE 20** Unleashed Mobile App for iOS and Android



Setting Up an Unleashed Wi-Fi Network  
Step 2: Configure Your Unleashed Network

FIGURE 21 Configuring Unleashed from the Mobile App



## Step 2b: Setup Using a Web Browser

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

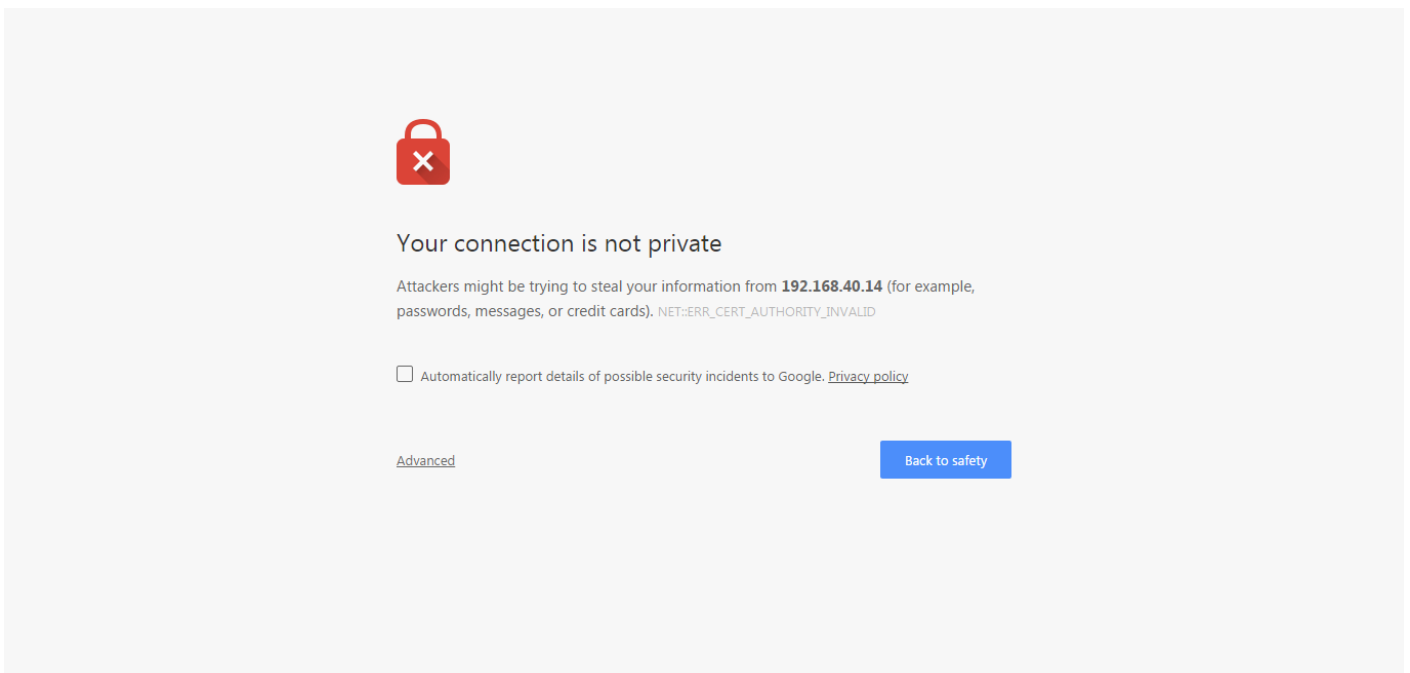
1. Using your the Wi-Fi configuration settings on your client device (such as a laptop or mobile device), select and associate to the **Configure.Me-[xxxxxx]** WLAN, and launch a web browser.
2. In your browser's URL bar, enter the following address and press **Enter**: [unleashed.ruckuswireless.com](http://unleashed.ruckuswireless.com).

**FIGURE 22** Connect to "Configure.Me-[xxxxxx]" WLAN, then launch a web browser



3. Depending on your browser, you may be presented with a security warning saying "This connection is not trusted" (Firefox) or "Your Connection is Not Private" (Chrome) or "There is a problem with this website's security certificate" (Internet Explorer). This is normal, as the Unleashed AP does not have an SSL certificate that is recognized by your browser.
4. Click **Advanced > Proceed to [IP address] (unsafe)** (Chrome), or **I Understand the Risks > Add Exception... > Confirm Security Exception** (Firefox), or **Continue to this website (not recommended)** (IE) to continue.

**FIGURE 23** Security warning (Chrome)



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

## Setting Up an Unleashed Wi-Fi Network

### Step 2: Configure Your Unleashed Network

6. 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, "*Unleashed Installation*", select your **Language** from the menu and the installation type from the list.
  - b) Select **Typical Install** for most typical installation scenarios.

#### NOTE

For information on **UMM Install** and **Local Upgrade** options, refer to [UMM Install](#) on page 93 and [Installation with Local Upgrade](#) on page 95.

- c) Click **Next**.

**FIGURE 24** Setup Wizard - Typical Install

The screenshot shows the 'Unleashed Installation' wizard interface. At the top left is the Ruckus logo (an ARRIS company). The title 'Unleashed Installation' is centered, with the version '200.8.10.3.118' on the right. The main content area has a light gray background and contains the following elements:

- Language:** A dropdown menu currently showing 'English'. A note to the right says: 'Select the display language that you want to use on the Web interface.'
- Typical Install:** A radio button that is selected. Below it, the text reads: 'This is the most typical way to install if one do not want to use UMM'.
- UMM Install:** A radio button that is unselected. Below it, the text reads: 'Use image from UMM to install an Unleashed network'. This section includes:
  - UMM Domain/IP:** A text input field. A note to the right says: 'UMM address from where the Unleashed Network can retrieve configuration'.
  - Config Template Name:** A text input field. A note to the right says: 'Configuration template pre-stored in UMM for the Unleashed Network'.
- Local Upgrade:** A radio button that is unselected. Below it, the text reads: 'Upgrade this Unleashed AP from a local image file'.

- d) On the *System* page, enter a **System Name** for the Unleashed system. This system name can be used to identify the Unleashed device on your local area network.
- e) Select your **Country Code** from the menu.

#### NOTE

This option is not displayed if the AP is shipped from the factory with a fixed country code.

- f) If you want to enable Mesh networking for your Unleashed network, select the check box next to **Mesh**. See [Mesh Networking](#) on page 293 for more information.

#### NOTE

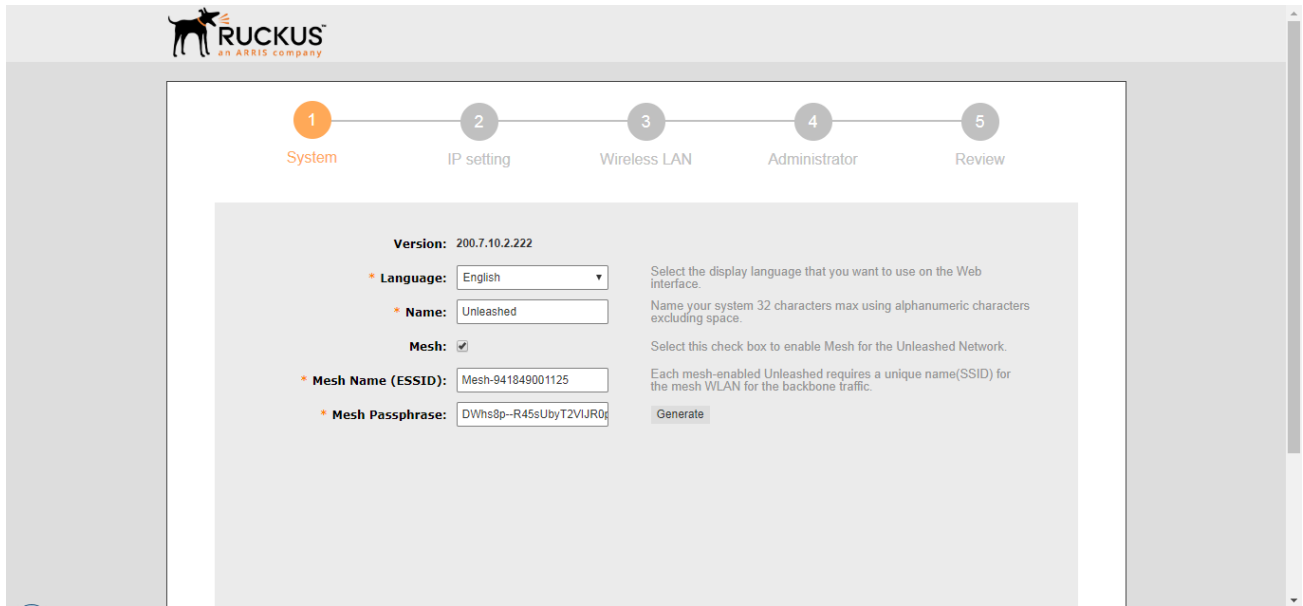
If the Unleashed AP does not support Mesh (e.g., R310), it can be configured as the Unleashed Master, but it will not be able to participate in the mesh network.

#### NOTE

If the Master AP is in Gateway mode and the WAN port is connected via 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.

- g) Click **Next** to continue.

FIGURE 25 Setup Wizard 1



- h) 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, etc.) and the other as a LAN port.

**NOTE**

If your modem/router already provides gateway functionality, do not enable Gateway mode on the Unleashed Master AP. For more information on Gateway mode, see [Gateway Mode](#) on page 275.

- i) Select whether to assign a manual IP address or allow the system to obtain an IP address automatically using DHCP. Default is Dynamic (DHCP).

**NOTE**

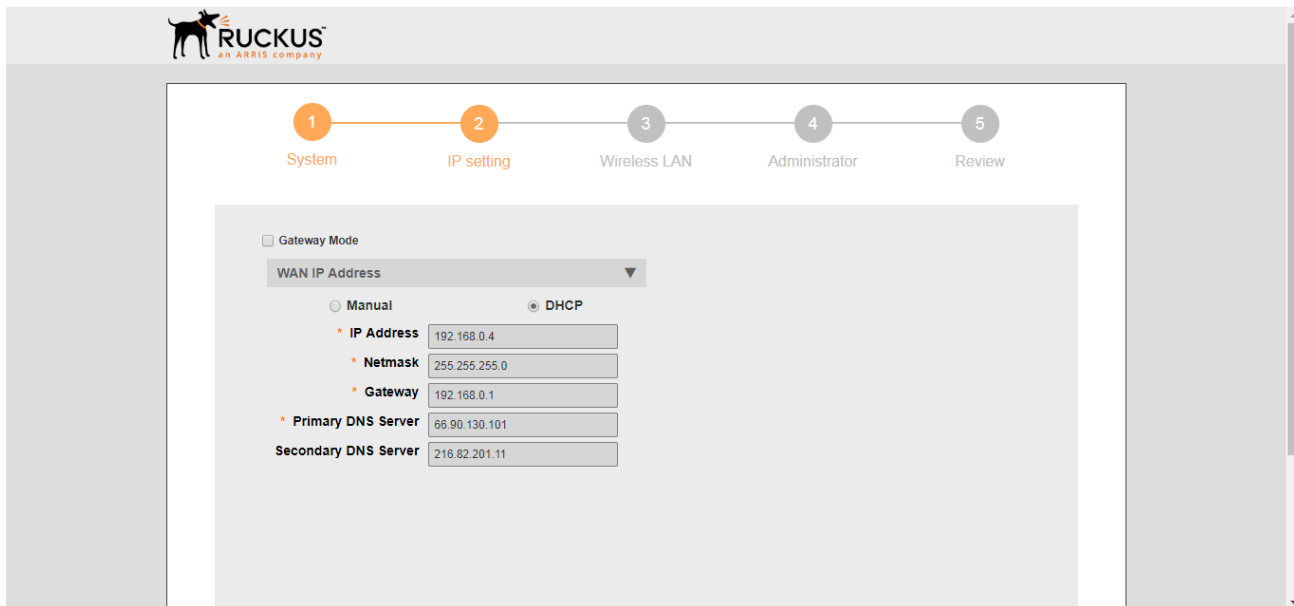
If you plan to manually assign and maintain IP addresses for your wireless network then select **Static (Manual)** and enter your Unleashed Master AP's IP address. Ensure that the IP address is outside the range assigned for Wi-Fi clients. Otherwise, leave the default of Dynamic (DHCP) and let Unleashed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

- j) If you choose Manual, enter an IP Address, Netmask, Gateway address and DNS server(s) 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 Unleashed's own subnet. (For more information, see [DHCP Server](#) on page 281.)

FIGURE 26 Setup Wizard 2



- k) Click **Next** to continue.
- l) On the **Wireless LAN** page, clear the text box and enter a **Name** for your first wireless LAN.
- m) Select an **Encryption Method** (Open or WPA2).

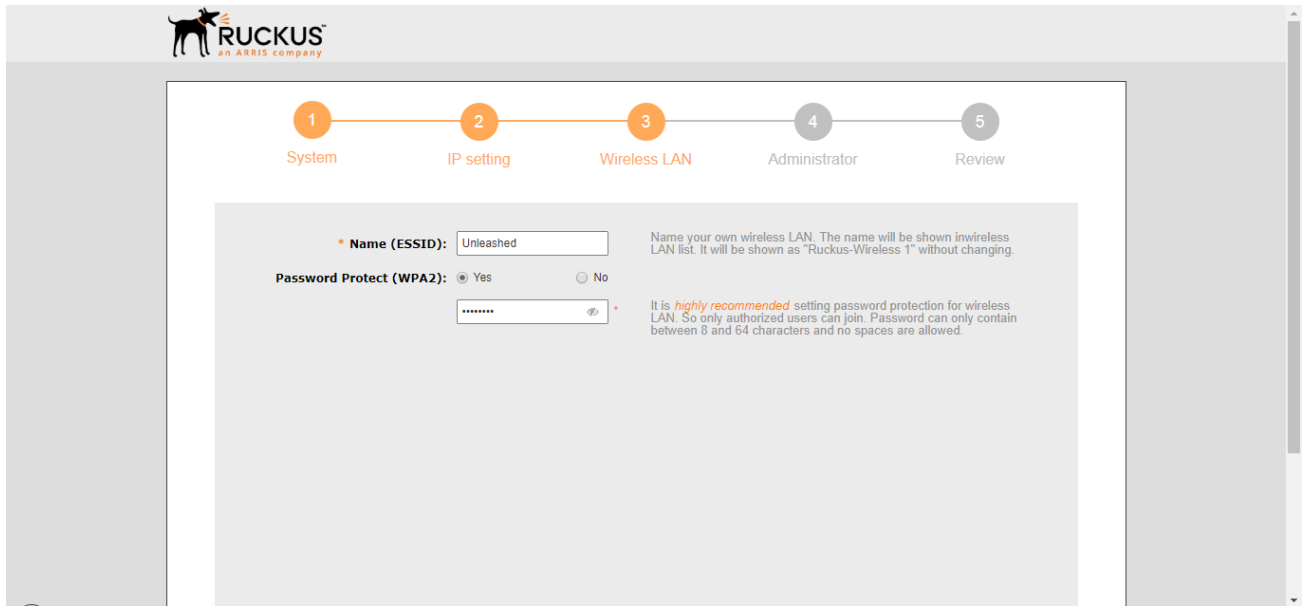
**NOTE**

WPA2 is highly recommend for the highest level of security.

- n) If WPA2 encryption is selected, enter a **Password** consisting of 8-63 alphanumeric characters.
- o) Click **Next** to continue.

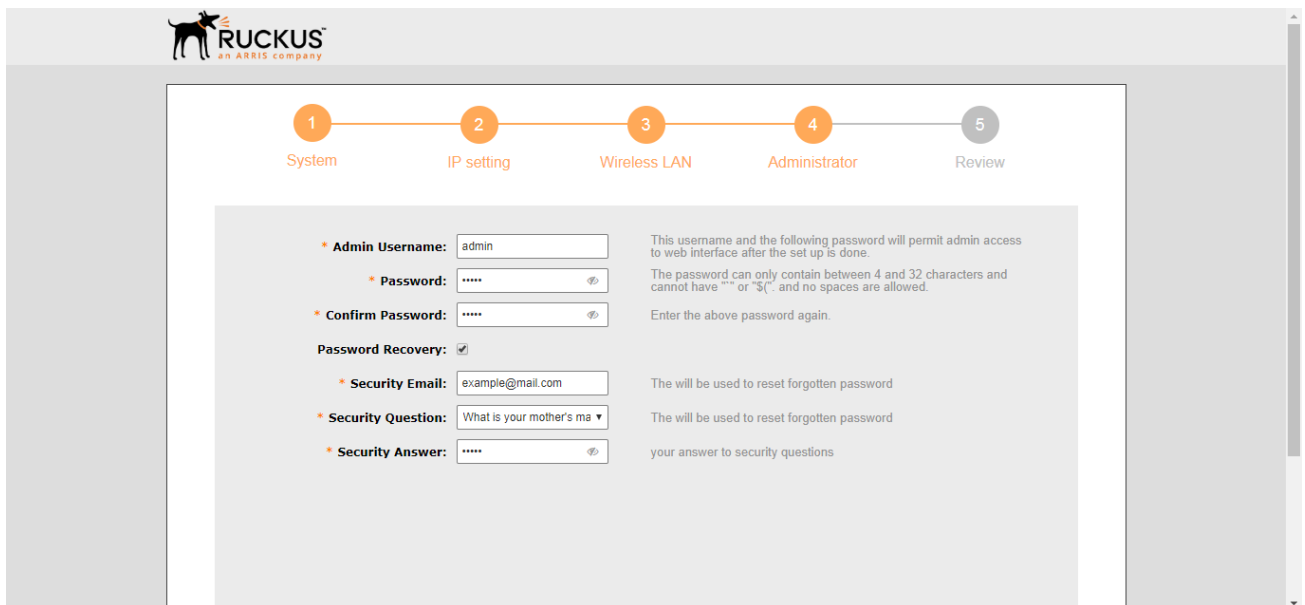


FIGURE 27 Setup Wizard 3



- p) On the **Administrator** page, enter an **Admin Username** and **Password**.
- q) Re-enter the password in **Confirm Password**.
- r) Optionally, enter a **Security Email**, **Security Question** and **Security Answer** to allow you to reset your password in the event that your username or password is forgotten.
- s) Click **Next** to continue.

FIGURE 28 Setup Wizard 4

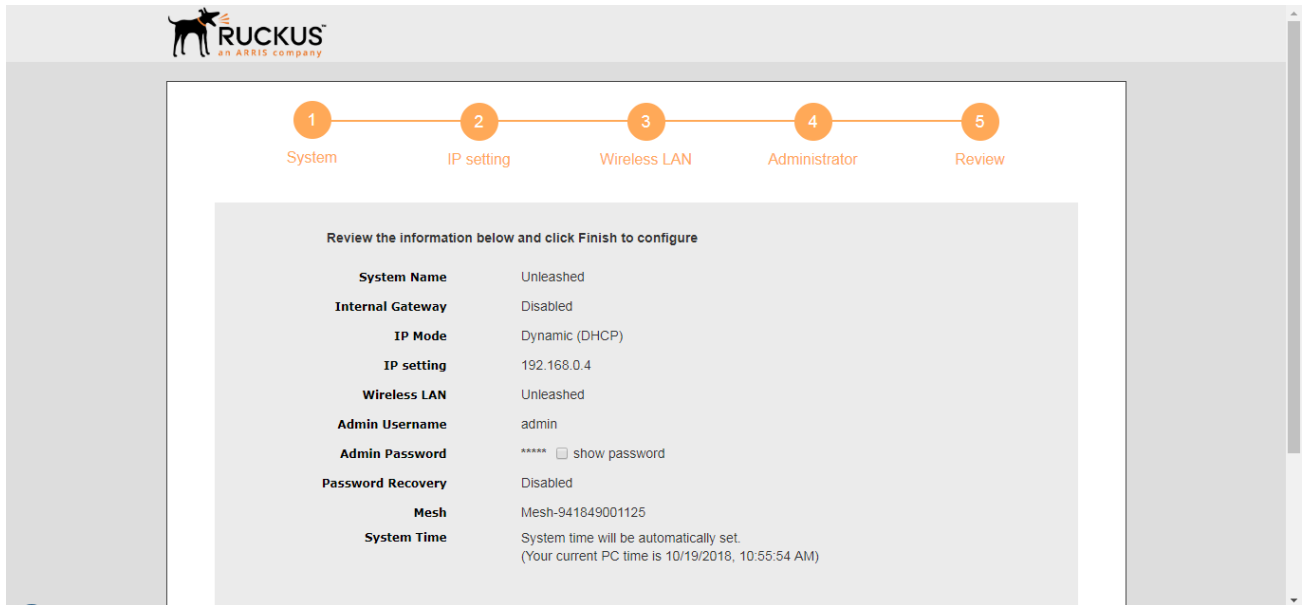


## Setting Up an Unleashed Wi-Fi Network

### Step 2: Configure Your Unleashed Network

- t) On the **Review** page, check that all the settings you have made are correct. If any settings need to be changed, click **Back** to go back to the previous wizard page.
- u) If you are satisfied with your choices, click **Finish** to complete the setup.

**FIGURE 29** Setup Wizard 5

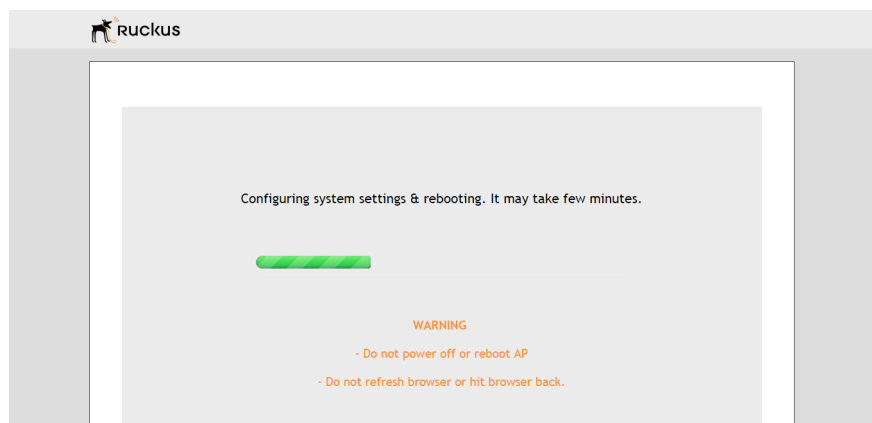


7. After clicking the **Finish** button, the Unleashed Master AP will reboot and a **Configuring system settings & rebooting** page is displayed. Wait for the progress screen to complete before proceeding.

#### NOTE

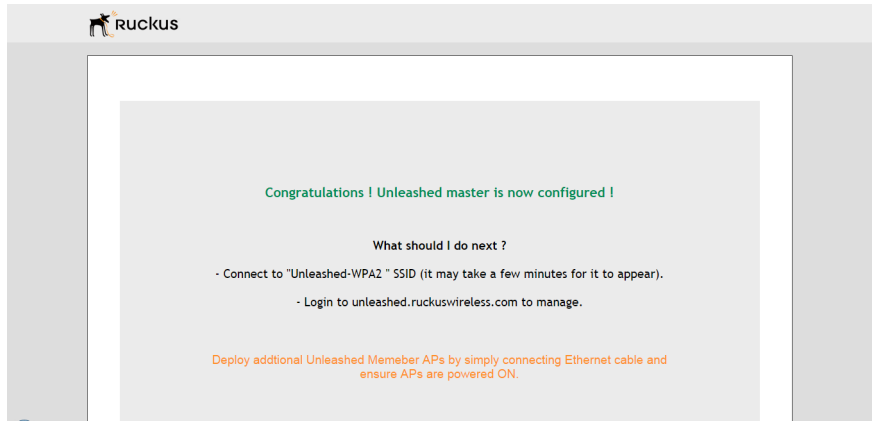
Do not disconnect power or network cables during this process, and do not click your browser's Back or Refresh buttons.

**FIGURE 30** Configuring system settings and rebooting progress screen



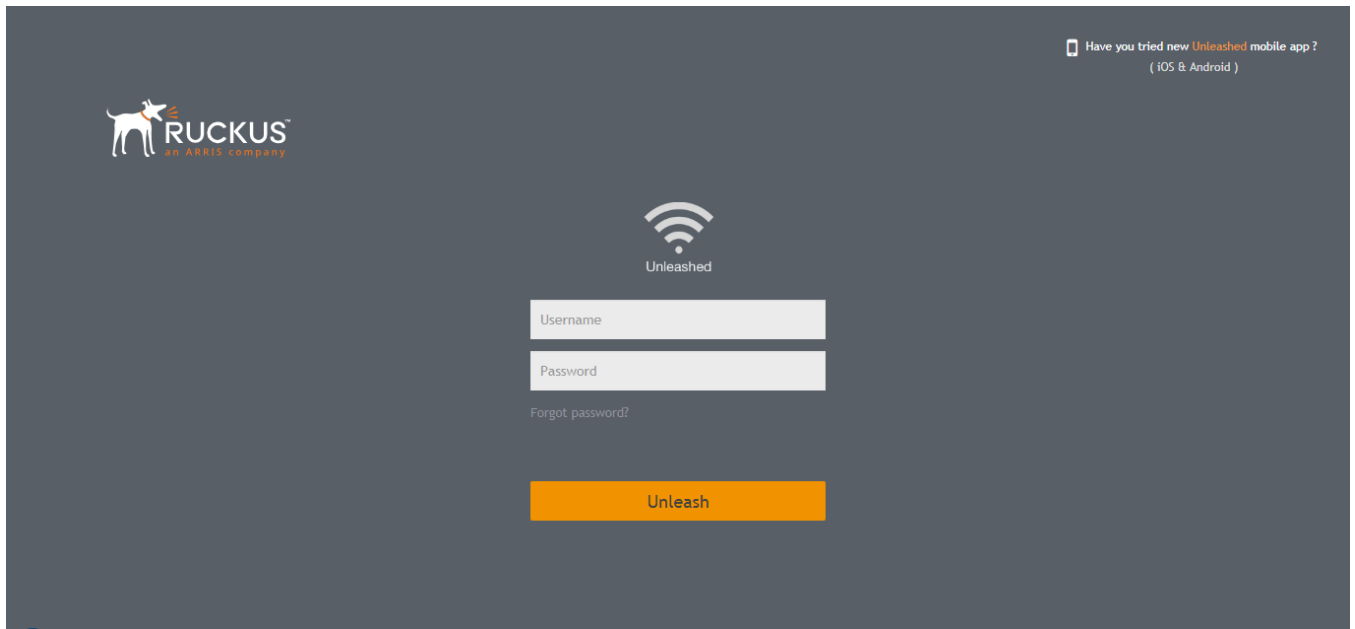
- After setup is complete, the "Congratulations!" screen appears. Ensure that you are connected to the WLAN that you configured, then click **Finish**. You will be redirected to the login page.

**FIGURE 31** "Congratulations! Unleashed Master is now configured" screen



- Enter your **User Name** and **Password**, and click **Unleash** to login.

**FIGURE 32** Login screen

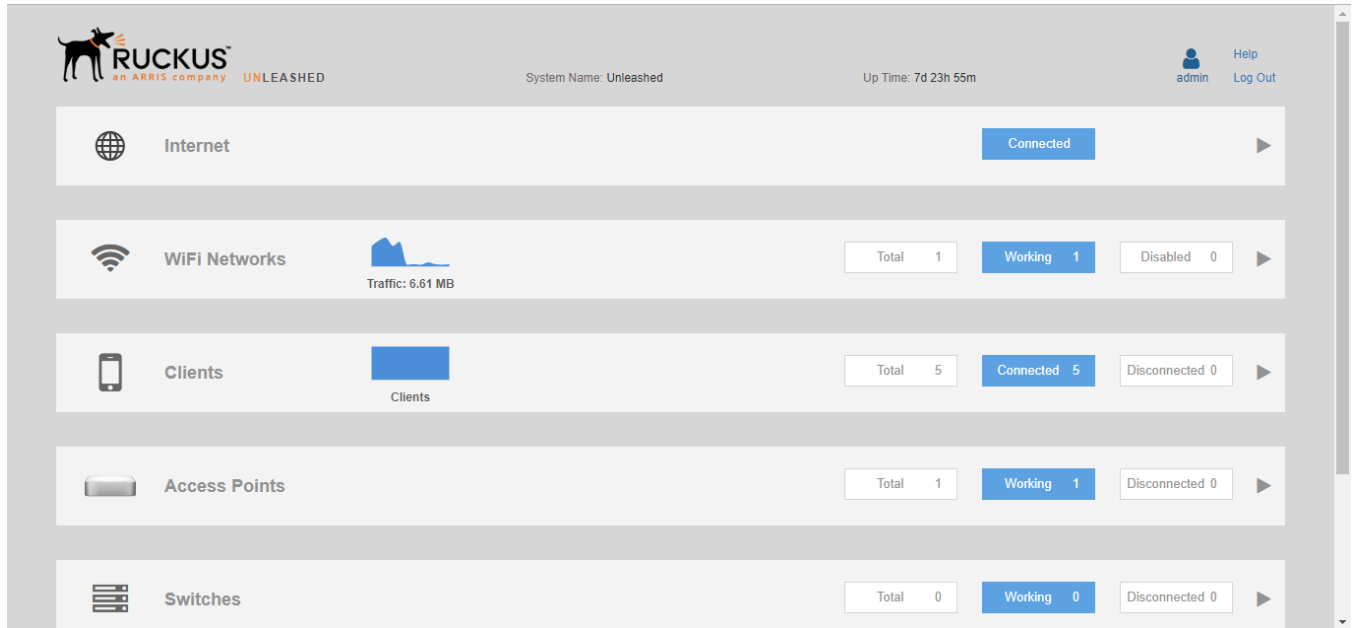


## Setting Up an Unleashed Wi-Fi Network

### Step 2: Configure Your Unleashed Network

10. After successful login, you will be presented with the **Unleashed Dashboard**, which displays an overview of your Ruckus Unleashed network.

**FIGURE 33** The Unleashed Dashboard

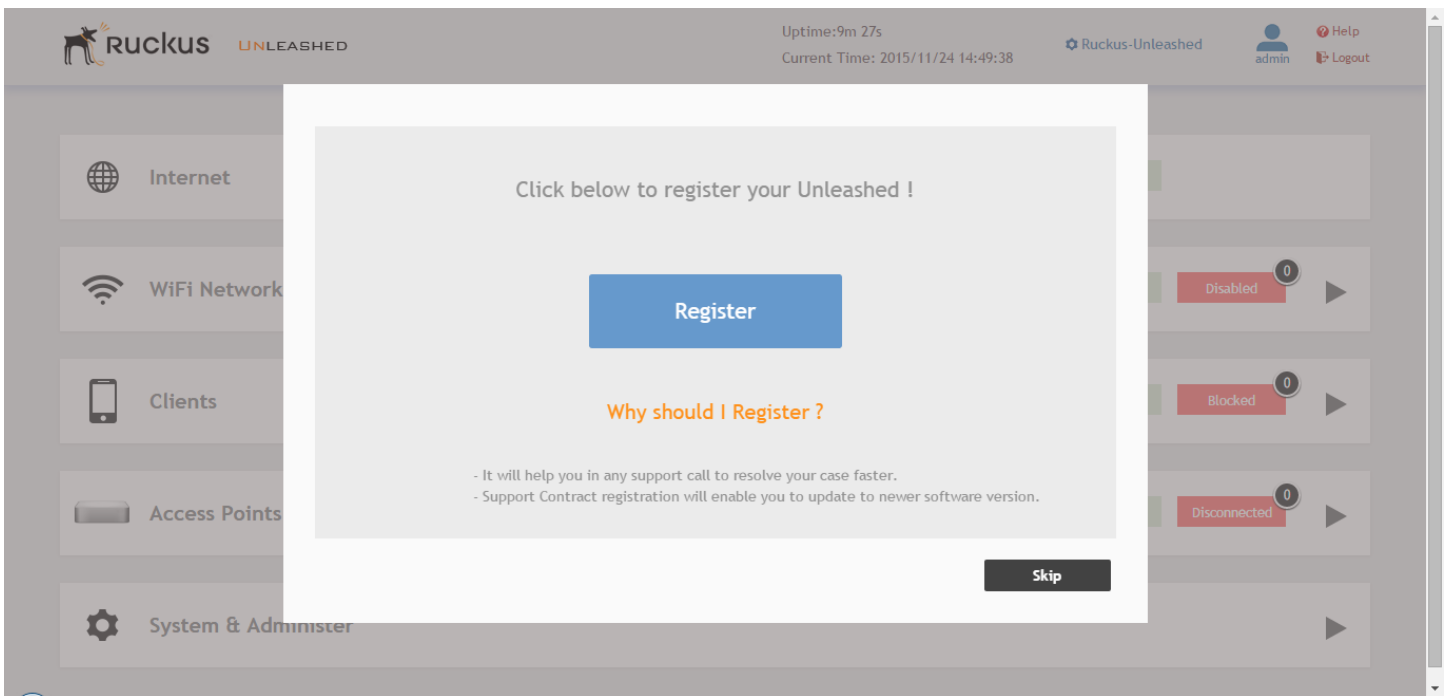


11. Continue to [Step 3: Customize Your Wireless LANs](#) on page 100.

#### **NOTE**

The first time that you log into the Unleashed Admin Interface, you will be presented with a Register screen, prompting you to register your Unleashed Master AP with Ruckus. This registration is optional, and you can skip this step and register later if you prefer. Ruckus recommends that you register your Unleashed APs with us to assist in receiving updates and important notifications, and to make it easier to receive support in case you need to contact Ruckus for customer assistance. See [Registration](#) on page 360 for more information.

**FIGURE 34** The Registration page (optional) appears the first time you log in - Click Register to register now, or click Skip to skip this step and register later.



### **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 first 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.

Setting Up an Unleashed Wi-Fi Network  
Step 2: Configure Your Unleashed Network

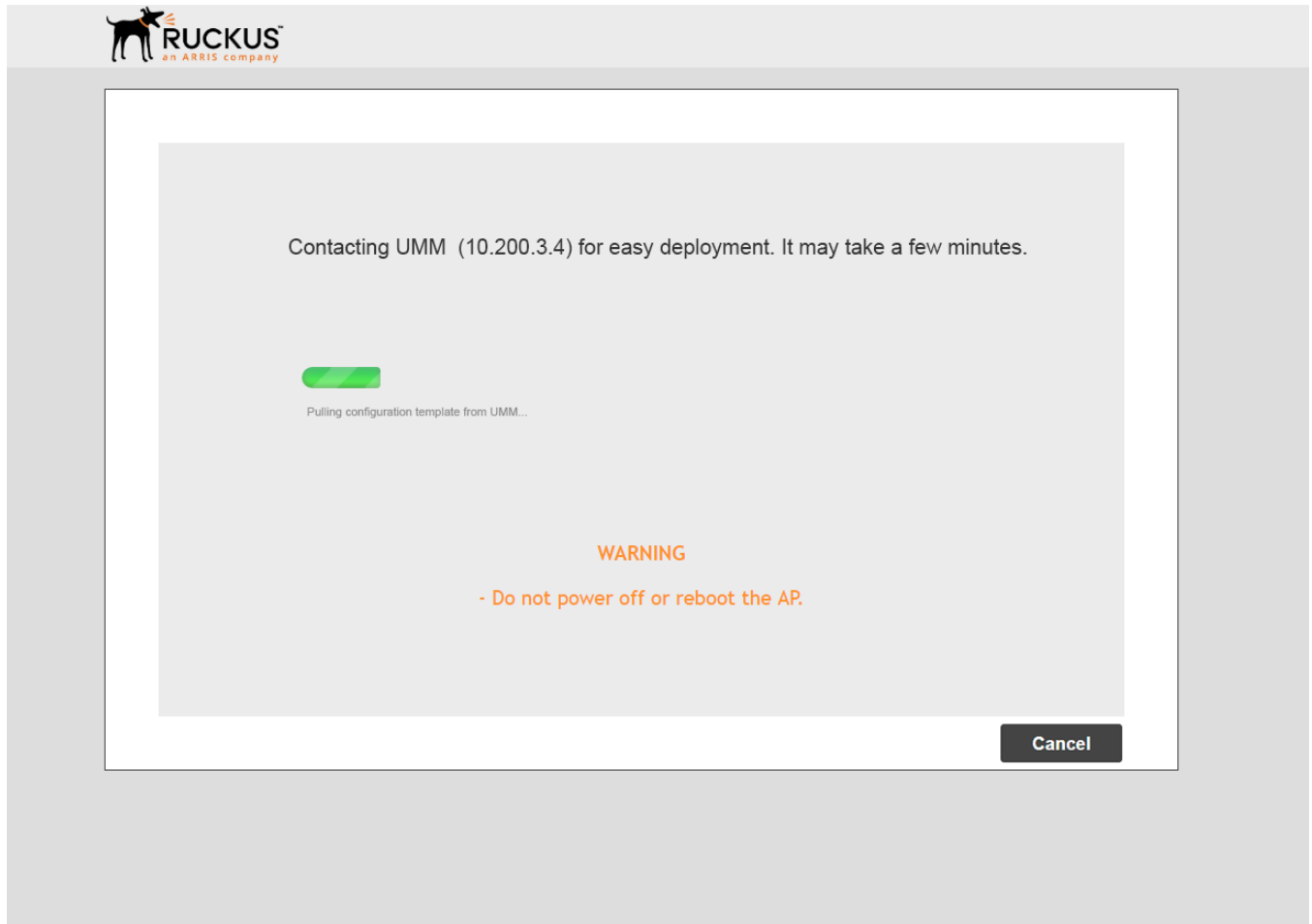
- 5. If successful, the configuration template is pushed to the AP and the Unleashed deployment is configured according to the template.

FIGURE 35 UMM Install

The screenshot shows the 'Unleashed Installation' web interface. At the top left is the Ruckus logo (an orange dog head) and the text 'RUCKUS an ARRIS company'. The page title is 'Unleashed Installation' and the version is '200.8.10.3.143'. The main content area has a light gray background and contains several configuration options:

- Language:** A dropdown menu is set to 'English'. A note says: 'Select the display language that you want to use on the Web interface.'
- Typical Install:** A radio button is unselected. The description is: 'This is the most typical way to install if one do not want to use UMM'.
- UMM Install:** A radio button is selected. The description is: 'Use image from UMM to install an Unleashed network'.
- UMM Domain/IP:** A text input field contains '10.10.13.17'. A note says: 'UMM address from where the Unleashed Network can retrieve configuration'.
- Config Template Name:** A text input field contains 'UMM Template 1'. A note says: 'Configuration template pre-stored in UMM for the Unleashed Network'.
- System Name:** A text input field contains 'Ruckus-Unleashed'. A note says: 'Name your system 32 characters max using alphanumeric characters excluding space.'
- Local Upgrade:** A radio button is unselected. The description is: 'Upgrade this Unleashed AP from a local image file'.

FIGURE 36 Contacting UMM for easy deployment



### **Installation with Local Upgrade**

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

To perform a local upgrade before completing the Unleashed setup:

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

Setting Up an Unleashed Wi-Fi Network  
Step 2: Configure Your Unleashed Network

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

FIGURE 37 Local Upgrade

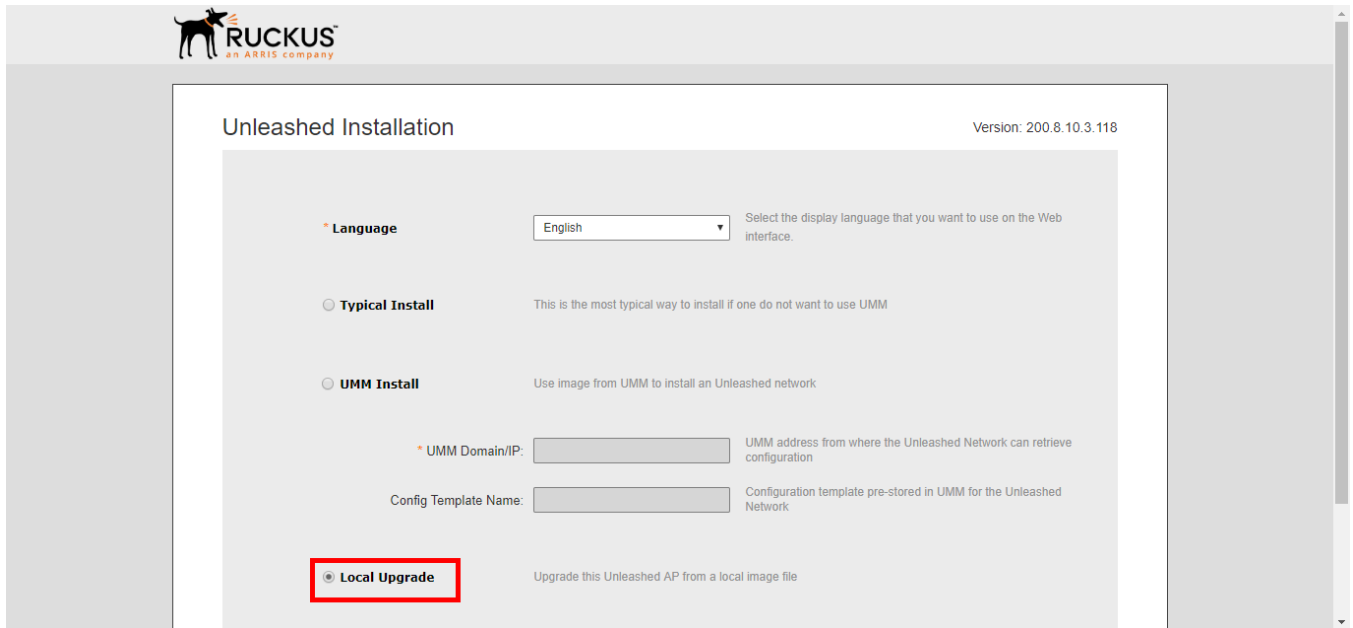
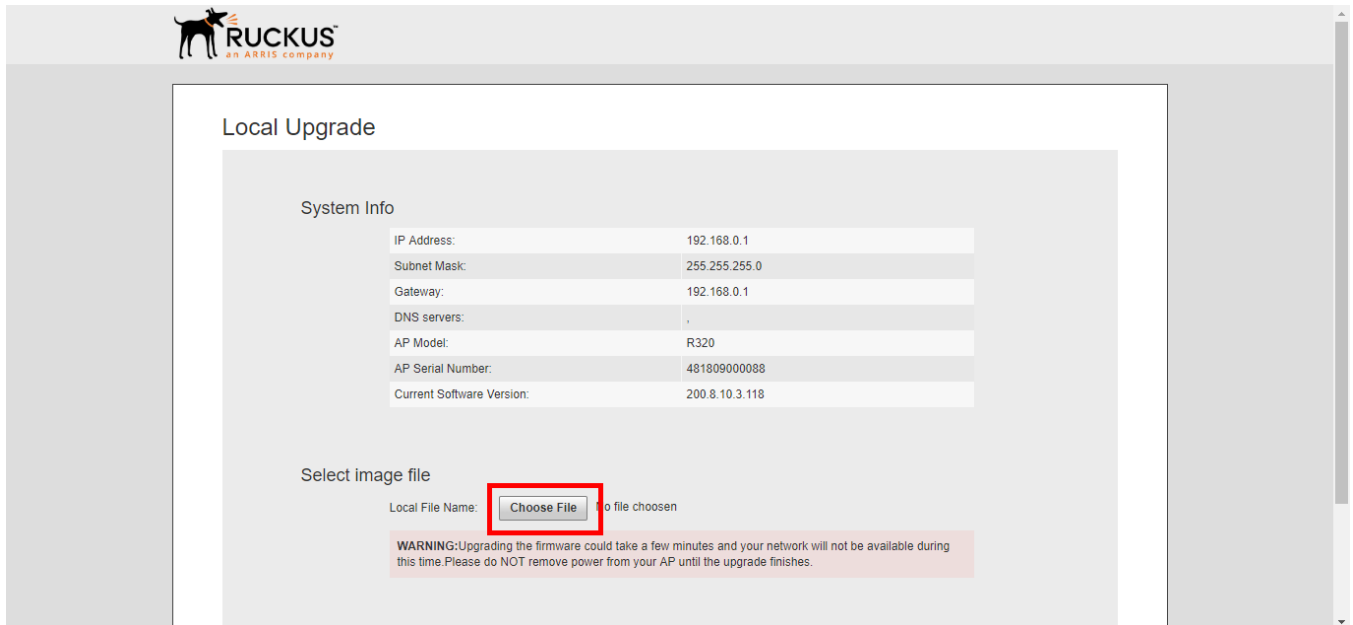


FIGURE 38 Choose local Unleashed image file to upgrade





## 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](http://support.ruckuswireless.com).

The Unleashed CLI Wizard Configuration Tool starts automatically.

## Setting Up an Unleashed Wi-Fi Network

### Step 2: Configure Your Unleashed Network

- 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

Enter WAN IP type [1]:
  1: DHCP Mode;
  2: Manual Mode;
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
IPv4 Mode=             DHCP
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 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

## Setting Up an Unleashed Wi-Fi Network

### Step 3: Customize Your Wireless LANs

```
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

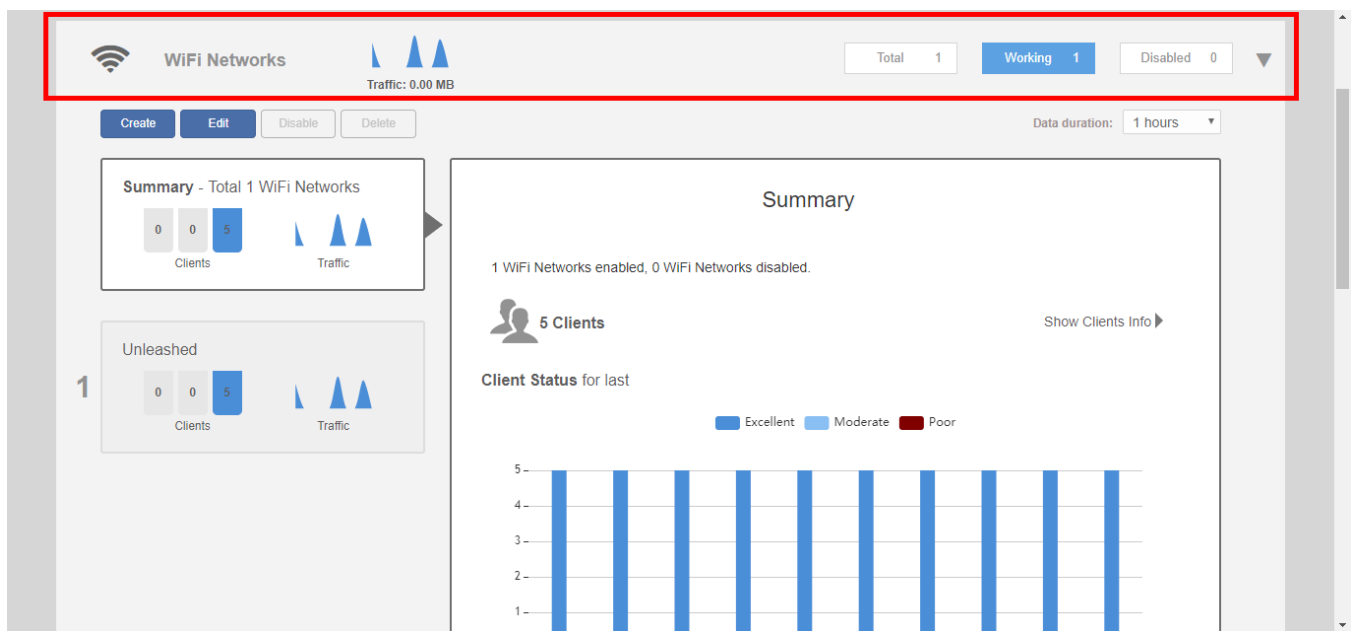
Once the Unleashed Master AP has been initialized, you can fine-tune the settings of your first WLAN (that you created during the setup wizard), and create any additional WLANs needed prior to attaching additional Unleashed member APs.

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:

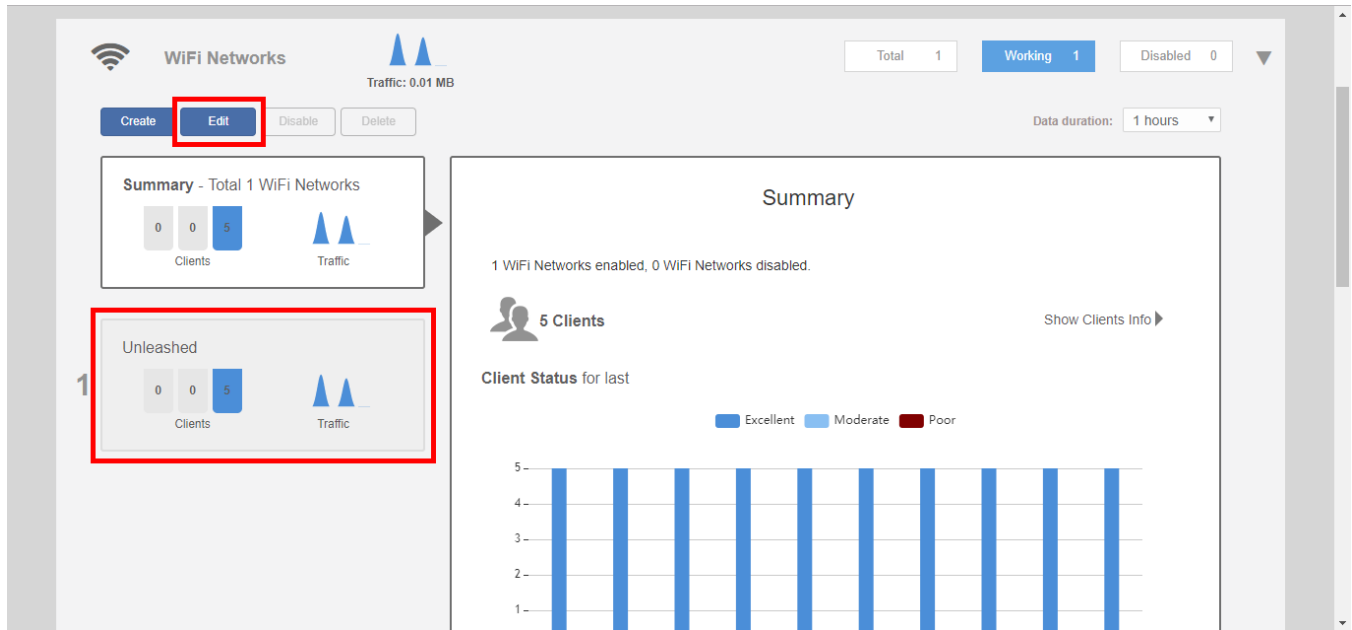
1. From the **Dashboard**, click anywhere in the **Wi-Fi Networks** section to expand the display of your deployed WLANs.

**FIGURE 39** 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 40** 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 802.1X 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 109.

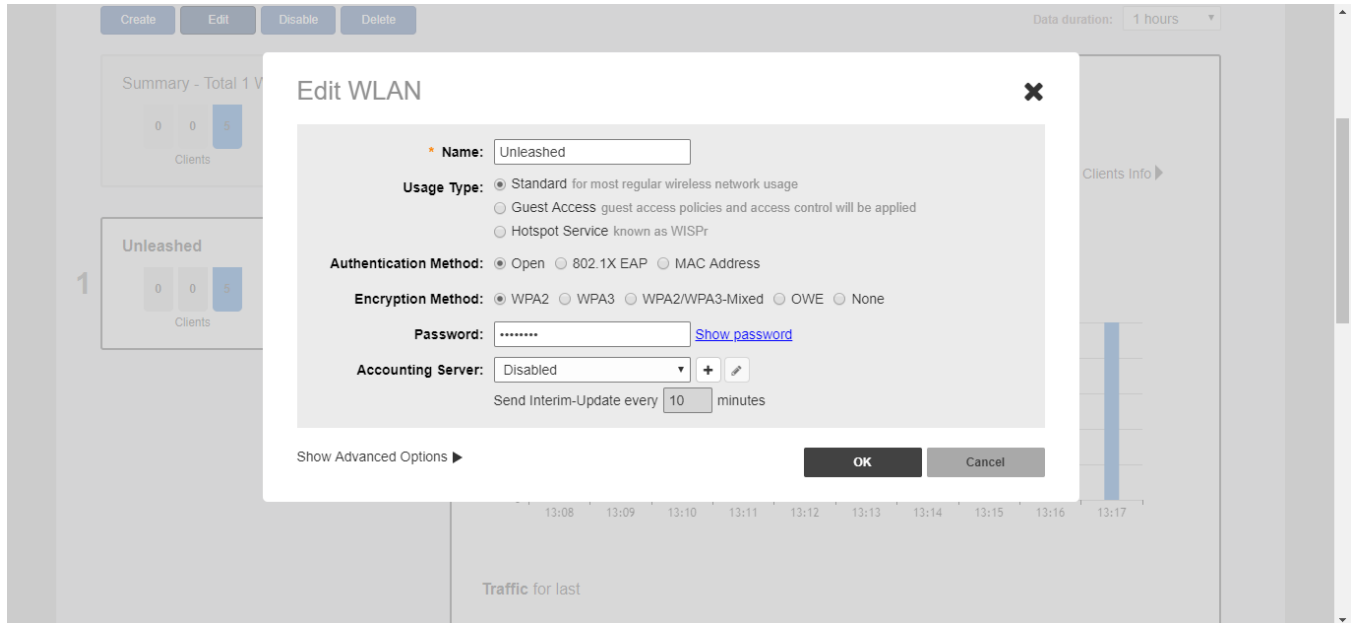
4. Click **OK** to save your changes.

## Setting Up an Unleashed Wi-Fi Network

### Step 4: Deploy Additional Unleashed Member Access Points

- 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 41** Editing an existing WLAN



Congratulations! Your Unleashed network is now configured and ready for use. You may now proceed to [Creating a New WLAN](#) on page 110, or [Step 4: Deploy Additional Unleashed Member Access Points](#) on page 102.

## 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](#)..... 103
- [Navigating the Dashboard](#)..... 103
- [Using the Dashboard Components](#)..... 104

## Unleashed Administration Interface Overview

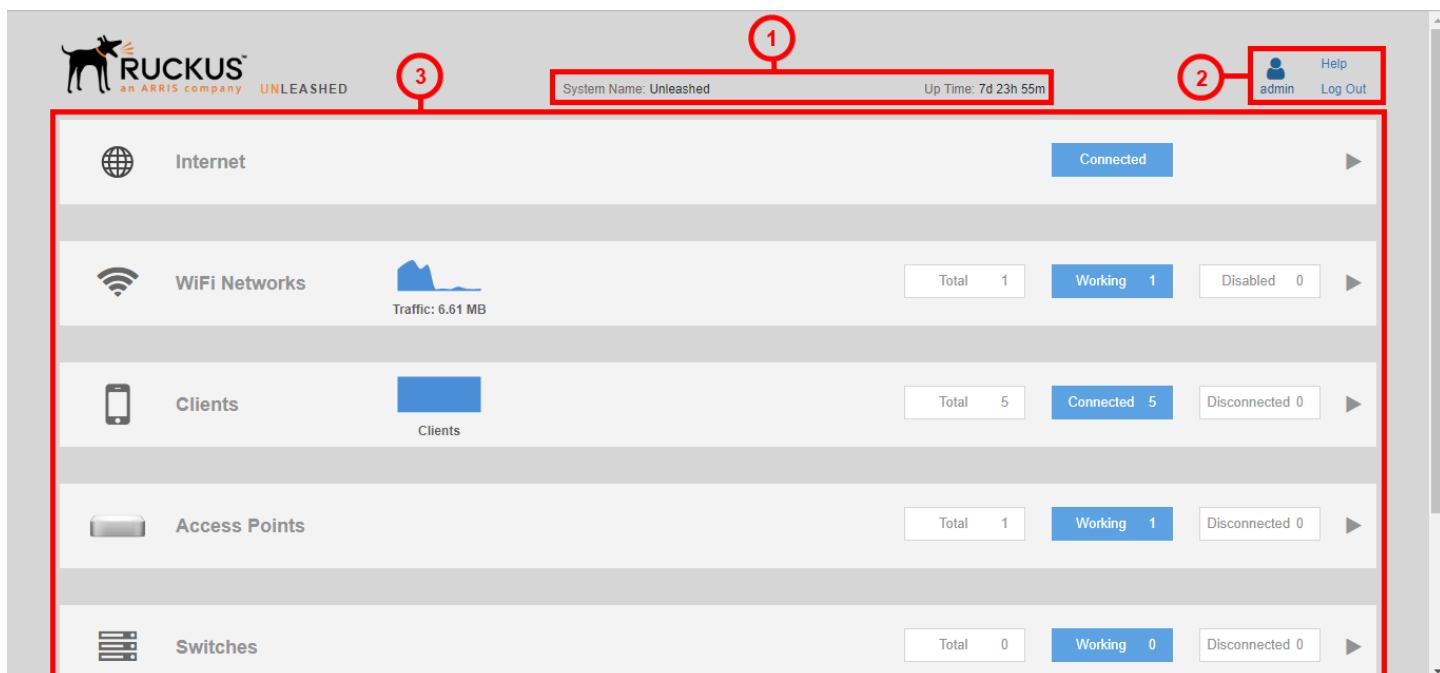
The Unleashed Admin Interface provides tools for use in managing all aspects of your Unleashed deployment.

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 platform's primary interface - used for monitoring and configuring all aspects of your Unleashed network - is called the Dashboard. The Dashboard is divided into three main sections, as shown in the following image. These three main sections and their subsections are described in the table below.

**FIGURE 42** The Dashboard



**TABLE 18** Unleashed Dashboard Components

Number	Component	Description
1	System Name and Uptime	Displays the System Name that you configured and the Uptime since the last reboot.

**TABLE 18** Unleashed Dashboard Components (continued)

Number	Component	Description
2	Admin Info	Displays currently logged in Admin name, a link to this <b>Online Help</b> , and a <b>Logout</b> button.
3	Network Components	These five subsections provide general overviews of each component. Click any of the components to expand the subsection for more detailed information and configuration options. See <a href="#">Using the Dashboard Components</a> on page 104.

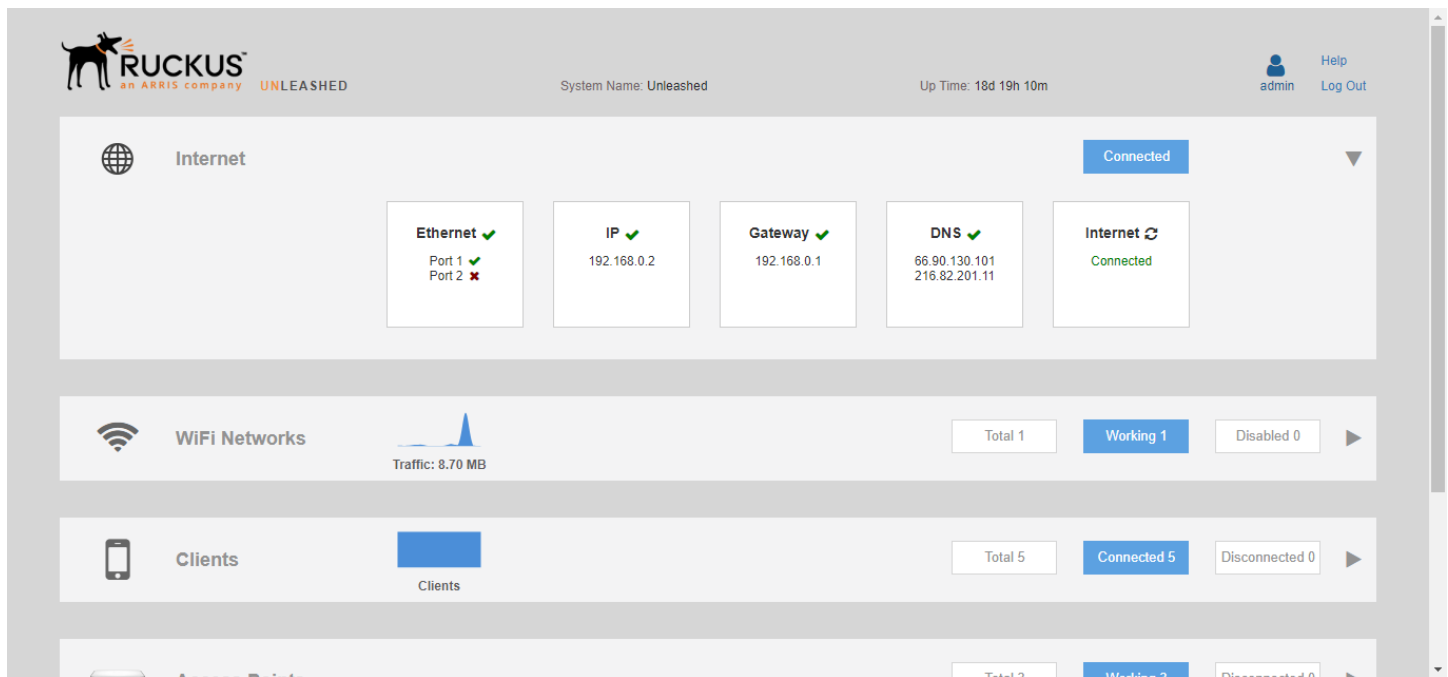
## Using the Dashboard Components

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

### Internet

This component provides details on the Unleashed 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 43** Internet component



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

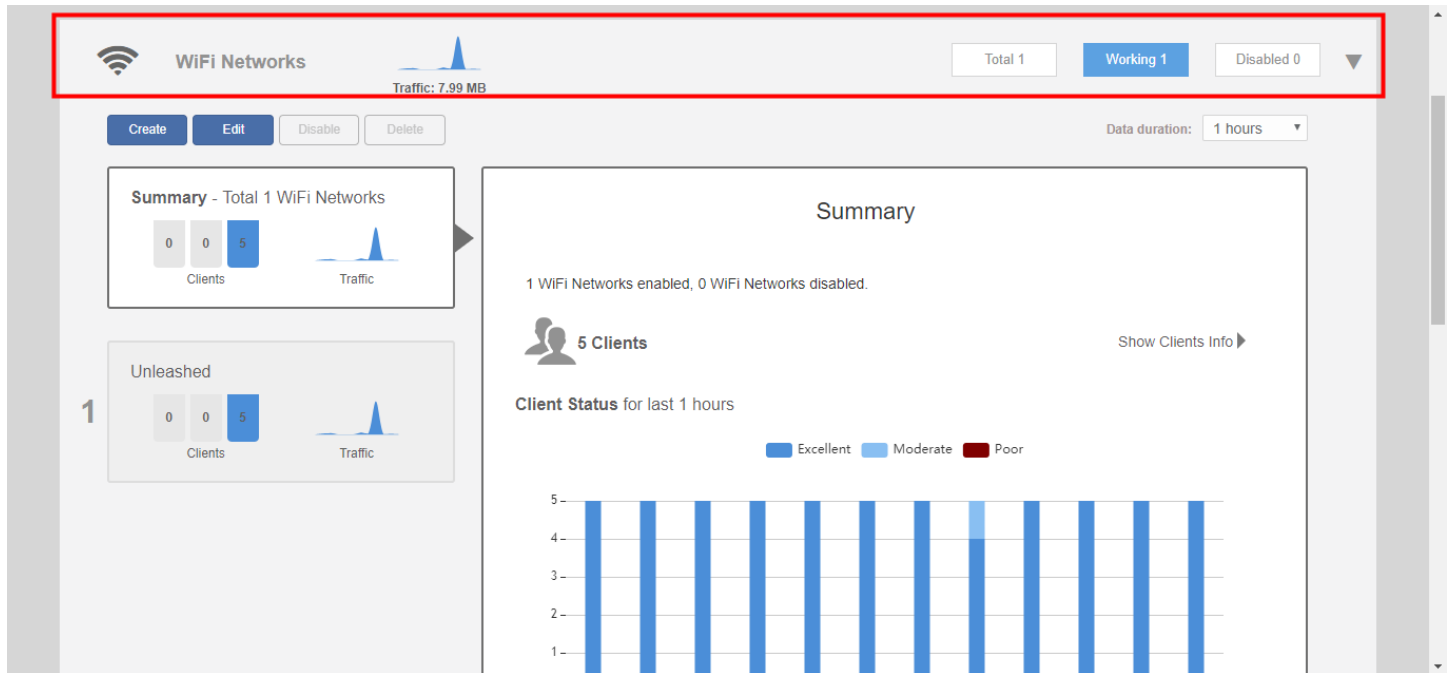
### Wi-Fi Networks

This component displays an overview of the wireless LANs that you have deployed. Its three categories display the numbers of *Total* wireless LANs, the number that are currently in *Working* state, and those that are in *Disabled* state.

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



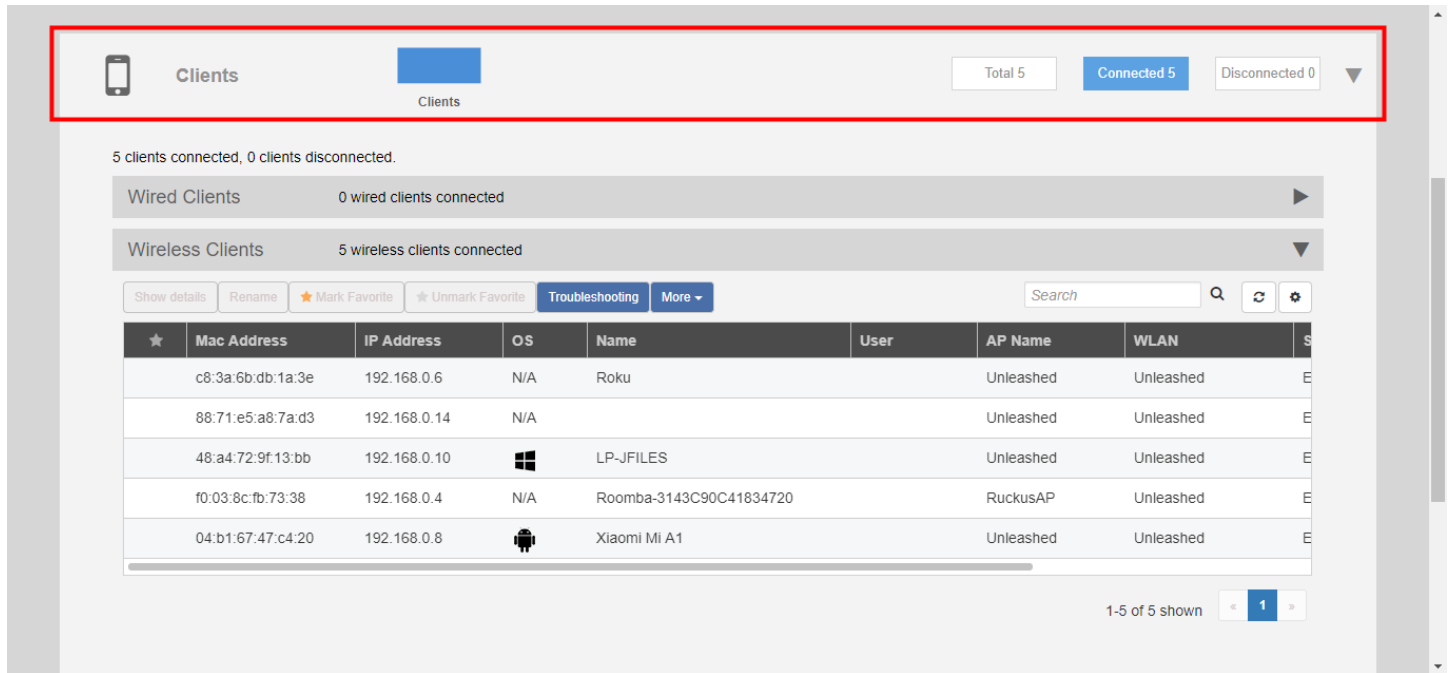
FIGURE 44 Wi-Fi Networks - click the section to display a list of all WLANs



## Clients

The Clients component provides an overview of the number of *Total*, *Connected* and *Blocked* clients. When expanded, 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 45 Clients Component



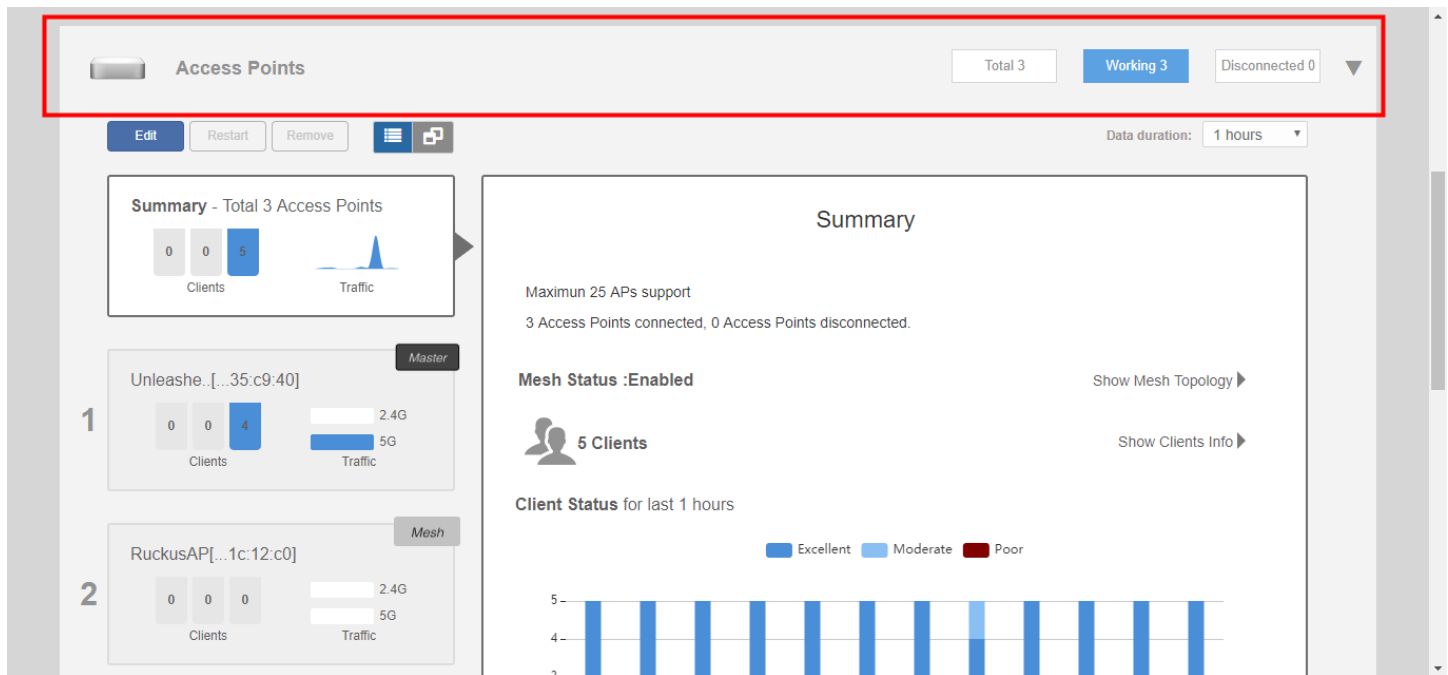
## Access Points

The Access Points component provides an overview of the Unleashed 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.

When the Access Points component is expanded, it displays a list of all of the APs being managed by your Unleashed 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.

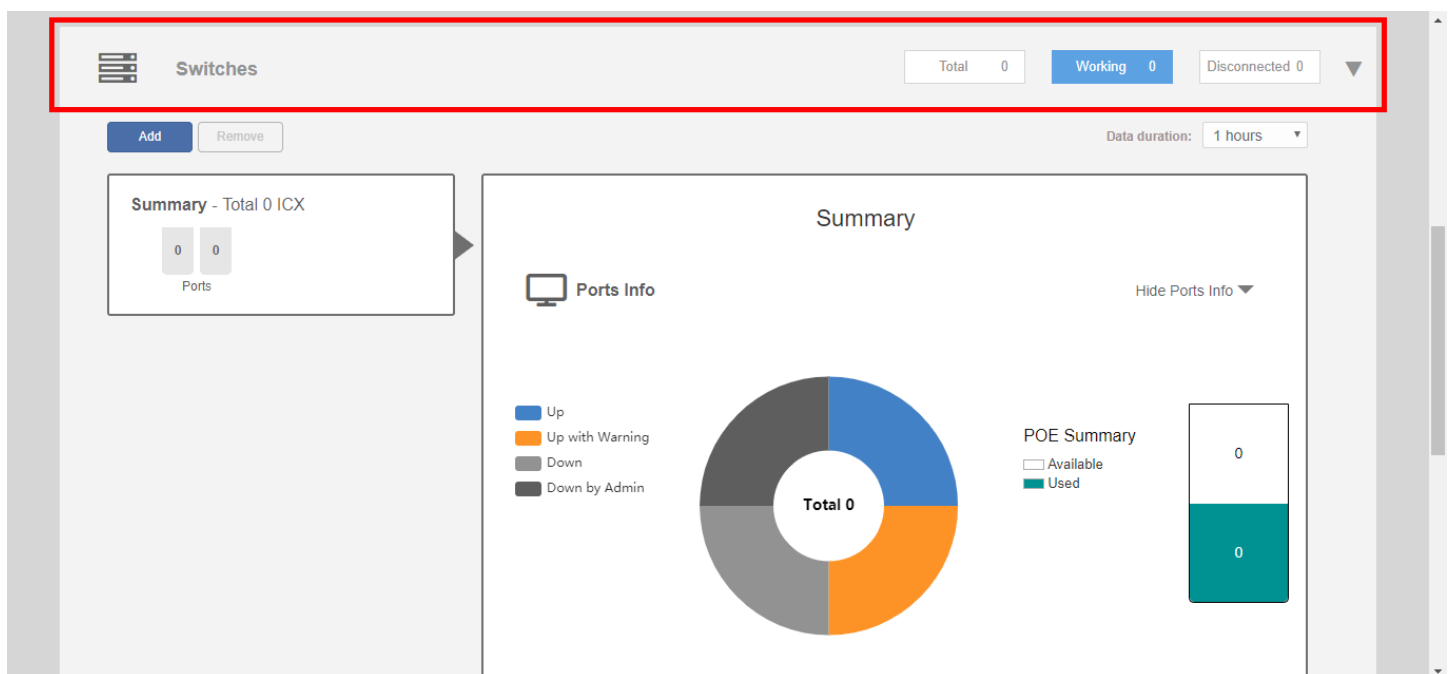
FIGURE 46 Access Points component - click an AP box to display details on that AP



## Switches

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

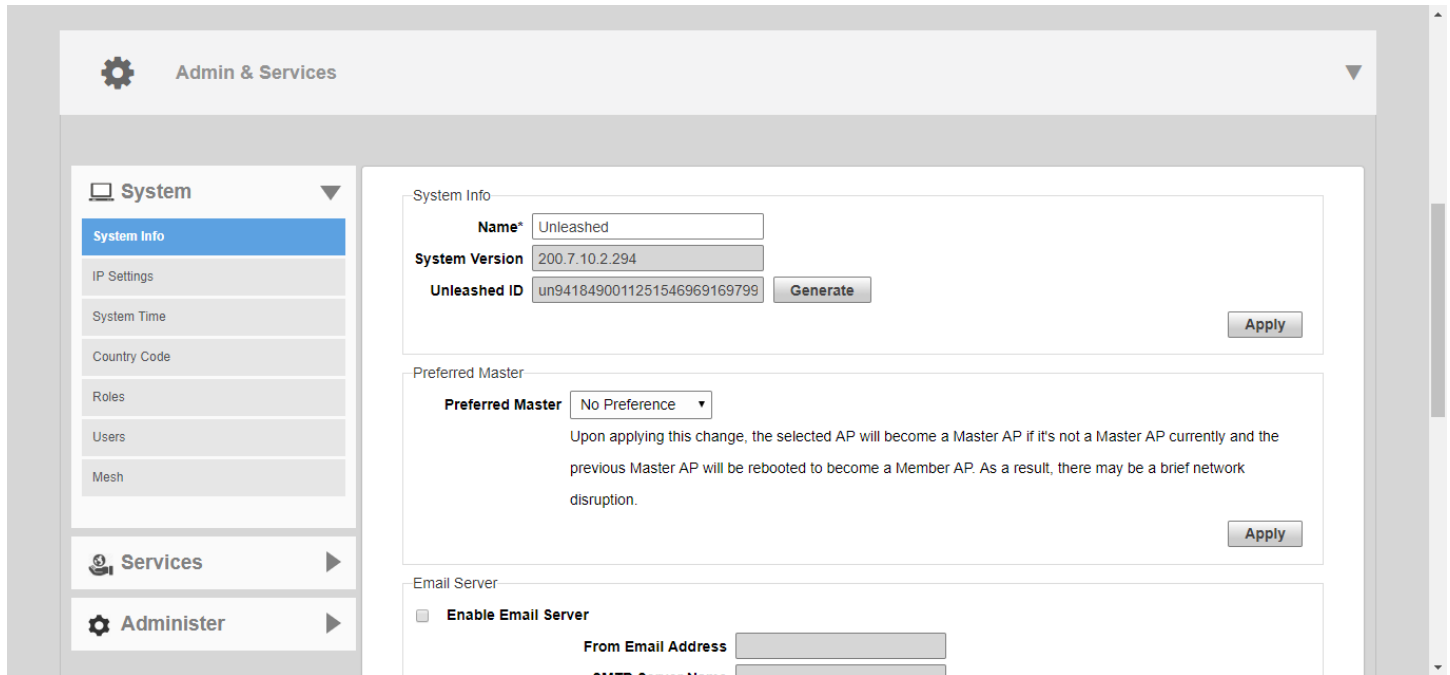
FIGURE 47 Switches component



## 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 (WIPS) services.

FIGURE 48 Admin & Services component



# WLAN Configuration

---

• WLAN Configuration Overview.....	109
• WLAN Usage Types.....	109
• Creating a New WLAN.....	110
• 802.1X EAP WLANs.....	112
• Guest WLANs.....	115
• Hotspot WLANs.....	175
• Configuring Global WLAN Settings.....	176
• Editing an Existing WLAN.....	177
• Deleting a WLAN.....	179
• Temporarily Disabling a WLAN.....	179

## WLAN Configuration Overview

The **Wi-Fi Networks** section of the Dashboard provides tools for managing all aspects of your Unleashed wireless local area networks.

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

## 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 115.
- **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 326.

## Creating a New WLAN

In addition to the initial WLAN you created during the Setup Wizard process, you can create new WLANs using the Wi-Fi Networks Dashboard component.

1. To create a new WLAN, expand the **Wi-Fi Networks** section and click **Create**.

FIGURE 49 Click Create to create a new wireless network

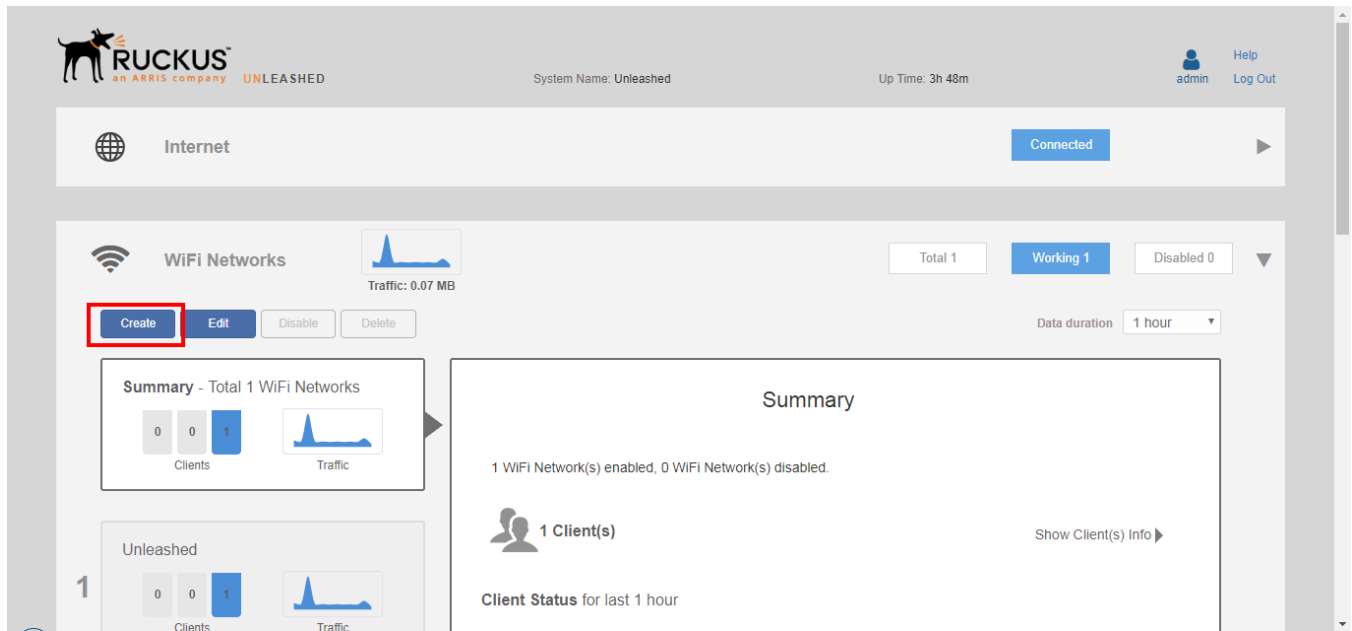


FIGURE 50 Creating a new WLAN



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:** 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 115.

**NOTE**

As of release 200.7, **Social Media** WLANs are a subset of Guest Access WLANs, and are configured using the Guest WLAN settings. Social Media WLANs require the visitor to log in using a social media account before being granted Internet access. For more information, see [Social Media WLANs](#) on page 159.

- **Hotspot Service:** Use this WLAN type for a Hotspot (aka, WISPr) WLAN. To deploy a Hotspot WLAN, you must first configure a Hotspot Service. For more information, see [Hotspot Services](#) on page 326.
4. Select the **Authentication Method** to use:

**NOTE**

Unless using an external authentication server (i.e., 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 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.
- **802.1X EAP:** Authentication 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.
- **MAC Address:** Authentication using the client's MAC address against an external RADIUS server or internal database.

**NOTE**

MAC address authentication using "Local Database" is available as of Unleashed release 200.7.

5. Select the **Encryption Method** to use:
  - **WPA2:** Encrypt 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:** 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) provides encrypted communications for open networks.
  - **None:** No encryption; communications are sent in clear text.
6. Enter a **Password** (WPA2), **SAE Password** (WPA3), or both for a WPA2/WPA3-Mixed WLAN. If the Encryption method is **OWE** or **None**, no password is required.
7. Choose whether a **Captive Portal (Web Authentication)** will be used for web-based authentication.

## WLAN Configuration

### 802.1X EAP WLANs

8. If either 802.1X EAP, MAC Address or Web Auth (Captive Portal) options are chosen, select an **Authentication Server** from the list.
  - a) 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, see [AAA Servers](#) on page 304.

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

#### NOTE

For advanced WLAN configuration options, see [Advanced WLAN Configuration](#) on page 181.

## 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 802.1X 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.

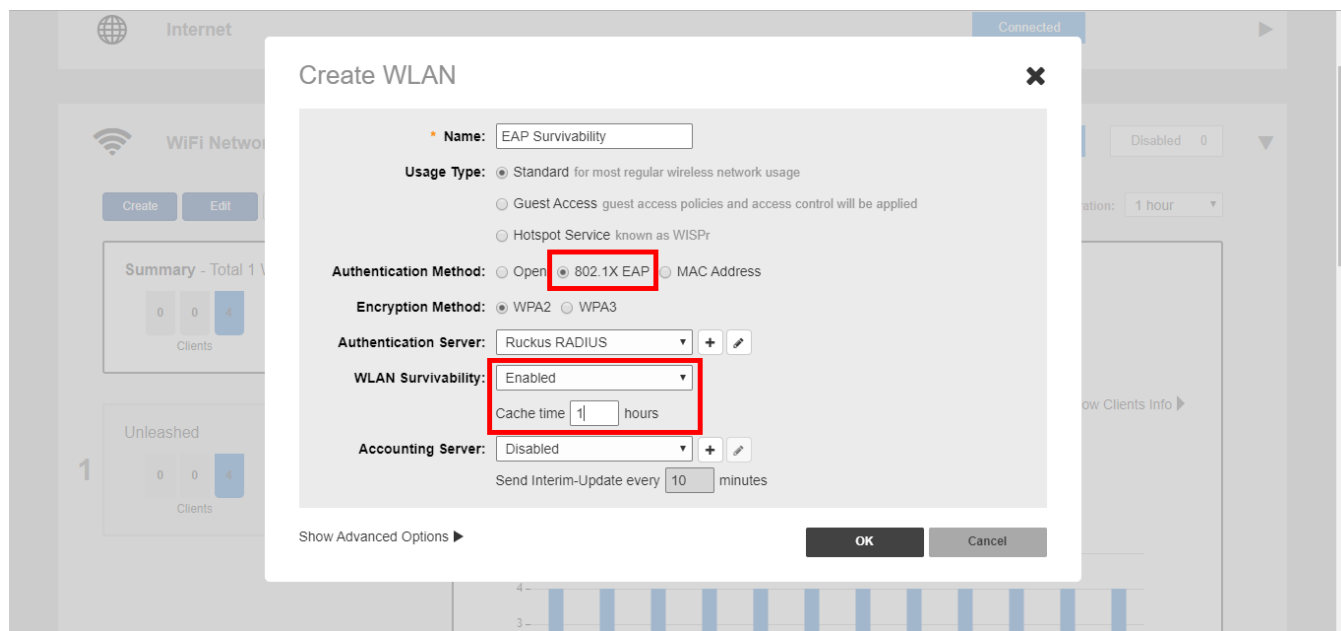
To configure WLAN Survivability for 802.1X WLAN clients:

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 51** 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 via the BYOD Onboarding Portal.

Unleashed provides the following options for different types of Guest WLANs:

- No authentication (open WLAN): Any client can connect, no password is required.
- Social Media Login: Visitors login using 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 admin (guest pass operator), or using the Self-Service Guest Pass feature.
  - Admin generated: Each Guest Pass has to be generated by a guest pass operator.
  - Self-service: 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 via email or SMS.

## Deploying a Guest WLAN

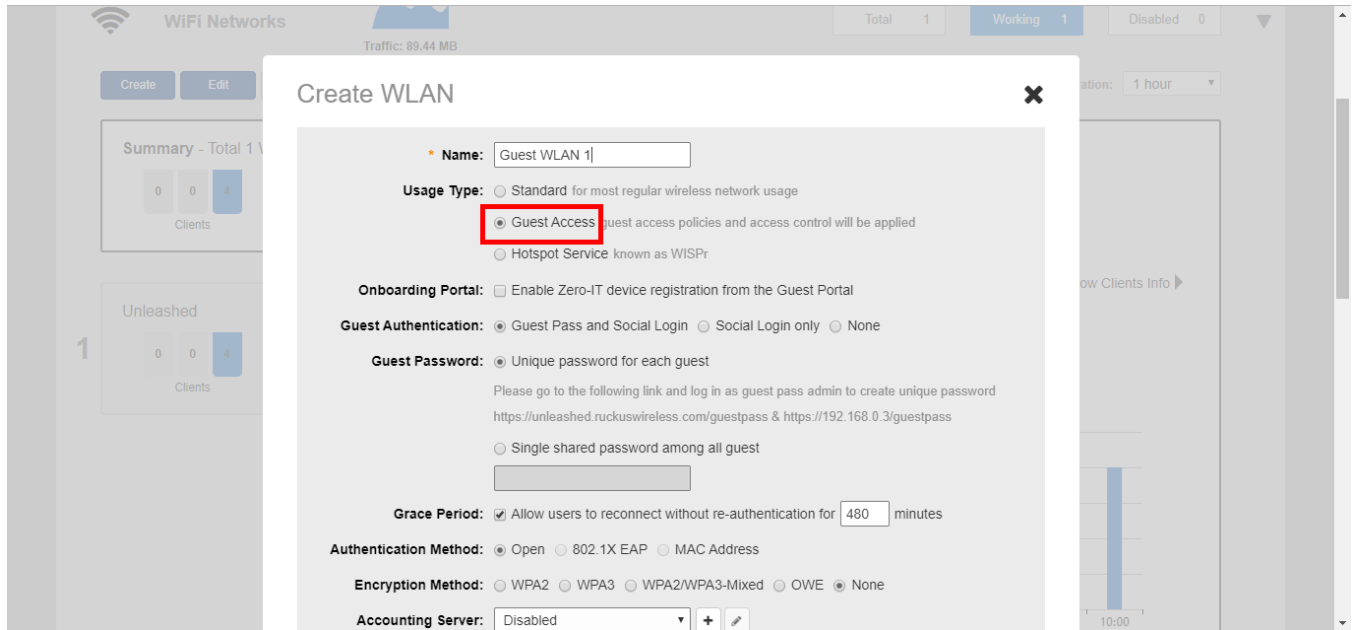
Unleashed provides extensive options for customizing guest wireless networks, both in terms of how users connect, and what access privileges they are given once connected.

To deploy a guest WLAN:

1. Go to **Wi-Fi Networks > Create**.
2. Type a **Name** for the guest WLAN.

3. In **Usage Type**, select **Guest Access**.

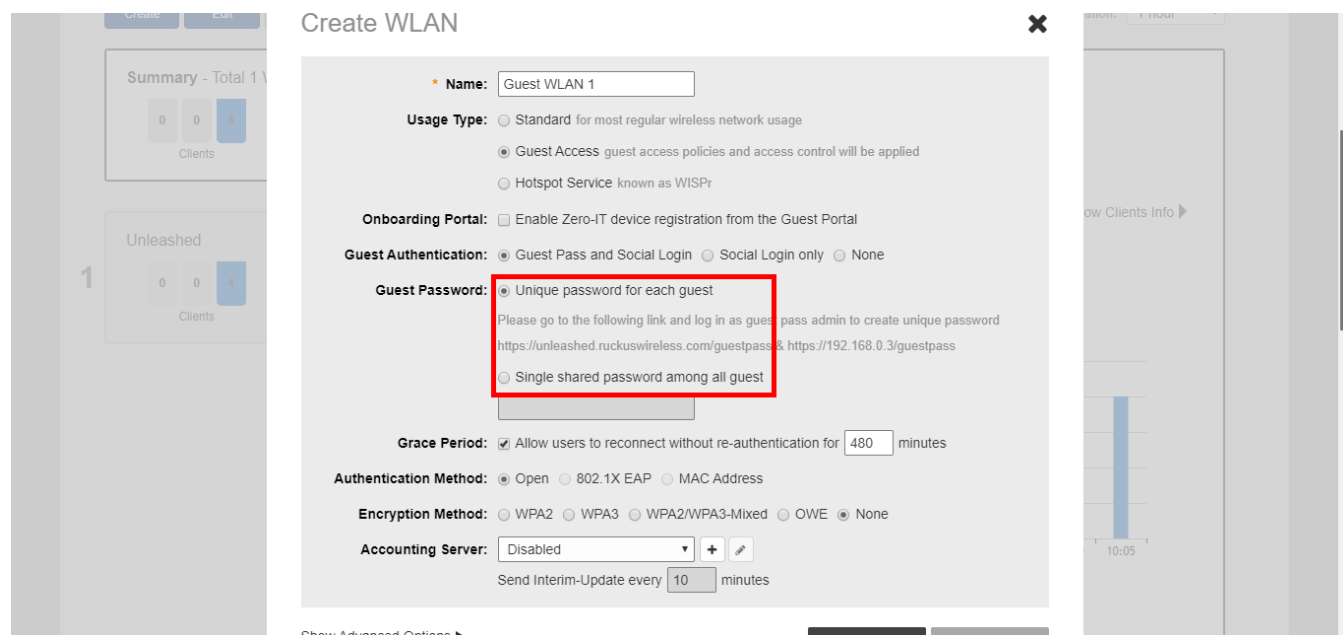
**FIGURE 52** Create a new Guest WLAN



4. In **Onboarding Portal**, choose whether to allow guests the option to register their devices on your internal (non-guest) WLANs using the Onboarding Portal. For more information, see [Using the BYOD Onboarding Portal](#) on page 127.
5. In **Guest Authentication**, choose whether to allow social media login or guest pass and social media login, or to allow anyone to connect with no password required ("None" authentication).

6. In **Guest Password**, if you selected **Guest Pass and Social Login** in the previous step, choose one of the following:
- **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, see [Working with Guest Passes](#) on page 133.
  - **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 53** Select single shared password among all guests or unique password for each guest



7. In **Grace Period**, enter a value in minutes to allow users to reconnect without re-authentication. Clear the check box to disable the grace period.
8. In **Authentication Method**, select one of the following:
- **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.
9. In **Encryption Method**, select one of the following:
- **WPA2:** Encrypt 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) provides encrypted communications for open networks.
  - **None:** No 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.)
10. In **Accounting Server**, select an AAA server from the list or click the + icon to create a new RADIUS Accounting server entry.
11. Optionally, click **Show Advanced Options**, and configure any advanced options, such as restricted subnet access, WLAN priority, access controls, application visibility, etc. See [Advanced WLAN Configuration](#) on page 181 for more information.
12. Click **Next**.

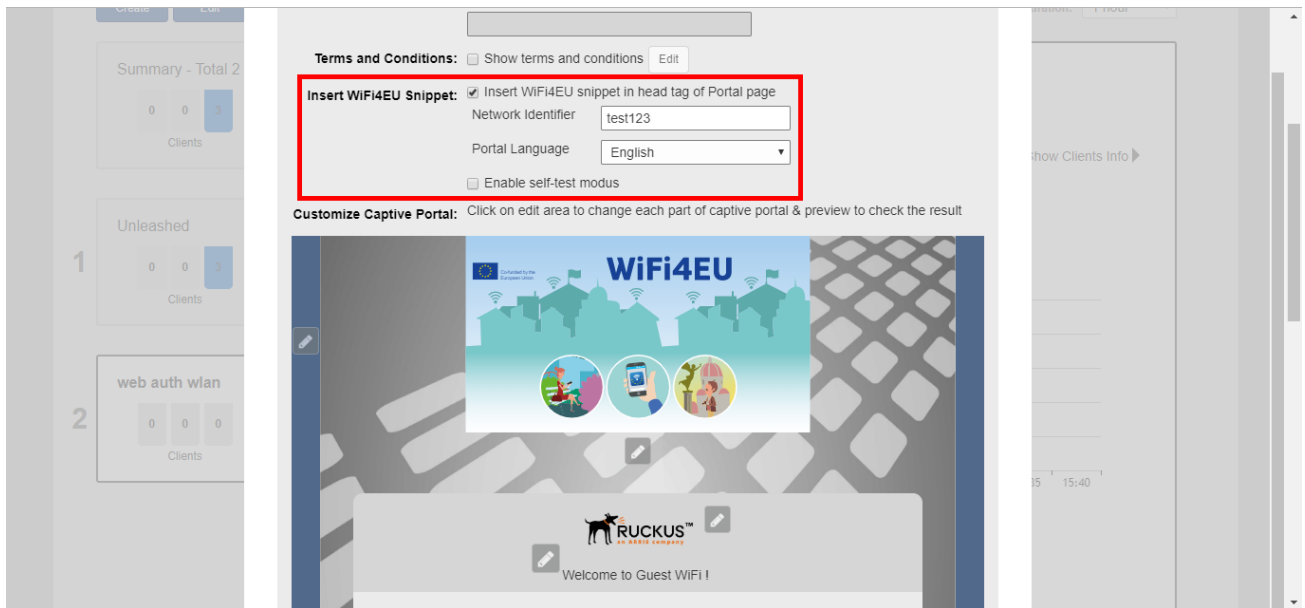
13. On the next screen customize the guest WLAN by configuring social media login options, guest pass self-service, redirection, terms and conditions and captive portal appearance.

FIGURE 54 Create Guest WLAN - page 2



- **Social Media Login(s):** Allow users to log in using their social media accounts. See [Social Media WLANs](#) on page 159.
- **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, see [Guest Pass Self-Service](#) on page 133.
- **Validity Period:** Choose whether the guest passes will be **effective from first use** or **effective from creation time**, and enter a value for **Expire new guest passes if not used within \_\_\_ days** if the **effective from first use** option is selected.
- **User Redirection URL:** Choose whether to redirect the user to the original website he/she wanted to visit after successful login, or to redirect to a URL you specify in the **Redirect user to this website** 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.
- **Insert WiFi4EU Snippet:** Insert WiFi4EU snippet in head tag of web auth portal page. This allows the WLAN to be used by members of the WiFi4EU "digital single market" for EU member states.

FIGURE 55 Insert WiFi4EU snippet

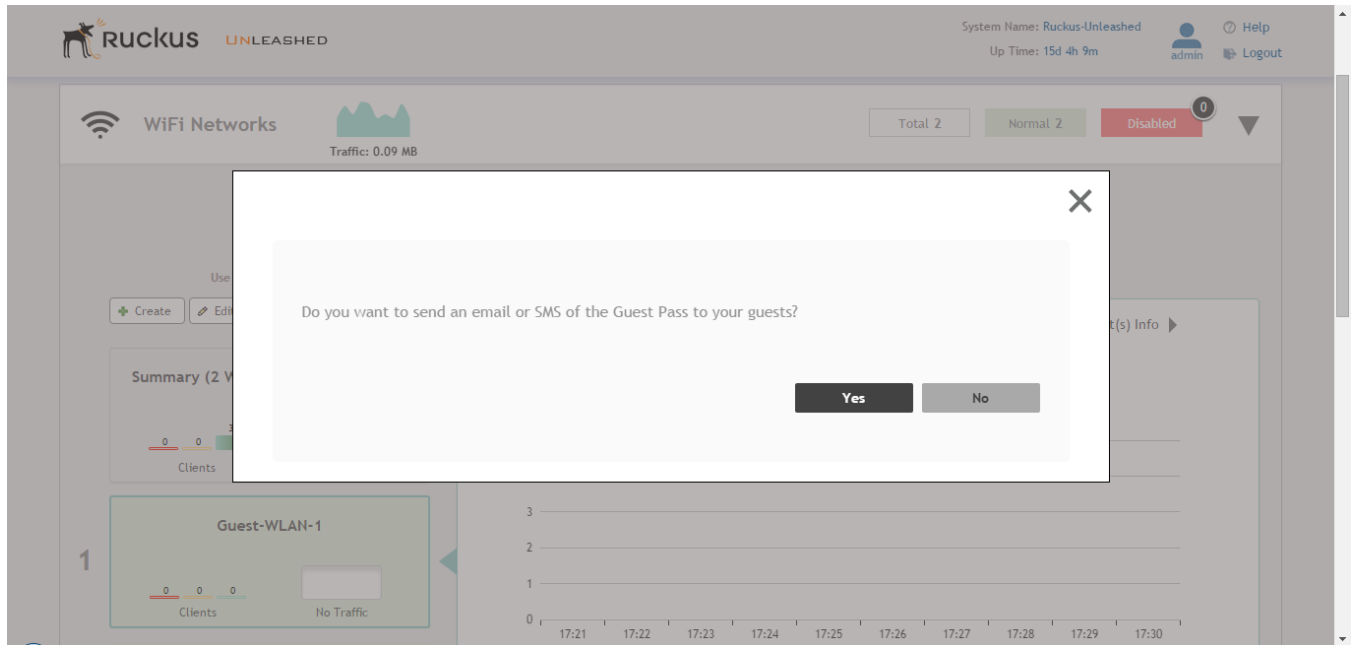


- **Customize Captive Portal:** Customize the banner, background image, background color, logo, welcome message, and opacity level. Click **Preview** to preview your changes.

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

15. 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** pages, if you prefer. See [Configuring Email Server Settings](#) on page 120 for more information.

**FIGURE 56** Continue to configure email and SMS delivery settings



16. Continue to [Configuring Email Server Settings](#) on page 120.

### **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 57** Email Server settings

The screenshot displays the configuration page for the Email Server. On the left, a sidebar contains navigation options: 'Country Code', 'Roles', 'Users', 'Mesh', 'Services', and 'Administration'. The main panel is divided into sections. The top section, 'Preferred Master', has a dropdown menu set to 'No Preference' and a warning message about network disruption upon applying changes, with an 'Apply' button. Below this is another 'Preferred Master' section with a checked 'Enable Email Server' option. This section contains several input fields: 'From Email Address' (test@example.com), 'SMTP Server Name' (smtp.example.com), 'SMTP Server Port' (587), 'SMTP Authentication Username' (username), 'SMTP Authentication Password' (masked with dots), and 'Confirm SMTP Authentication Password' (masked with dots). A blue link for 'SMTP Encryption Options' is located below the password fields. At the bottom right of this section are 'Test' and 'Apply' buttons. The bottom section, 'SMS Settings', has a checked 'Enable SMS Server' option and a checked 'Country Code' option. It also includes radio button options for default settings and a partially visible 'Twilio account information' section.

## 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 58 Configuring SMS settings

The screenshot shows the 'SMS Settings' configuration page. At the top, there is a section for 'SMTP Encryption Options' with 'Test' and 'Apply' buttons. Below this, the 'SMS Settings' section is expanded. It features a checked 'Enable SMS Server' checkbox. Under 'Country Code', there are three radio button options: 'No default and ask user to input' (selected), 'Use default +12 and allow user to change', and 'Use default +12 and disallow user to change'. The 'Twilio account information' section includes input fields for 'Account SID', 'Auth Token', and 'From PhoneNumber', with a '[register a new Twilio account]' link. The 'Clickatell account information' section includes input fields for 'User Name', 'Password', 'API Id', and 'From PhoneNumber', with a '[register a new Clickatell account]' link. The 'Customized Server' section has a 'Method' dropdown menu set to 'GET' and a large text area for the 'URL'.

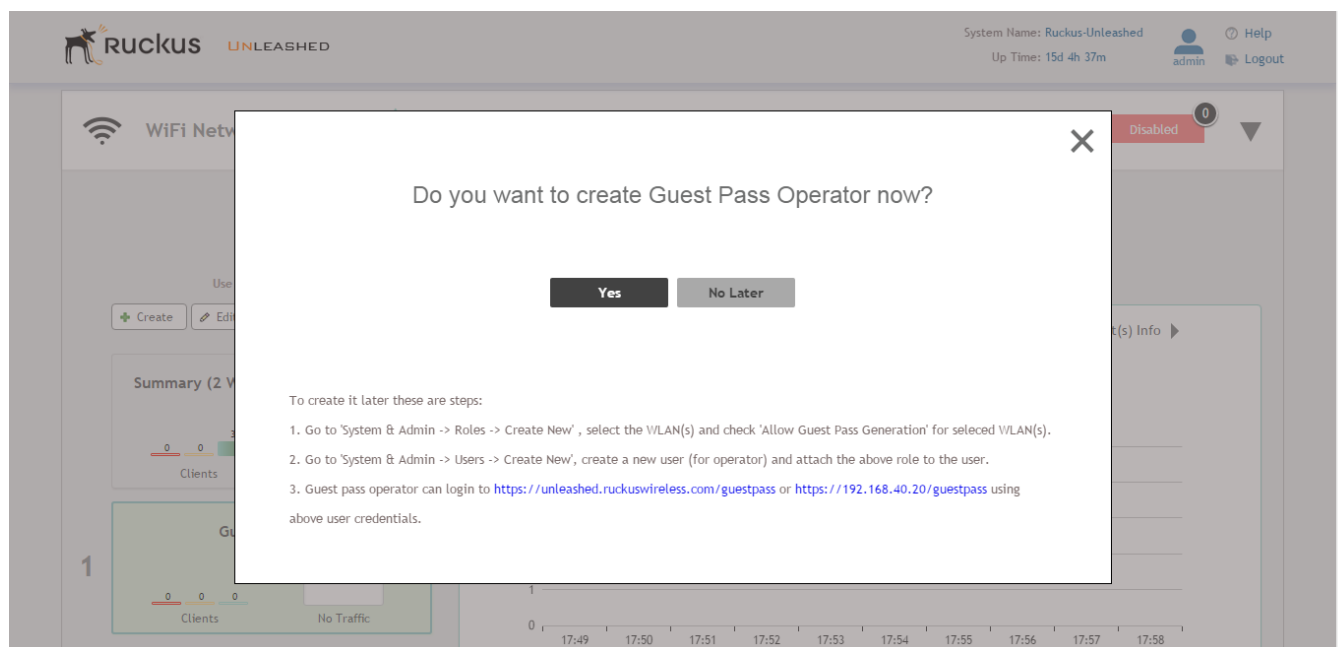
## Creating a Guest Pass Operator

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 59** Optionally configure a Guest Pass Operator now



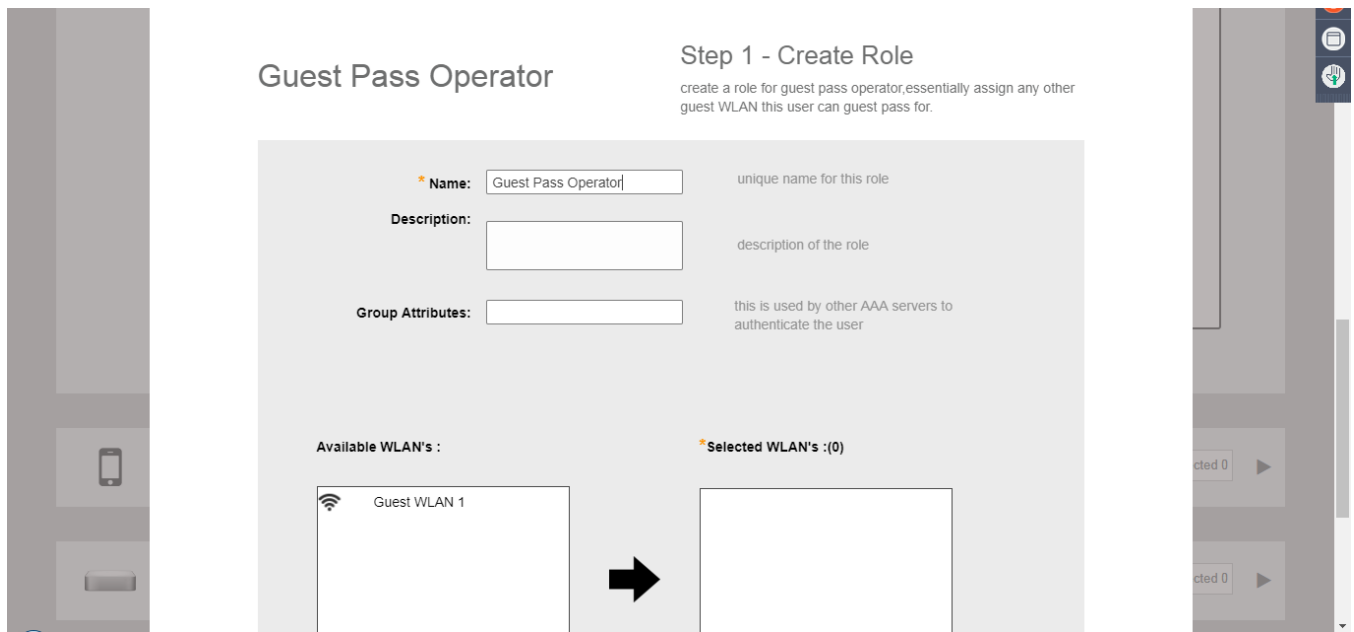
2. Click **Yes** to configure this role now. Or click **No Later** to configure these settings later.

### 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.

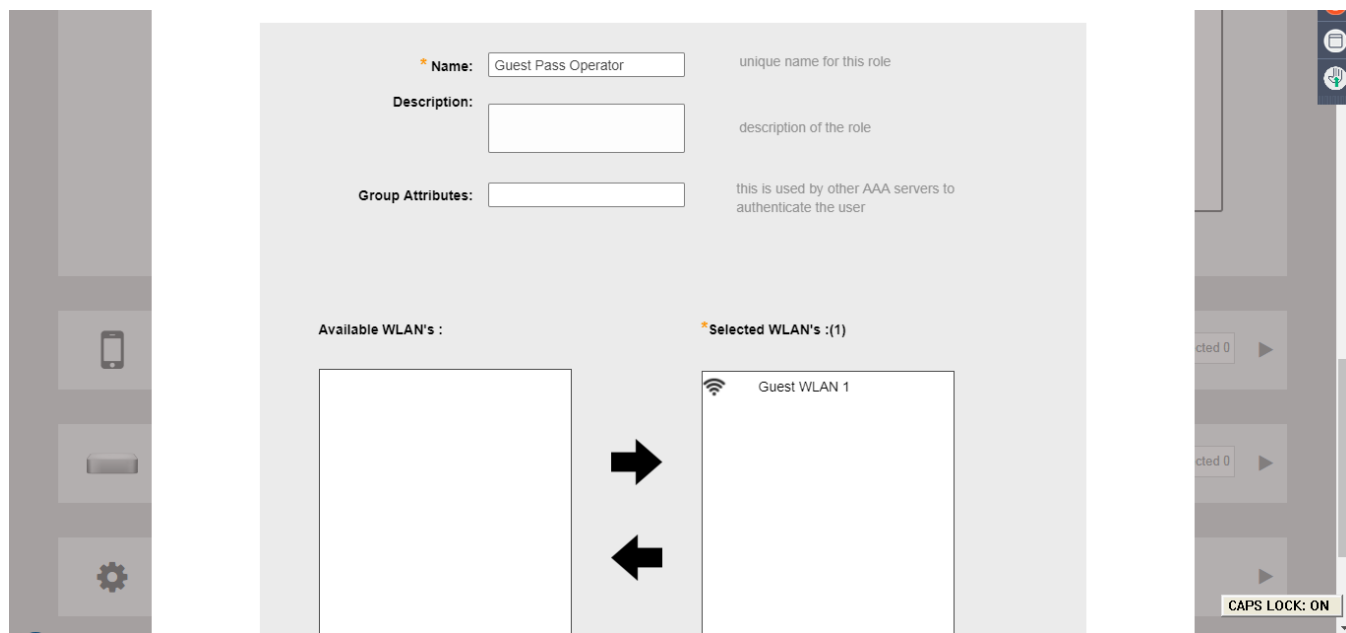
**FIGURE 60** Create Guest Pass Operator - step 1



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.)

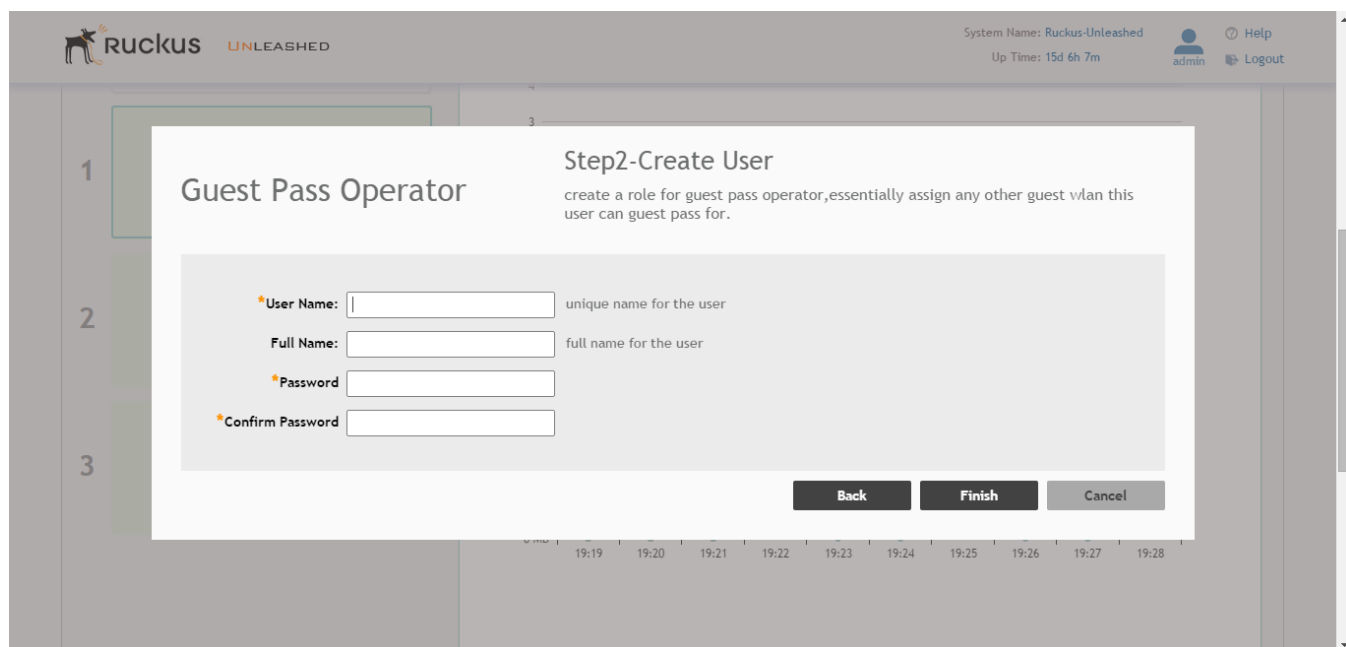
5. Click **Next** to continue.

**FIGURE 61** Move 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 62** Create Guest Pass Operator - step 2

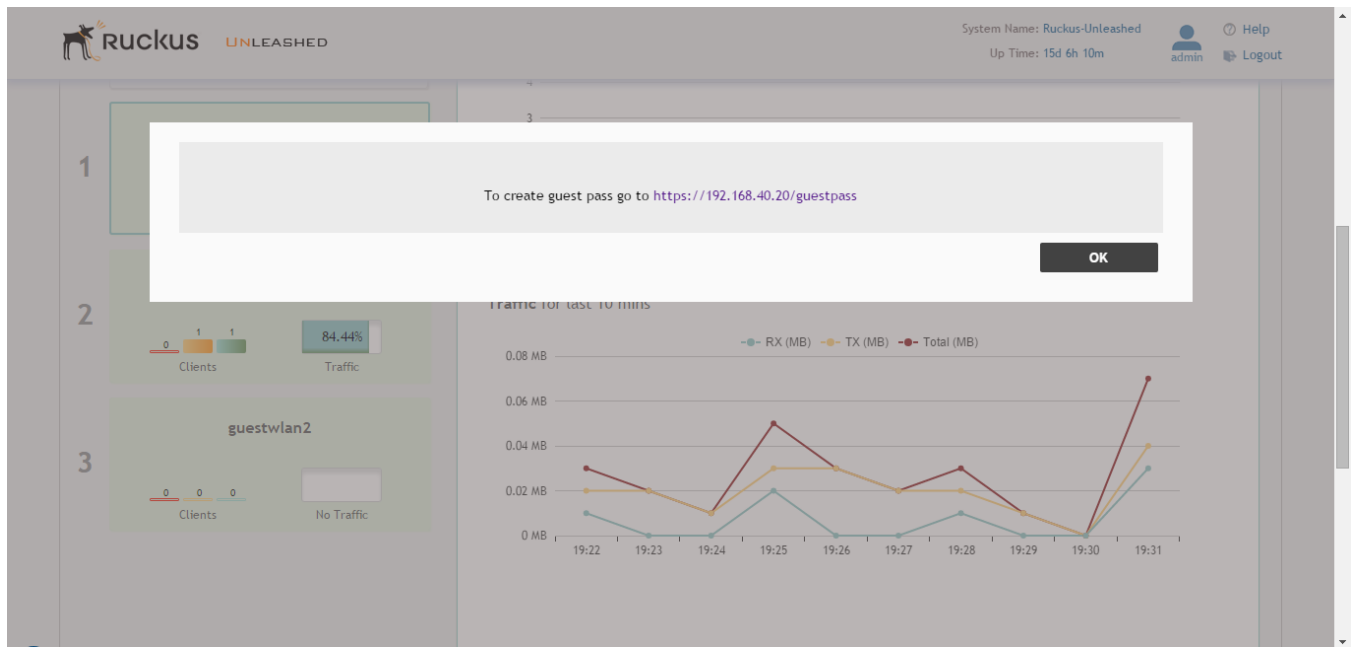


7. You have completed creating a user with the Guest Pass operator role. The confirmation screen displays the URL where this user can create guest passes.

**NOTE**

Users with the Guest Pass operator role can login to <https://unleashed.ruckuswireless.com/guestpass> or [https://\[host\\_ip\\_address\]/guestpass](https://[host_ip_address]/guestpass) using the above user credentials.

**FIGURE 63** 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.

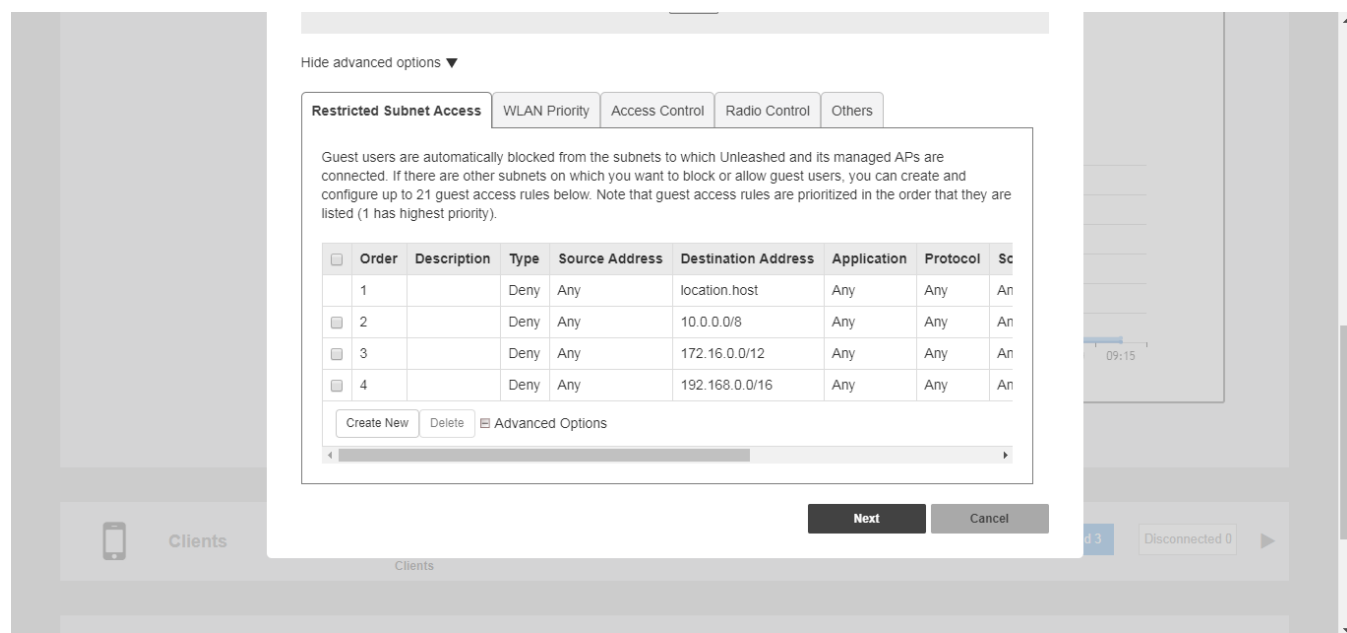
You can create up to 32 subnet access rules, which will be enforced both on both the Unleashed Master AP and all connected member APs.

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 64** 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:

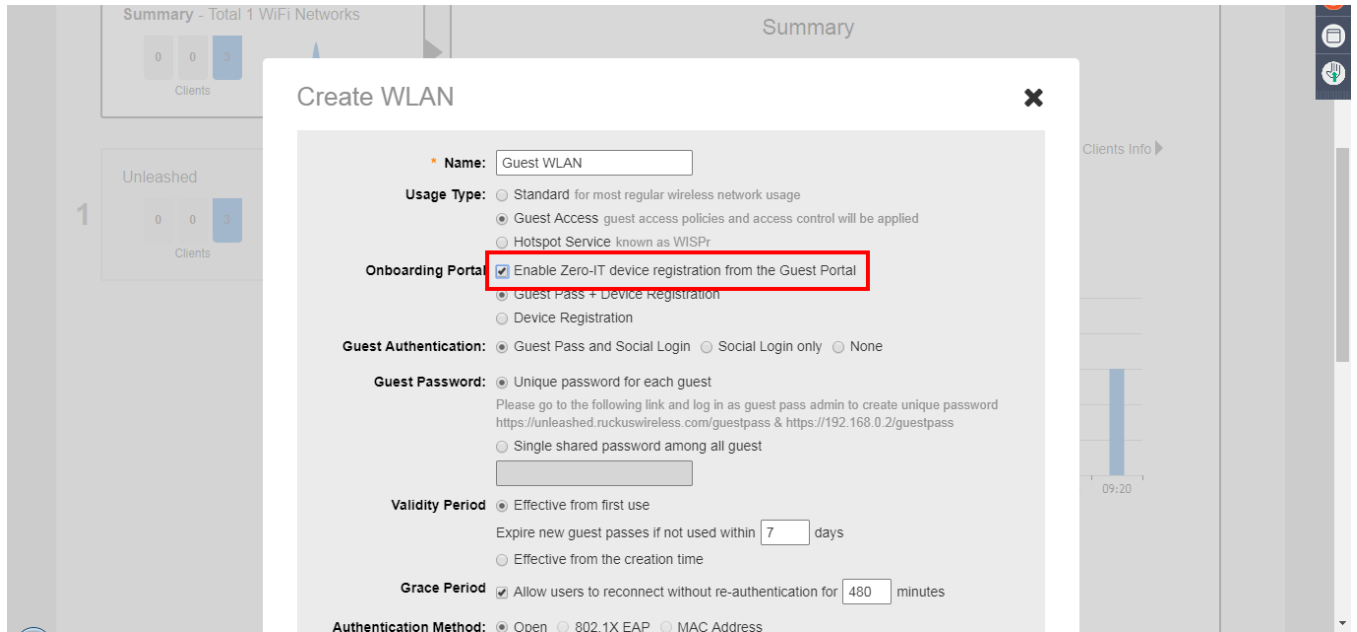
1. Expand the **Wi-Fi Networks** section of the Dashboard.
2. Select an existing guest WLAN and click **Edit** or click **Create** to configure a new guest WLAN.
3. Enable the check box next to **Onboarding Portal** to enable Zero-IT device registration from the Guest Portal.
4. Select one of the following 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 133.
6. Click **Next** to continue to the next guest WLAN configuration page.

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

**NOTE**

For information on these settings, see [Deploying a Guest WLAN](#) on page 115.

**FIGURE 65** Enable Onboarding Portal

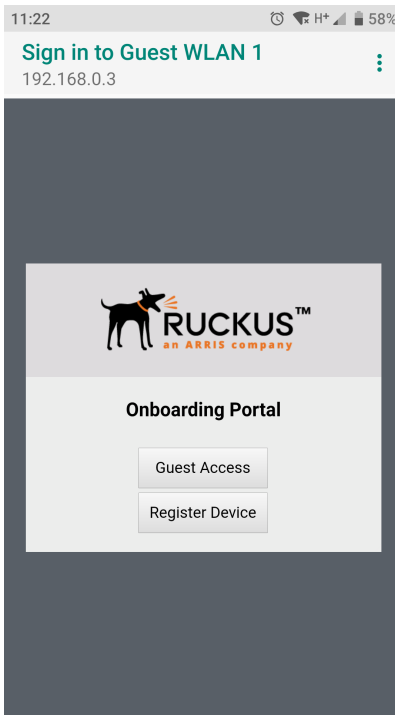


When a client connects to the open Guest WLAN for the first time, the Ruckus **Onboarding Portal** page is displayed. The screen displays one or both of the following options, depending on your choice in Step 4 above:

- **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.

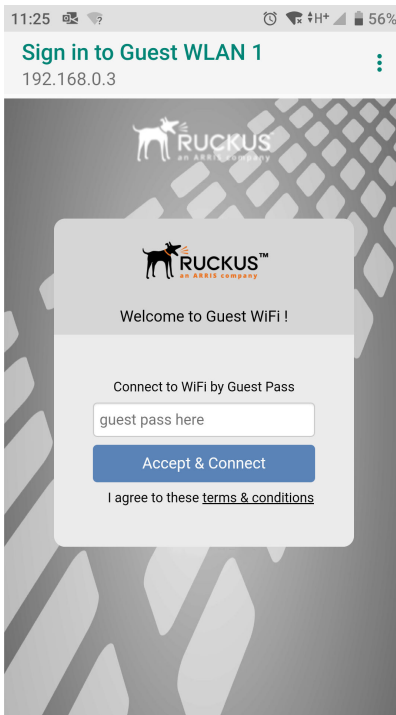


**FIGURE 66** The Onboarding Portal for mobile devices



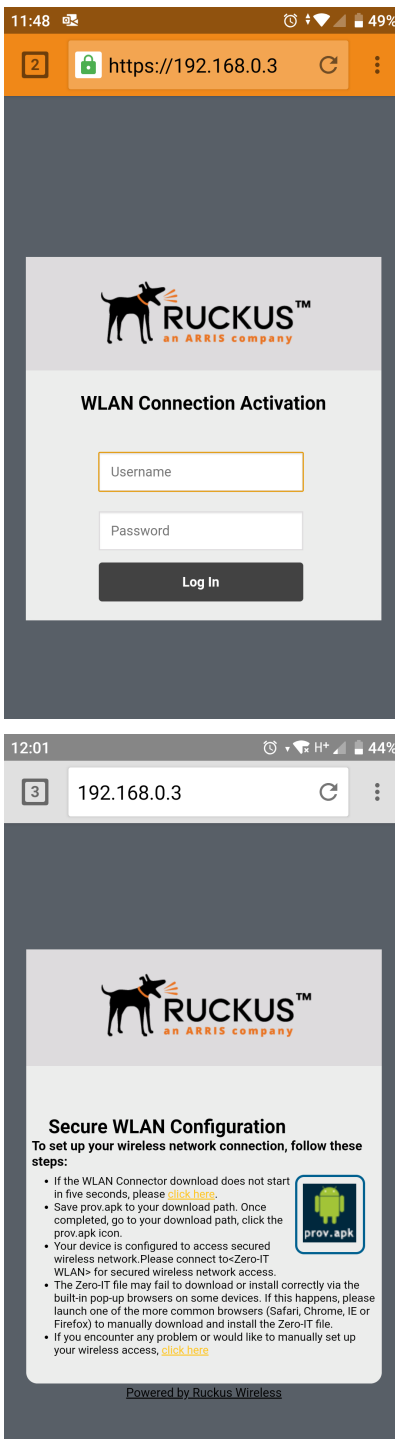
If the user clicks the **Guest Access** button, the process is the same as when connecting to a Guest WLAN and all settings on the **Guest Access** configuration page will be put into effect.

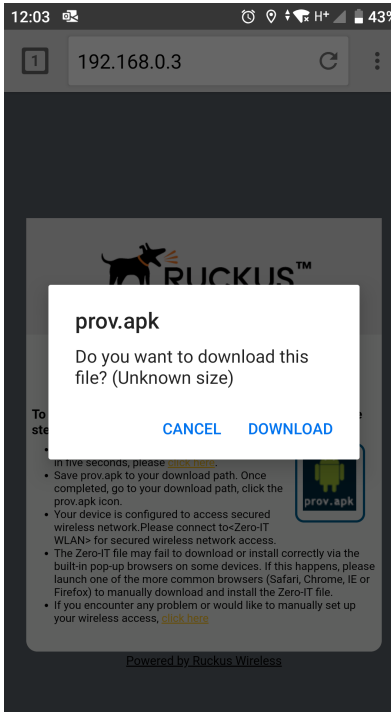
**FIGURE 67** Guest Access welcome and terms of use screens



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 68 Activate device using the WLAN Connection Activation screen, and download 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.

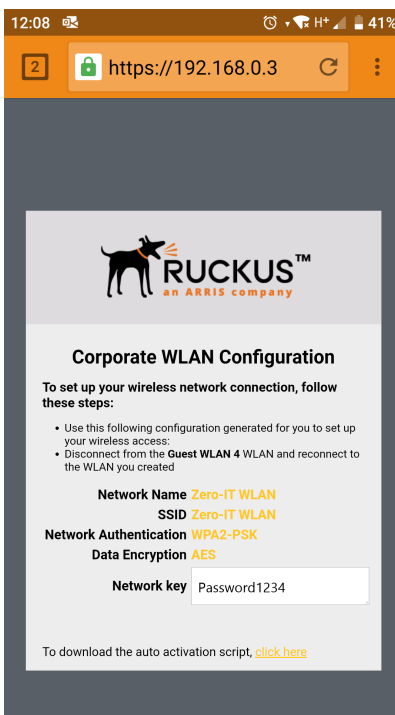
**NOTE**

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 69** 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.

## 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.

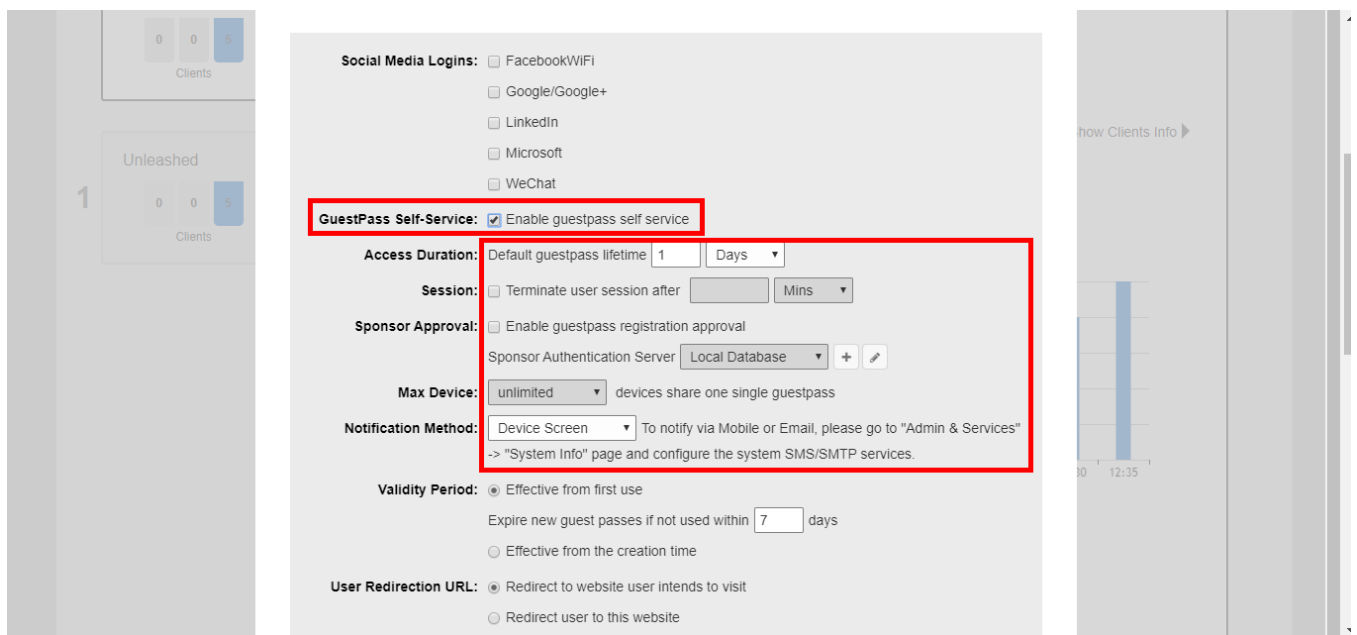
### Enabling Guest Pass Self-Service

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 70** 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 135.)
  - **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, he or she submits registration information along with a Sponsor's email address and waits for sponsor approval.

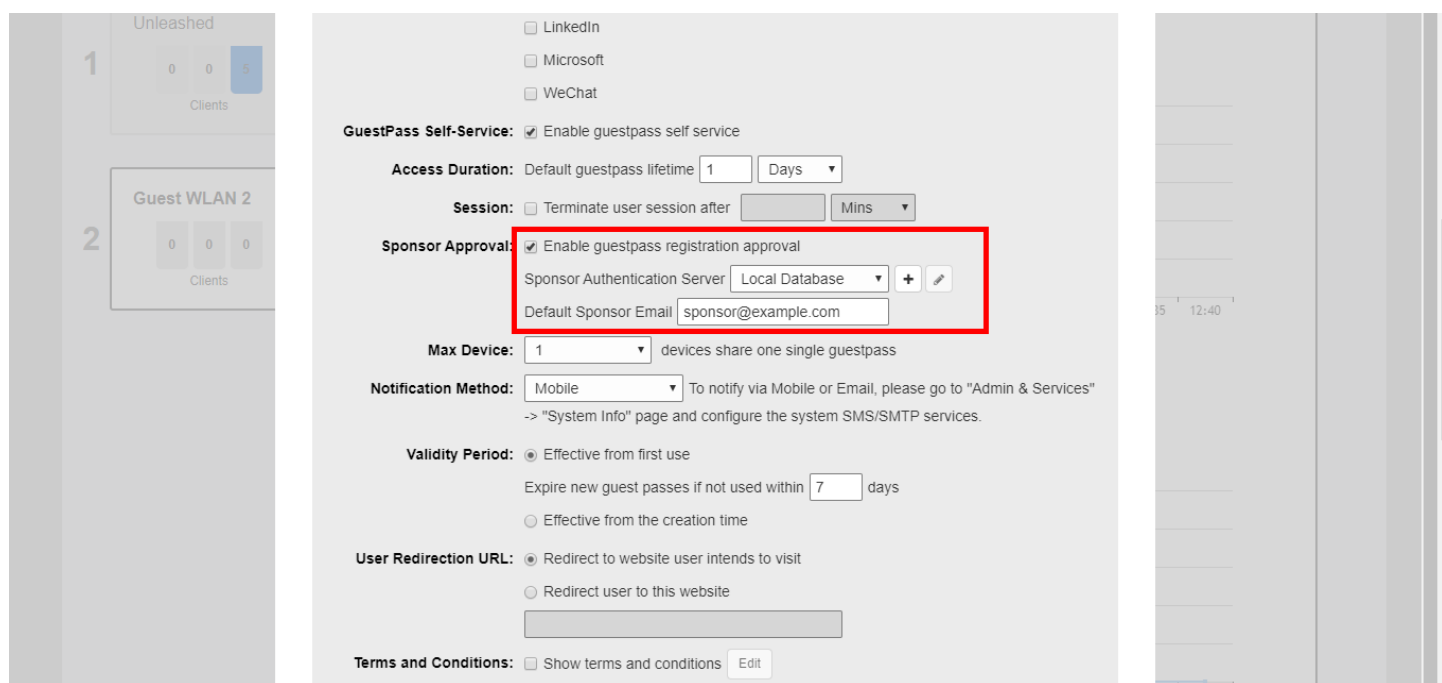
The Sponsor receives an email request and clicks a link to allow this user access to the guest WLAN. Once the registration is approved, Unleashed then generates a guest pass and sends it to the user via email and/or SMS using the contact information the user provided.

#### NOTE

If using Sponsor Approval, Unleashed must be configured with your SMTP settings for email delivery, or with a valid Twilio or Clickatell account to deliver guest passes via SMS. See [Customizing the Guest Pass Email Content](#) on page 158 and [Customizing the Guest Pass SMS Content](#) on page 159 for more information.

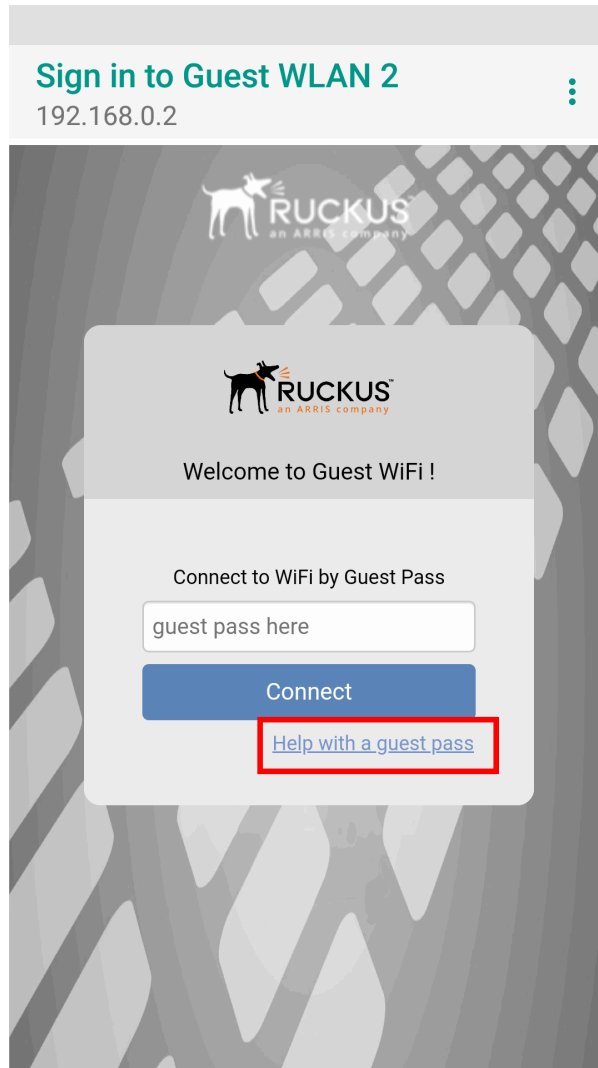
To configure sponsor approval, select the Sponsor Approval check box, select a sponsor authentication server (default is local database), and optionally enter a **Default Sponsor email** address.

**FIGURE 71** Enable Sponsor Approval for self-service guest passes



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 72** Welcome to Guest WiFi - click "Help with guest pass" for options

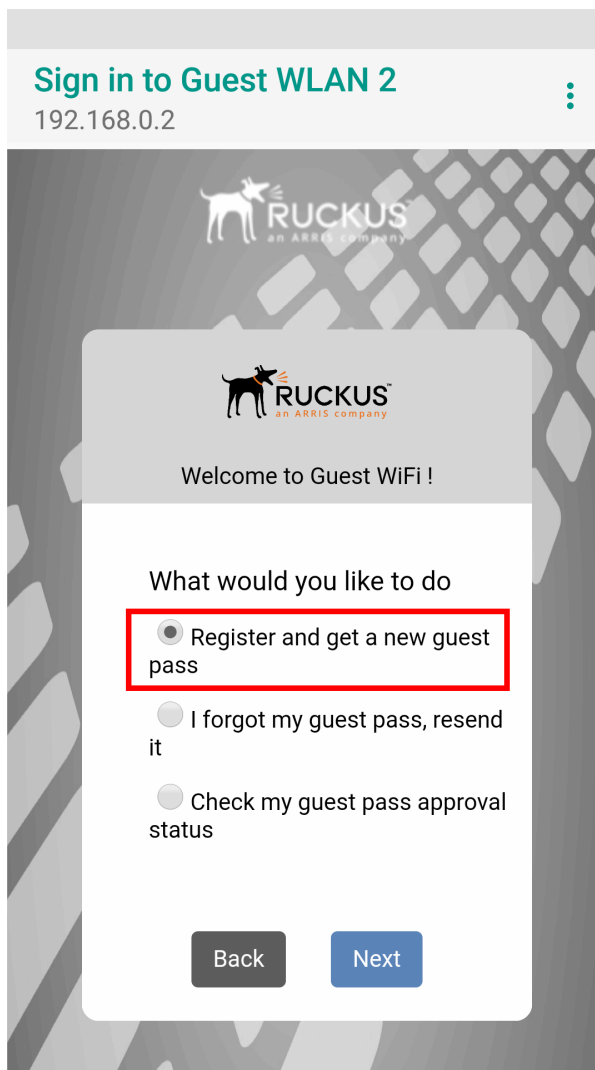




To request, approve and activate a sponsor-approved guest pass, use following procedure:

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

**FIGURE 73** Request a new guest pass



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

**FIGURE 74** Enter name, guest email and sponsor email to request sponsor approval

Sign in to Guest WLAN 2  
192.168.0.2

**RUCKUS**  
an ARXIS company

Welcome to Guest WiFi !

Register Guest

James

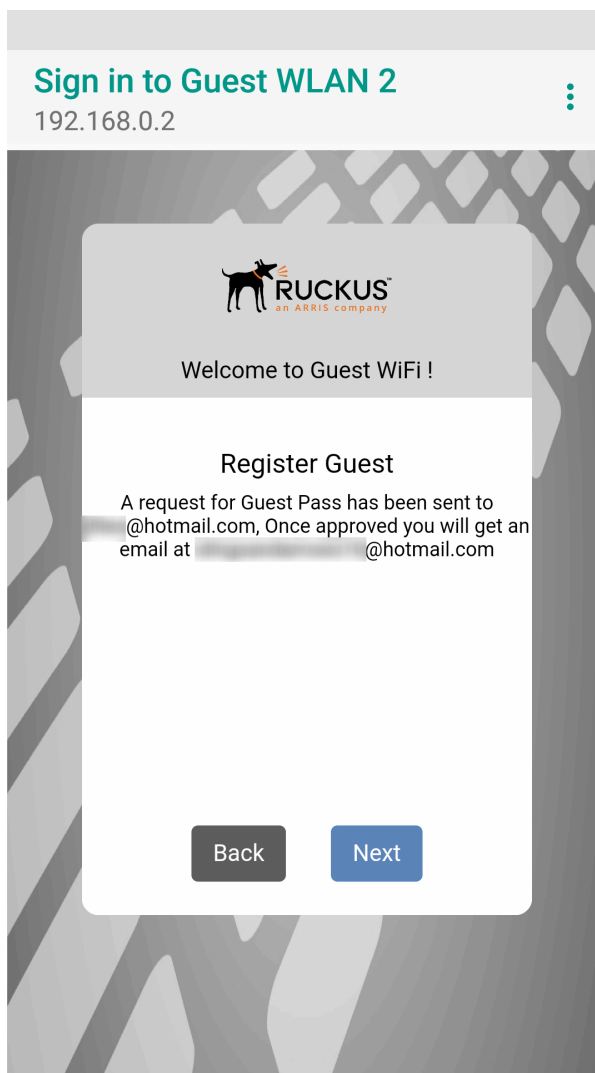
@hotmail.com

James guest

Back Next

3. A guest pass request email is sent to the sponsor's address, and the **Guest Access request submitted** screen is displayed.

**FIGURE 75** Guest pass request submitted



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

5. As the sponsor, open the email and click the link to open the **Sponsor/Approver Authentication** page.

**FIGURE 76** Sponsor Accept Email

Dear Sponsor/Admin,

You are a designated approver for [redacted]@hotmail.com's WiFi access. Click link below to approve or reject the request.

[https://192.168.0.2/user/sponsor\\_login.jsp?](https://192.168.0.2/user/sponsor_login.jsp?email=GKGGGJGMGFHDEAGIPHEGNGBGJGMCODGPGN&user=HDGMGJGOGHHDGBGOGEGBHCHCGPHHHDDBDAAEAGIPHEGNGBGJGMCODGPGN&ssid=EHHFGFHDHECAFHEMEBEOCADC)

[email=GKGGGJGMGFHDEAGIPHEGNGBGJGMCODGPGN&user=HDGMGJGOGHHDGBGOGEGBHCHCGPHHHDDBDAAEAGIPHEGNGBGJGMCODGPGN&ssid=EHHFGFHDHECAFHEMEBEOCADC](https://192.168.0.2/user/sponsor_login.jsp?email=GKGGGJGMGFHDEAGIPHEGNGBGJGMCODGPGN&user=HDGMGJGOGHHDGBGOGEGBHCHCGPHHHDDBDAAEAGIPHEGNGBGJGMCODGPGN&ssid=EHHFGFHDHECAFHEMEBEOCADC)

Name: [redacted]@hotmail.com

Mobile No:

Email: [redacted]@hotmail.com

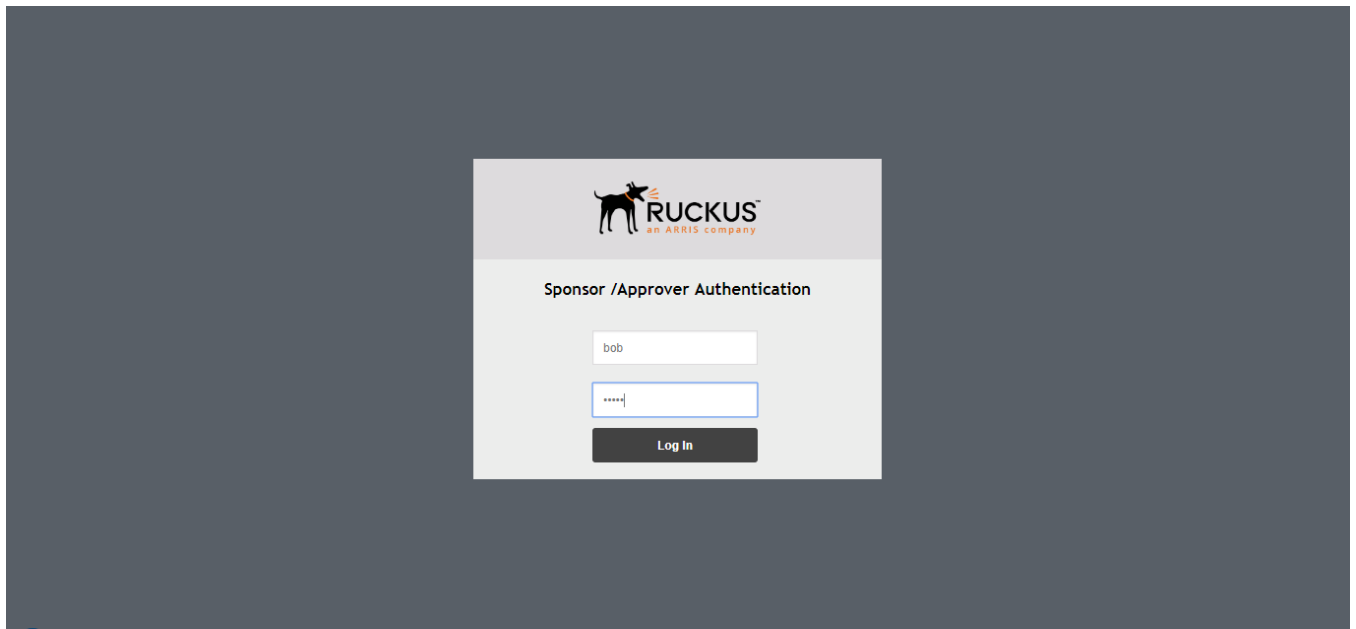
SSID: Guest WLAN 2

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

**NOTE**

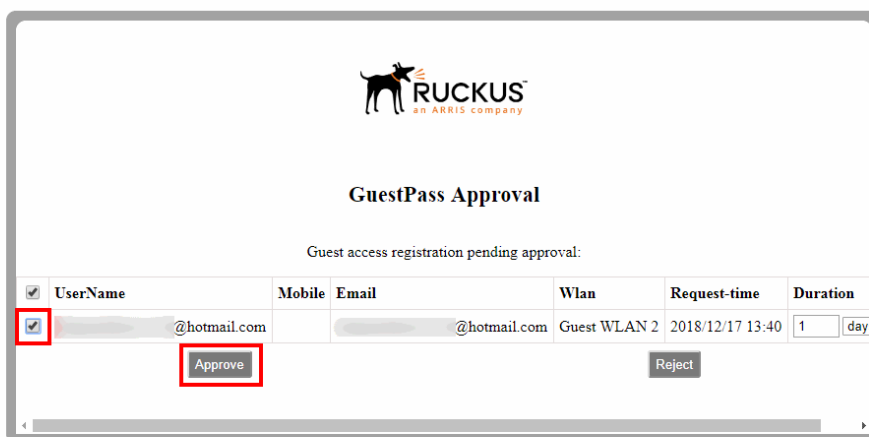
This user name and password must exist on the Authentication Server (Local Database, Active Directory, or RADIUS) configured for this guest access service.

**FIGURE 77** Sponsor Login

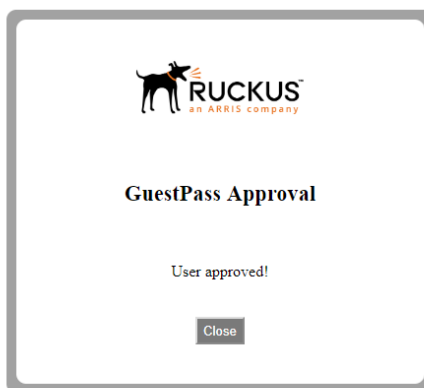


7. Upon successful login, the **Guest Pass Approval** page appears, displaying the name, phone and email addresses of all pending guest pass requests. Select the check boxes next to each guest pass you wish to approve, set the **Duration** for each, and click **Approve** to approve them.

**FIGURE 78** Guest Pass Approval



**FIGURE 79** Guest pass approved



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

9. As a guest user, open this email and copy the **Guest Pass** code to the clipboard.

**FIGURE 80** Guest pass activation email

Greetings, [REDACTED]@hotmail.com

You have been granted ~~access to the~~ company wireless network

Your guest pass key is **DMBXV-PHIQM**

This guest pass is valid until 1 day later once activated, and has to be activated in 7 days.

Connect your wireless-ready device to this network: Guest WLAN 2, as detailed in the instructions printed below.

Please follow the instruction below:

Finding the Wireless "Guest" Network

- 1 Find "Guest" SSID on device.
- 2 Select the "Guest" SSID and and click Connect.
- 3 If a Wireless Network Connection confirmation dialog box asks you to confirm "connecting to an unsecured network", click Connect Anyway. A connection status dialog appears, while a network address is obtained and initial connection established.
- 4 Once your device is connected proceed to the next step.

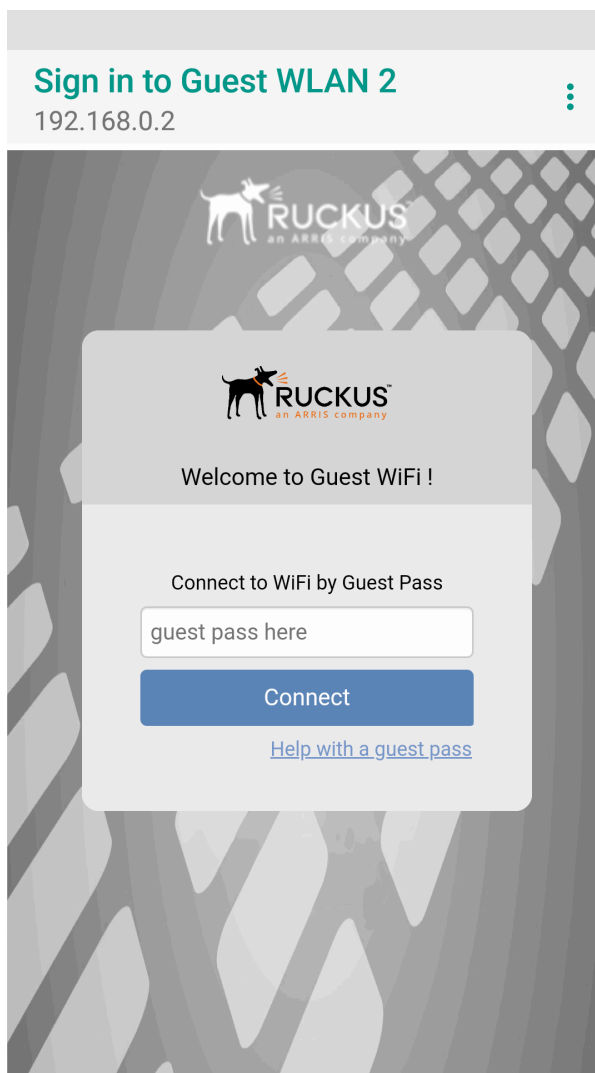
Logging into the Network as a Guest

- 1 Start a web browser and try to connect to any valid Internet site. The wireless network login page automatically appears.
- 2 Select "I'm a Guest and would like to access the Internet" and then click Next.
- 3 When "Guest Pass" page appears, enter the text of your guest pass key by typing or pasting and click Login.  
When the browser displays "Authenticated" page, your network connection is now active."

10. Launch a web browser and browse to any URL. You will be redirected to the **Welcome** login page.

11. Enter the **Guest Pass** code received in the activation email (or SMS) and click **Connect**.

**FIGURE 81** Enter Guest Pass code and click Connect



12. 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 288.

For more information on creating a Guest Pass Operator role, refer to [Creating a Guest Pass Operator](#) on page 123.

## Generating and Delivering a Single Guest Pass

You can provide the following instructions 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 can be configured so that a single guest pass can be shared by multiple users.

### NOTE

The following procedure will guide you through generating and delivering a guest pass. For instructions on how to generate multiple guest passes, see [Generating and Printing Multiple Guest Passes at Once](#) on page 148.

### NOTE

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

To generate a single guest pass:

1. In your web browser's address bar, type the URL of the **Unleashed Guest Pass Generation** page:

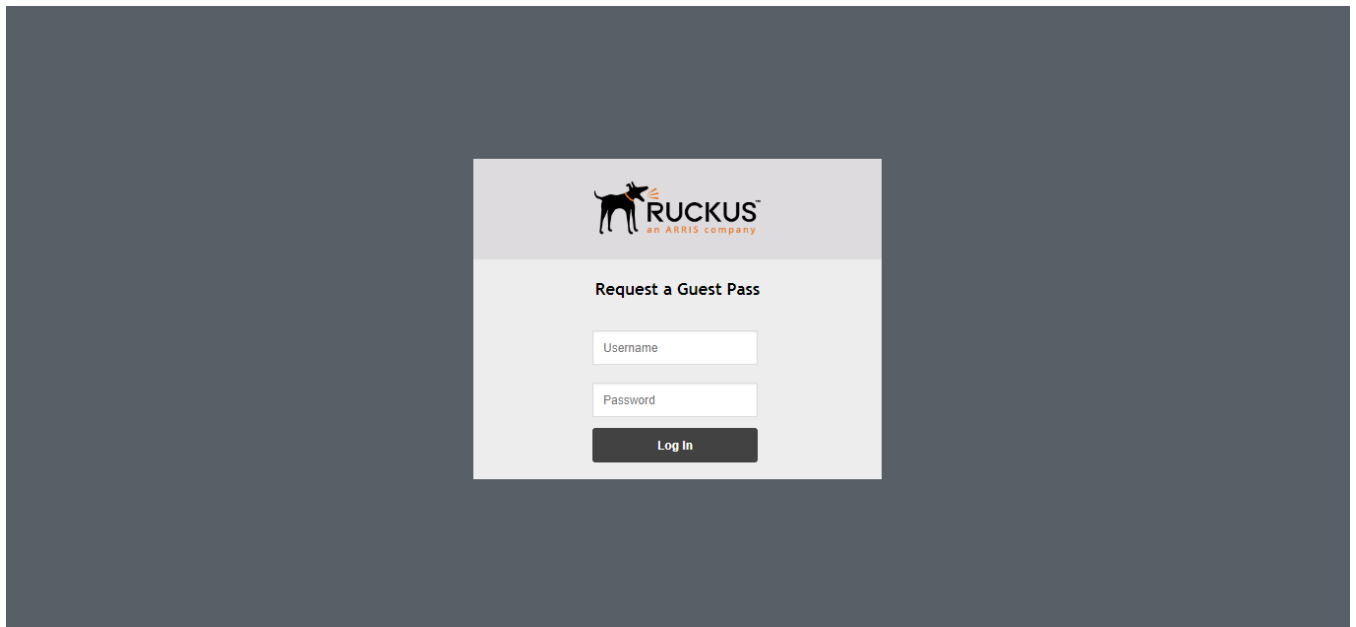
```
https://{unleashed-hostname-or-ipaddress}/guestpass
```

2. In **User Name**, type your user name. In **Password**, type your password.

### NOTE

This user must have guest pass generation privileges, as described in [Controlling Guest Pass Generation Privileges](#) on page 143.

**FIGURE 82** Request a Guest Pass



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



4. On the **Guest Information** page, fill in the following options:

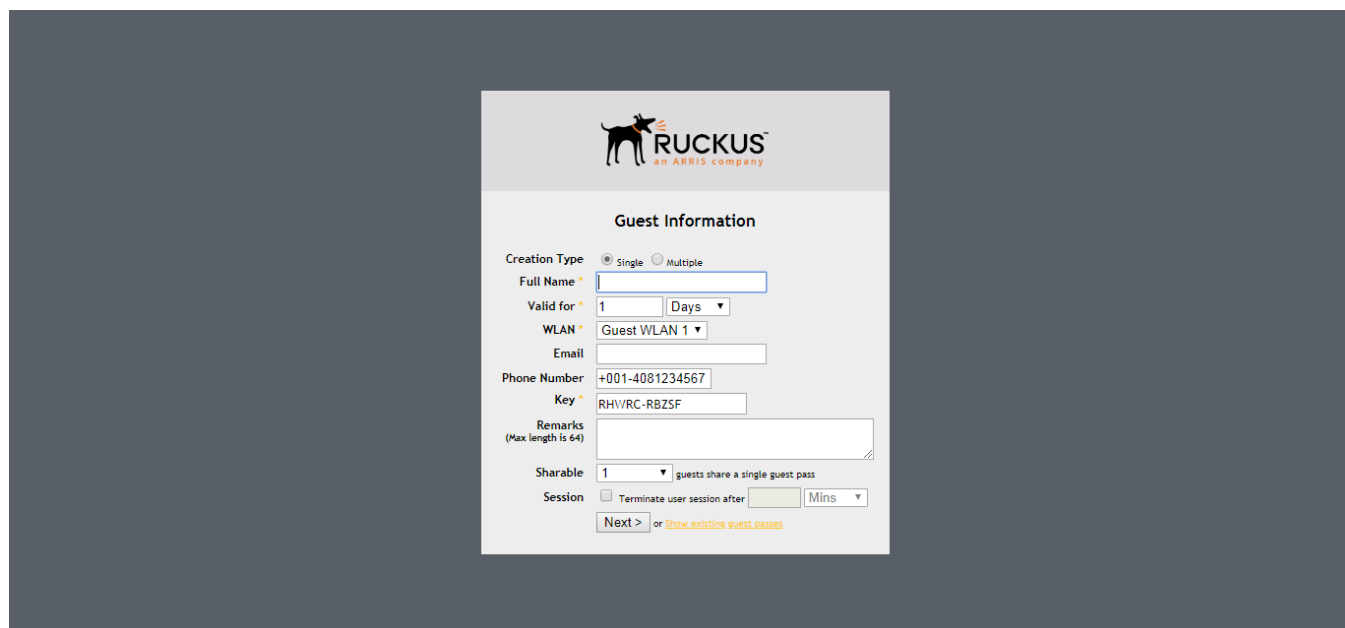
- **Creation Type:** Choose **Single** to generate a single guest pass. To generate multiple guest passes in batch, see [Generating and Printing Multiple Guest Passes at Once](#) on page 148.
- **Full Name:** Type the name of the guest user for whom you are generating the guest pass.
- **Valid for:** Specify the time period when the guest pass will be valid. Do this by typing a number in the blank box, and then selecting a time unit (Hours, Days or Weeks).
- **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 Unleashed generated. If you want to use a key that is easy to remember, delete the random key, and then type a custom key. For example, if Unleashed generated the random key OVEGS-RZKFF, you can change it to "joe-guest-key". Customized keys must be between 1 and 16 ASCII characters.

**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.

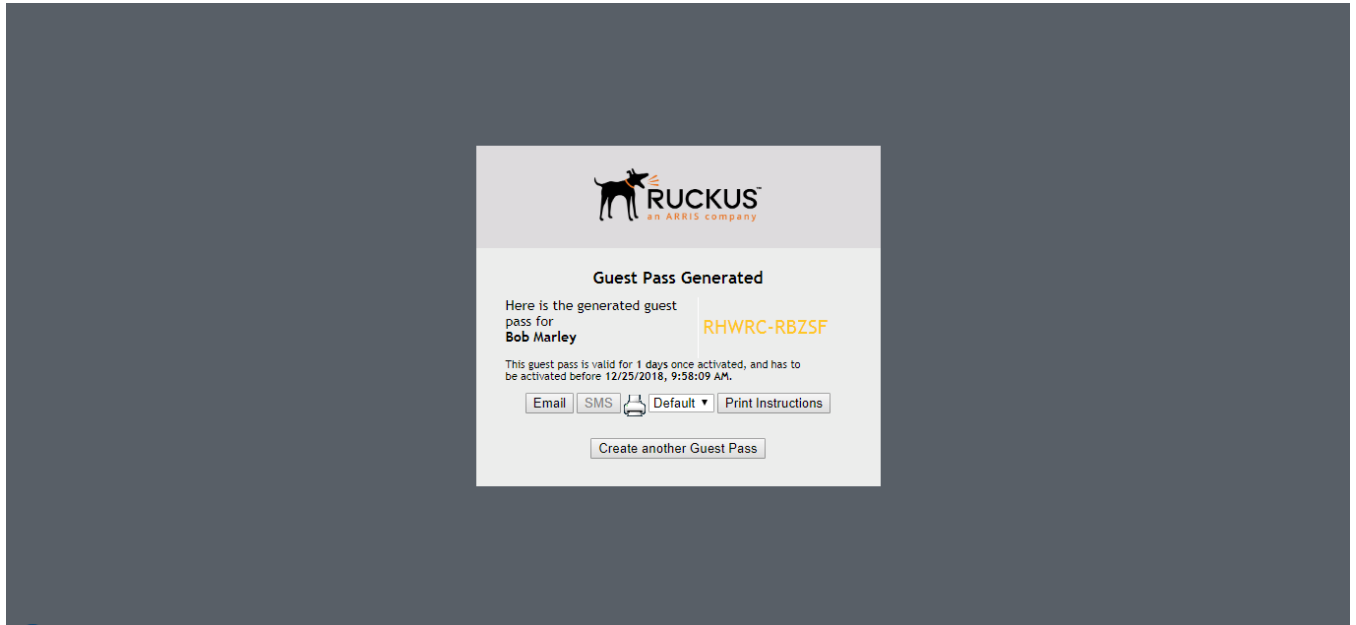
- **Remarks** (optional): Type any notes or comments. For example, if the guest user is a visitor from a partner organization, you can type the name of the organization.
- **Sharable:** Use this option to allow multiple users to share a single guest pass.
- **Session:** Enable this check box and select a time increment after which guests will be required to log in again. If this feature is disabled, connected users will not be required to re-log in until the guest pass expires.

**FIGURE 83** Creating a Guest Pass



5. Click **Next**. The **Guest Pass Generated** page appears. This page presents the guest pass key and options for delivering this key to your guest(s). 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 84** Guest pass generated



6. If you want to print out the guest access instructions, select the guest pass instructions that you want to print out from the drop-down menu. If you did not create custom guest pass printouts, select **Default**.
7. Click **Print Instructions**. A new browser page appears and displays the guest pass instructions. At the same time, the **Print** dialog box appears.
8. Select the printer that you want to use, and then click **Print** to print the guest pass instructions.

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

**FIGURE 85** Click Email to send the guest pass key to the email entered on the Guest Information screen

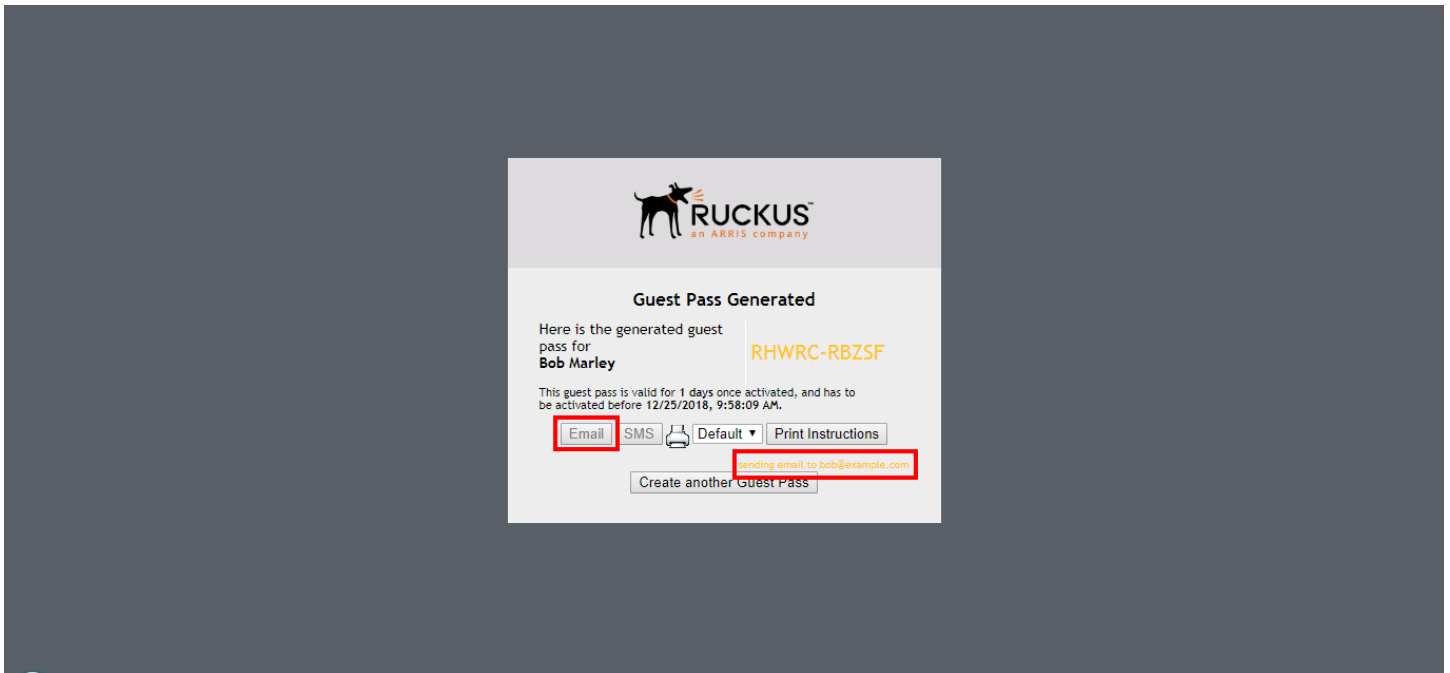


FIGURE 86 Sample Guest Pass Printout

## Connecting as a Guest to the Corporate Wireless Network



Greetings, **Bob Marley**

You have been granted access to the company wireless network, which you can use to access both the World Wide Web and Internet, and to check your personal email.

Your guest pass key is **RHWRC-RBZSF**

This guest pass is valid for **1 days** once activated, and has to be activated before **12/25/2018, 9:58:09 AM**

Connect your wireless-ready PC to this network: **Guest WLAN 1**, as detailed in the instructions printed below.

Before you start, please review the following requirements.

### Requirements

- A wireless-network-ready computer
- The corporate "guest" network name
- The guest pass (a text "key")

### Connecting

Using your guest pass to connect requires a series of two procedures: (1) connecting your PC to the company "guest" network, then (2) logging in as a qualified guest.

#### Finding the Wireless "Guest" Network

- 1 On your PC/Windows desktop, check the system tray for a Wireless Connection icon (the tool tip reads "Wireless Network Connection/[name]").
- 2 Right-click this icon and choose **View Available Wireless Networks**.
- 3 When the Wireless Network Connection window appears, the "guest" WLAN will be listed.
- 4 Select the WLAN "guest" network (various "neighbor nets" may also be listed) and click **Connect**.
- 5 If a Wireless Network Connection confirmation dialog box asks you to confirm "connecting to an unsecured network", click **Connect Anyway**.
- 6 A connection status dialog appears, while a network address is obtained and initial connection established.
- 6 When the Wireless Network Connection window displays "**Connected**", you can close this window and proceed to the next procedure.

#### Logging into the Network as a Guest

- 1 Start a web browser and try to connect to any valid Internet site. The wireless network login page automatically appears.
- 2 Select "I'm a Guest and would like to access the Internet" and then click **Next**.
- 3 When the Unleashed WebUI "Guest Pass" page appears, enter the text of your guest pass key (by typing or pasting) and click **Login**.
- 4 When the browser displays a Unleashed WebUI "Authenticated" page, your connection is active.
- 4 You can now check your personal email and browse the Web.

### Important

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 148.

### Generating and Printing Multiple Guest Passes at Once

You can provide the following instructions to users with guest pass generation privileges.

#### NOTE

The following procedure will guide you through generating and printing multiple guest passes. For instructions on how to generate a single guest pass, see [Generating and Delivering a Single Guest Pass](#) on page 144.

#### NOTE

Before starting, make sure that your computer is connected to a local or network printer.

To generate and print multiple guest passes at the same time:

1. In your web browser's address bar, type the URL of the Unleashed Guest Pass Generation page:

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

2. In **User Name**, type your user name. In **Password**, type your password.
3. Click **Log In**. The **Guest Information** page appears. On this page, you need to provide information about the guest users to enable Unleashed to generate the guest passes.

4. On the **Guest Information** page, fill in the following options:

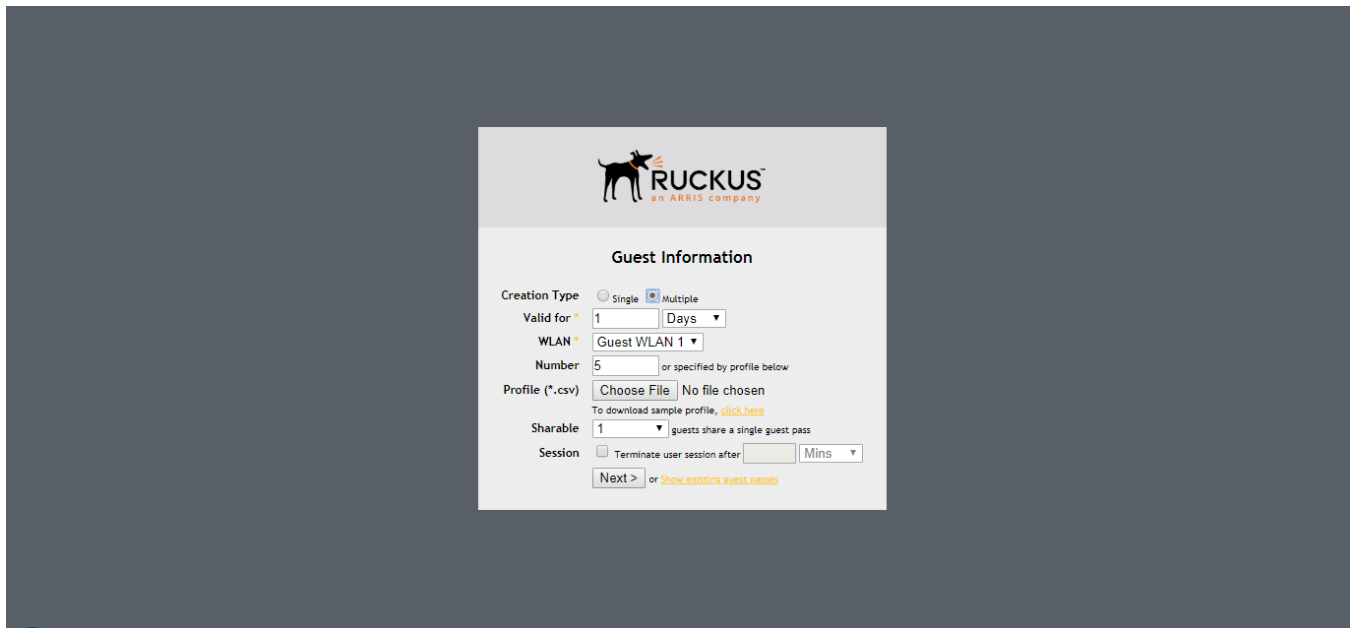
- **Creation Type:** Click Multiple.
- **Valid for:** Specify the time period during which the guest passes will be valid by typing a number in the blank box, and then selecting a time unit (Days, Hours, or Weeks).
- **WLAN:** Select one of the existing WLANs with which the guest users will be allowed to associate.
- **Number:** Select the number of guest passes that you want to generate. Unleashed will automatically populate 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 (see Creating a Guest Pass Profile), use this option 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:** Enable this check box and select a time increment after which guests will be required to log in again. If this feature is disabled, connected users will not be required to re-log in until the guest pass expires.

**FIGURE 87** Generating Multiple Guest Passes

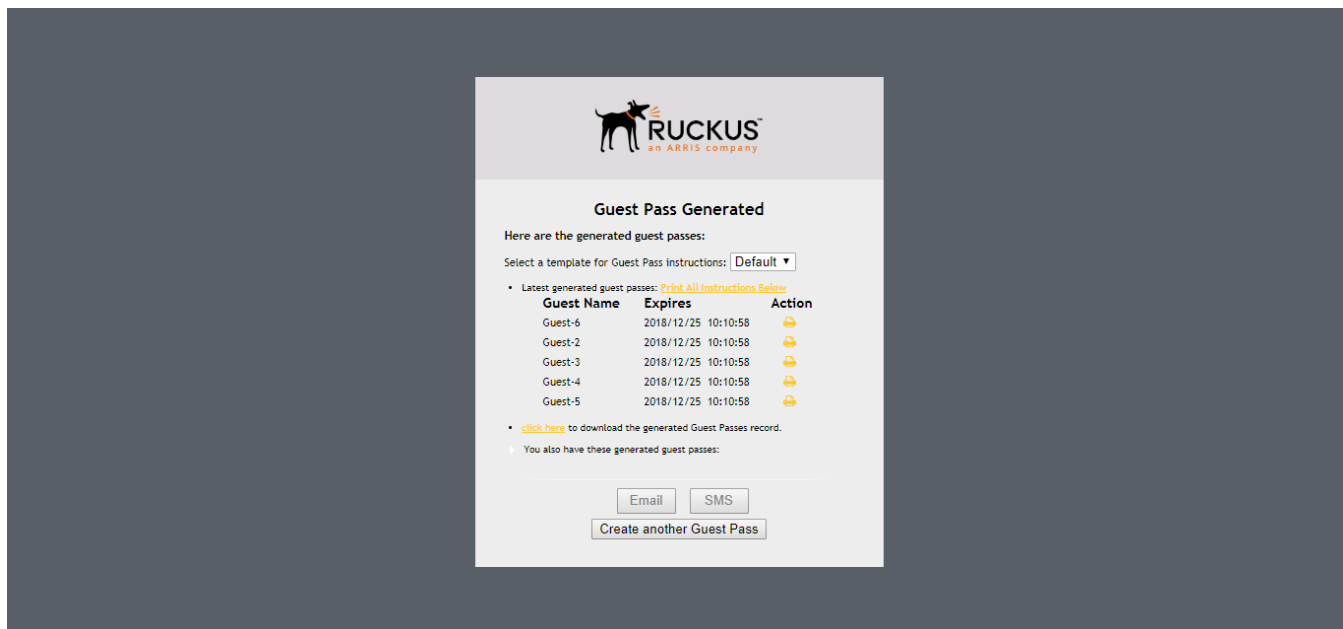


**NOTE**

If you want to be able to identify the guest pass users by their names (for monitoring or auditing purposes in a hotel setting, for example), click **Choose File**, and upload a guest pass profile instead. See [Creating a Guest Pass Profile](#) on page 151 for more information.

- Click **Next**. The **Guest Pass Generated** page appears, displaying the guest pass user names and expiration dates.

**FIGURE 88** Multiple Guest Passes generated



- In **Select a template for Guest Pass instructions**, select the guest pass instructions that you want to print out. If you did not create custom guest pass printouts, select **Default**.
- Print the instructions for a single guest pass or print all of them.
  - To print instructions for all guest passes, click **Print All Instructions**.
  - To print instructions for a single guest pass, click the **Print** link 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. At the same time, the **Print** dialog box appears.
- Select the printer that you want to use, and then click **Print** to print the guest pass instructions.

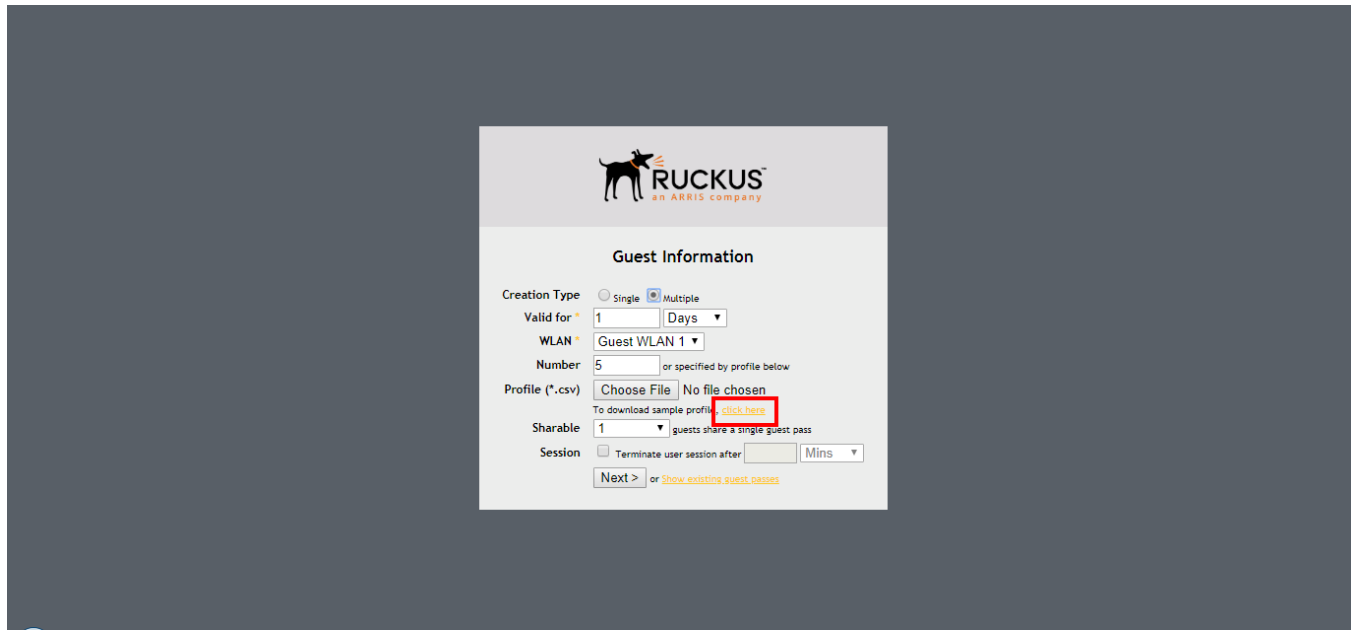
You have completed generating and printing multiple guest passes for your guest users. If you want to save a record of the guest passes that you have generated, click the **Click here** link in "Click here to download the generated Guest Passes record," and then download and save the CSV file to your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

### Creating a Guest Pass Profile

- Log in to the guest pass generation page.
- In **Creation Type**, click **Multiple**.

3. Click the [click here](#) link in **To download a profile sample, click here.**

**FIGURE 89** Download 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:** Type the name of the guest user (one name per row).
  - **Remarks:** (Optional) Type any note or remarks about the guest pass.
  - **Key:** Type a guest pass key consisting of 1-16 alphanumeric characters. If you want Unleashed to generate the guest pass key automatically, leave this column blank.

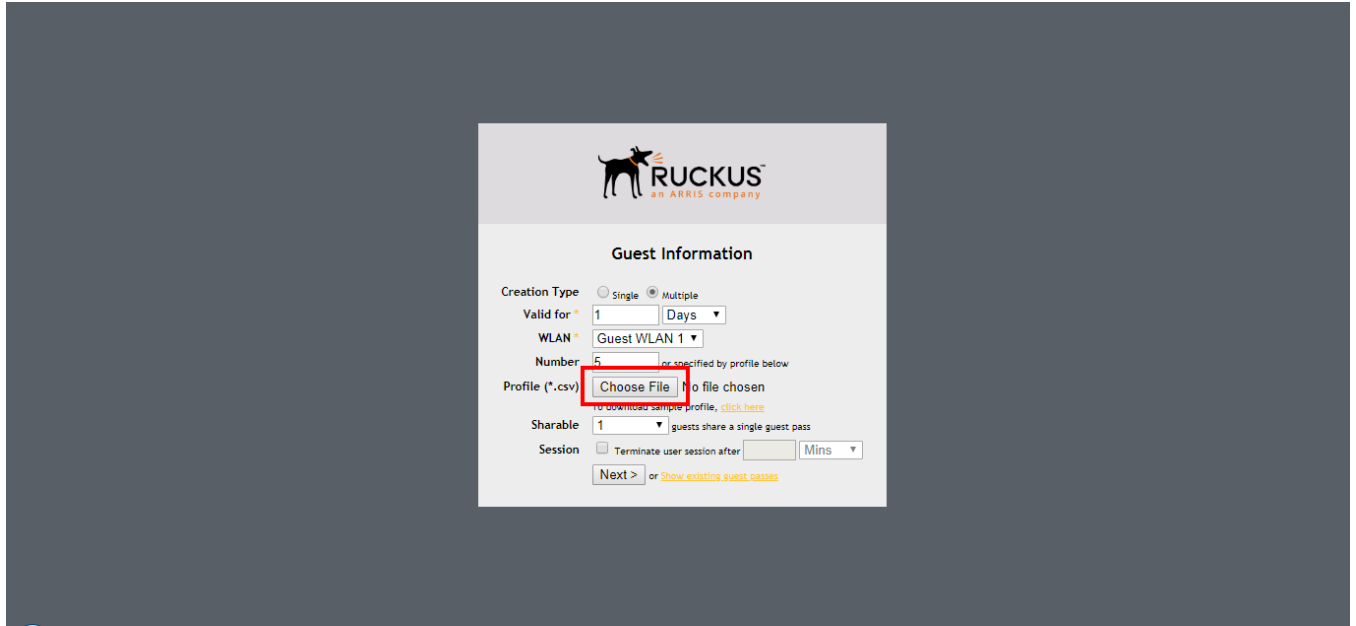
**FIGURE 90** Edit the csv file in a spreadsheet application

	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	AAAAAAA	someone@example.com	14081234567		
3	Batch-Guest-2	Batch generation	AAAAAAB	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

- Go back to the *Guest Information* page, and then complete steps 4 to 8 in [Generating and Printing Multiple Guest Passes at Once](#) on page 148 to upload the guest pass profile and generate multiple guest passes.

**FIGURE 91** Import batch generation csv file

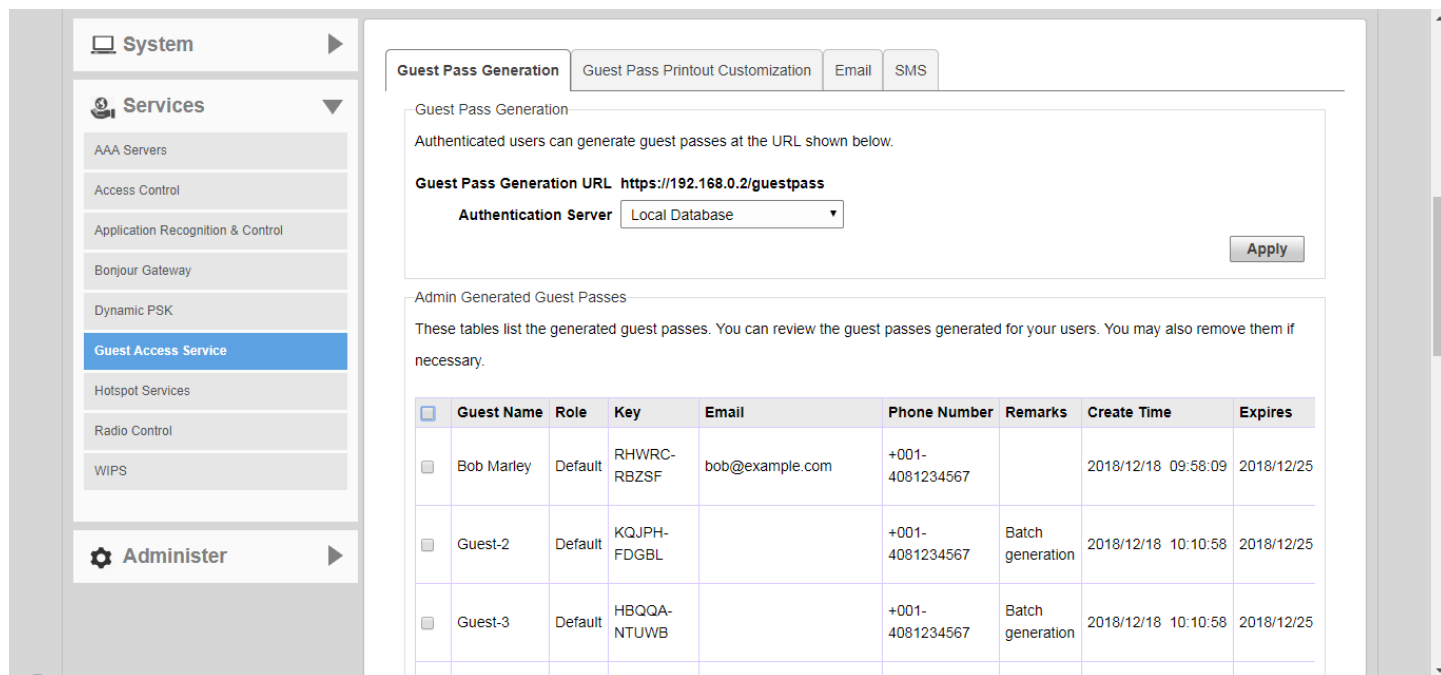


### Monitoring Generated Guest Passes

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

- Go to **Admin & Services > Services > Guest Access Service > Guest Pass Generation**.
- Review the generated guest passes in the **Admin Generated Guest Passes** and **Self-Service Generated Guest Passes** tables.
- 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 92 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.

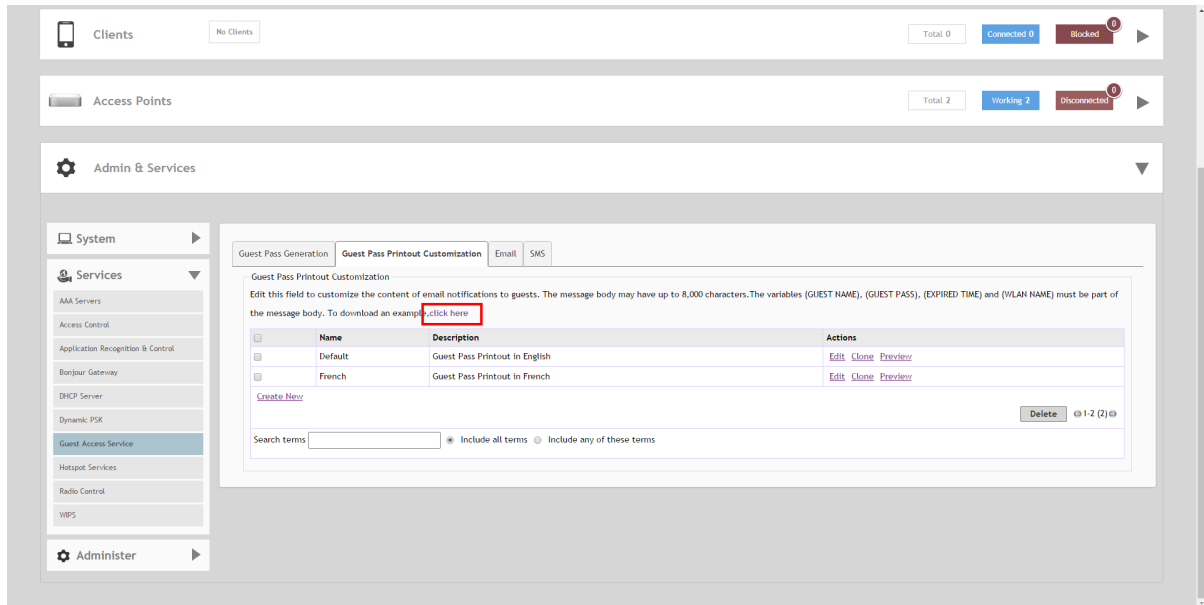
As administrator, you can create custom guest pass printouts. For example, if your organization receives visitors who speak different languages, you can create guest pass printouts in other languages.

To create a custom guest pass printout:

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

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

**FIGURE 93** Guest Pass Printout customization



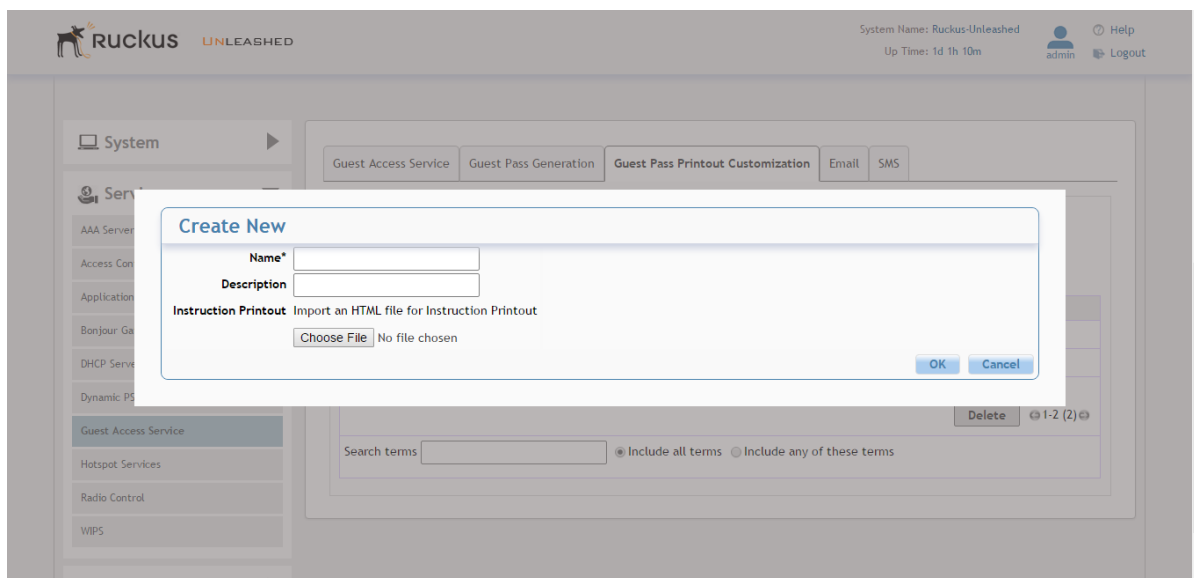
3. Save the HTML file to your computer.
4. Using a text or HTML editor, customize the guest pass printout. Note that only ASCII characters can be used. You can do any or all of the following:
  - Reword the instructions
  - Translate the instructions to another language
  - Customize the HTML formatting

**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 157.

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

**FIGURE 94** Create New Guest Pass Printout file



- 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**.
- In **Description** (optional), add a brief description of the guest pass printout.
- Click **Choose File**, select the HTML file that you customized earlier, and then click **Open**. Unleashed copies the HTML file to its database.
- 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 19** 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.

**TABLE 19** Tokens that you can use in the guest pass printout (continued)

Token	Description
{GP_VALID_TIME}	Date and time when the guest pass expires.
{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.

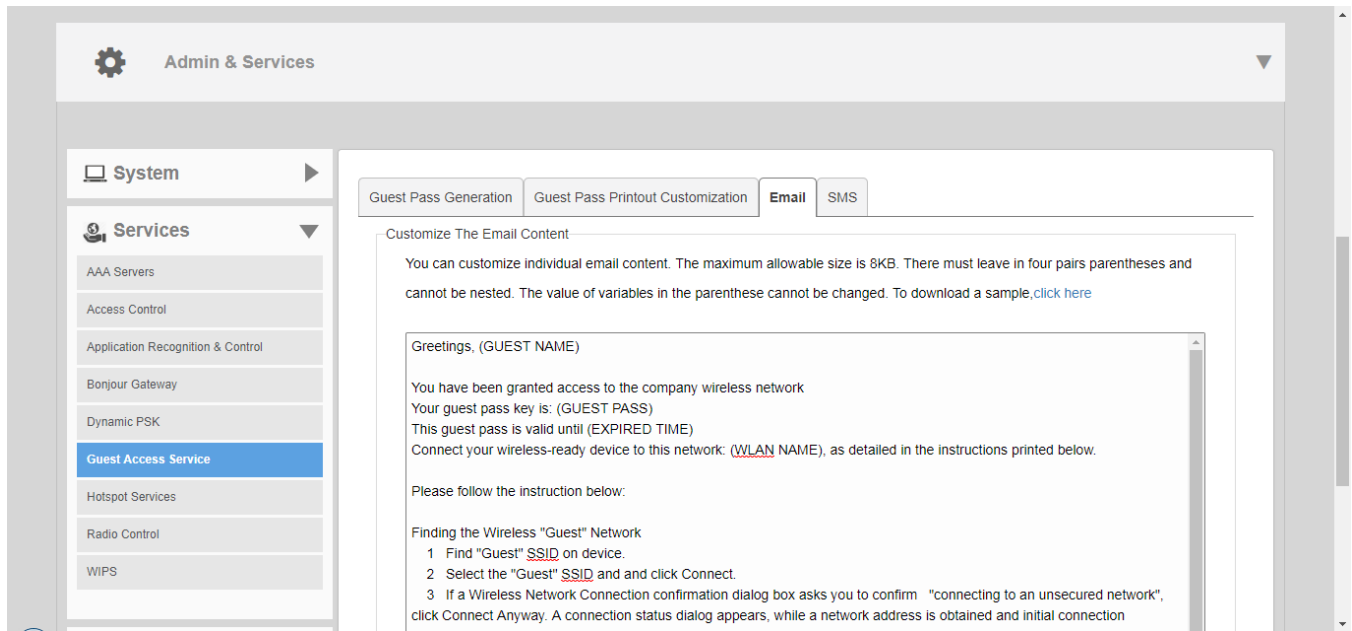
**NOTE**

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 120.

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 95** Customize guest pass email content



## Customizing the Guest Pass SMS Content

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

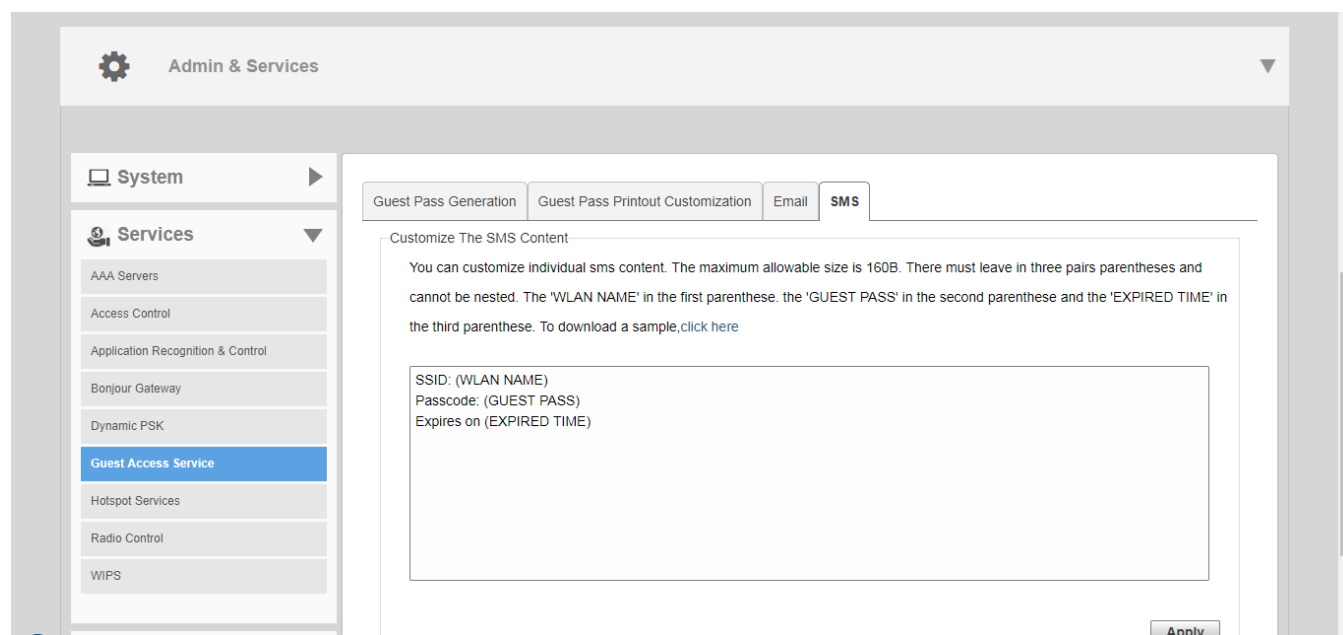
### NOTE

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 120.

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 96** 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 161
- [Google/Google+](#) on page 161
- [LinkedIn](#) on page 167
- [Microsoft Live](#) on page 170

## WLAN Configuration

### Guest WLANs

- [WeChat](#) on page 174

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

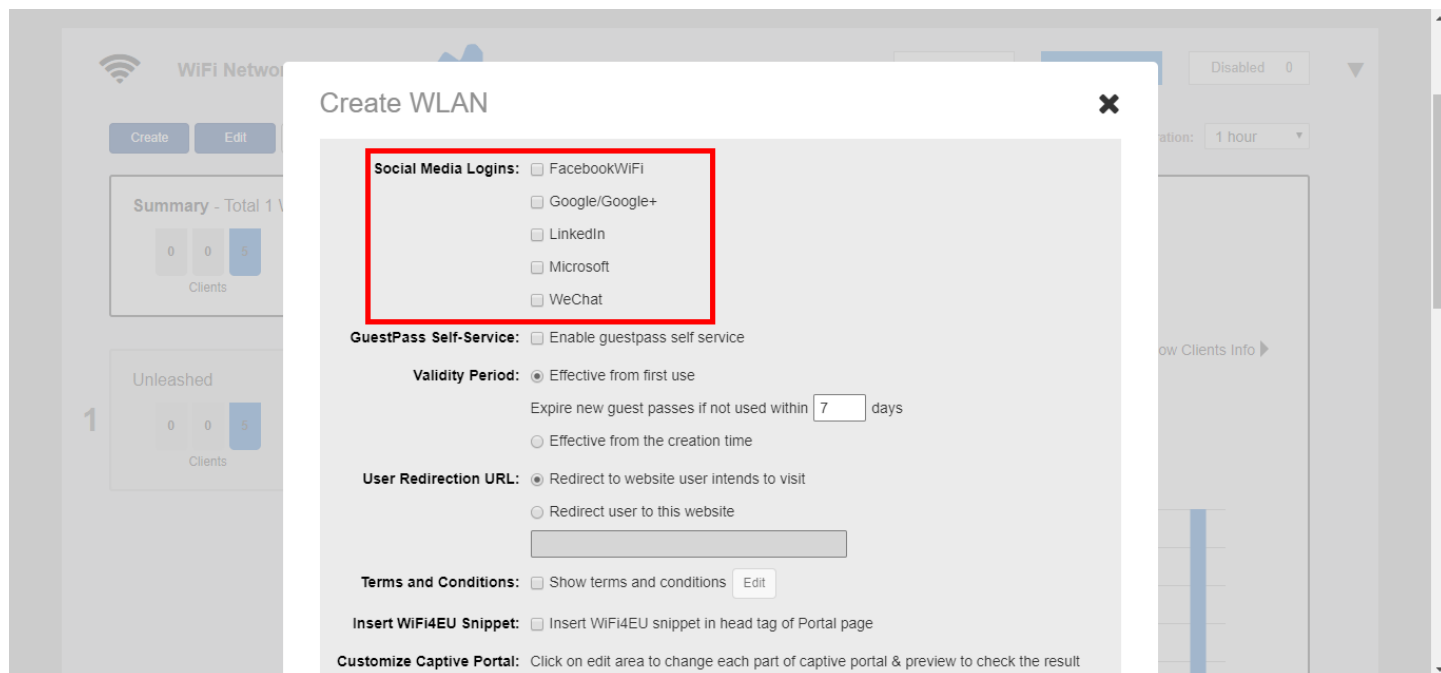
Beginning with release 200.6, multiple social media login types can be enabled for the same WLAN.

**FIGURE 97** Creating a Social Media WLAN

The screenshot displays the configuration page for a WLAN named "social-media". The "Usage Type" is set to "Guest Access", which is highlighted with a red box. The "Guest Authentication" is set to "Guest Pass and Social Login", also highlighted with a red box. The "Guest Password" is set to "Unique password for each guest". The "Validity Period" is set to "Effective from first use" with an expiration of 7 days. The "Grace Period" is checked and set to 480 minutes. The "Authentication Method" is "Open", "Encryption Method" is "None", and the "Accounting Server" is "Disabled".



FIGURE 98 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.

Unleashed provides a default internal Google client ID. If you do not have or do not want to create your own client ID, leave the **Use my own client ID** check box unchecked.

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.

## WLAN Configuration

### Guest WLANs

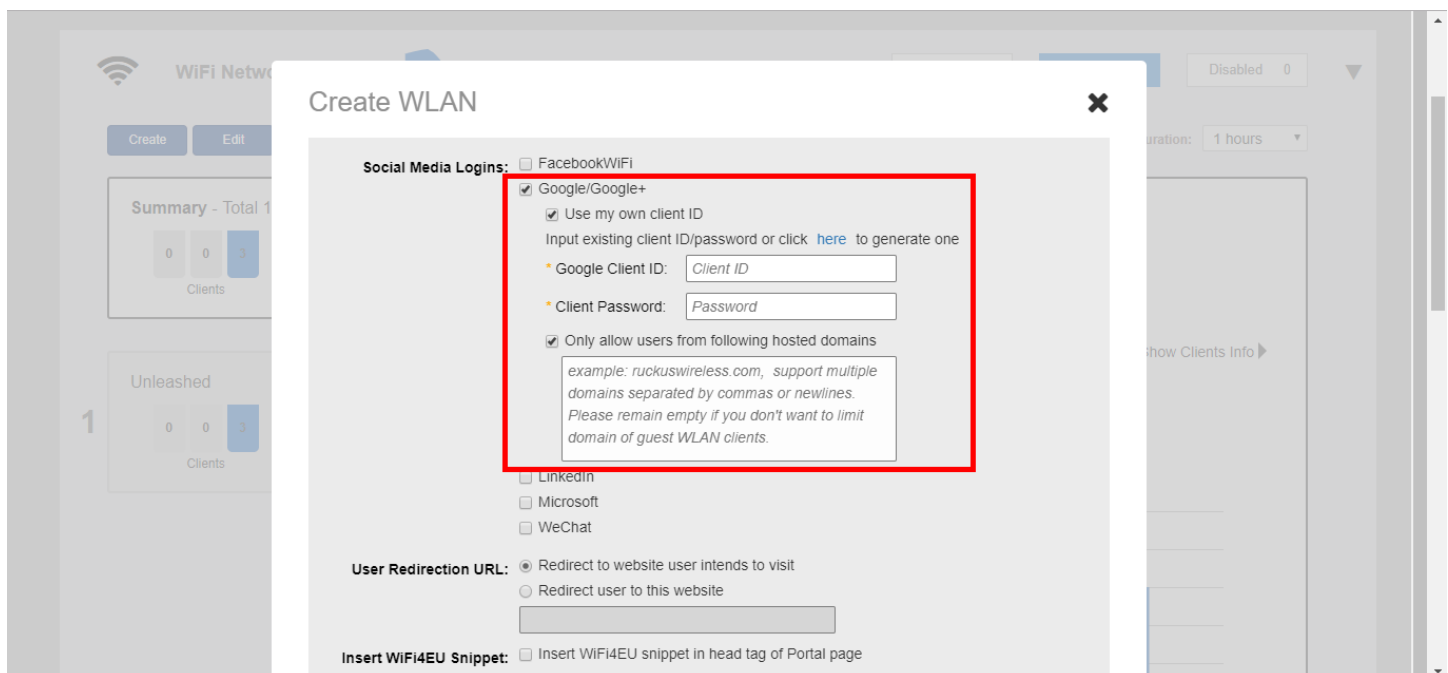
To limit Google/Google+ login to a specific domain or several domains, enable the **Only allow users from the following hosted domains** option and enter the domain names, separated by commas, in the text box below.

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 this feature and enter the company's Google domain (*company\_name.gmail.com*). This will prevent 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 99** Unleashed provides a default client ID, or you can use an existing Google client ID and password



The screenshot shows the 'Create WLAN' configuration dialog in the Unleashed interface. The 'Social Media Logins' section is expanded, and the 'Google/Google+' option is selected. The 'Only allow users from following hosted domains' checkbox is checked. A red box highlights the 'Google/Google+' section, including the 'Use my own client ID' option, the 'Google Client ID' and 'Client Password' input fields, and the 'Only allow users from following hosted domains' checkbox and its associated text box. The text box contains the following text: 'example: ruckuswireless.com, support multiple domains separated by commas or newlines. Please remain empty if you don't want to limit domain of guest WLAN clients.'

### 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. Manually generate an OAuth 2.0 client ID for Google+ social media WLANs using the following procedure.

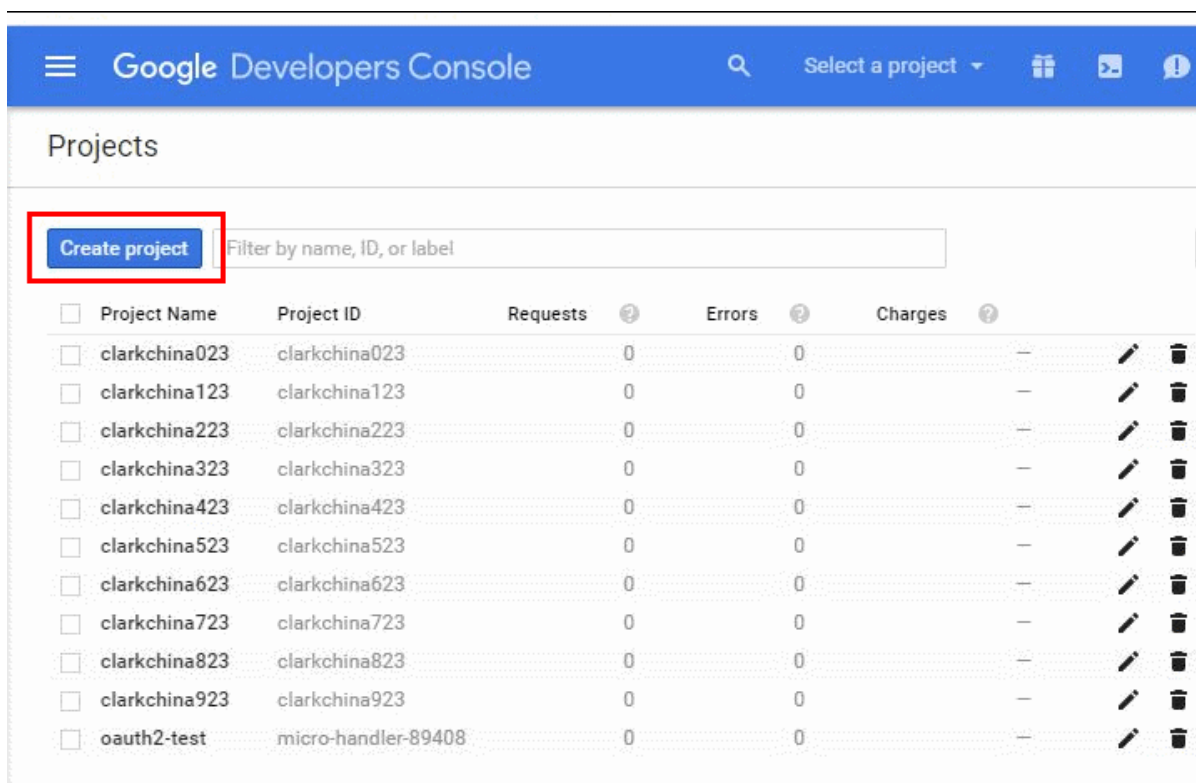
To create a project ID in the Google Developers Console:

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**

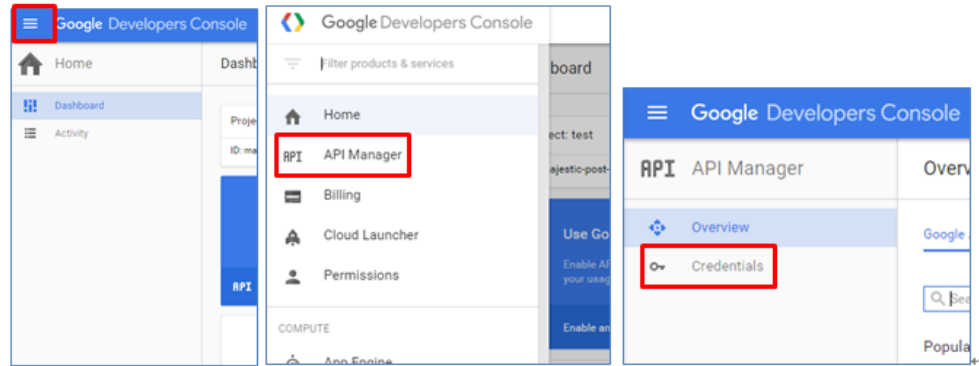
Alternatively, click the **Click here** link to create a new application/project link from within the Unleashed guest access settings.

**FIGURE 100** Create new project on Google OAuth Console



2. Once the project has been created, go to the **Credentials** page and create new credentials for it.

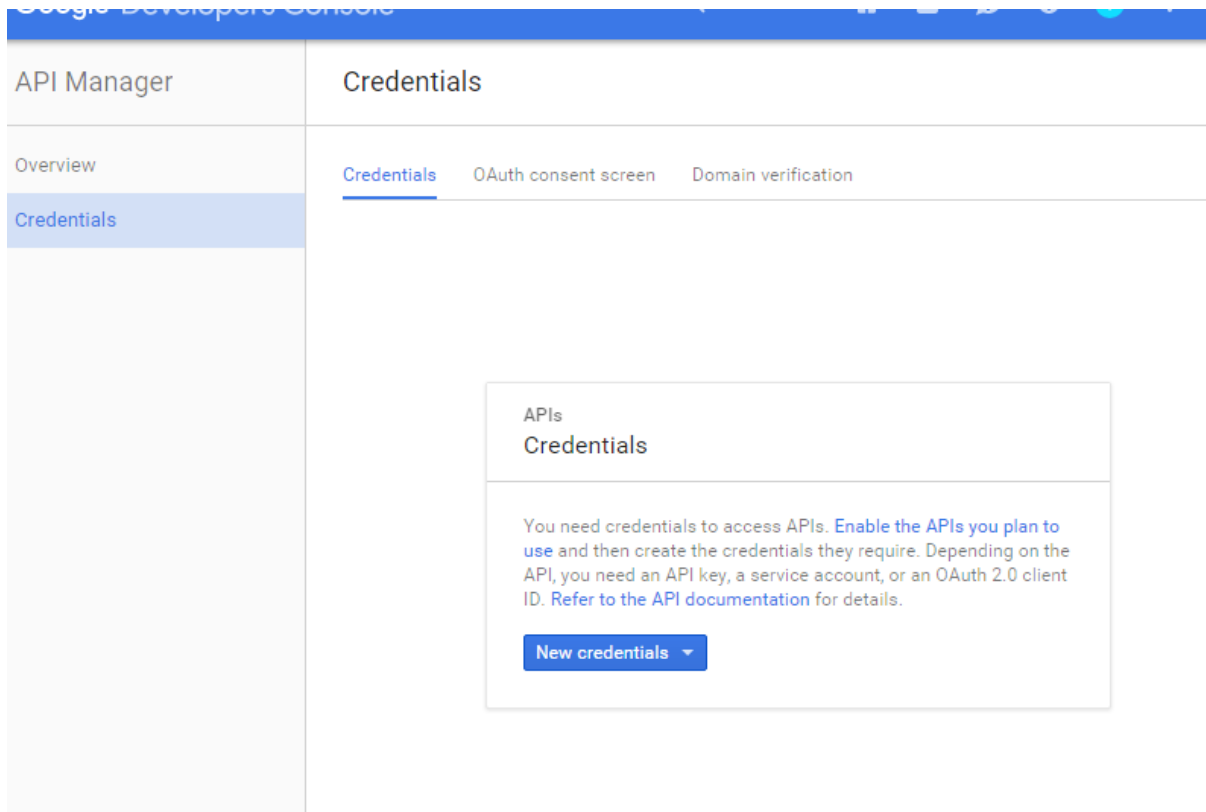
**FIGURE 101** How to get to the Credentials page



Alternatively, use this link to go directly to the Credentials page and select the project: [https://console.developers.google.com/project/\\_/apiui/credential](https://console.developers.google.com/project/_/apiui/credential).

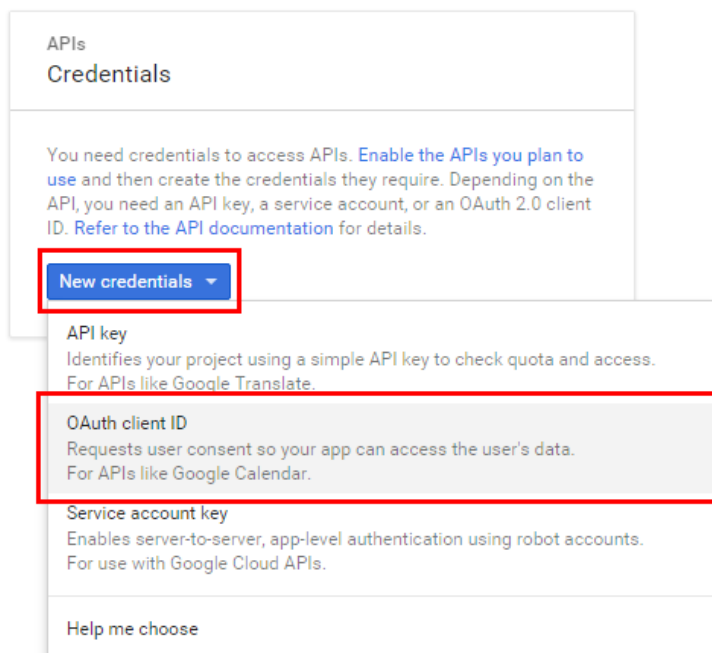
3. The **Credentials** page appears, as shown below.

**FIGURE 102** Credentials page



4. Click **New credentials**, and select **OAuth client ID** as shown below

**FIGURE 103** New credentials - OAuth client ID



- For Application type, select Web application, and for Authorized redirect URIs, enter *unleashed.ruckuswireless.com* as shown below.

**NOTE**

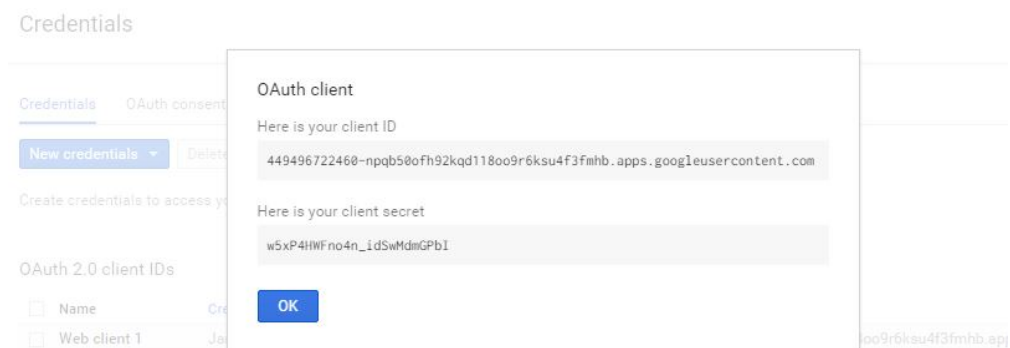
If you have imported a certificate with FQDN to Unleashed, you should use the real FQDN instead of “unleashed.ruckuswireless.com”. For example, if the FQDN is “mydomain.com”, the Authorized redirect URIs should be “<http://mydomain.com/user/auth.jsp>”.

**FIGURE 104** Select Web application and enter Authorized redirect URI

The screenshot shows the 'Credentials' configuration page in the Unleashed management interface. The page is divided into a left sidebar and a main content area. The main content area has a title 'Credentials' and a back arrow icon. Below the title, there is a section for 'Create client ID'. Underneath, the 'Application type' is set to 'Web application', which is highlighted with a red box. Other options include 'Android Learn more', 'Chrome App Learn more', 'iOS Learn more', 'PlayStation 4', and 'Other'. The 'Name' field contains 'Web client 1'. The 'Restrictions' section includes 'Authorized JavaScript origins' with the value 'http://www.example.com' and 'Authorized redirect URIs' with the value 'http://zd.ruckuswireless.com/user/auth.jsp', both of which are highlighted with red boxes. At the bottom, there are 'Create' and 'Cancel' buttons.

6. Click **Create**. If successful, Google will display a **Client ID** and **Client secret**, as shown.

**FIGURE 105** OAuth Client ID and Client Secret



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

### LinkedIn

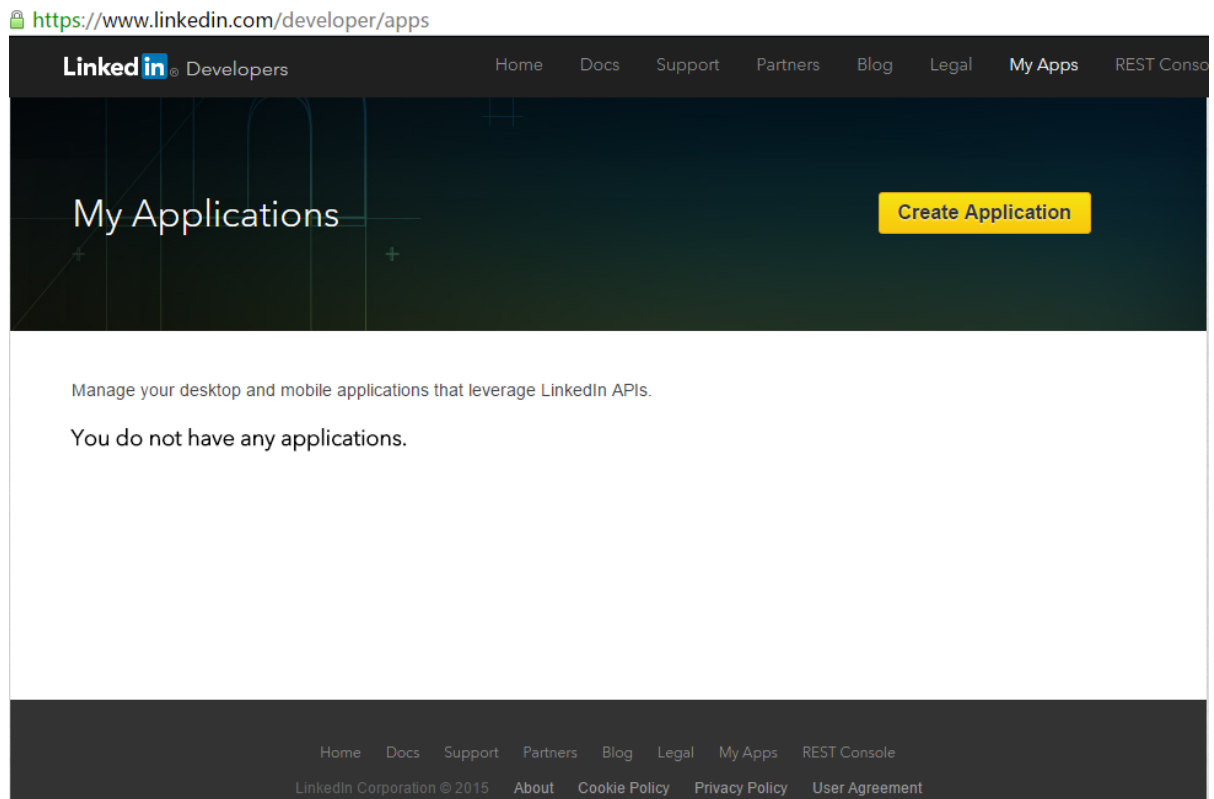
To configure a LinkedIn social media WLAN, you must first configure an application on the LinkedIn developer apps website.

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**

1. Go to the following URL to access the LinkedIn developer network: <https://www.linkedin.com/developer/apps>.

**FIGURE 106** LinkedIn My Applications



2. Click **Create application**.



3. Enter the required application information and click **Submit**.

**FIGURE 107** Create a New LinkedIn Application

Create a New Application


**Company Name: \***  
Create a new Company ▾

**Company Name: \***

**Name: \***

**Description: \***

**Application Logo: \***



**Application Use: \***  
Select One... ▾

**Website URL: \***

**Business Email: \***

**Business Phone: \***

I have read and agree to the [LinkedIn API Terms of Use](#).

4. LinkedIn will provide you with the **Client ID** and **Client Secret**. Enter a valid redirect callback URL: <http://unleashed.ruckuswireless.com/user/auth.jsp>.

**NOTE**

If you have imported a certificate with FQDN to Unleashed, you should use the real FQDN instead of “unleashed.ruckuswireless.com”. For example, if the FQDN is “mydomain.com”, the Authorized redirect URIs should be “<http://mydomain.com/user/auth.jsp>”.

**FIGURE 108** LinkedIn Authentication Keys

Authentication Keys

Client ID: 756d9w65zy52n

Client Secret: jdFAZ3geOV9yiBbQ

Default Application Permissions

r\_basicprofile     r\_emailaddress     rw\_company\_admin  
 w\_share

OAuth 2.0

Authorized Redirect URLs:

5. Change the application status from “Development” to “Live”.

### 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](https://portal.azure.com/#blade/Microsoft_AAD_RegisteredApps/ApplicationsListBlade).

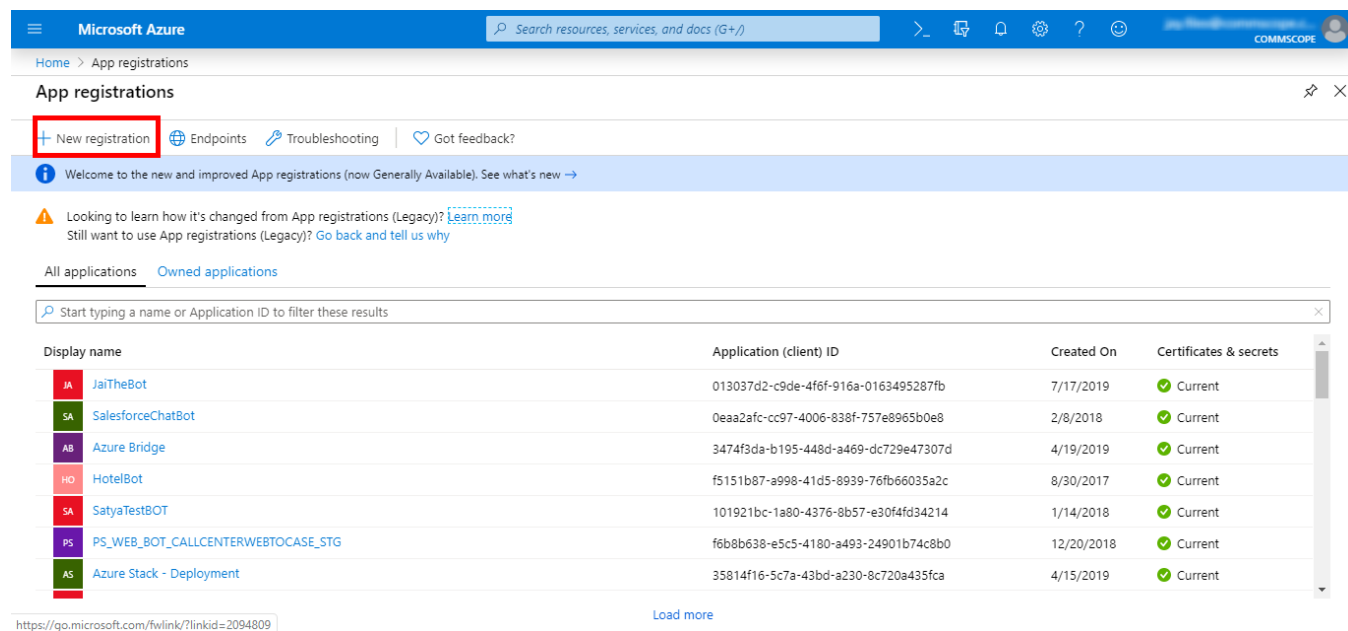
### OAuth Setup Procedure for Microsoft Live Social Media Login

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](https://portal.azure.com/#blade/Microsoft_AAD_RegisteredApps/ApplicationsListBlade).

2. Click **New Registration**.

**FIGURE 109** Create a new app registration



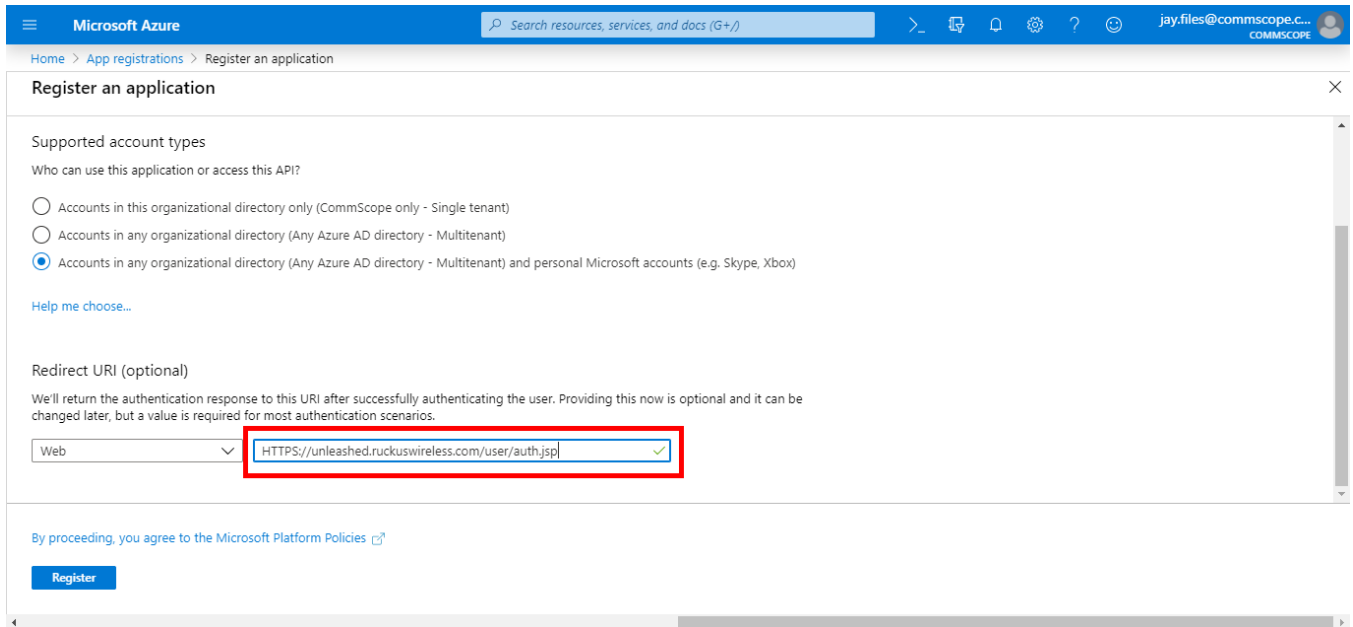
3. Enter a **Name** for the application.
4. For Support Account Types, select the **Accounts in any organizational directory and personal Microsoft accounts** button (see [Figure 110](#)).

5. In **Redirect URI**:, provide a valid redirect callback URL, for example:
  - [HTTPS://unleashed.ruckuswireless.com/user/auth.jsp](https://unleashed.ruckuswireless.com/user/auth.jsp) (see [Figure 110](#)).

**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".

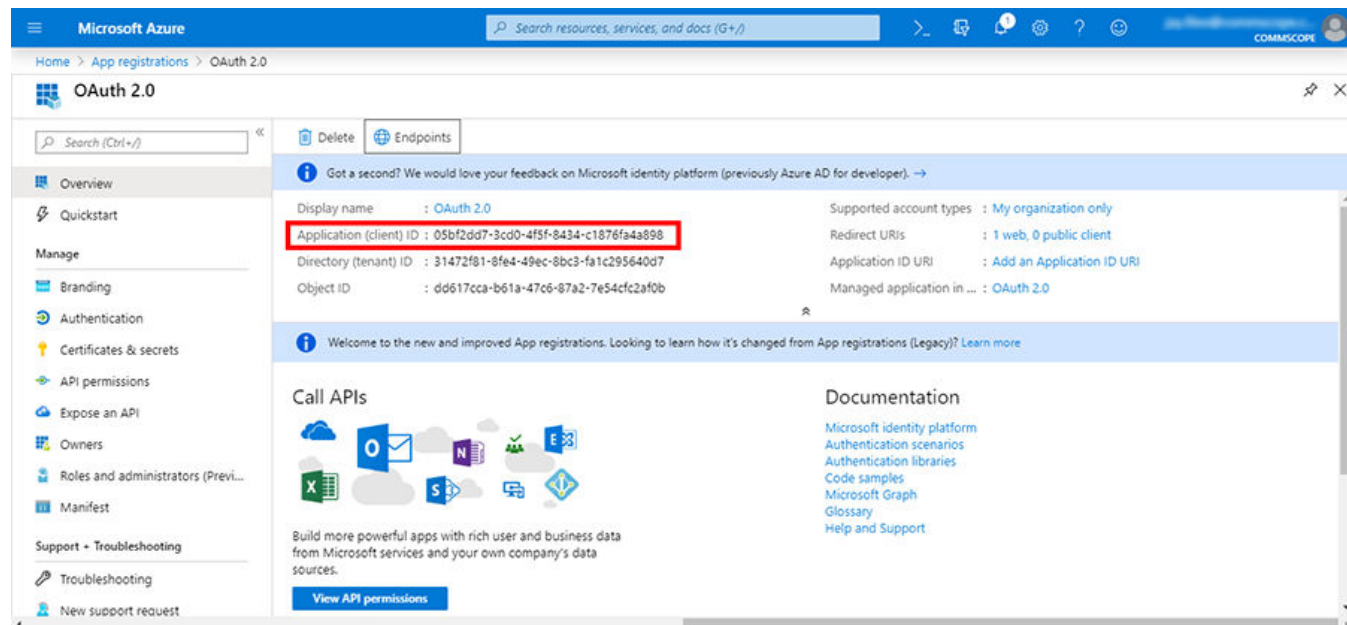
**FIGURE 110** Register an Application configuration settings



6. Click **Register**.

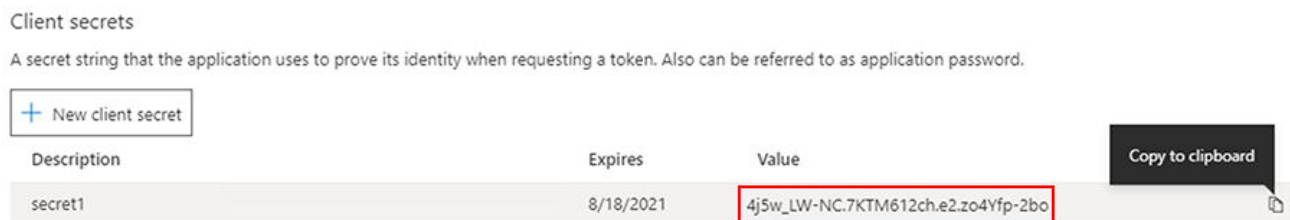
7. Microsoft will provide you with the **Application (client) ID**. Take note of this value, as you will need to enter it into the Unleashed web interface later.

**FIGURE 111** 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 112** 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 111](#).
  - Client Password: The client secret described in [Figure 112](#).

**FIGURE 113** Create WLAN configuration screen - Microsoft Social Media Login

## Create WLAN

The screenshot shows the 'Create WLAN' configuration screen. Under 'Social Media Logins', the 'Microsoft' option is selected with a checked checkbox. Below it, there is a text input field for 'Microsoft Client ID' containing 'Client ID' and another for 'Client Password' containing 'Password'. There are also radio buttons for 'Enable HTTPS' (selected) and 'Enable HTTP'. Below these are checkboxes for 'WeChat', 'FacebookWiFi', 'Google/Google+', and 'LinkedIn'. Under 'GuestPass Self-Service', there is a checkbox for 'Enable guestpass self service'. Under 'Validity Period', the 'Effective from first use' option is selected, and a text input field shows '7' days. The 'Effective from the creation time' option is also visible.

### 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.

- 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.)
- 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 114** Enter domain name or IP addresses to allow access to unauthenticated users

The screenshot displays the configuration page for a Walled Garden. At the top, there are several settings:
 

- Grace Period:** A checkbox for "Allow users to reconnect without re-authentication for" is checked, with a value of 480 minutes.
- Authentication Method:** Radio buttons for "Open", "802.1X EAP", and "MAC Address". "Open" is selected.
- Encryption Method:** Radio buttons for "WPA2", "WPA3", "WPA2/WPA3-Mixed", "OWE", and "None". "None" is selected.
- Accounting Server:** A dropdown menu set to "Disabled" with a "+" icon to add a server. Below it, "Send Interim-Update every" is set to 10 minutes.

 Below these settings is a "Hide Advanced Options" link. A series of tabs are present: "Restricted Subnet Access", "WLAN Priority", "Access Control", "Radio Control", "Walled Garden" (which is highlighted), and "Others".
   
 The "Walled Garden" tab contains the following text:
 

Unauthenticated users are allowed to access the following destinations:  
(e.g. \*.mydomain.com, mydomain.com, \*.mydomain.\*, 192.168.1.1:80, 192.168.1.1/24 or 192.168.1.1:80/24)

 Below this text is a table with the following structure:
 

Order	Destination Address	Action
1	*.mydomain.com	Save Cancel

 At the bottom left of the table area are "Create New" and "Delete" buttons. At the bottom right of the entire configuration area are "Next" and "Cancel" buttons.

## 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.

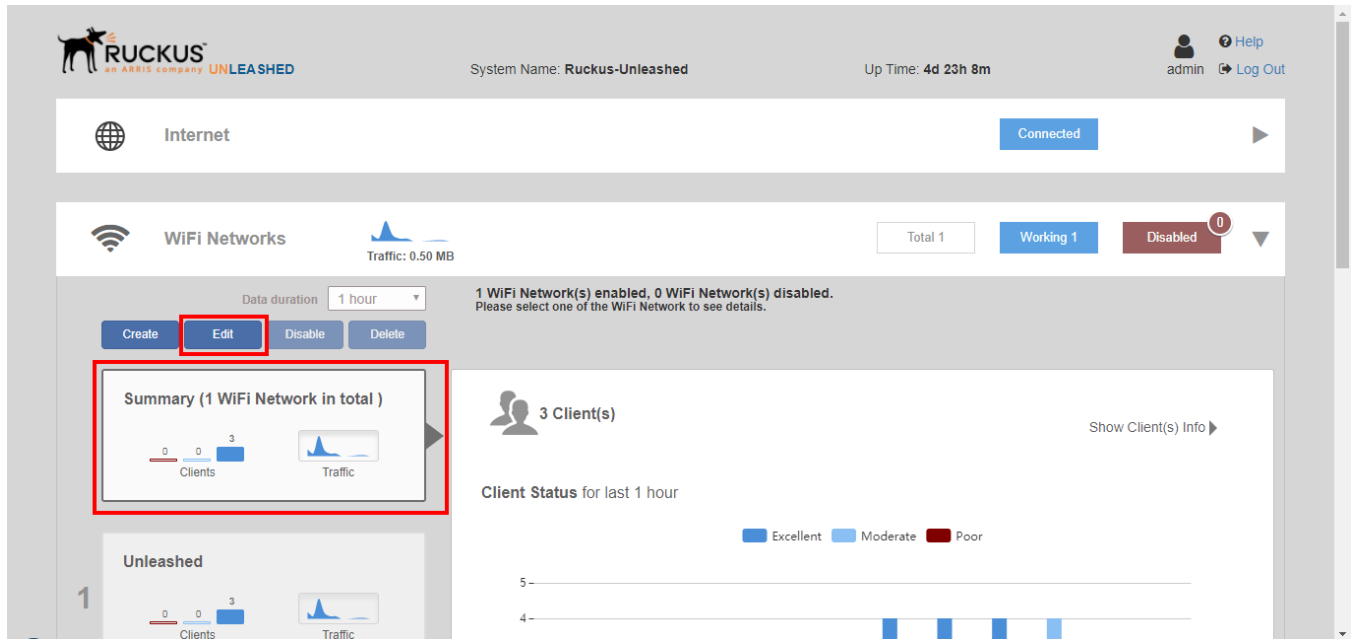
Unleashed supports Hotspot WLANs that conform to the WISPr (Wireless Internet Service Provider roaming) standard. For more information on Hotspot services, see [Hotspot Services](#) on page 326.

## Configuring Global WLAN Settings

Select the Summary box and click Edit to edit global settings for all WLANs.

1. To configure global settings for all WLANs, expand the **Wi-Fi Networks** section, select the Summary WLAN box, and click the **Edit** button.

**FIGURE 115** Click Edit to configure global settings for all WLANs



2. When the **Global Configuration** dialog appears, select any 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**

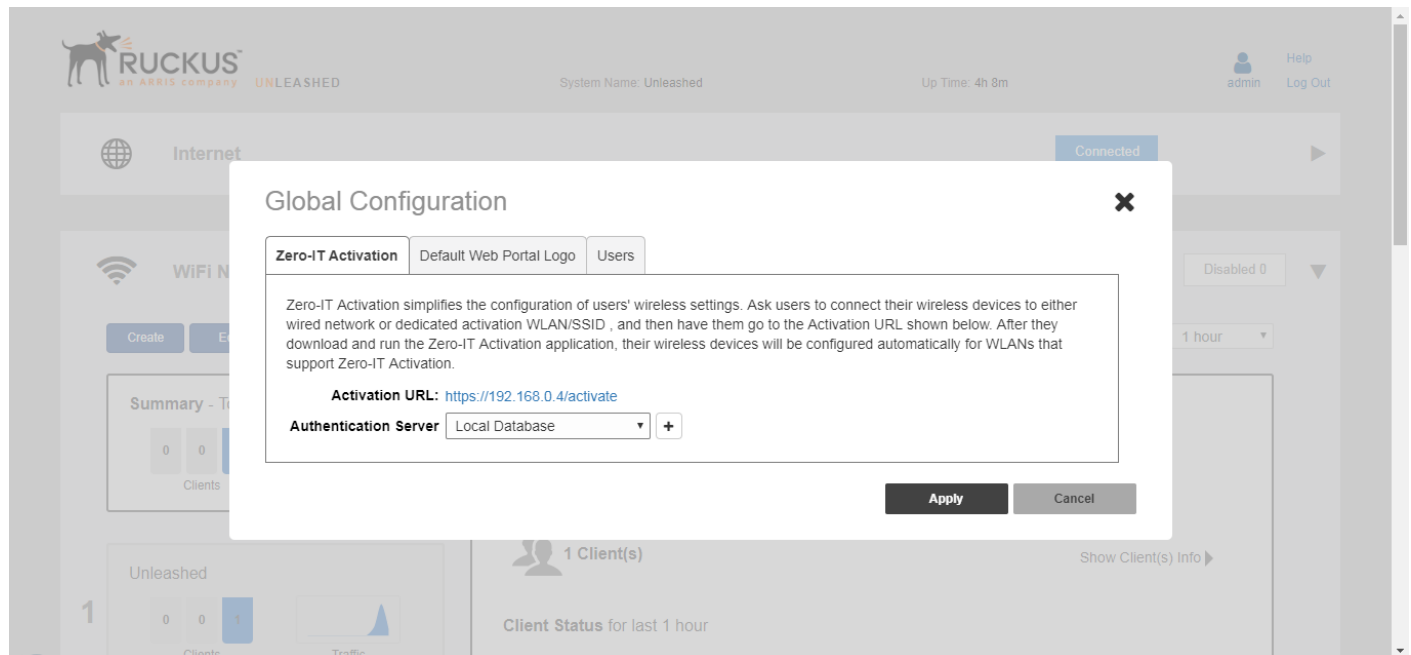
The recommended image size is 138 x 40 pixels. Max file size is 20kb.

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



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

**FIGURE 116** Global Configuration settings for all WLANs



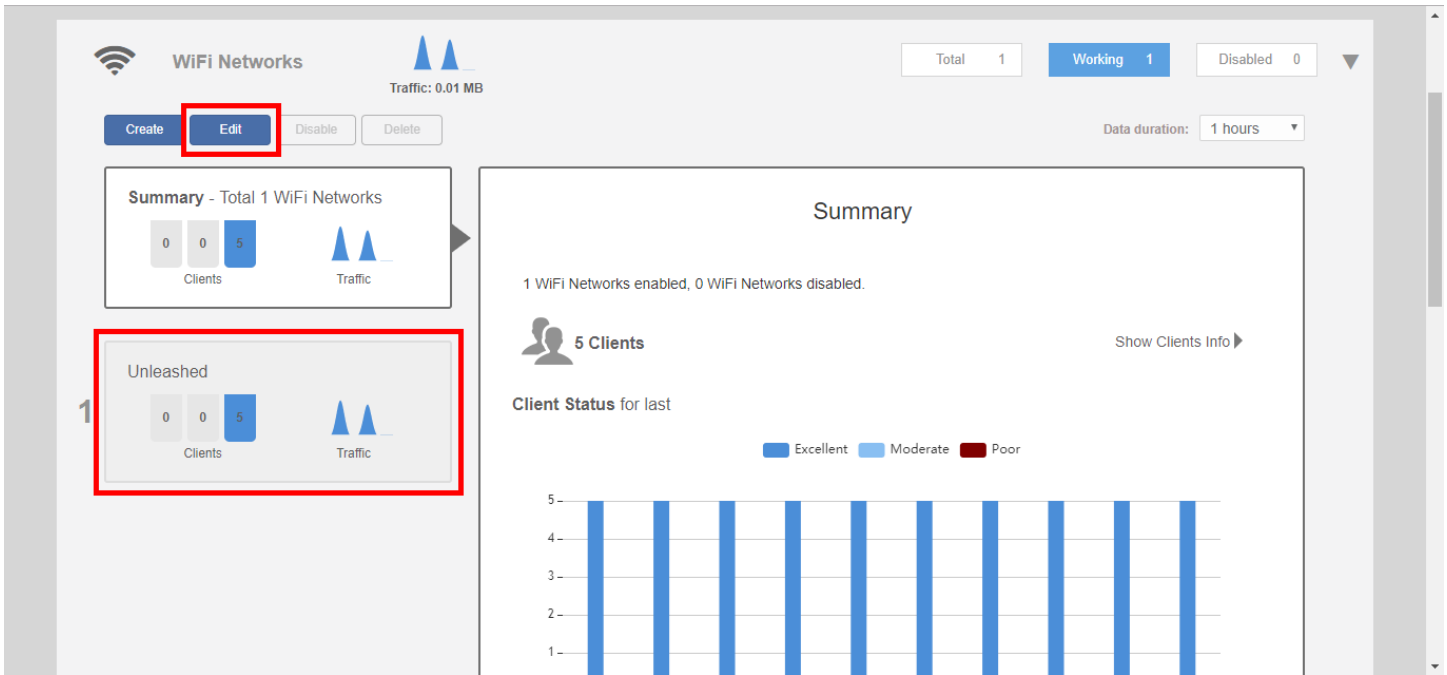
## Editing an Existing WLAN

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

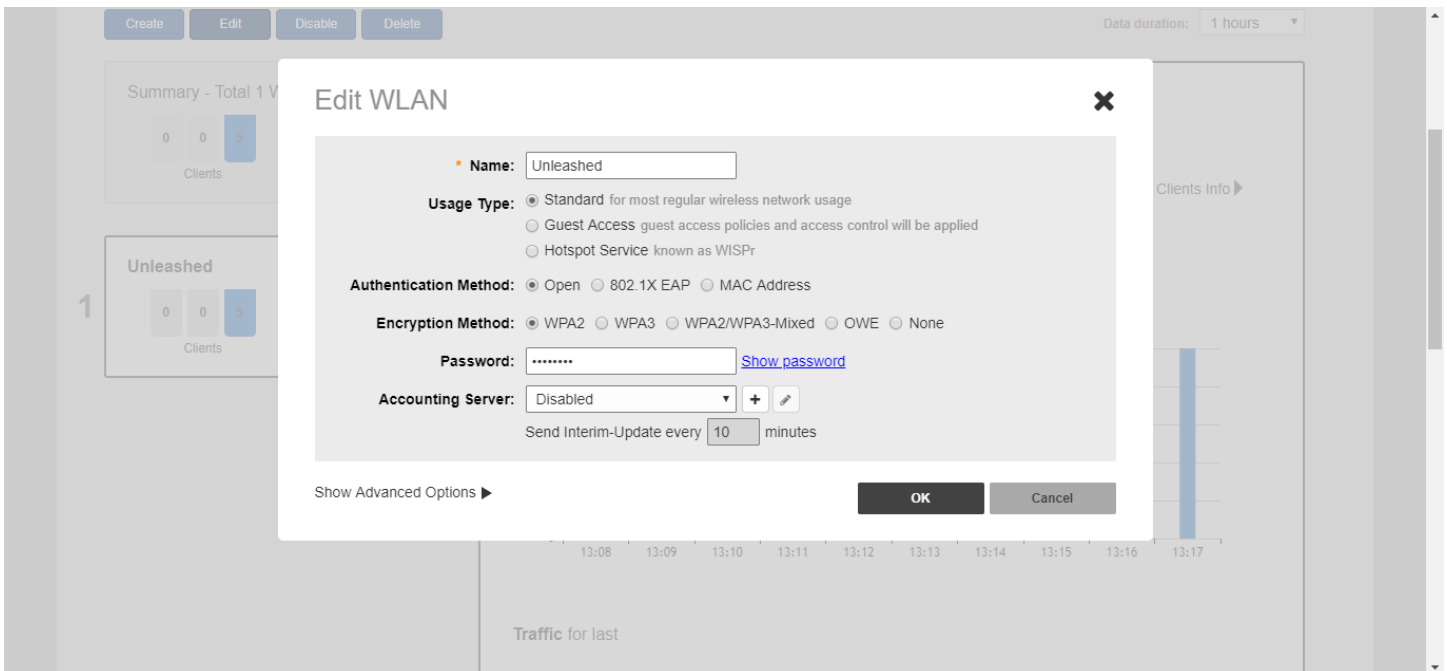
## WLAN Configuration

### Editing an Existing WLAN

**FIGURE 117** Click Edit to edit an existing WLAN



**FIGURE 118** Modify WLAN settings

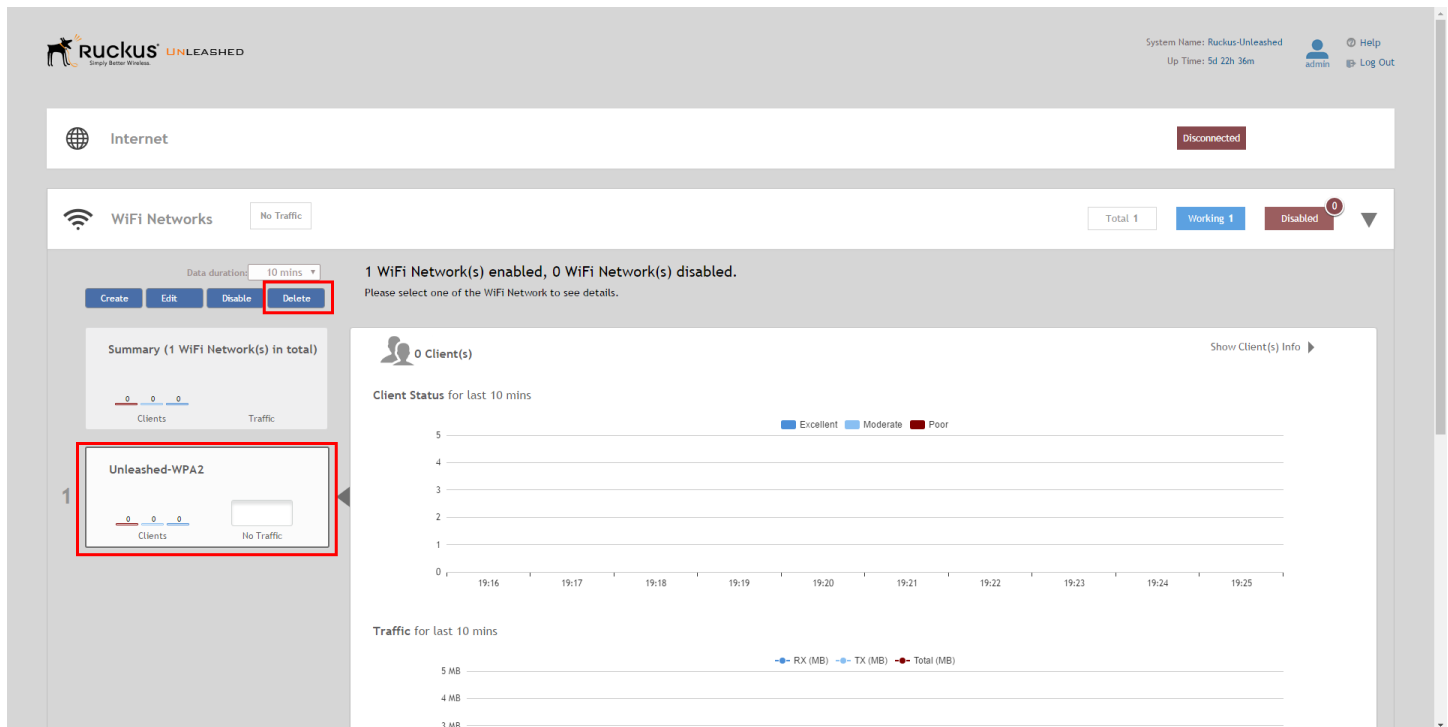


If you made any changes, click **OK** to confirm your changes.

## Deleting a WLAN

To delete a WLAN, open the **Wi-Fi Networks** section, select the **WLAN box** from the list on the left side that you want to delete, and click **Delete**.

FIGURE 119 Deleting a WLAN



Click **OK** when prompted to delete the selected WLAN.

## Temporarily Disabling a WLAN

To temporarily disable a WLAN:

1. Open the **Wi-Fi Networks** section, select the **WLAN box** from the list on the left side that you want to disable, and click **Disable**.
2. A confirmation dialog appears, click **OK** to confirm.
3. To re-enable, click the **Enable** button.

# WLAN Configuration

## Temporarily Disabling a WLAN

FIGURE 120 Click Disable to temporarily disable a WLAN

The screenshot displays the 'WiFi Networks' management interface. At the top, it shows 'No Traffic' and a summary of 'Total 4' networks, with 'Working 2' and 'Disabled 2'. Below this, there are buttons for 'Create', 'Edit', 'Disable', and 'Delete'. A 'Data duration' dropdown is set to '10 mins'. A summary section indicates '2 WiFi Network(s) enabled, 2 WiFi Network(s) disabled' and prompts the user to 'Please select one of the WiFi Network to see details.' On the left, a list of four networks is shown: 'Guest WLAN 1', 'Guest WLAN 2', 'Unleashed-WPA2', and 'adsfadsf'. The 'Disable' button for 'Guest WLAN 1' is highlighted with a red box. The right side of the interface shows the details for the selected network, including '0 Client(s)', 'Client Status for last 10 mins' (a bar chart showing 0 clients in Excellent, Moderate, or Poor status), and 'Traffic for last 10 mins' (a line chart showing 0 MB of RX, TX, and Total traffic).

# Advanced WLAN Configuration

---

- [Advanced WLAN Configuration Overview.....](#) 181
- [Configuring Advanced WLAN Options.....](#) 181
- [Zero-IT and DPSK Settings.....](#) 183
- [WLAN Priority Settings.....](#) 189
- [Access Control Settings.....](#) 190
- [Application Policies.....](#) 191
- [Radio Control Settings.....](#) 194
- [Other Advanced WLAN Settings.....](#) 195

## Advanced WLAN Configuration Overview

The WLAN Advanced options include settings such as WLAN priority, access controls, rate limiting, application visibility, radio controls and other advanced settings.

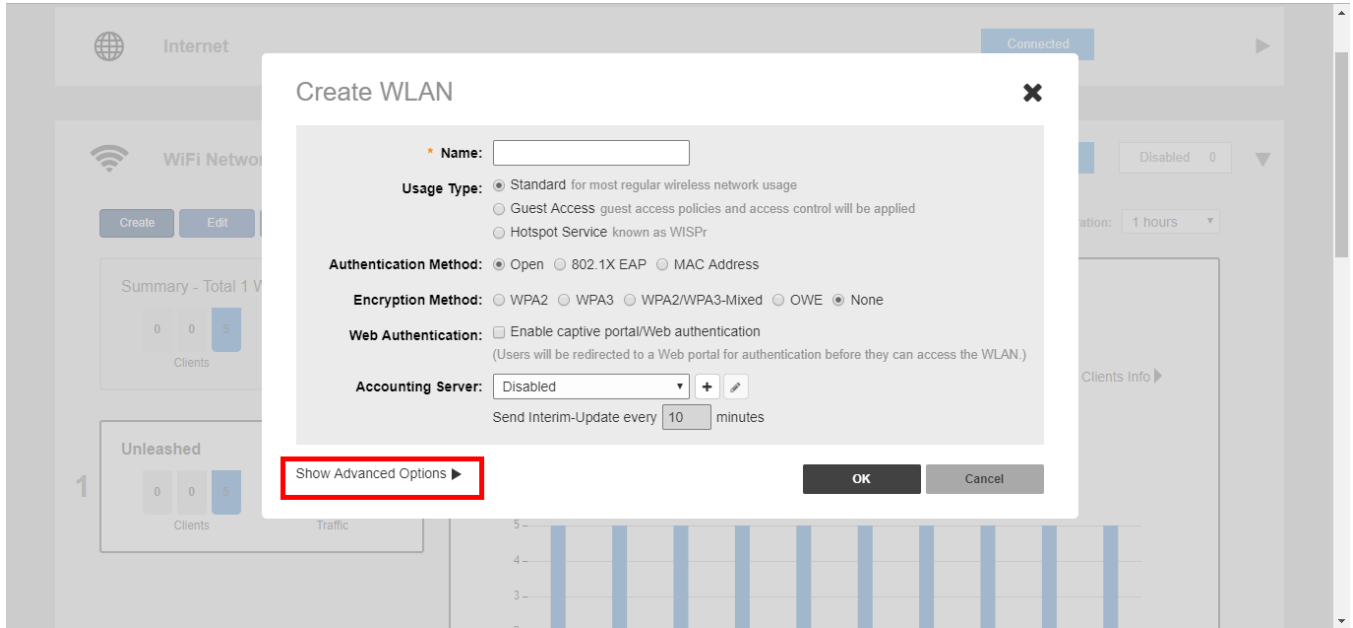
## Configuring Advanced WLAN Options

To edit the advanced options for a WLAN:

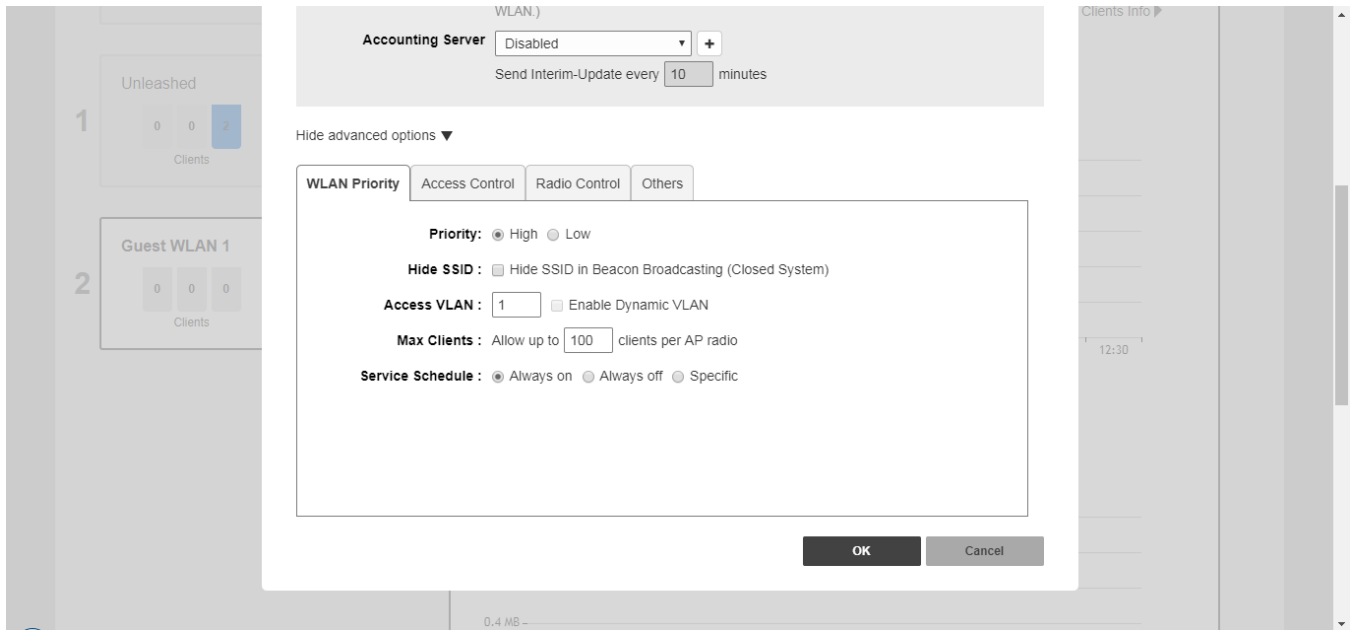
1. Select the WLAN you want to configure from the **Wi-Fi Networks** component and click **Edit**, or click **Create** to create a new custom WLAN.

- Click the arrow next to **Show advanced options** to expand the advanced options section.

**FIGURE 121** Click Show Advanced Options



**FIGURE 122** 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 183.
  - **WLAN Priority:** Contains options for setting the WLAN's priority level, WLAN visibility, Access VLAN, Max Clients and Service Schedule. See [WLAN Priority Settings](#) on page 189.
  - **Access Control:** Contains options for configuring Call Admission Control, Rate Limiting, Access Controls, Application Visibility and Application Denial Policies. See [Access Control Settings](#) on page 190.
  - **Radio Control:** Contains options for configuring radio settings including Fast BSS transition, Background Scanning, Load Balancing and Band Balancing. See [Radio Control Settings](#) on page 194.
  - **Others:** Contains options for configuring Force DHCP, client Inactivity Timeout, and Wireless Client Isolation. See [Other Advanced WLAN Settings](#) on page 195.
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

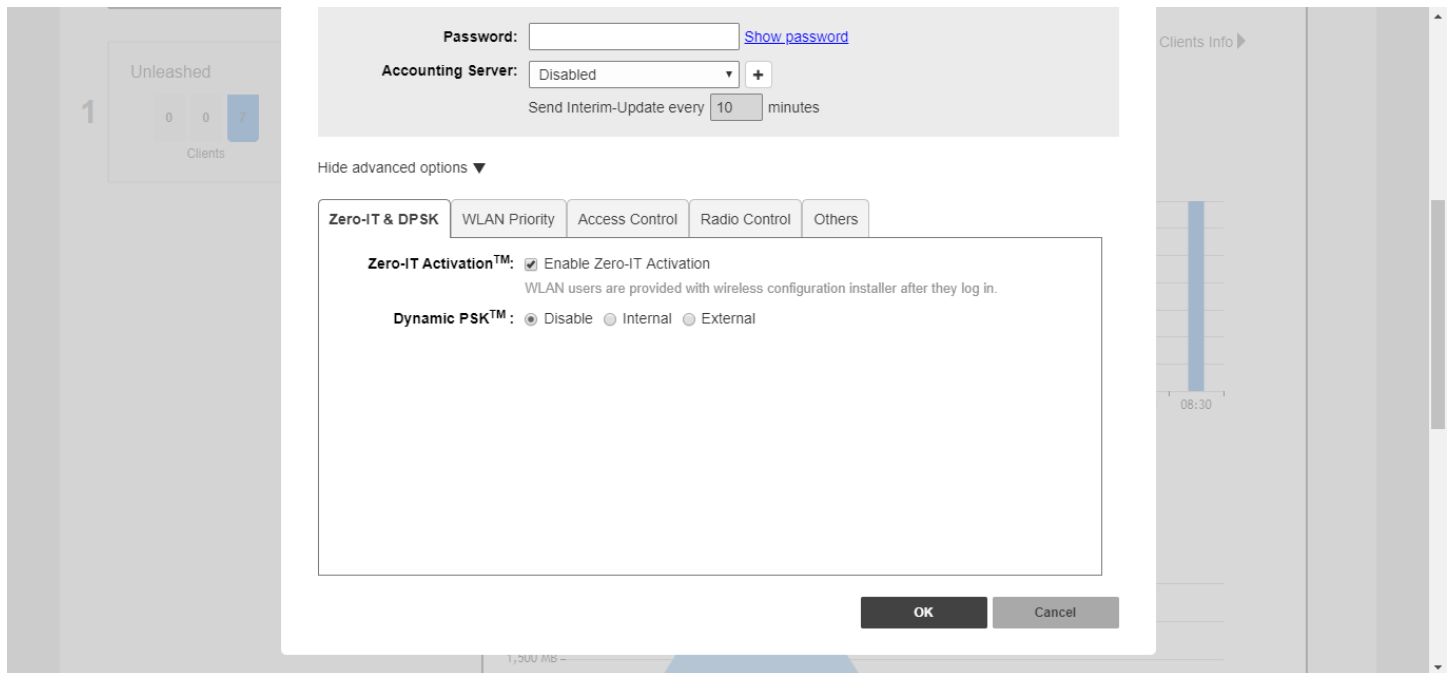
Zero-IT Activation allows network users to self-activate their devices for secure access to your wireless networks with no manual configuration required by the network administrator.

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 123 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 185 for more information).
6. Click **OK** to save.

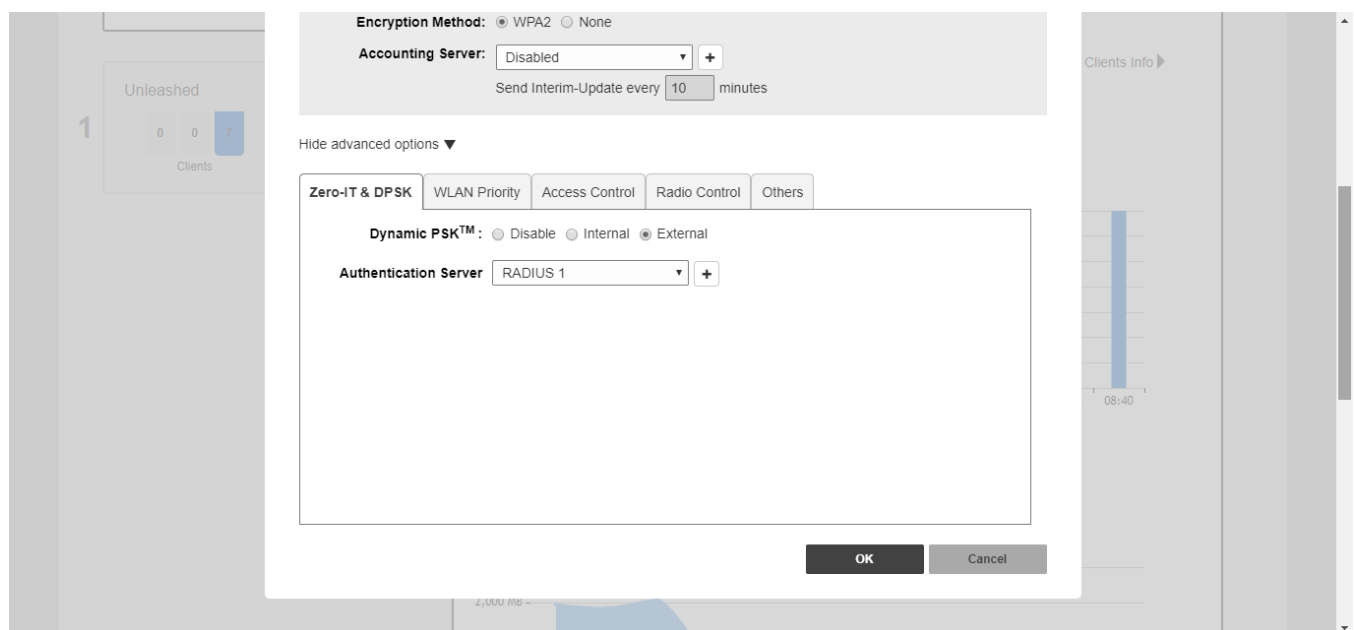
This WLAN is now ready to allow users to self-configure their client devices using a Zero-IT auto-configuration file that will be provided once a user successfully logs in to the WLAN.

## Enabling DPSK for a WLAN

To enable DPSK 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 **Open/WPA2** for **Authentication** and **Encryption** methods.
3. Click **Show advanced options**, then select the **Zero-IT & DPSK** tab.
4. Locate the **Dynamic PSK** settings and select one of the following options:
  - **Internal**: Use the internal database for client authentication.
  - **External**: Use an external AAA (RADIUS) server for client authentication.
5. If using an external RADIUS server for authentication, select the **Authentication Server** from the list, and click **OK** to save.

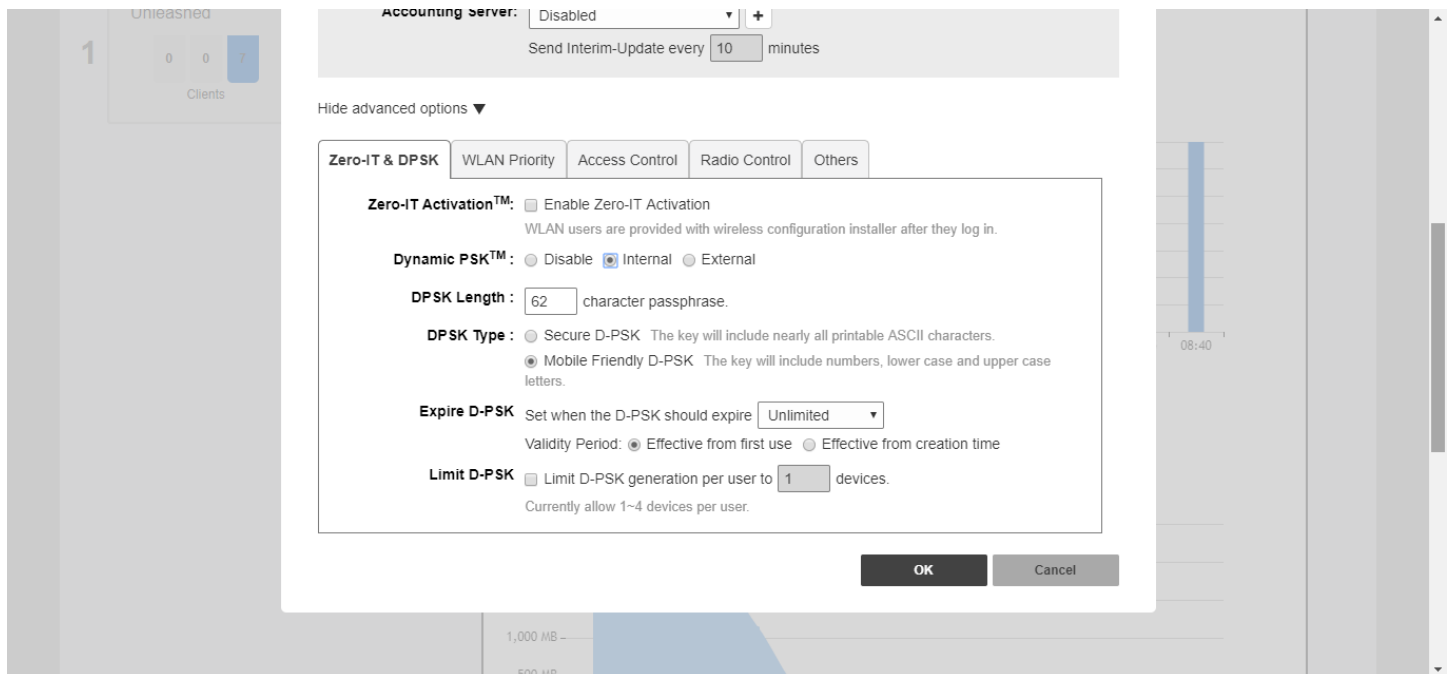
**FIGURE 124** Using an external RADIUS server for DPSK authentication



6. If using the internal database, continue with the following steps.
7. In **DPSK Length**, enter a PSK passphrase length (between 8 and 62 characters).
8. In **DPSK Type**, choose whether to use **Secure DPSK** or **Mobile Friendly DPSK**.
  - **Secure DPSK**: Includes almost all printable ASCII characters, including periods, hyphens, dashes, etc. This option is more secure, however it is difficult to input for mobile clients whose keyboards may not contain the entire set of printable ASCII characters.
  - **Mobile Friendly DPSK**: Choose this option if this WLAN will be used for mobile clients. This option limits the range of characters to lower case and upper case letters and numbers, which 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.)
9. **Expire DPSK**: Set when the DPSK should expire. In **Validity** period, choose whether the DPSK expiration period will start from first use or creation time.
10. **Limit DPSK**: By default each authenticated user can generate multiple DPSKs. Select this option to limit the number of DPSKs each user can generate (1-4).
11. 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 125** Using the internal database for DPSK authentication



**NOTE**

For information on DPSK management and batch generation, see [Dynamic PSK](#) on page 322.

### Using External DPSK with RADIUS Authentication

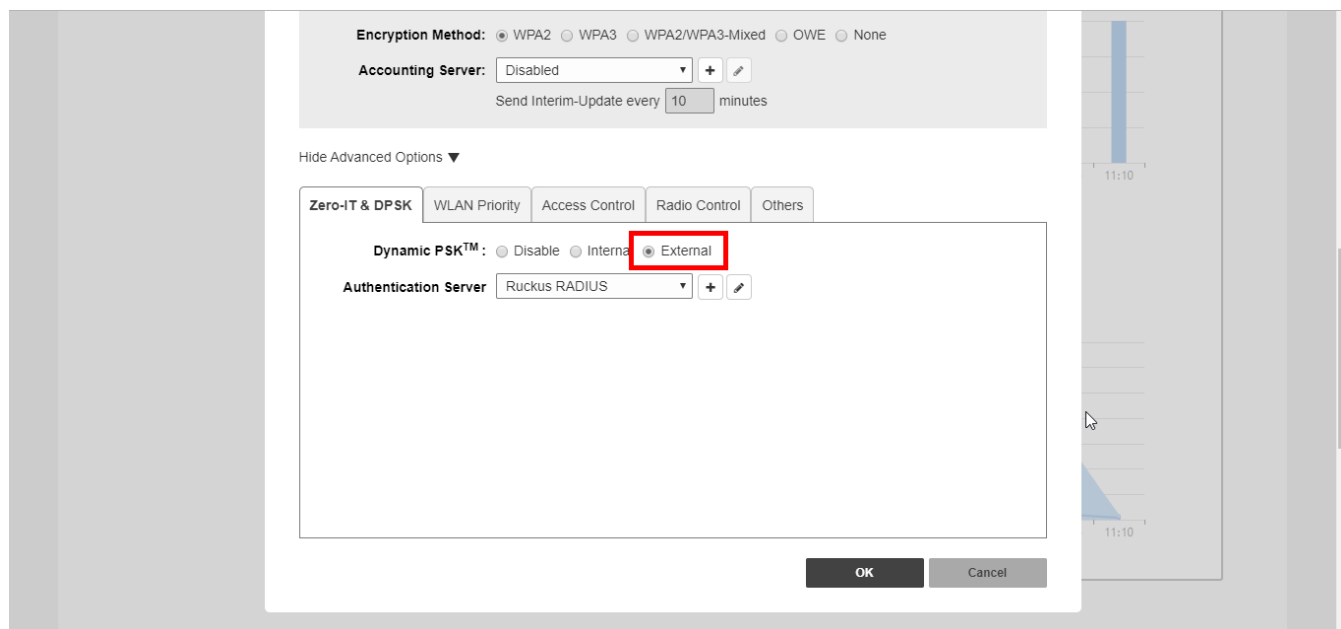
Using an external AAA server for managing Dynamic Pre-Shared Keys provides several advantages to internal DPSKs stored on the AP/controller.

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 126** 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.
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 20** 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 and 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 21** 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.

**TABLE 21** Access-accept/Access-reject message parameters (continued)

4	VLAN assignment	The following triplet of AVPs: <ol style="list-style-type: none"> <li>1. Tunnel-Type</li> <li>2. Tunnel-Medium-Type</li> <li>3. Tunnel-Private-Group-Id</li> </ol>	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 ). <ol style="list-style-type: none"> <li>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).</li> <li>2. Tunnel-Medium-Type is set to the string value of "802"</li> <li>3. Tunnel-Private-Group-Id is set to the value "&lt;VLAN ID&gt;". VLAN ID has a value between 1 and 4094 and is encoded as a string (see RFC-3580).</li> </ol>
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

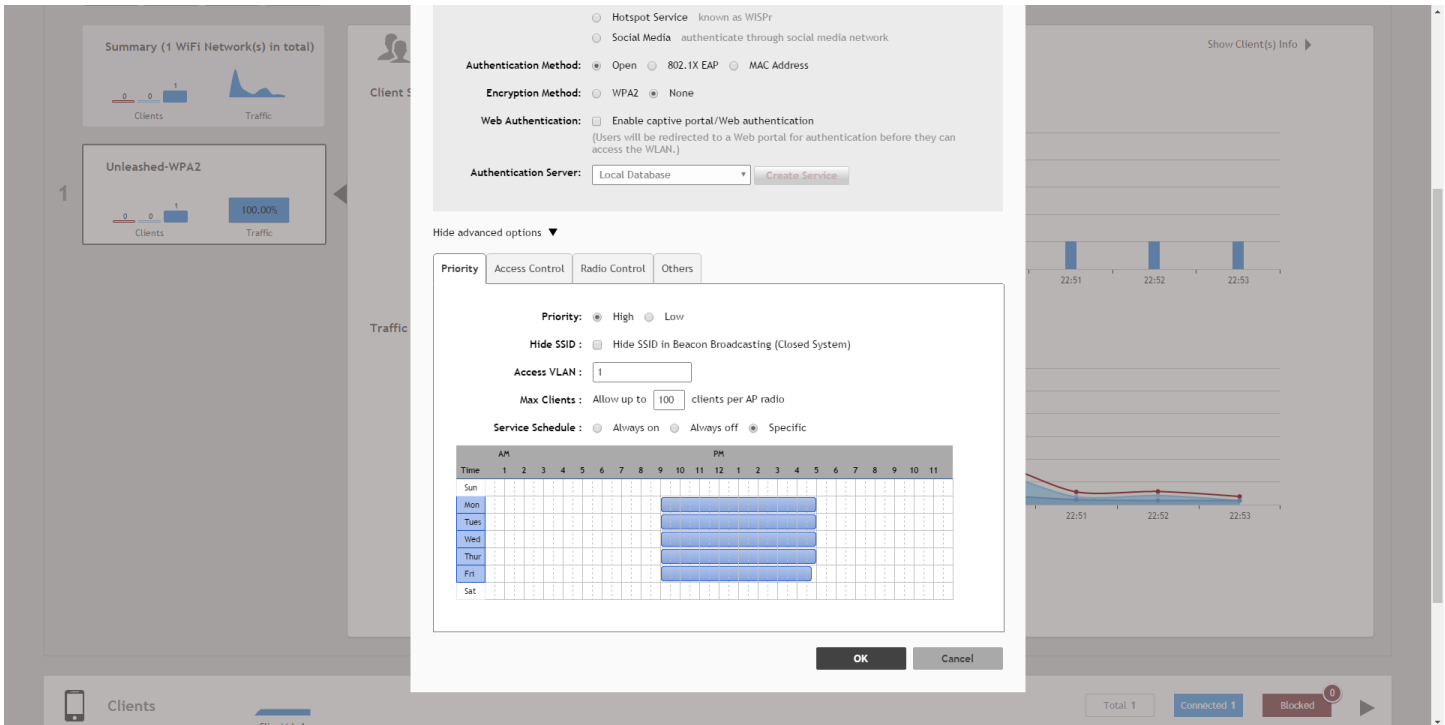
The **WLAN > Advanced Options > Priority** tab provides the following options:

- **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 285.

FIGURE 127 Configuring a specific Service Schedule for a WLAN



## Access Control Settings

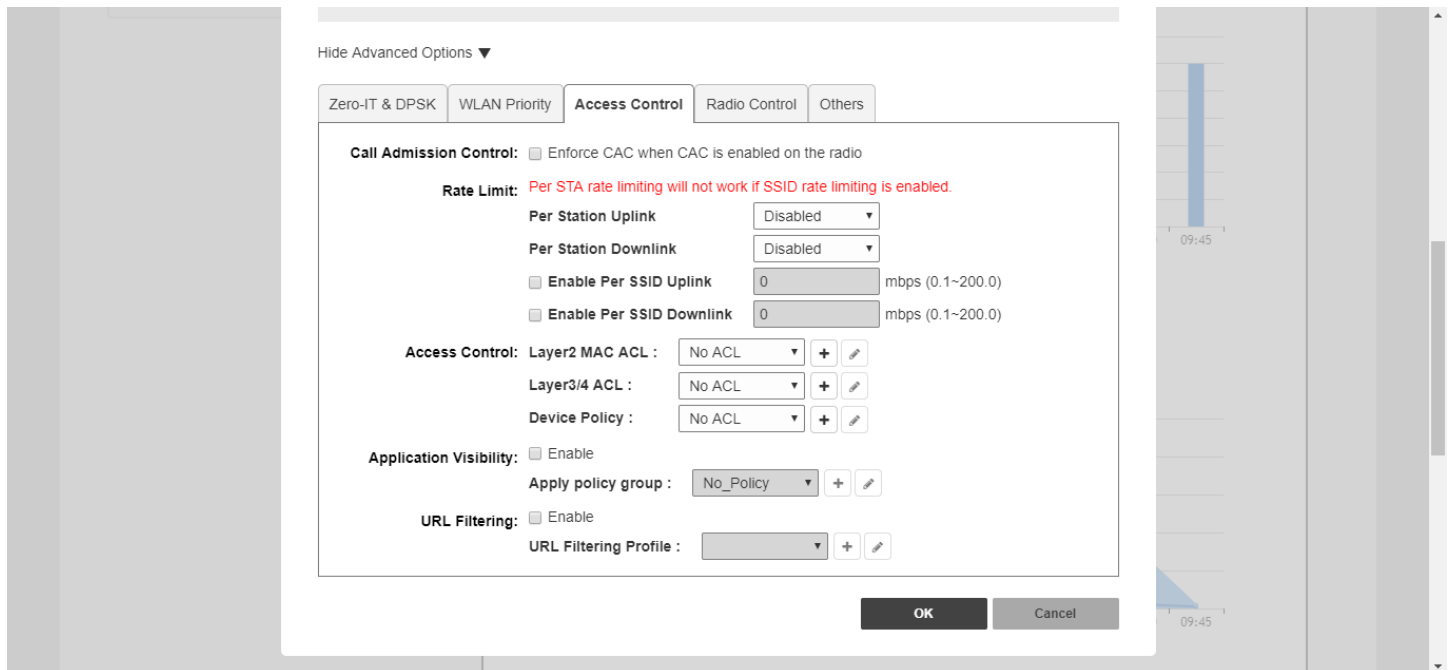
The *WLAN > Advanced Options > Access Control* page provides the following options:

- **Call Admission Control:** (Disabled by default). Enable Wi-Fi Multimedia Admission Control (WMM-AC) to support Polycom/Spectralink VIEW certification. When enabled, the AP announces in beacons if admission control is mandatory or not 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 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 needs to be policed to ensure adequate voice/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 10 calls on the 5 GHz radio (seven active 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 (i.e., client) is limited to the rate specified in the traffic policy, and that policy can be applied on either the uplink or downlink. Toggle 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:** Toggle 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, see [Access Control](#) on page 308.
- **Application Visibility:** Enable this option to allow APs to collect client application data, which can then be consolidated for use by the [Application Recognition and Control](#) on page 313 pie charts, and can be used to deny access or rate limit application traffic based on admin-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, see [Application Policies](#) on page 191.

**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 342.

**FIGURE 128** Advanced WLAN settings - Access Control configuration



## Application Policies

For instructions on configuring Application Control Policies, see [Creating an Application Control Policy](#) on page 192.

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 315.

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**

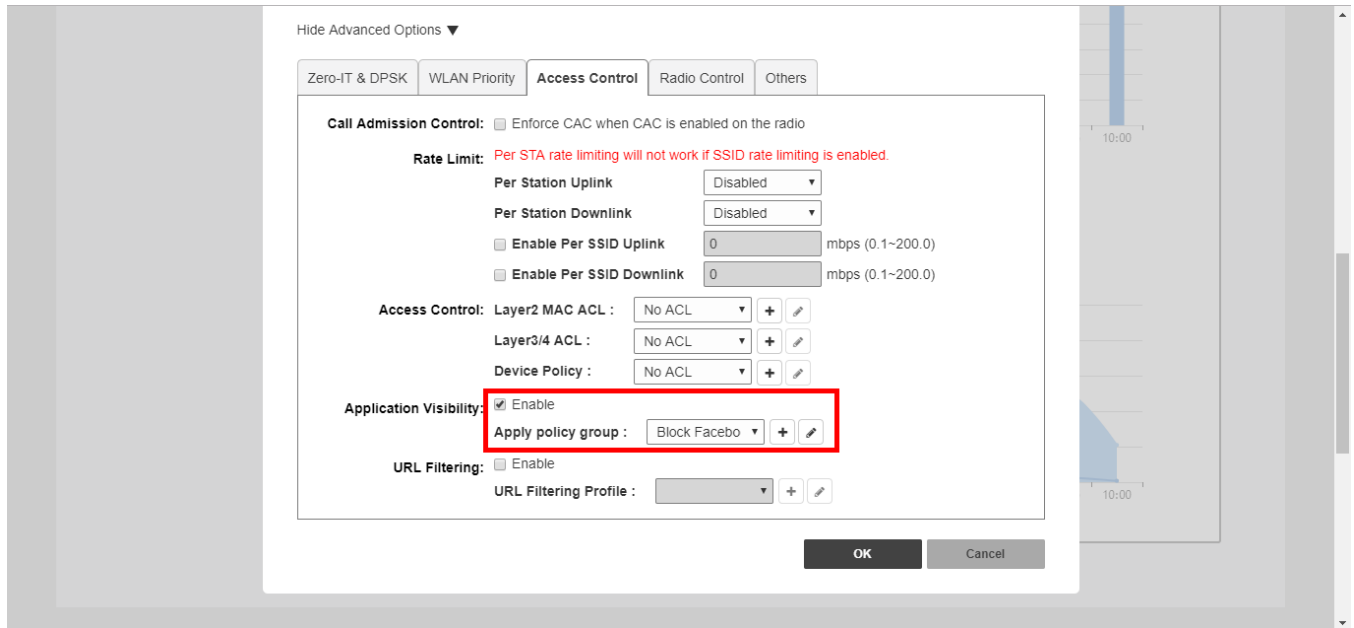
Alternatively, go to *Admin & Services > Services > Application Recognition & Control > Application Policy* to configure multiple application policies and then apply them to WLANs one by one.

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.

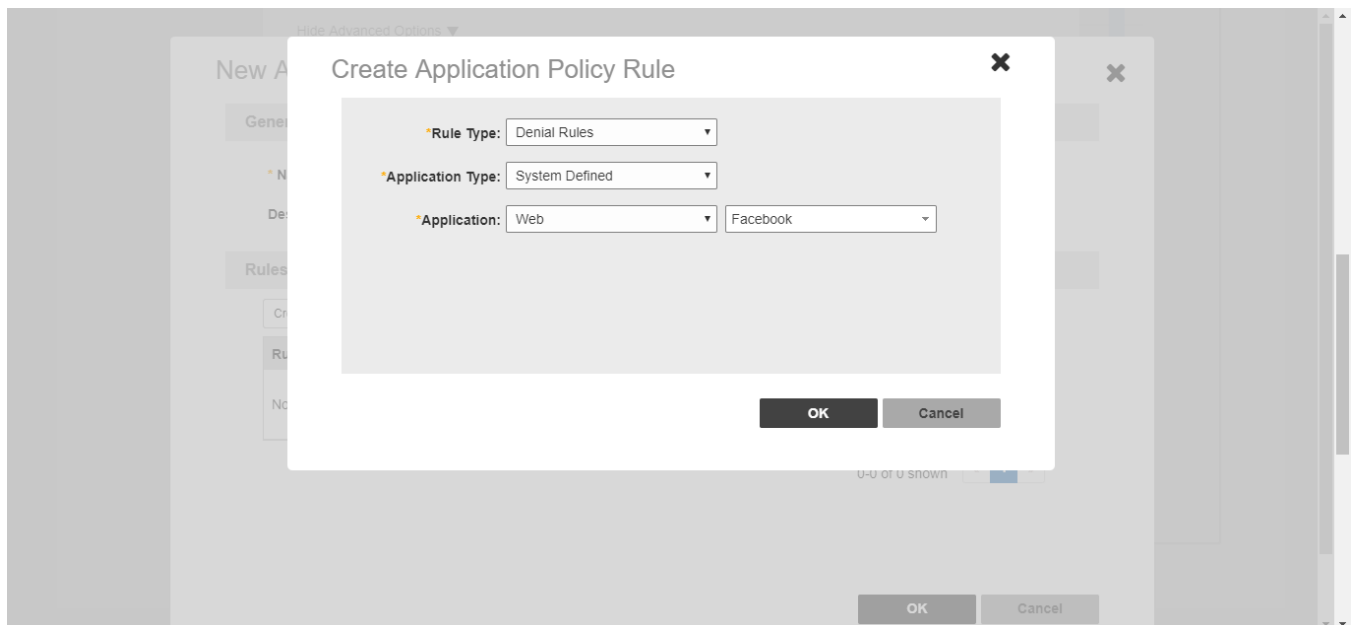


10. Click **Save** to save the rule, and click **OK** to save the policy.

**FIGURE 129** Applying an Application Control Policy to a WLAN



**FIGURE 130** Creating an Application Control Policy for a specific website



## Radio Control Settings

The *WLAN > Advanced Options > Radio Control* tab provides options for configuring WLANs individually. Many of these options can also be configured globally from the *Enhanced Services > Radio Control* page. For information on configuring global radio control options, see [Configuring Global AP Settings](#) on page 204.

The following options can be configured on a per-WLAN basis:

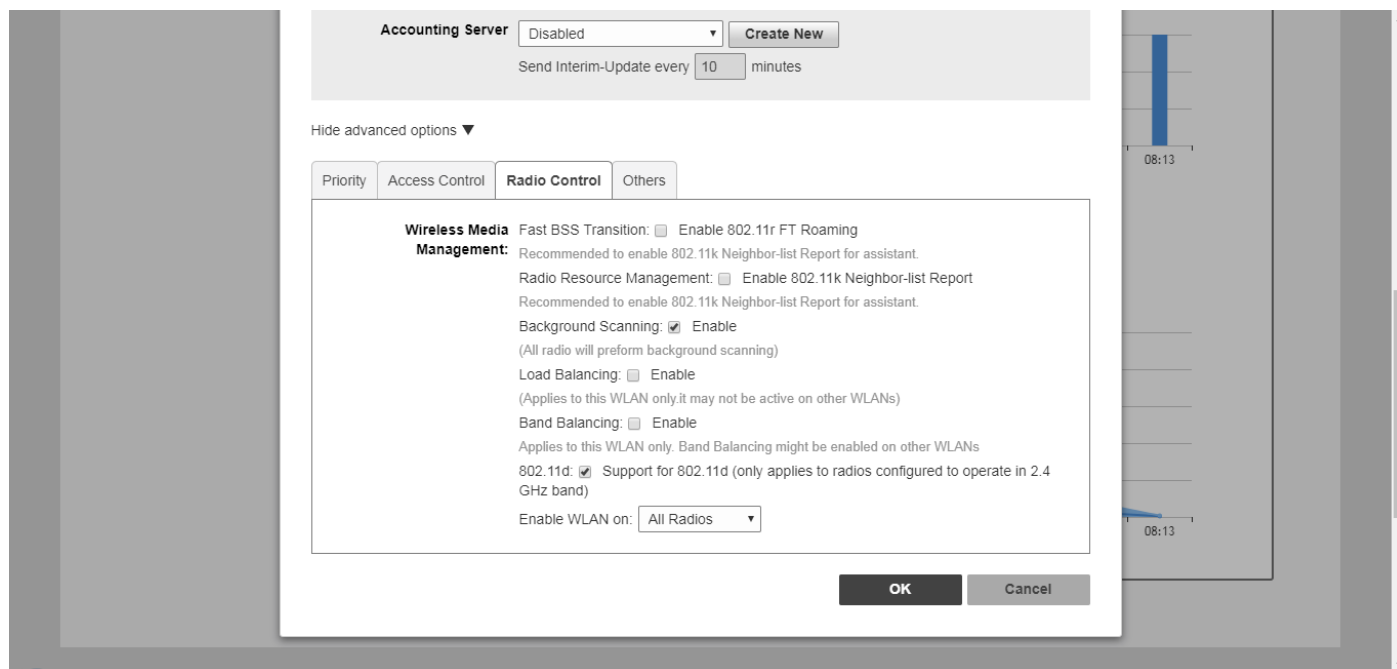
- **Fast BSS Transition:** (Disabled by default) The Fast BSS Transition feature uses messages and procedures defined in 802.11r to allow continuous connectivity for wireless devices in motion, with fast and secure handoffs from one AP to another. A fast BSS transition is a BSS transition in the same 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 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 Unleashed web interface to balance the number of clients per radio on adjacent APs. "Adjacent APs" are determined by the Unleashed Master AP by measuring the RSSI during channel scans. After startup, the Unleashed 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 Unleashed Master AP immediately updates the list of adjacent radios and refreshes the client limits at each affected AP. Once the Unleashed 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:** Band balancing balances the client load on radios by distributing clients between the 2.4 GHz and 5 GHz radios. This feature is enabled by default. 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:** 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. This option is enabled by default. For optimal performance of Apple iOS devices, it is recommended that you enable this option.

### NOTE

Some legacy embedded devices (such as wireless bar code scanners) may not operate properly if this option is enabled.

- **Enable WLAN on:** Manually enable/disable WLAN service per radio. Default is enabled on both radios. Select **2.4 GHz only** to disable WLAN service on the 5 GHz radio, or **5 GHz only** to disable WLAN service on the 2.4 GHz radio.

FIGURE 131 Radio Control options



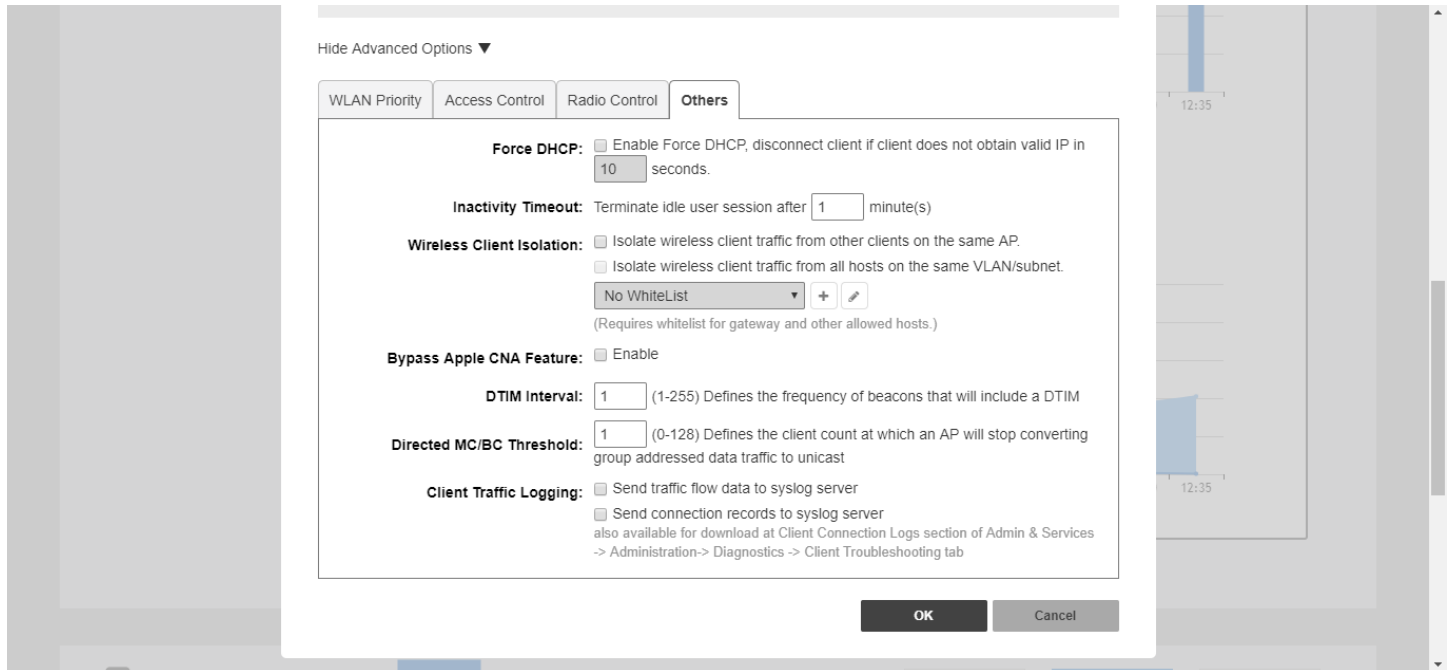
## Other Advanced WLAN Settings

The *WLAN > Advanced Options > 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. This prevents 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 (1 to 500 minutes).
- **Wireless Client Isolation:** In Wireless Client Isolation, select the level of client isolation you want to enforce:
  - **Isolate wireless client traffic from other clients on the same AP:** Enable 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:** Prevent clients from communicating with any host on the same subnet or VLAN other than those listed on the Client Isolation Whitelist. If this option is chosen, you must select a Whitelist from the drop-down list. (See [Configuring Client Isolation Whitelists](#) on page 196.)
- **Bypass Apple CNA Feature:** 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. (See [Bypass Apple CNA](#) on page 197).
- **DTIM Interval:** Configure the Delivery Traffic Indication Message 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, thereby increasing battery consumption.
- **Directed MC/BC Threshold:** Directed Multicast/Broadcast is a feature that allows Ruckus APs to convert incoming broadcast and multicast traffic to unicast, reducing airtime utilization and improving data throughput performance. Enter a value to set the client count at which an AP will stop converting group addressed data traffic to unicast traffic.
- **Client Traffic Logging:** Configure options for log generation and delivery to syslog server (see [Client Connection Troubleshooting](#) on page 263):
  - **Send traffic flow data to syslog server:** Unleashed sends client flow data only to the syslog server.

- **Send connection records to syslog server:** Unleashed sends client connection event logs only to the syslog server.

FIGURE 132 WLAN > Advanced Options > Others tab



## Configuring Client Isolation Whitelists

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 white list.

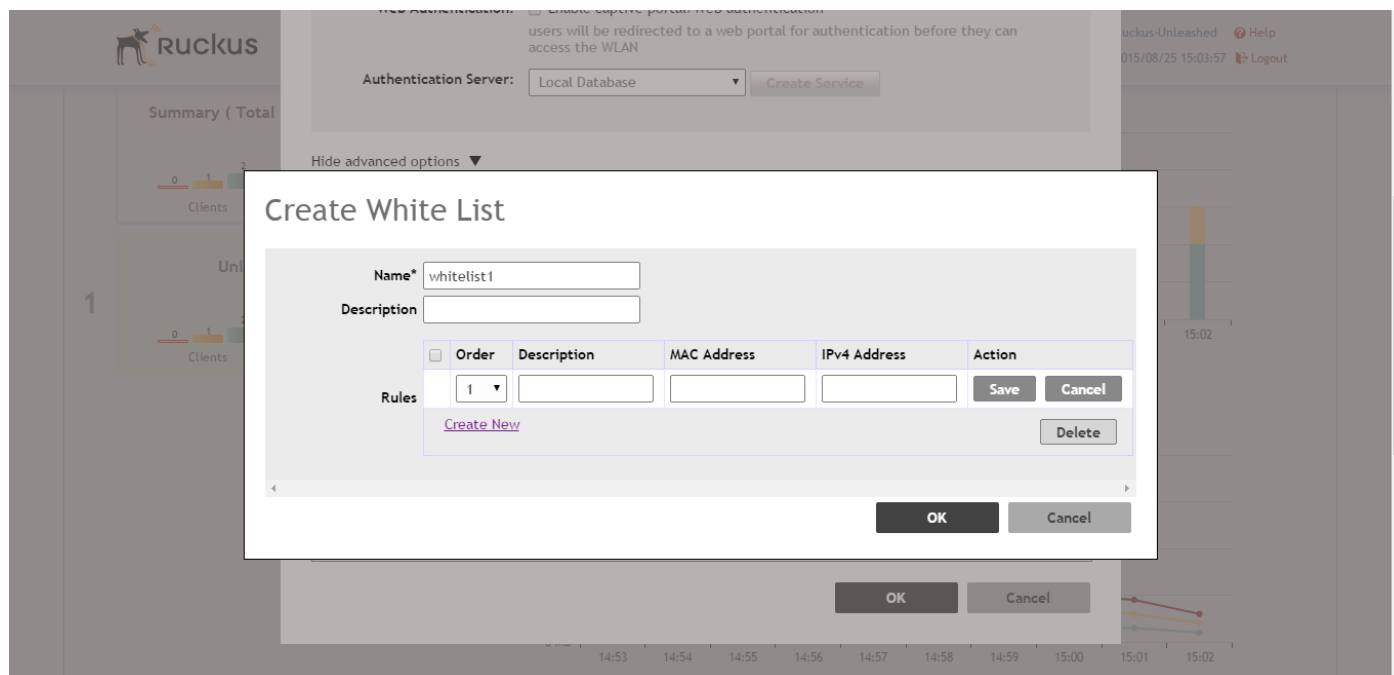
You can create exceptions to client isolation (such as allowing access to a local printer, for example) by creating Client Isolation Whitelists.

To configure a Client Isolation Whitelist:

1. Go to **Wi-Fi Networks > Advanced Options > Others**.
2. Select both check boxes under **Wireless Client Isolation**. (Isolate wireless clients from other clients on the same AP, and from all hosts on the same VLAN/subnet).
3. Click **Create Whitelist**.
4. Enter a **Name** and optionally a **Description** for the access policy.
5. In **Rules**, you can create multiple device-specific rules for each device to be white 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**.

- Click **OK** to save the white list.

**FIGURE 133** Configuring a Client Isolation Whitelist



## 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.

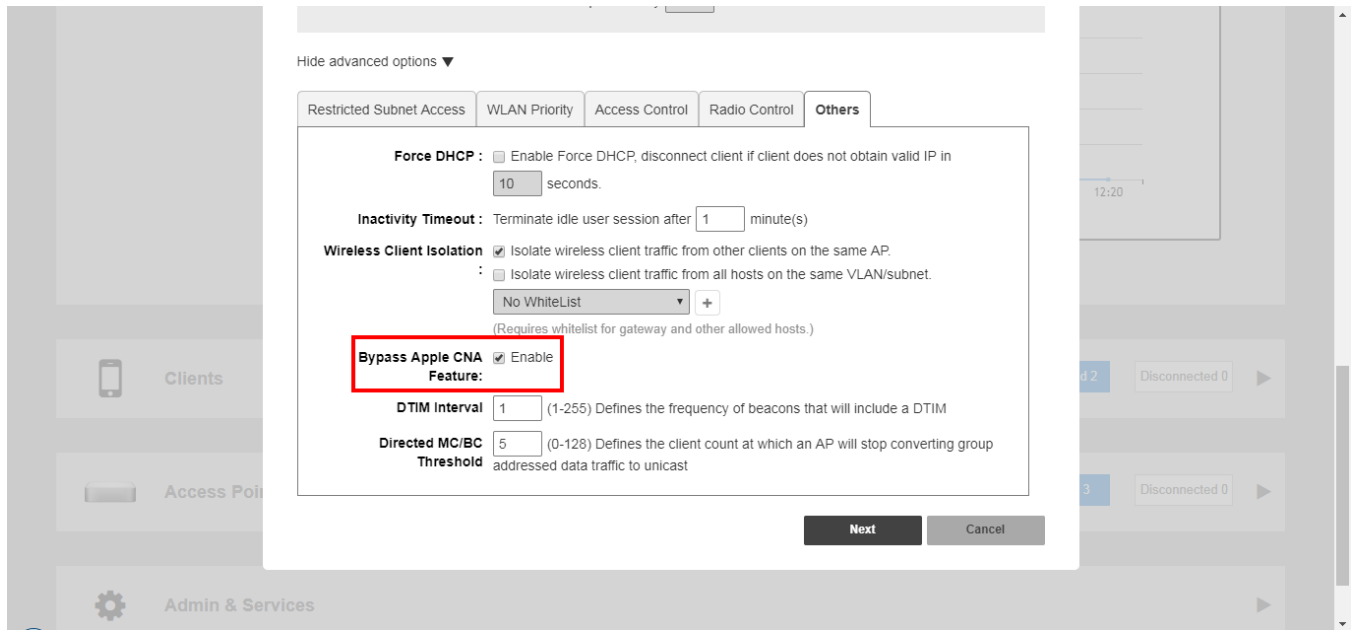
ZoneDirector provides an option to work around the Apple CNA feature if it is not desirable for your specific deployment. With CNA bypass enabled, captive portal (web-based authentication) login must be performed by opening a browser to any unauthenticated page (http) to get redirected to the login page.

To enable Apple CNA bypass, use the following procedure:

- 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)
- Click **Show Advanced Options**.
- Click the **Others** tab.

4. Select the **Enable** check box next to **Bypass Apple CNA Feature**.
5. Click **OK** to save your changes.

**FIGURE 134** Enable Bypass Apple CNA feature



# Access Point Configuration

---

• Access Point Configuration Overview.....	199
• Show Mesh Topology.....	200
• Show Client Info.....	201
• Show Events and Alarms.....	203
• Configuring Global AP Settings.....	204
• Monitoring an Individual AP.....	210
• Configuring an Individual AP.....	214
• Working with AP Groups.....	218
• Restarting an AP.....	232
• Removing an AP.....	233

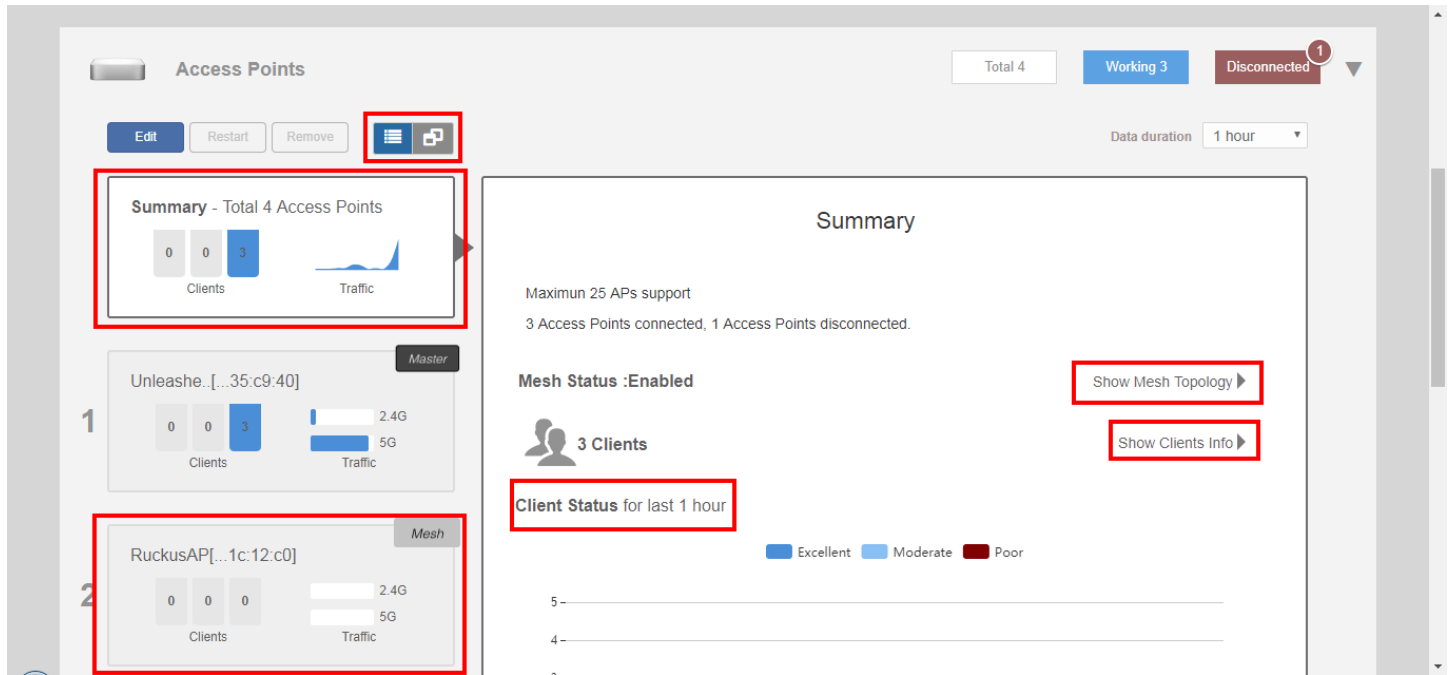
## Access Point Configuration Overview

The *Access Points* component provides tools for monitoring and configuring all Unleashed APs at once, and for configuring each AP individually.

Expand the component to view an overview of the connected and disconnected Unleashed APs that are recognized by this Unleashed network. This screen contains the following elements:

- **Summary Box:** Click this box to view a summary of all APs' clients, signal quality and traffic statistics.
- **Individual AP Boxes:** Click any of these boxes to view details specific to that 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, see *Working with AP Groups*.
- **Show Mesh Topology:** Click this link to view the Mesh topology.
- **Show Client 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 client signal quality across all connected APs at one-minute intervals (over the last 10 minutes).
- **Traffic** graph: This graph displays the Received (Rx), Transmit (Tx) and Total traffic values over time for the last 10 minutes, at one-minute intervals.

FIGURE 135 Access Points Component



## 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 136 Mesh Topology

The screenshot displays the 'Access Points' configuration page. At the top right, it shows 'Total 4' access points, with 'Working 3' and 'Disconnected 1'. Below this, there are buttons for 'Edit', 'Restart', and 'Remove', along with a 'Data duration' dropdown set to '1 hour'. The main content area is divided into two sections. On the left, there are three summary cards for different access points: 'Summary - Total 4 Access Points', 'Unleashed...35:c9:40' (labeled '1' and 'Master'), and 'RuckusAP[...1c:12:c0]' (labeled '2' and 'Mesh'). Each card shows client counts and traffic graphs. On the right, a larger 'Summary' section provides more details. It states 'Maximun 25 APs support' and '3 Access Points connected, 1 Access Points disconnected.' Below this, the 'Mesh Status :Enabled' is shown, with a 'Hide Mesh Topology' button highlighted in a red box. A table lists the mesh topology details:

Tree	Access Points	Signal	Description	Channel
+	d4:c1:9e:35:c9:40			36
+	f0:b0:52:1c:12:c0	41		36
+	f0:b0:52:1b:f0:40	49		36

Below the table, it shows '3 Clients' and a 'Show Clients Info' link. At the bottom, it indicates 'Client Status for last 1 hour'.

## Show Client Info

Click this link to display the currently connected clients list.

FIGURE 137 Client Info summary

The screenshot displays the 'Access Points' management page. At the top, it shows 'Total 4' access points, with 'Working 3' and 'Disconnected 1'. Below this, there are buttons for 'Edit', 'Restart', and 'Remove', along with a 'Data duration' dropdown set to '1 hour'. A summary card for 'Total 4 Access Points' shows 0 clients and a traffic graph. A sidebar on the left lists three access points: 'Unleashed [d4:c1:9e:35:c9:40]' (Master), 'Unleashed [d4:c1:9e:35:c9:40]' (1), and 'RuckusAP[...1c:12:c0]' (Mesh, 2). The main content area is for the selected 'Unleashed [d4:c1:9e:35:c9:40]' access point, showing '3 Clients' and a 'Hide Clients Info' button. A table lists the clients:

★	Mac Address	IP Address	OS	Name
	64:a2:f9:bc:cb:53	192.168.0.13	Android	OnePlus_6T
	f0:03:8c:fb:73:38	192.168.0.11	N/A	
	04:b1:67:47:c4:20	192.168.0.8	Android	MyClient

Below the table, it shows '1-3 of 3 shown' and a 'Show WLANs Info' button. At the bottom left, it indicates '2 WLANs'.

# Show Events and Alarms

Click this link to display a list of events and alarms for all APs or for the selected AP.

**FIGURE 138** Show/hide Events & Alarms

The screenshot shows the Ruckus management interface. On the left, there are summary cards for 'Clients' and 'Traffic'. The main area displays '5 Clients' and 'Events & Alarms'. A red box highlights the 'Hide Events & Alarms' dropdown menu. Below this, there are tabs for 'Events' and 'Alarms', and a table of events.

Maximum 128 APs and 10 AP groups support  
1 Access Points connected, 0 Access Points disconnected.

5 Clients [Show Clients Info](#)

Events & Alarms **Hide Events & Alarms**

Events Alarms

Search

Date/Time	Severity	Activities
2019/11/04 09:36:39	High	A new Same-Network Rogue[d4:c1:9e:35:c9:5c] w
2019/11/04 09:36:38	High	A new Same-Network Rogue[d4:c1:9e:35:c9:58] w
2019/11/04 09:31:49	High	A new Same-Network Rogue[44:1e:98:1b:f0:dc] w
2019/11/04 09:31:48	High	A new Same-Network Rogue[44:1e:98:1b:f0:d8] w
2019/11/04 09:30:17	High	A new Same-Network Rogue[f0:b0:52:1c:12:cc] wi
2019/11/04 09:30:16	High	A new Same-Network Rogue[f0:b0:52:1c:12:c8] wi
2019/11/04 09:19:25	High	A new Same-Network Rogue[f0:b0:52:1b:f0:4c] wif

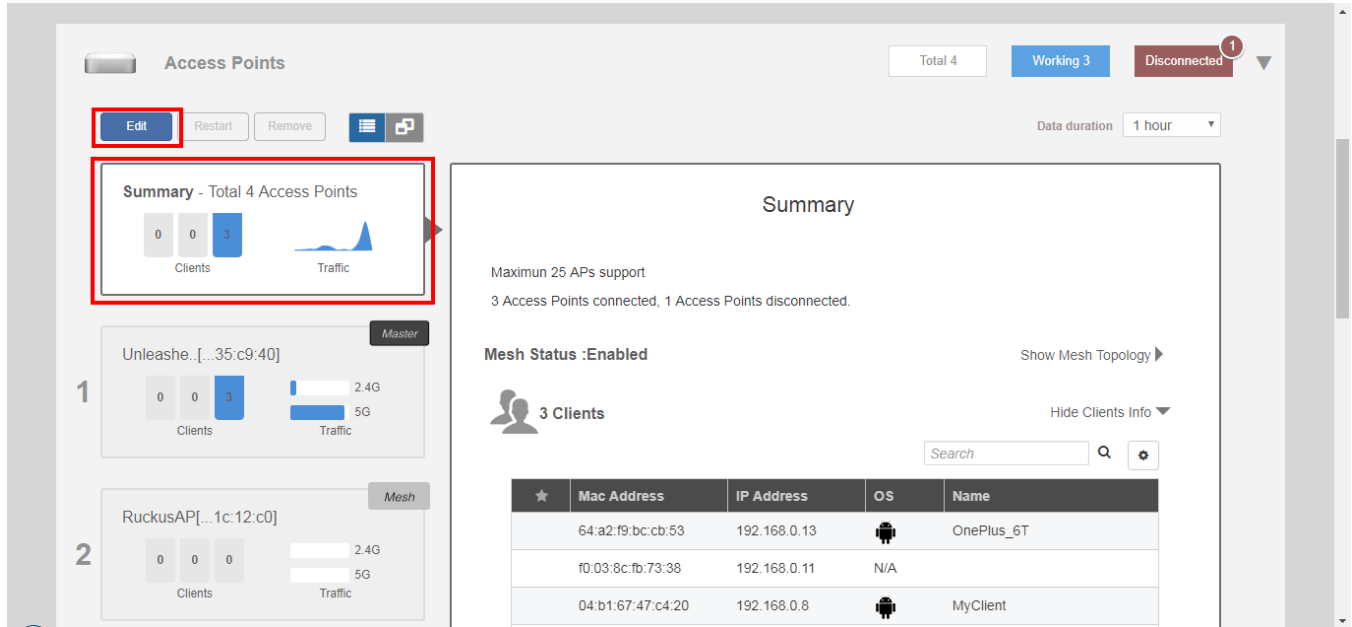
## Configuring Global AP Settings

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 139** Click Edit to configure AP global settings



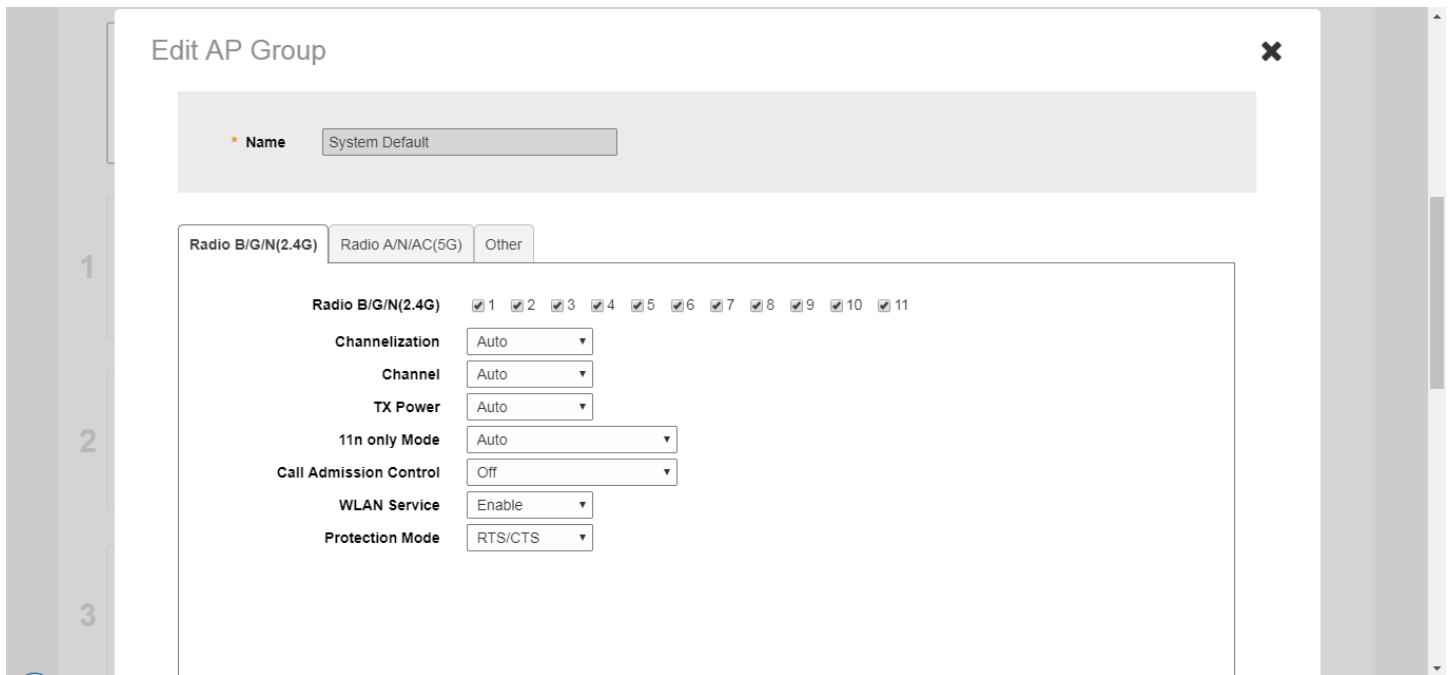
2. Configure the following global AP settings according to your preferences:
  - **Radio B/G/N (2.4G)**: Configure options for the 2.4 GHz radio on all Unleashed APs.
  - **Radio A/N/AC (5G)**: Configure options for the 5 GHz radio on all Unleashed APs.
  - **Others**: Configure Model-Specific controls including Max Clients by AP model, and whether to disable status LEDs.
3. Click **OK** to save your changes.

### Radio B/G/N (2.4G)

Select or deselect channels from which to choose during the automatic channel selection process or select a specific channel on which to operate, or enable 11n only mode, or enable Call Admission Control or Spectralink Compatibility for this radio.

Additionally, you can disable WLAN service for this radio entirely.

FIGURE 140 2.4 GHz radio configuration screen

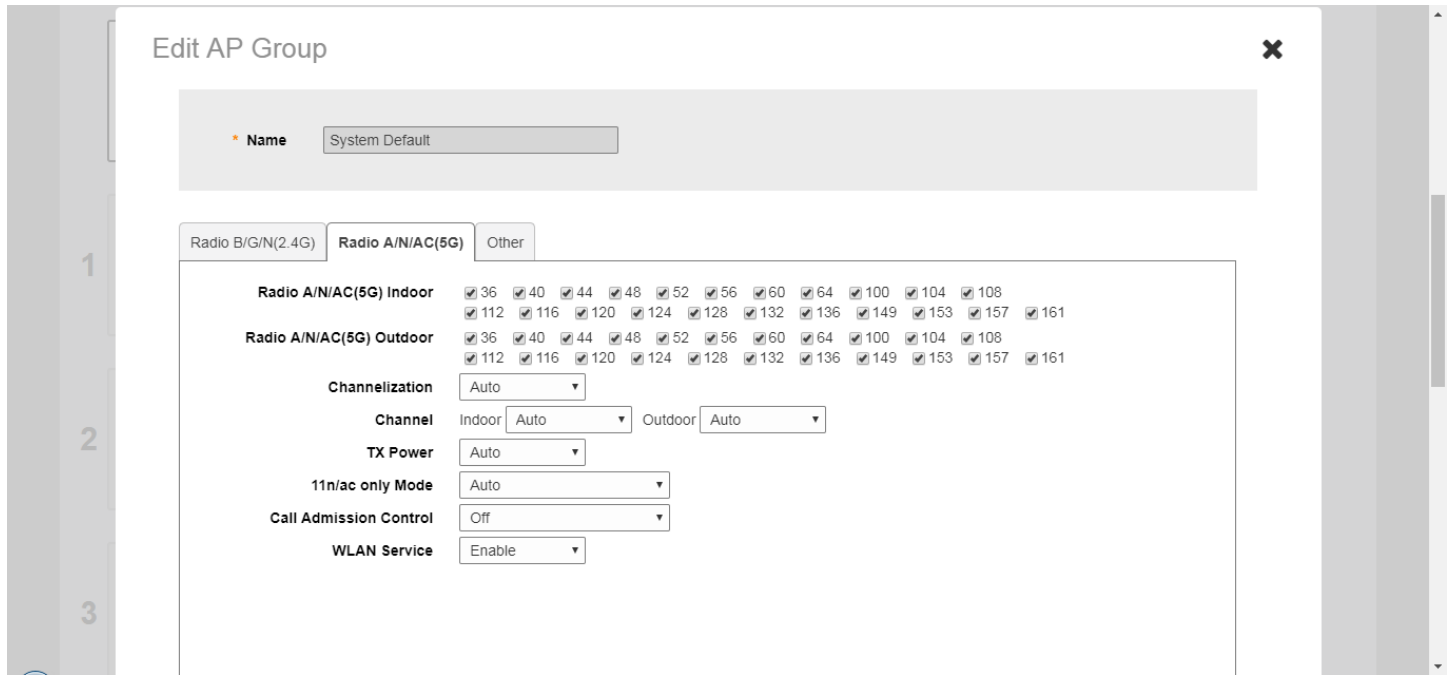


## Radio A/N/AC (5G)

Select or deselect channels from which to choose during the automatic channel selection process or select a specific channel on which to operate, or enable 11n/ac only mode, or enable Call Admission Control or Spectralink Compatibility for this radio.

Additionally, you can disable WLAN service for this radio entirely.

FIGURE 141 System Default AP group 5 GHz radio configuration screen



## Others

The **Access Points > Summary > Edit > Others** 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 207.

FIGURE 142 Configuring other AP settings

1

2

3

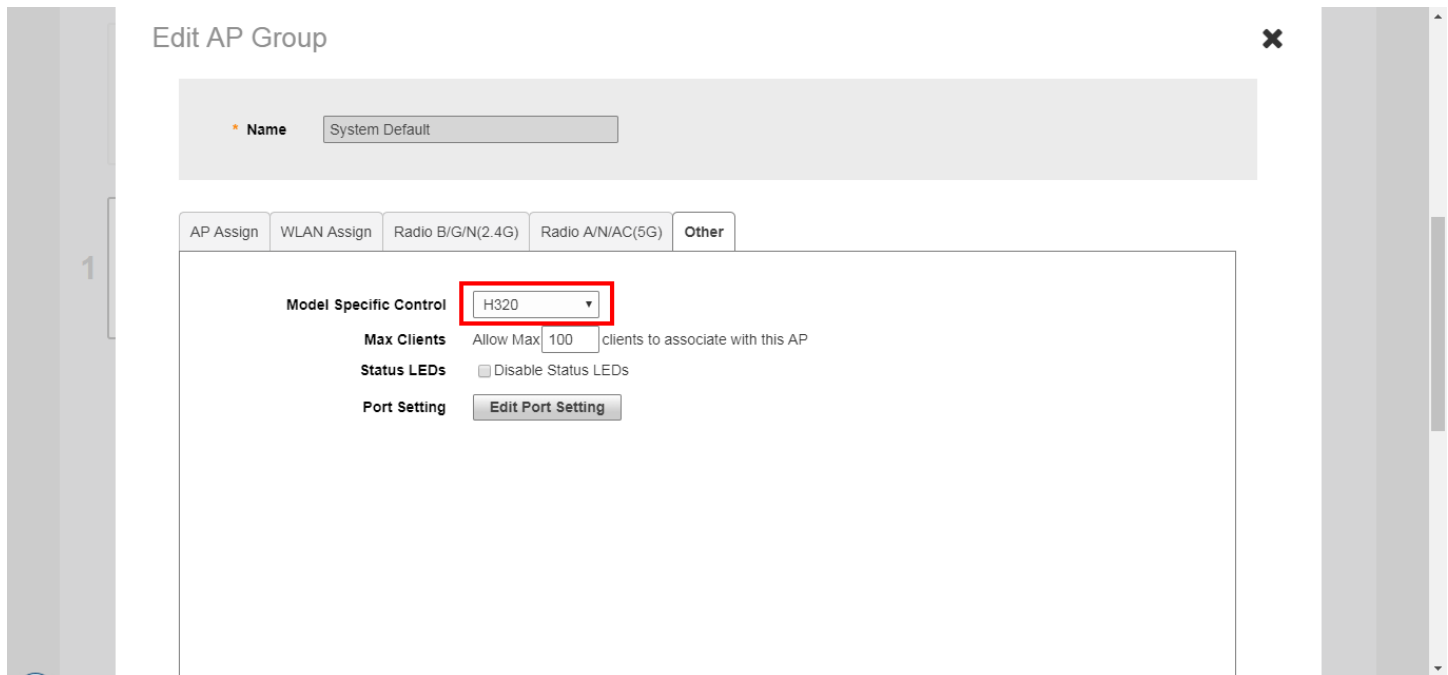
### **Modifying Model Specific Controls**

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 143 Model Specific Controls



Configure any of the following settings for each model independently, and click **Finish** to save your changes:

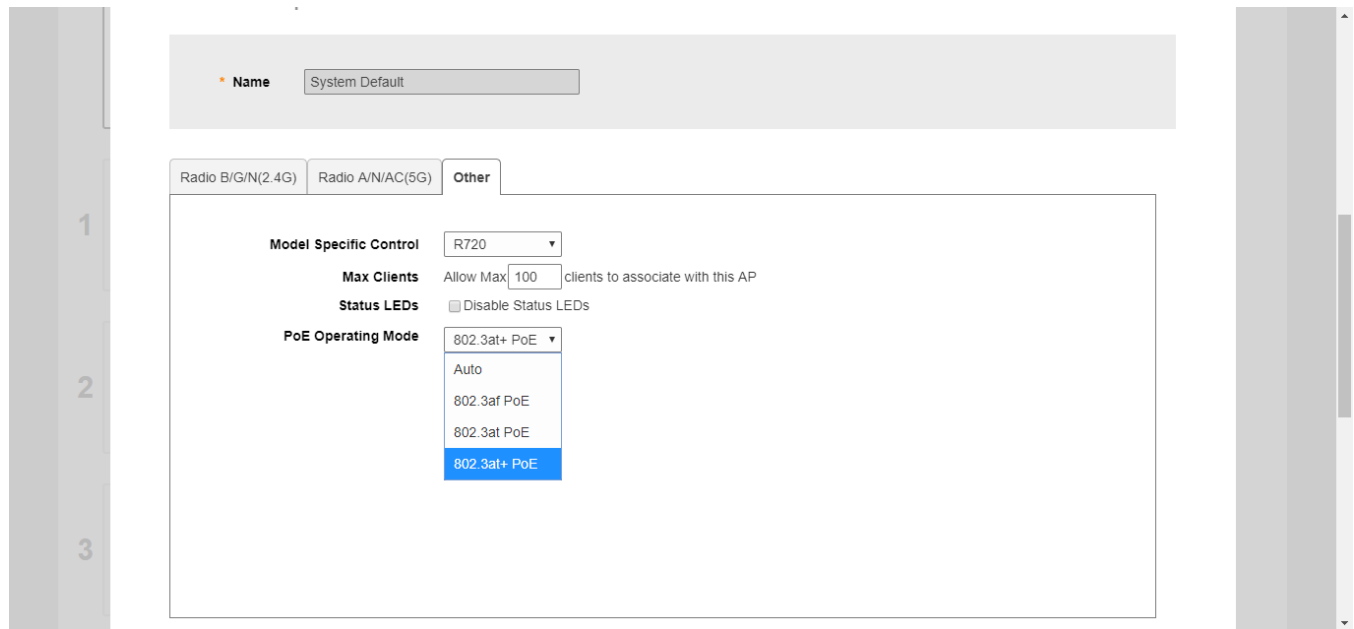
- **Max Clients:** Set the maximum number of clients that can associate per AP. Note that different AP models have different maximum client limitations.
- **PoE Out Ports:** Enable PoE out ports (specific AP models only).
- **Status LEDs:** Disable the external LEDs on certain AP models. This can be 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 227 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 389.



FIGURE 144 PoE Operating Mode



### Disabling Access Point LEDs

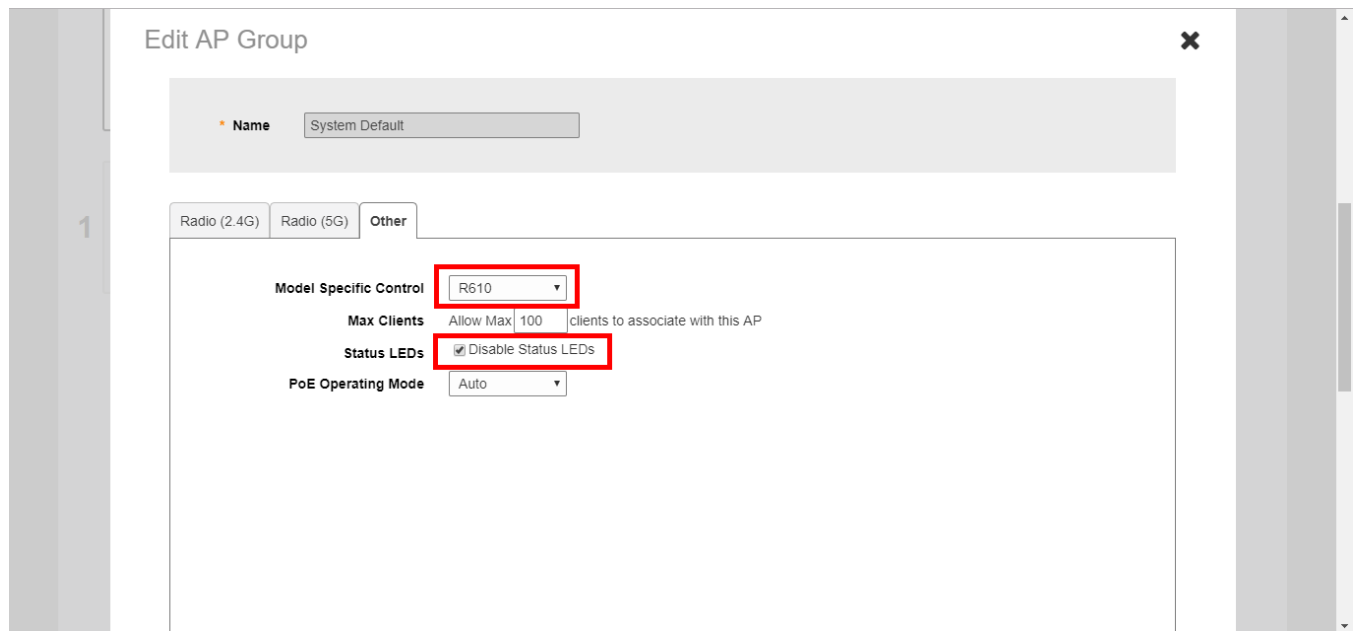
In some situations, customers may wish to disable the LED lights on the access points to avoid drawing attention to them, when installed in a public location, for example.

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 145** Select model and enable the option "Disable Status LEDs"

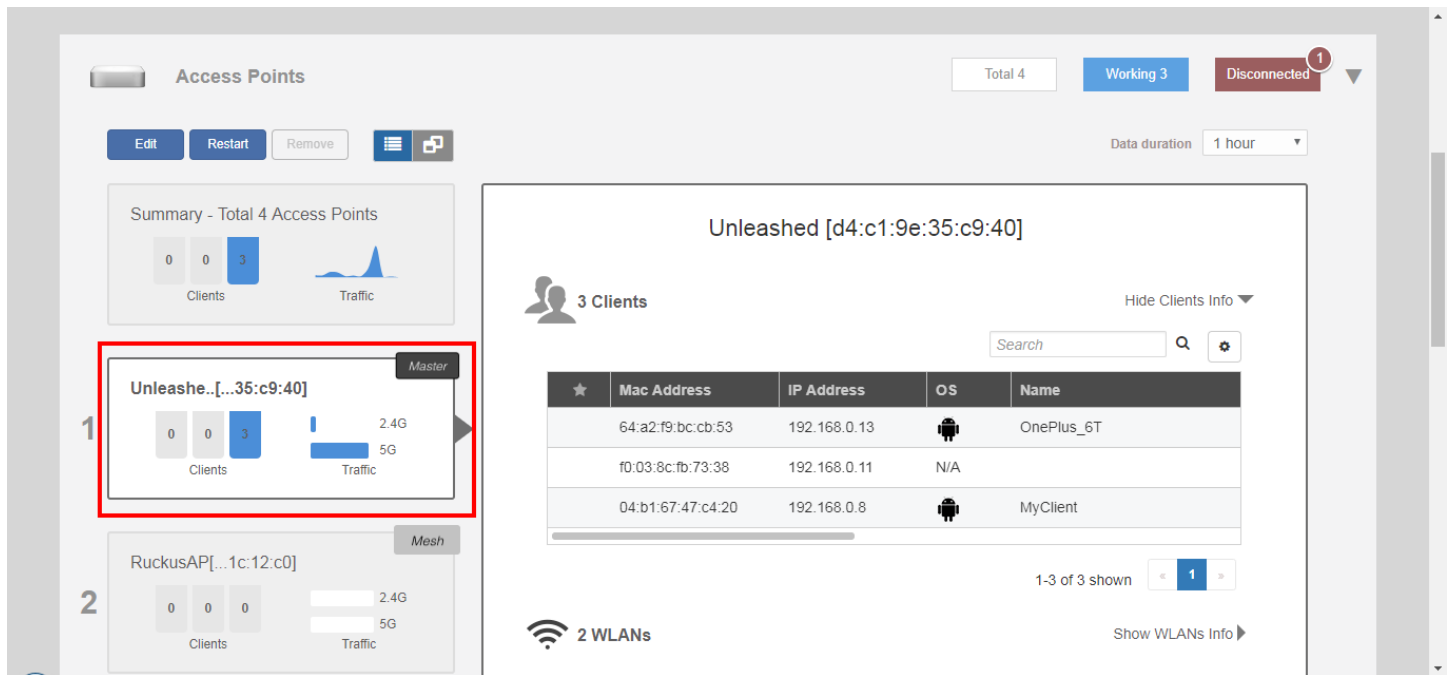


## Monitoring an Individual AP

The AP detail display includes buttons that can be used to **Edit**, **Restart** or **Remove** the AP from the network, graphs displaying signal quality and traffic statistics, and links to more detailed information on the AP and its connected clients.

To monitor and configure an AP individually, click on its box on the left side of the screen when the **Access Points** component is expanded.

FIGURE 146 Viewing an individual AP by clicking on its box



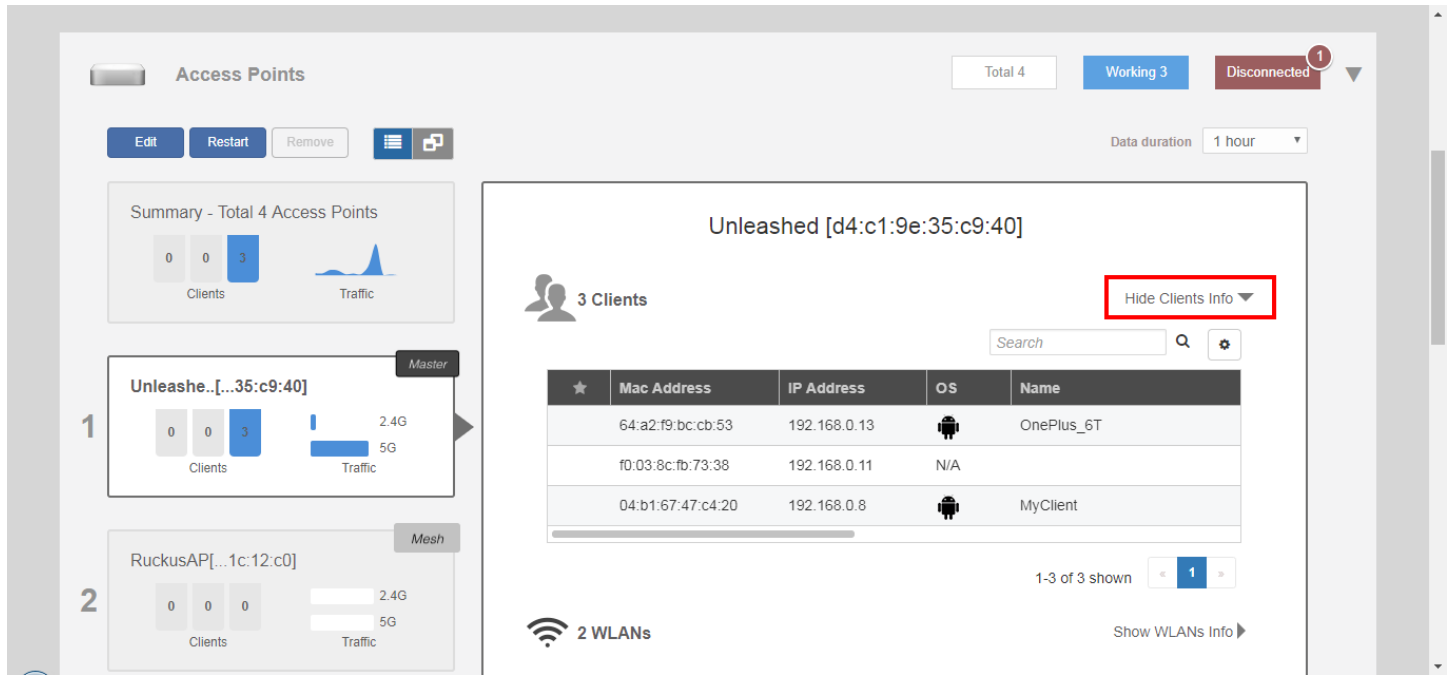
The individual AP monitoring screen contains the following UI elements:

- **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 Unleashed network.
- **Remove:** Click this button to remove this AP from the Unleashed network.
- **Show Client 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 System Overview:** 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 147 Show Client Info from AP page



## Show System Overview

Click this link to display the AP's system information.

Click the **Show System Overview** link to display detailed information on this AP. The expanded section displays the AP's general information, radio channels in use, mesh type, max clients, firmware version, and two buttons: **Save Logs** and **Speed Test**.

Click **Save Logs** to generate a txt log file that can be useful for troubleshooting. Click **Speed Test** to measure the AP's connection performance.

### NOTE

The Max Clients displayed for the Unleashed Master AP may be lower than the configured maximum, as the Unleashed Master has to perform additional tasks other than serving clients. The Master AP maximum client load varies by AP model. These limits apply only to the current Unleashed Master AP. All other member APs will honor the max clients set from the global AP model-specific controls page (**Access Points > Summary > Edit > Others > Max Clients**).

The AP system overview also displays the AP's Ethernet port status, including link status (up/down) and link speed.

FIGURE 148 System Overview Info

Summary - Total 4 Access Points

0 Clients 3 Traffic

1 Unleashed [d4:c1:9e:35:c9:40] Master

0 Clients 0 Traffic 2.4G 5G

2 RuckusAP [1c:12:c0] Mesh

0 Clients 0 Traffic 2.4G 5G

3 RuckusAP [1b:f0:40] Mesh

0 Clients 0 Traffic 2.4G 5G

Unleashed [d4:c1:9e:35:c9:40]

3 Clients Show Clients Info ▶

2 WLANs Show WLANs Info ▶

Hide System Overview Info ▼

Mac Address	d4:c1:9e:35:c9:40
IP Address	192.168.0.2
External IP:Port	192.168.0.2:12225
Model	r610
S/N	941849001125
GPS Coordinates	
Mesh Type	Root AP
Current Channel(802.11a/n/ac)	36
Current Channel(802.11b/g/n)	1
Max Clients	100
Version	200.7.10.2.270

FIGURE 149 Click Download Logs to save the AP's current log file as a txt file on your computer

2 WLANs Show WLANs Info ▶

Hide System Overview Info ▼

Mac Address	d4:c1:9e:35:c9:40
IP Address	192.168.0.2
External IP:Port	192.168.0.2:12225
Model	r610
S/N	941849001125
GPS Coordinates	
Mesh Type	Root AP
Current Channel(802.11a/n/ac)	36
Current Channel(802.11b/g/n)	1
Max Clients	100
Version	200.7.10.2.270
Role Fixed	no
Logs	Download Logs 📄

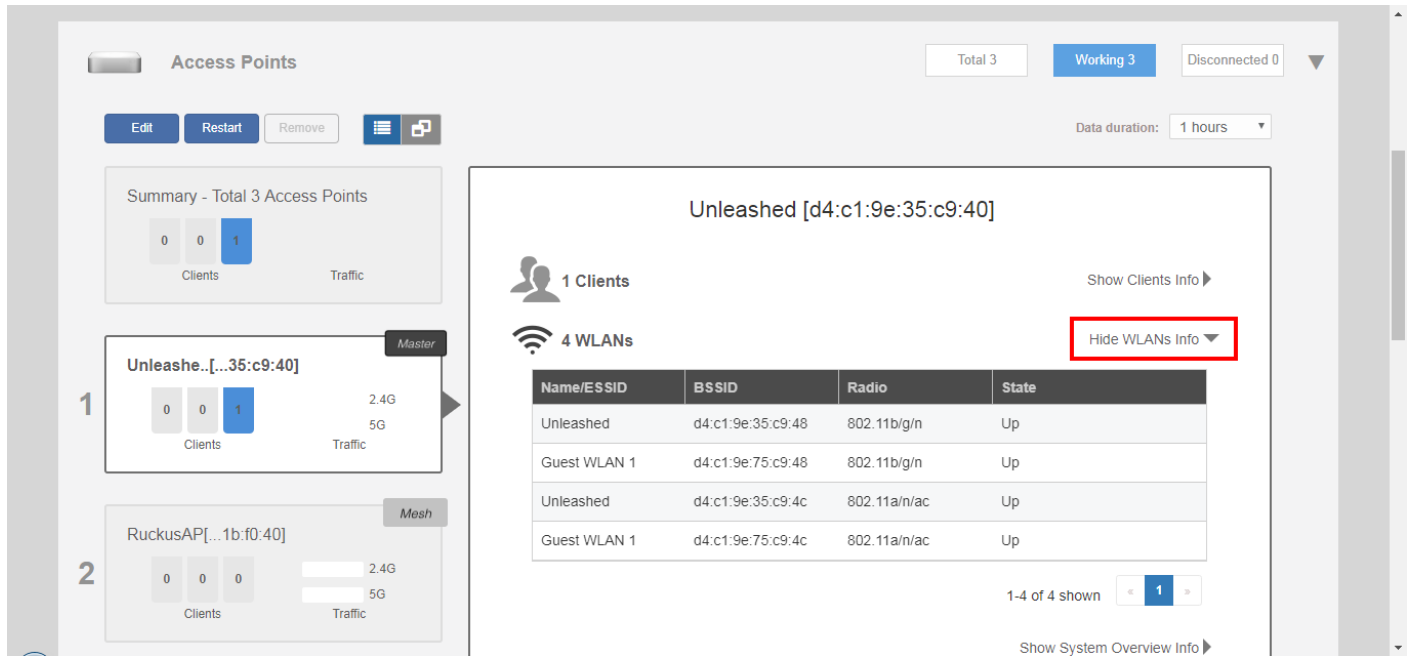
LAN Port Status ⓘ

## Show WLANs Info

Click this link to display the AP's WLAN information.

Click the **Show WLANs Info** link to display the list of WLANs that are currently deployed on this AP. The expanded section displays the WLAN name (ESSID), BSSID (MAC address), Radio, and state (up or down).

FIGURE 150 Show AP WLAN info



## Configuring an Individual AP

To configure a specific AP, go to **Dashboard > Access Points**, click on the AP you want to configure, and click **Edit**.

FIGURE 151 Click Edit to configure an AP

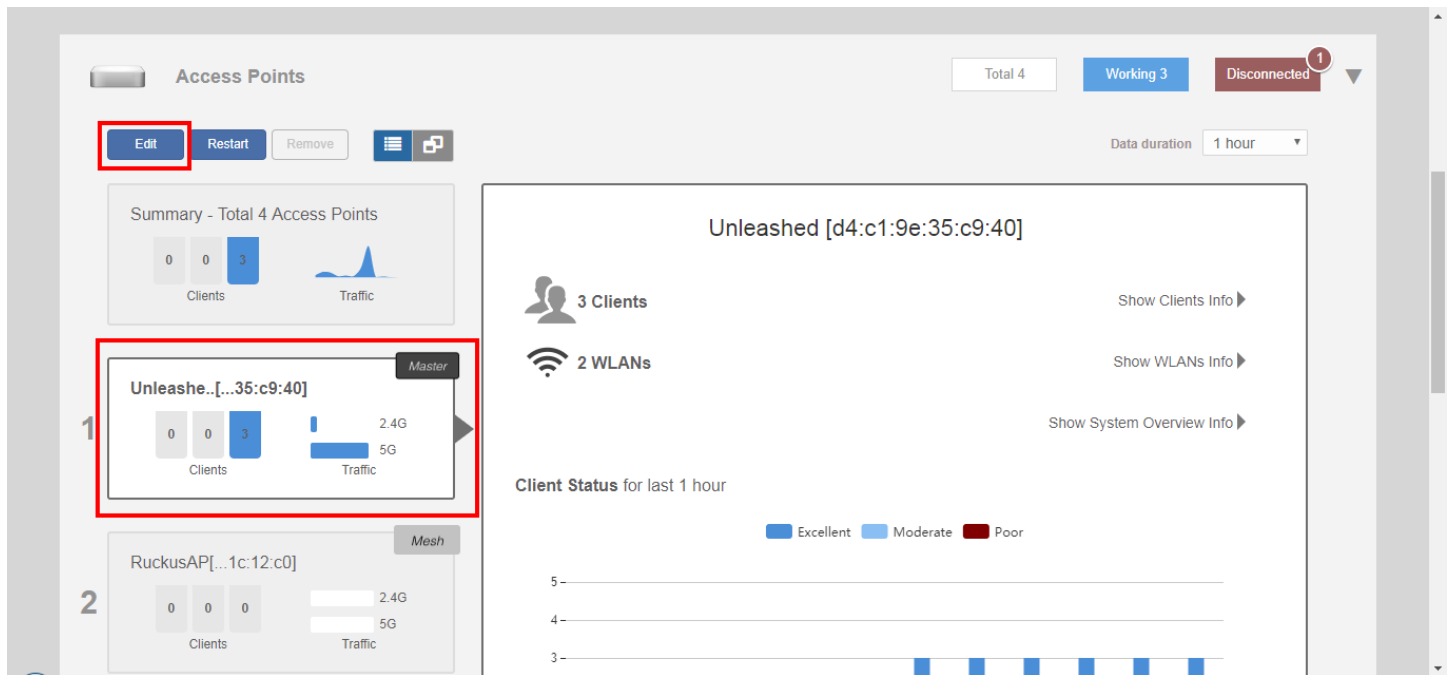
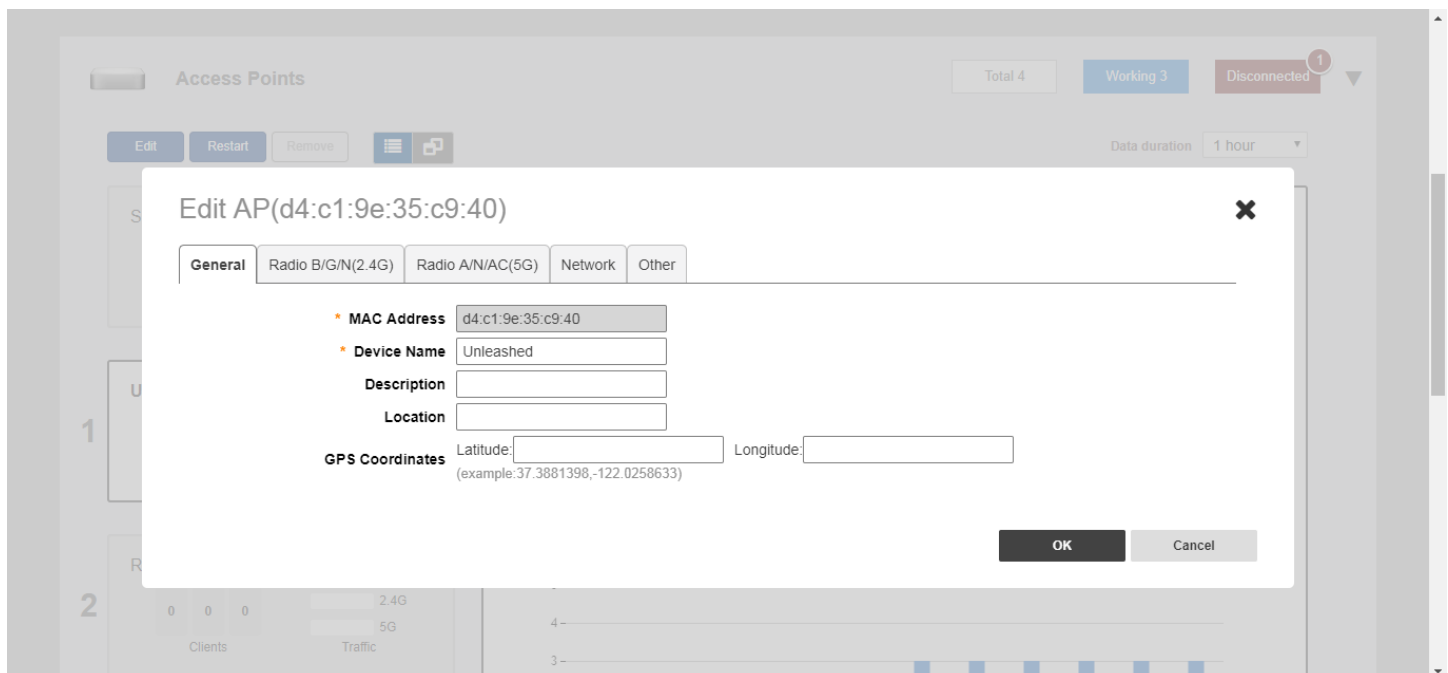


FIGURE 152 Editing an AP's configuration settings



In general, the settings available on the individual AP's **Edit** screens are the same as those for global AP settings (see [Configuring Global AP Settings](#) on page 204). Configuring these settings for an individual AP overrides the global AP settings.

## Access Point Configuration

### Configuring an Individual AP

However, some settings are only configurable on a per-AP basis, as follows:

- **General:** Configure the AP's Device Name, Description, Location and GPS Coordinates.
- **Radio B/G/N (2.4G):** Enable/disable WLAN service for this radio.
- **Radio A/N/AC (5G):** Enable/disable WLAN service for this radio.
- **Network:** Configure a manual (static) IP address, or allow the AP to obtain an IP address using DHCP.

#### NOTE

For the current Unleashed Master AP, you cannot configure the IP address settings here. You must go to **Admin & Services > System > Device IP Settings** to change the Master's IP settings.

- **Other:** Designate this AP to serve as a Bonjour Gateway AP (See [Bonjour Gateway](#) on page 319), or enable/disable the AP's Status LEDs, or override the AP group's PoE operating mode settings and configure specific PoE power mode for this AP.

**FIGURE 153** Configure an AP with a static IP address from the AP's Edit > Network tab

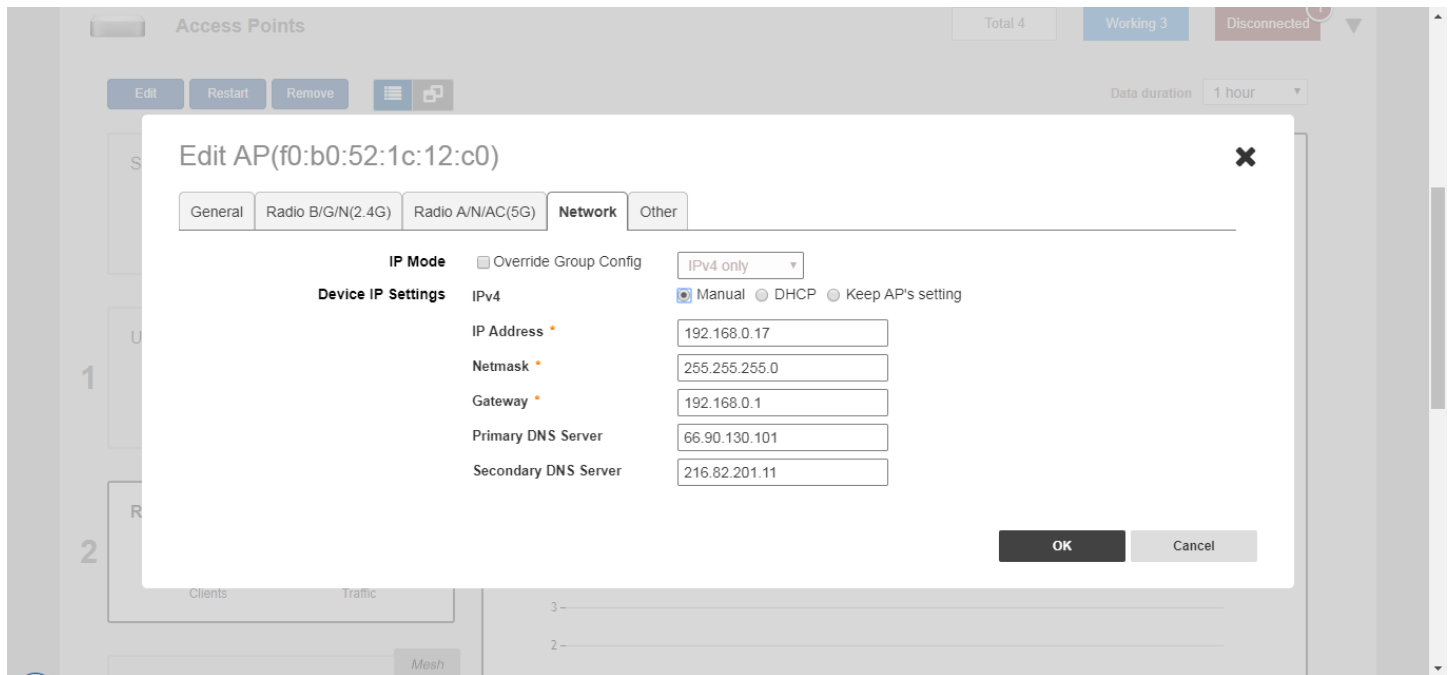
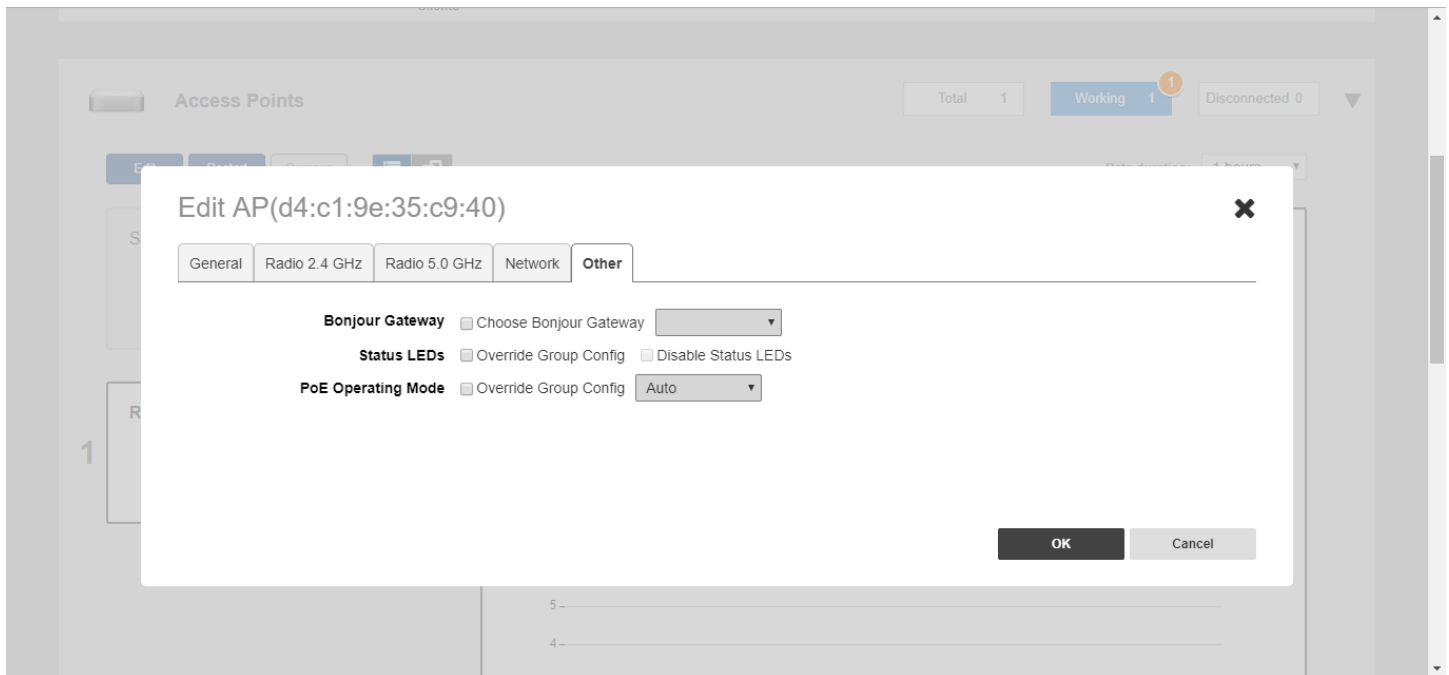




FIGURE 154 Other AP settings

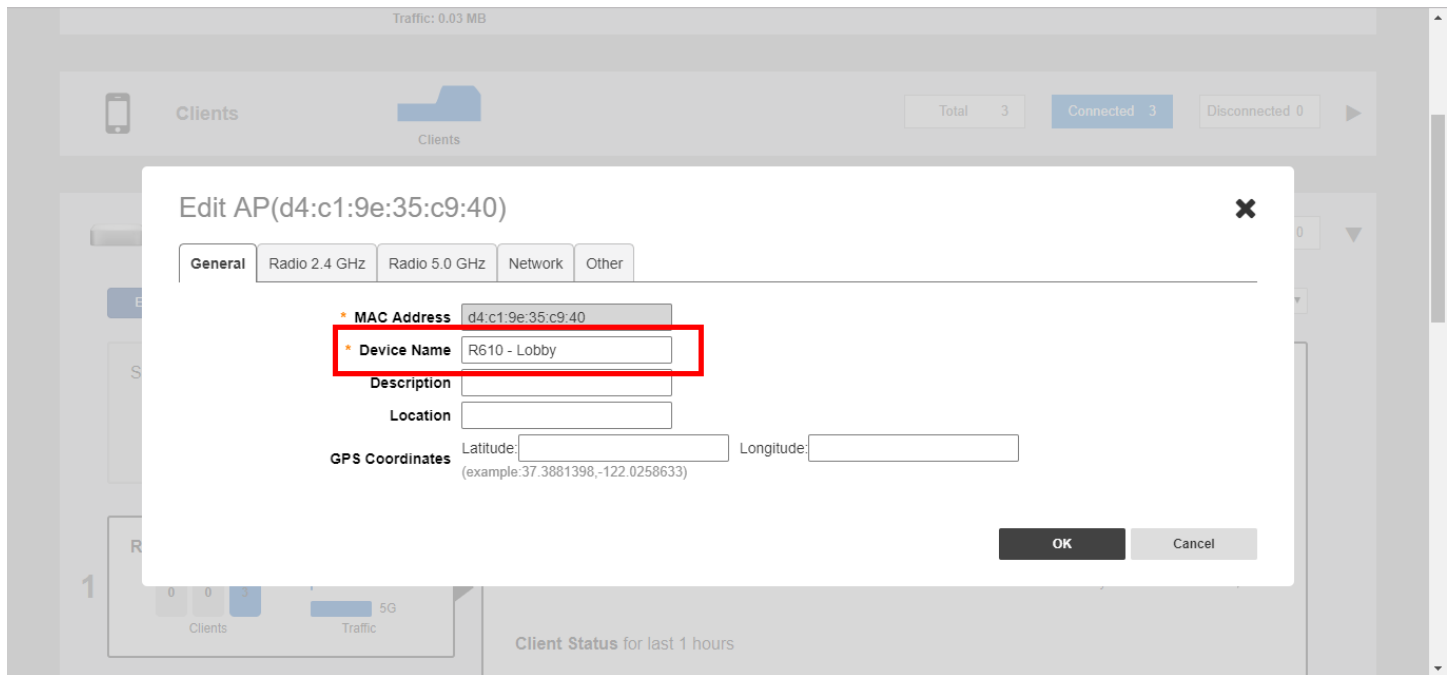


## Renaming an AP

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 155 Renaming an AP



## Working with AP Groups

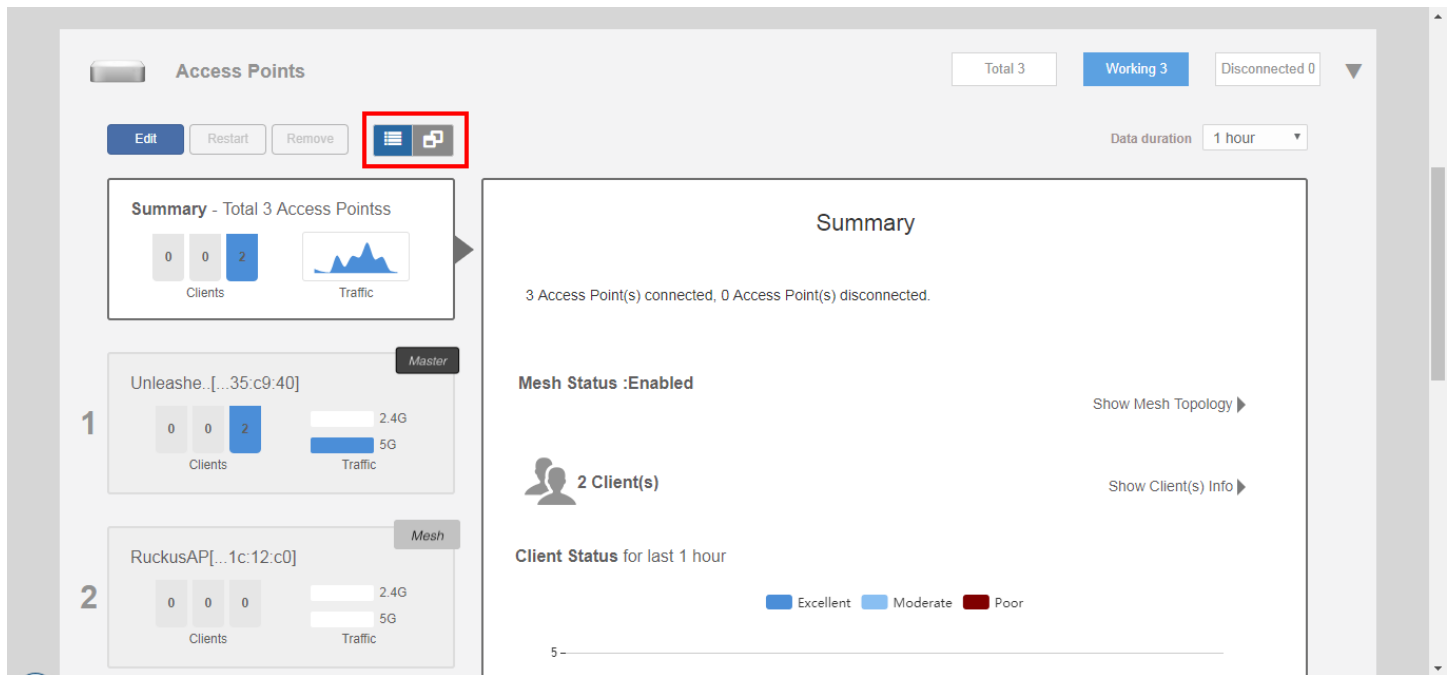
Access Point Groups can be used to define configuration options and apply them to groups of APs at once, without having to modify each AP's settings individually.

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 156 Set View Mode to AP Group



## Modifying the System Default AP Group

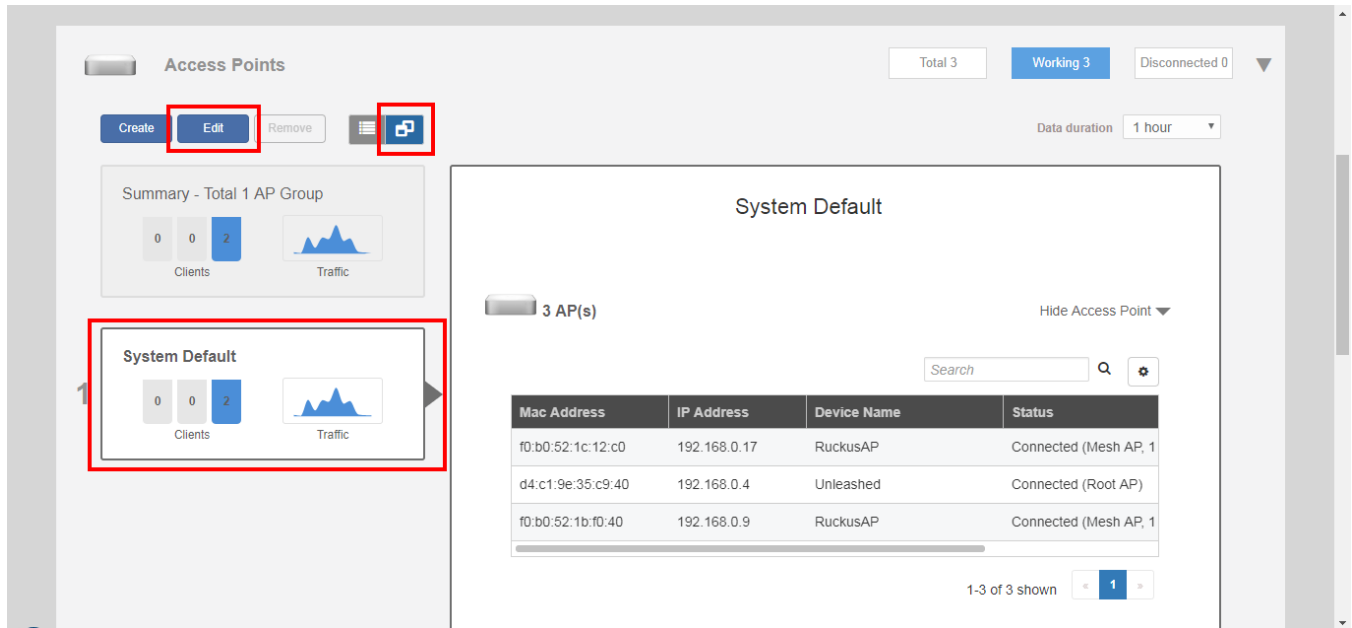
If you want to configure global settings for default behavior for all access points, modify the System Default AP group and apply settings to all APs at once.

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 157** Click Edit to configure the AP group



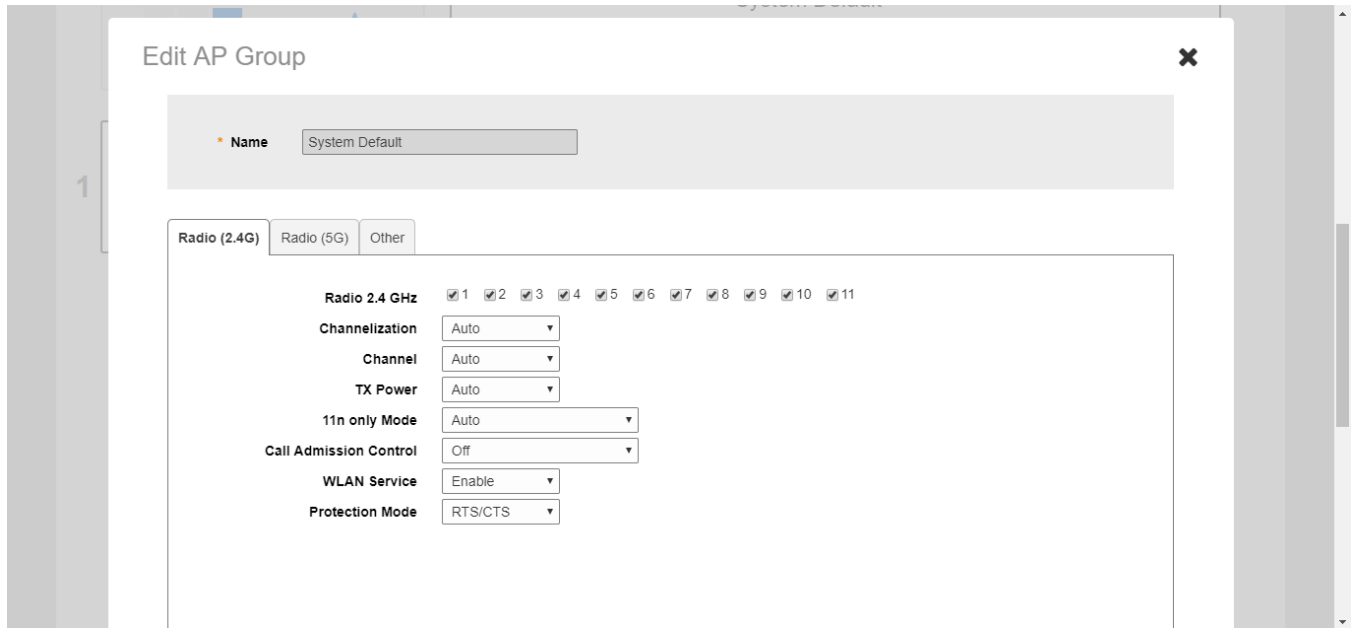
The *Edit AP Group* form appears.

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.
  - **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
  - **11n only Mode:** Force all 802.11n and 11ac APs to accept only 802.11n/ac compliant devices on the 2.4 GHz or 5 GHz radio. If 11n/ac Only Mode is enabled, all older 802.11b/g devices will be denied access to the radio.
  - **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 207.
  - **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 389.
    - **Port Setting:** Refer to [Configuring AP Ethernet Ports](#) on page 227 for more information on configuring AP-specific Ethernet port settings.

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

**FIGURE 158** Configure AP group settings



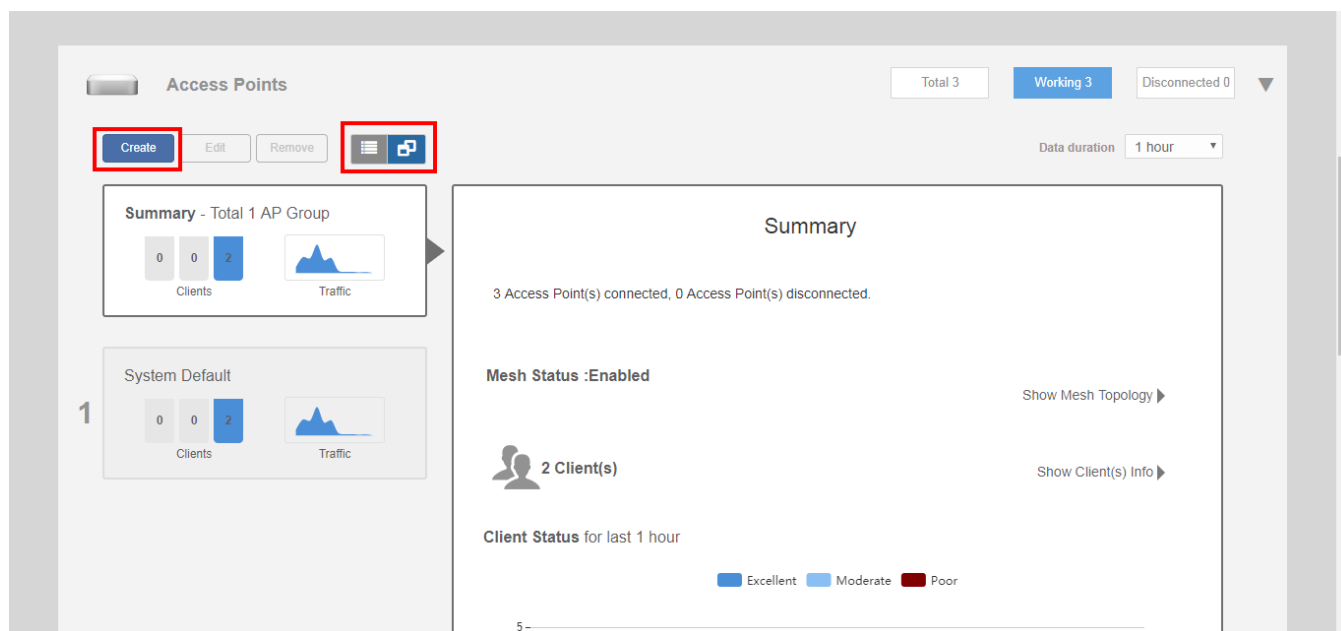
## Creating a New AP Group

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 159** Create 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).

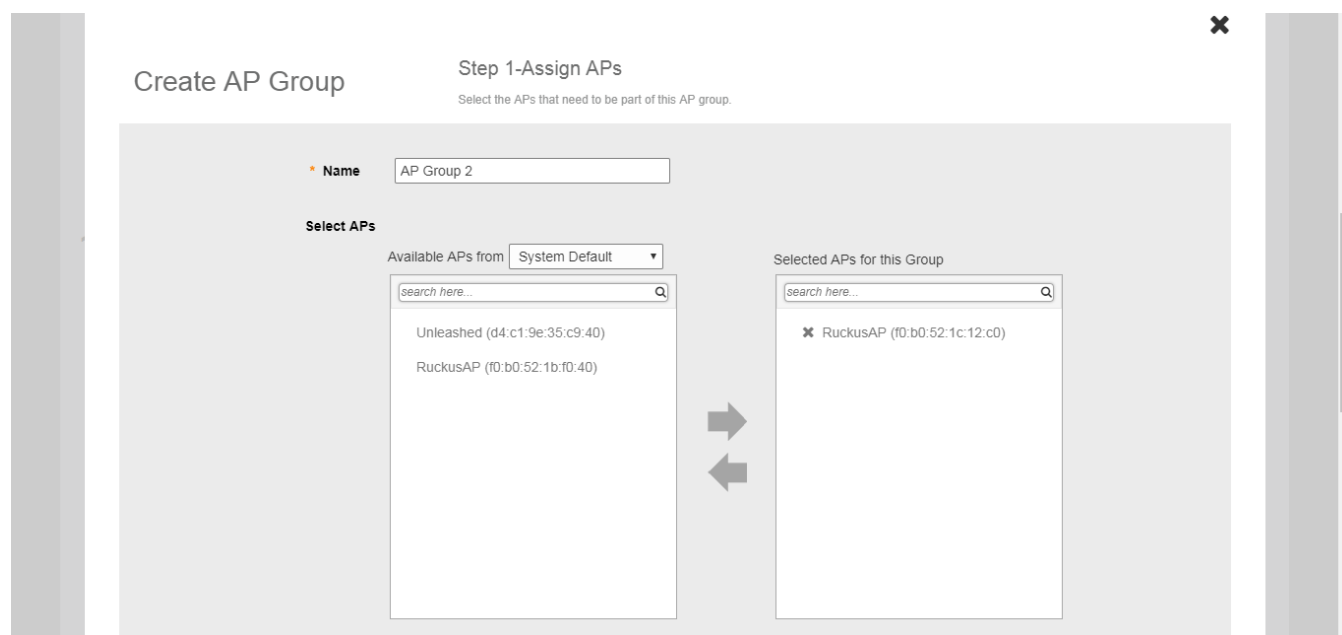
Max = max allowable Tx power according to country regulations

Min = 0dBm per chain for 11n APs, 2dBm per chain for 11ac APs
  - **11n only Mode:** Force all 802.11n APs to accept only 802.11n compliant devices on the 2.4 GHz radio. If 11n Only Mode is enabled, all older 802.11b/g devices will be denied access to the radio.
  - **11n/ac/ax only Mode:** Force all 802.11n/11ac/11ac APs to accept only 802.11n/ac/ax compliant devices on the 5 GHz radio. If 11n/ac/ax Only Mode is enabled, all older 802.11b/g devices will be denied access to the radio.
  - **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 160** Create new AP group



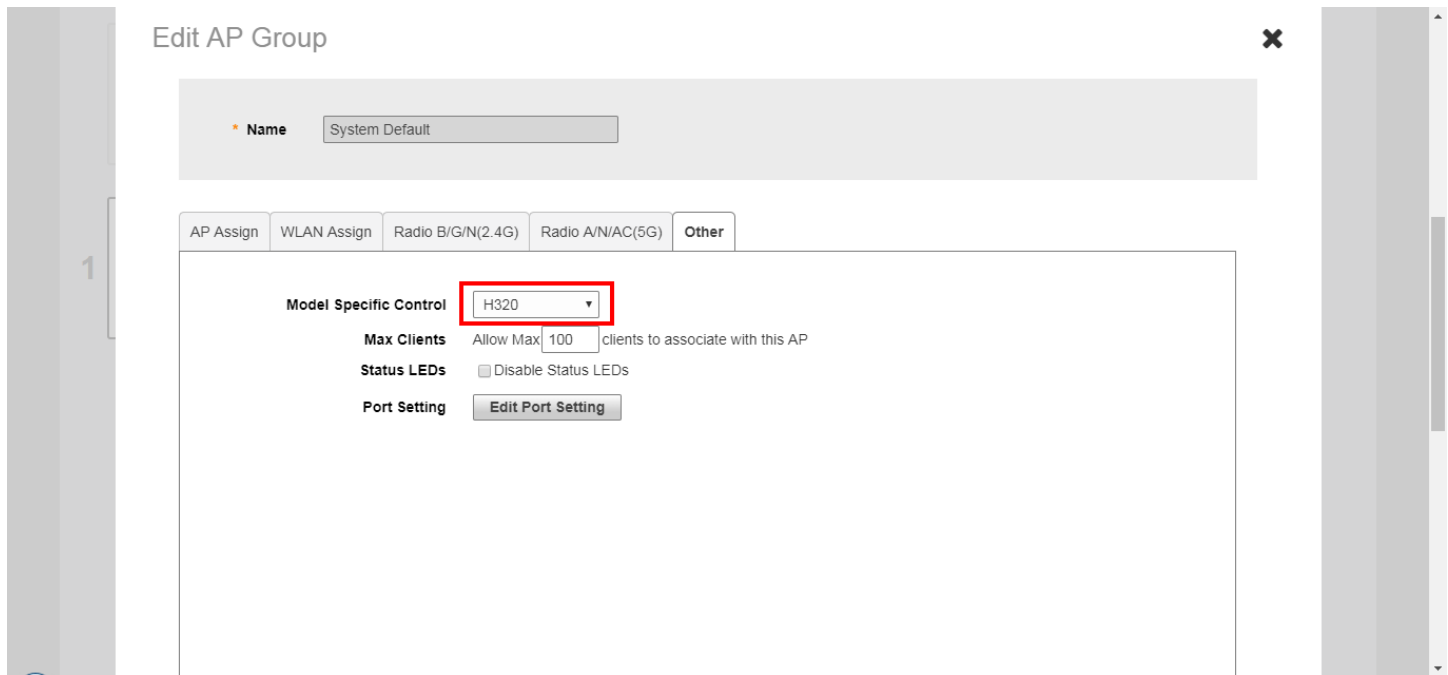
## Modifying Model Specific Controls

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 161 Model Specific Controls



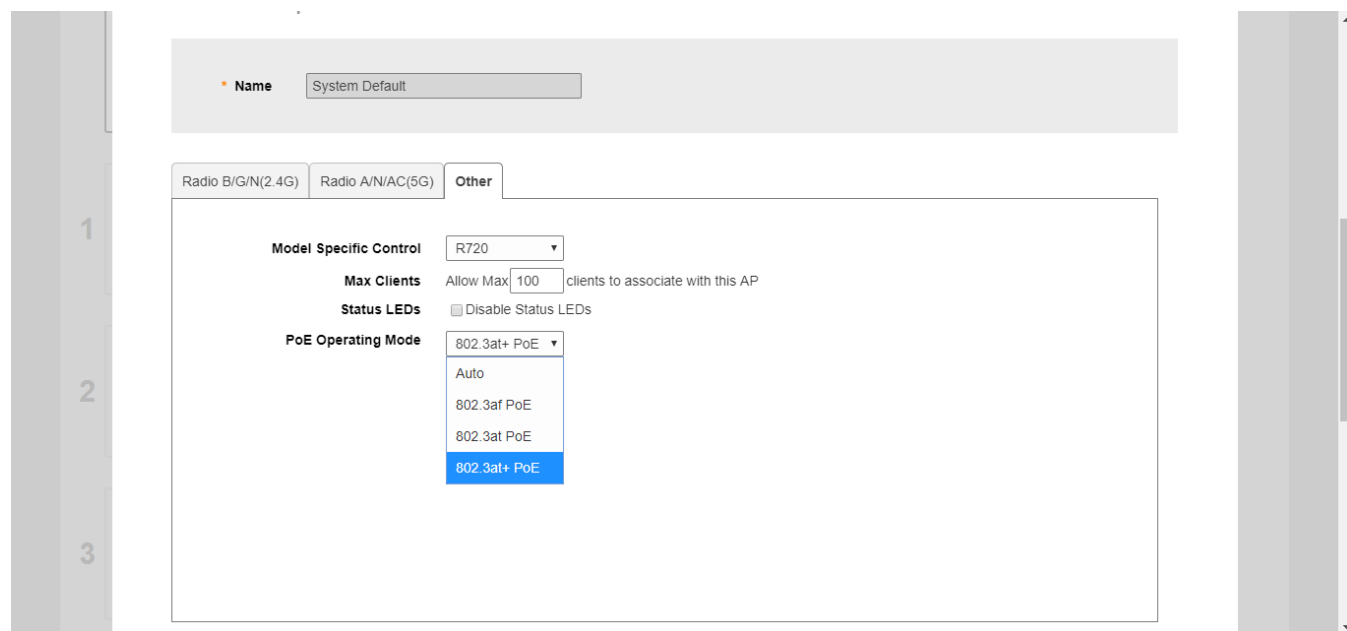
Configure any of the following settings for each model independently, and click **Finish** to save your changes:

- **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 227 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 389.

FIGURE 162 PoE Operating Mode



## Configuring AP Ethernet Ports

You can use AP groups to configure Ethernet ports on all APs of a certain model.

### NOTE

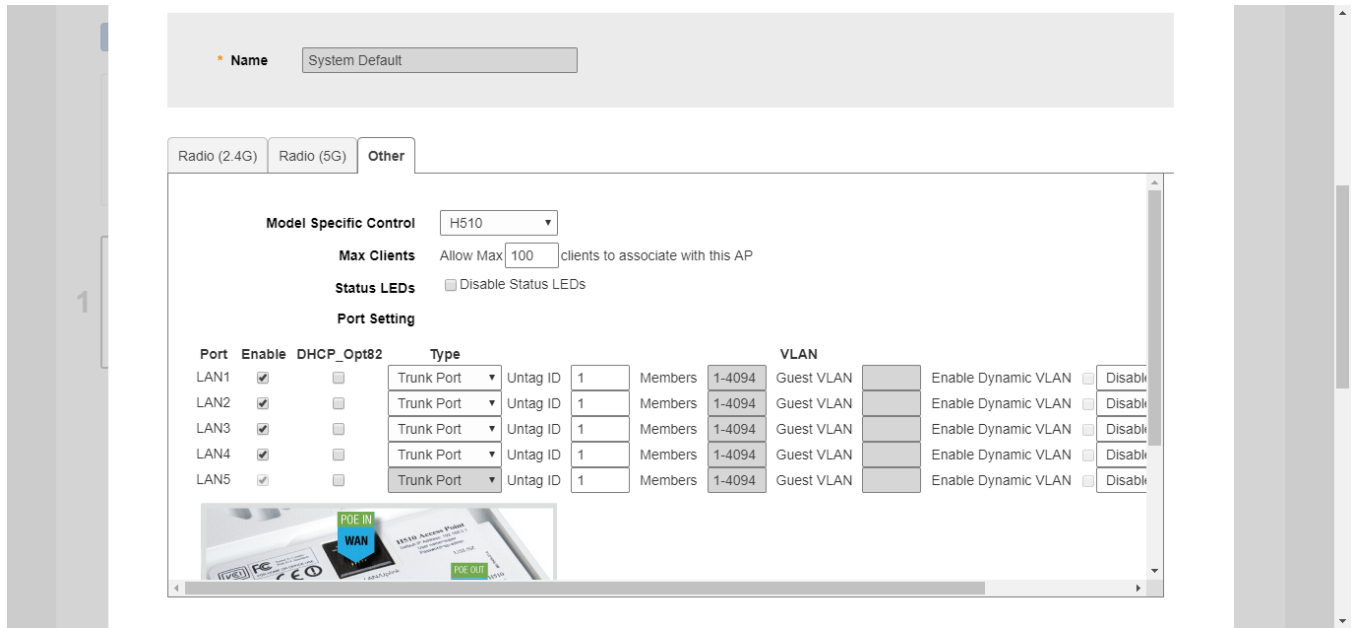
Currently, only Unleashed H320 and H510 wall-plate APs provide Ethernet port configuration options.

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 163** Configure AP Ethernet ports



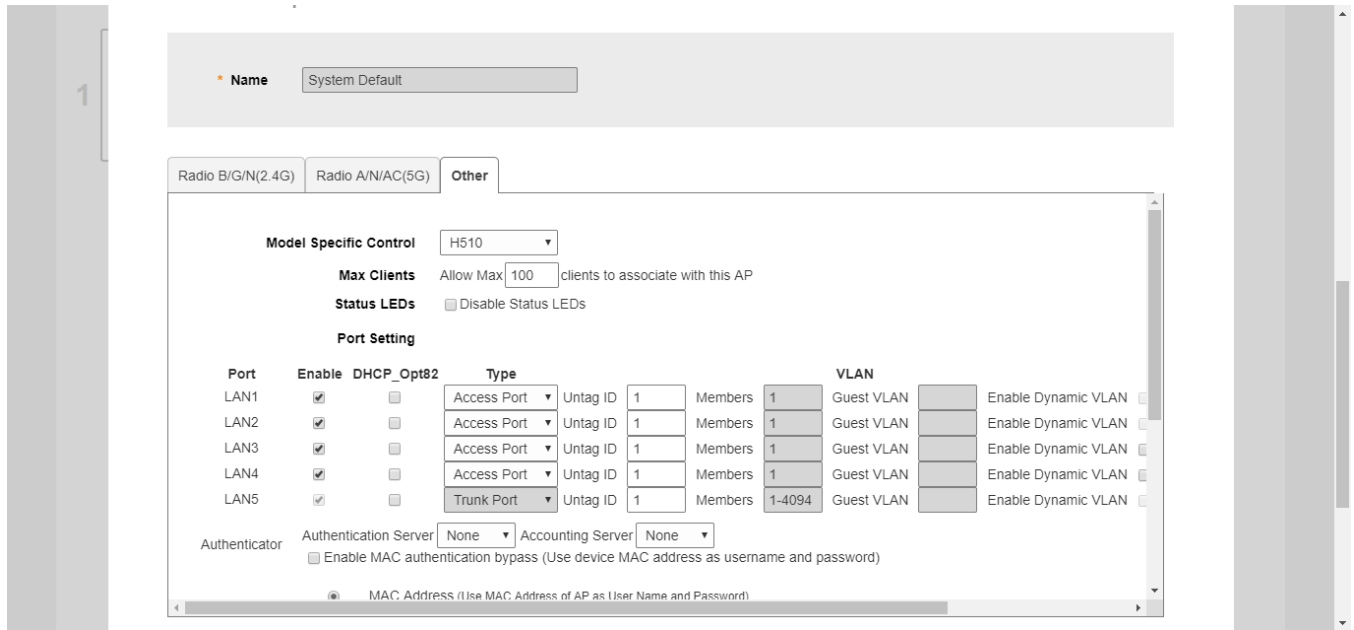
11. In **802.1X**, select whether the port will be used as an 802.1X Supplicant, Authenticator (port-based or MAC-based), or whether 802.1X is disabled on the port. AP Ethernet ports can be individually configured to serve as either an 802.1X supplicant (authenticating the AP to an upstream authenticator 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*.

12. 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.
13. 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.

14. Click **Finish** to save your changes.

**FIGURE 164** H510 Port Settings: Enable, DHCP Option 82, Port Type and VLAN Untag ID



**FIGURE 165** H510 Port Settings: Guest VLAN, Dynamic VLAN and 802.1X

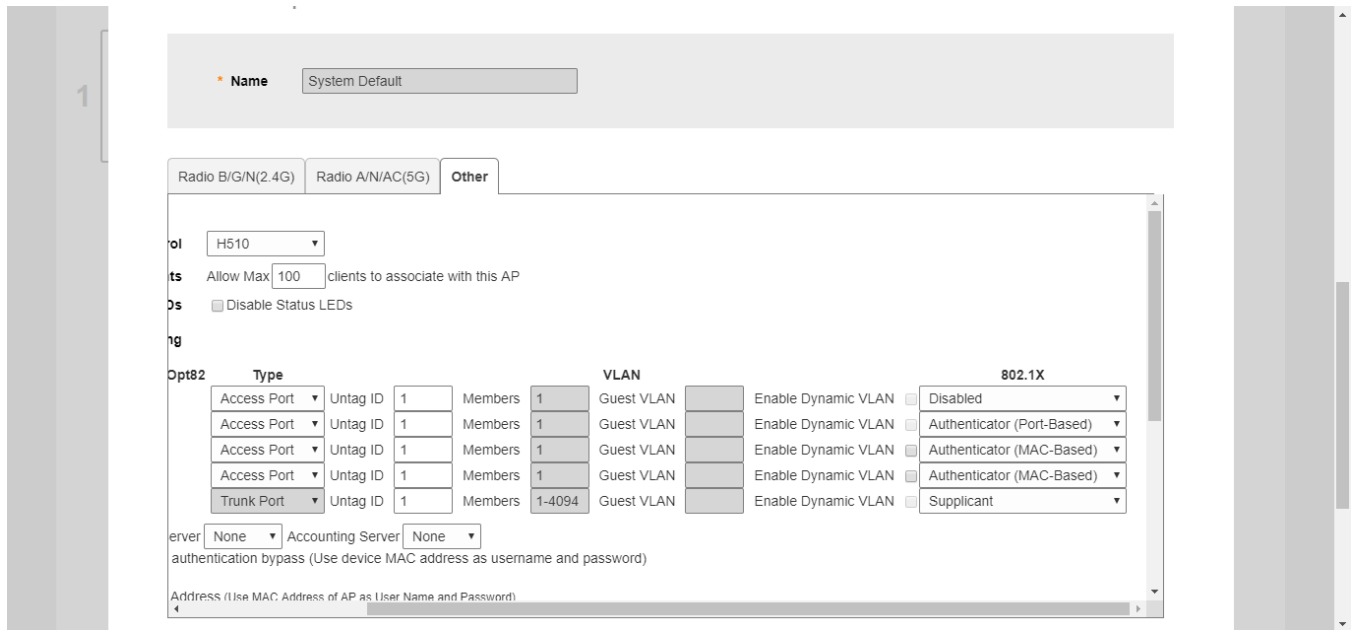
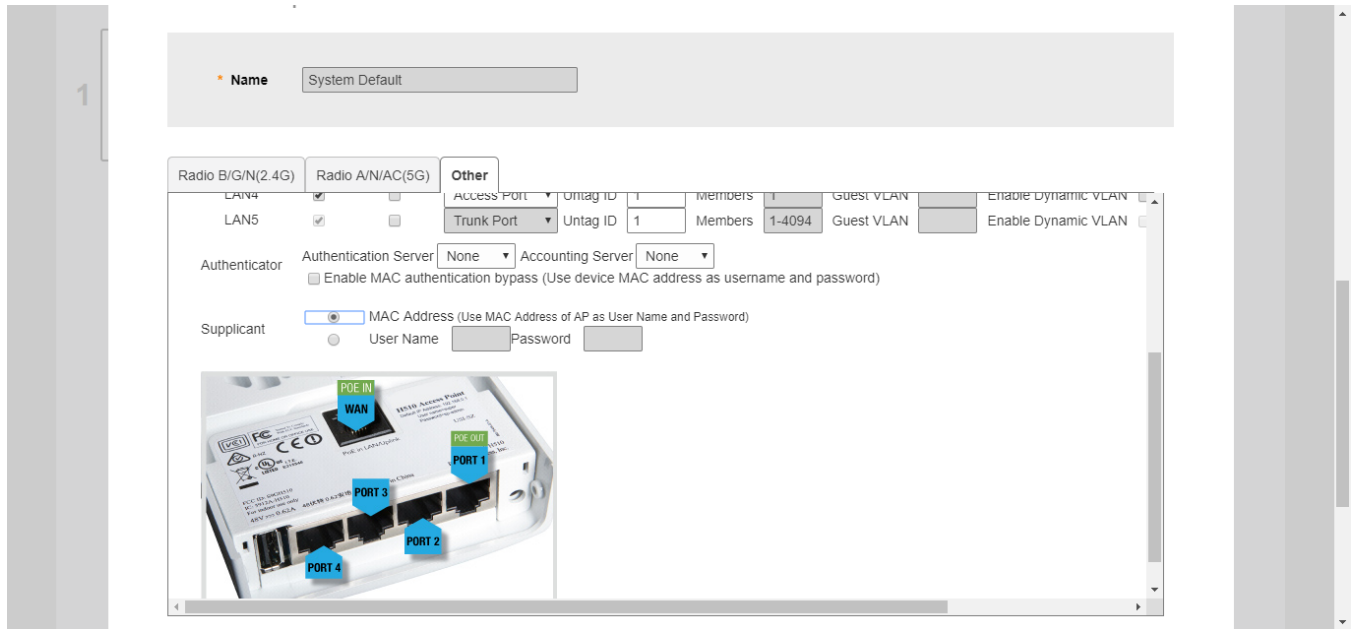


FIGURE 166 H510 Authenticator and Supplicant settings



## 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 Port and enter any valid VLAN ID in the VLAN ID field (valid VLAN IDs are 2-4094).

The following table describes the behavior of incoming and outgoing traffic for Access Ports with VLANs configured.

**TABLE 22** 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.

## Access Point Configuration

### Restarting an AP

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 167** Monitor currently connected 802.1X wired clients

The screenshot shows the 'Clients' dashboard with the following components:

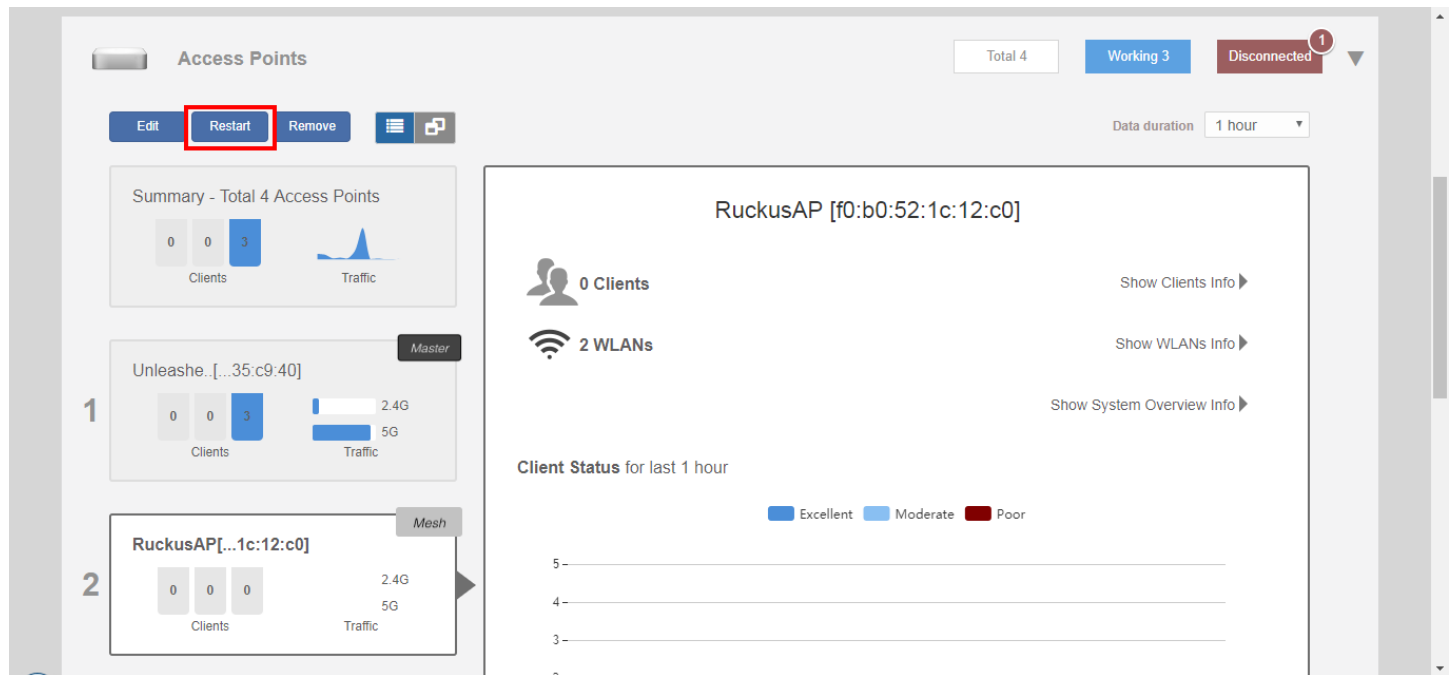
- WiFi Networks:** Total 1, Working 1, Disabled 0. Traffic: 0.09 MB.
- Clients:** Total 1, Connected 1, Disconnected 0.
- Wired Clients:** 0 wired clients connected. A table with columns: Mac Address, User/IP, Access Point, VLAN, Status. The table is empty with the message "No data available." Below the table, it shows "0-0 of 0 shown" and a page number "1".
- Wireless Clients:** 1 wireless clients connected.
- Access Points:** Total 1, Working 1, Disconnected 0.

## 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 168 Click Restart to reboot a single AP



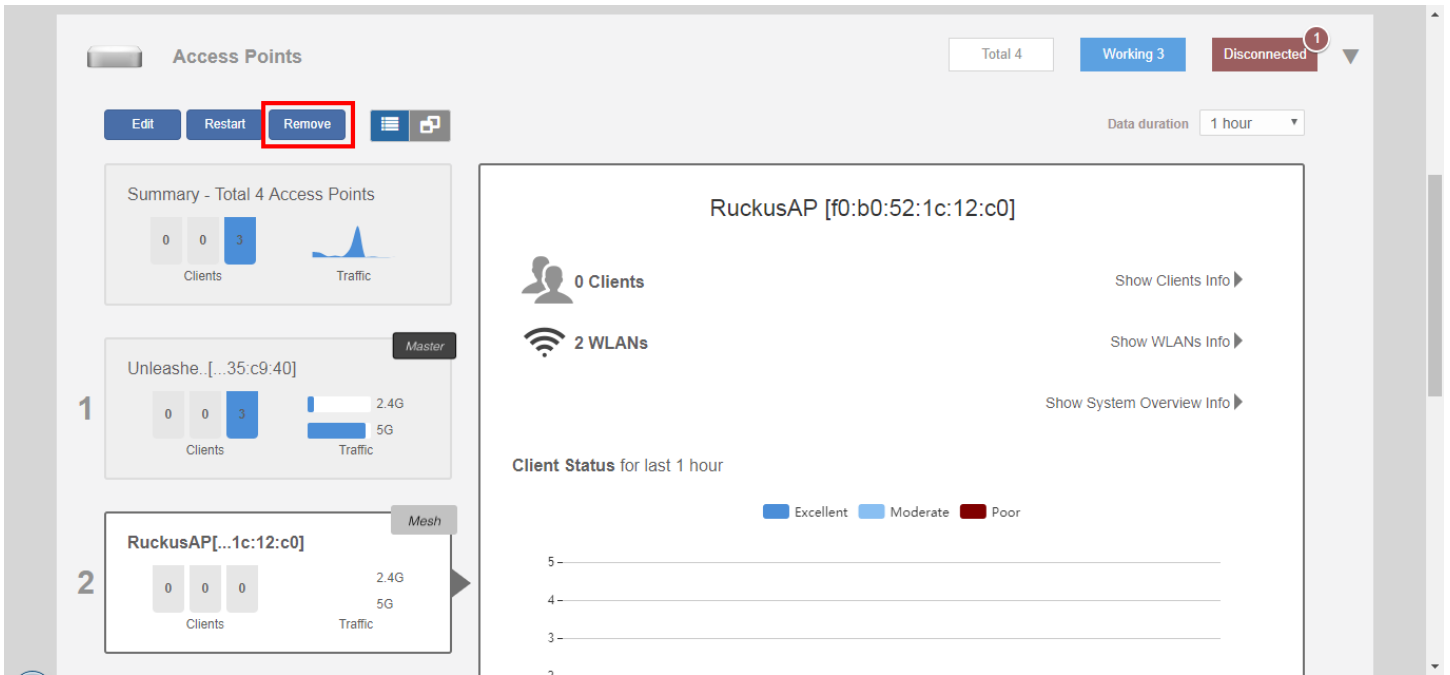
**NOTE**

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 169 Removing an AP



# ICX Switch Management

---

- ICX Switch Management Overview..... 235
- Preparing an ICX Switch for Unleashed Management..... 236
- Approving a New Switch to Join Unleashed..... 239
- Monitoring Connected ICX Switches..... 242
- Managing Switch Ports..... 243
- Backup and Restore Switch Configuration..... 246
- Upgrading ICX Switch Firmware..... 249

## 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.

ICX switch management allows you to monitor status, view usage statistics, and perform some 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:

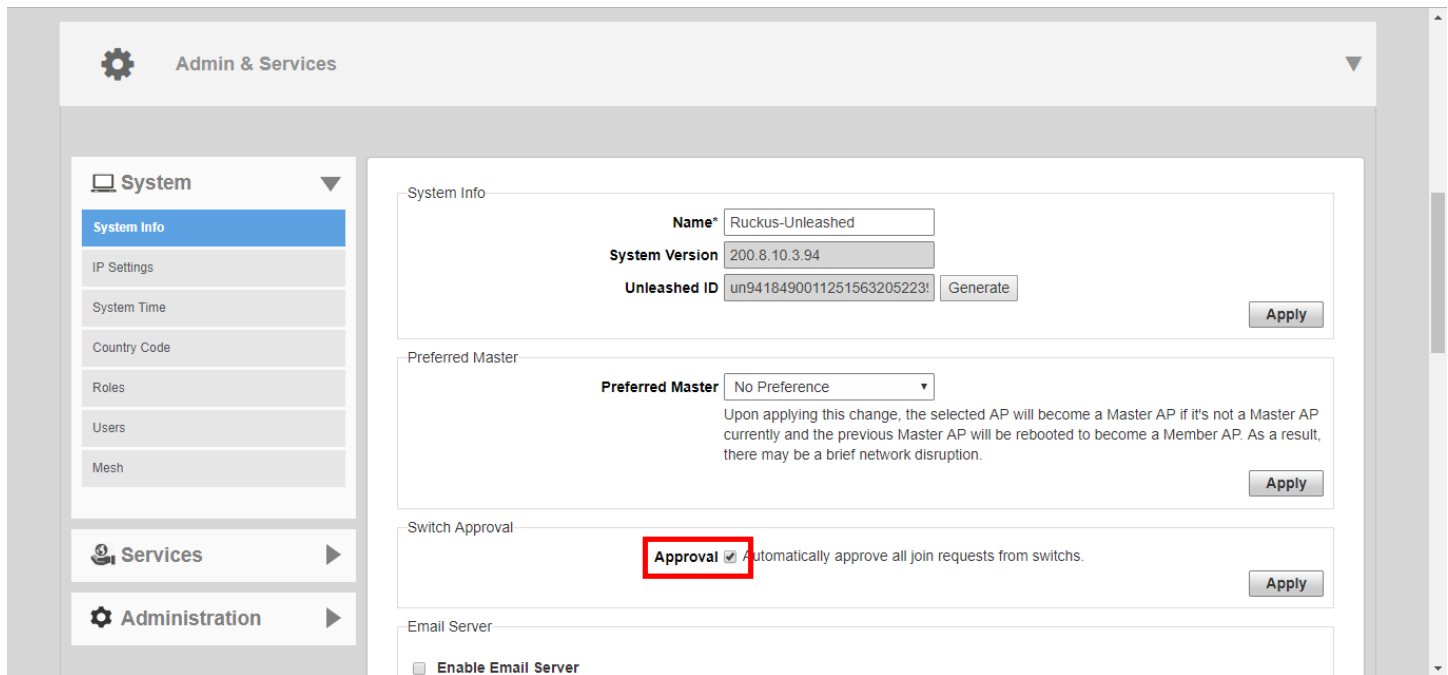
<https://support.ruckuswireless.com>. On the site, select **Products > Ruckus ICX Switches > Technical Documents**, and choose the platform and document of interest.

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 170 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#
```

## ICX Switch Management

### Preparing an ICX Switch for Unleashed Management

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.

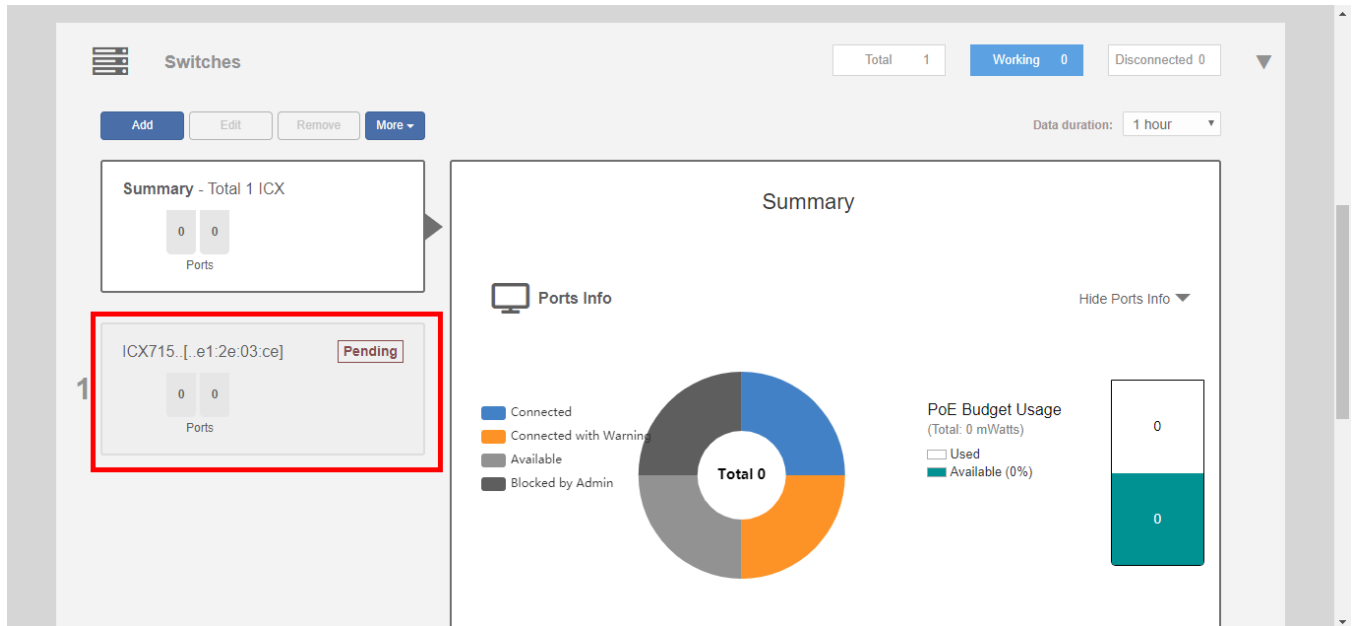
## Approving a New Switch to Join Unleashed

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 171** Select a switch that is pending approval

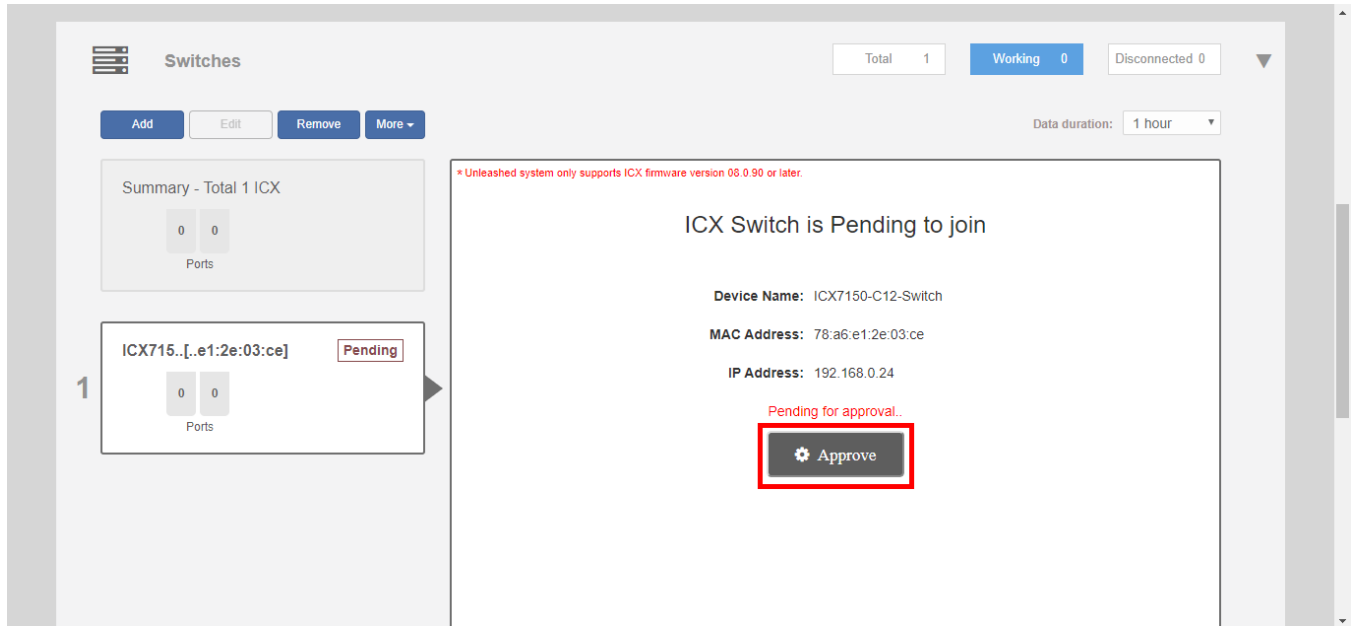


## ICX Switch Management

### Approving a New Switch to Join Unleashed

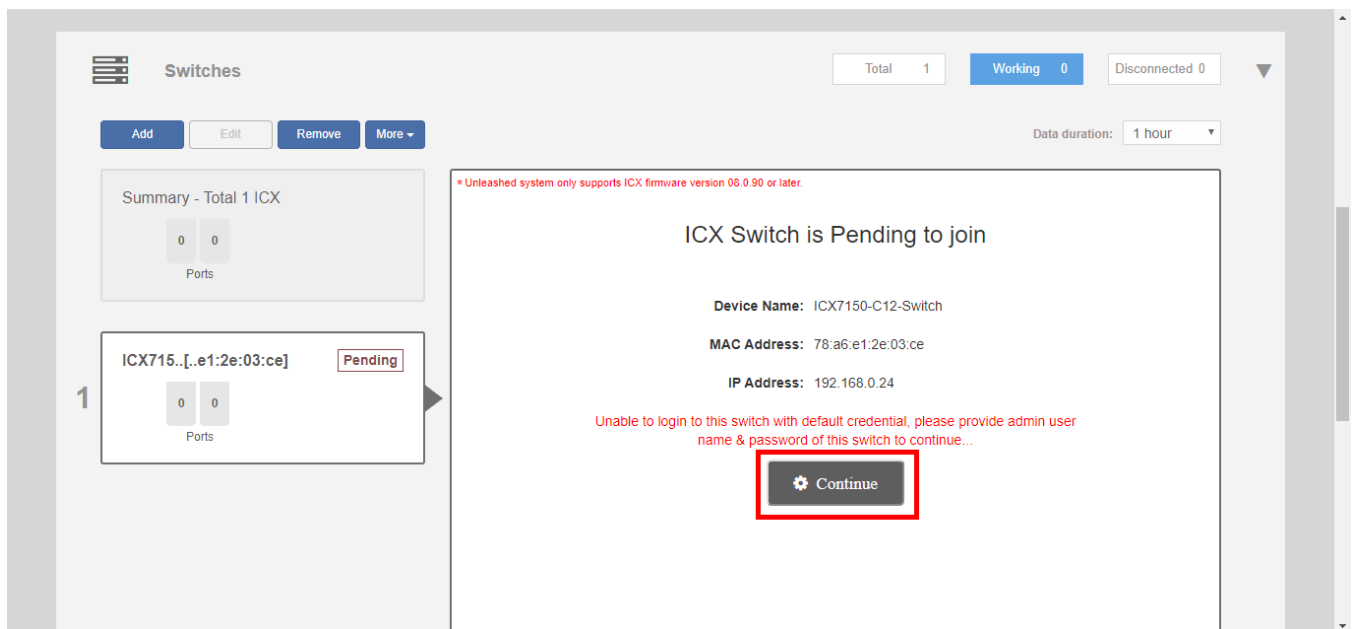
2. Click **Approve**. If the switch is in factory default state, it will automatically connect and be listed as connected once the connection is established and the page is refreshed.

**FIGURE 172** 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.

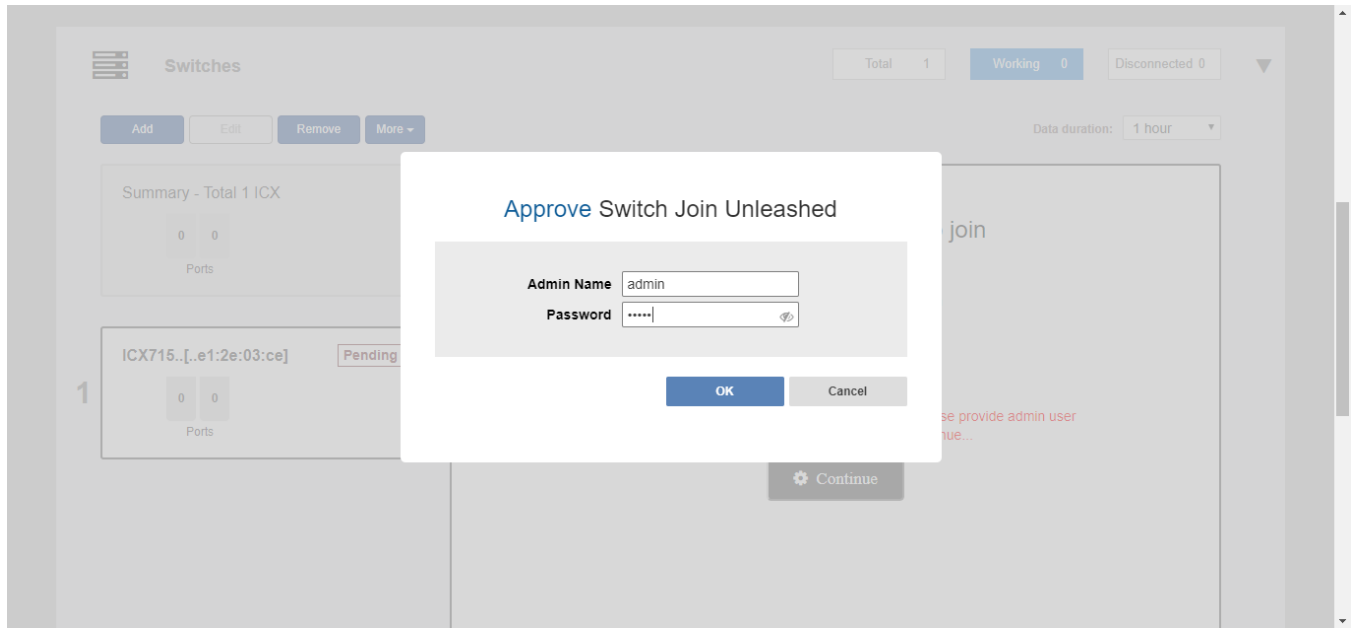
**FIGURE 173** Click Continue





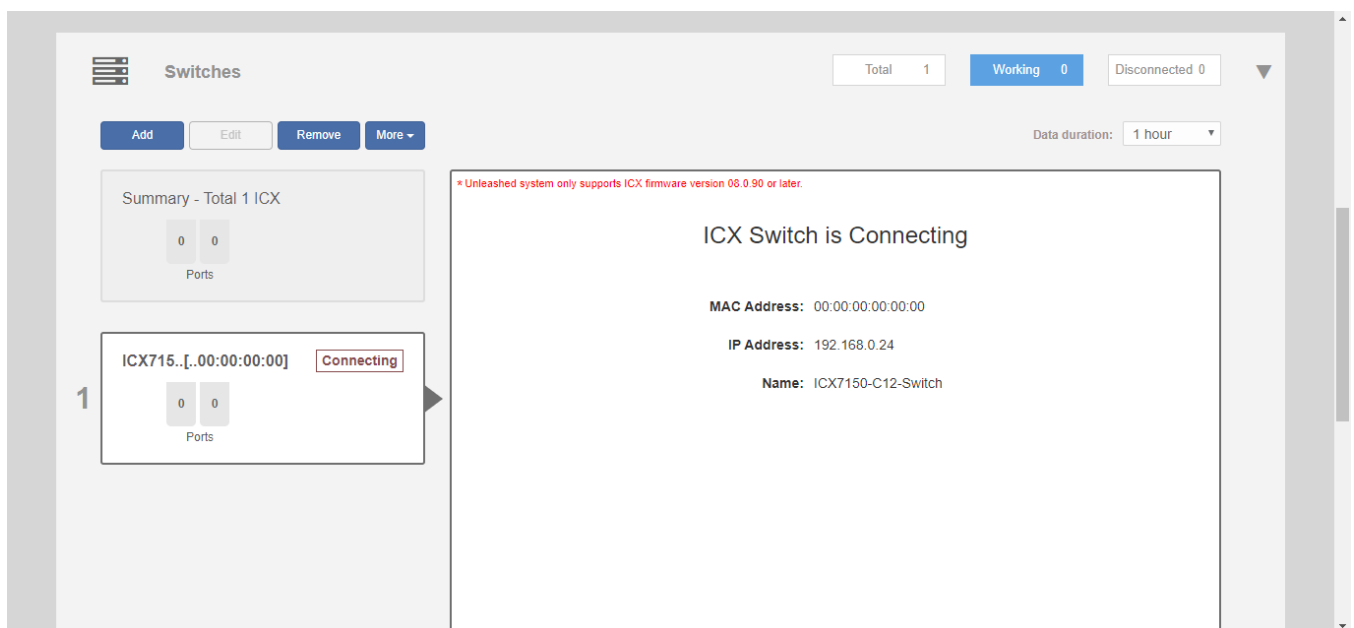
4. In the *Approve Switch to Join Unleashed* dialog that appears, enter the **Admin Name** and **Password** to authenticate to the switch.

**FIGURE 174** 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 175** ICX switch connecting



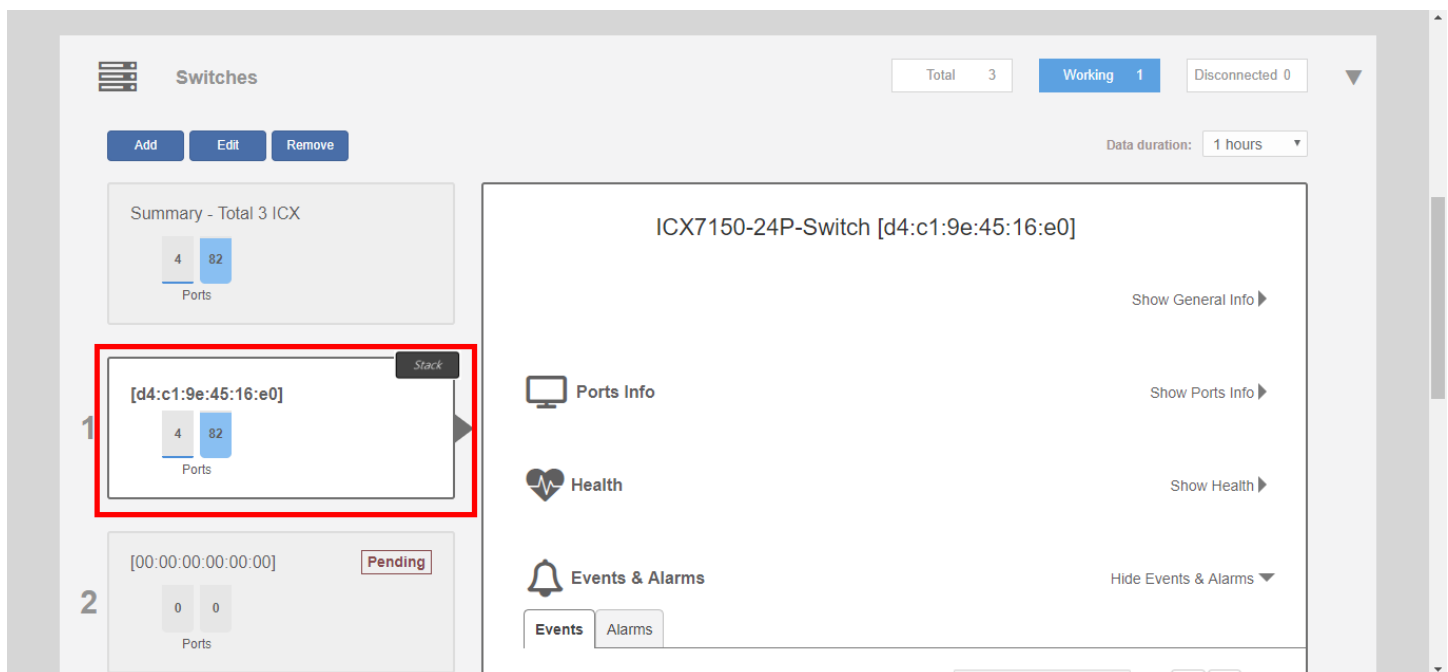
## Monitoring Connected ICX Switches

Expand the *Switches* dashboard component and select a connected switch to view general info, port status, health details and events and alarms on the selected switch.

The following details are displayed when the links are expanded:

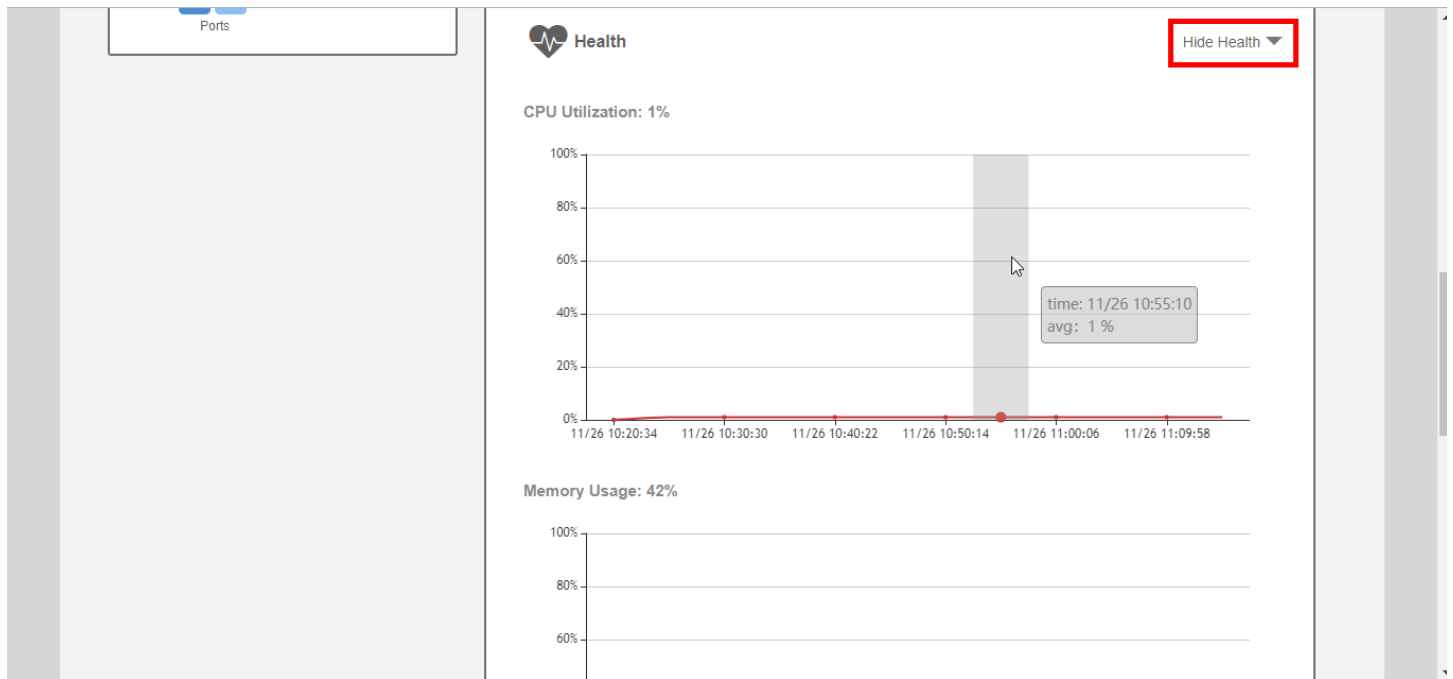
- **General Info:** Displays general device information such as device name, IP address, MAC address, software version and uptime.
- **Ports Info:** Displays the number of ports used and available, PoE power budget usage, and details on specific ports when selected from the port diagram or port list.
- **Health:** Displays hardware status info such as CPU and memory utilization.
- **Events & Alarms:** Displays a list of alarm and event system messages.

**FIGURE 176** Select 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 177 Monitoring switch health details



## Managing Switch Ports

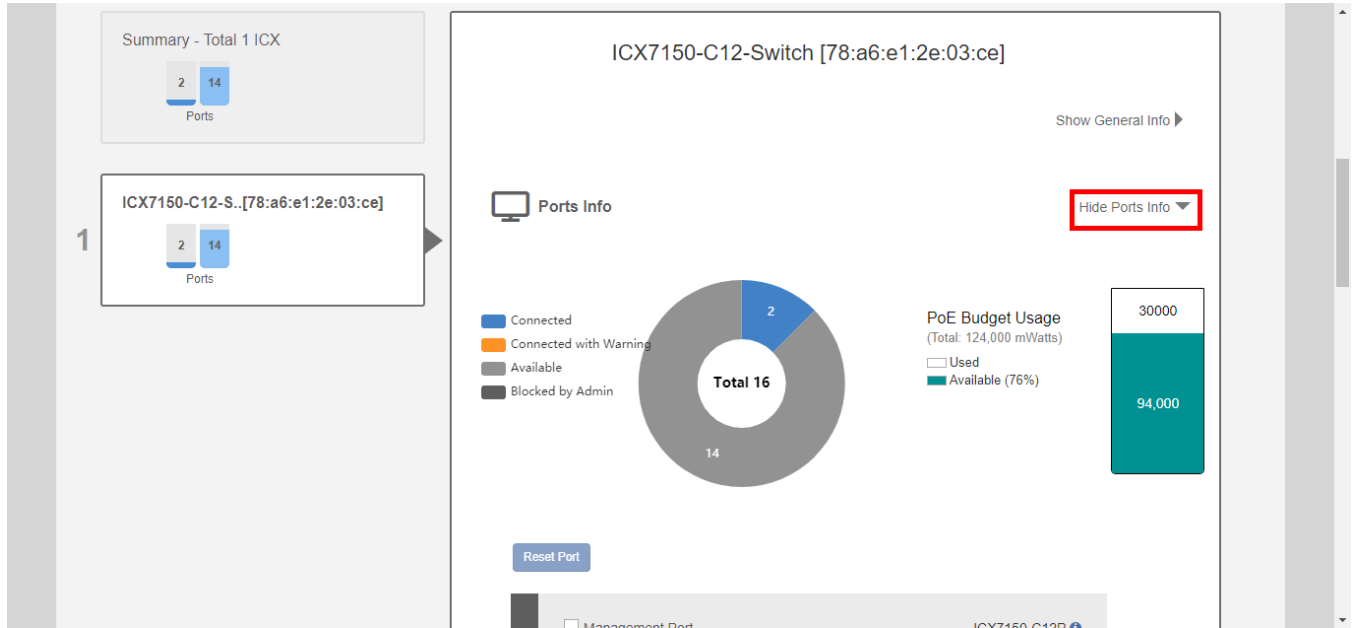
The "Ports Info" link expands to display information on overall switch status such as the number of ports used and available and PoE power budget usage. Individual switch ports can be managed by selecting the specific port from the switch port diagram or from the port list table below.

To manage ICX switch ports:

1. Expand the **Switches** dashboard component, and select a connected switch from the list on the left.

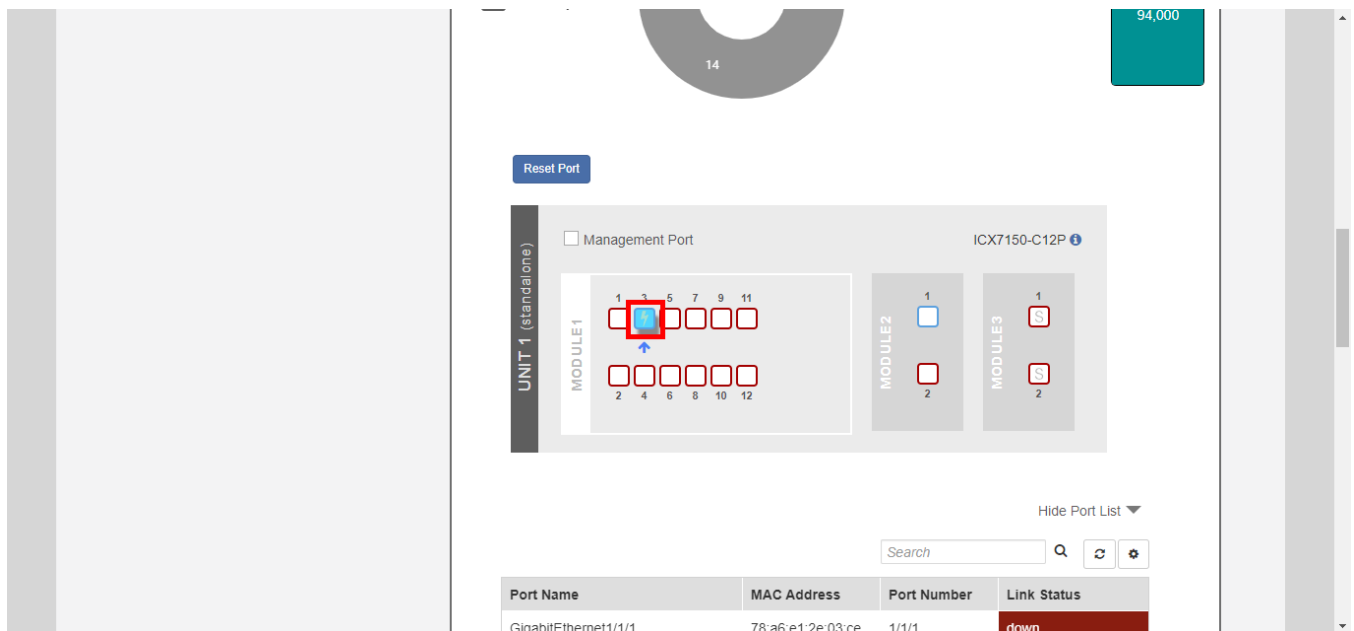
2. Click **Show Ports Info** to expand the port details view.

**FIGURE 178** The "Ports Info" view displays summary info and per-port details



3. Select an individual port from the port diagram or port list table.

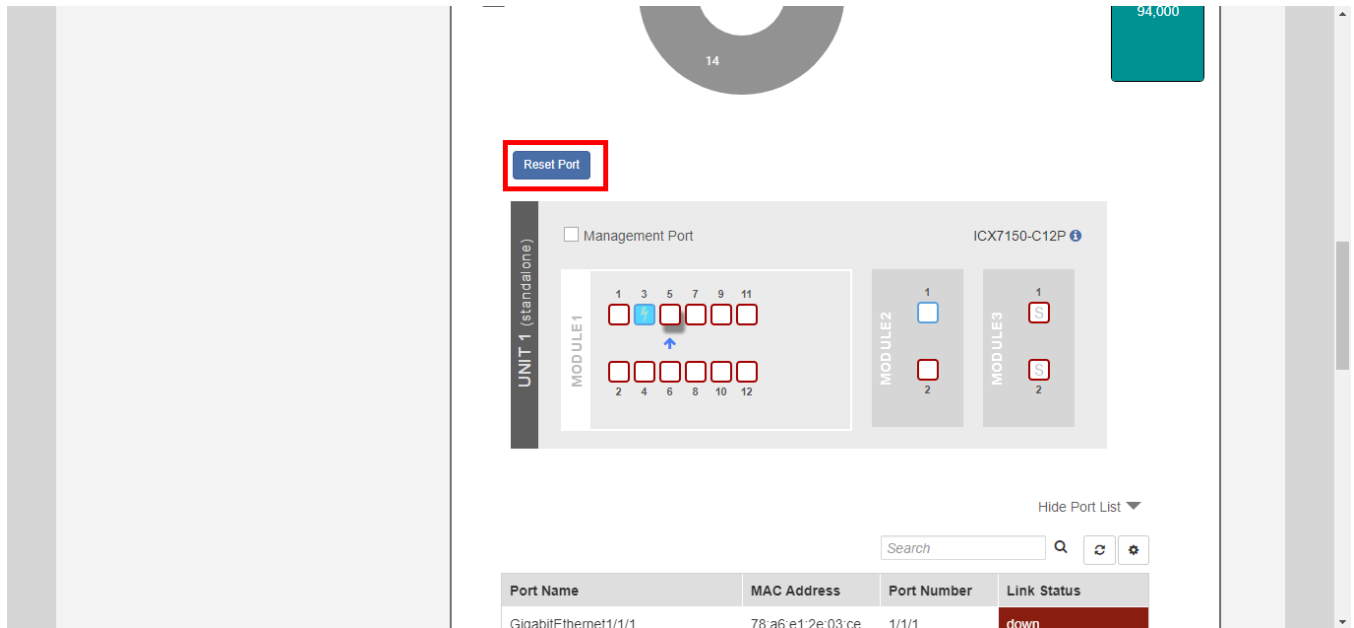
**FIGURE 179** Select a switch port to display details on that port



4. Review the details in the switch port list for the port selected.

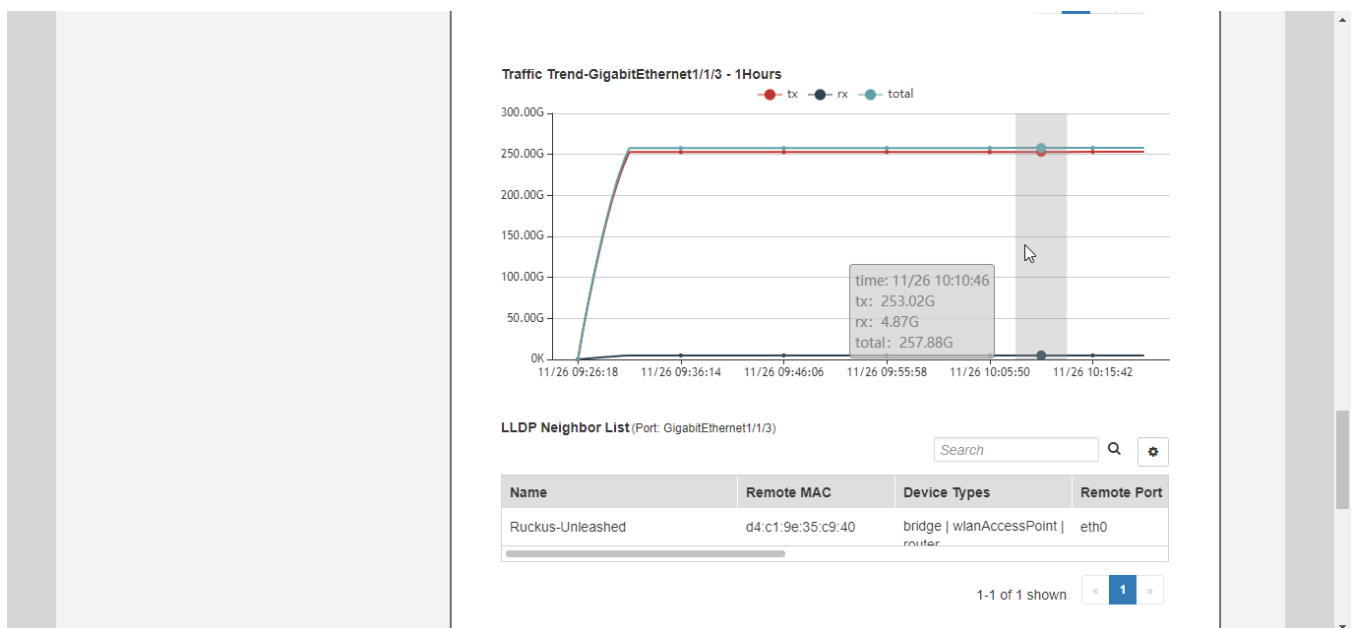
- To reboot a device connected to a PoE switch port, click the **Reset Port** button. The port reset button can be used to power cycle a connected device by powering down and back up a PoE port.

**FIGURE 180** Resetting a switch port



- Scroll down to view the traffic trend chart and LLDP neighbor list for a port.

**FIGURE 181** Viewing a port's traffic statistics and LLDP neighbors



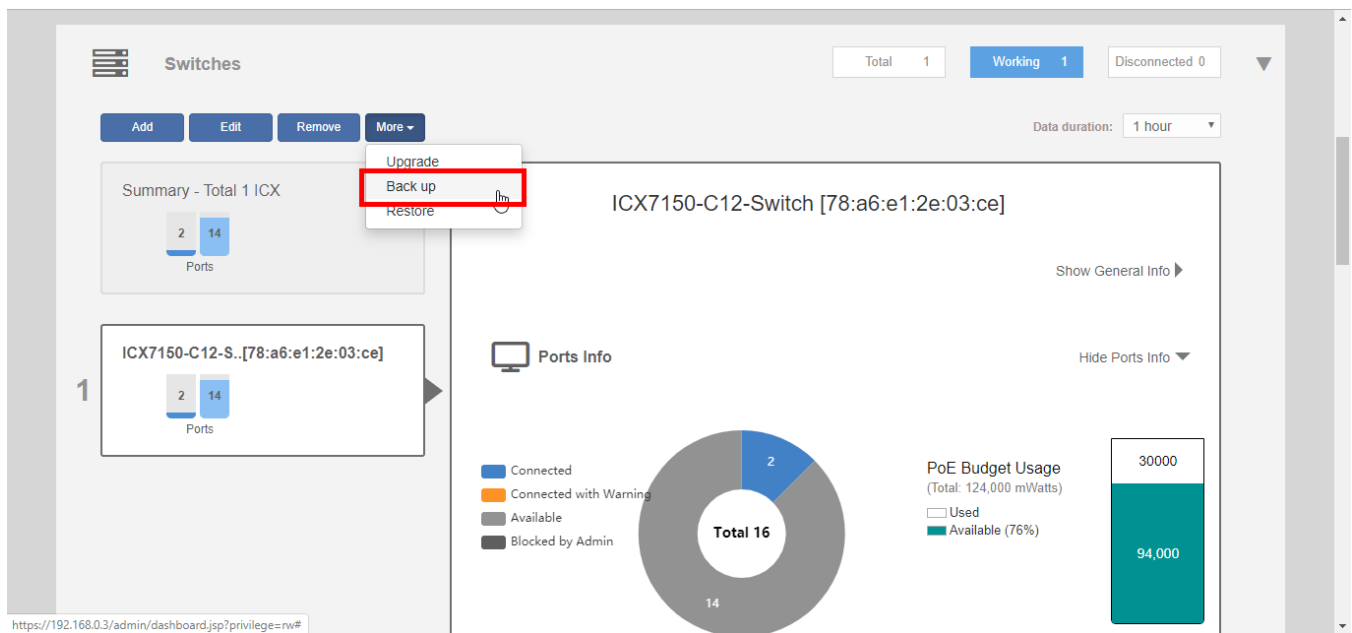
## Backup and Restore Switch Configuration

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.

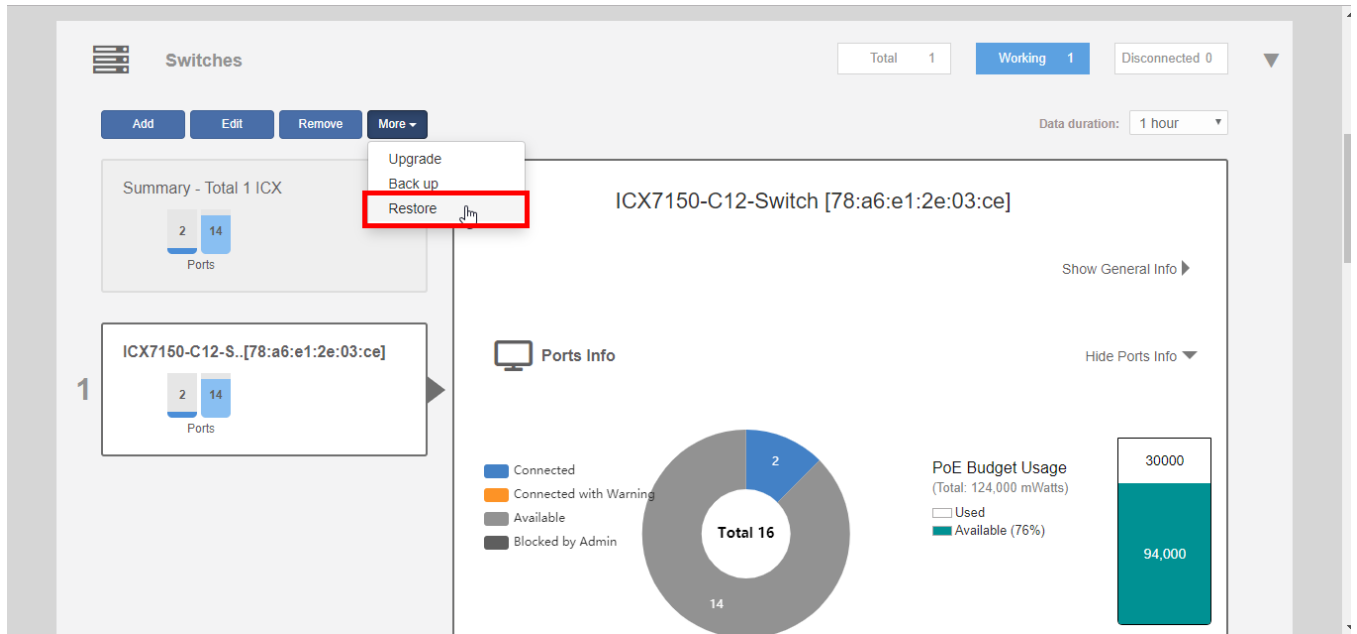
**FIGURE 182** Back up switch configuration



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.

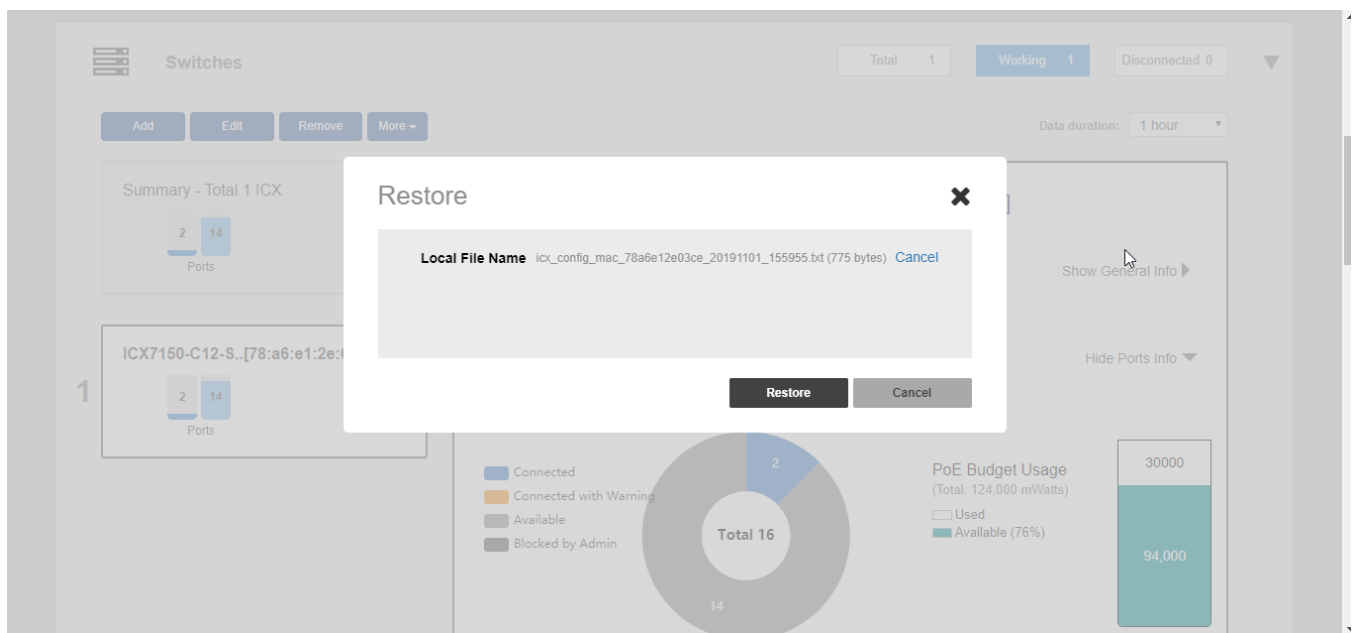
- To restore configuration settings from a previously saved backup file, click **More > Restore**.

**FIGURE 183** Restore switch configuration



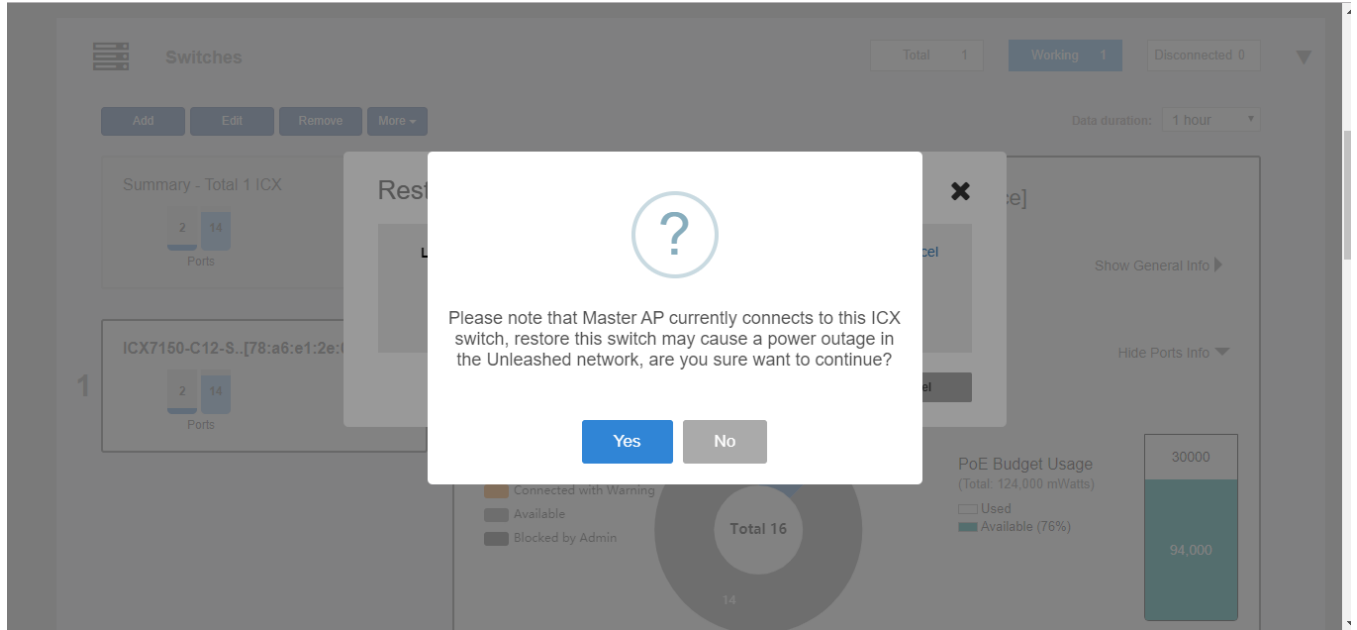
- In the *Restore* dialog, click **Choose File** and select a valid backup file.
- Click **Restore**.

**FIGURE 184** Restore configuration from backup file



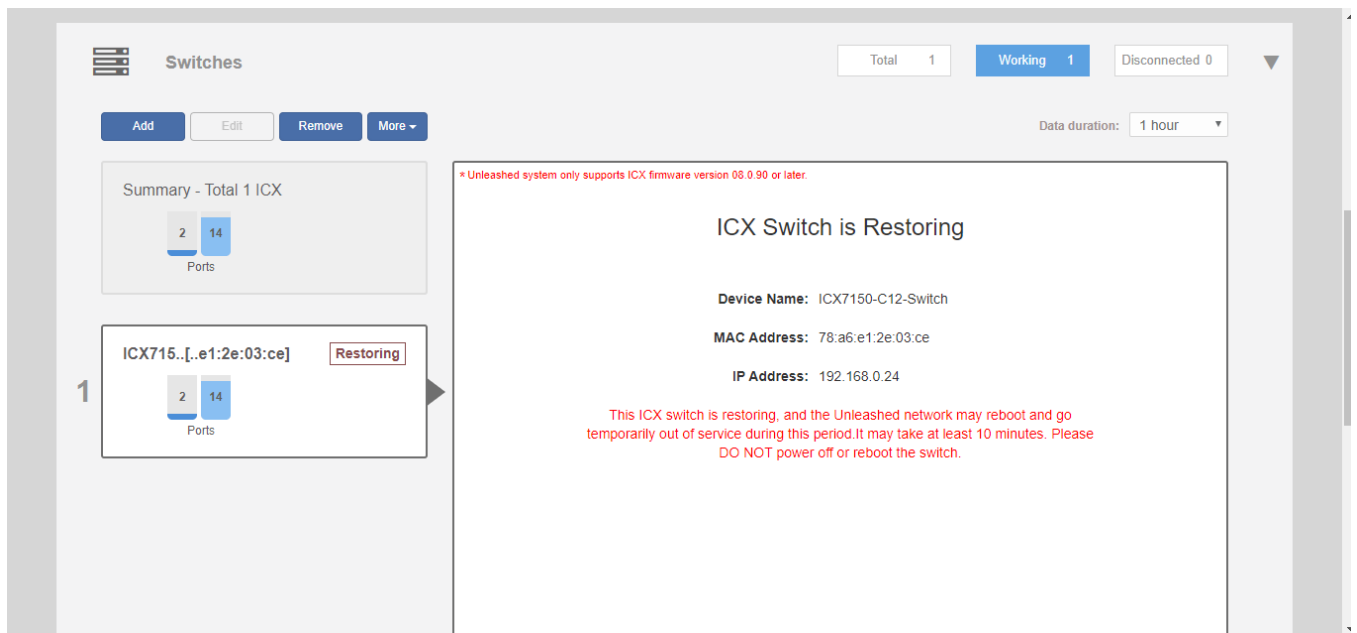
8. A warning message appears notifying you that the restore process will cause a power outage to the Unleashed network. Click **Yes** to confirm.

**FIGURE 185** Switch restore warning



9. The *Switch restore in process* screen appears, notifying you that the restore process may take 10 minutes or more.

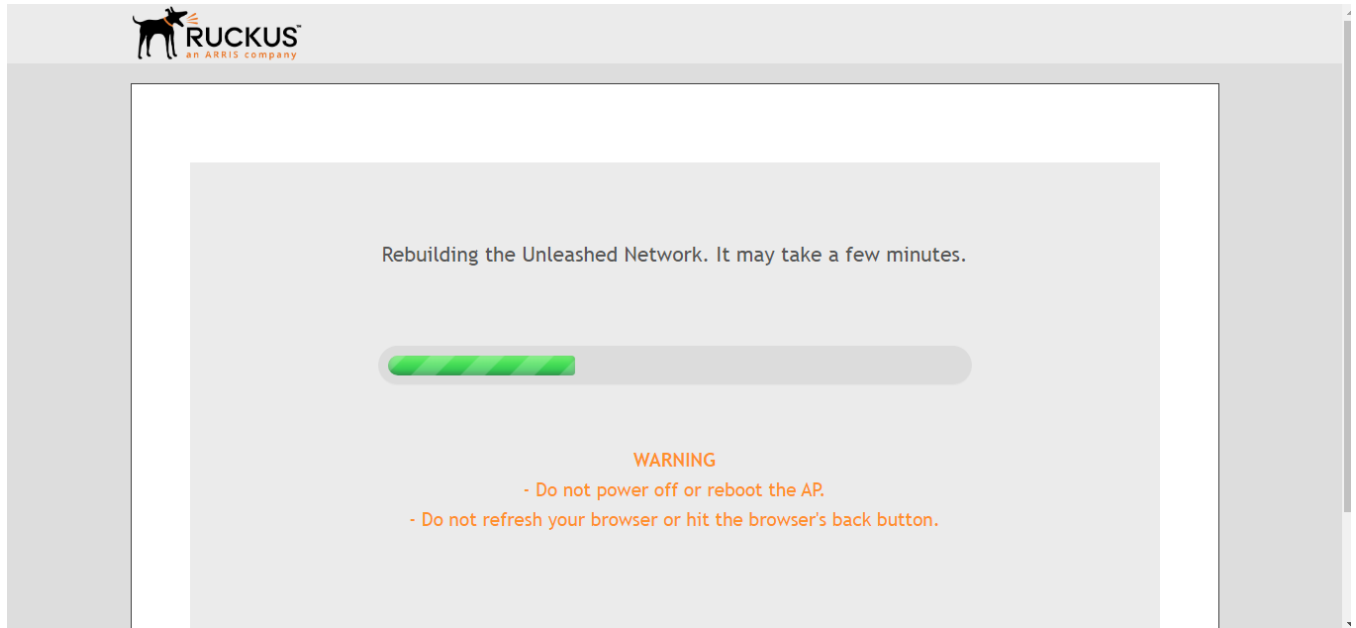
**FIGURE 186** Switch restore in process





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 187** Rebuilding Unleashed Network



11. When the process is finished, the restored switch appears in the connected device list.

## Upgrading ICX Switch Firmware

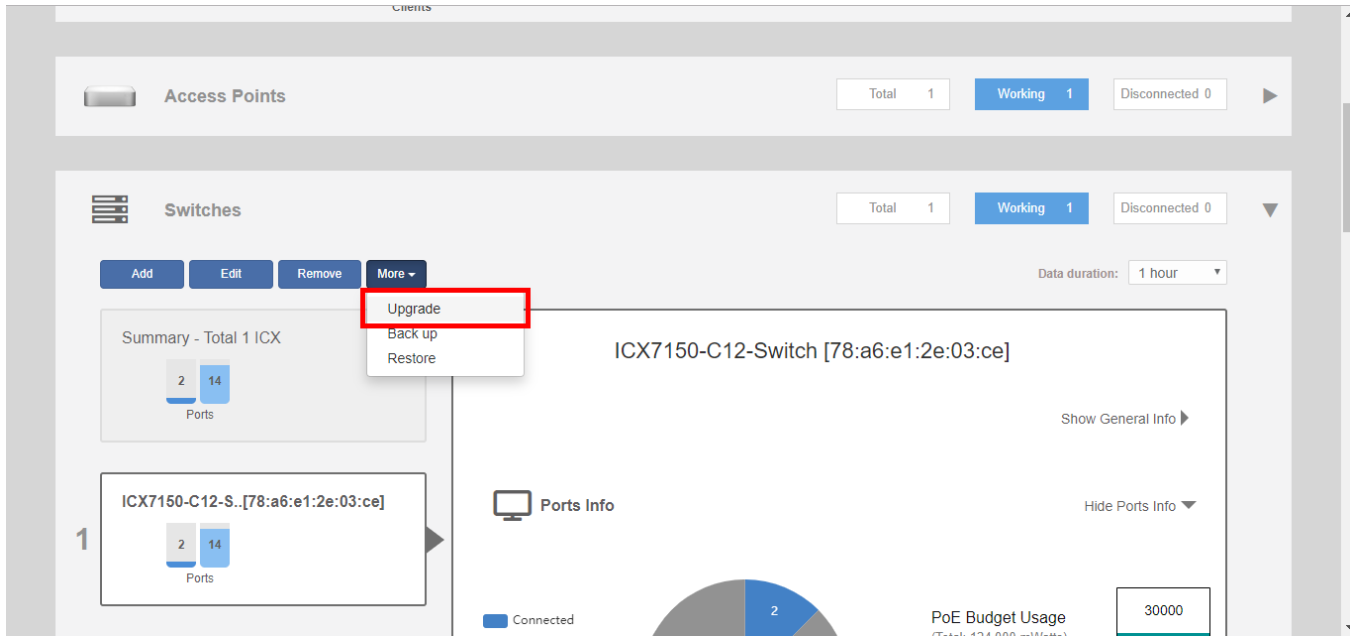
Unleashed management requires FastIron firmware version 08.0.90 or later.

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.

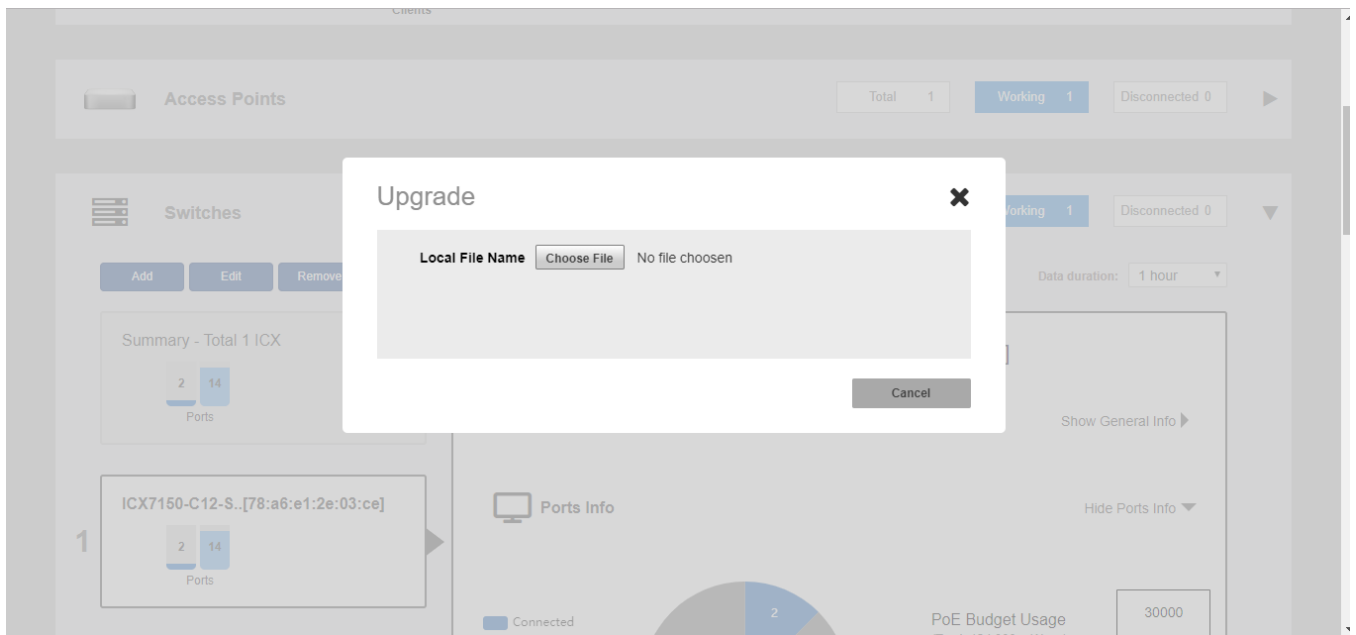
2. Click **More > Upgrade**.

**FIGURE 188** Upgrading an ICX switch



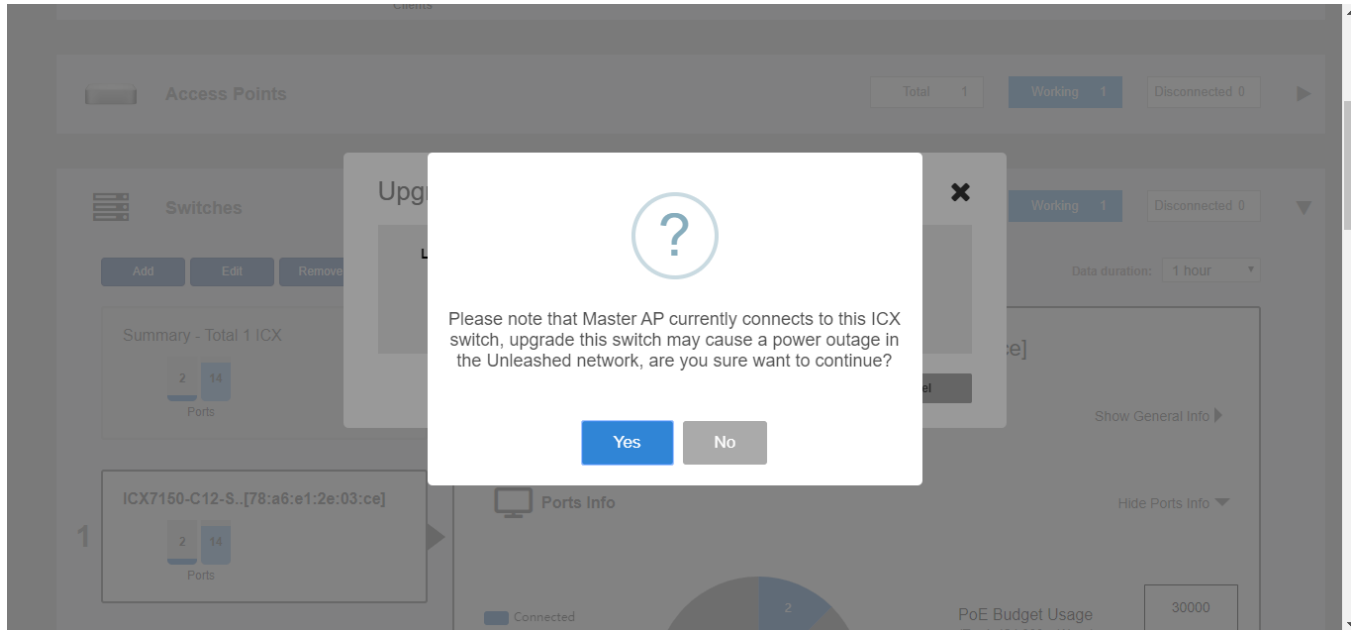
3. In the *Upgrade* dialog, click **Choose File** and select a valid FastIron image file.

**FIGURE 189** Choose upgrade image file



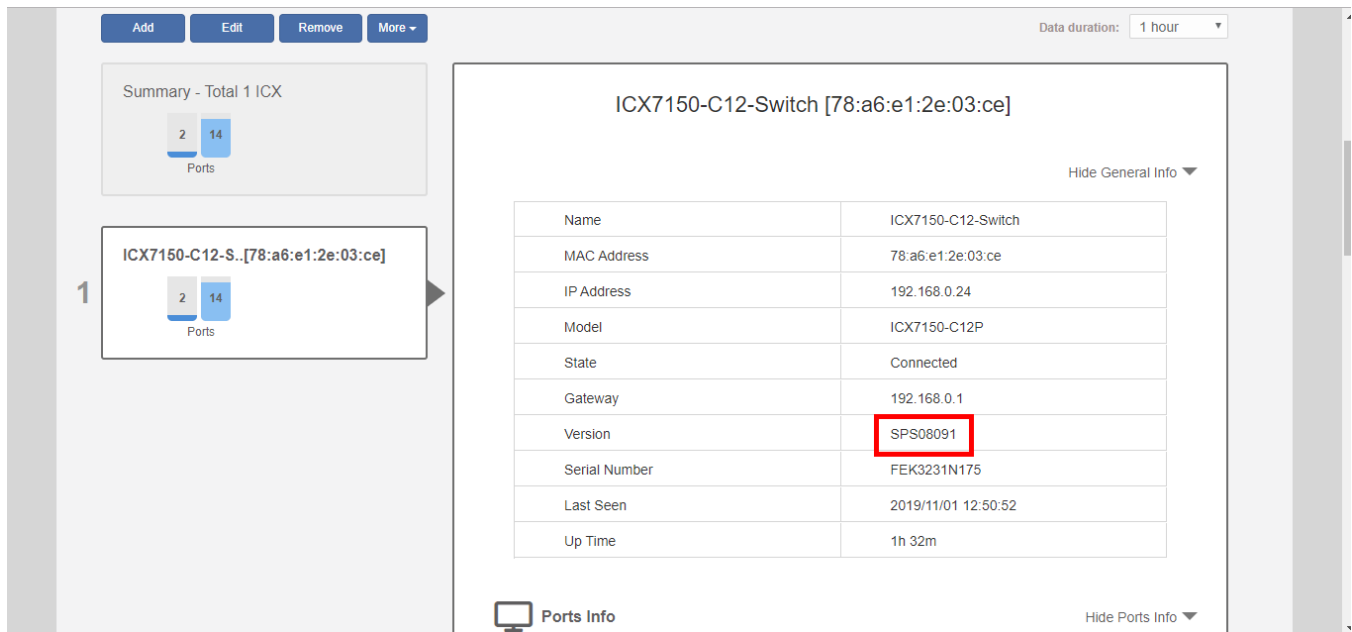
- Click **Upgrade**. A warning message appears notifying you that the upgrade will cause a power outage to your Unleashed APs. Click **Yes** to continue.

**FIGURE 190** Upgrade warning message



- When the upgrade is complete, Unleashed reboots and displays the switch in the connected device list.
- Verify the new firmware version from the **Show General Info** display.

**FIGURE 191** Verify switch version





# Working with Clients

- Client Management Overview..... 253
- Viewing the Clients List..... 253
- Renaming a Client..... 255
- Deleting a Client..... 257
- Permanently Blocking a Client Device..... 257
- Marking a Client as a Favorite..... 258
- Running a SpeedFlex Performance Test on a Wireless Client..... 259
- Client Connection Troubleshooting..... 263
- Adding User Accounts to the Internal User Database..... 265
- Authenticating Clients Using an External Database..... 265

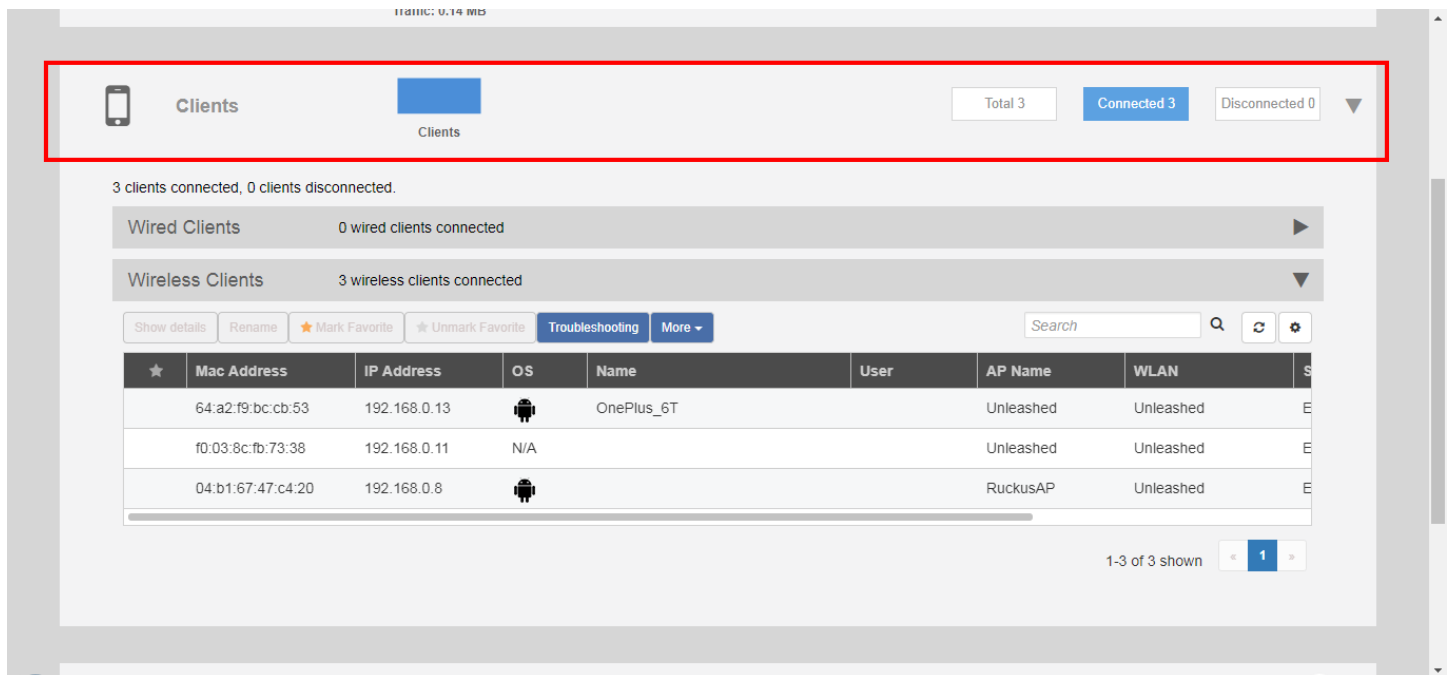
## Client Management Overview

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 192** Viewing the currently connected Clients list



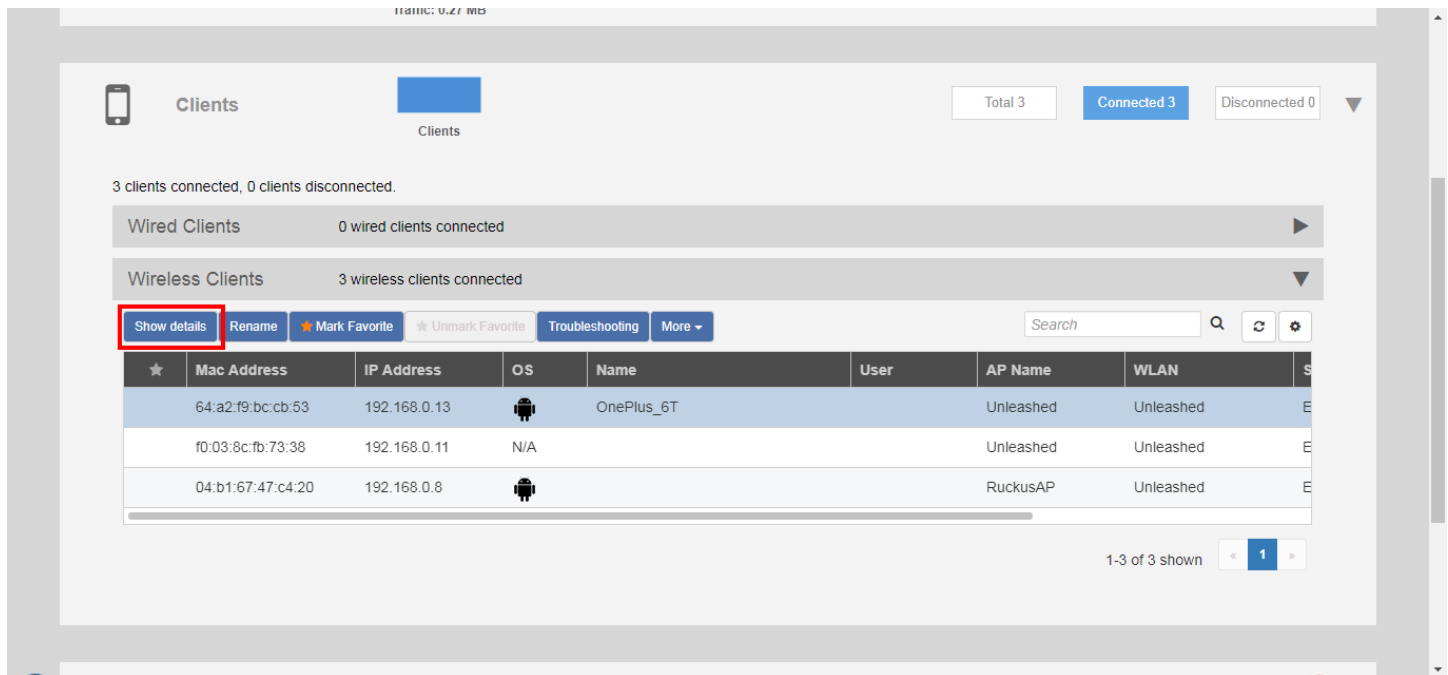
## Working with Clients

### Viewing the Clients List

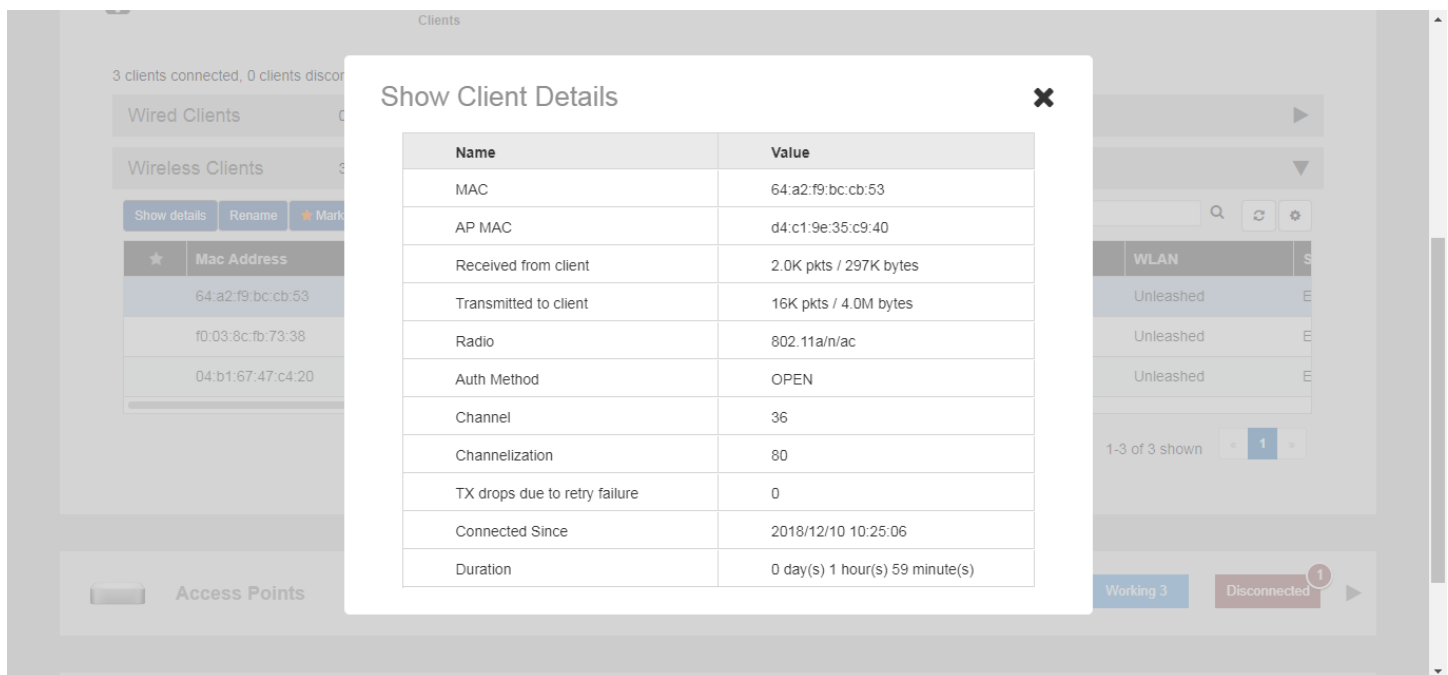
The clients list displays the number of connected and blocked clients, along with a table that lists the details on the client such as its MAC address, IP address, OS, Hostname, User, connected AP, WLAN, and Signal level indicator.

To view additional details about a specific client, select the client from the list and click **Show Details**.

**FIGURE 193** Click Show Details to view client details



**FIGURE 194** 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.

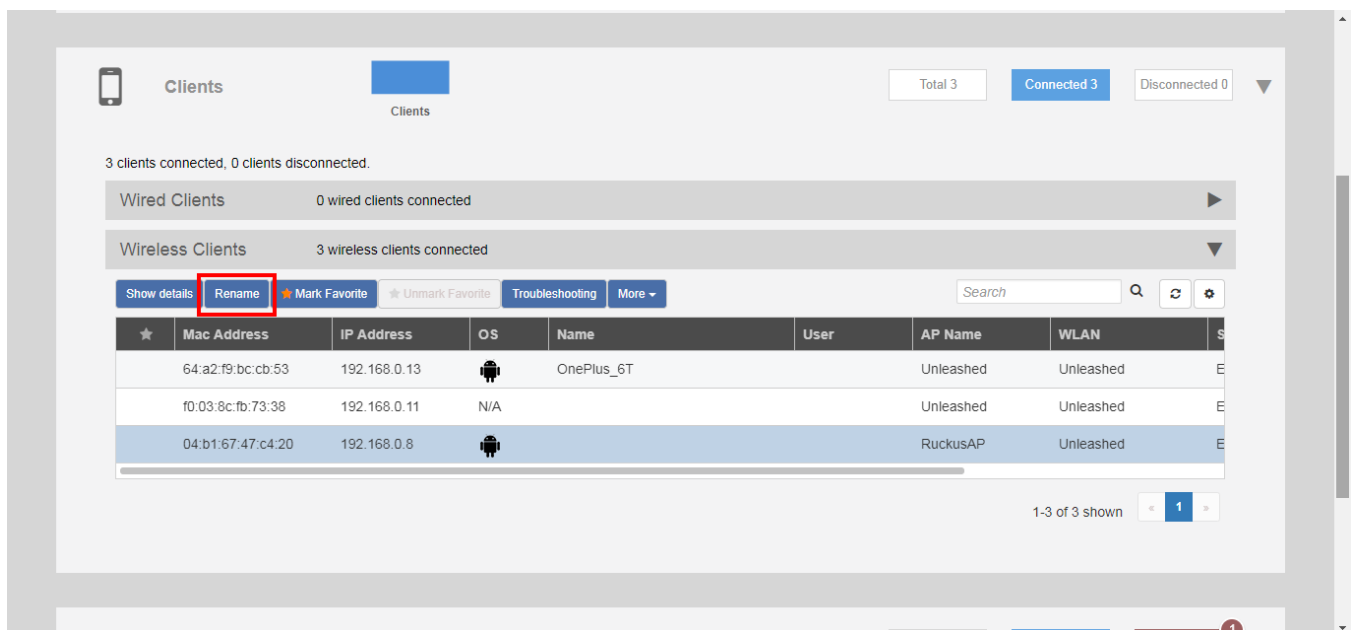
Entering a custom host name manually via the web interface is one way to address this issue.

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**.

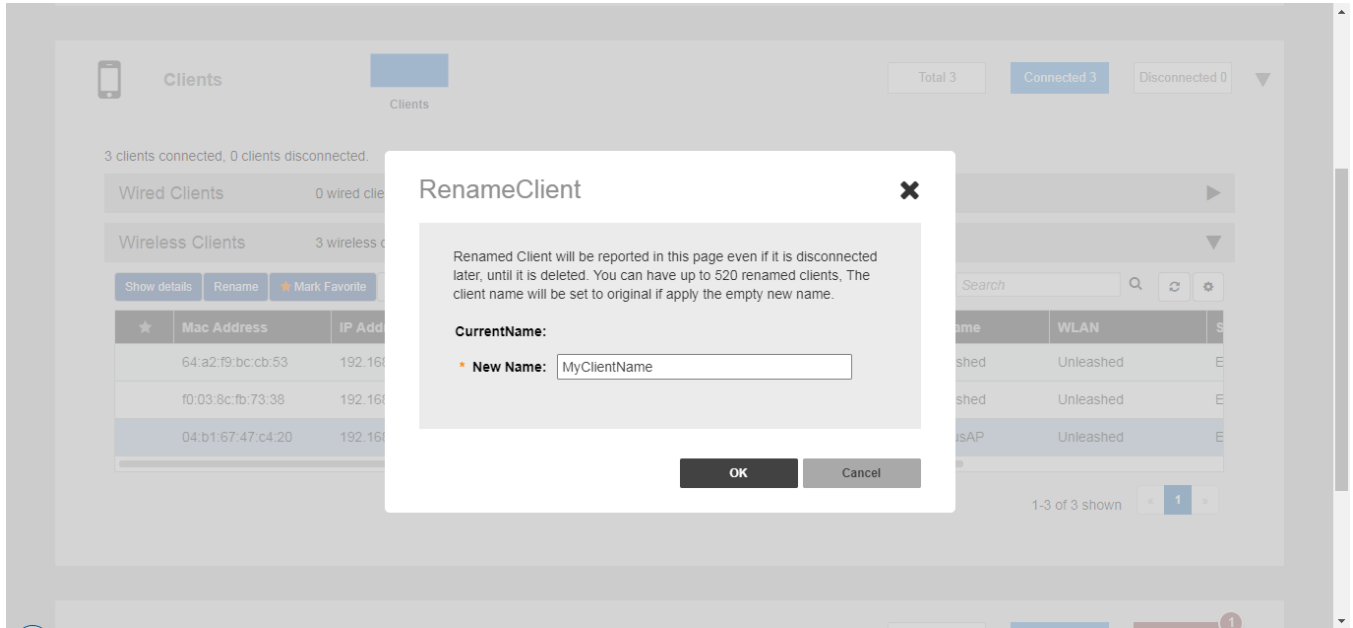
**FIGURE 195** Rename a client



The *Rename Client* dialog appears.

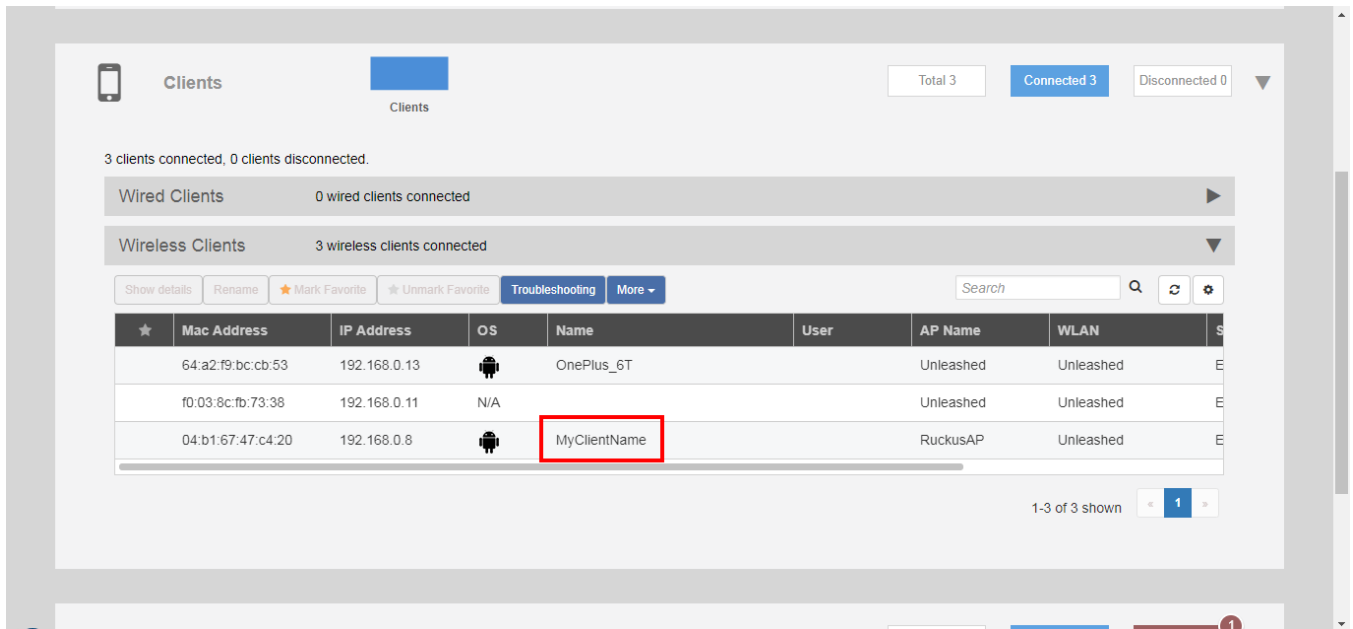
3. Enter the **New Name**, and click **OK**.

**FIGURE 196** Enter new client name



4. The new client name now appears in clients lists in the *Host Name* column.

**FIGURE 197** New name appears in Host Name



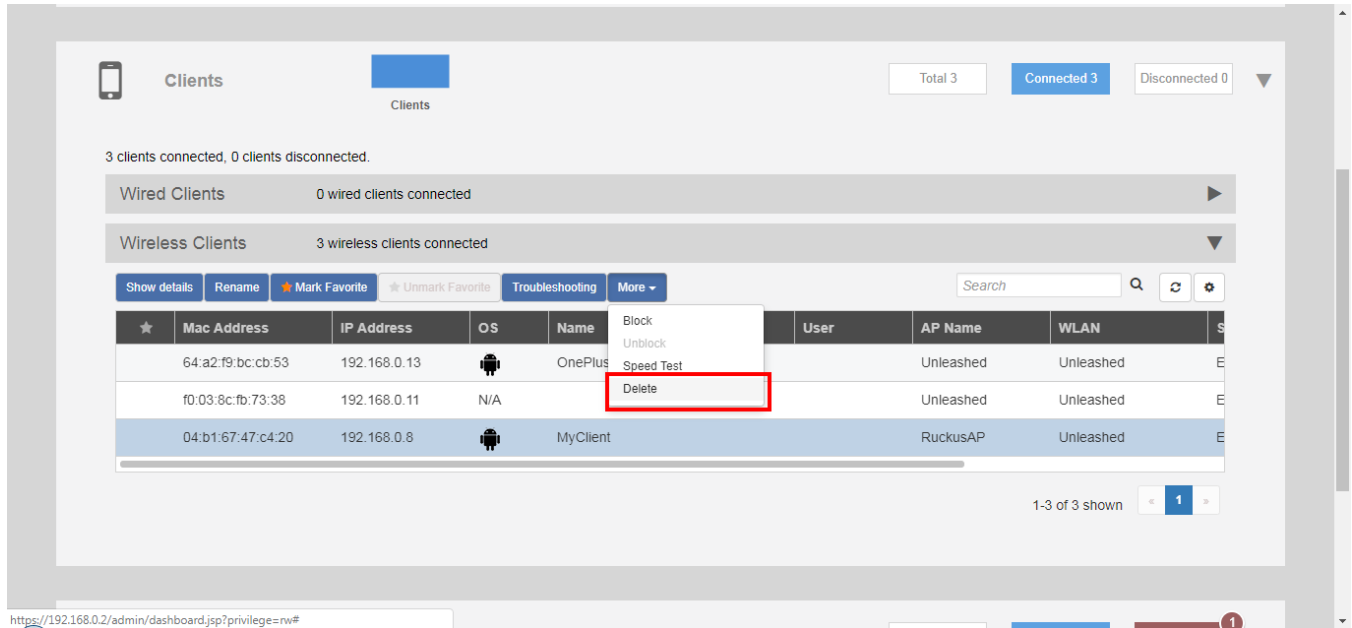


## Deleting a Client

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 198** 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 257.

## Permanently Blocking a Client Device

Follow these steps to permanently block a client device from WLAN connections.

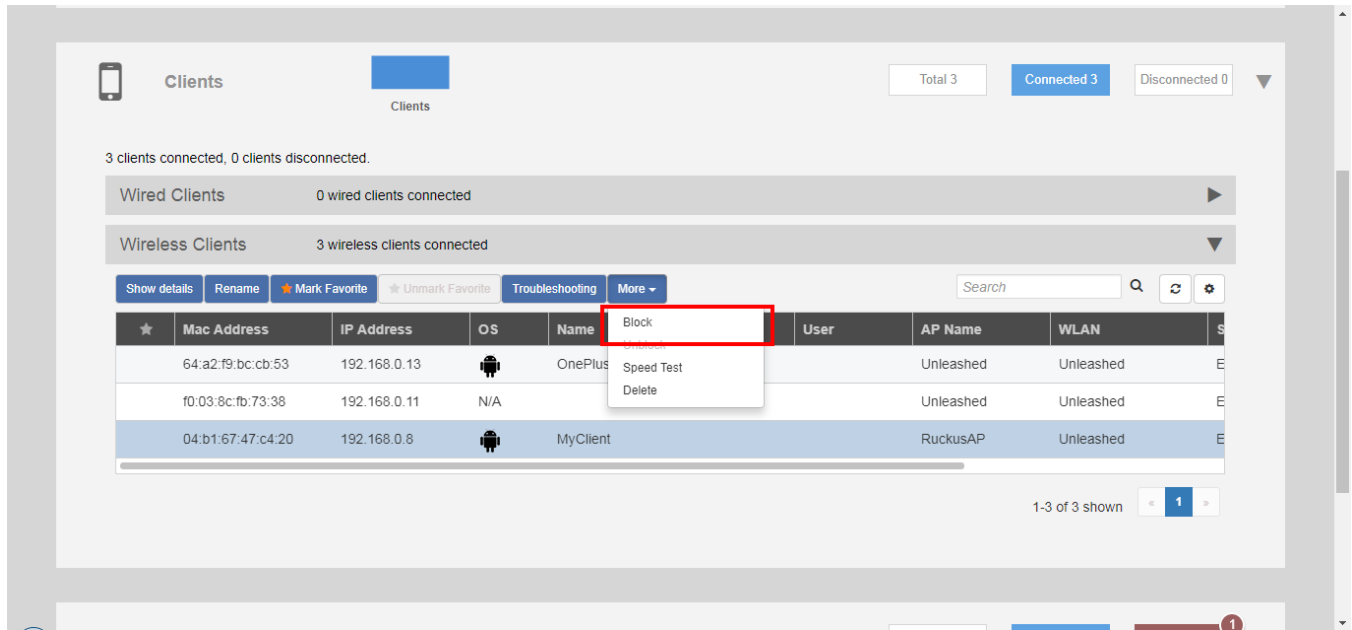
1. Look at the *Status* column to identify any unauthorized users.

## Working with Clients

### Marking a Client as a Favorite

2. 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 199** Block a client to permanently prevent it from joining your network(s)



3. The status is changed to *Blocked*. This will prevent 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

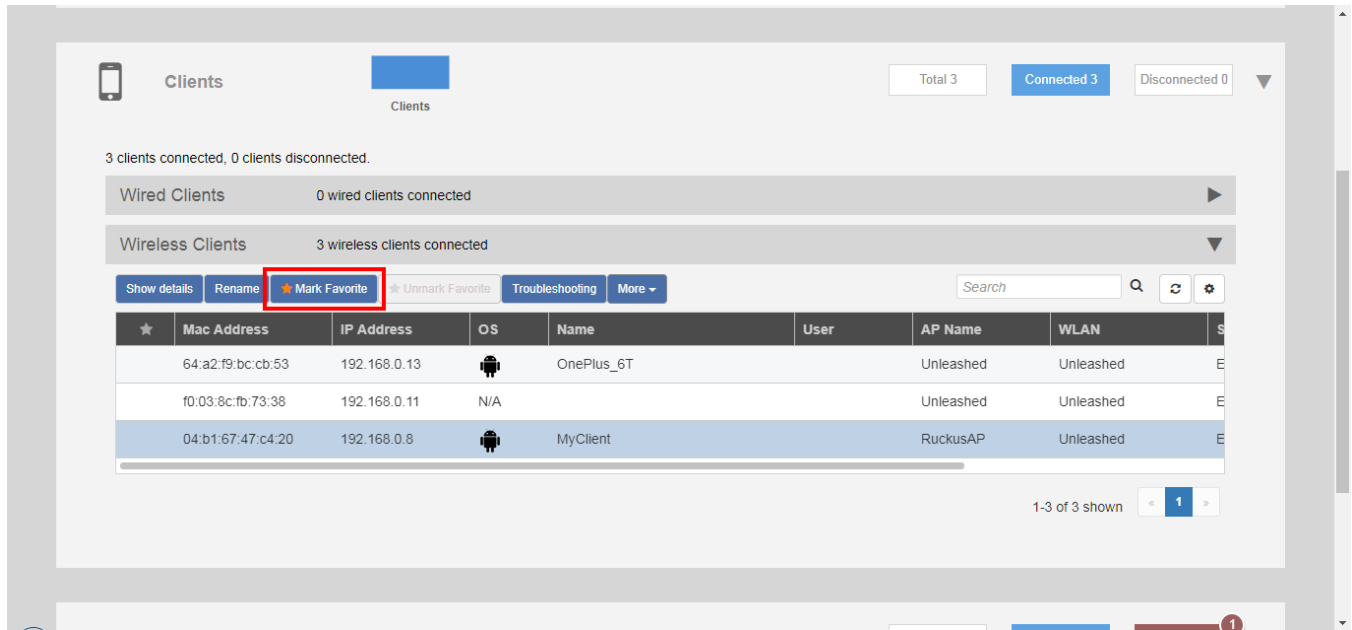
Unleashed supports a maximum of 20 favorite clients.

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 200** 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.

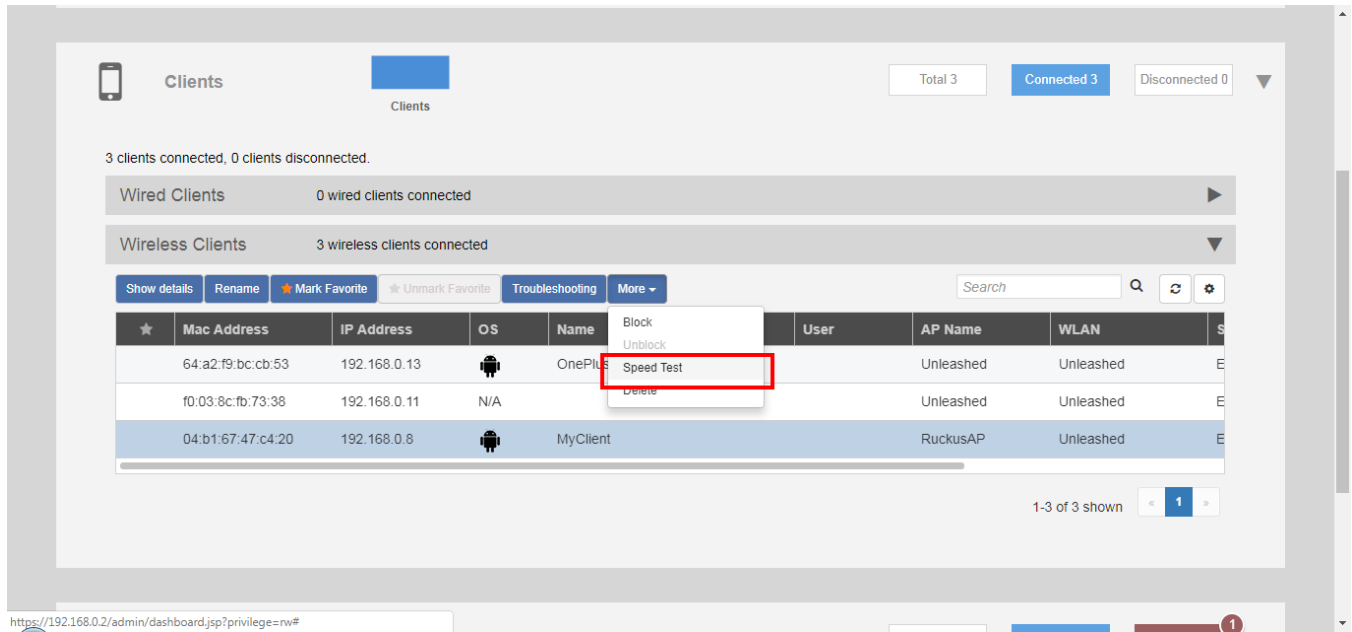
1. Expand the **Clients** menu.

## Working with Clients

### Running a SpeedFlex Performance Test on a Wireless Client

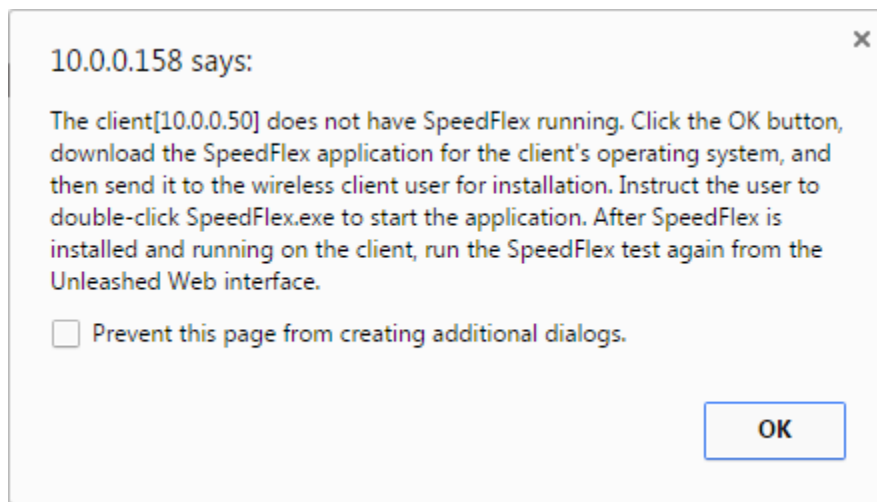
2. Select a client device from the list and click **Speed Test** from the **More** pull-down menu.

**FIGURE 201** Select a client and click Speed Test

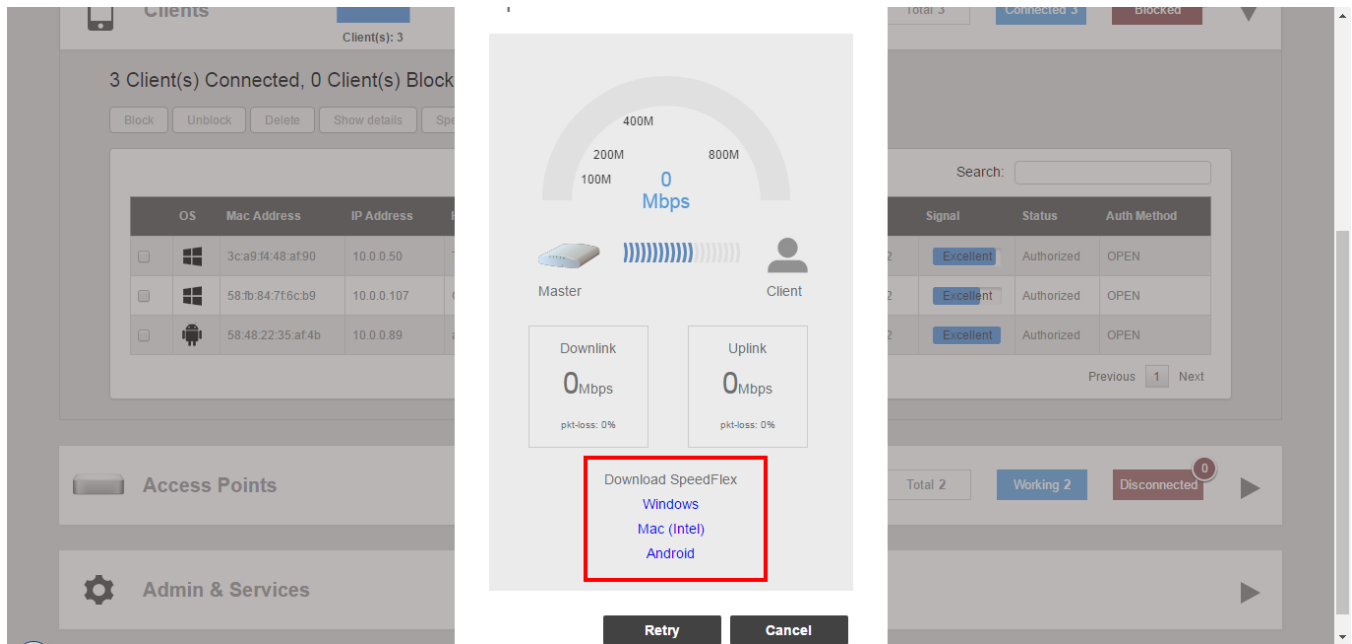


3. A Speed Test dialog appears. Click **Start** to begin.
4. If the SpeedFlex application is not already running on the client, follow the instructions to install and run the application on your client device.

**FIGURE 202** The client does not have SpeedFlex running



- Download the SpeedFlex application for your Operating System. Choices are:
  - Windows
  - Mac (Intel)
  - Android

**FIGURE 203** Download SpeedFlex

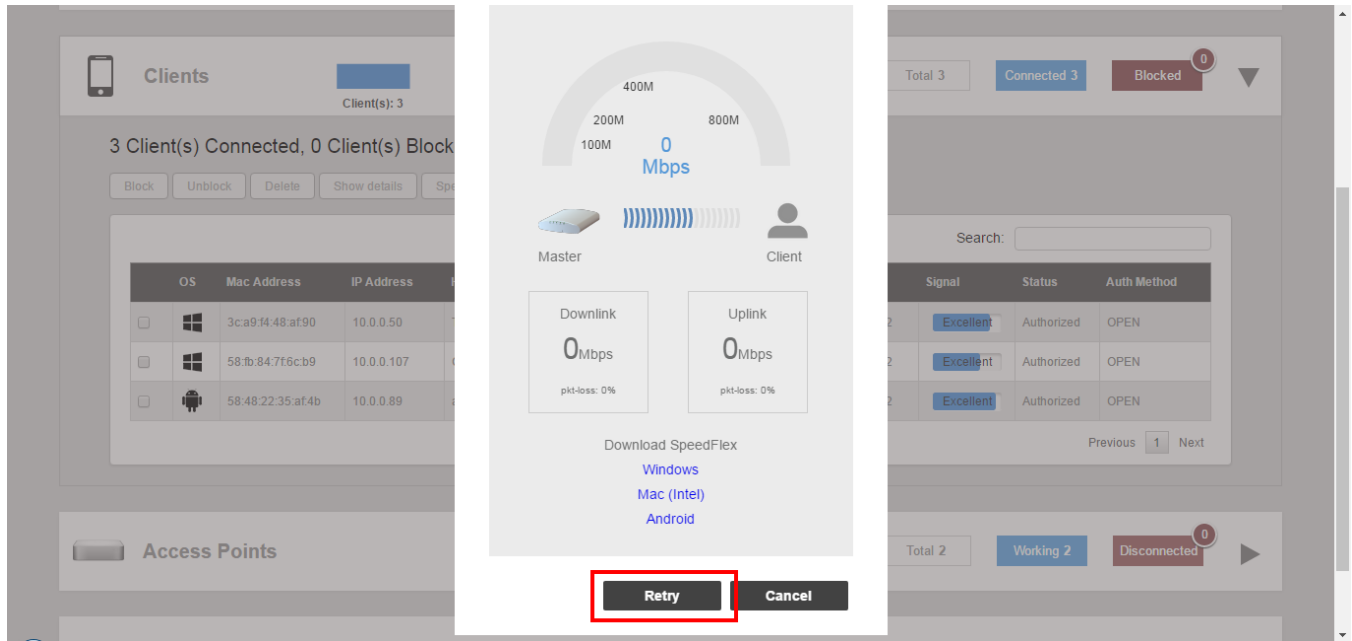
- Install and run the application.

## Working with Clients

Running a SpeedFlex Performance Test on a Wireless Client

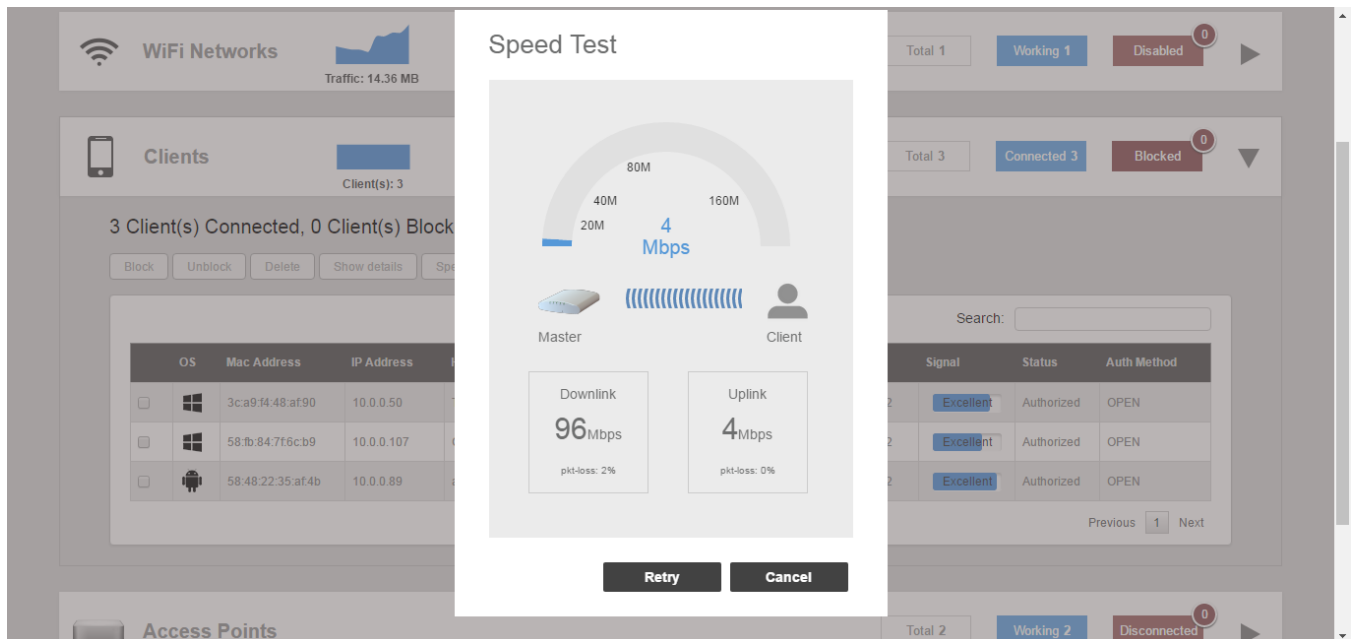
7. With the application running, click **Retry**.

**FIGURE 204** Click Retry



8. When the test is complete, the average Downlink and Uplink speed results are displayed along with packet loss percentages.

**FIGURE 205** 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.

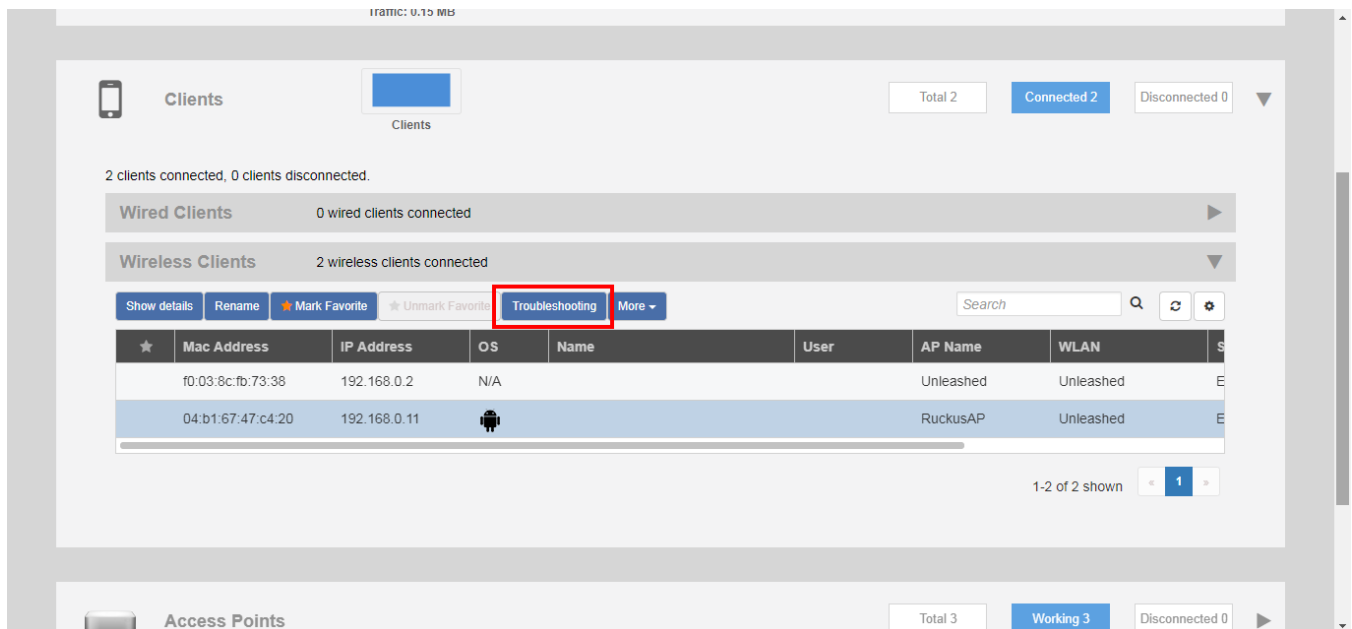
**NOTE**

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**.

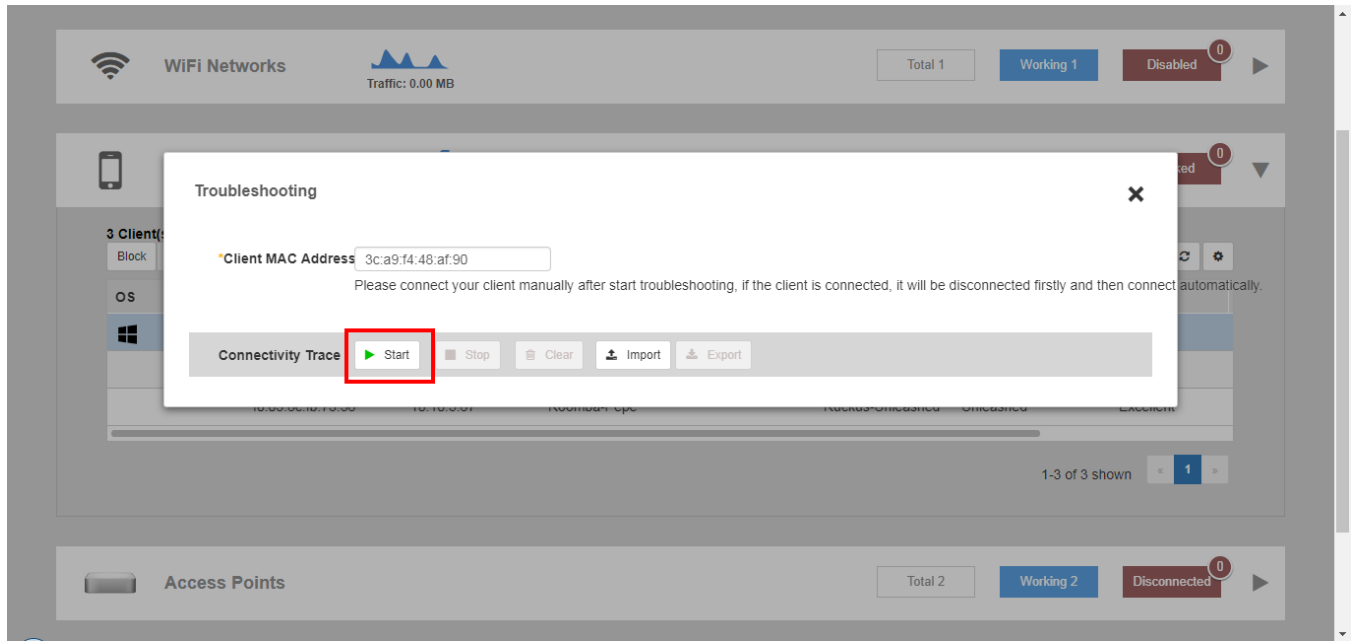
**FIGURE 206** Click Troubleshooting to perform client connectivity trace



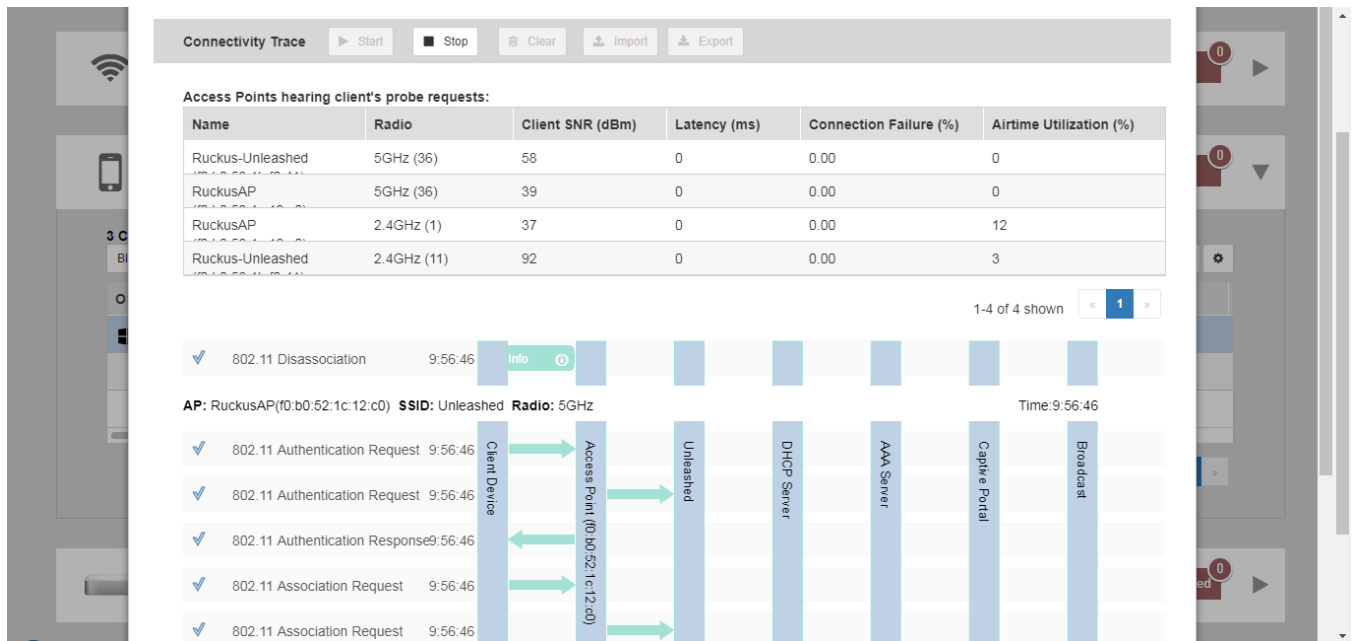
The *Troubleshooting* screen appears.

- In *Connectivity Trace*, click the **Start** button to begin. The association trace begins. The page refreshes to display detailed results.

**FIGURE 207** Click Start to begin connectivity trace



**FIGURE 208** Connectivity trace in progress



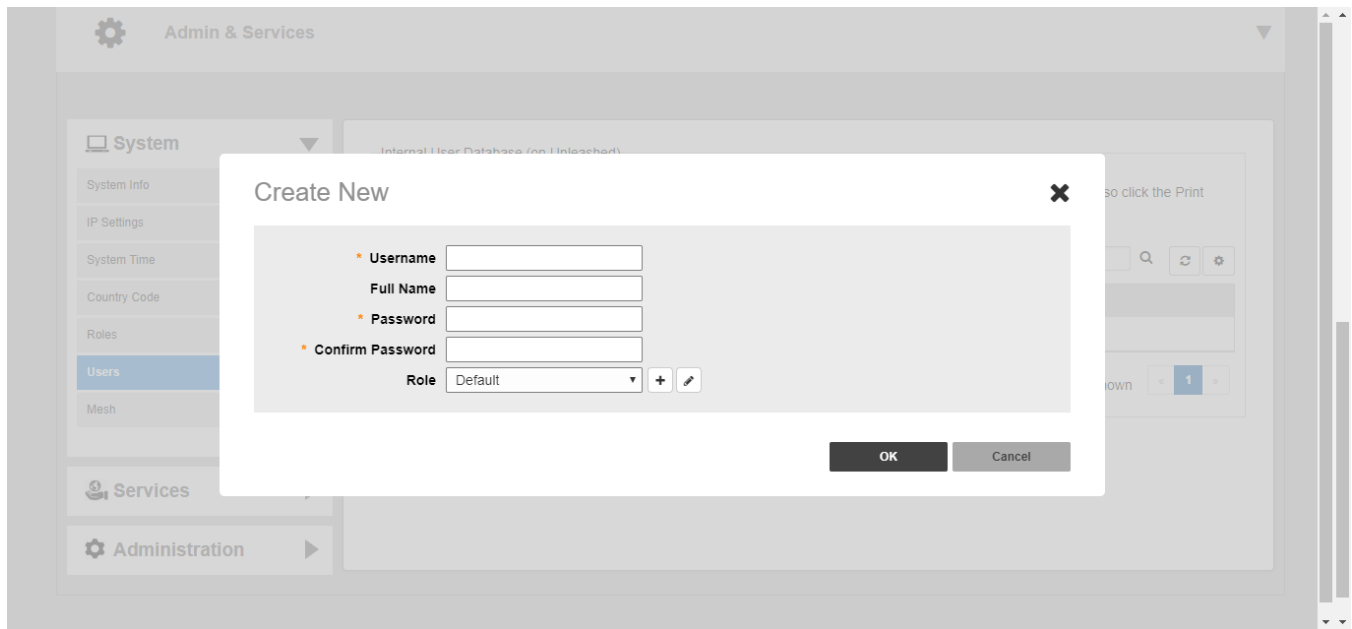
- Examine the results to isolate the problematic step in the process.
- If needed, you can download the client connectivity data to a file, which can later be imported for analysis. Click **Export** to download the data file and save it to your local computer. Click **Import** to import a previously exported file back into Unleashed.



## 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 209** 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 304.



# Configuring Admin & Services Settings

---

- [Admin & Services Overview](#)..... 267
- [System Settings](#).....267
- [Services](#)..... 303
- [Administration Settings](#)..... 348

## 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:

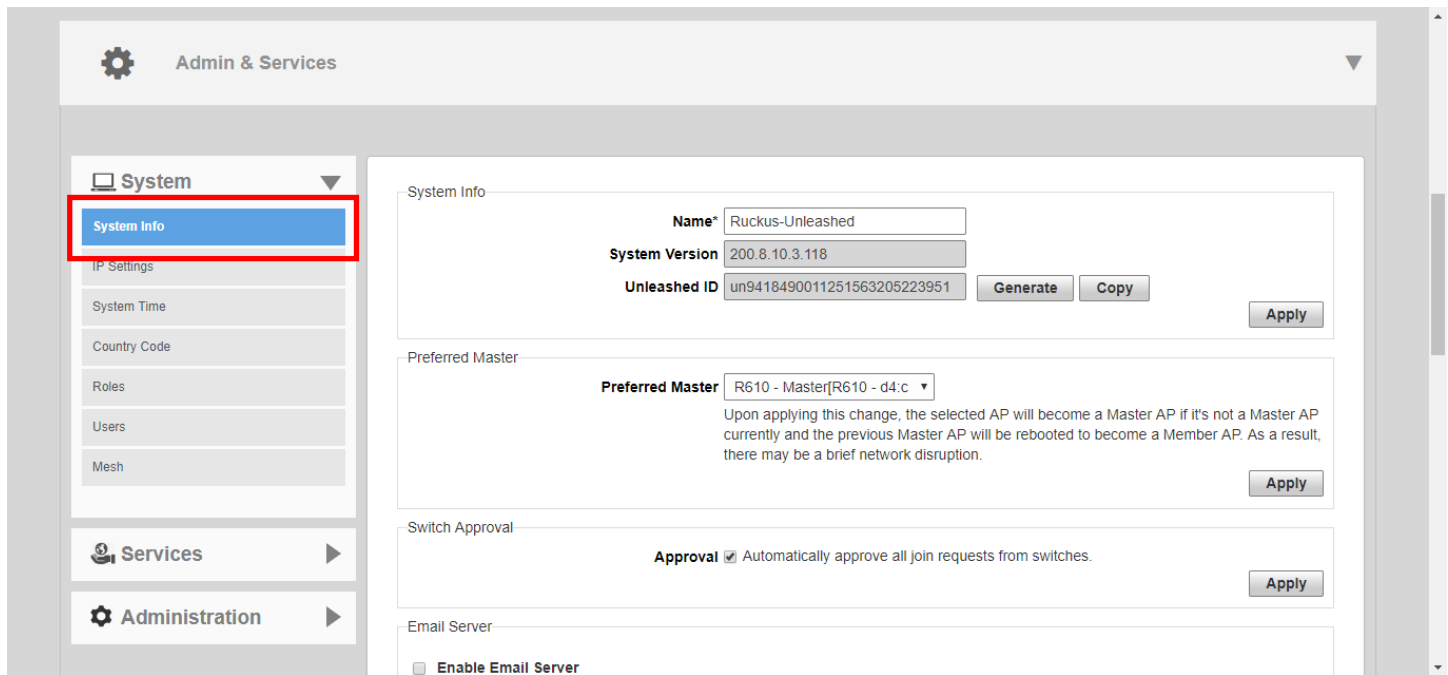
- [System Settings](#) on page 267
- [Services](#) on page 303
- [Administration Settings](#) on page 348

## 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 210** 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

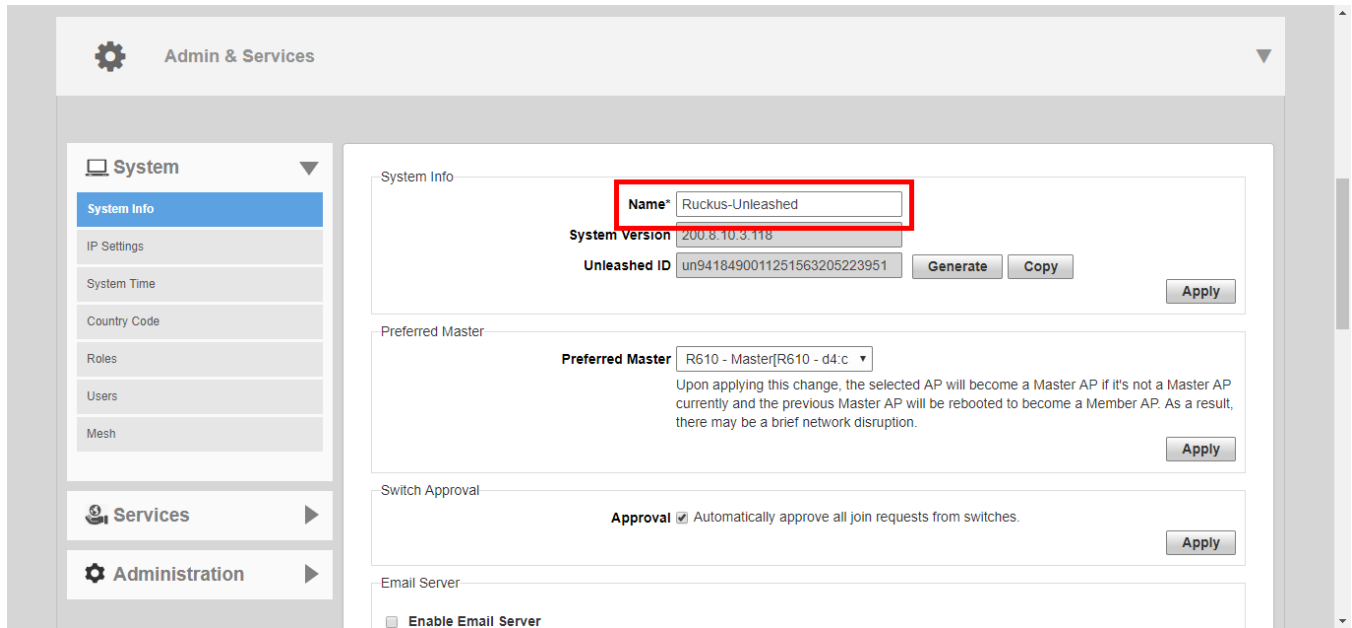
The **System Info** page displays the current system firmware version and provides an option to reconfigure the system name.

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 211** The System Info page displays the firmware version and system name



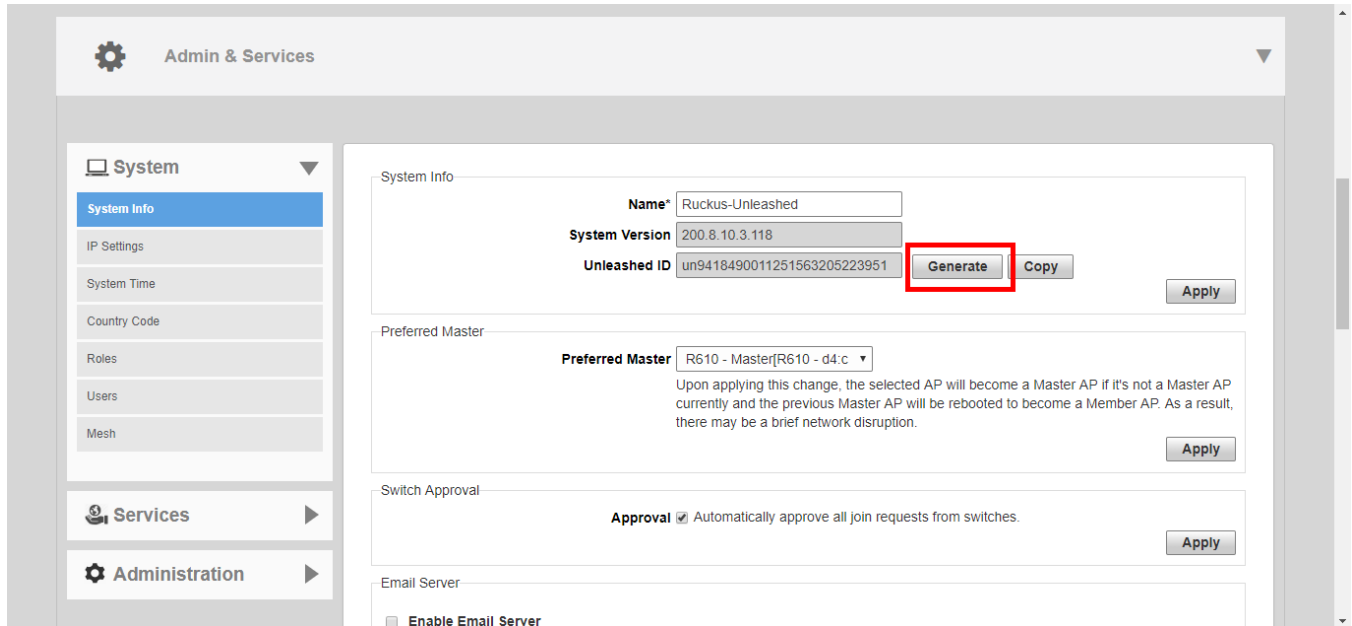
### Generating an Unleashed ID

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 212** Generating a new Unleashed ID for use in remote management



### Designating a Preferred Master AP

Designating an AP as the Preferred Master allows one Unleashed AP to be the default Master AP, while other member APs remain on standby ready to take over if the Master AP is offline.

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 option, users can configure one of the APs to have priority. 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.

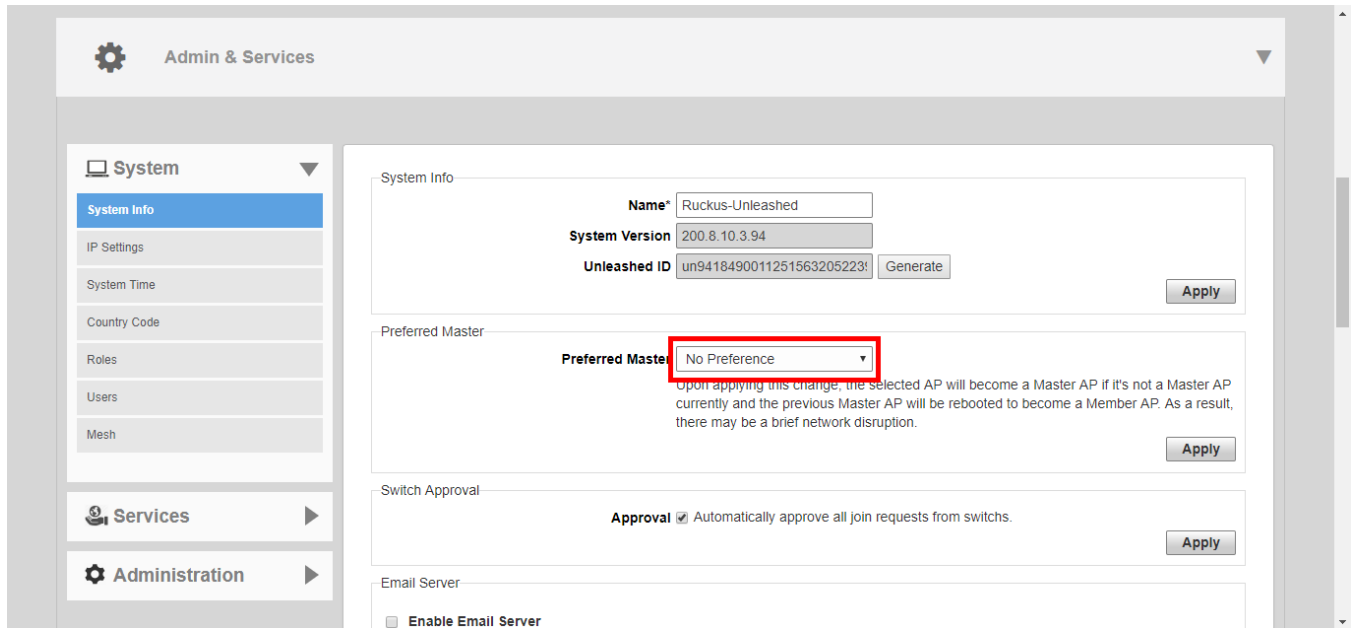
Any (non-mesh) AP can become the Master if the preferred Master is offline, but when the Preferred Master comes back online, it will assume the Master role again.

To configure an AP as the Preferred Master AP:

1. Go to **Admin & Services > System > System Info** and locate the **Preferred Master** option.

2. Select an AP from the list and click **Apply**.

**FIGURE 213** Designate an AP as the Preferred Master



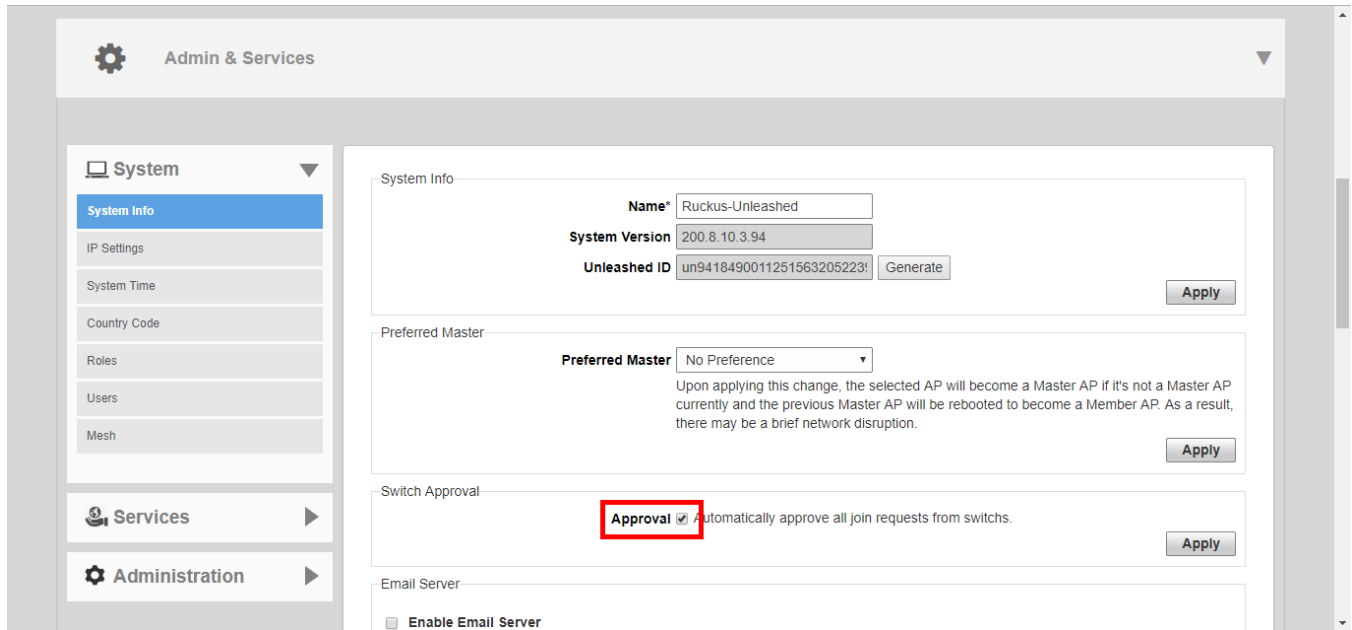
### Enabling Automatic Switch Approval

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 214** 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 215** 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 216** Configuring SMS settings

SMTP Encryption Options

Test Apply

SMS Settings

Enable SMS Server

Country Code

No default and ask user to input

Use default +12 and allow user to change

Use default +12 and disallow user to change

Twilio account information

Account SID  [register a new Twilio account]

Auth Token

From PhoneNumber

Clickatell account information

User Name  [register a new Clickatell account]

Password

API Id

From PhoneNumber

Customized Server

Method

URL

## 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 need to update the IP address and DNS server settings of your Unleashed Master AP, follow the steps outlined below.

#### NOTE

As soon as the IP address has been changed (applied), you will be disconnected from your web interface connection to the Unleashed Master AP. You can log into the web interface again by using the new IP address in your web browser.

To change the IP address settings:

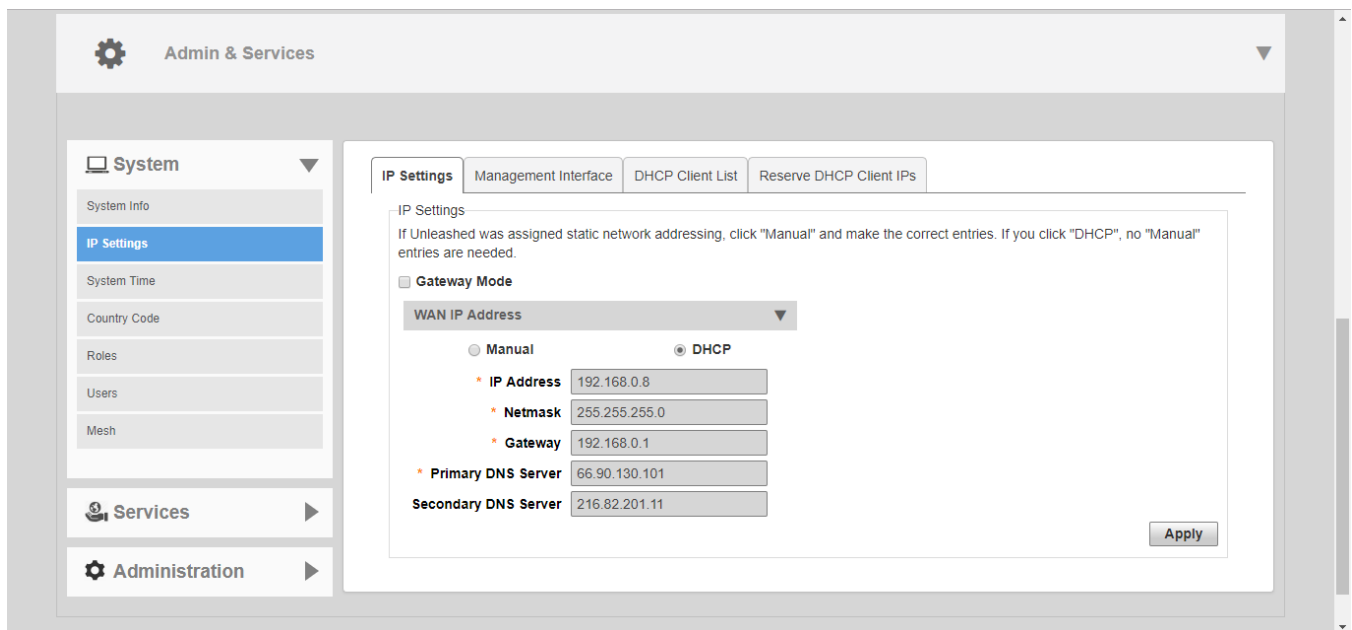
1. Go to **Admin & Services > System > IP Settings**.
2. Review the **IP Settings** options.

#### NOTE

Upon enabling Gateway mode, all devices will reboot immediately. See [Gateway Mode](#) on page 275.

3. Select one of the following:
  - **Manual:** If you select Manual, enter the correct information in the now-active fields (IP Address, Netmask, and Gateway are required).
  - **DHCP:** If you select DHCP, no further information is required. The Unleashed Master will obtain an IP address automatically.
4. Click **Apply** to save your settings. You will lose connection to the Unleashed Master.
5. To log back into the web interface, use the newly assigned IP address in your web browser or use the UPnP application to rediscover the Unleashed Master AP.

**FIGURE 217** Configuring device IP address settings



## Gateway Mode

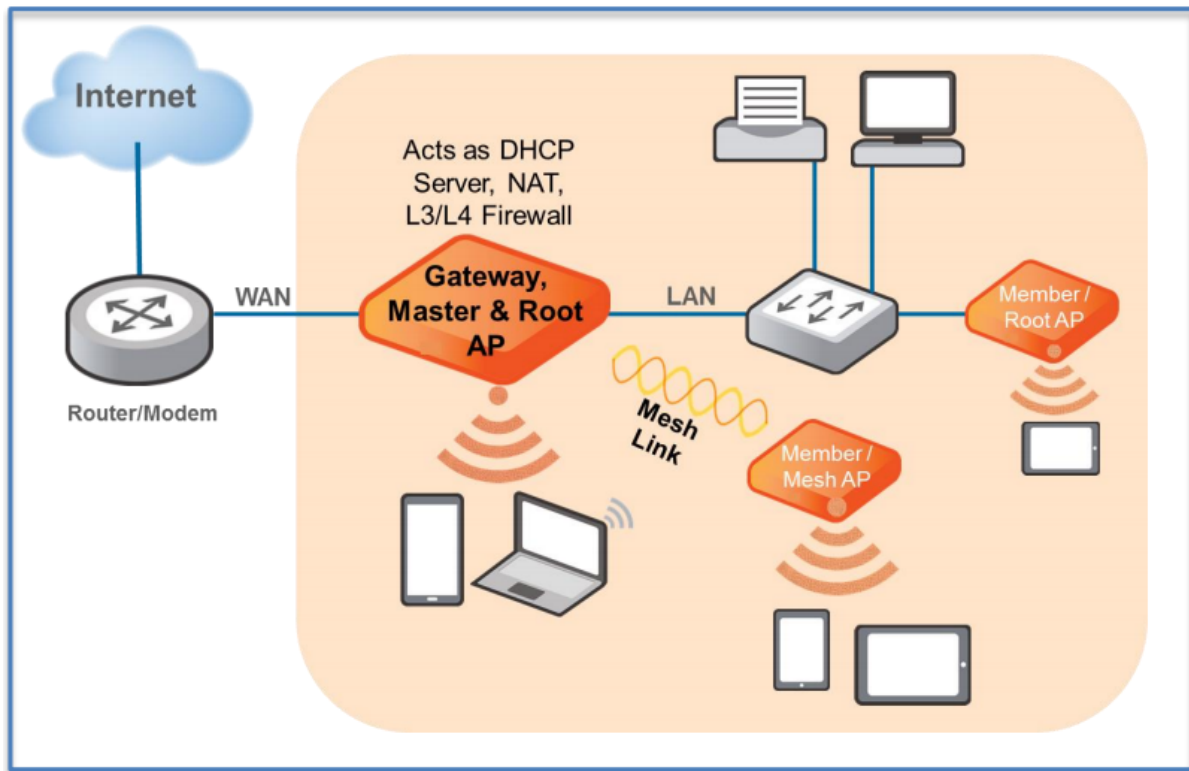
An Unleashed AP must have at least two Ethernet ports to support Gateway mode.

Gateway mode provides a solution for SMB customers who need to provide private IP addresses for clients and do not have an existing gateway router, or who connect to their ISP over PPPoE. Enable Gateway mode to provide Network Address Translation (NAT) and DHCP functionality to assign private IP addresses to member APs and clients.

### NOTE

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.

FIGURE 218 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 new Master AP's web UI to configure it manually.

### Configuring Gateway Mode

The Unleashed Master AP can be configured to serve as a gateway router.

To configure the Unleashed Master AP as a Gateway:

1. Go to *Admin & Services > System > IP Settings*.
2. Enable the **Gateway Mode** option and configure the WAN and LAN IP address settings as follows.

#### NOTE

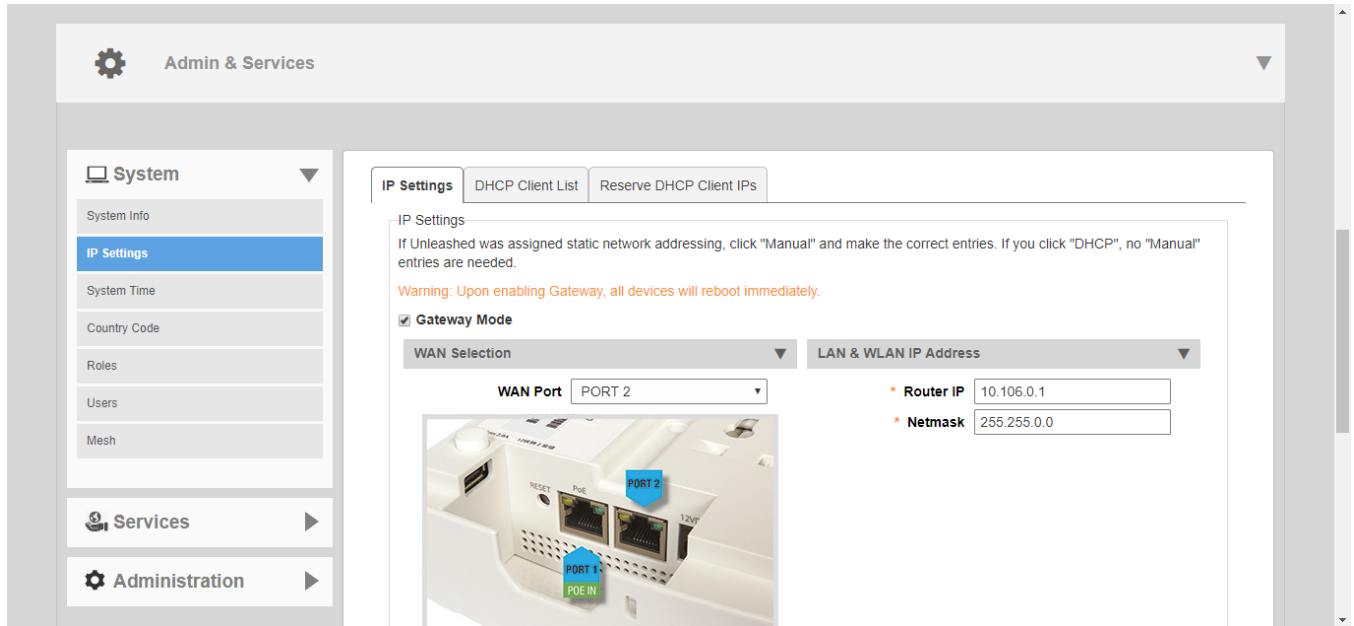
Alternatively, in factory default state, connect to the Unleashed Master AP and perform the initial setup as described in [Step 2b: Setup Using a Web Browser](#) on page 85. On the second wizard screen (**Management IP**) select **Enabled** in **Gateway Mode**.

3. Designate which port will be the WAN (uplink) port. The Gateway AP must have at least two Ethernet ports. Use the AP illustration below to identify which port is LAN1 and LAN2 on the AP, and select the relevant port from the **WAN Port** list.

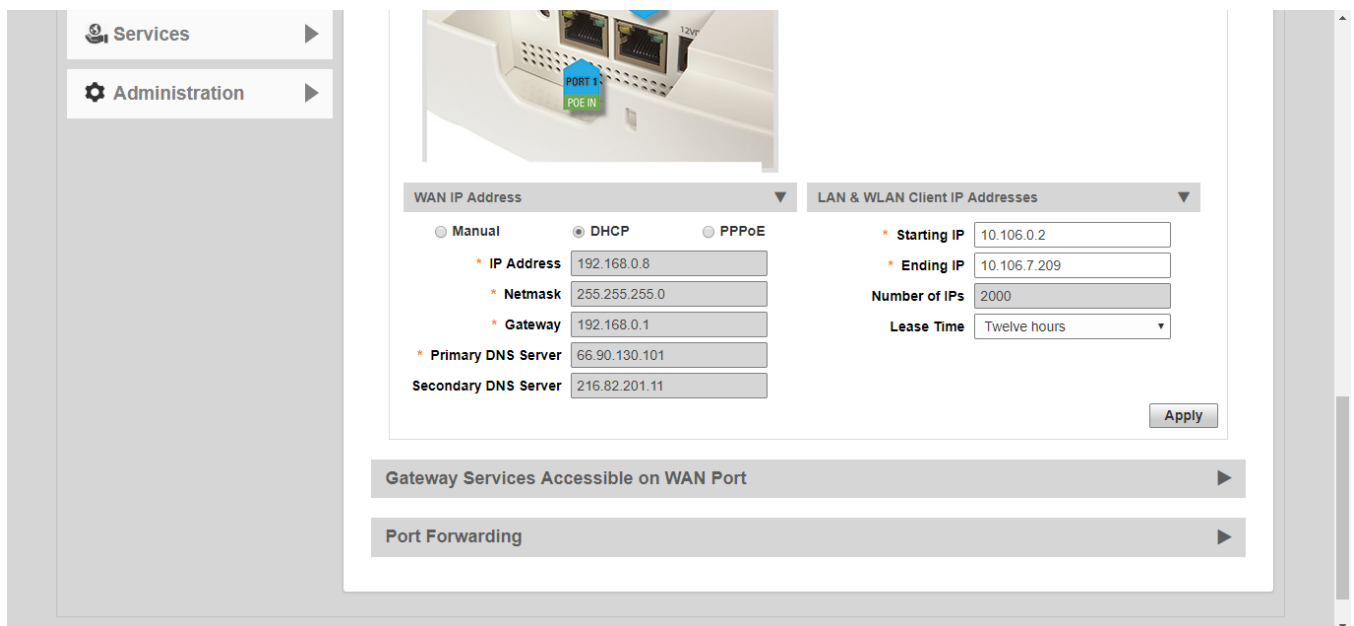
4. Configure how the WAN (uplink) port obtains its IP address:
  - **Dynamic (DHCP):** When Dynamic is selected, the WAN port is assigned an IP address automatically.
  - **Static (Manual):** When Static is selected, enter an **IP Address**, **Netmask** and **Gateway** address in the required fields, and optionally enter primary/secondary DNS server addresses.
  - **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 Port IP:** Enter the IP address for the LAN port.
  - **LAN Port Netmask:** Enter the Netmask.
  - **Starting IP:** Enter the first IP address 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.

6. Click **Next**, and continue to complete the setup wizard. 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.

**FIGURE 219** Enable gateway mode



**FIGURE 220** Configure WAN and LAN/WLAN IP addresses



### **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**

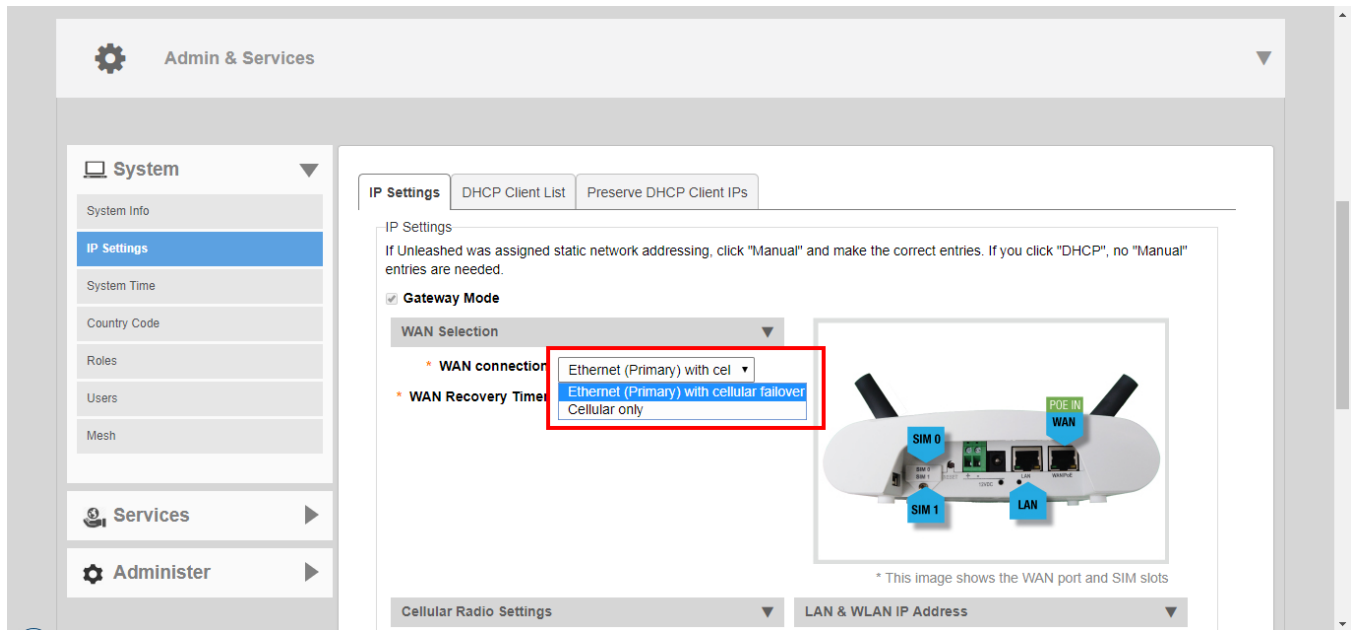
The Unleashed M510 provides additional options for configuring the LTE uplink mode.

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 221 Select WAN uplink connection mode

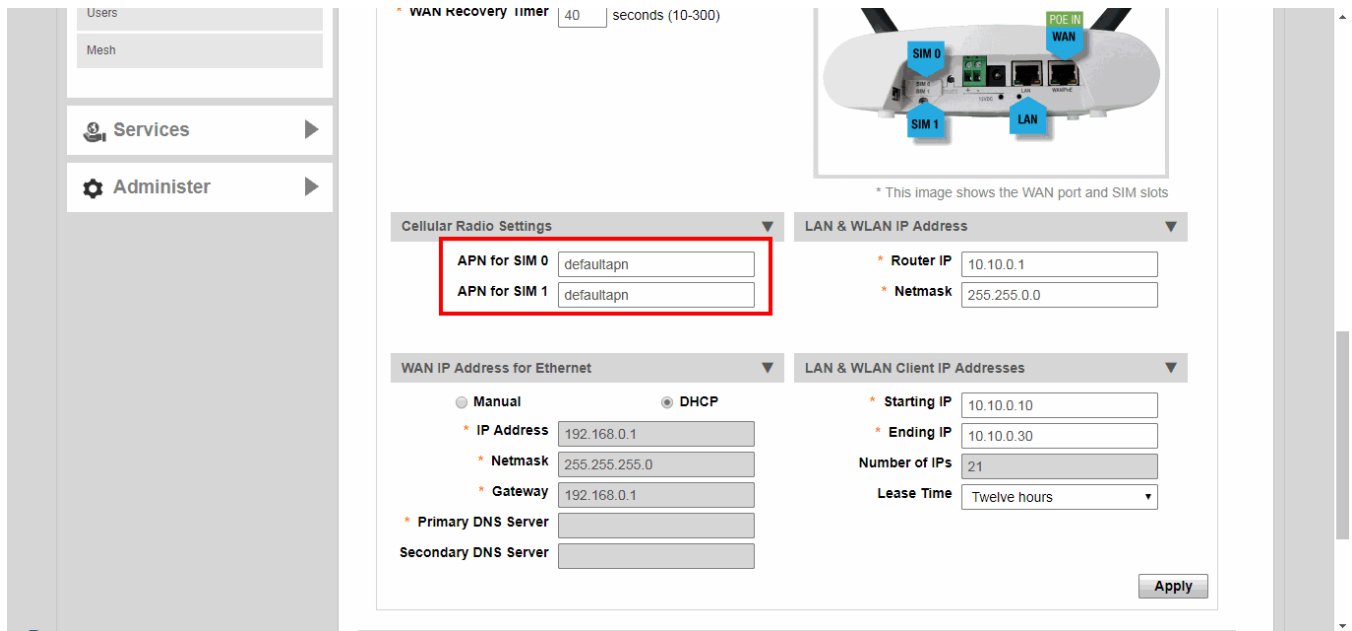


3. In **WAN Recovery Timer**, enter a value in seconds after which failover to LTE uplink will occur.
4. In **Cellular Radio Settings**, enter the Access Point Name for each SIM card. The APN identifies the mobile network operator and the data network that the client intends to connect to.
5. If the *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.



- Configure internal WLAN and LAN IP address settings as described in *Configuring Device IP Address Settings*.

**FIGURE 222** M510 Cellular Radio Settings



## DHCP Server

Unleashed provides a built-in DHCP server that you can enable to assign IP addresses to devices that are connected to the 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 Unleashed Master AP must be assigned a manual (static) IP address. If you configured 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.

To configure the built-in DHCP server:

- Go to **Admin & Services > System > IP Settings**.
- In *WAN Address*, select **Manual**, and enter static IP settings (IP address, Netmask, Gateway and DNS settings) for the WAN IP address.
- In *LAN and WLAN Client IP Addresses*, enable the **DHCP Server** check box.
- In **Starting IP**, type 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 Unleashed Master AP. If the value that you typed is invalid, an error message appears and prompts you to let Unleashed automatically correct the value. Click **OK** to automatically correct the entry.
- In **Ending IP**, type 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 Unleashed Master AP. The default value is 200.
- In **Lease Time**, select a time period for which IP addresses will be allocated to DHCP clients. Options range from six hours to two weeks (default is one week).

7. Click **Apply**.

**NOTE**

If you typed an invalid value in any of the text boxes, an error message appears and prompts you to let Unleashed automatically correct the value. Click **OK** to change it to a correct value.

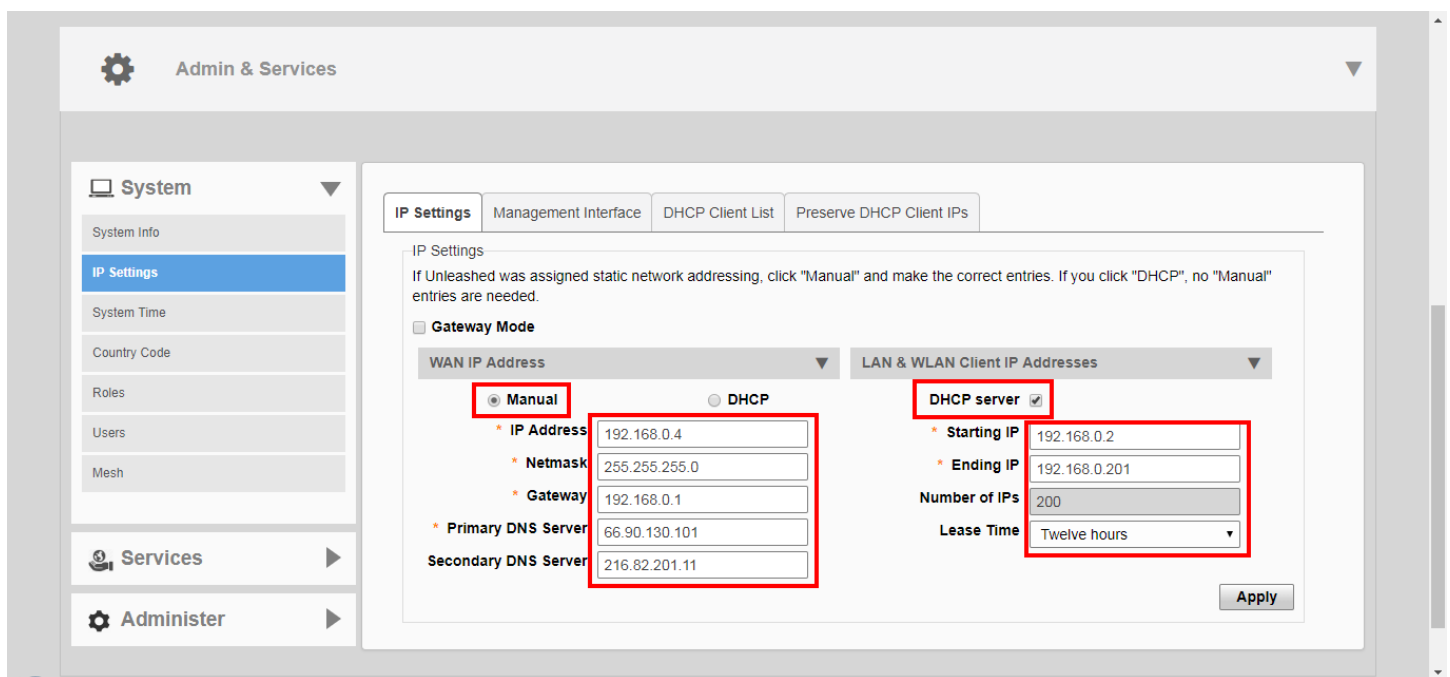
**NOTE**

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 DHCP server, Ruckus also recommends enabling rogue DHCP server detection. For more information, refer to [Rogue DHCP Server Detection](#) on page 341.

**NOTE**

Make sure the DHCP address pool is routable to the internet and non-overlapping with other devices. Because Unleashed in non-gateway mode does not support NAT (Network Address Translation), this is important to avoid IP address conflicts. For example, if your router uses the 192.168.0.x subnet, you should use any subnet *other* than 192.168.0.x for your Unleashed DHCP subnet.

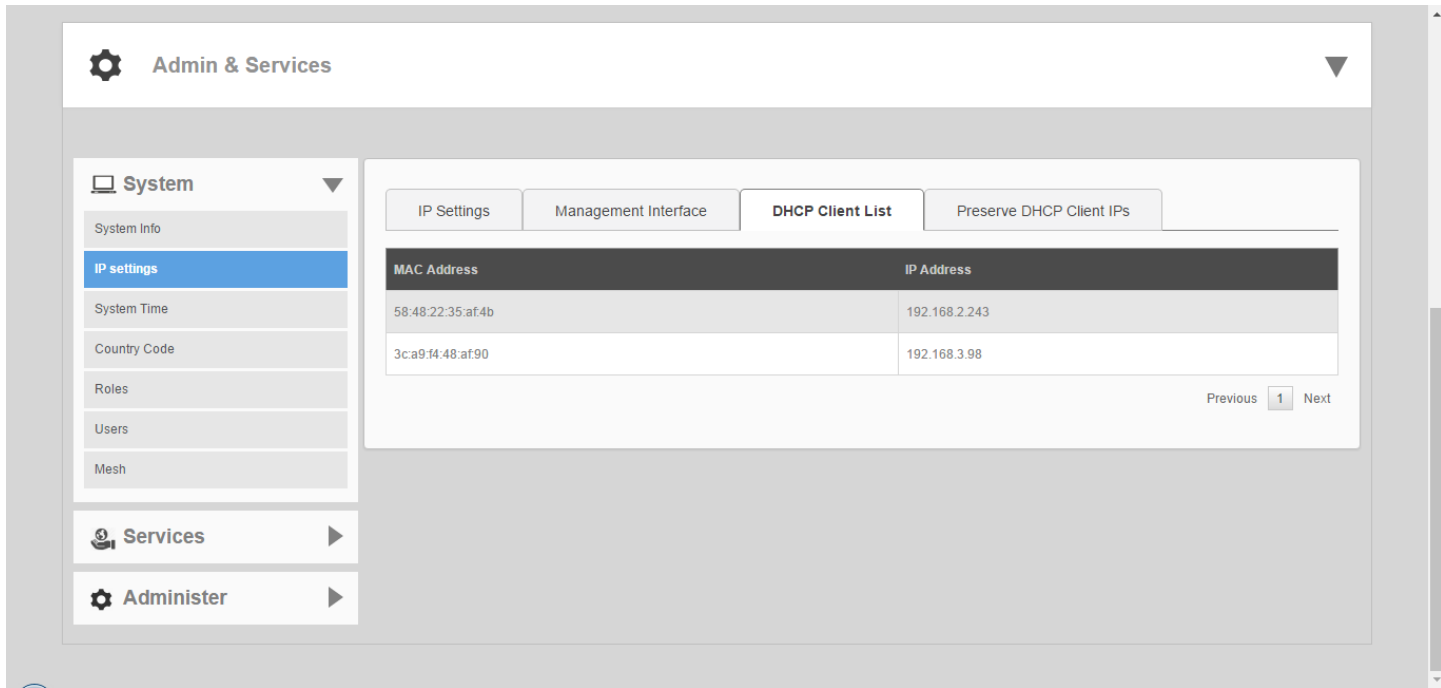
**FIGURE 223** DHCP Server configuration



**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 224 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 225 Create New Reserved IP Address

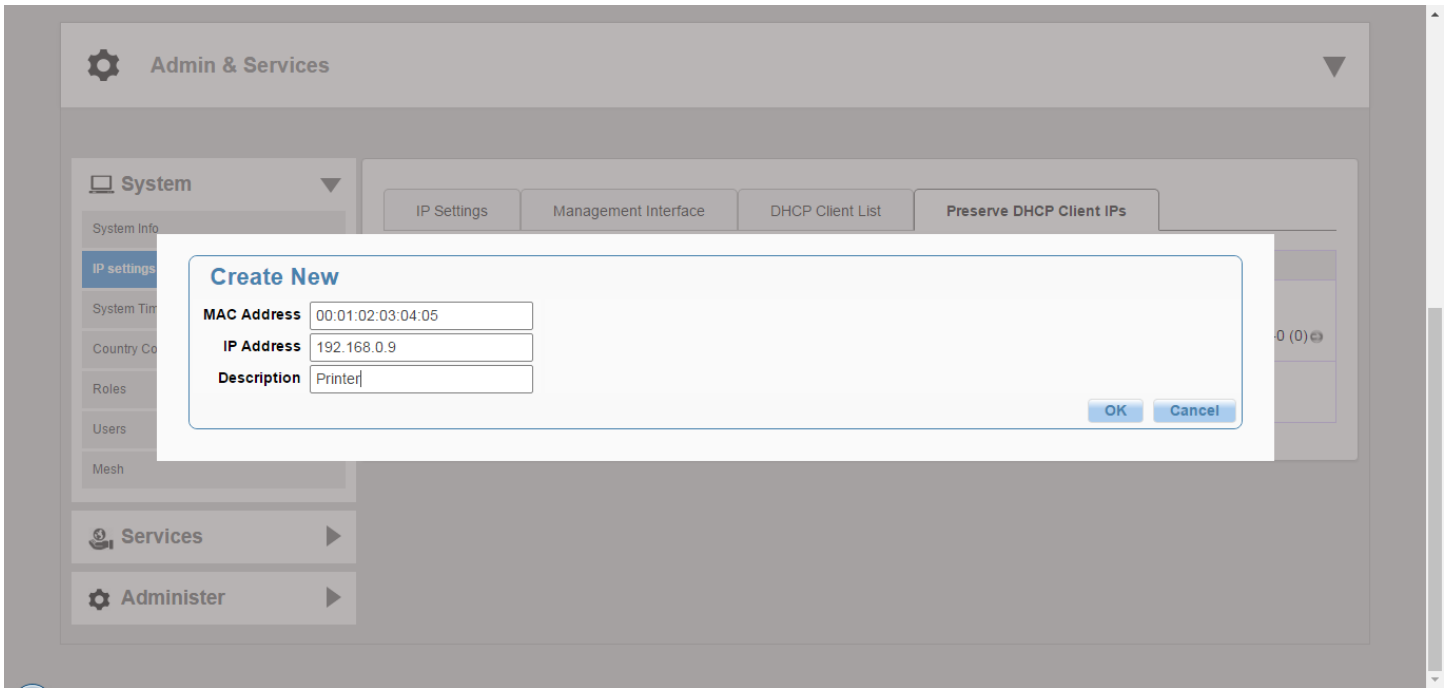
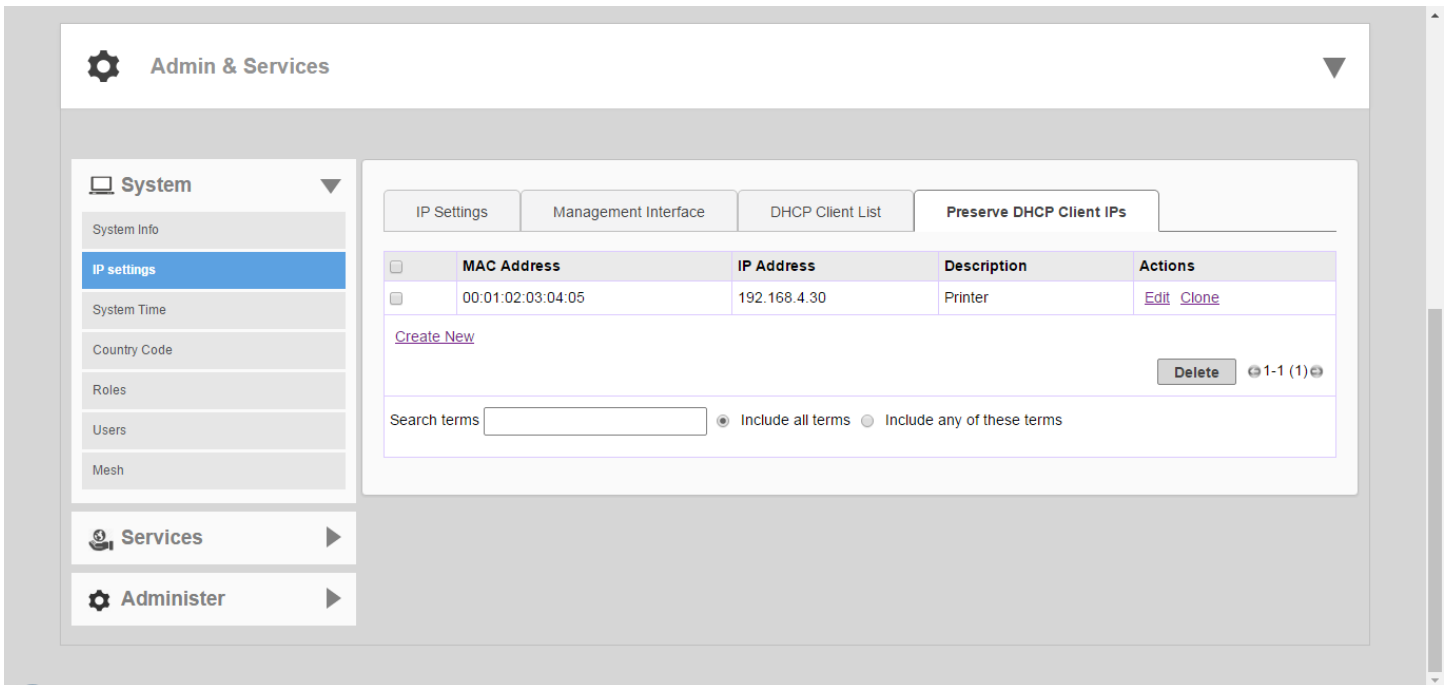


FIGURE 226 Reserved IP Addresses



## Configuring a Management Interface

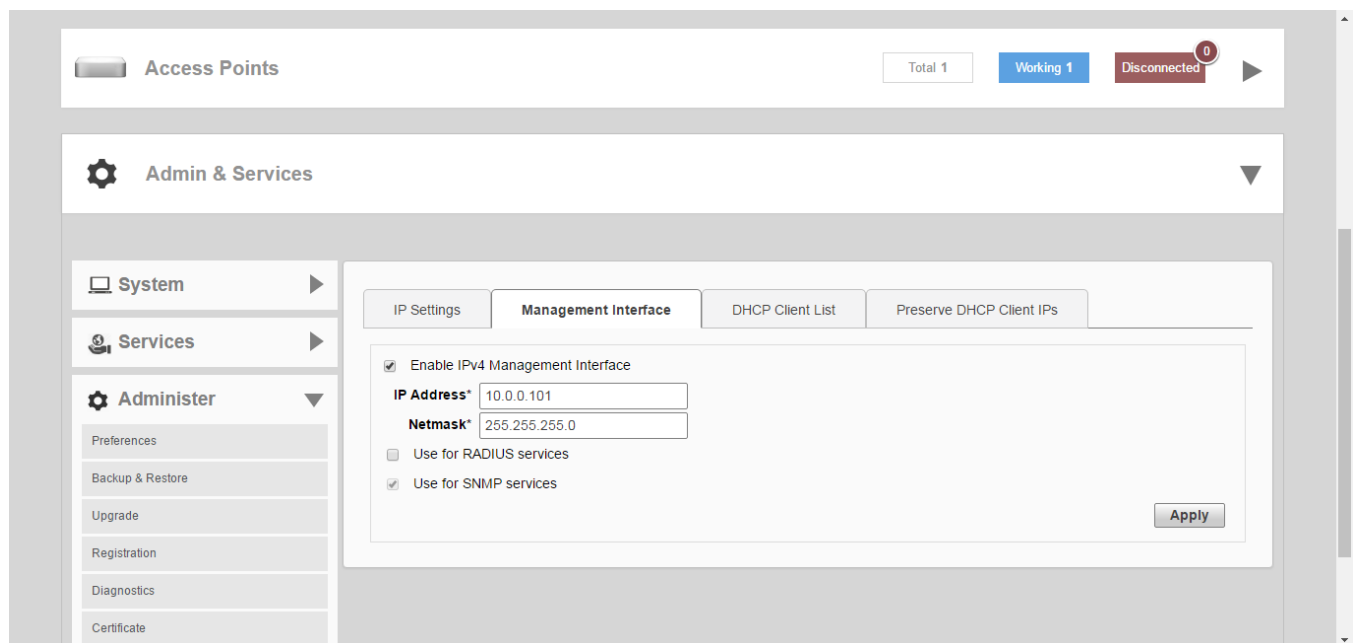
The Management IP address can be configured to allow an administrator to manage the Unleashed network from a single IP address, regardless of which Unleashed AP is currently the Unleashed Master AP.

The Management IP can be reached from anywhere on the network as long as it is routable via the default Gateway configured in **Device IP Settings**. Then, you only have to remember one IP address.

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. Optionally, 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.
5. 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 227** Management Interface



## Configuring the System Time

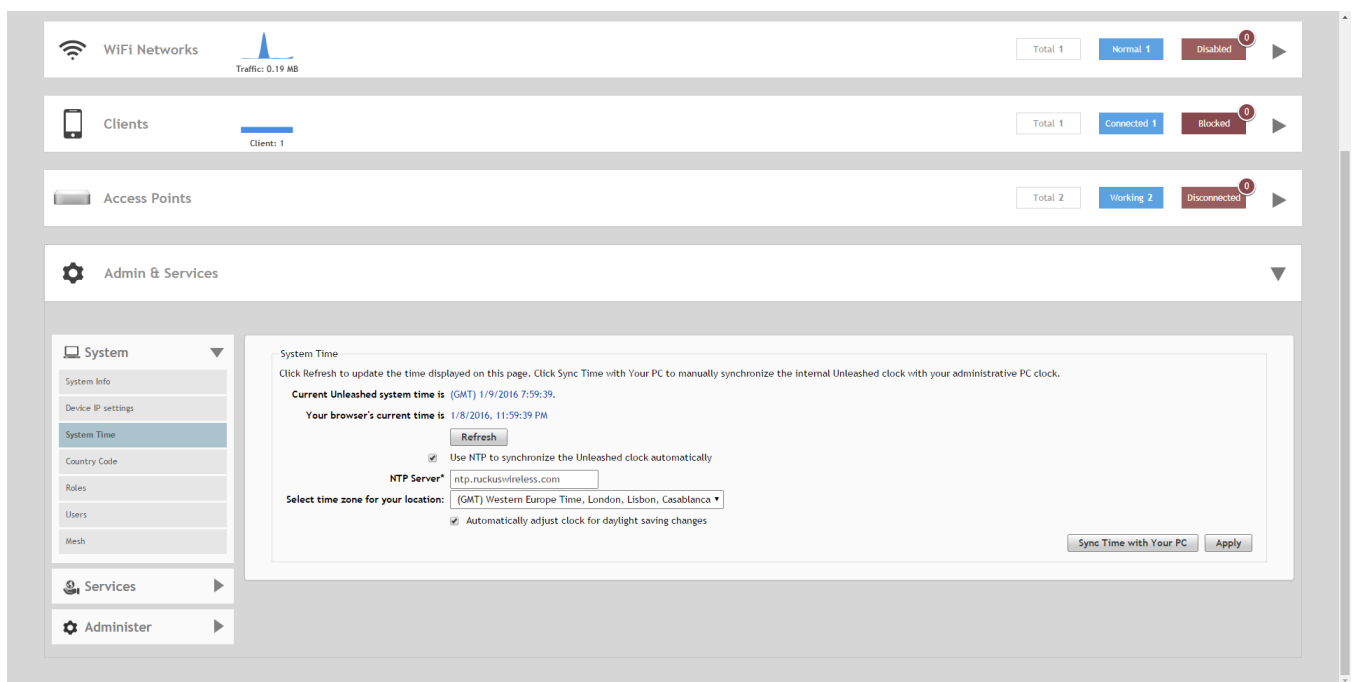
By default, the Unleashed network automatically updates its system time using the Network Time Protocol (NTP), which periodically polls an NTP server and synchronizes its time with the NTP server. You can also sync time with your PC to manually synchronize the internal clock with your admin PC's clock.

To configure the system time:

1. Go to **Admin & Services > System > System Time**.

- The **System Time** page provides the following options:
  - Refresh:** Click this to update the Unleashed time display (a static snapshot) from the internal clock.
  - Use NTP Server** (Enabled by default): Clear this check box to disable this option.
  - 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.
  - Select time zone for your location:** Choose your time zone from the dropdown menu. Setting the proper time zone ensures that timestamps on log files are in the proper time zone.
  - Sync Time with your PC:** If needed, click this to update the internal clock with the current time settings from your administration PC.
- Click **Apply** to save the results of any resynchronization or NTP server settings changes.

FIGURE 228 System Time



## 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 Unleashed network does not violate local and national regulatory restrictions.

Setting the Country Code for the Unleashed Master 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 Unleashed network.

### NOTE

Unleashed APs sold in the United States are fixed to US country code, and cannot be changed.

To set the Country Code to the proper location:

- Go to **Admin & Services > System > Country Code**.

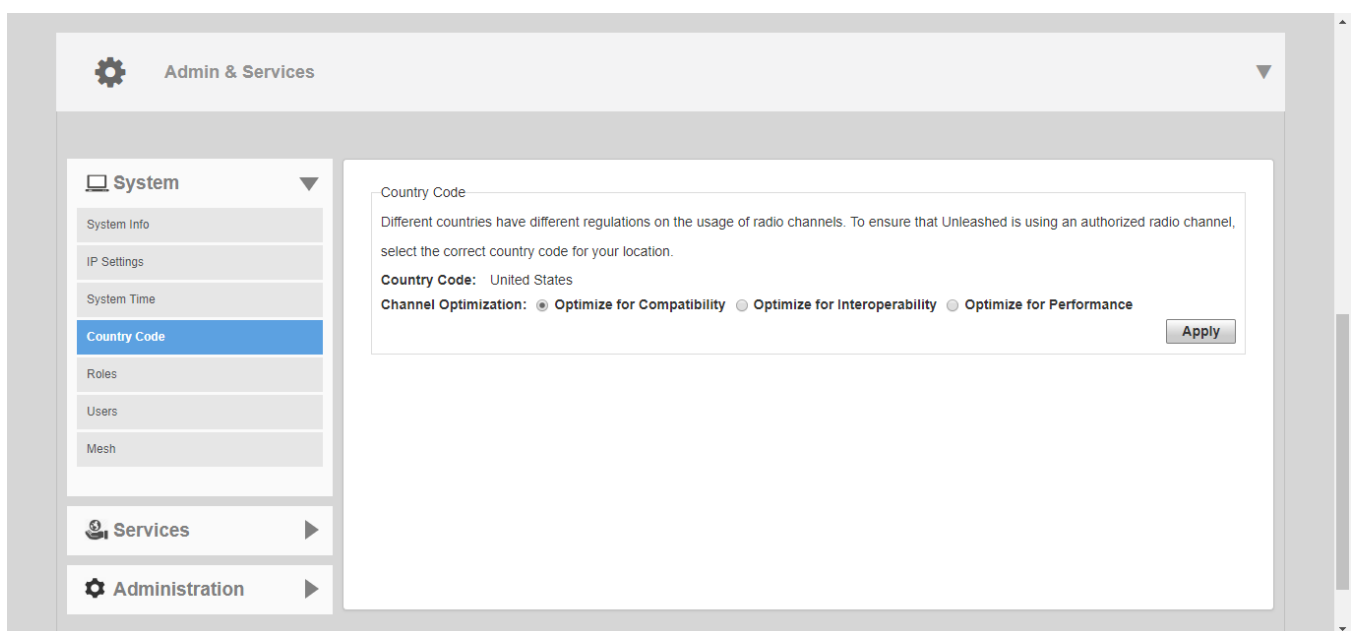
2. Choose your location from the **Country Code** drop-down menu.
3. In **Channel Optimization**, select one of the following options:
  - **Optimize for Compatibility:** Allows the following channels: 36, 40, 44, 48, 149, 153, 157, 161, 165 (non-DFS channels).
  - **Optimize for Interoperability:** 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 229** The Country Code page



### 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 23** 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.)

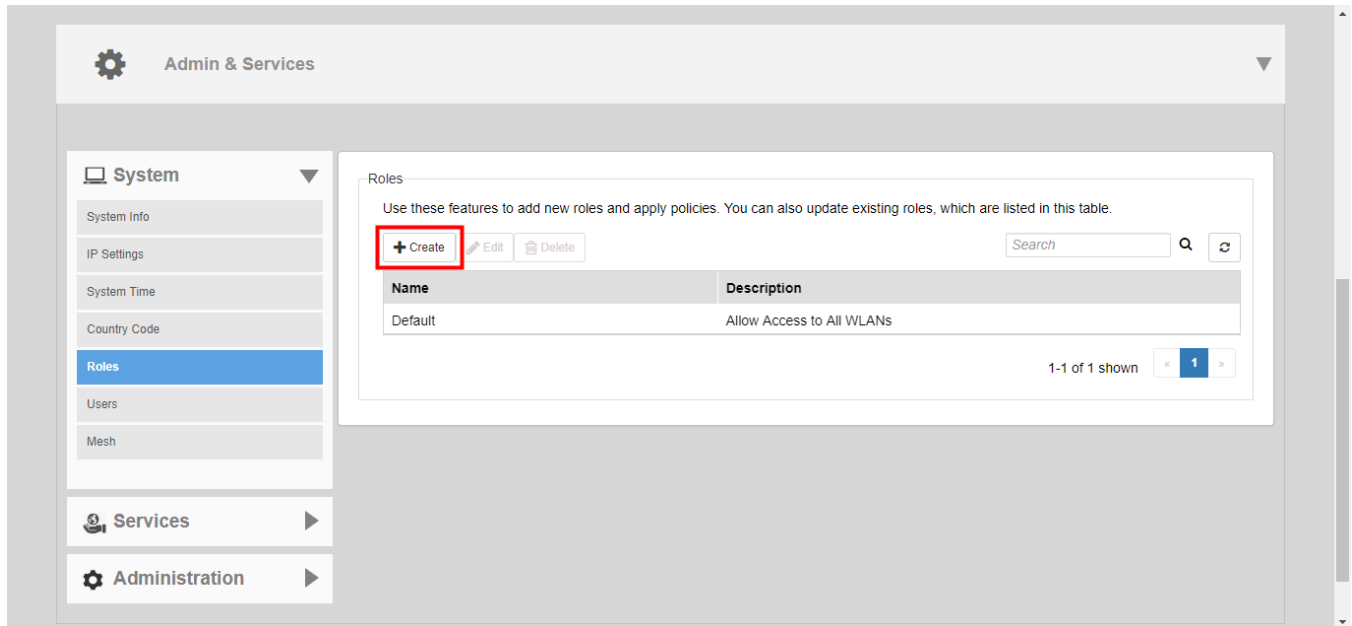
To create a new user Role:

1. Go to **Admin & Services > System > Roles**. The **Roles** page appears, displaying a Default role in the **Roles** table.



2. Click **Create**.

**FIGURE 230** 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.

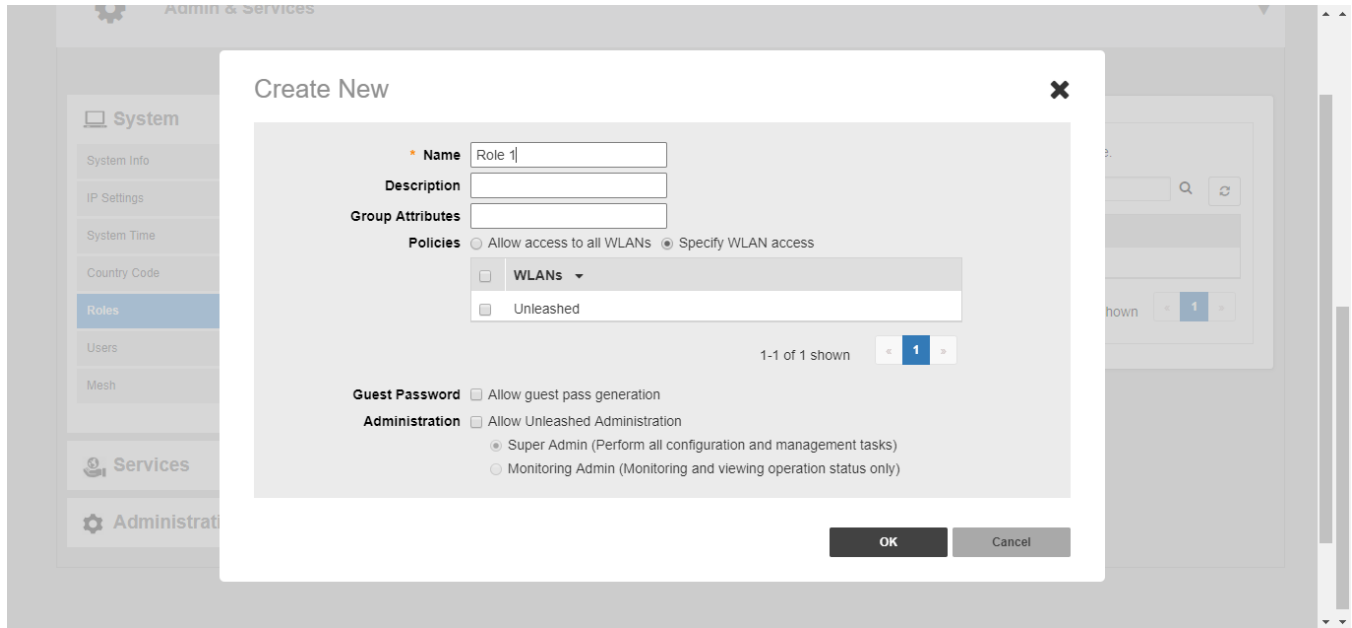
**NOTE**

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 231** Creating a new user Role



## Adding New Users to the Local Database

Once your Unleashed 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 304.

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 288.
5. Click **OK** to save your settings. Be sure to communicate the user name and password to the appropriate end user.

FIGURE 232 The Users page

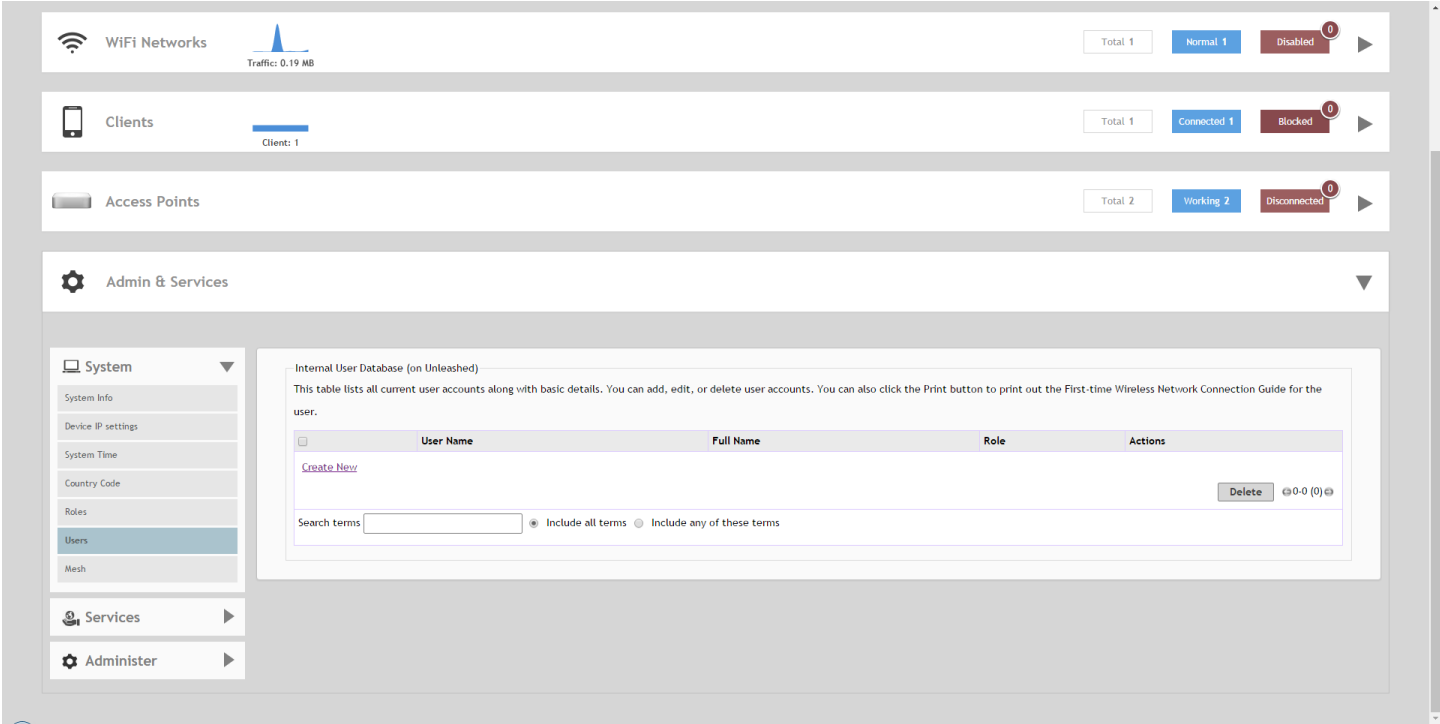
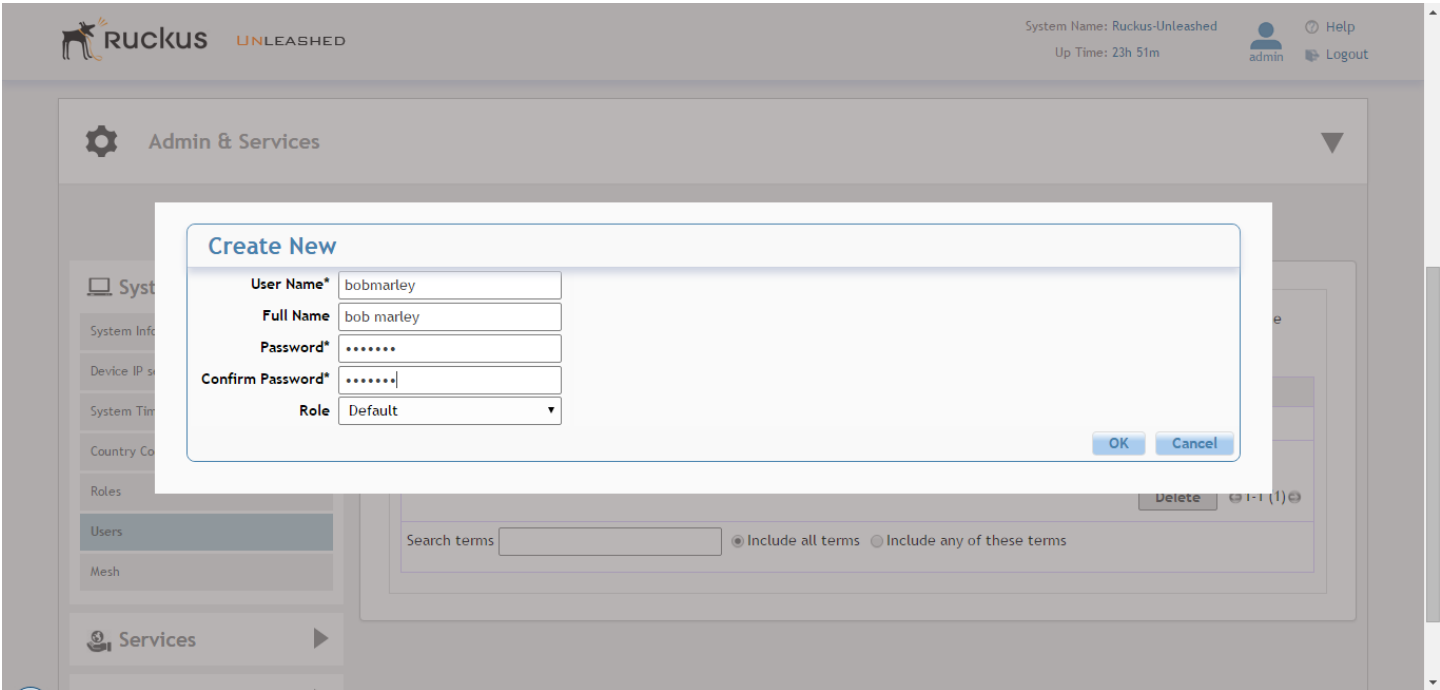


FIGURE 233 Creating a new User on the internal database



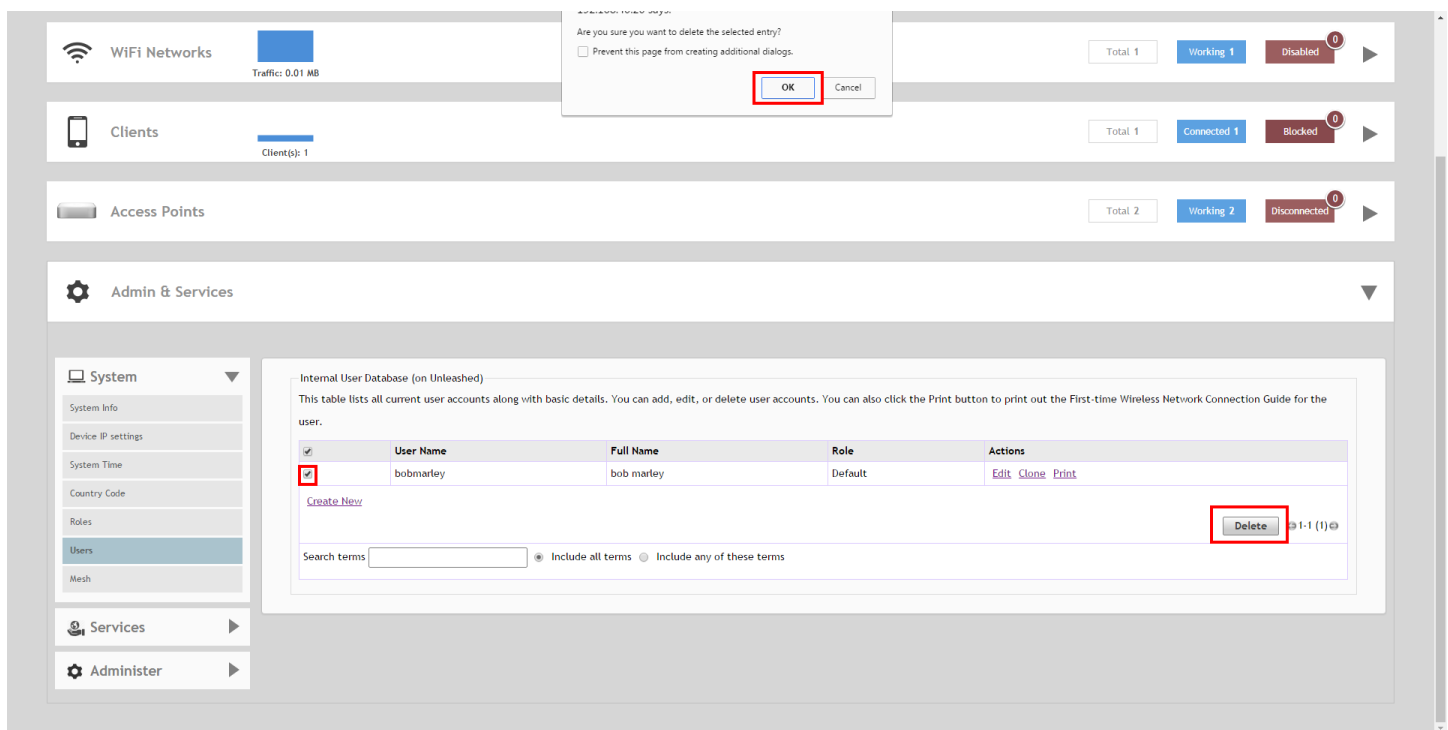
## Changing an Existing User Account

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 288.)
5. Click **OK** to save your changes. Be sure to communicate the relevant changes to the appropriate end user.

## 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 234 Deleting a user from the internal database



## 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, Unleashed member APs communicate with the Unleashed 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 24** 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 Unleashed Master AP through its Ethernet (wired) interface. The Unleashed Master AP itself must also be a Root AP.
Mesh AP (MAP)	A mesh node that communicates with the Unleashed Master AP through its wireless interface via 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 Unleashed Master AP can manage more than one mesh tree. There is no limit on the number of mesh trees per Unleashed Master. For example, an 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.

See [Supported Mesh Topologies](#) on page 293 for more information.

### Supported Mesh Topologies

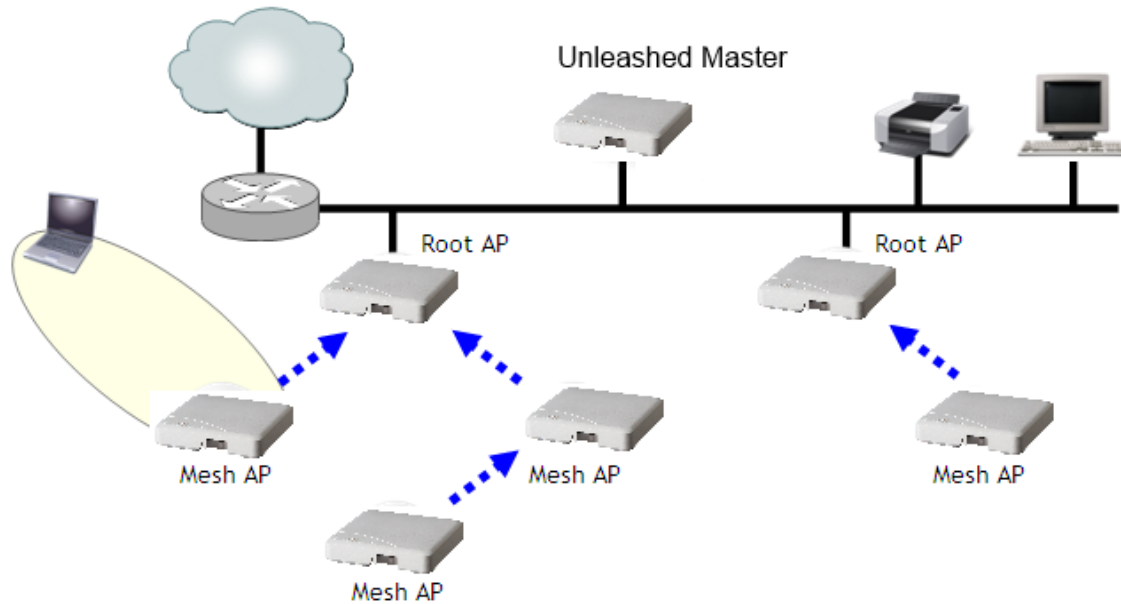
Smart Mesh networks can be deployed in three types of topologies:

- 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."

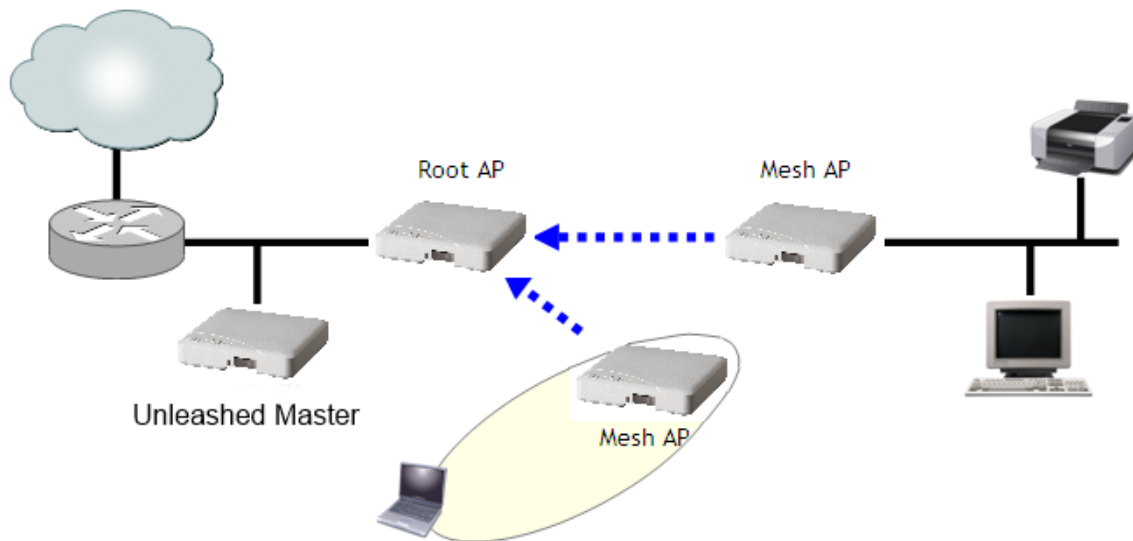
FIGURE 235 Mesh - standard topology



### 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 236 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.

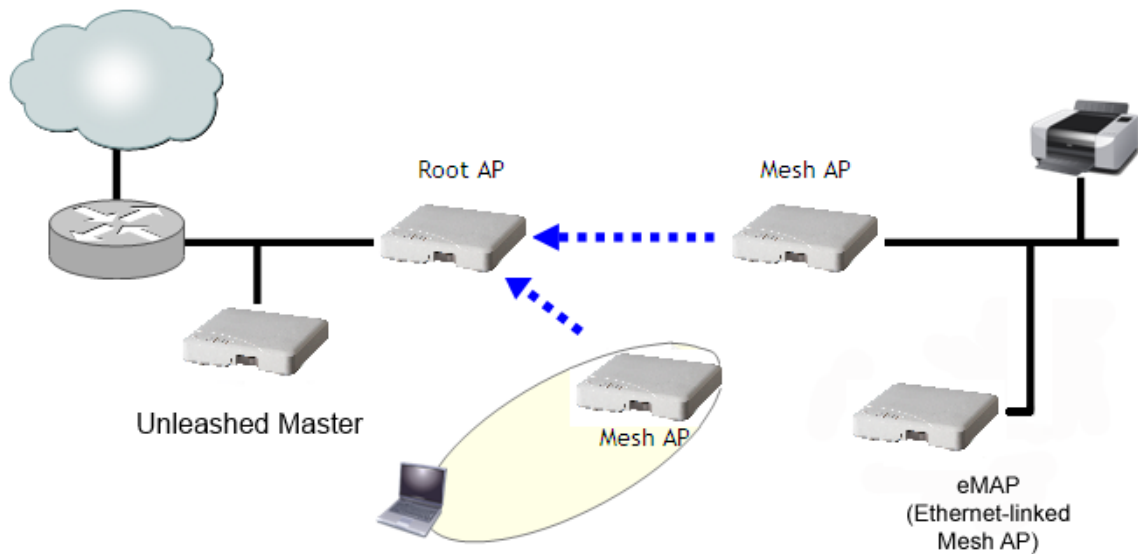
Multiple eMAPs can be connected to a single Mesh AP to, for example, bridge a wired LAN segment inside a building to a wireless mesh outdoors.

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 237 eMAP - Hybrid Mesh topology



### Configuring Mesh Settings

You can configure Mesh settings from the **Admin & Services > System > Mesh** page.

To configure Mesh settings, select the check box next to **Enable Mesh**. Optionally, you can change the **Mesh Name (ESSID)** and the **Mesh Passphrase**, or click **Generate** to generate a new random Mesh passphrase.

**NOTE**

Once you have enabled Mesh, you cannot disable it again without resetting the Unleashed Master AP to factory defaults (see [Restore to Factory Settings](#) on page 351).

**NOTE**

If you enabled Mesh during the Setup Wizard process, you do not need to configure it again here.

**NOTE**

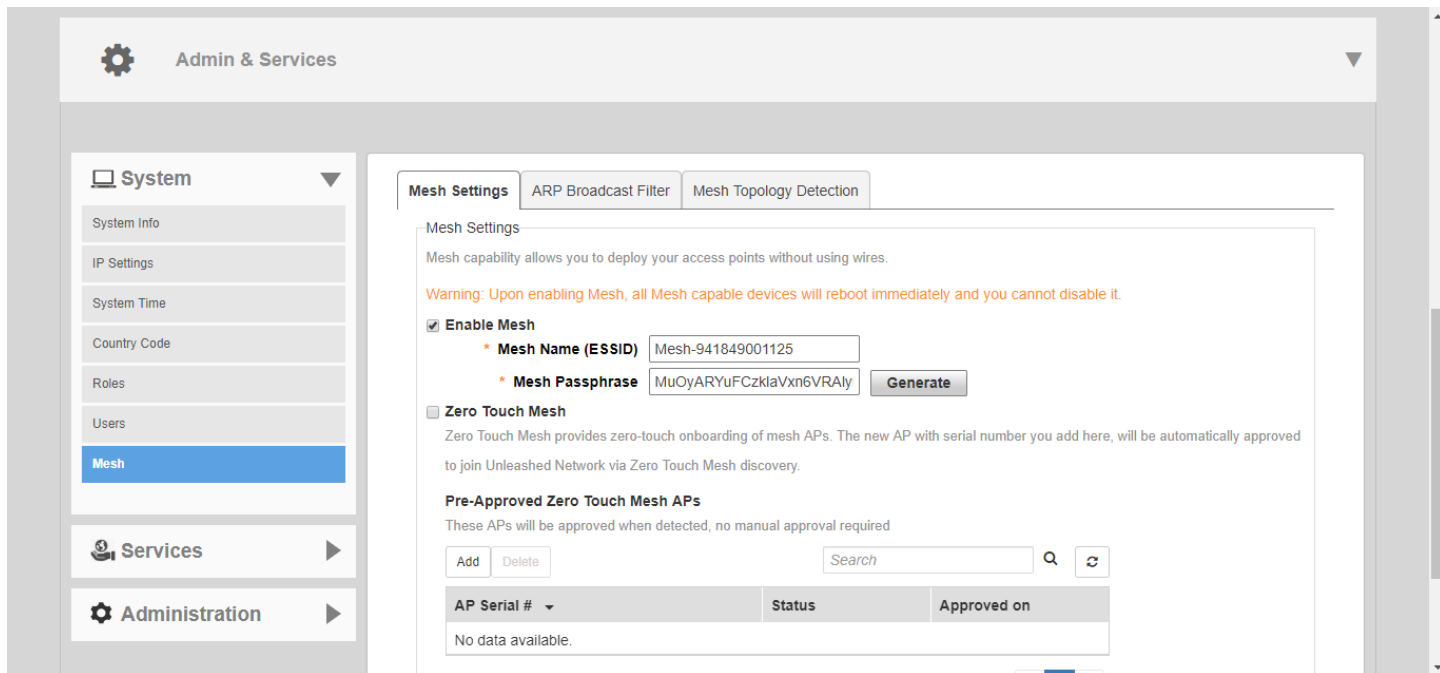
The Unleashed Master AP cannot be a Mesh AP. The Unleashed Master can only be a Root AP in a Mesh topology.

**NOTE**

Unleashed H320 does not support Mesh.



FIGURE 238 Mesh settings



### Zero Touch Mesh

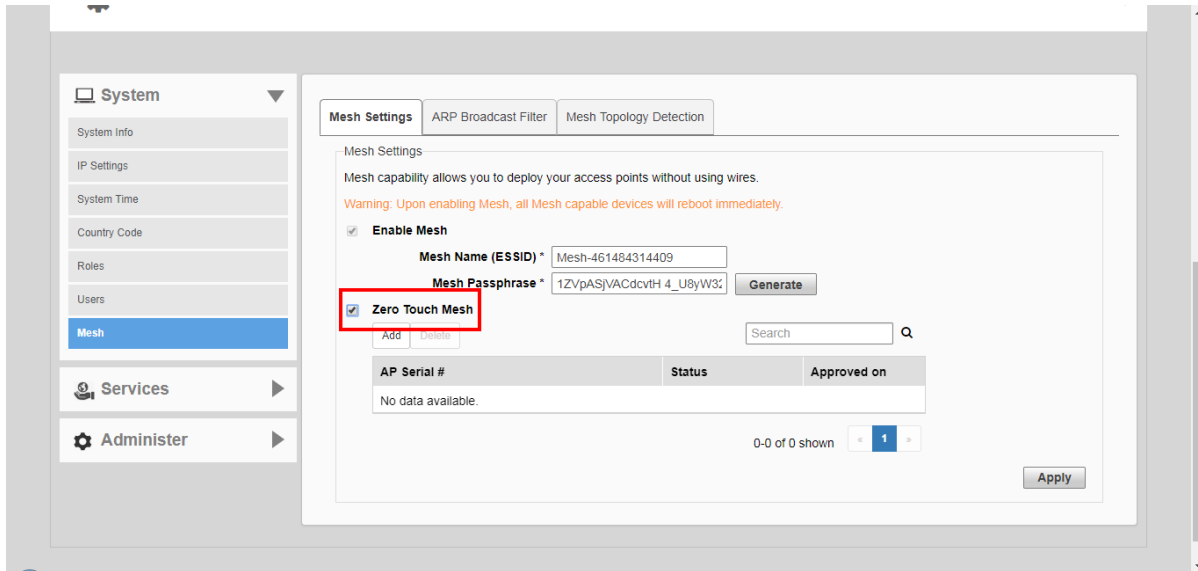
Zero Touch Mesh allows customers to skip the mesh configuration priming process, enabling Mesh APs already installed in their permanent locations to auto-discover, auto-provision and auto-form a mesh network without priming.

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 239 Enabling Zero Touch Mesh



### Onboarding Mesh APs with Zero Touch Mesh

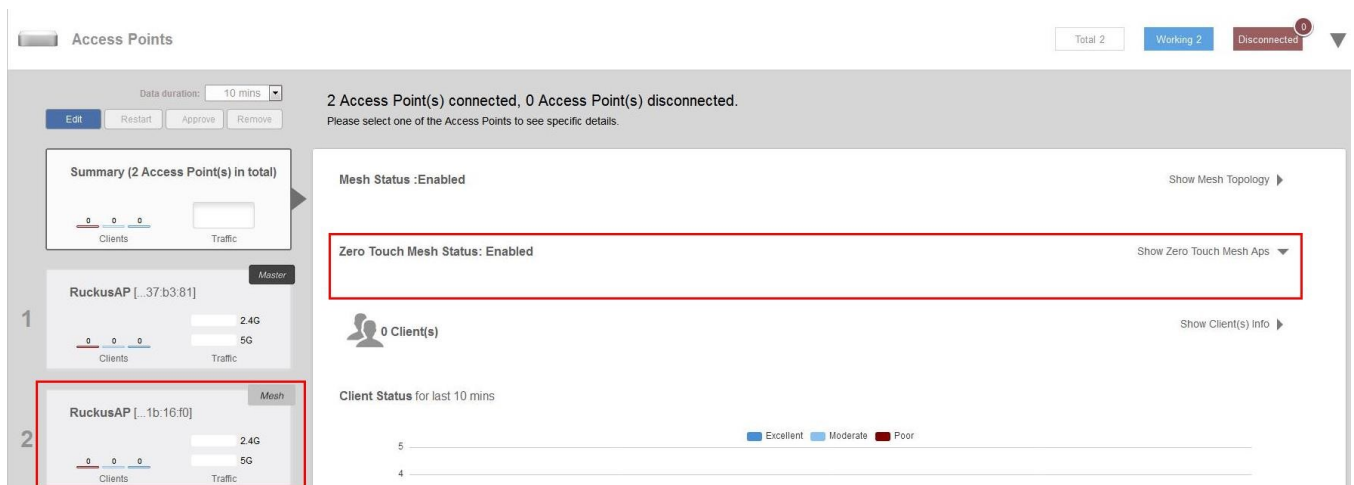
To allow Unleashed Mesh APs to join the Mesh network without first connecting them via Ethernet, use the following procedure:

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.

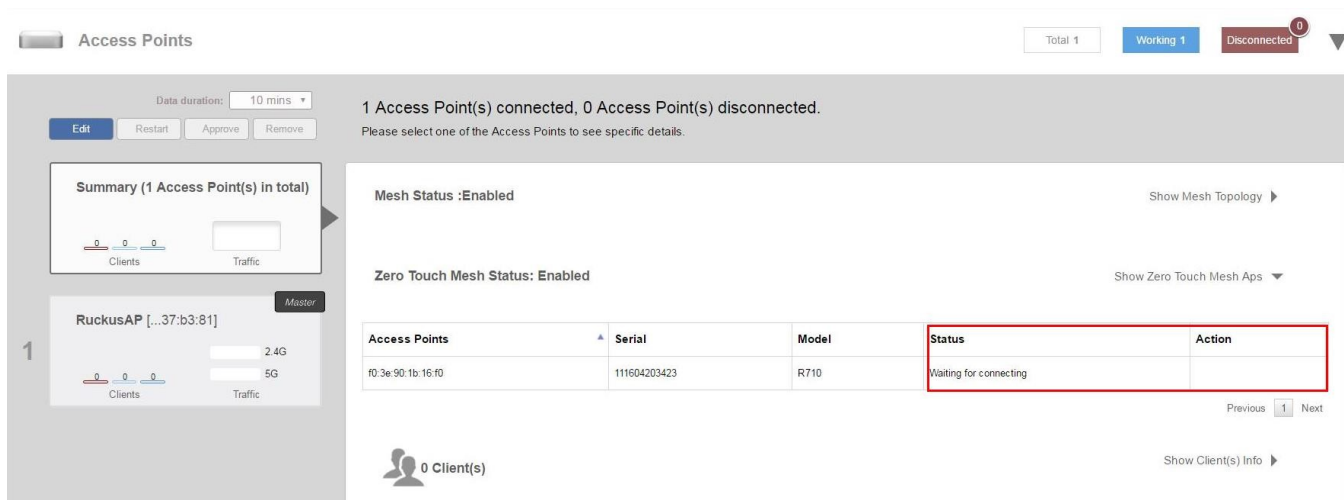
4. Go to **Access Points > Summary > Show Zero Touch Mesh APs**.

FIGURE 240 Show Zero Touch Mesh APs

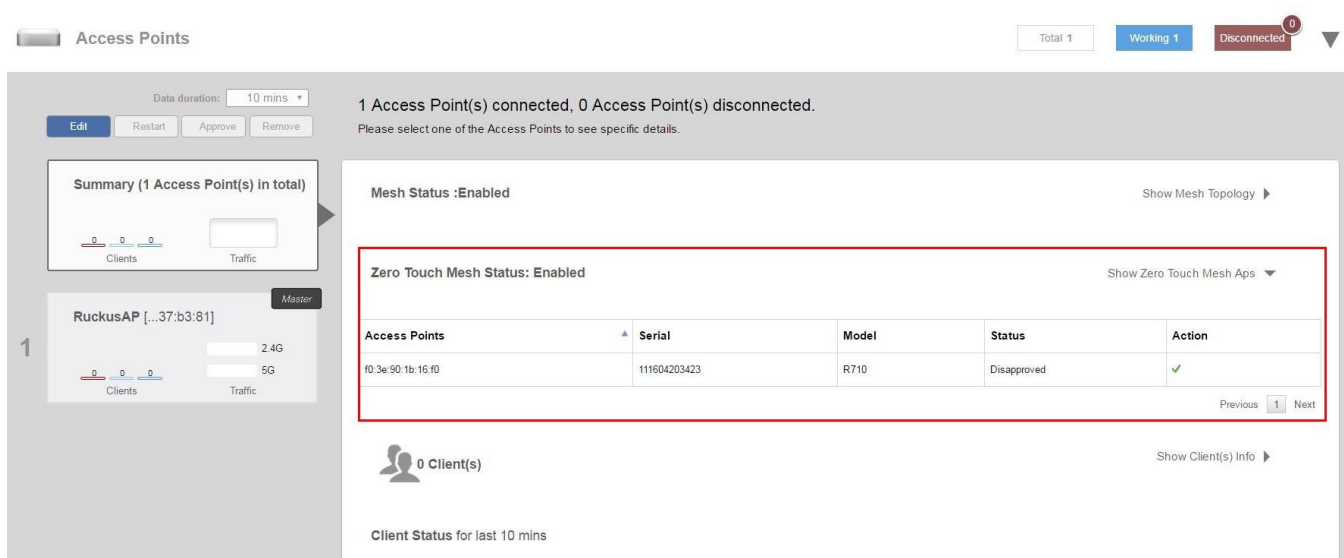


- When a supported AP attempts to join, it will appear in the *Zero Touch Mesh AP* table. Click the **Approve** button to approve the AP.

**FIGURE 241** Waiting for connection



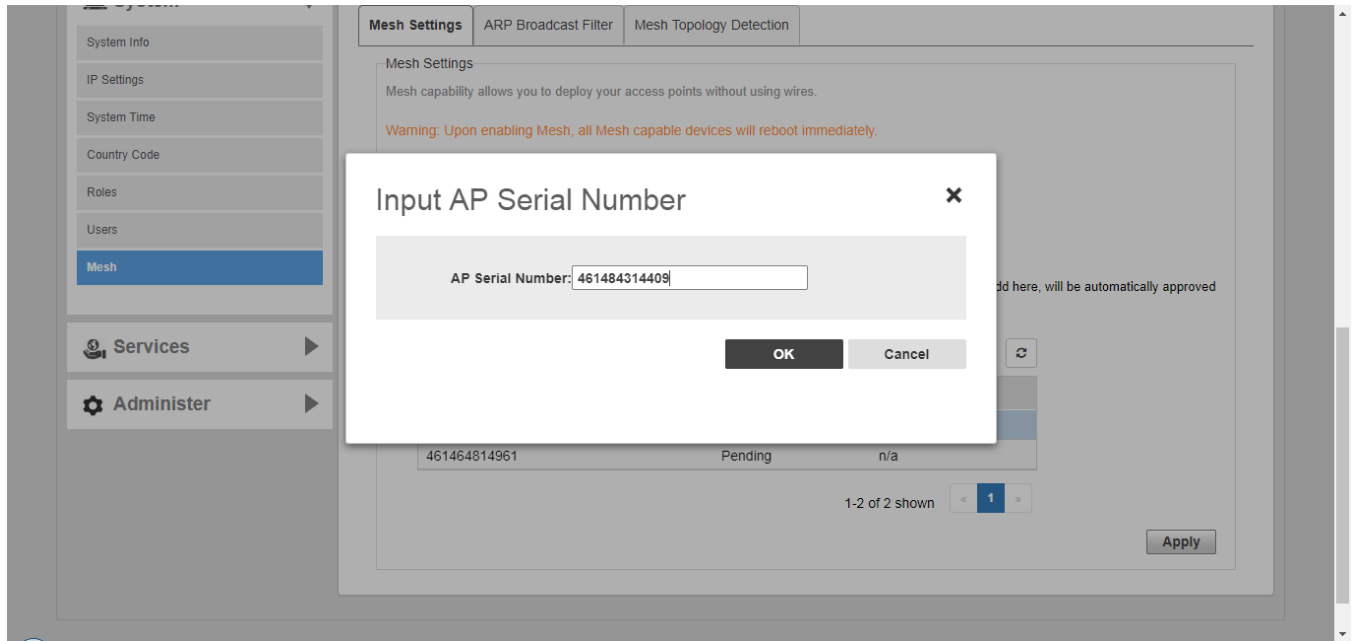
**FIGURE 242** Click Approve to allow the AP to join



- 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.
- 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 243** 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.

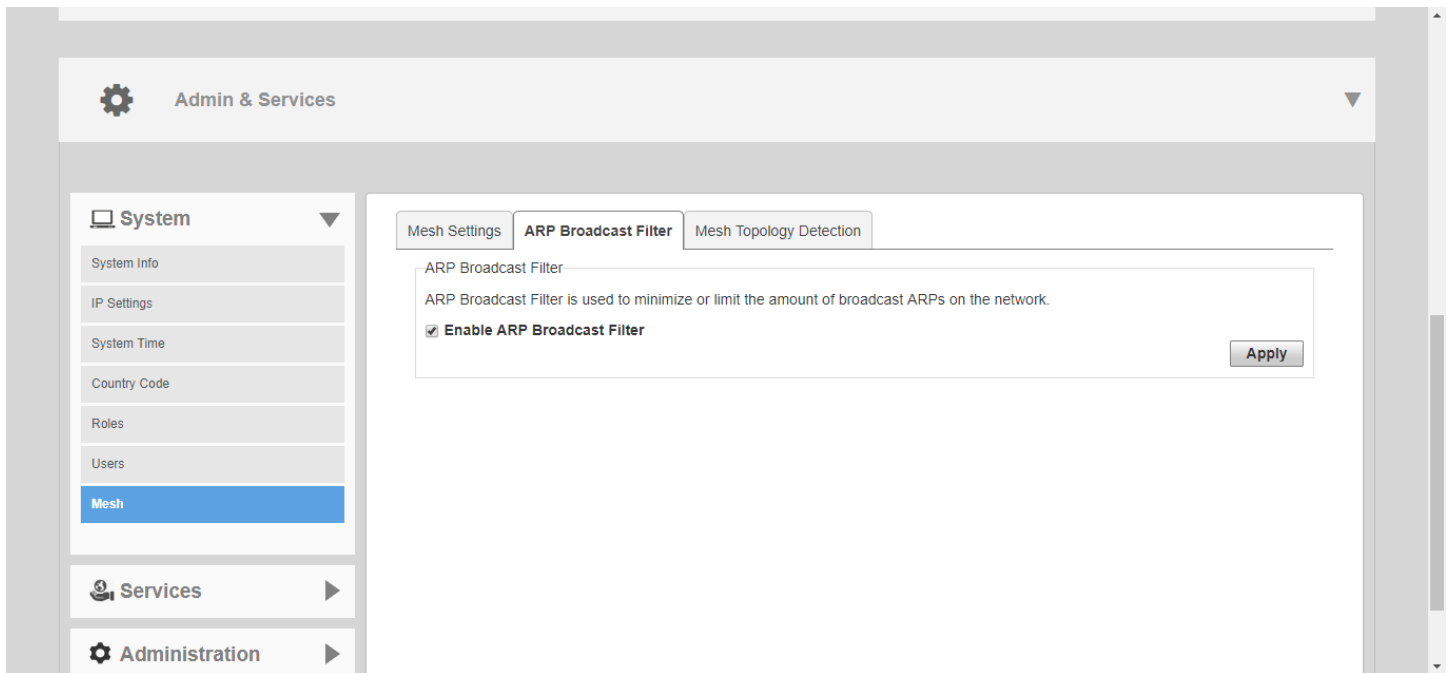
### **ARP Broadcast Filter**

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 244 ARP Broadcast Filter



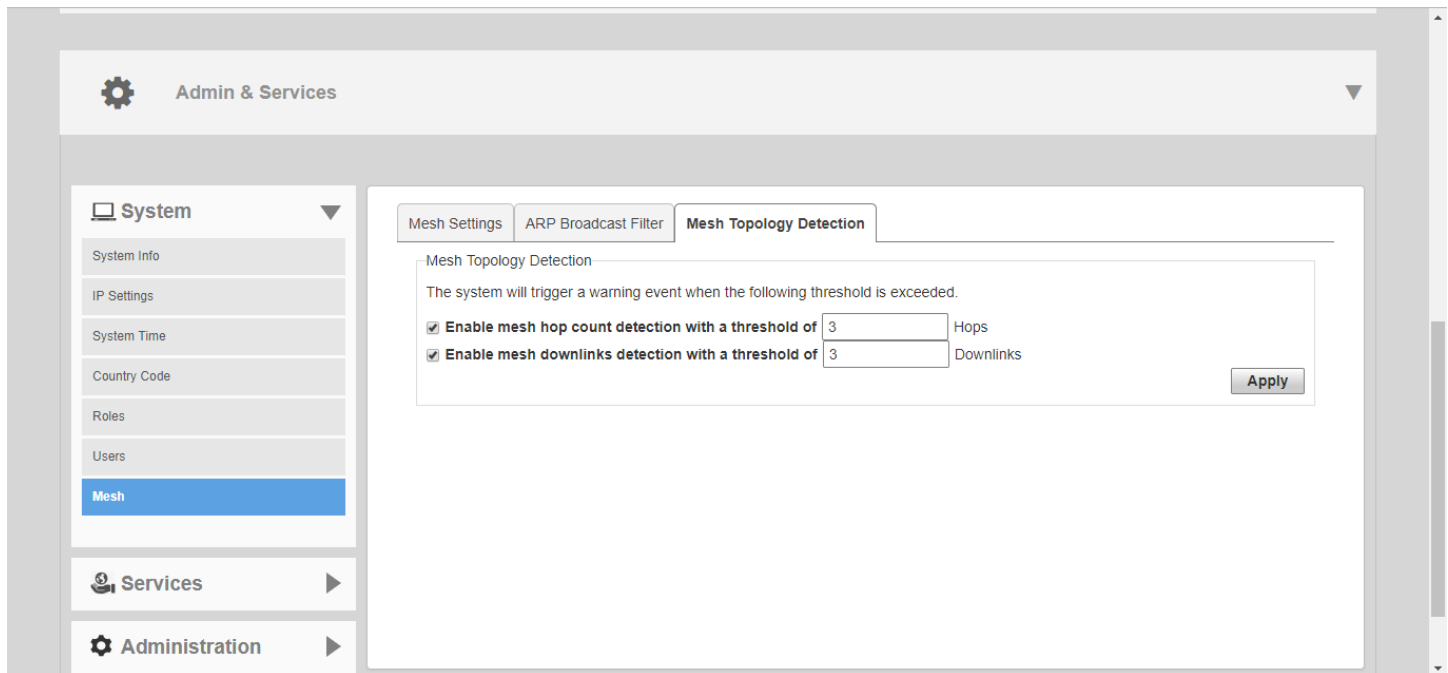
### **Mesh Topology Detection**

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 245 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 246** Configuring syslog settings

The screenshot shows a configuration page for syslog settings. The 'Log Settings' section is highlighted with a red box. It contains the following fields:

- Remote Syslog:**
  - Enable reporting to remote syslog server at  (IP Address) for
  - Inherit remote syslog server for APs
- Facility Name:**
- Priority Level:**

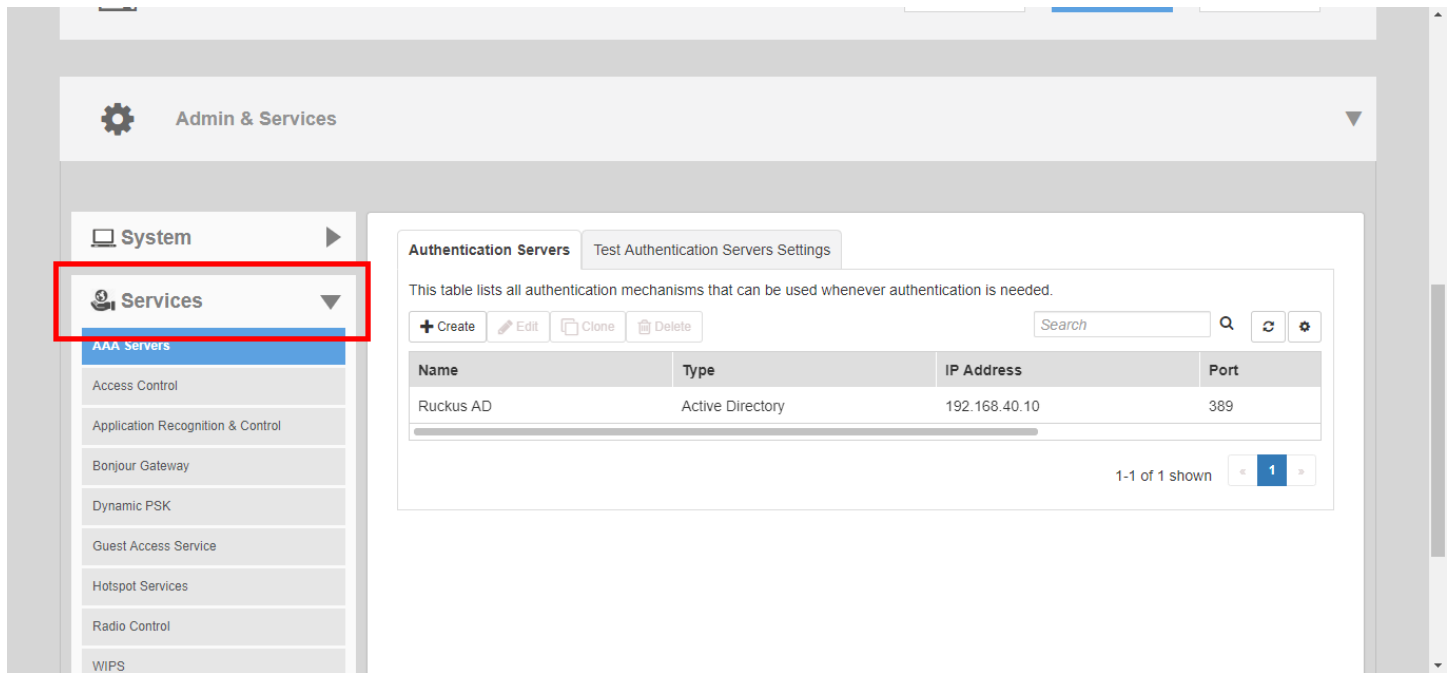
There is an **Apply** button at the bottom right of the highlighted section.

## 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 247 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

To configure 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. 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 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/TLS1.2.
    - **IP Address:** Enter the IP address of the AD server.
    - **Port:** The default port number (3268, 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 will be available in the Test Authentication Settings section to choose to test against the primary or the backup RADIUS server.
    - **IP Address:** Enter the IP address 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 Unleashed and the RADIUS server.
    - **Confirm Secret:** Repeat the shared secret.
    - **Retry Policy:** Enter a Request Timeout value (in seconds) and a Max Number of Retries value in the relevant fields.
4. Click **OK** to save your AAA server entry.

FIGURE 248 The AAA Servers page

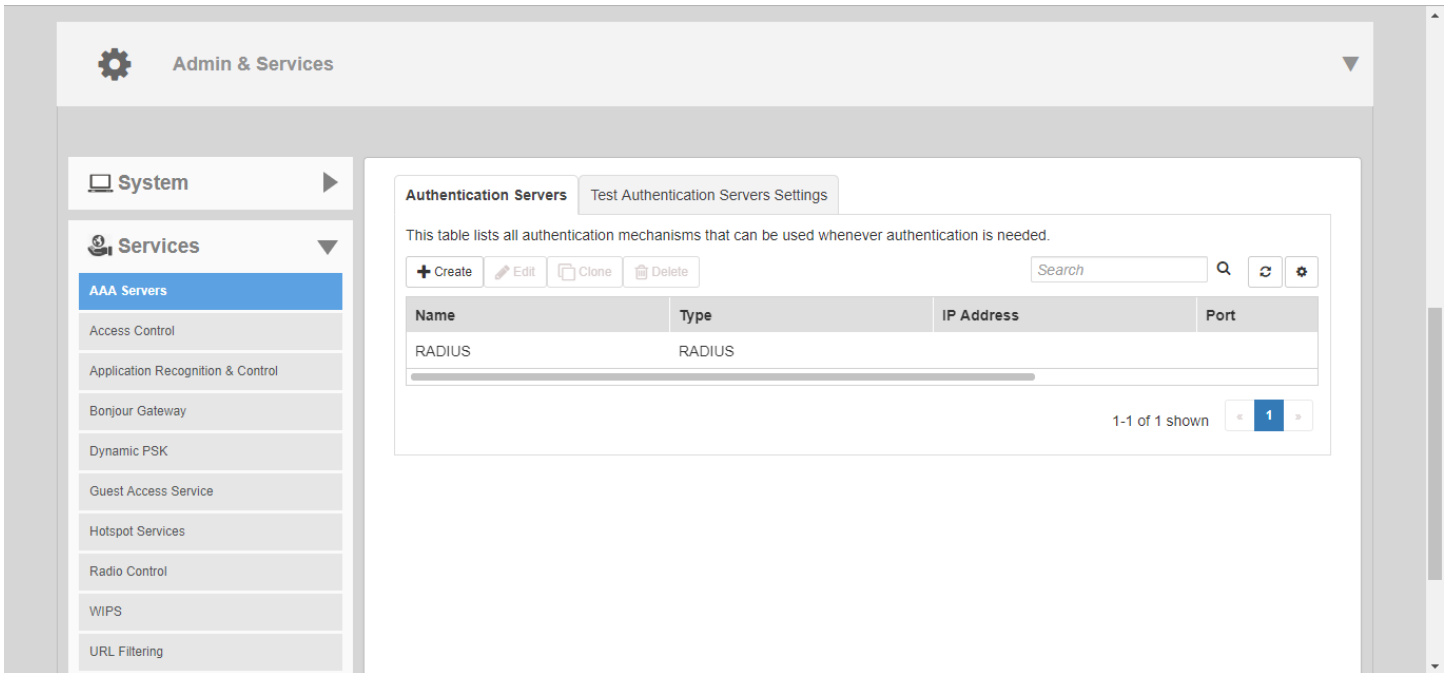


FIGURE 249 Microsoft Active Directory server configuration

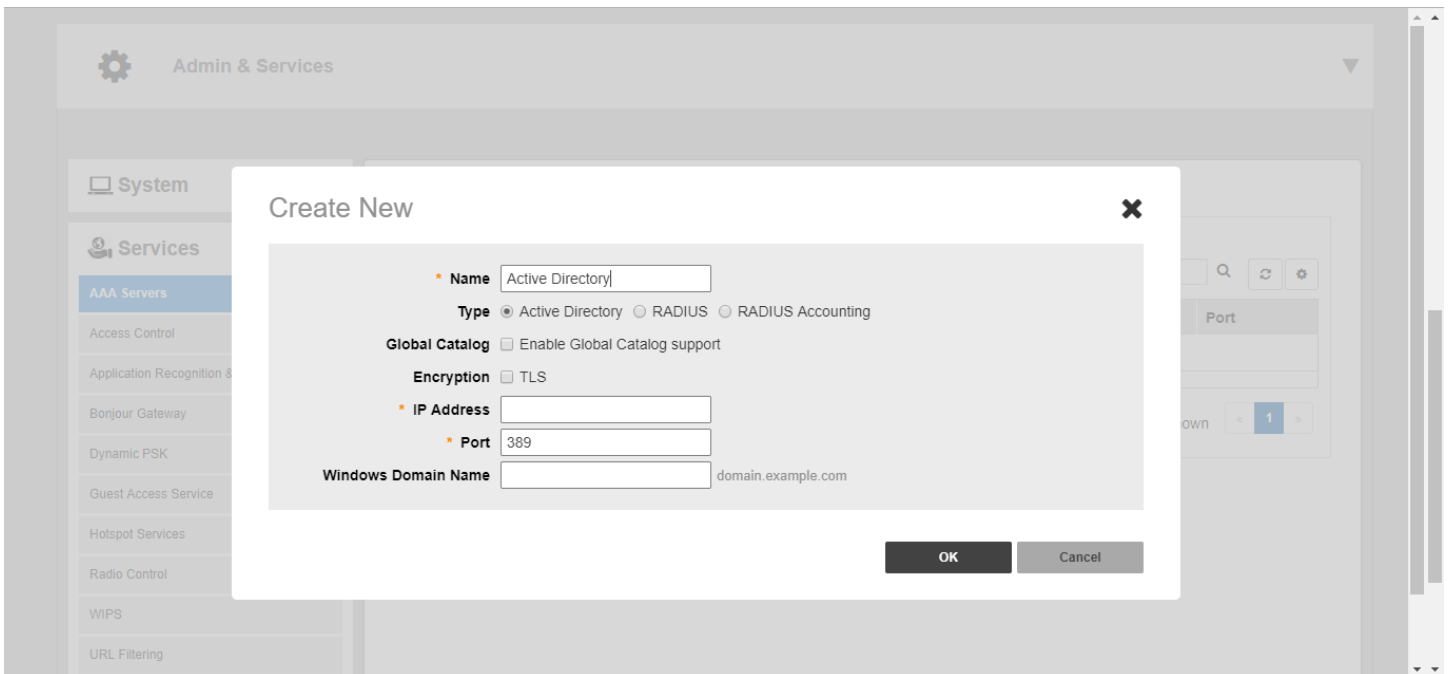
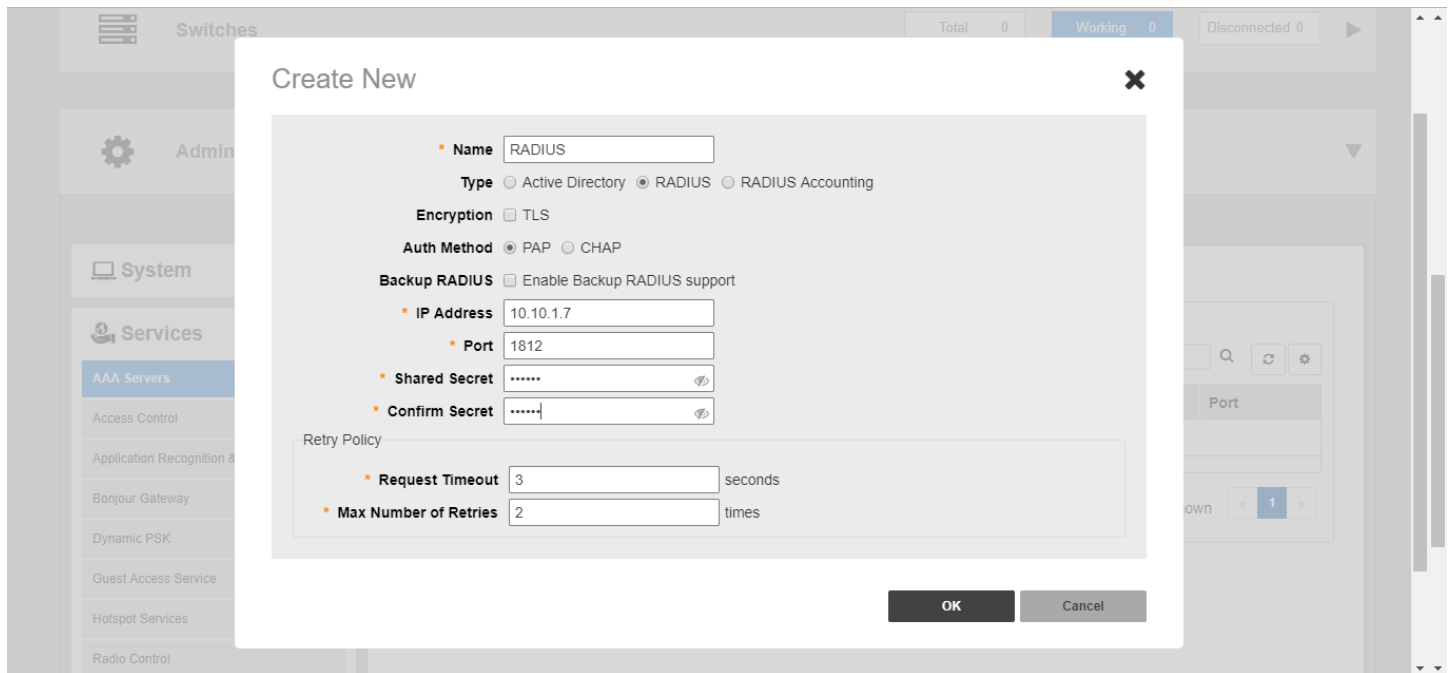


FIGURE 250 RADIUS server configuration



## 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:

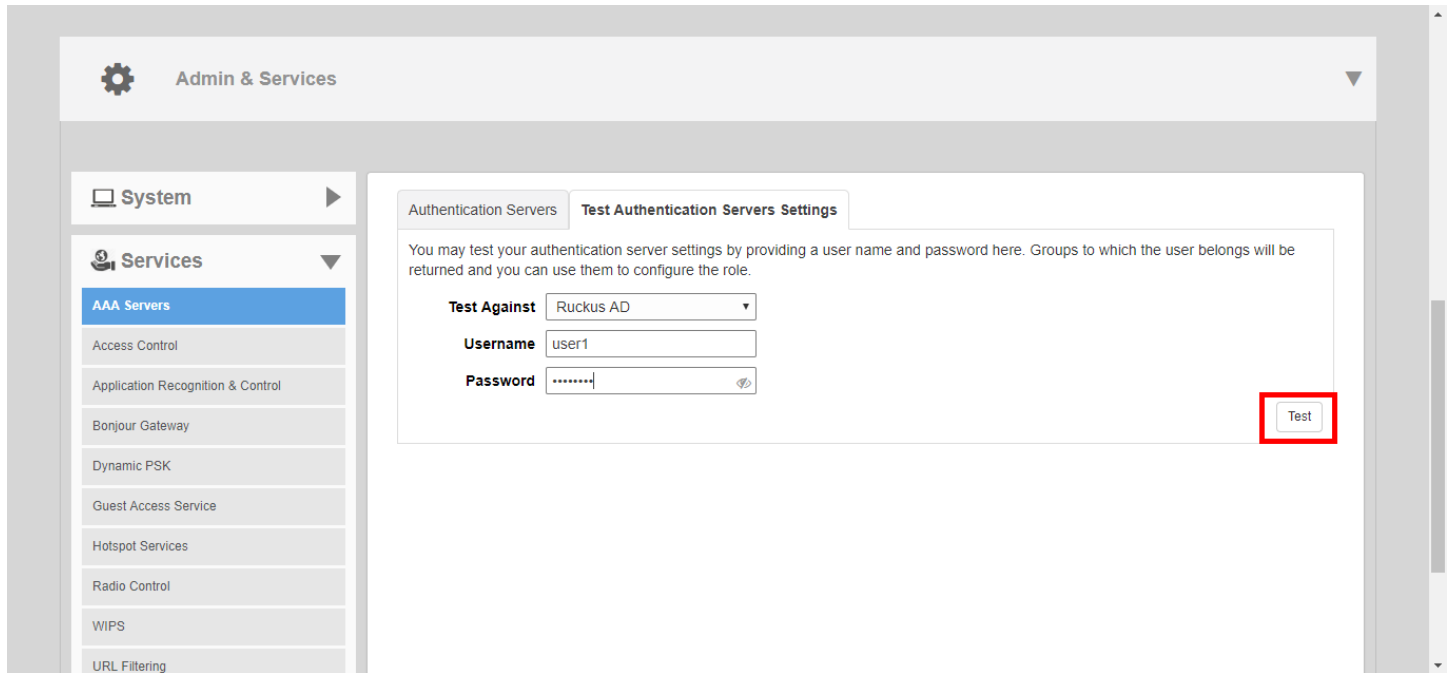
```
Success! Groups associated with this user are "{group_name}". This user will be assigned a role of {role}.
```

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.

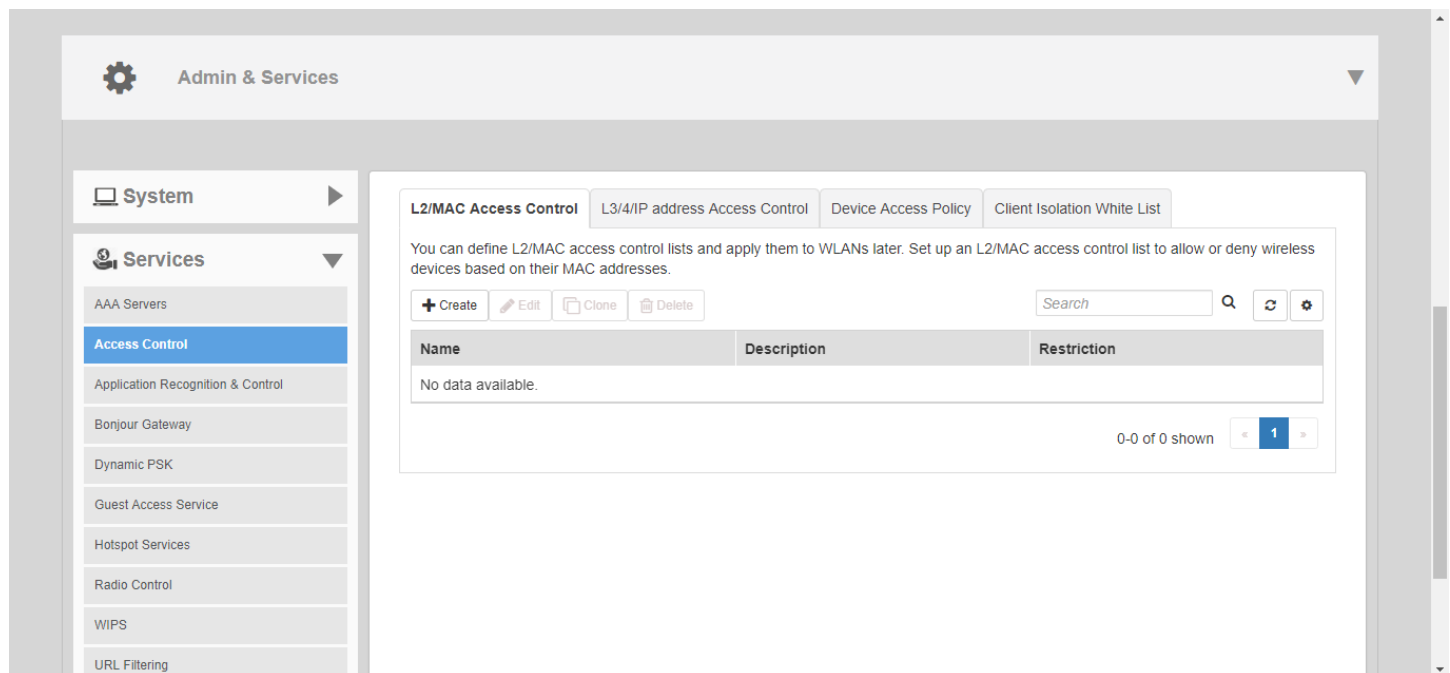
FIGURE 251 Testing authentication server settings



## Access Control

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 Whitelists, which are necessary when Wireless Client Isolation is enabled on a WLAN.

FIGURE 252 Configuring Access Controls



### Creating a Layer 2/MAC Address Access Control List

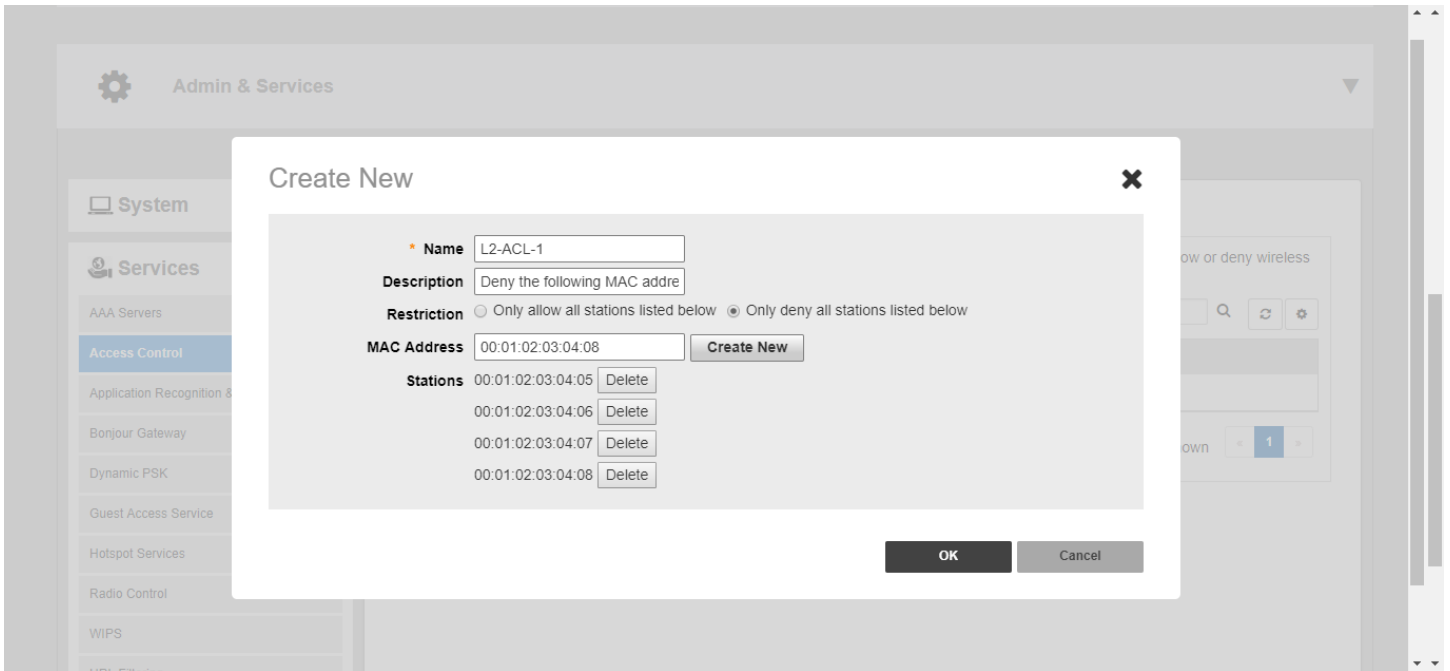
Using the Access Controls configuration options, you can define Layer 2/MAC address ACLs, which can then be applied to one or more WLANs (upon WLAN creation or edit). ACLs are either allow-only or deny-only; that is, an ACL can be set up to allow only specified clients or to deny only specified clients. 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 253** 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:

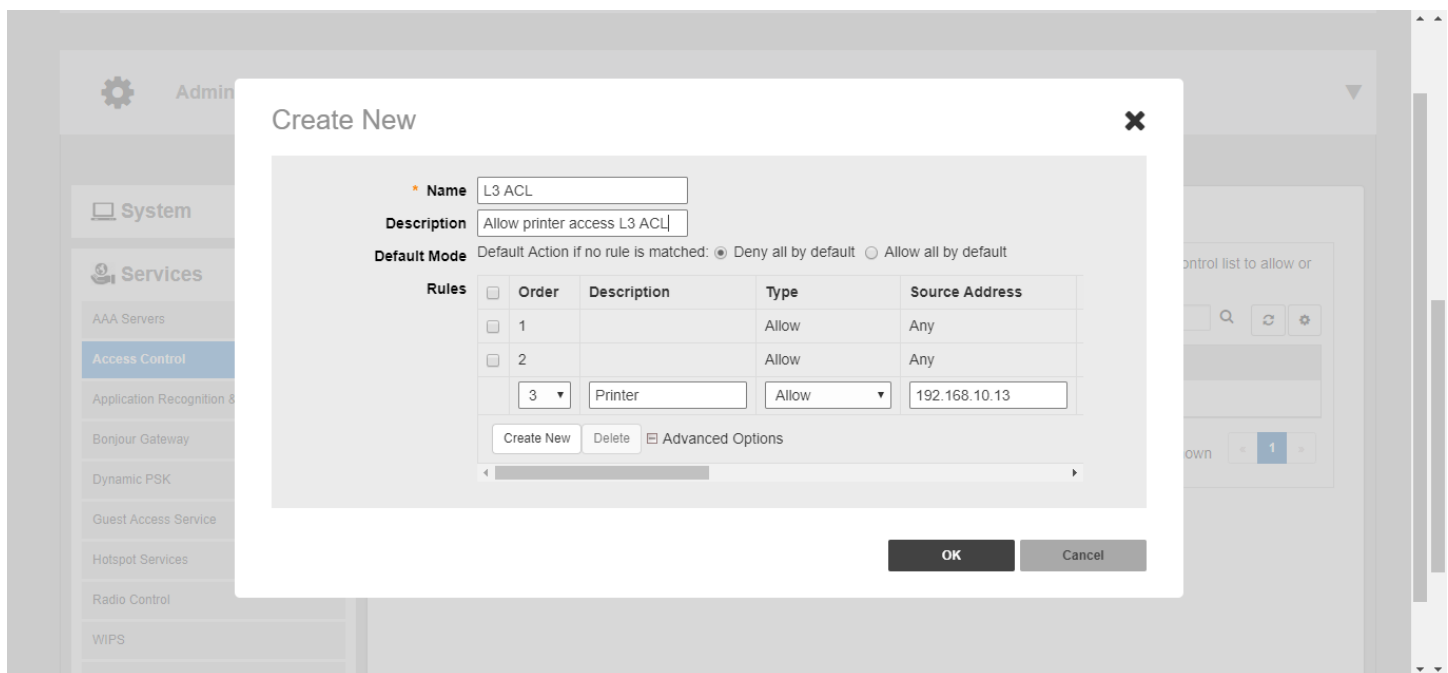
- Destination IP Address
- Application
- Protocol
- Destination Port

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 254** 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.

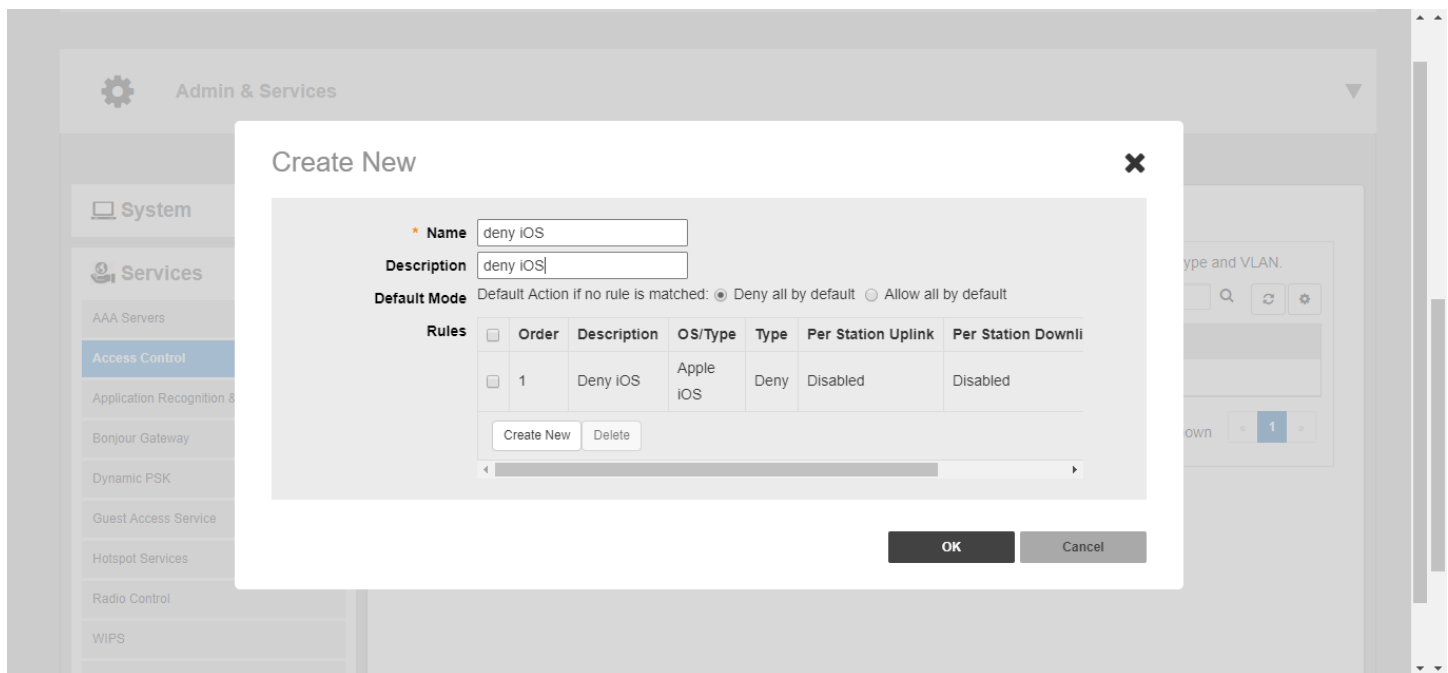
Using the **Device Access Policy** settings, the Unleashed system can identify the type of client attempting to connect, and perform control actions such as permit/deny and rate limiting based on the device type.

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 255 Creating a Device Access Policy



### Configuring Client Isolation White 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 white list.

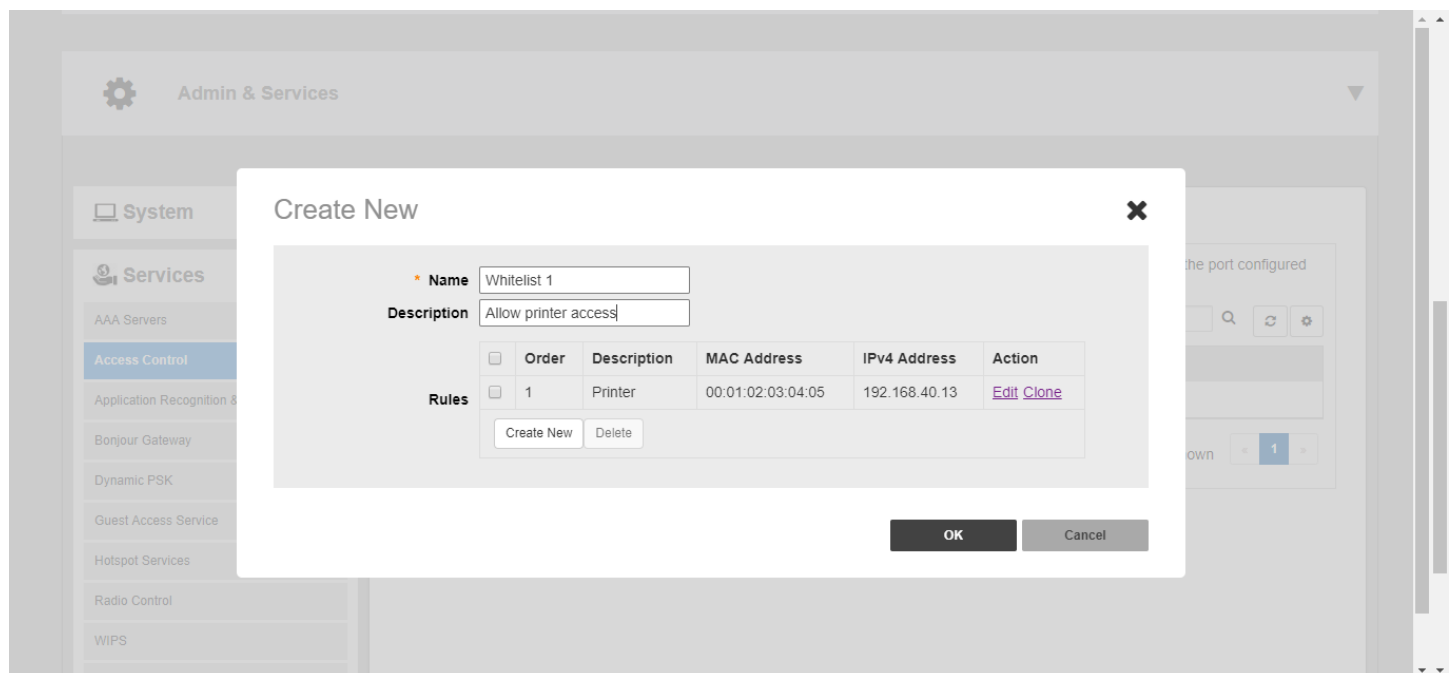
You can create exceptions to client isolation (such as allowing access to a local printer, for example) by creating Client Isolation White Lists.



To create a Client Isolation White List:

1. Go to **Admin & Services > Services > Access Control > Client Isolation White List**.
2. Click **Create New**.
3. Enter a **Name** and optionally a description for the whitelist policy.
4. In **Rules**, you can create multiple device-specific rules for each device to be white listed.
  - **Description:** Description of the device.
  - **MAC Address:** Enter the MAC address of the device.
  - **IPv4 Address:** Enter the IP address of the device.
5. Click **Save** to save the rule you created.
6. 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**.
7. Click **OK** to save the white list.

**FIGURE 256** Creating a Client Isolation White 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 257 Application Overview page

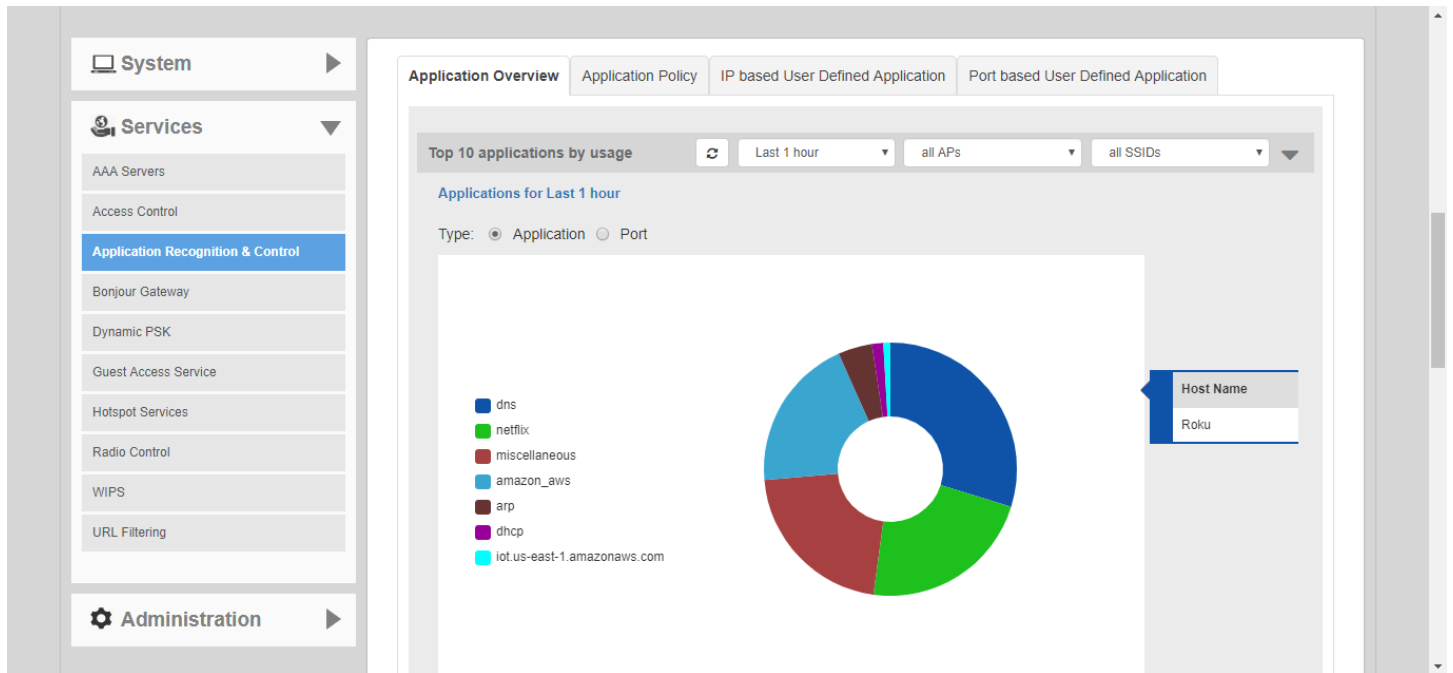
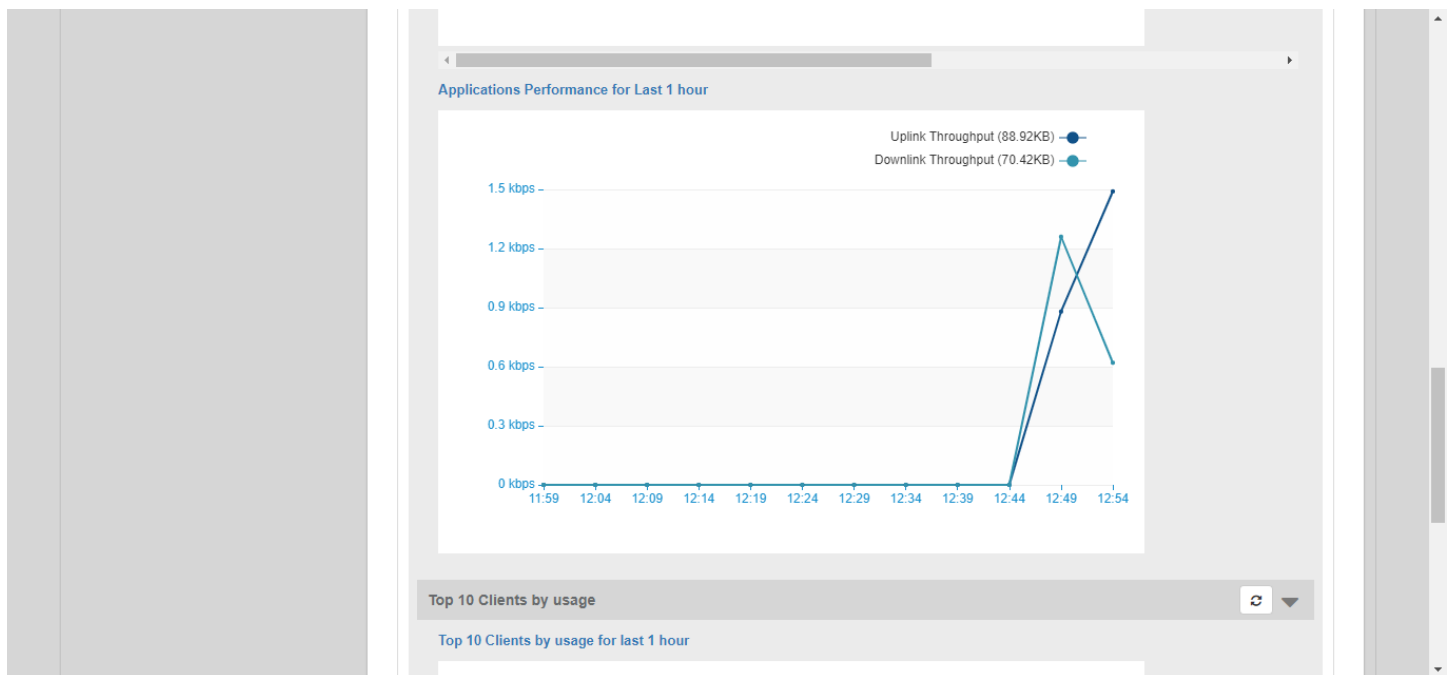
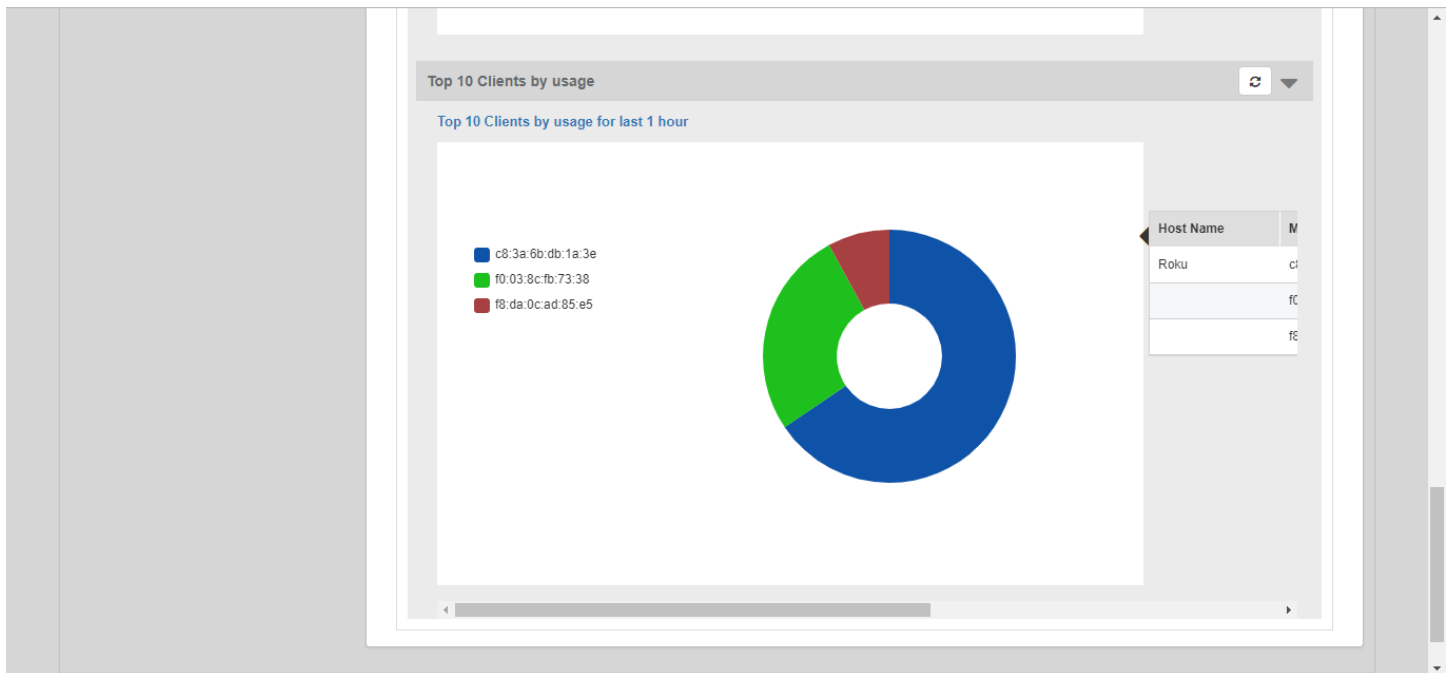


FIGURE 258 Application Performance



**FIGURE 259** 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 191.

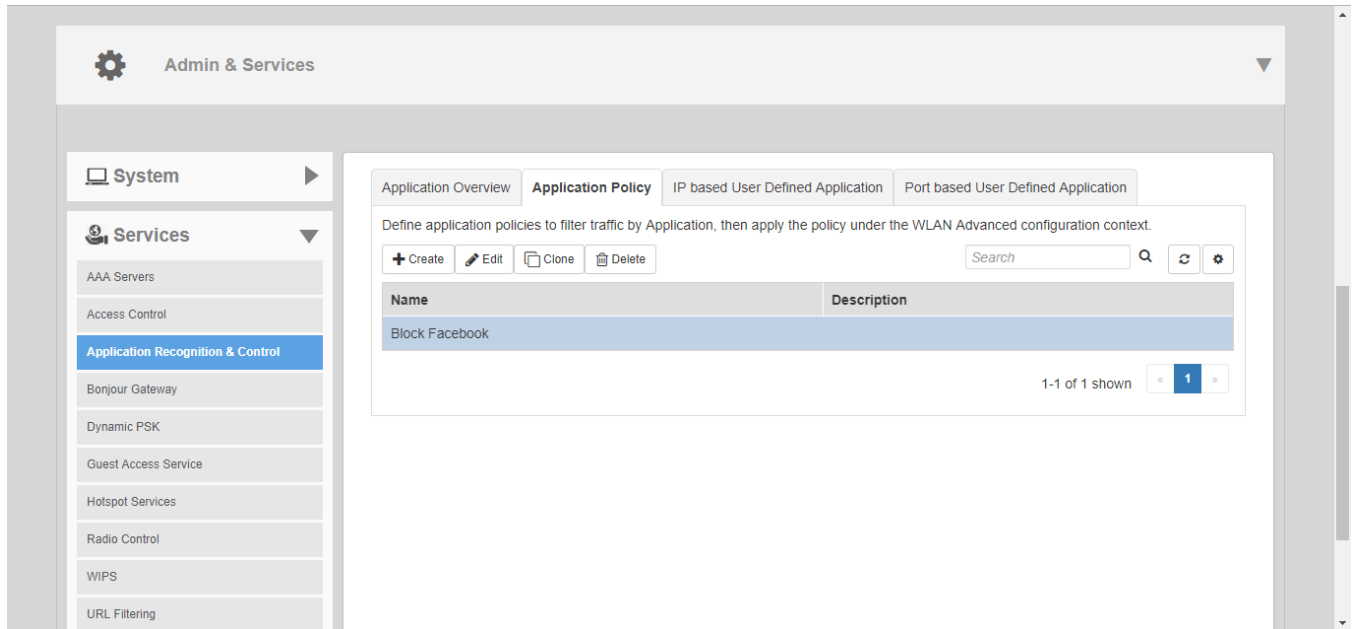
In addition to creating an Application Policy directly from the WLAN advanced options configuration screens, you can also create multiple policies from the **Admin & Services > Services > Application Recognition and Control > Application Policy** page, and then apply them to your WLANs one by one from the WLAN advanced options.

To create an Application Policy:

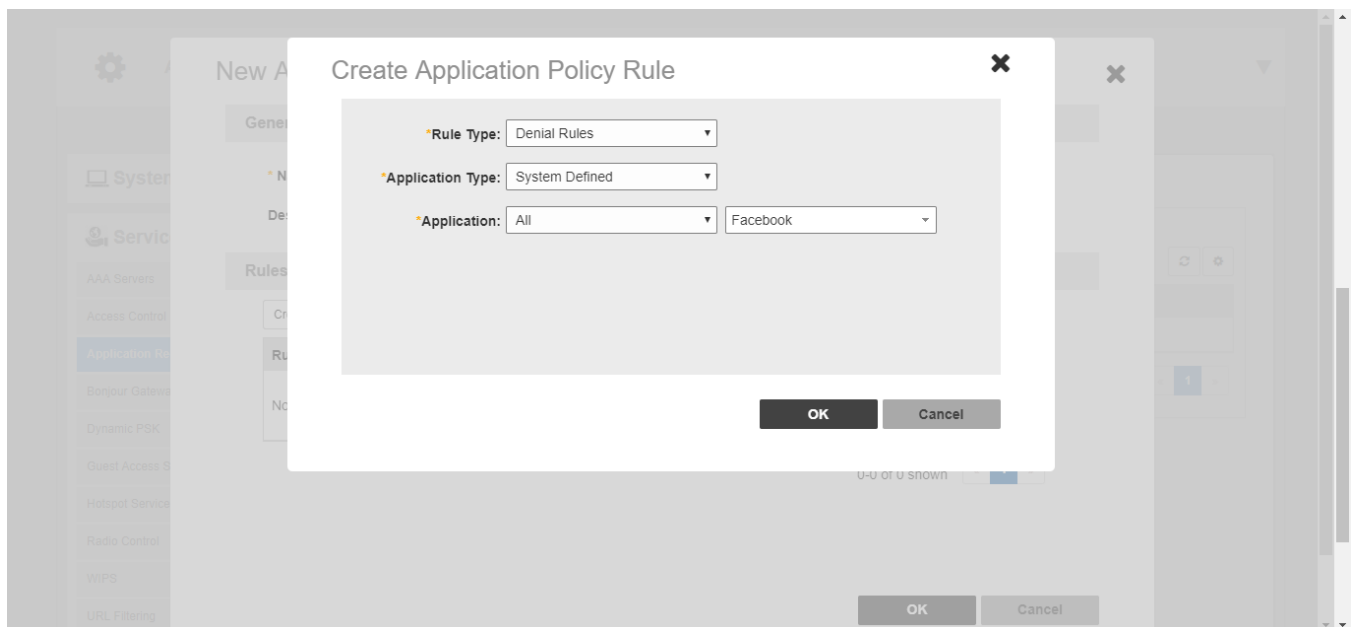
1. Go to **Admin & Services > Services > Application Recognition and Control**, and click the **Application Policy** tab.
2. Click **Create New** to create a new policy.
3. Enter a **Name** and optionally a **Description** for the policy.
4. In **Rules**, click **Create New** to create a new rule for 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 260** Application Policy



**FIGURE 261** 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 181.

## 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:

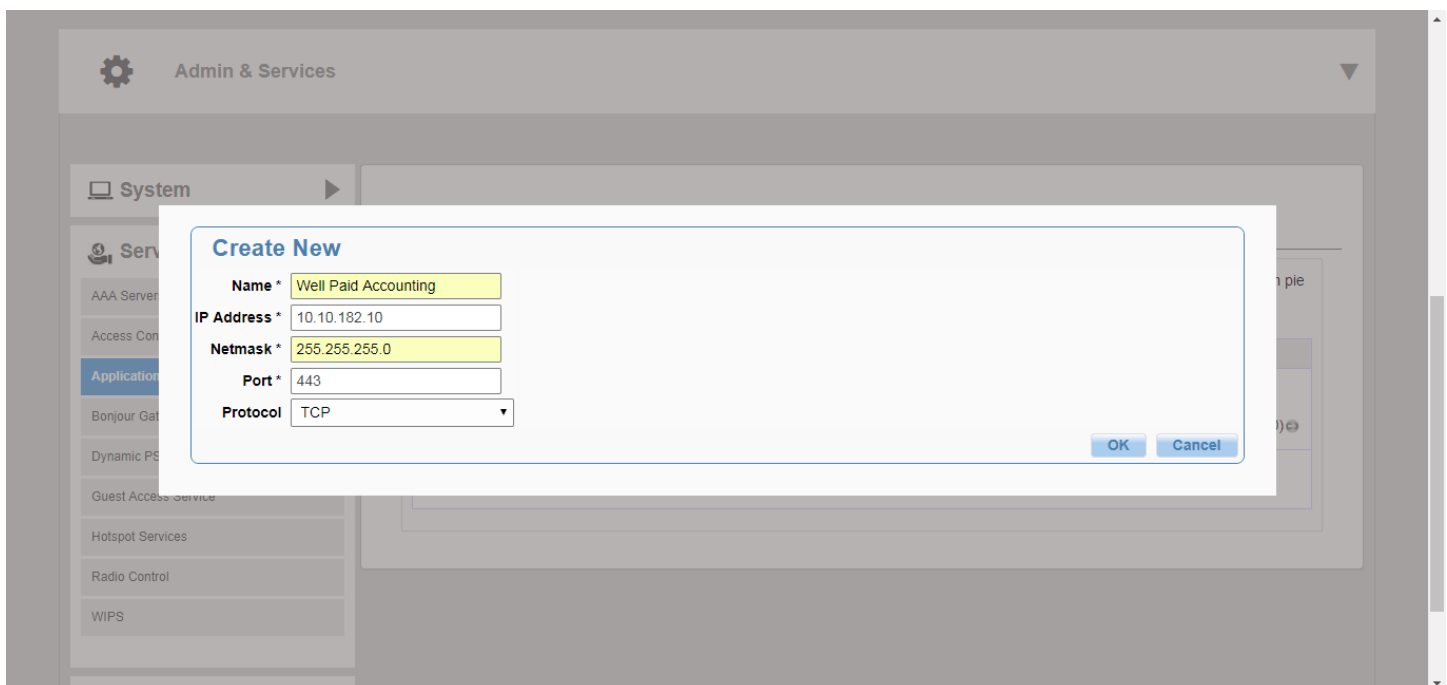
1. IP-based user defined applications
2. System defined applications
3. Port-based user defined applications

## 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 262** Create new IP based User Defined Application



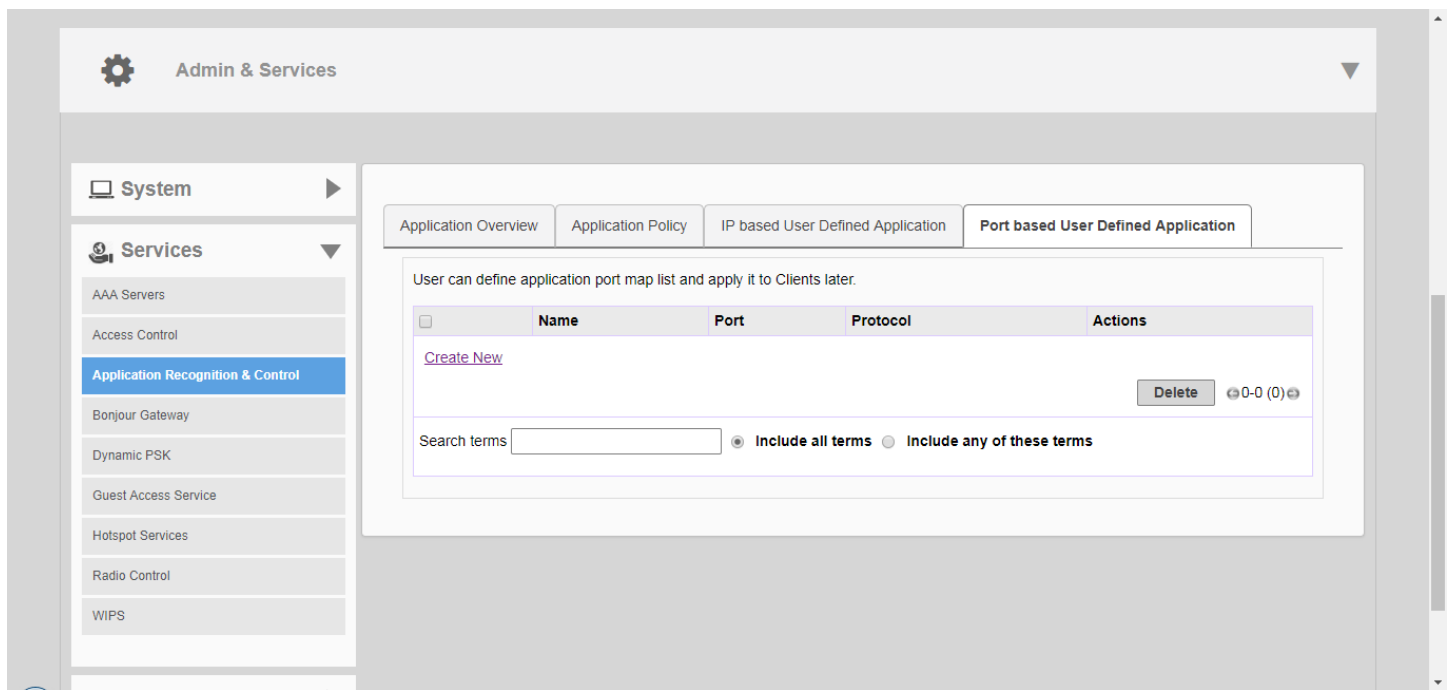
### Port Based User Defined Applications

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.

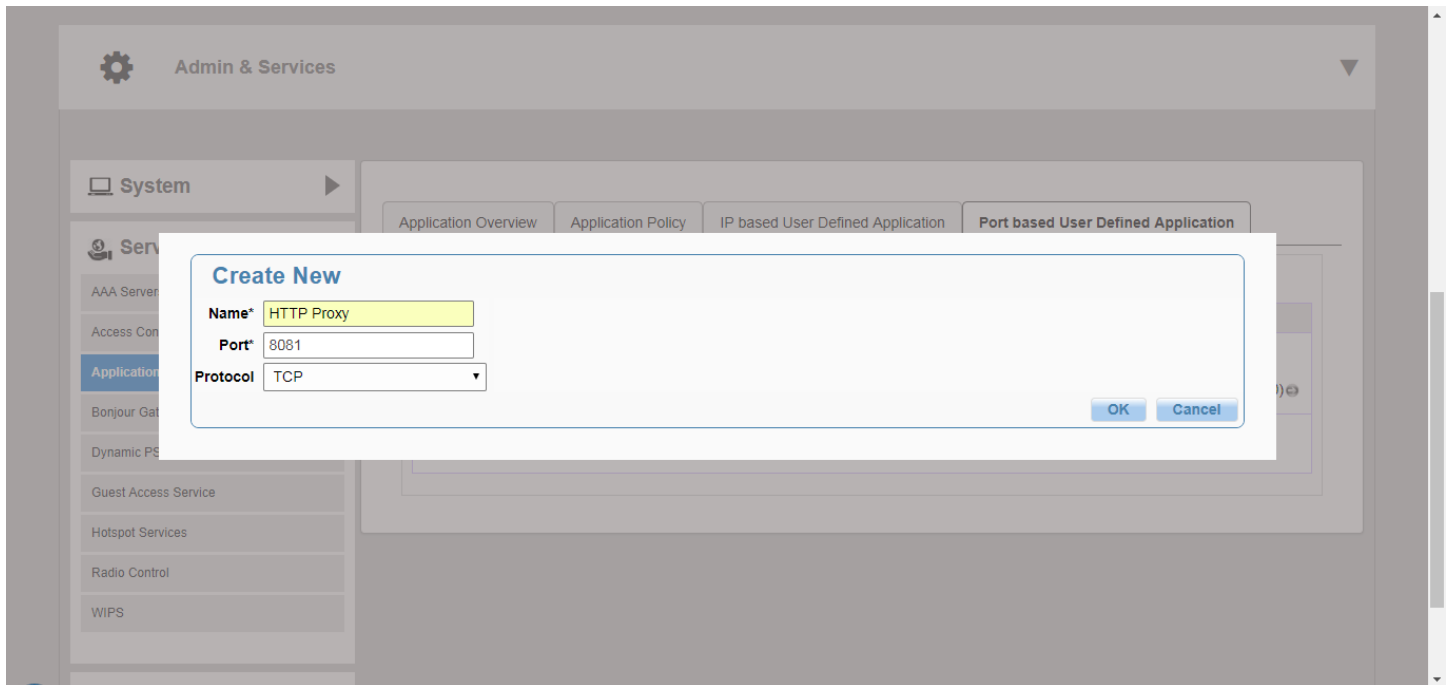
This type of application categorization is the least granular in configuration and hence it has the lowest priority as a means of application identification. If for example you configure a port-based user-defined Application for port 80/TCP, any such matching wireless traffic not identified by either an IP-based application or the default embedded applications will be identified as belonging to this application.

**FIGURE 263** Application Port Mapping



**FIGURE 264** 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.

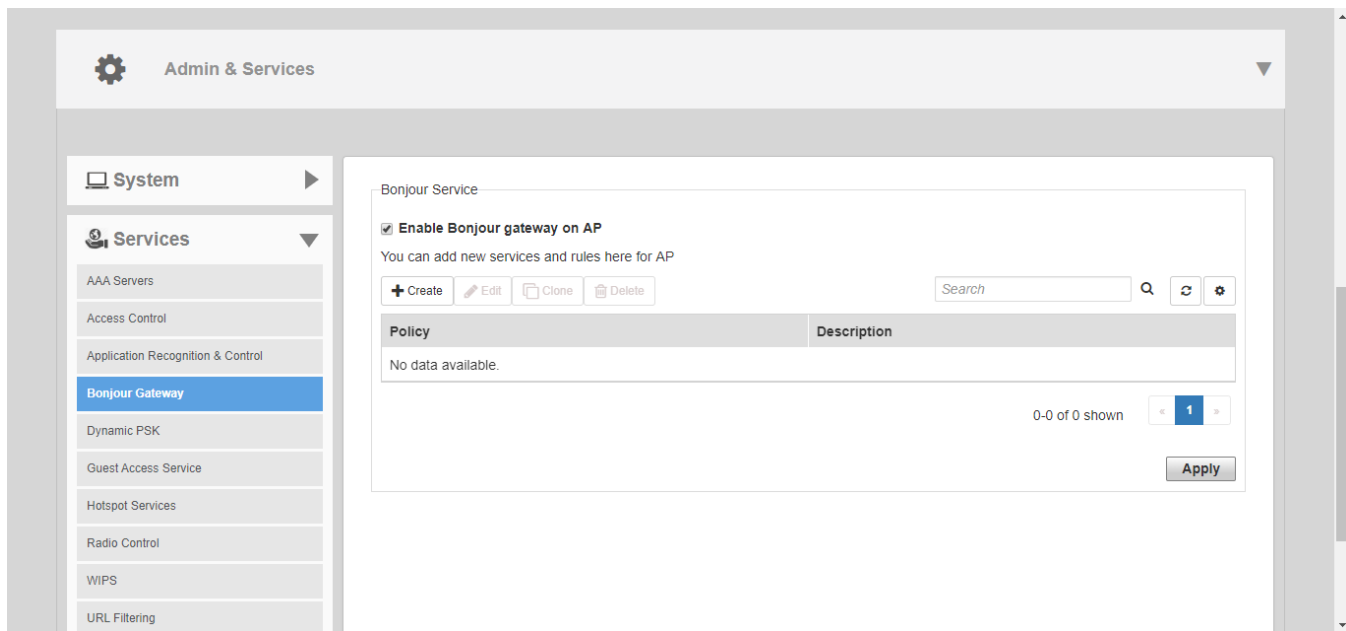
To configure rules for bridging Bonjour services across VLANs:

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.

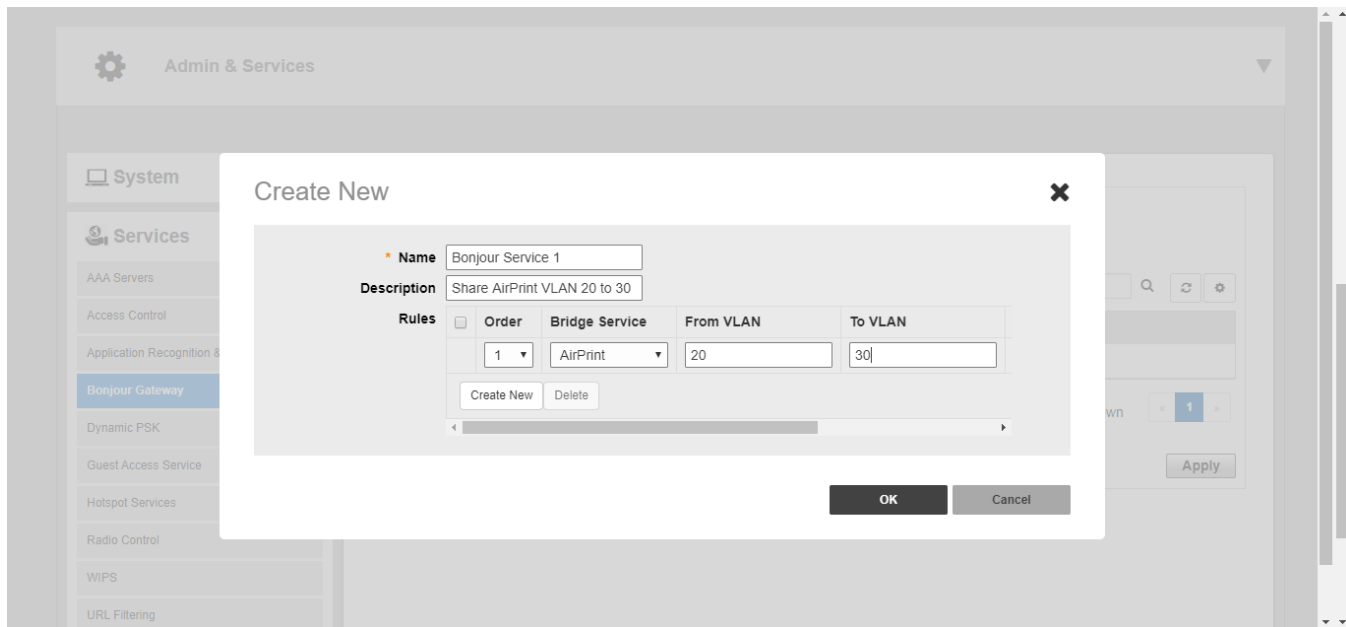


9. Click **Apply** to save the Bonjour Service.

**FIGURE 265** Bonjour Gateway configuration



**FIGURE 266** 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

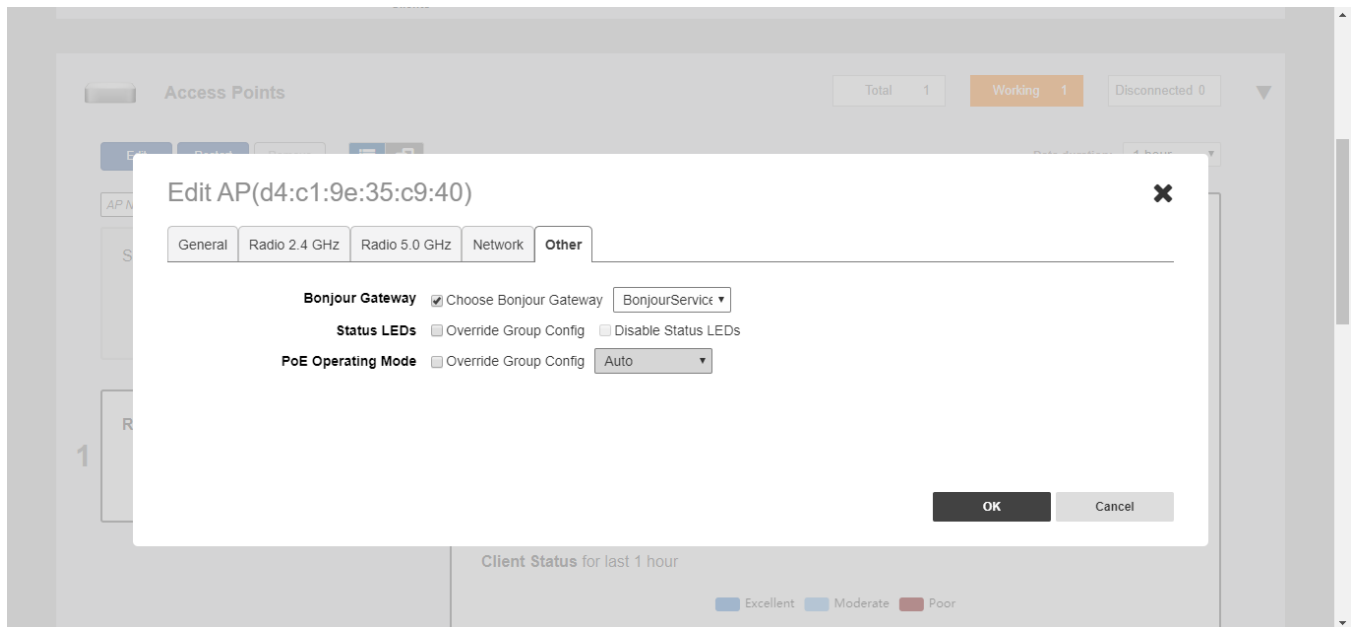
Bonjour services can consume significant memory and CPU resources (especially when a large number of rules is created). Therefore, Ruckus recommends deploying the Bonjour services to an AP that is *not* the Unleashed Master AP.

### 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 267** Select Bonjour service to be deployed on an AP



## Dynamic PSK

Use the *Services > Dynamic PSK* options to generate and manage admin-generated DPSKs.

### Generating DPSKs in Batch

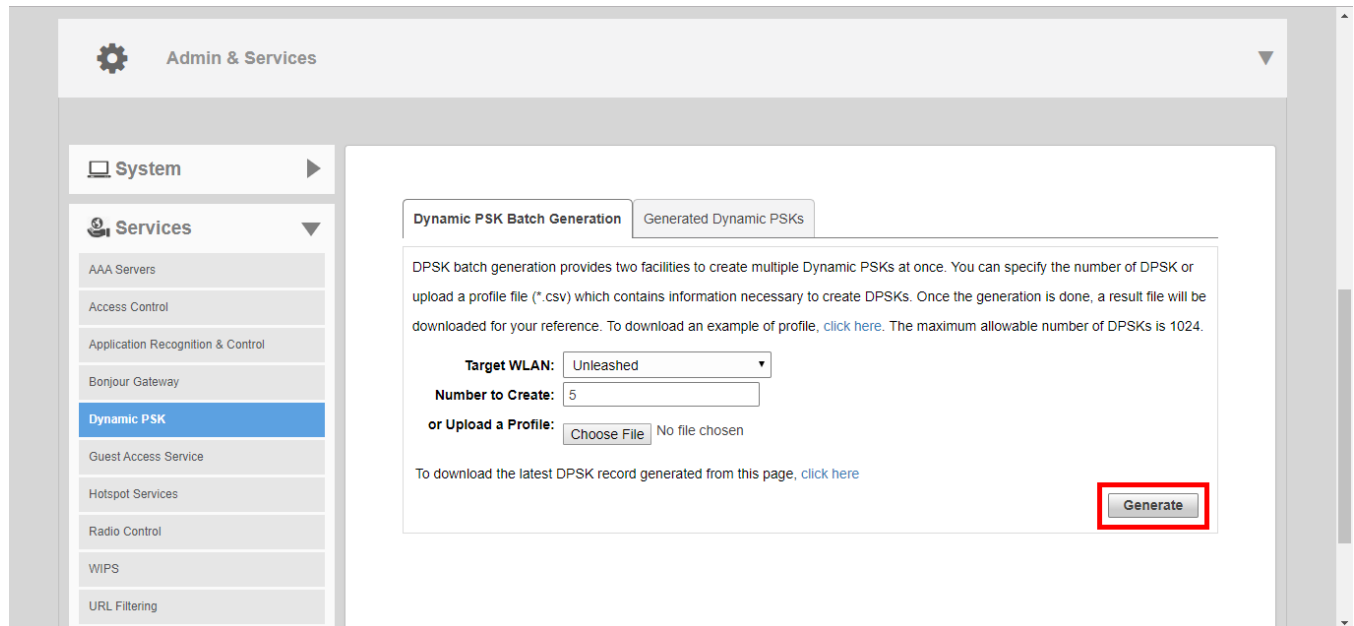
You can create between 1 and 50 Dynamic PSKs at once from the *Dynamic PSK Batch Generation* tab.

To generate DPSKs:

1. Go to *Admin & Services > Services > Dynamic PSK*.

2. In *Dynamic PSK Batch Generation*, enter the following options:
  - **Target WLAN:** Select the WLAN to which the DPSKs will be applied. (A WLAN with DPSK enabled must exist before this feature is available.)
  - **Number to Create:** Enter a number of DPSKs to generate (1-50, default 5).
  - **Upload a Profile:** Refer to *Uploading a Dynamic PSK Profile*.
3. Click **Generate** to generate the requested number of keys.

**FIGURE 268** Create DPSKs automatically



4. Click the *Generated Dynamic PSKs* tab to view the keys you created.

### Uploading a Dynamic PSK Profile

Use this procedure to batch generate multiple DPSKs using a csv file that can be edited in a spreadsheet program (such as Microsoft Excel).

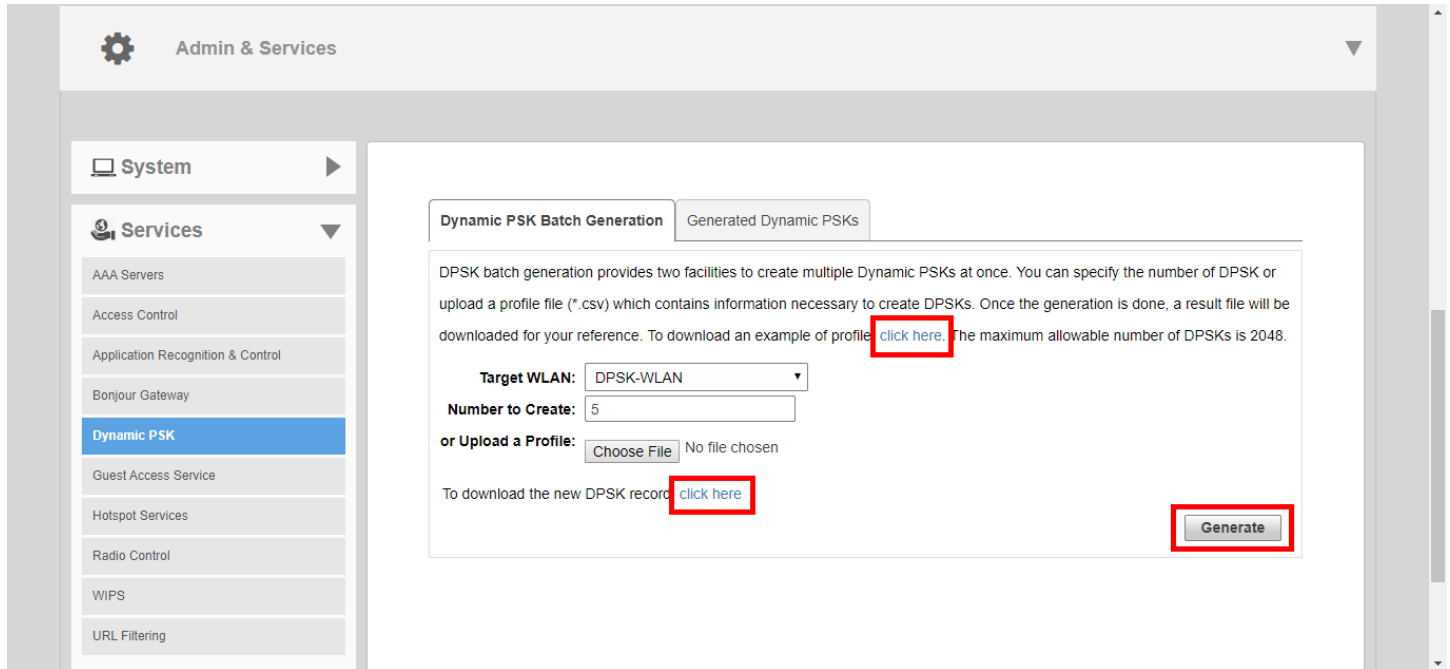
Creating a DPSK batch generation profile is useful if you want to customize the user names that will be used for accessing the DPSK WLAN, as opposed to user names such as "BatchDPSK\_User\_1," etc.

1. Go to **Admin & Services > Services > Dynamic PSK**.
2. In the **Dynamic PSK Batch Generation** tab, 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) Type the name of the user (one name per row).
  - **MAC Address:** (Optional) If you know the MAC address of the device that the user will be using, type it here.
6. Go back to the **Dynamic PSK Batch Generation** screen, and click the **Choose File** button to upload the CSV file you edited.
7. Select the **Target WLAN** and **Number to Create**.

8. 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) by clicking the **Click Here** link at the end of the "To download the generated DPSK record,click here" sentence.

**FIGURE 269** Dynamic PSK batch generation



## Viewing Generated DPSKs

In addition to downloading the generated DPSK record in CSV format, you can also view the DPSKs that have been generated from the *Generated Dynamic PSKs* tab.

**FIGURE 270** Viewing generated DPSKs

The screenshot shows the 'Admin & Services' interface. On the left, the 'Services' menu is expanded to 'Dynamic PSK'. The main area has two tabs: 'Dynamic PSK Batch Generation' and 'Generated Dynamic PSKs'. The 'Generated Dynamic PSKs' tab is active, showing a table with the following data:

<input type="checkbox"/>	User	MAC Address	WLANs	Created	Expires
<input type="checkbox"/>	BatchDPSK_User_1	00:00:00:00:00:00	Unleashed	2019/09/06 12:52:38	Unlimited
<input type="checkbox"/>	BatchDPSK_User_2	00:00:00:00:00:00	Unleashed	2019/09/06 12:52:38	Unlimited
<input type="checkbox"/>	BatchDPSK_User_3	00:00:00:00:00:00	Unleashed	2019/09/06 12:52:38	Unlimited
<input type="checkbox"/>	BatchDPSK_User_4	00:00:00:00:00:00	Unleashed	2019/09/06 12:52:38	Unlimited
<input type="checkbox"/>	BatchDPSK_User_5	00:00:00:00:00:00	Unleashed	2019/09/06 12:52:38	Unlimited

Below the table, there is a search section with a text input field, radio buttons for 'Include all terms' (selected) and 'Include any of these terms', and buttons for 'Delete All', 'Delete', and a pagination indicator '1-5 (5)'.

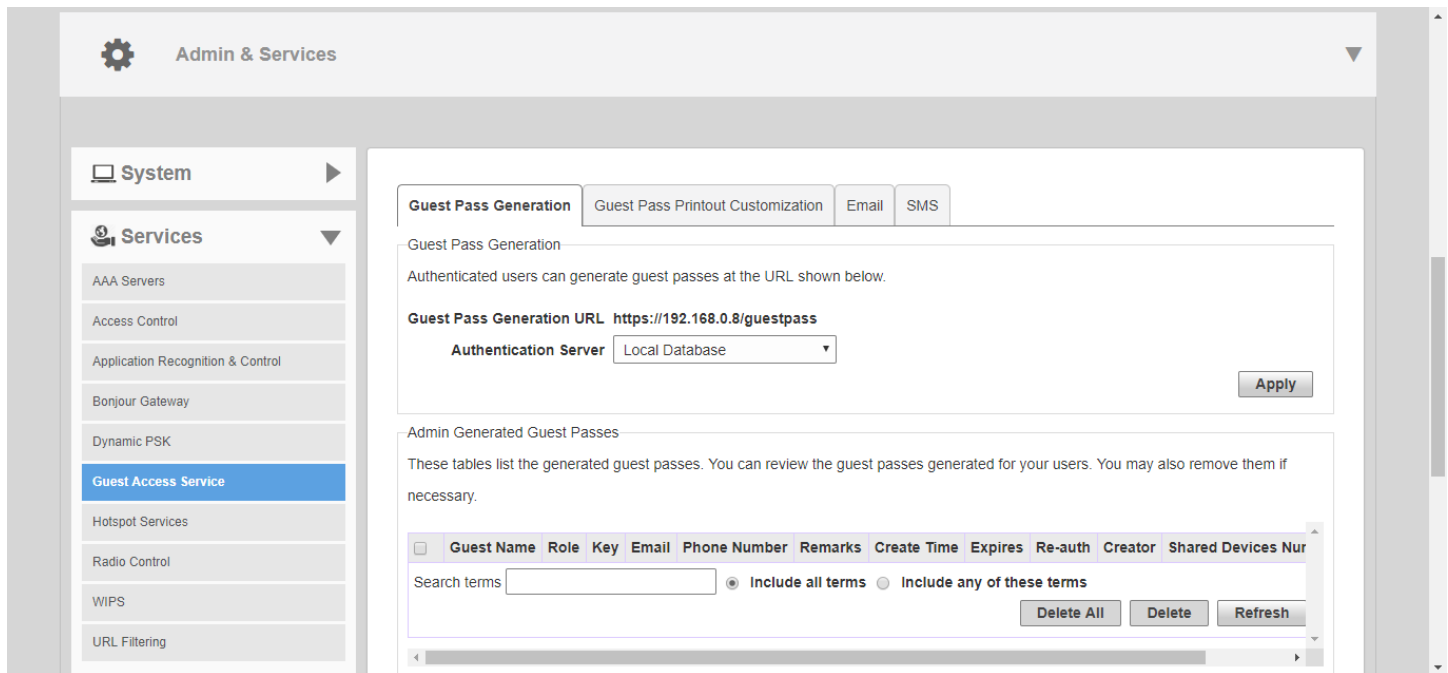
## Guest Access Services

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 115 in *Creating a New WLAN*.

FIGURE 271 Monitor and configure guest pass options from the Admin & Services > Services > Guest Access Service page



## 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](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 181 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 329.

FIGURE 272 The Hotspot Services page

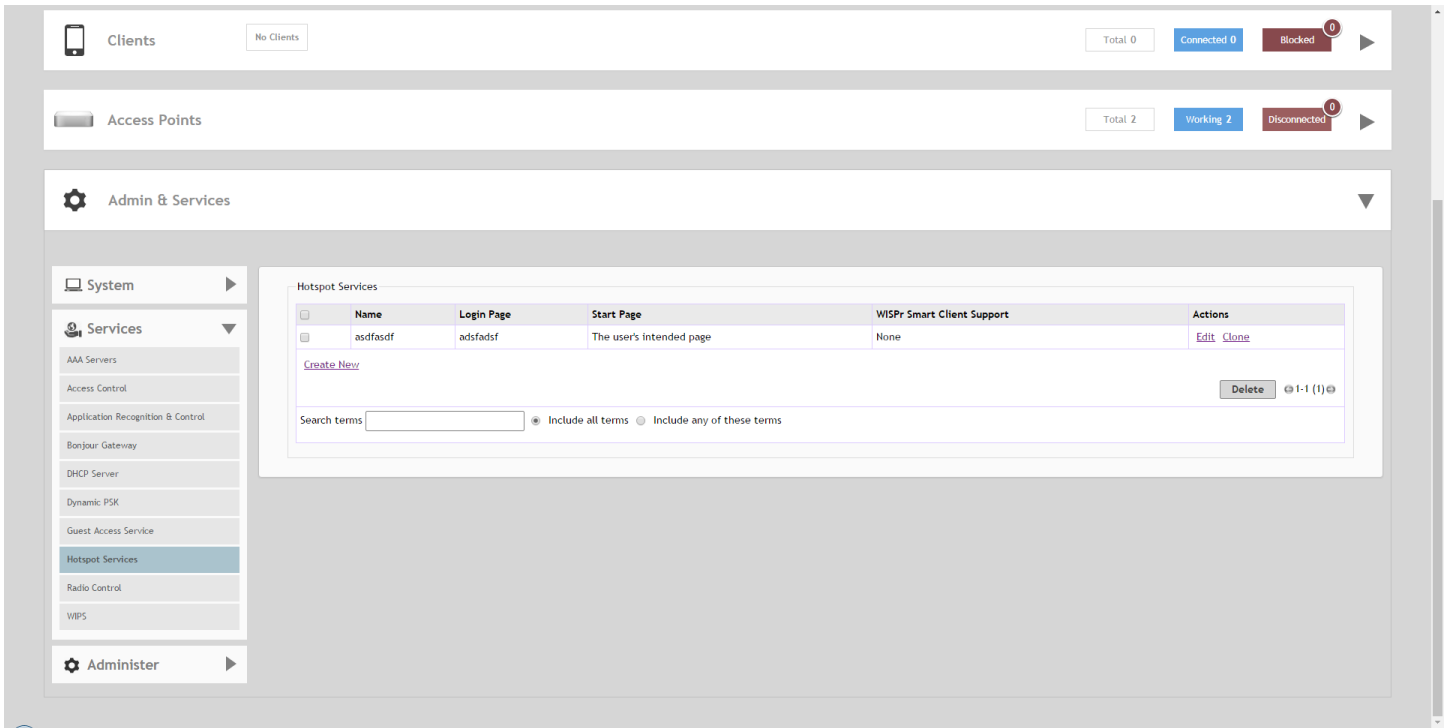
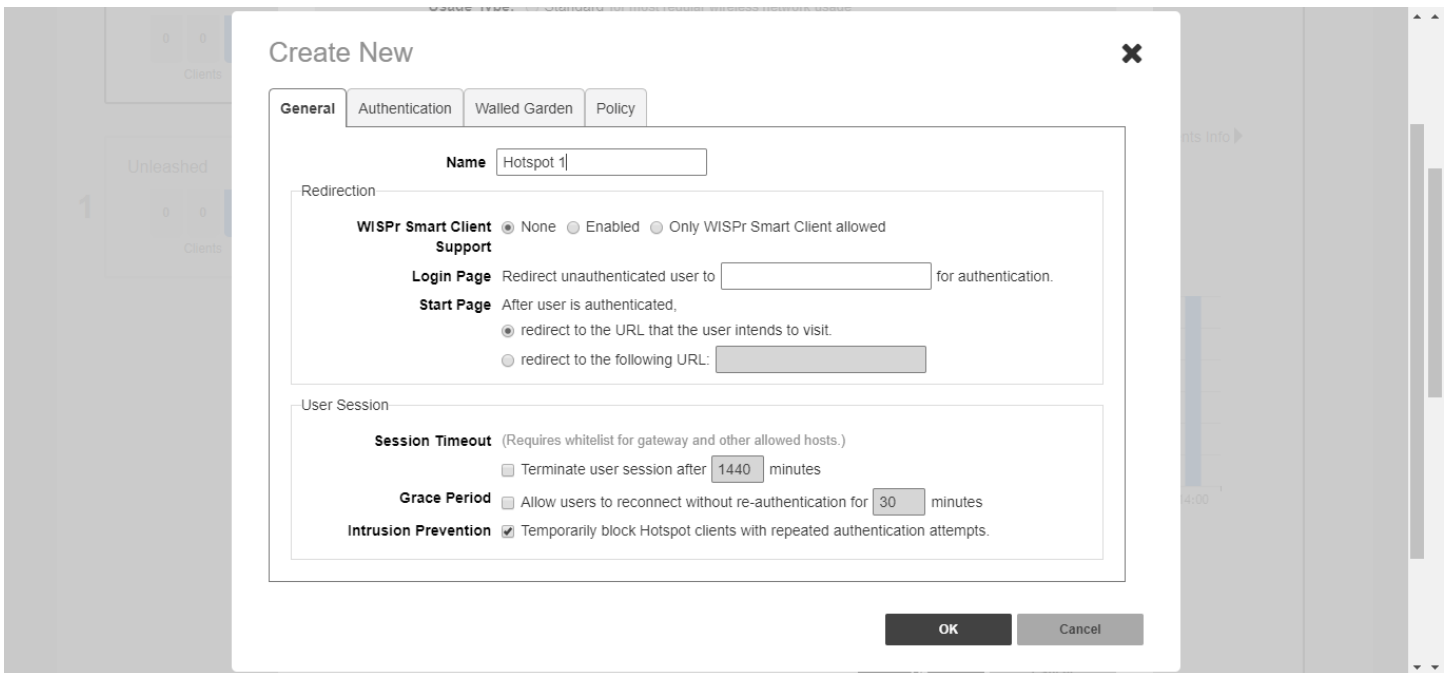


FIGURE 273 Creating a new Hotspot service





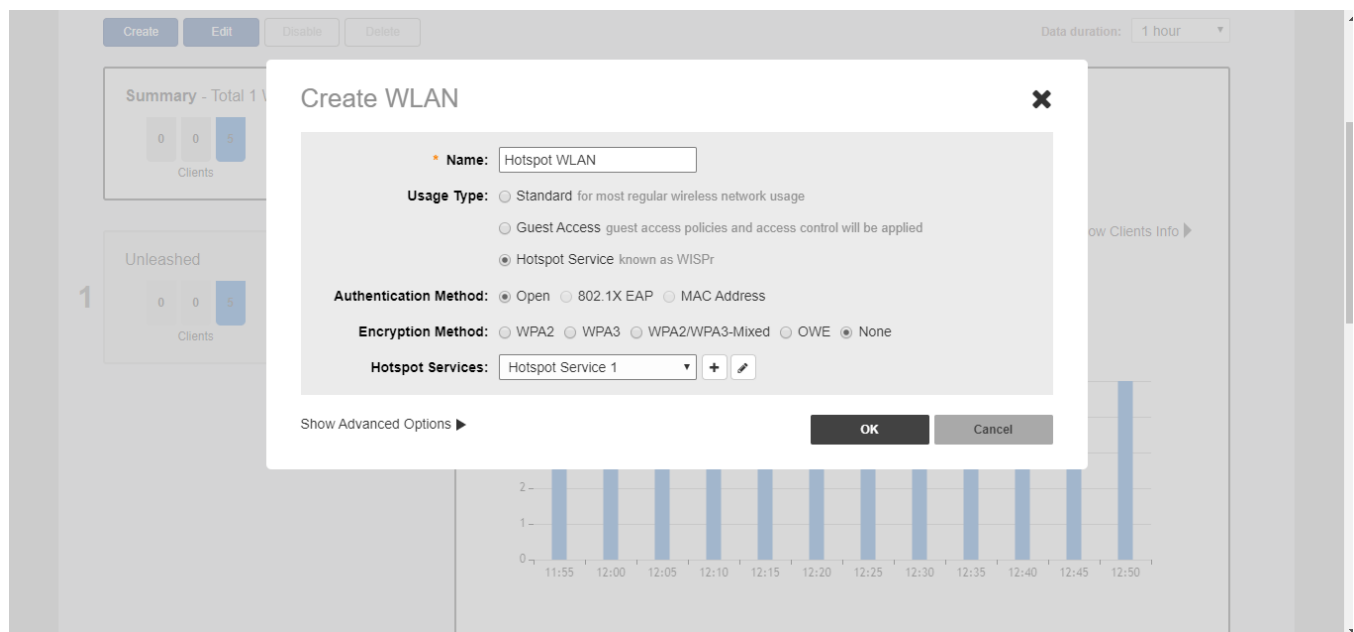
## Assigning a WLAN to Provide Hotspot Service

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 326).
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 274** 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

Unleashed uses built-in network "self healing" diagnostics and tuning tools to maximize wireless network performance.

### Automatically Adjust AP Radio Power

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 Unleashed 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 Unleashed 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 331).

#### 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.

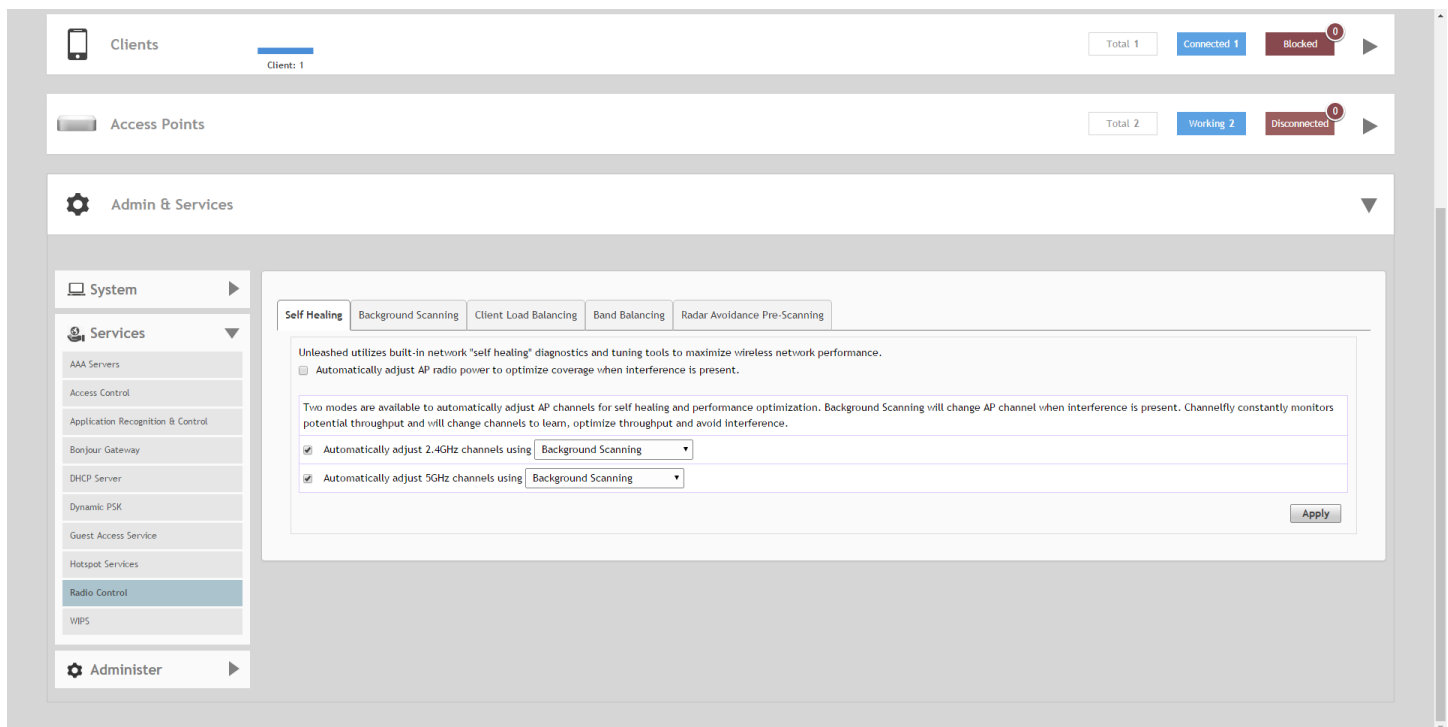
ChannelFly can react to large measured drops in throughput capacity in as little as 15 seconds, while smaller drops in capacity may take longer to react to.

### 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 275 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 20) 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 20) that you want to set between each scan.

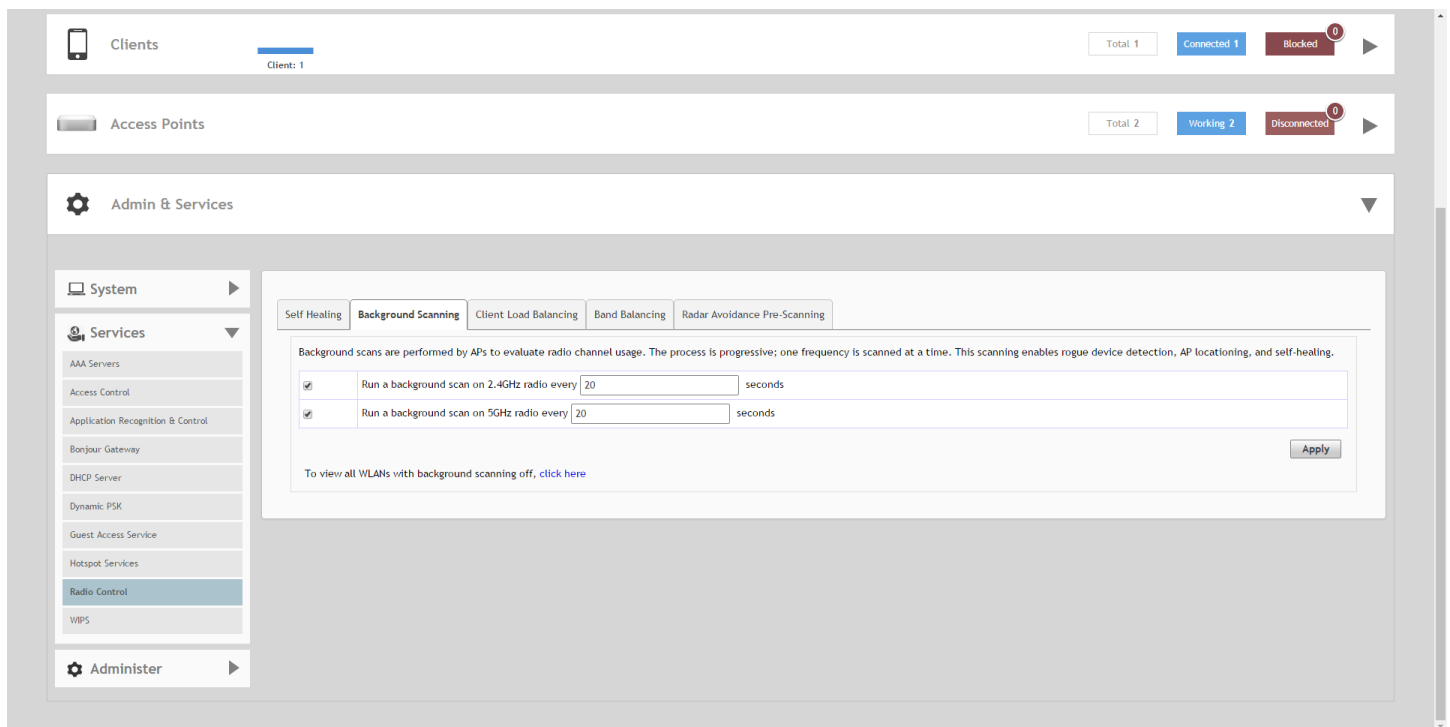
**NOTE**

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**

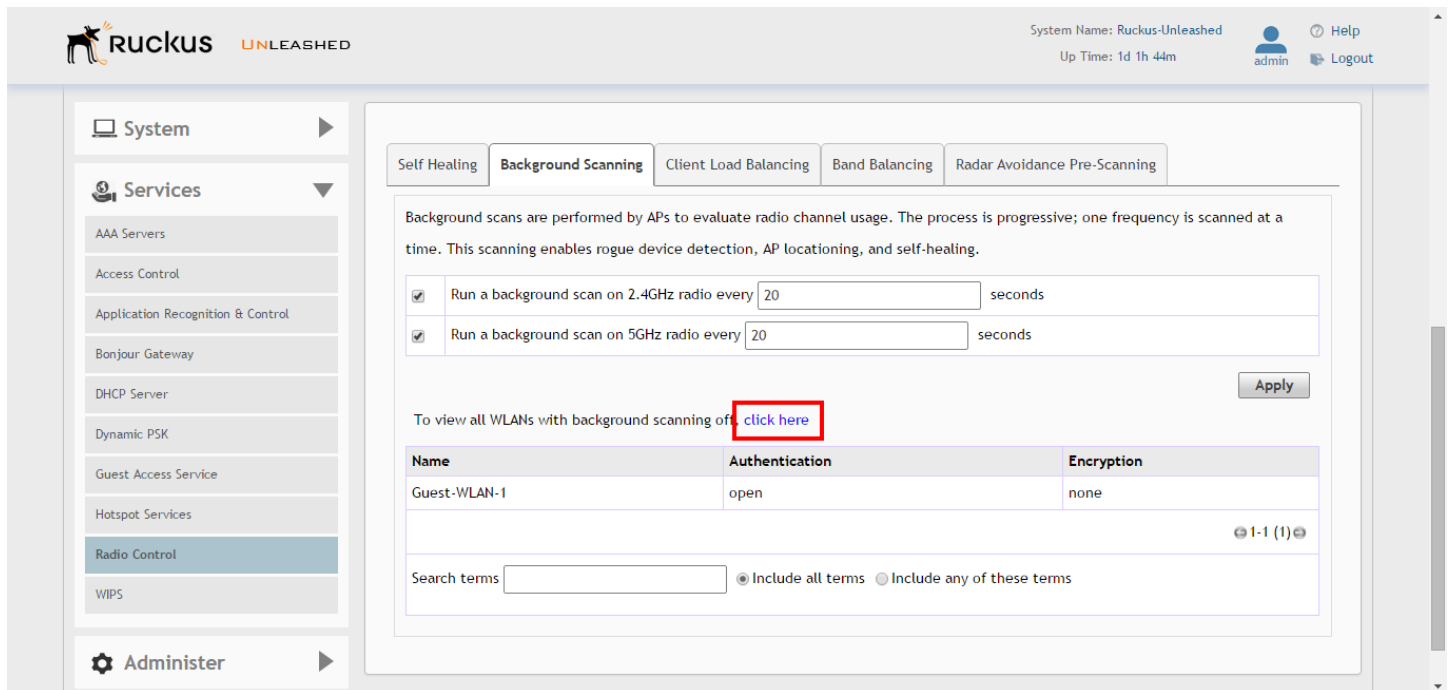
You can also disable Background Scanning on a per-WLAN basis from the **Dashboard > Wi-Fi Networks** screen. To disable scanning for a particular WLAN, click the **Edit** link next to the WLAN for which you want to disable scanning, open **Advanced Options**, select the **Radio Control** tab, and click the check box next to **Disable Background Scanning**.

**FIGURE 276** 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 277 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:

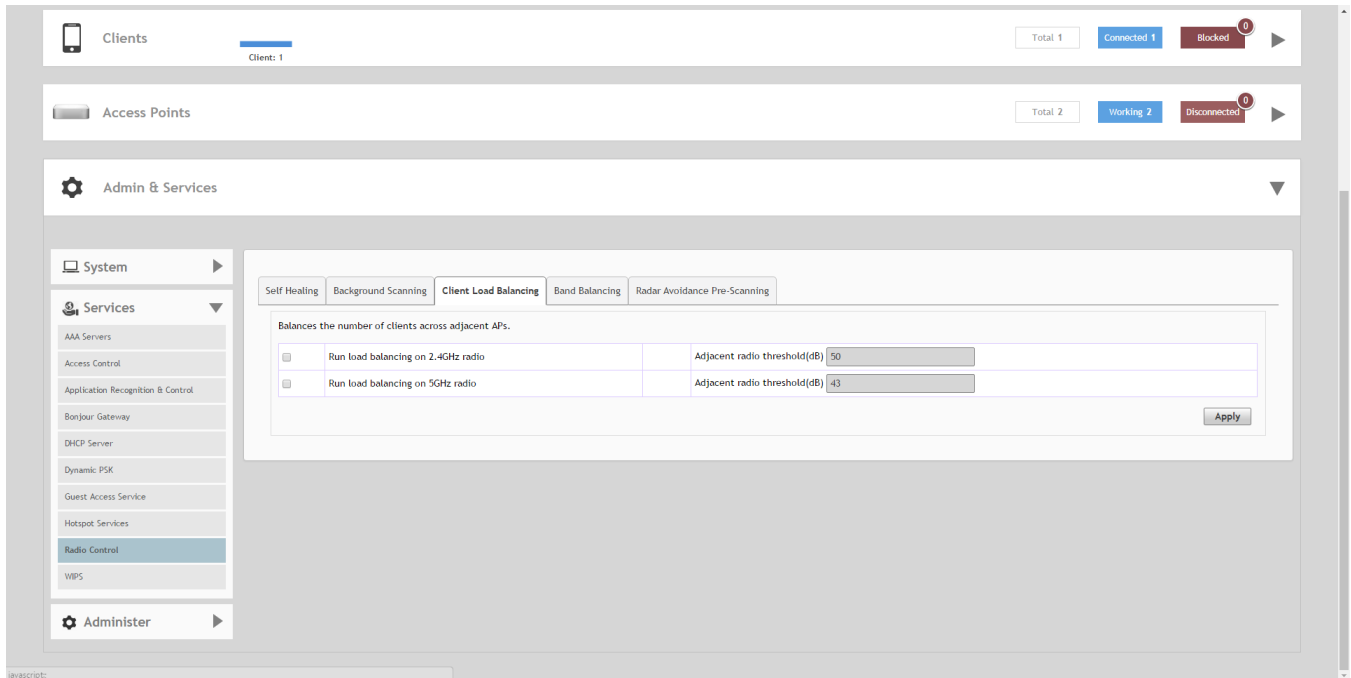
- Load balancing does not disassociate clients already connected.
- Load balancing takes action before a client association request, reducing the chance of client misbehavior.
- The process does not require any time-critical interaction between APs.
- Provides control of adjacent AP distance with safeguards 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 278** Client Load Balancing



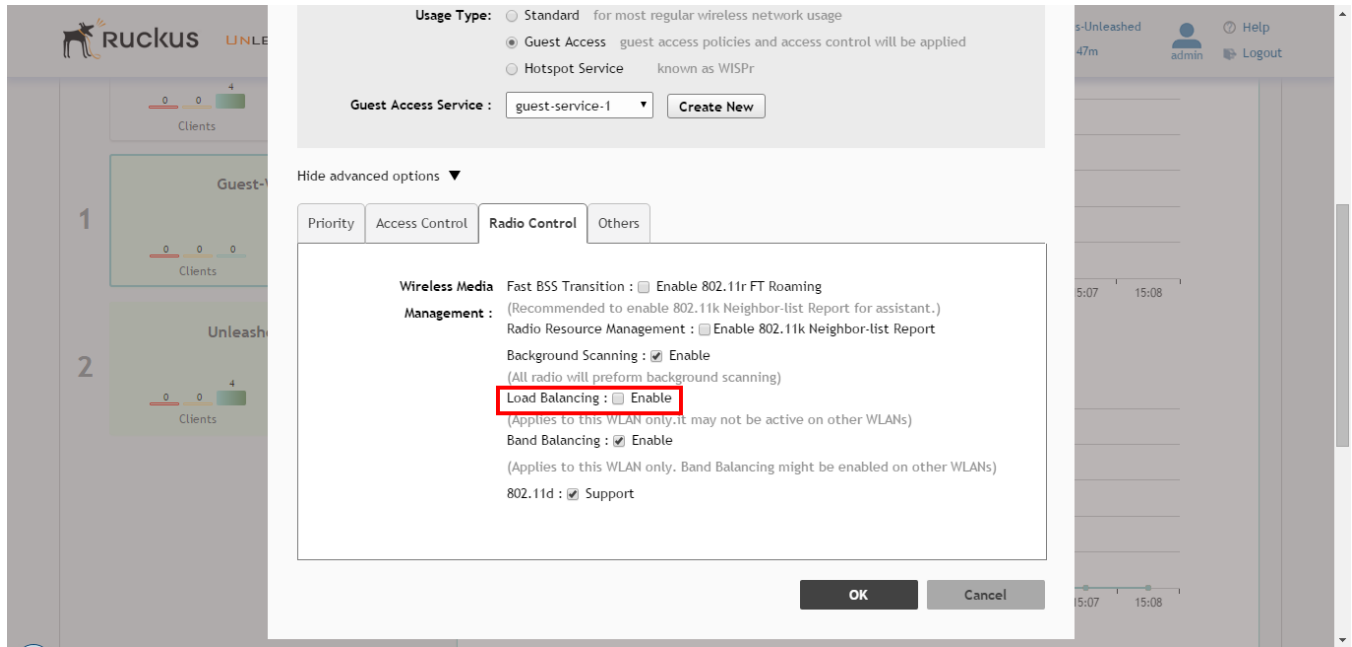
### Disabling Load Balancing for a WLAN

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 279** Disable Load Balancing for a WLAN



## Band Balancing

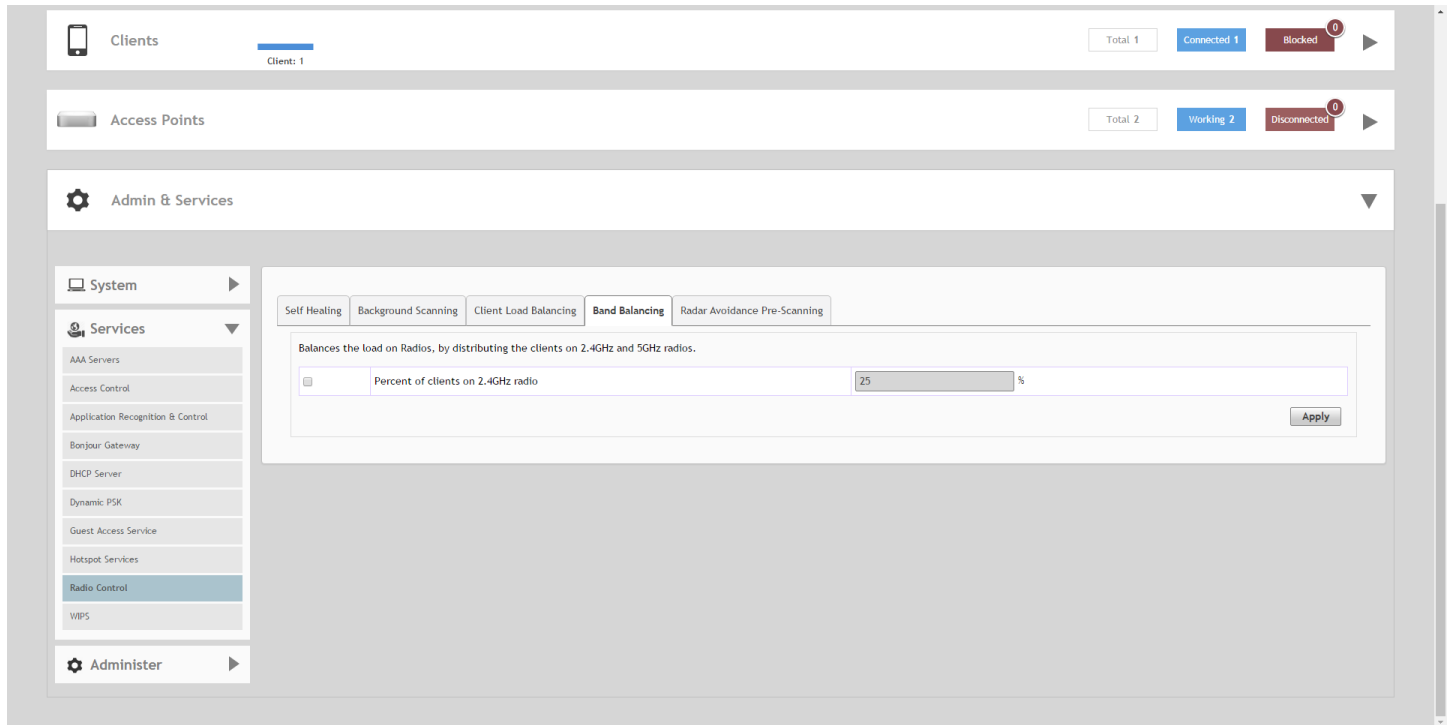
Band balancing attempts to balance the client load on radios by distributing clients between the 2.4 GHz and 5 GHz radios. This feature is disabled by default. To balance the number of clients connecting to the two radios on an AP, the AP encourages dual-band clients to connect to the 5 GHz band when 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 194 for the WLAN using the WLAN Advanced Options.

FIGURE 280 Band Balancing

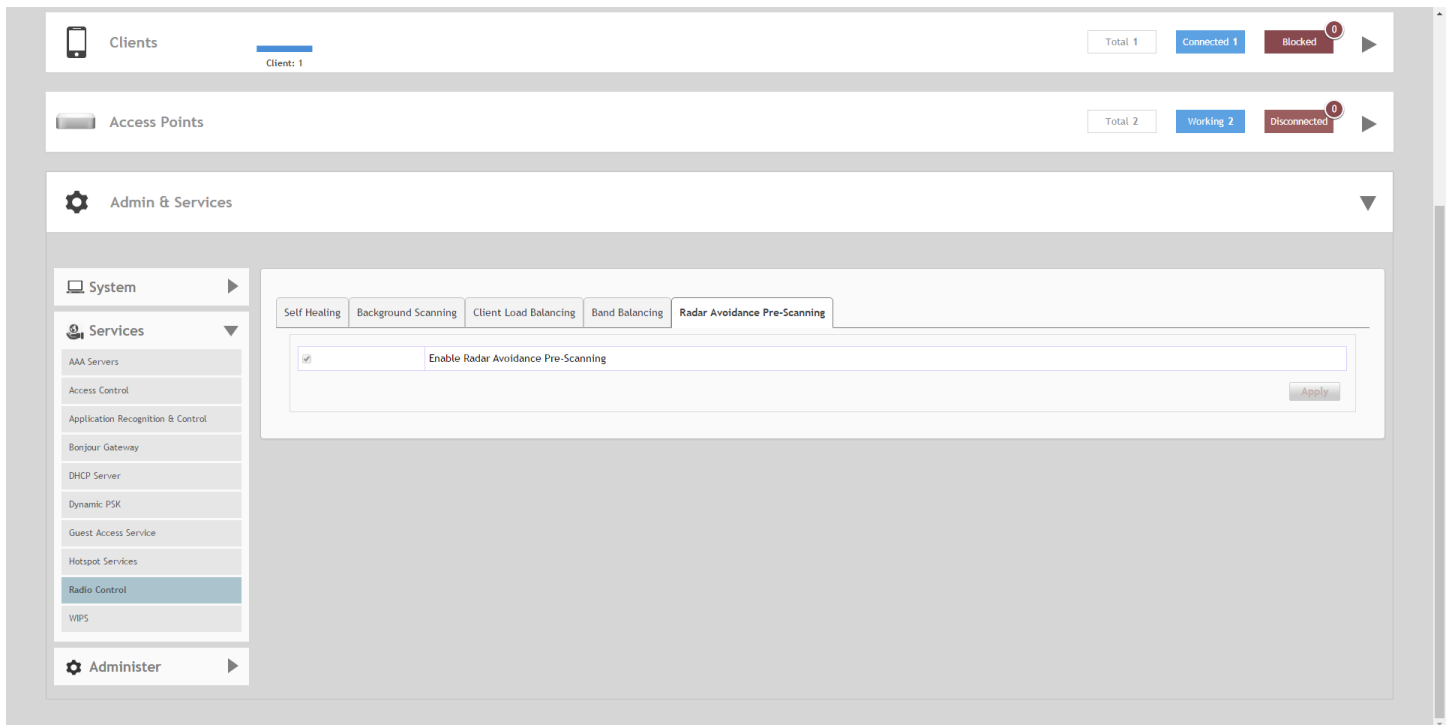


### **Radar Avoidance Pre-Scanning**

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 286).



FIGURE 281 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)

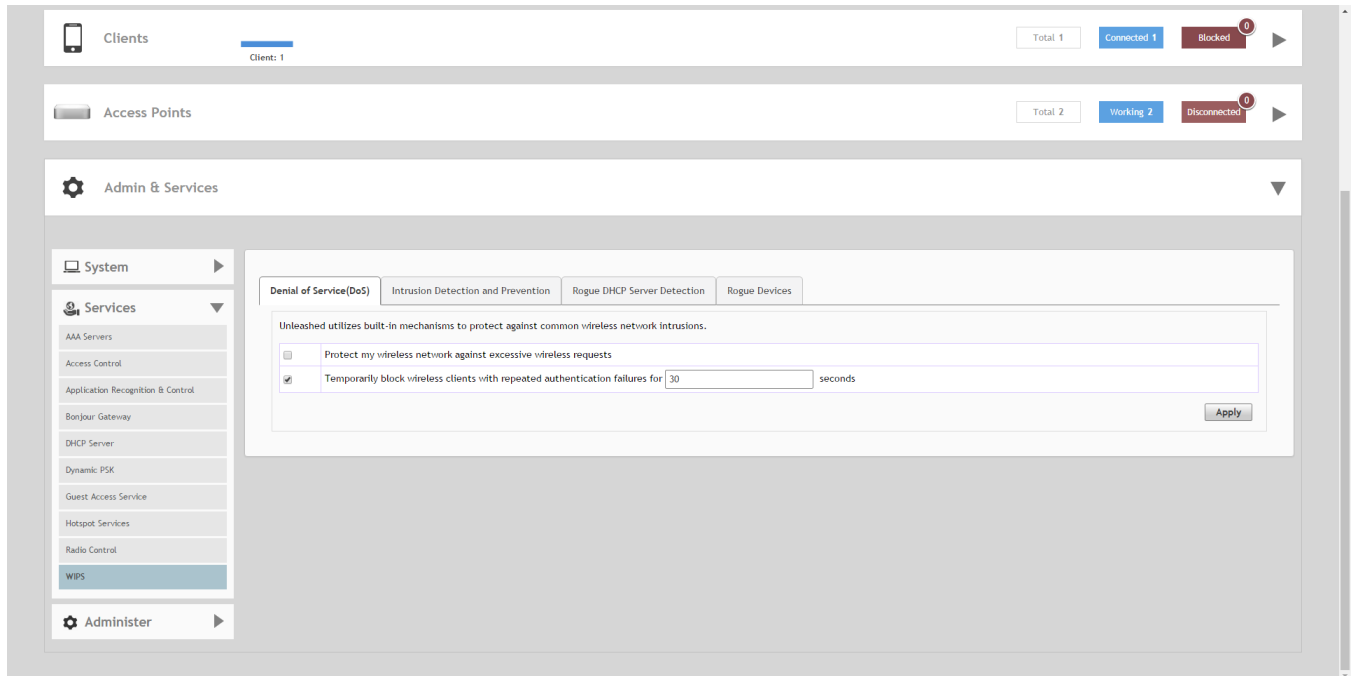
Two options are provided to protect the wireless network from Denial of Service attacks.

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 this capability 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 282** 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.

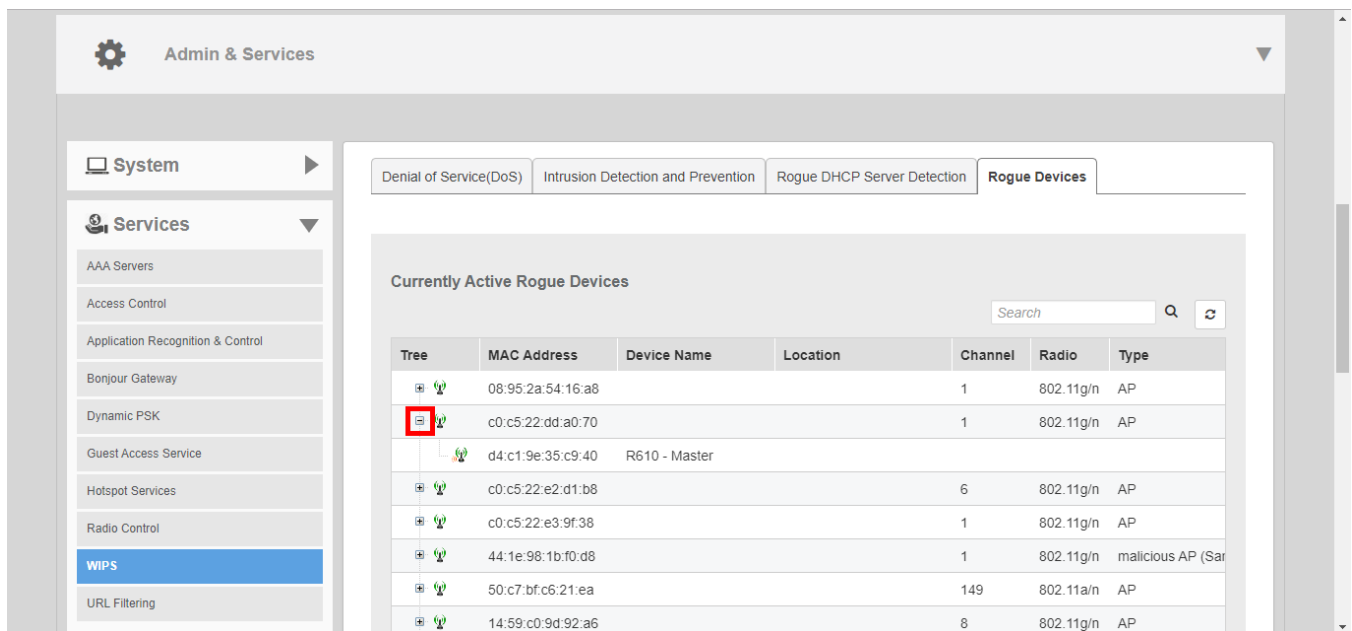
### Managing Rogue Devices

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.

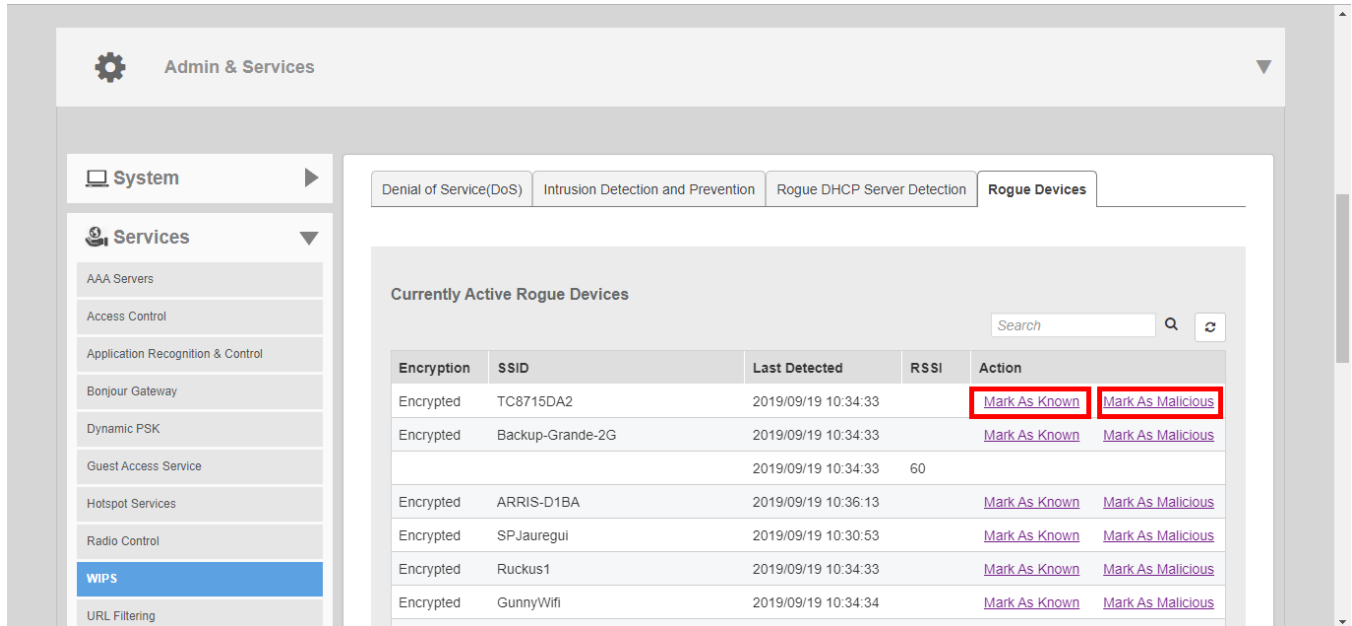
**FIGURE 283** Monitoring rogue devices - expand the view to show which APs are detecting this rogue device



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.

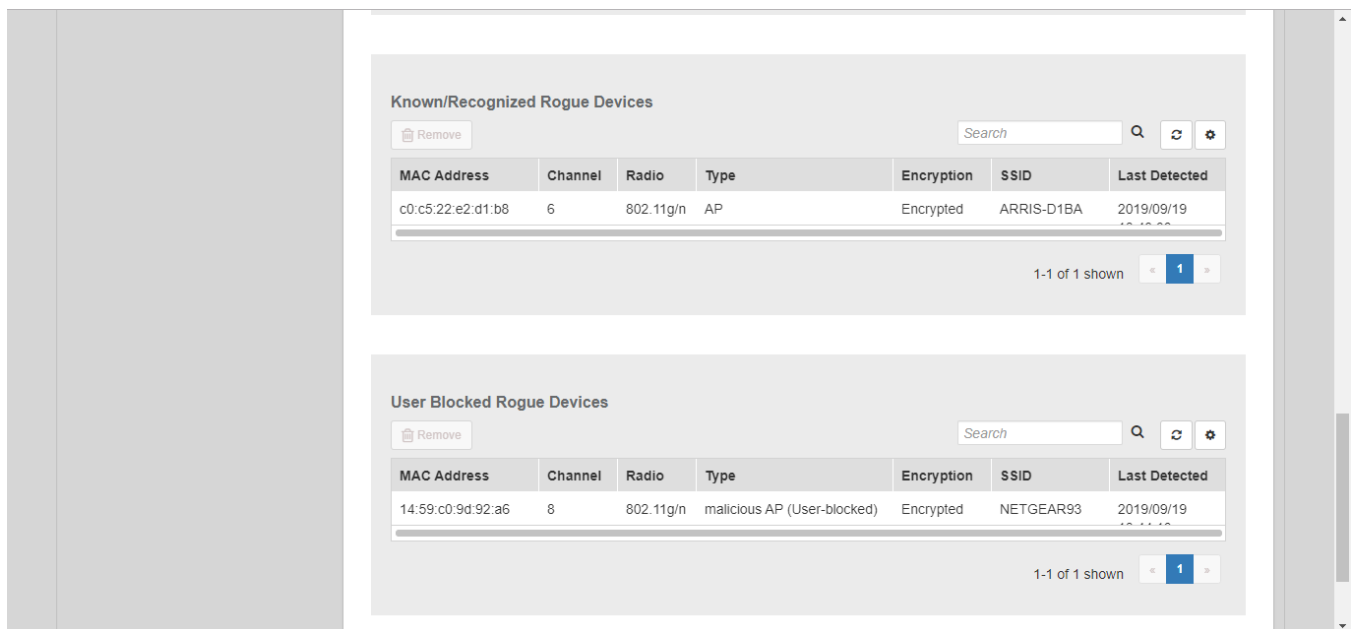
- To mark a rogue device as "Malicious" rogue (with the goal of physically locating and removing the offending device), click **Mark as Malicious**.

**FIGURE 284** Marking rogue devices as known or malicious



- You can monitor and manage the lists of known/recognized and user-blocked rogue devices using the two tables below.

**FIGURE 285** Manage known rogue devices

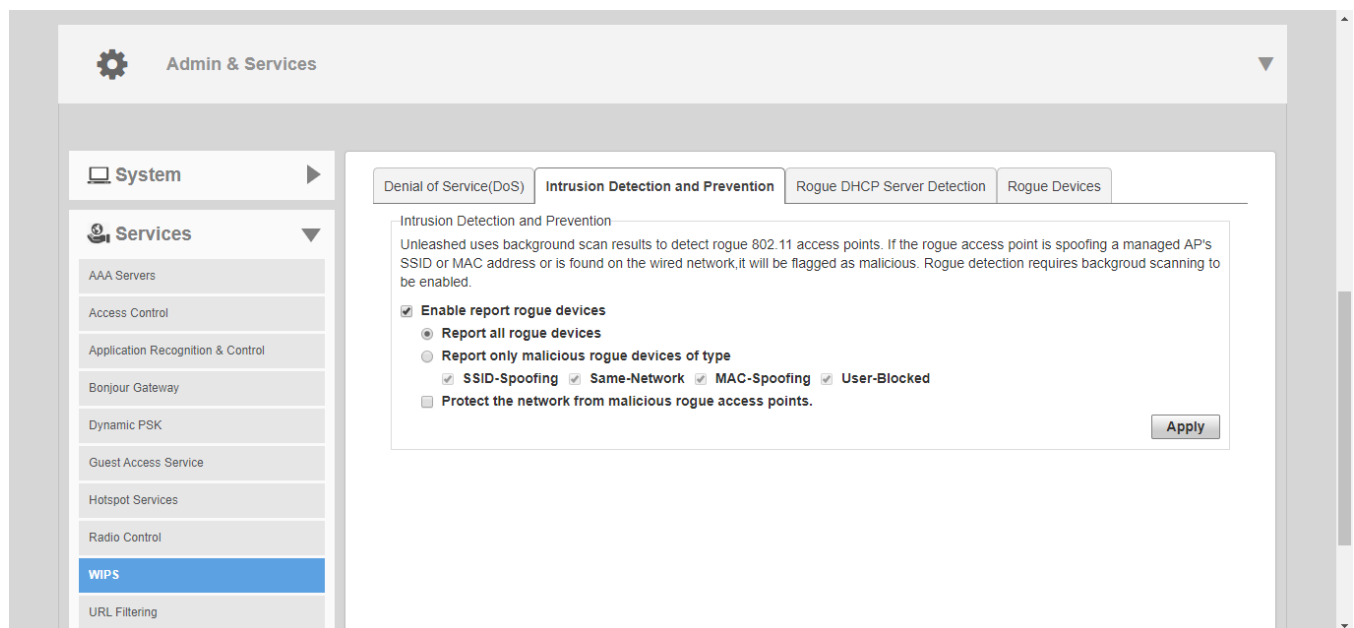


### Rogue AP Detection

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 WLAN (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 286** Intrusion Detection and Prevention



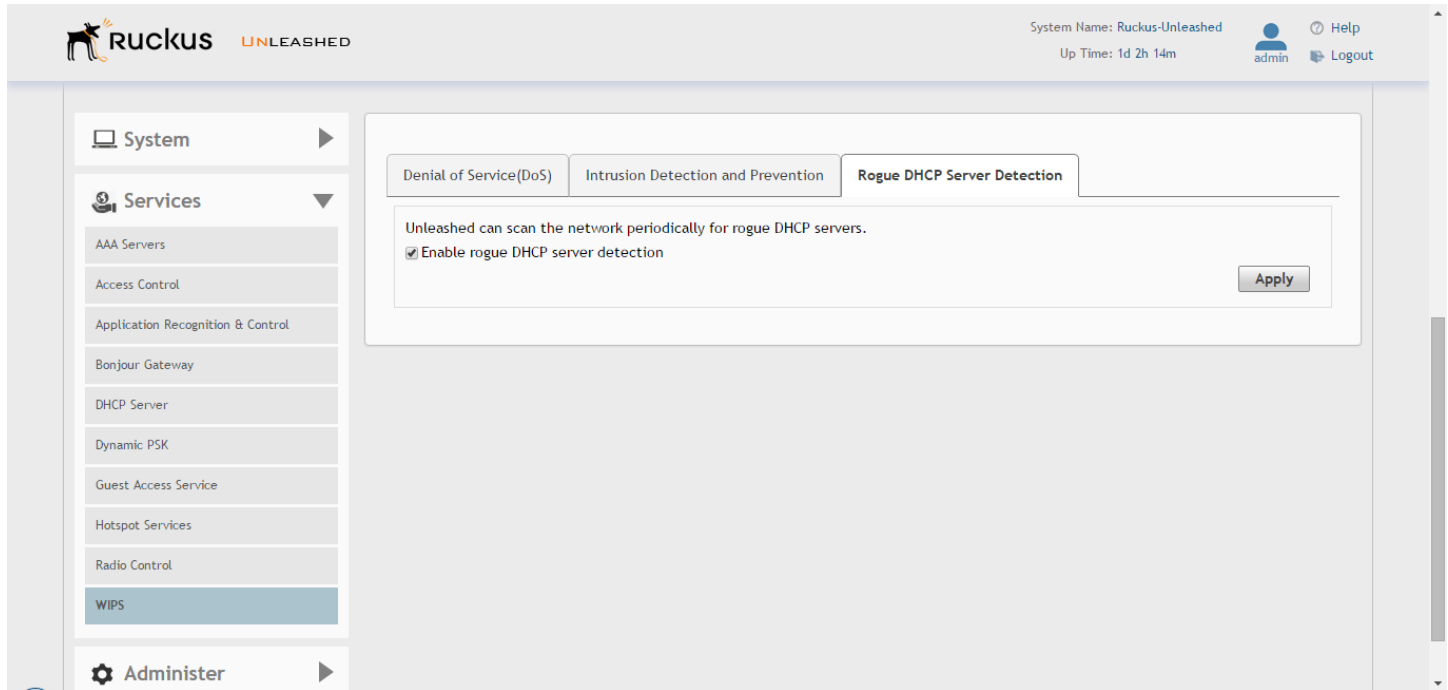
### Rogue DHCP Server Detection

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, Unleashed scans the network every five seconds for unauthorized DHCP servers and generates an event every time it detects a rogue DHCP server.

FIGURE 287 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 blacklists and whitelists.

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>).

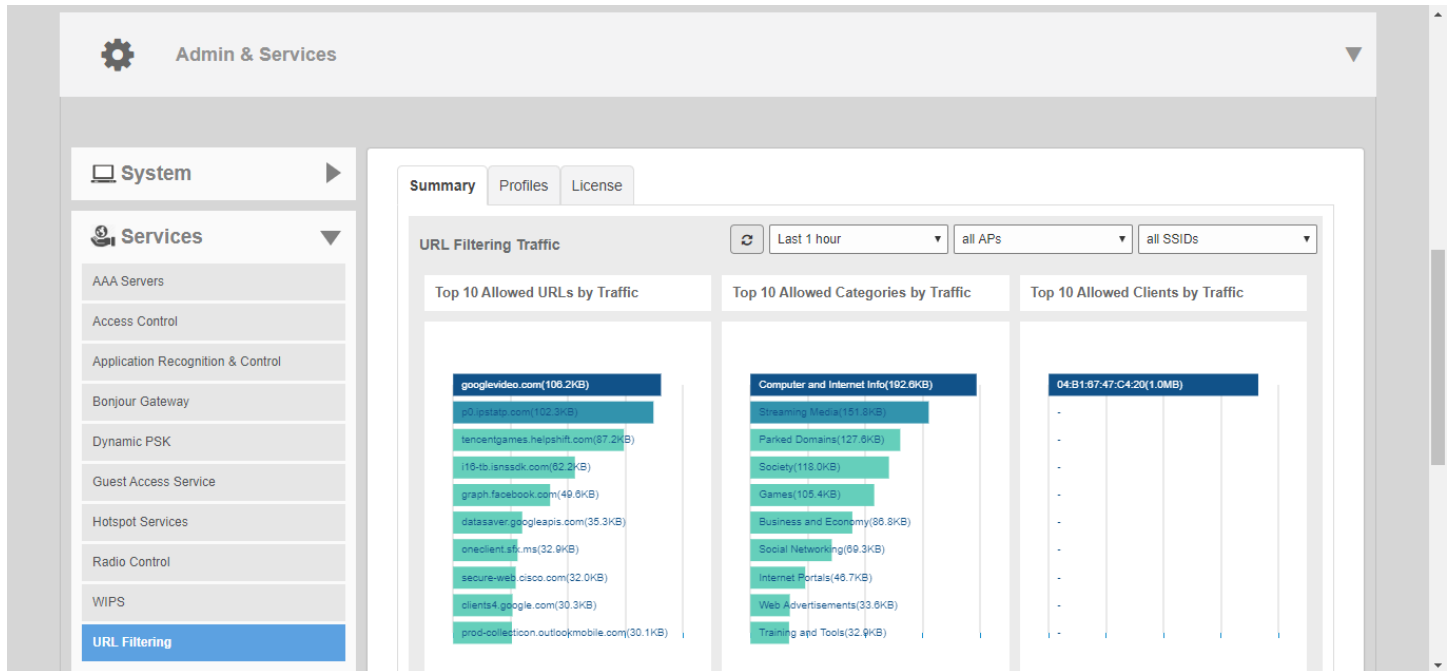
To deploy URL filtering, you must create a URL filtering profile using either one of the preset category groups or a customized selection of categories. Once a profile is created, you can apply it to one or more WLANs.

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 288 URL Filtering



### Creating a URL Filtering Profile

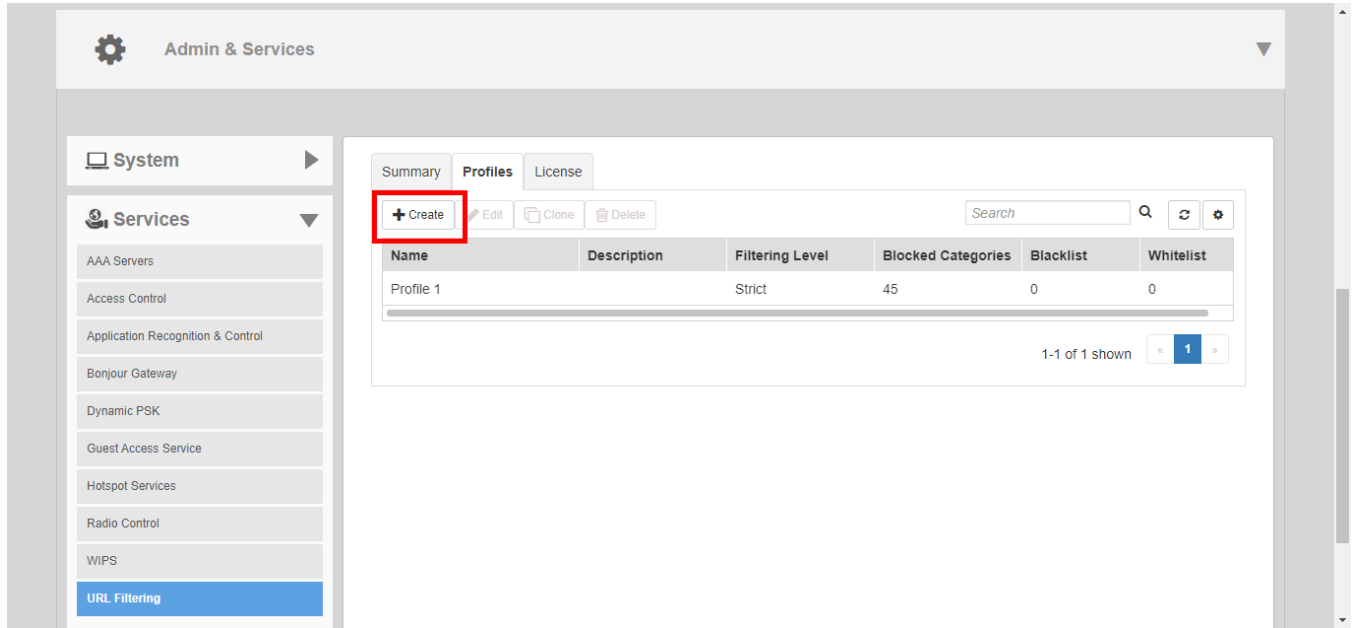
You must create a URL filtering profile before you can apply the profile to a WLAN or to a user role.

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 289** Creating a URL filtering profile



4. Enter a **Name** and optionally a **Description** for this profile.



- Select one of the content filtering category groups, in increasing order of strictness, or select **Custom**, and select any number of individual categories.

FIGURE 290 Select level of strictness

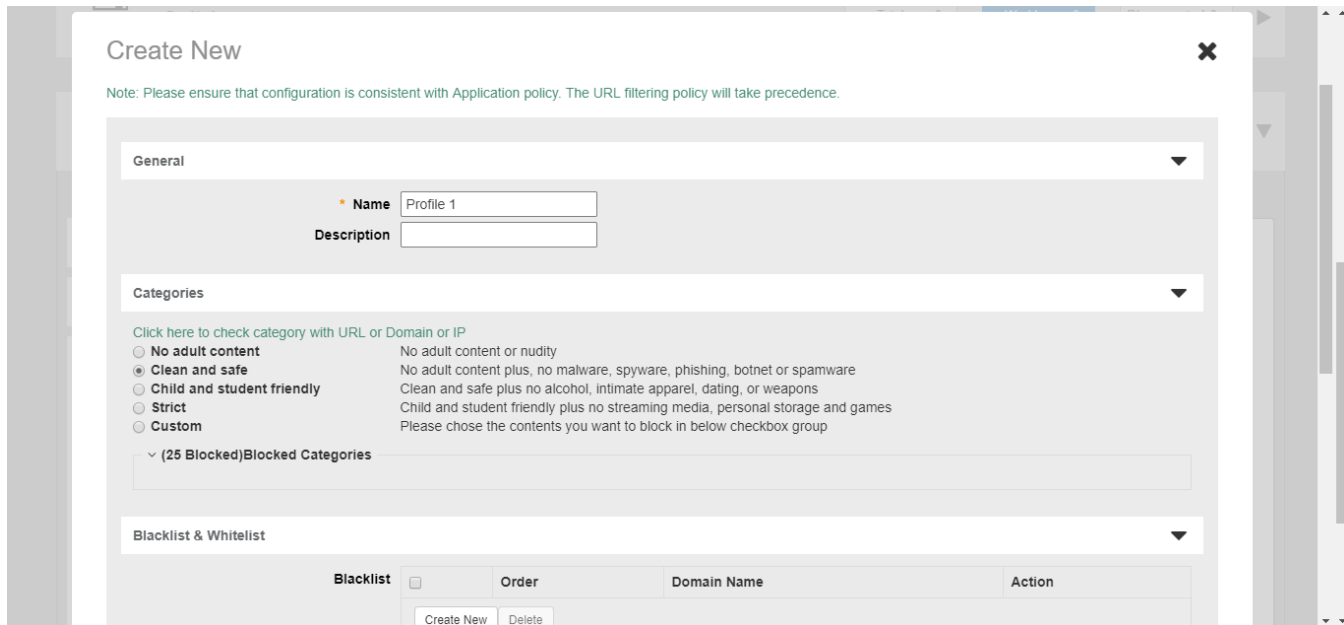
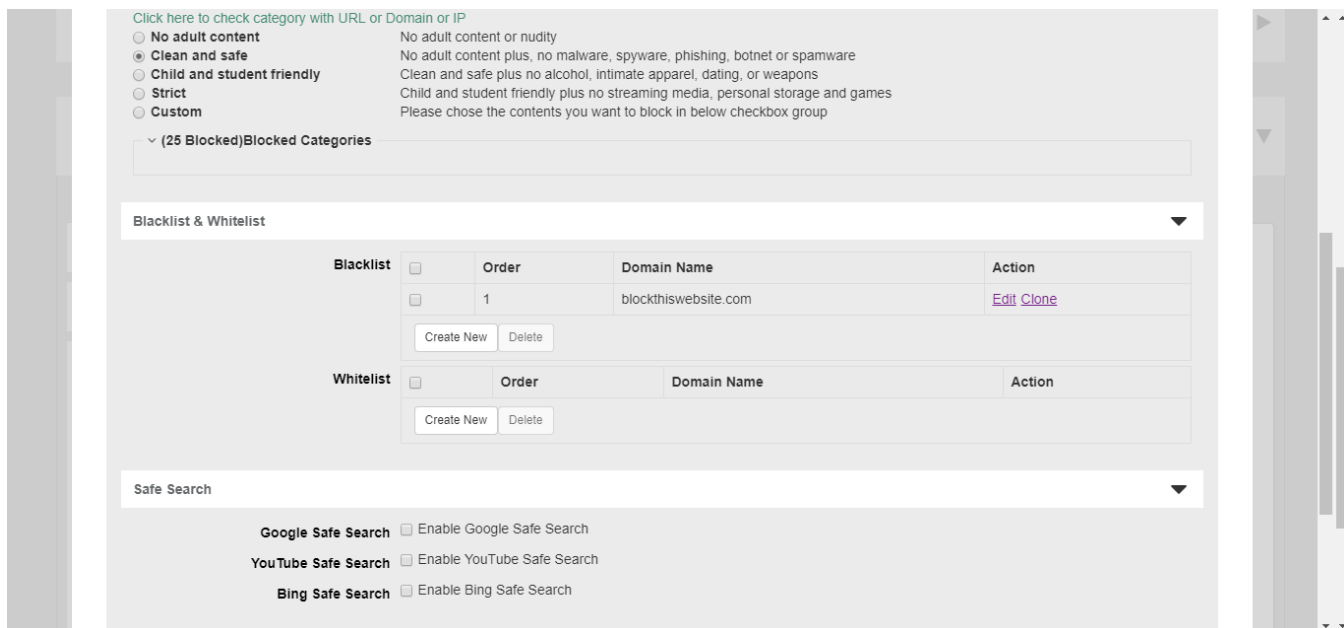


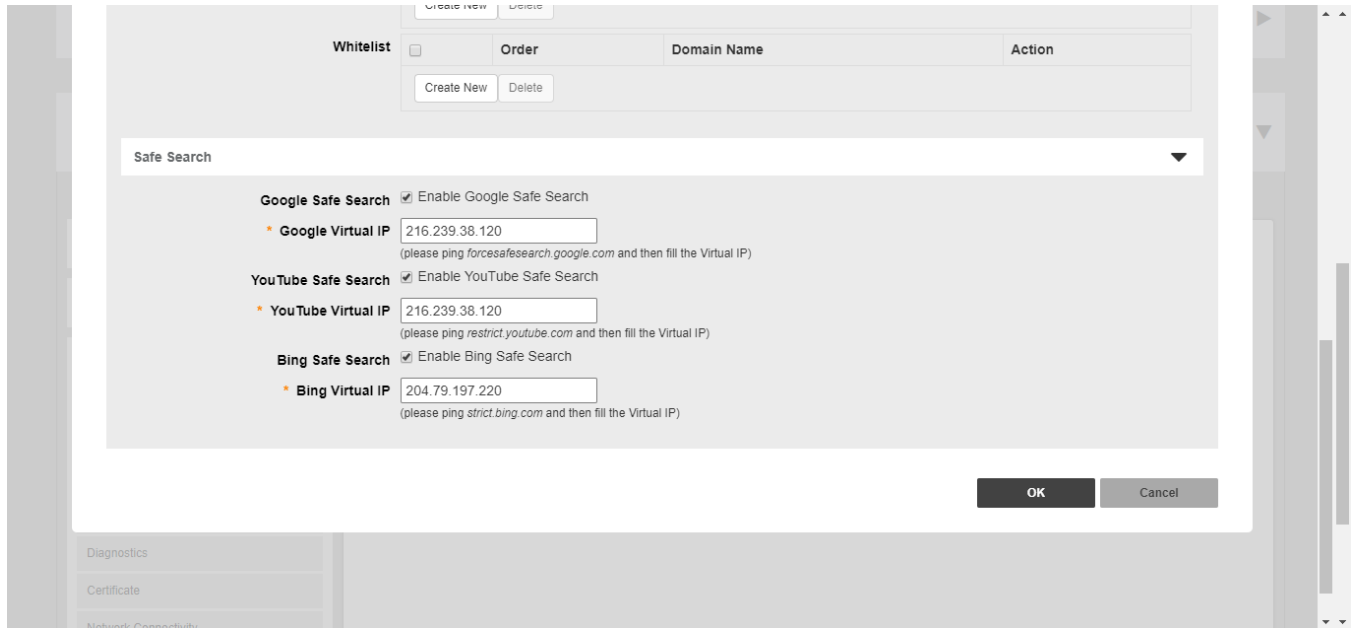
FIGURE 291 Blacklisting or whitelisting a specific URL



- Optionally, in *Blacklist & Whitelist*, you can add custom URLs to either block or allow. Whitelist and blacklist entries override the rules configured above. A maximum of 16 blacklist and 16 whitelist entries can be created per profile.

7. Optionally, in *Safe Search*, enable or disable "Safe Search" functionality from Google, Youtube or Bing.

**FIGURE 292** Enable Google, Youtube and Bing Safe Search options



8. Click **OK** to save your changes. A maximum of 32 profiles can be created.

### **Applying a URL Filtering Policy to a WLAN**

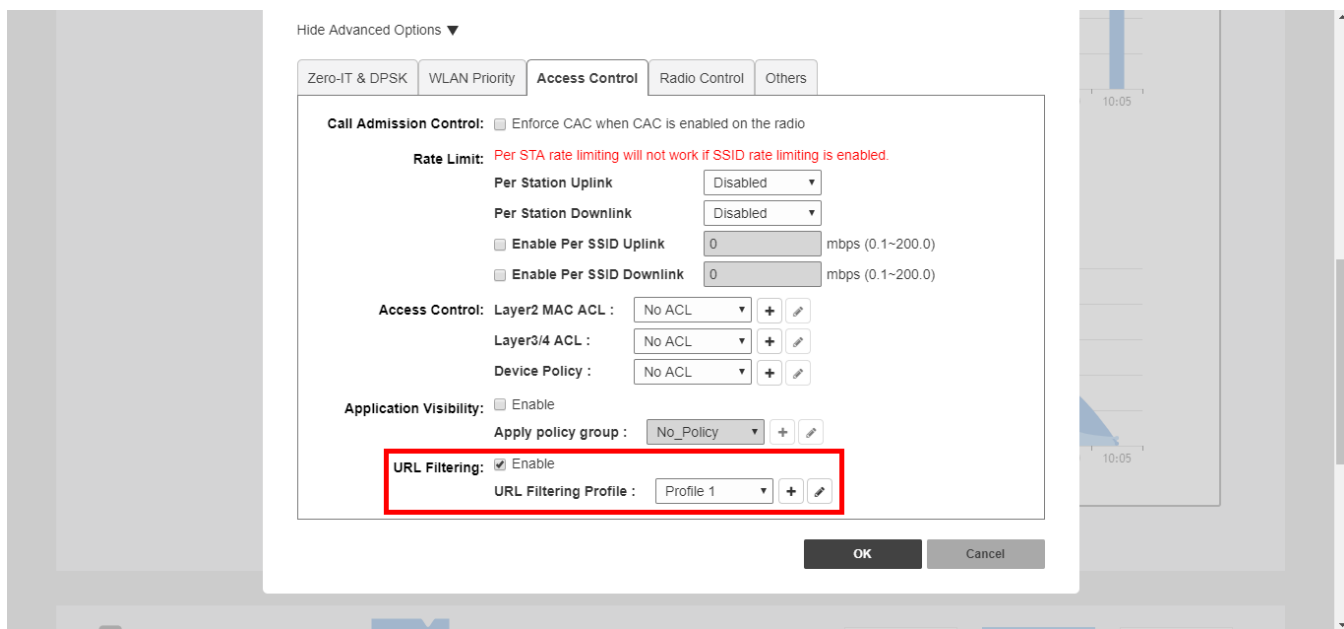
Once a URL filtering policy has been created, you can apply it to your wireless networks using the following procedure.

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 293** Enabling URL filtering for a WLAN



### Working with URL Filtering Licenses

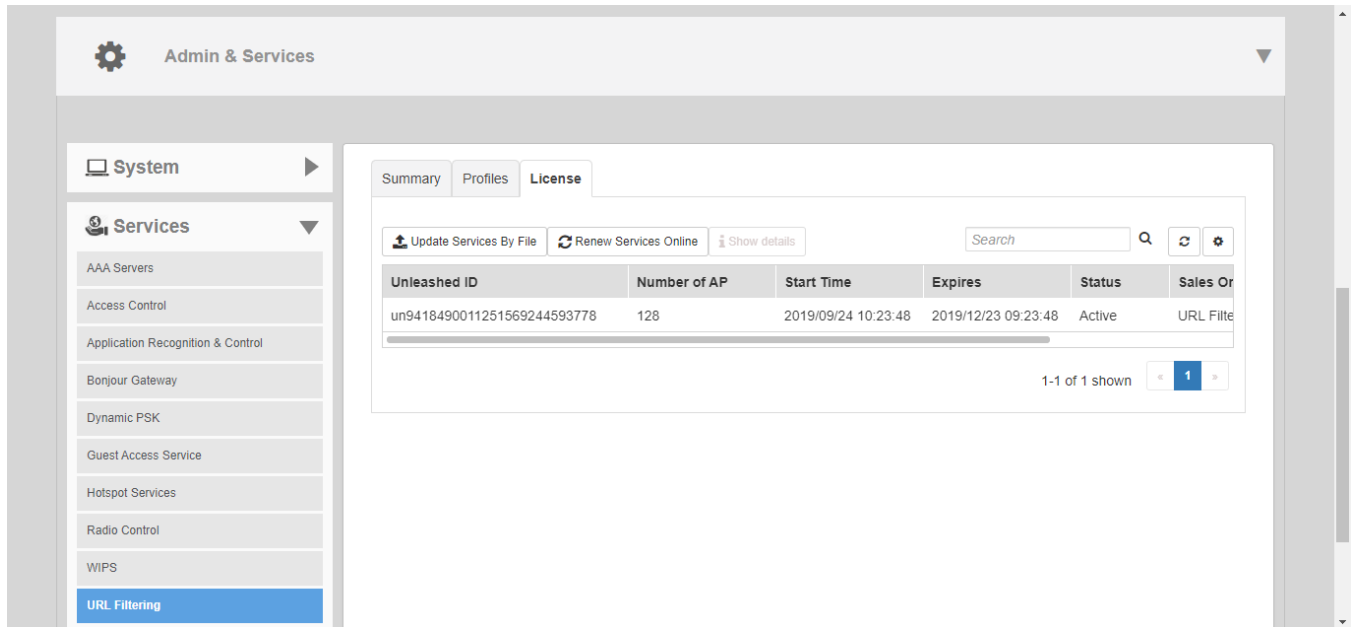
URL Filtering service requires an active URL filtering license to function. URL filtering licenses can be purchased from Ruckus partners and distributors, and a temporary license is also available to allow customers to try out the service for a limited time before purchasing.

To manage URL filtering licenses:

1. Go to **Admin & Services > Services > URL Filtering**.

- In the **License** tab, configure any of the following:
  - Update Services By File:** Import a new locally saved license file.
  - Renew Services Online:** Connect to Ruckus license server to download a license file.
  - Show Details:** Select the license file from the list and click Show Details to view license expiration details.

FIGURE 294 Working with URL filtering licenses



## 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 295 Configuring administrator preferences

The screenshot shows the 'Admin & Services' configuration page. On the left is a navigation menu with 'Administration' expanded to show 'Preferences'. The main content area is divided into sections: 'Language' (set to English), 'Administrator Name/Password' (with 'Authenticate using the admin name and password' selected, 'Admin Name' set to 'admin', and 'Fallback to admin name/password if failed' checked), and 'Setup Password Recovery' (with 'Enable Password Recovery' unchecked). Each section has an 'Apply' button.

FIGURE 296 Enabling password recovery

This screenshot is similar to Figure 295 but highlights the 'Setup Password Recovery' section with a red box. In this section, 'Enable Password Recovery' is now checked. Below this, there are fields for 'Security Email' (example@example.com), 'Security Question' (a dropdown menu), and 'Security Answer'.

## 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 297** Backup and Restore

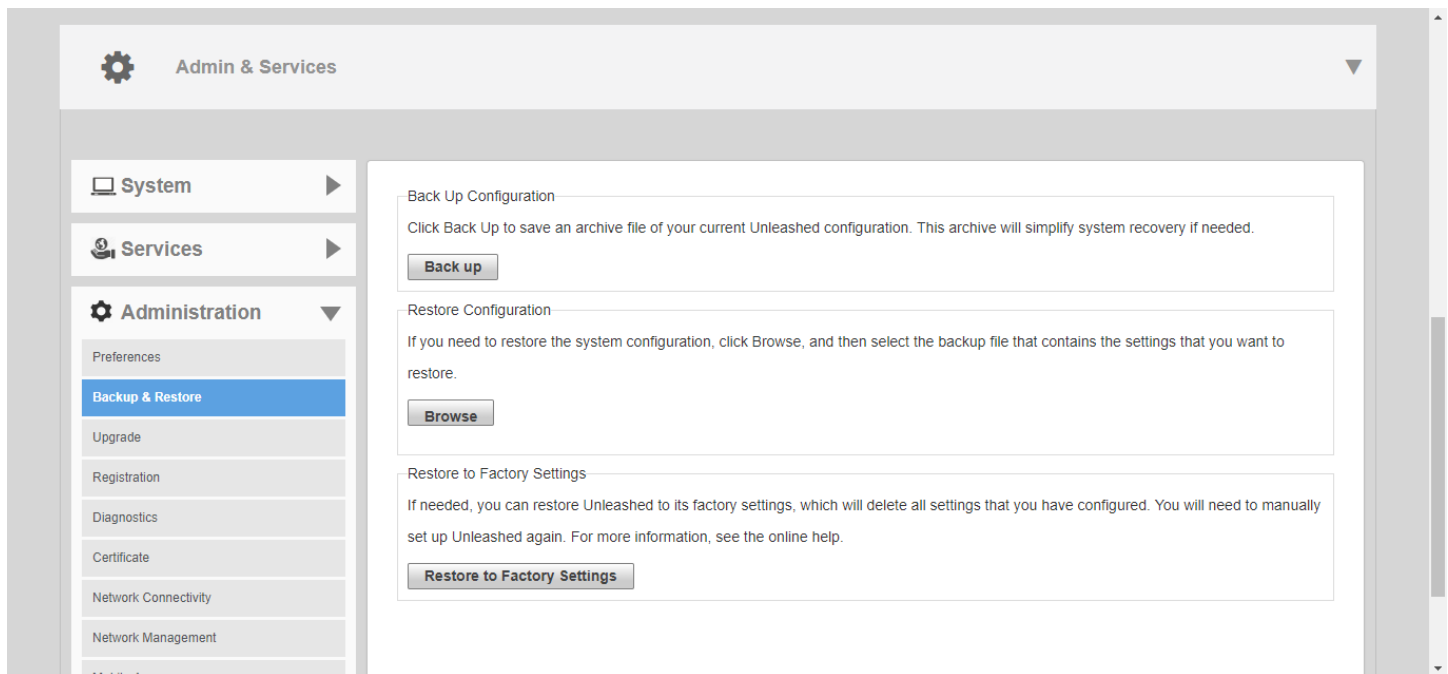
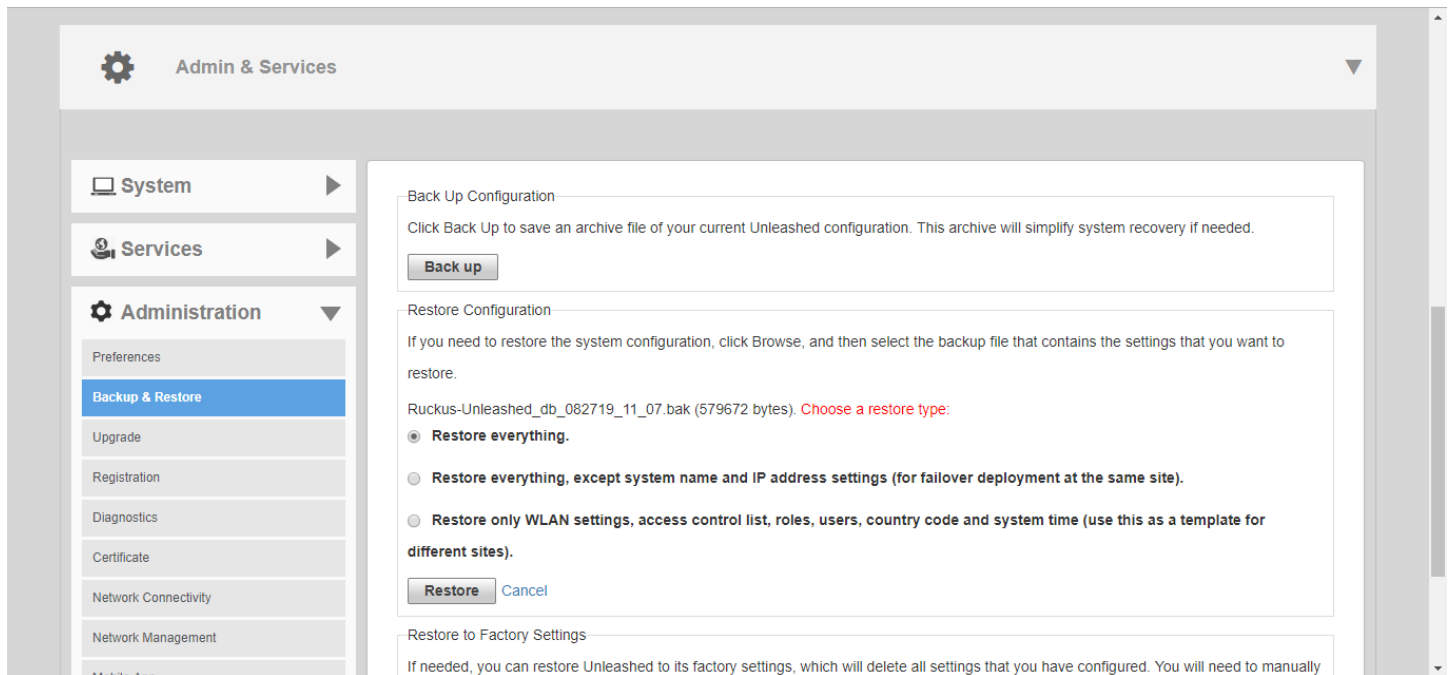


FIGURE 298 Choose a Restore type



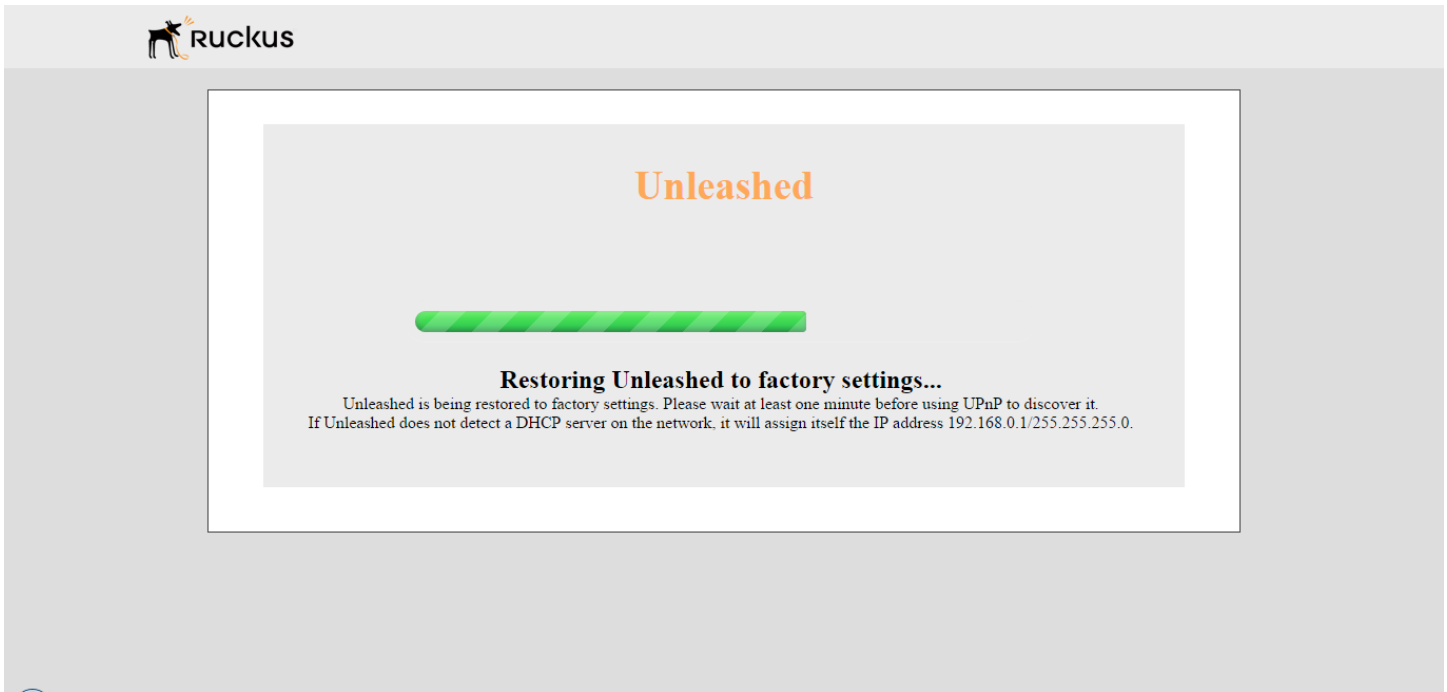
### Restore to Factory Settings

In certain extreme conditions, you may want to re-initialize your Unleashed Master AP and reset it to factory default state. Once the Unleashed 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 will need to be reconfigured.

To reset your Unleashed 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.
4. The **Restoring Unleashed to factory settings** progress screen appears. Wait for this progress screen to finish before attempting to login again.
5. Repeat the initial setup and configuration procedures as described in [Setting Up an Unleashed Wi-Fi Network](#) on page 81.

FIGURE 299 Restore Factory Settings progress screen



### Alternate Factory Default Reset Method

If you are unable to complete a software-based resetting of Unleashed, you can do the following "hard" restore:

#### NOTE

Do not disconnect the Unleashed Master AP from its power source until this procedure is complete.

1. Locate the **Reset** pin hole on the rear panel of the Unleashed Master AP.
2. Insert a straightened paper clip in the hole and press for at least 6 seconds.
3. After the reset is complete, the PWR LED will initially be solid red, indicating bootup in process, then blinks green, indicating that the system is in factory default state.
4. After you complete the Setup Wizard, the PWR LED will be steady green.

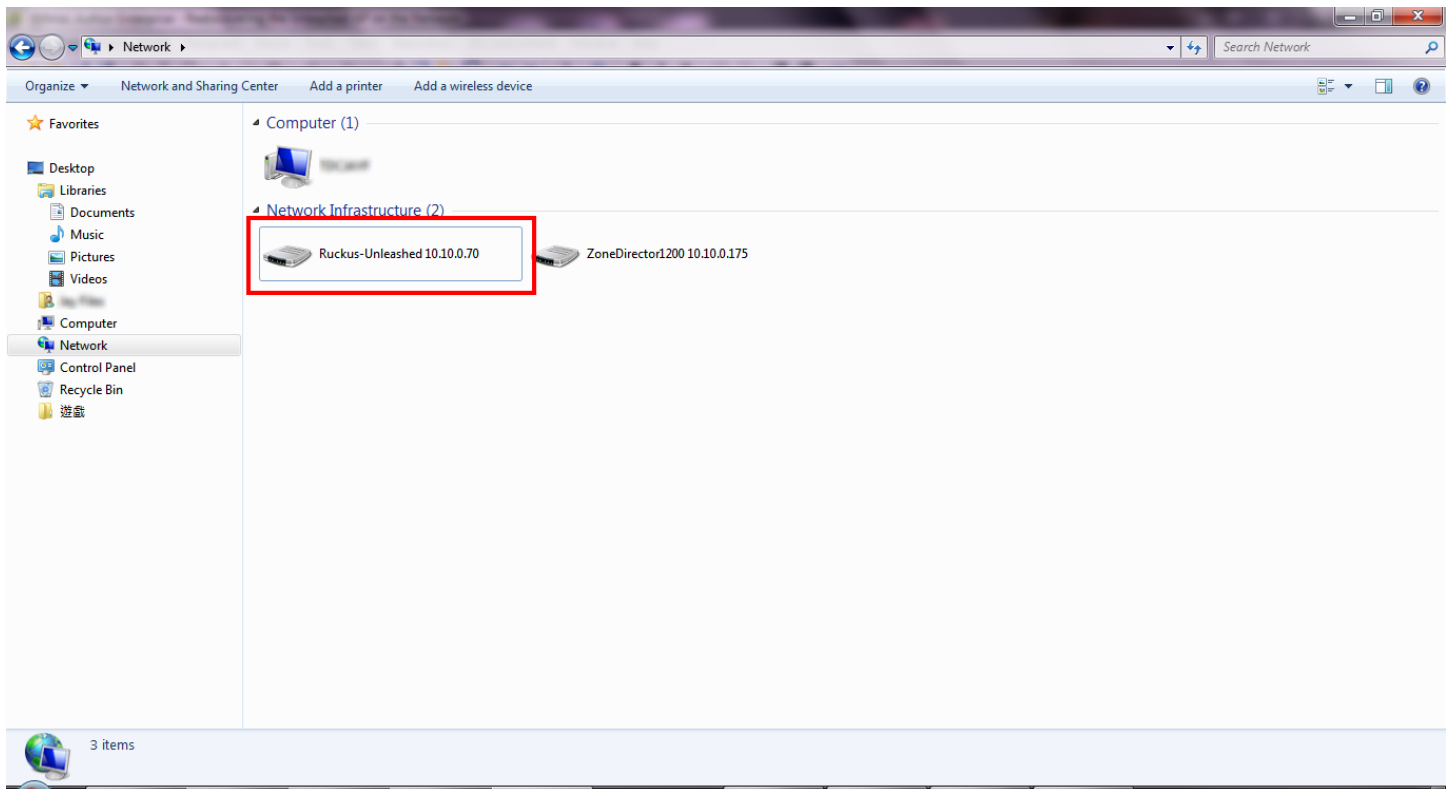
### Rediscovering the Unleashed AP on the Network

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 300 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 353
- [Local Upgrade](#) on page 357

### Online Upgrade

Use the Online Upgrade method to upgrade your Unleashed network with the latest firmware available from the Ruckus Unleashed firmware server.

To upgrade the Unleashed Master AP and all connected Unleashed member APs using the Online Upgrade method, use the following procedure:

1. Go to **Admin & Services > Administer > Upgrade**.
2. Select **Online Upgrade**.

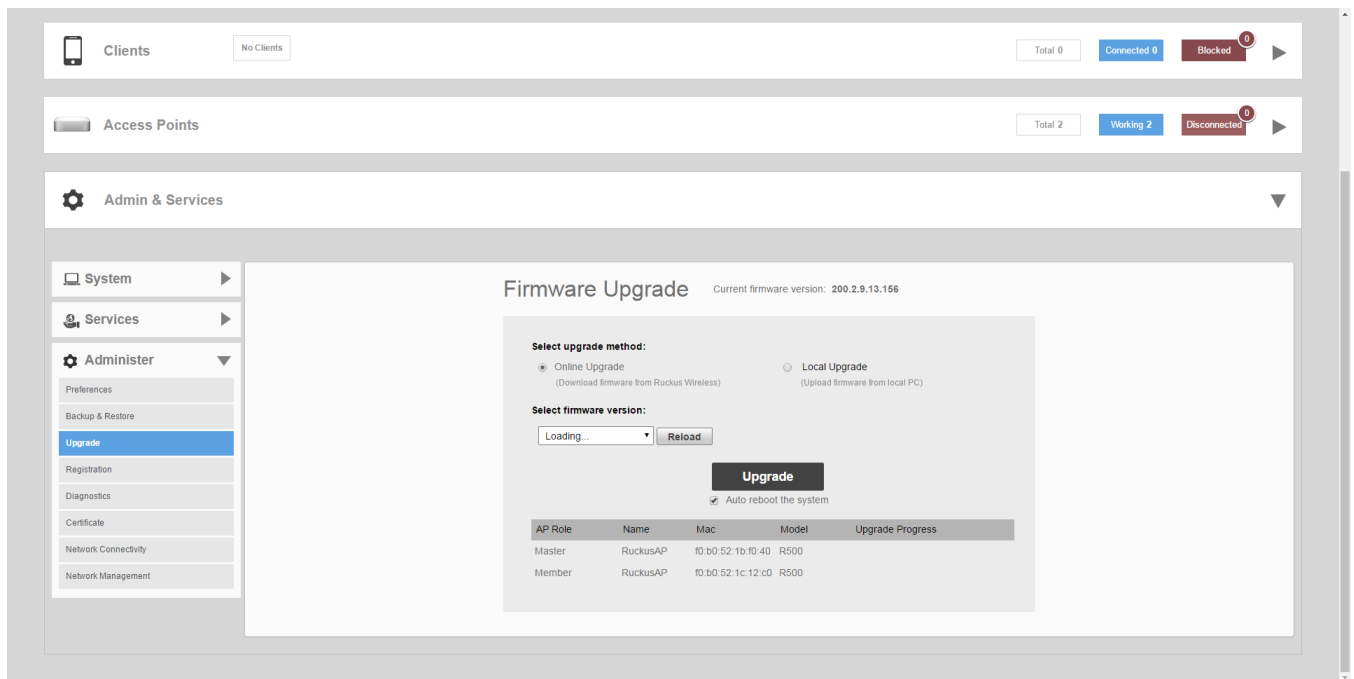
3. Select one of the available firmware versions from the **Select firmware version** drop-down menu.

**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 would prefer to wait until all APs have the new firmware before rebooting them all at once (i.e., if you have multiple Unleashed AP models that require different firmware image files, you can choose to reboot all Unleashed R710 APs as soon as the firmware is loaded and then move on to R500 APs, or you could choose to wait and reboot all models at once at the end.)

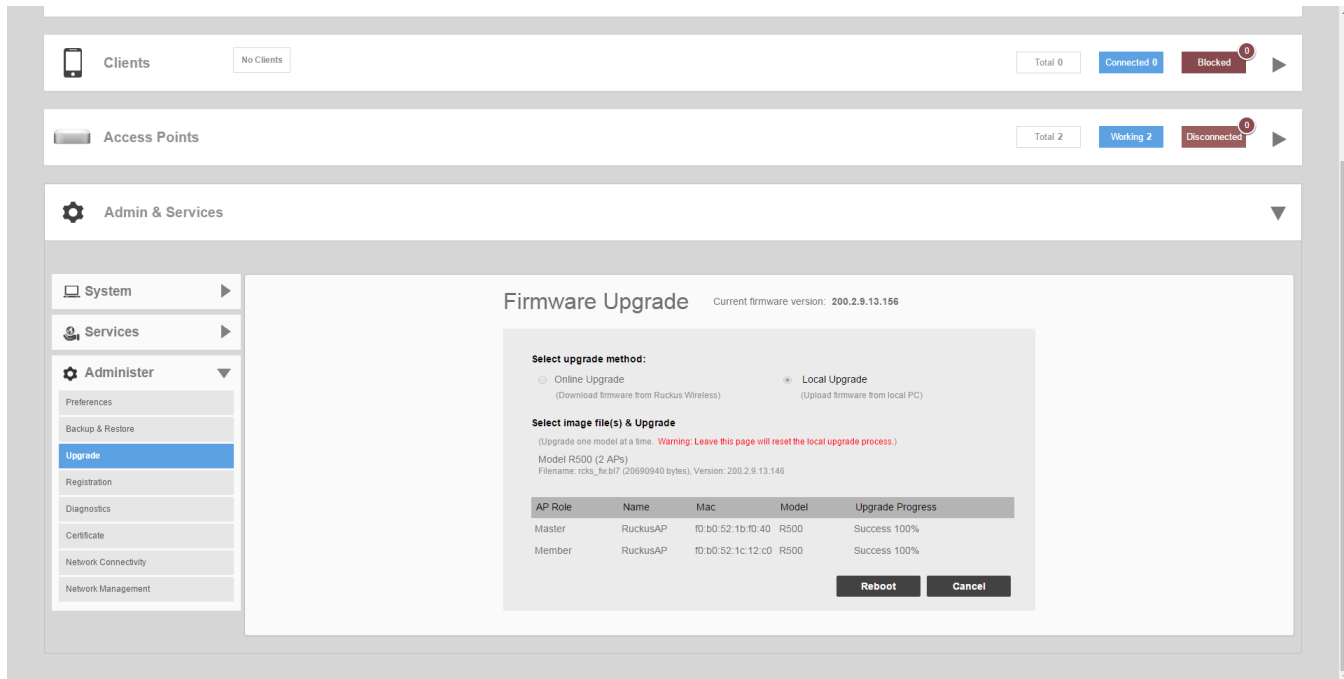
4. Click **Upgrade** to begin upgrading the Unleashed APs shown in the list.

**FIGURE 301** The Upgrade page



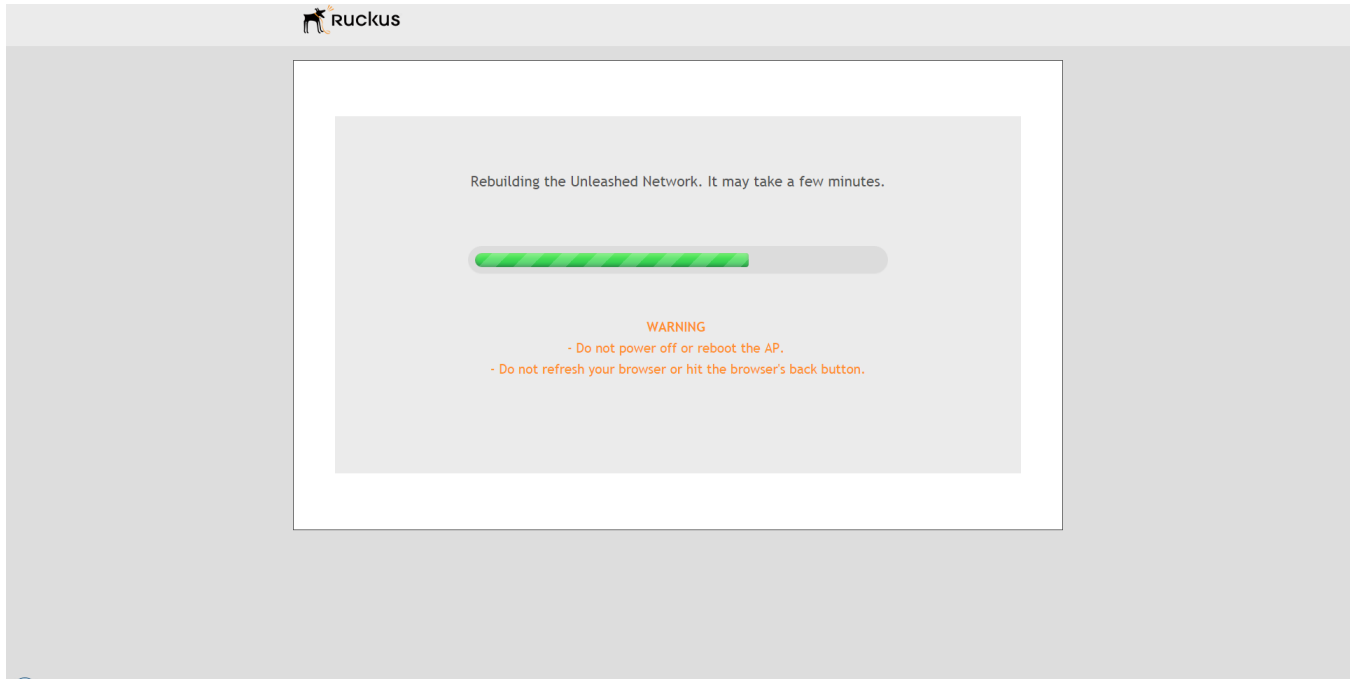
- The **Upgrade Progress** column displays the progress for each AP. Once completed, the column will display "Success 100%" next to each AP for which the upgrade was successful.

**FIGURE 302** Upgrade successful, click Reboot to reboot the APs and apply the new firmware



- When all of the APs in the list are displayed as "Success 100%" in the **Upgrade Progress** column, click **Reboot**. A "Rebuilding the Unleashed Network" progress screen appears. Wait until the process completes.

**FIGURE 303** "Rebuilding the Unleashed Network" progress screen



- Once complete, you will be redirected to the Unleashed login page.
- Log in and go to **Admin & Services > System > System Info** to confirm the new software build number.

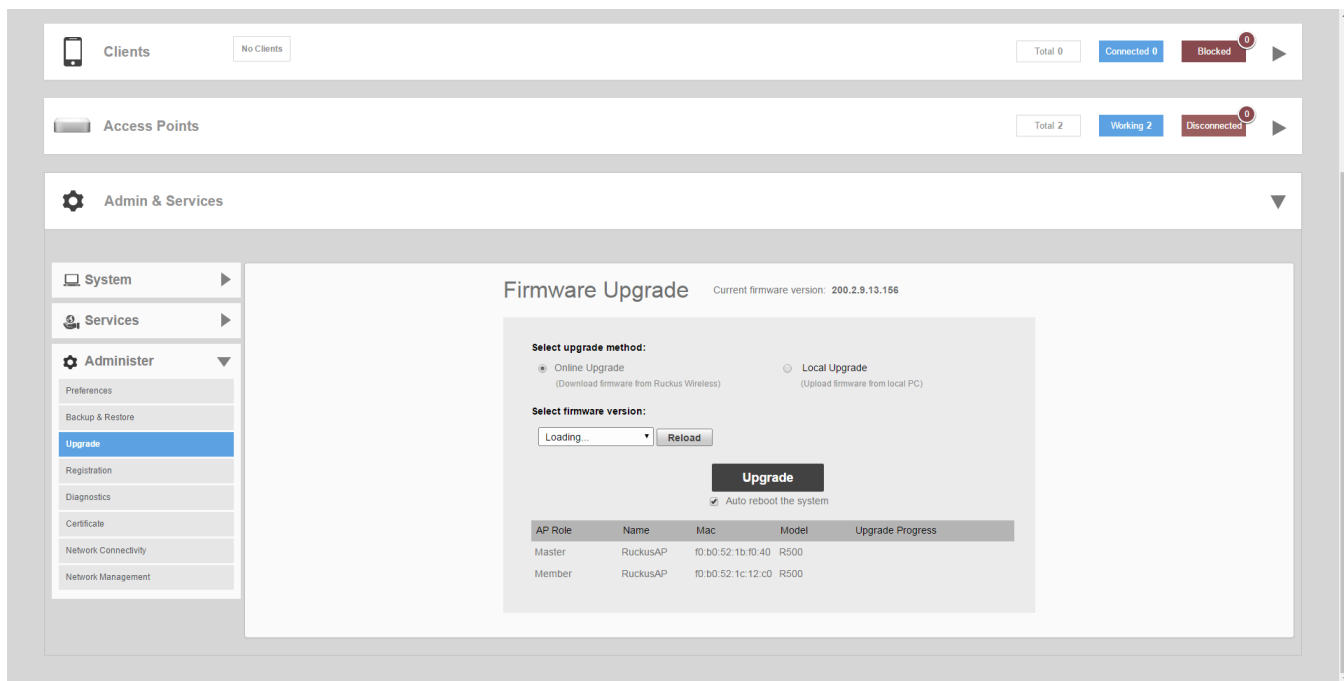
## Local Upgrade

Use the Local Upgrade method to upgrade your Unleashed network using firmware files that you have downloaded from the Ruckus Support site.

To upgrade the Unleashed Master AP and all connected Unleashed member APs using the Local Upgrade method, use the following procedure:

1. Go to **Admin & Services > Administer > Upgrade**.

**FIGURE 304** The Upgrade page



2. Select **Local Upgrade** as the upgrade method.

3. Click **Browse** to locate the Unleashed firmware image file on your local computer. Unleashed will perform a check to make sure it is the proper image for the AP model before proceeding.

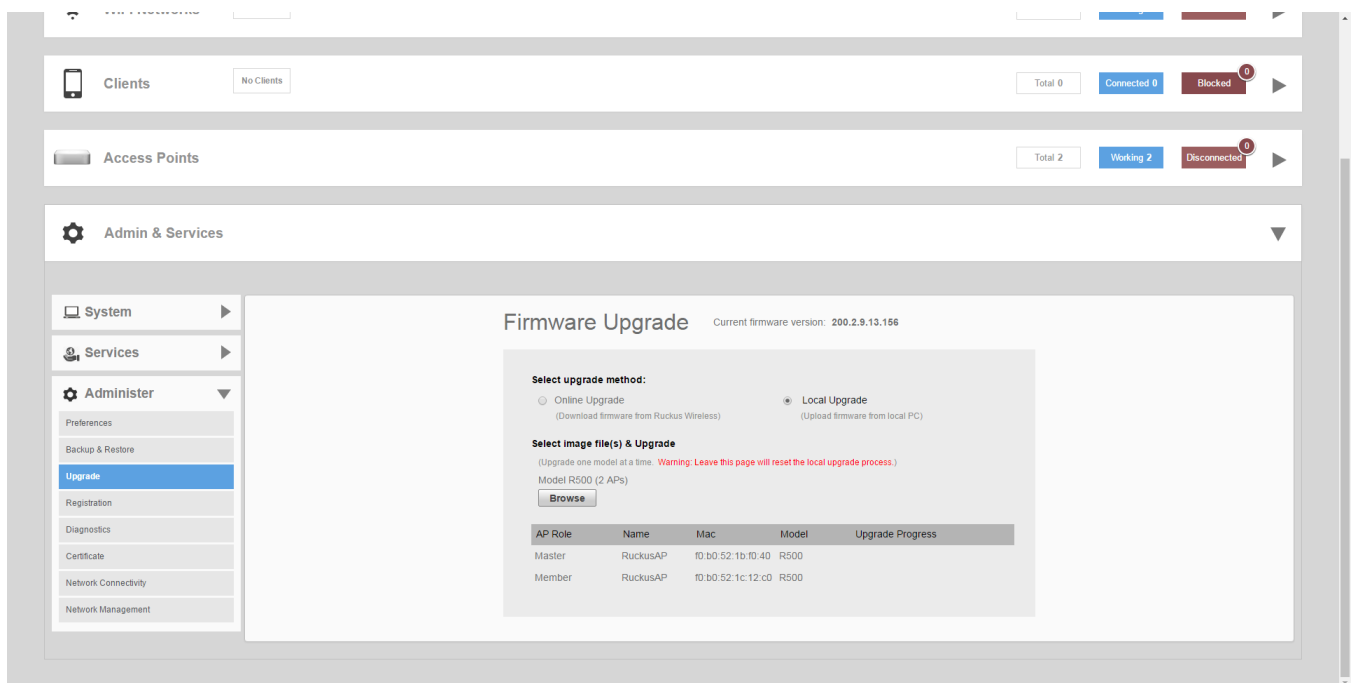
**NOTE**

Each Unleashed AP model has a different firmware image file that must be loaded onto the Unleashed Master and then distributed to all member APs of that model. So, for example, if you have a mix of 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 Unleashed AP with the incorrect model firmware, there is no check to ensure that you do not upgrade/downgrade an Unleashed AP to a Ruckus Solo AP (standalone) firmware image. If you do this, the AP will no longer function as an Unleashed AP until Unleashed firmware is re-loaded onto it.

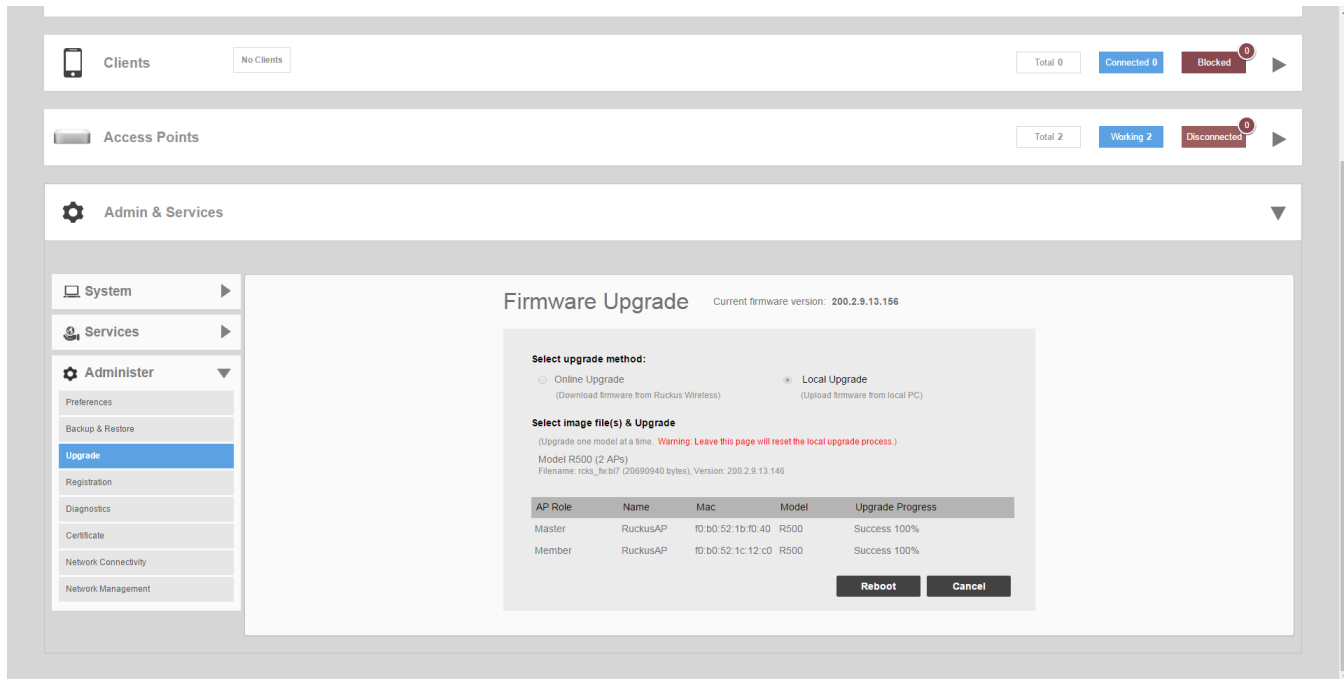
**FIGURE 305** Local Upgrade



4. Click **Upgrade** to begin upgrading the Unleashed APs shown in the list.

- 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.

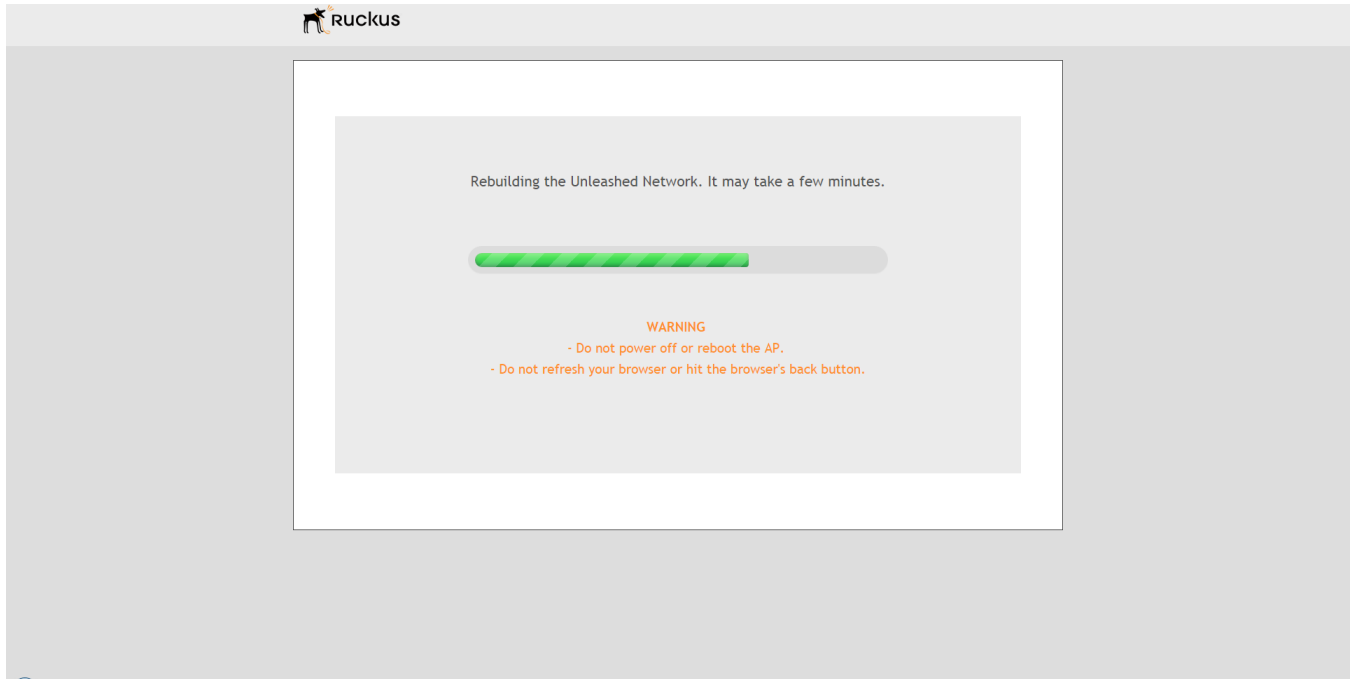
**FIGURE 306** Upgrade successful, click Reboot to reboot the APs and apply the new firmware



- Repeat steps 3-5 for any additional Unleashed AP models.

- When all of the APs in the list are displayed as "Success 100%" in the **Upgrade Progress** column, click **Reboot**. A "Rebuilding the Unleashed Network" progress screen appears. Wait until the process completes.

**FIGURE 307** "Rebuilding the Unleashed Network" progress screen



- Once complete, you will be redirected to the Unleashed login page.
- Log in and go to **Admin & Services > System > System Info** to confirm the new software build number.

## Registration

Ruckus encourages you to register your Unleashed products to receive updates and important notifications, and to make it easier to receive support in case you need to contact Ruckus for customer assistance. You can register your Unleashed Master AP along with all connected member APs in one step using the Registration page.

### NOTE

To ensure that all registration information for all of your APs is included, be sure to register after all APs have been installed. If you register the Unleashed Master AP before installing the other member APs, the registration will not include the other member APs' information.

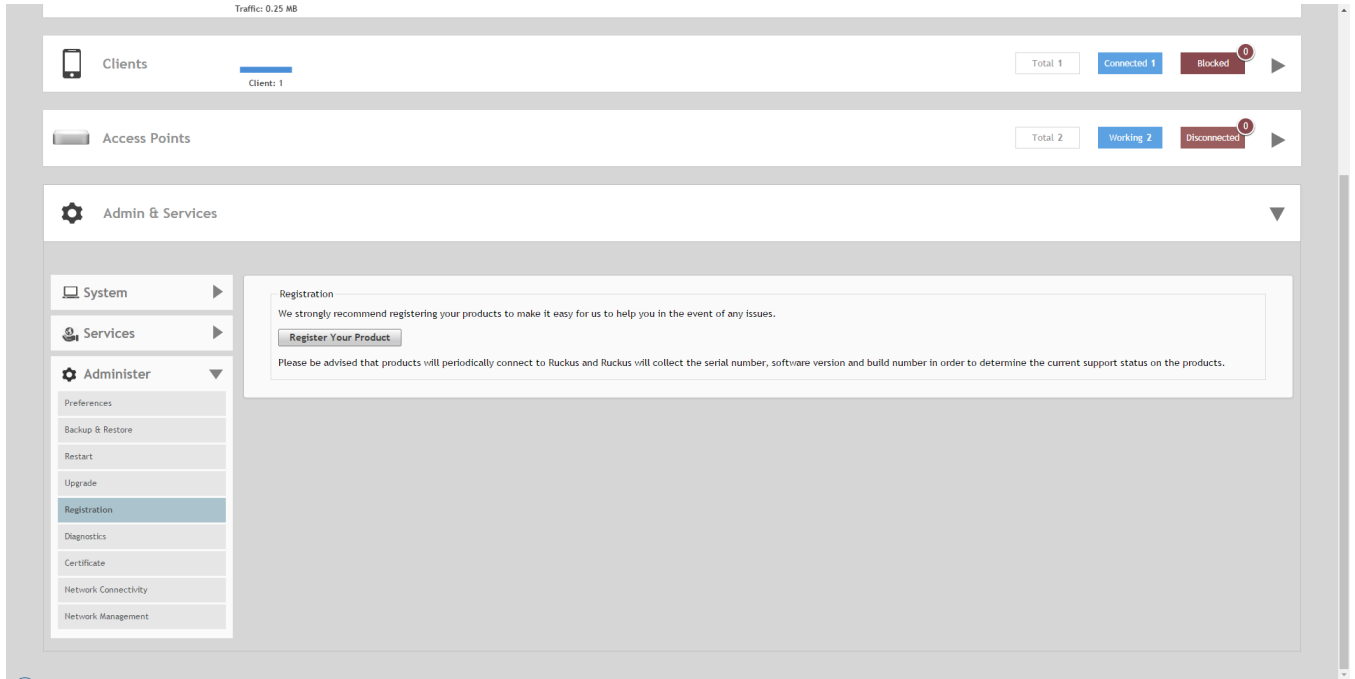
To register your Unleashed network:

- Go to **Admin & Services > Administer > Registration**.



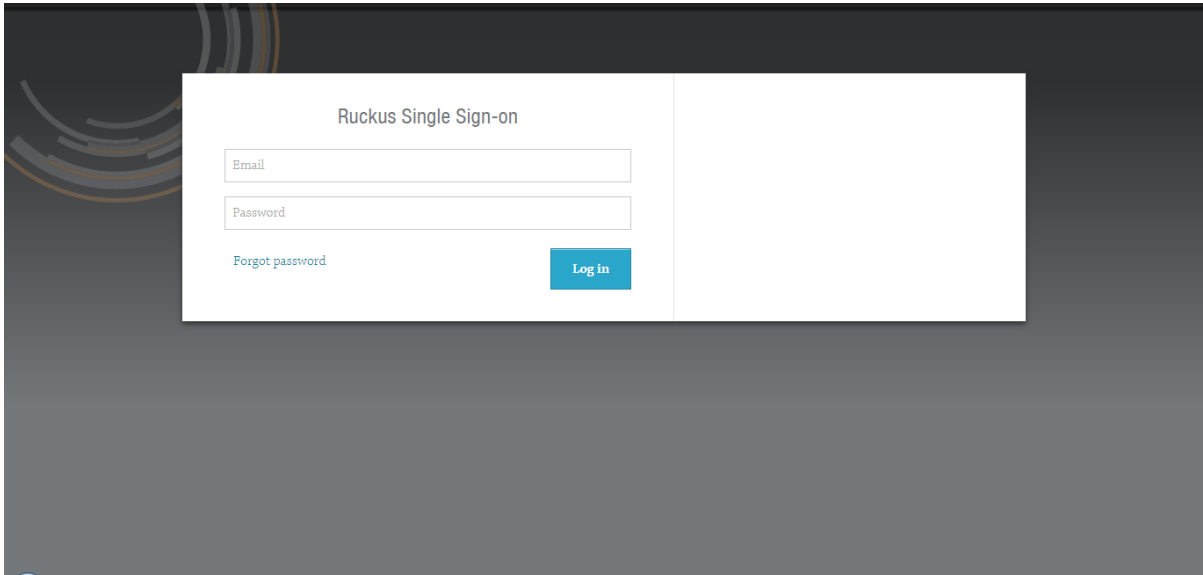
2. Click **Register Your Product**. You will be redirected to the Ruckus registration website, where you will need to enter your login details and Sales Purchase Agreement code (if known).

**FIGURE 308** The Registration page



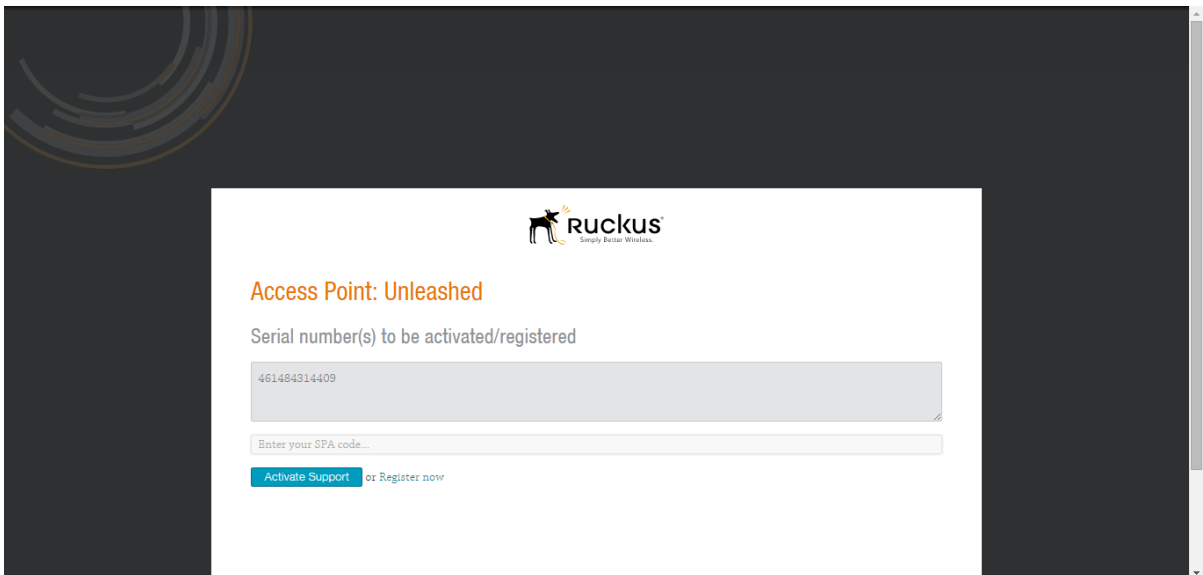
3. If you do not already have a Ruckus Support portal account, you will first need to create one. Go to [https://support.ruckuswireless.com/get\\_access\\_now](https://support.ruckuswireless.com/get_access_now) to create a support account, and then go back to the Unleashed web interface and click the **Register Your Product** button (again) to associate your product serial numbers to your Ruckus Support account.

**FIGURE 309** Ruckus Support portal login



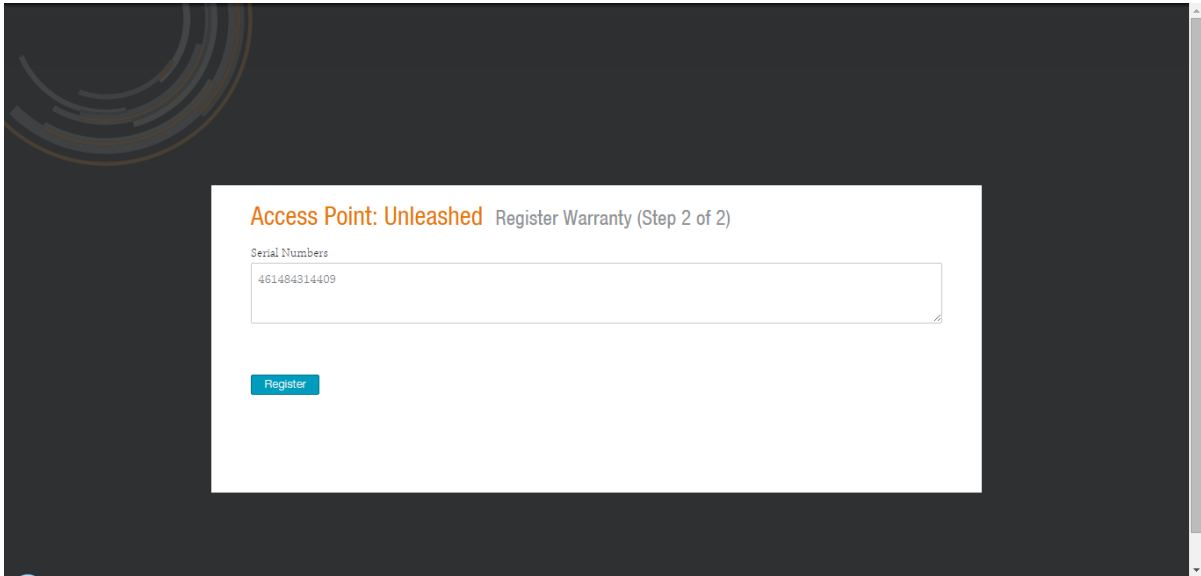
4. The Ruckus product registration system automatically retrieves a list of your connected device serial numbers and displays them on the page.
5. Click **Activate Support** to activate product support for your Unleashed APs.

**FIGURE 310** Activate Support



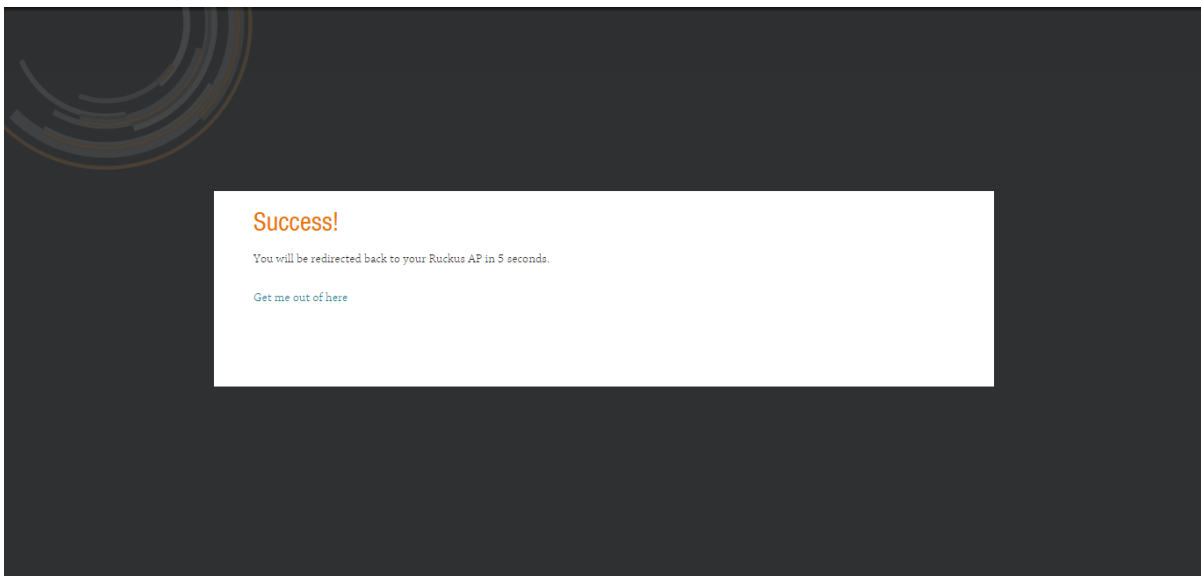
6. Click **Register** to register your Unleashed AP warranty.

**FIGURE 311** Register Warranty (Step 2 of 2)



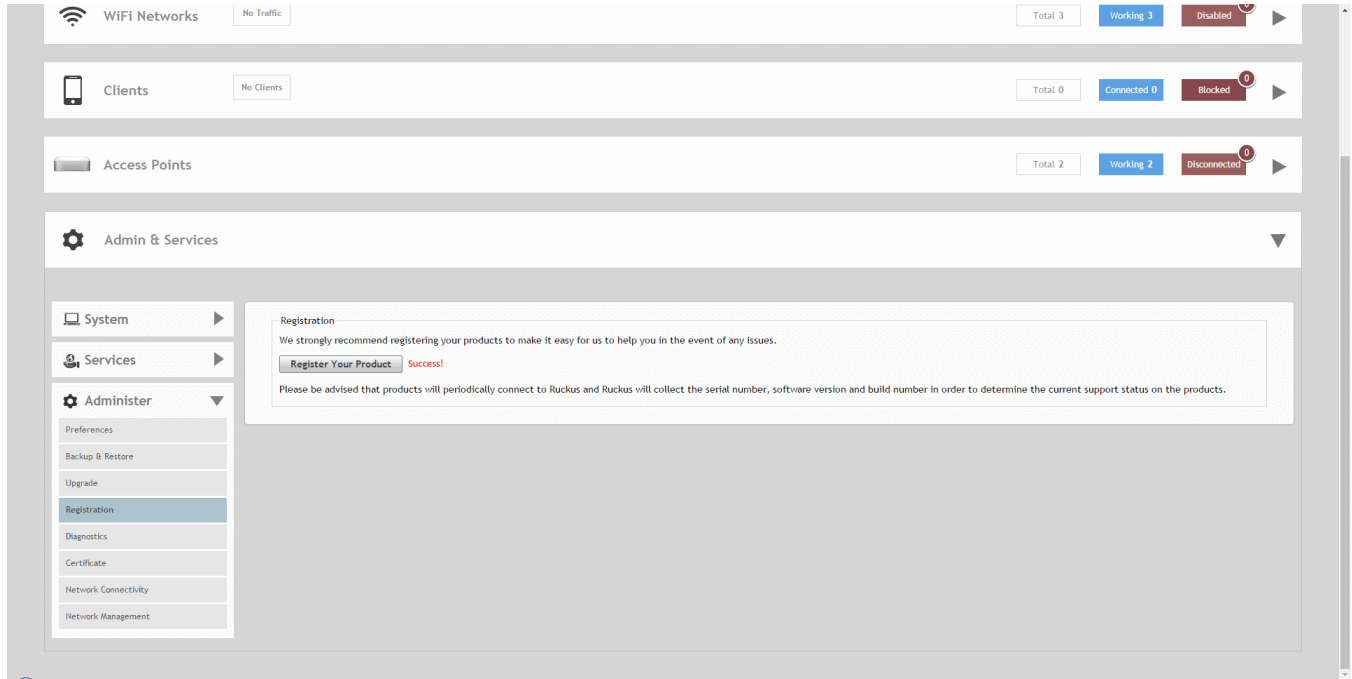
7. The **"Success!"** page is displayed. You will be redirected back to your Unleashed web interface in a few seconds. If you prefer not to wait, click **Get me out of here** to be redirected immediately.

**FIGURE 312** Success - Support activation successful



- The screen refreshes to display your Unleashed Master AP's Registration page, with a "Success" message indicating successful product support registration.

**FIGURE 313** Success - Unleashed Registration page

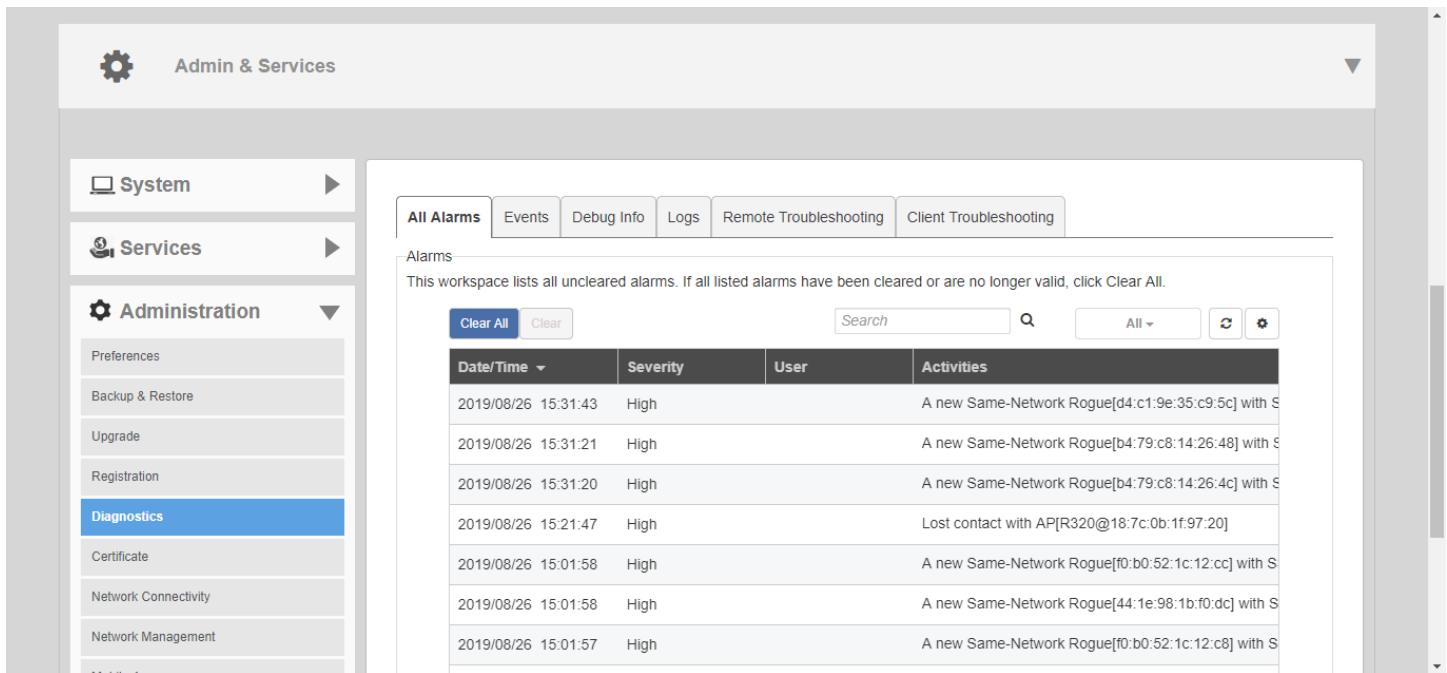


Your Unleashed access points are now registered with Ruckus.

## Diagnostics

The *Diagnostics* pages provide options for troubleshooting and diagnostics, including configuration settings for alarms, viewing system event log messages, configuring which debug info is to be collected in log files, saving the current logs to your local computer, and an option to begin a remote troubleshooting session (for Ruckus Support remote assistance).

FIGURE 314 Diagnostics



### Viewing Alarms

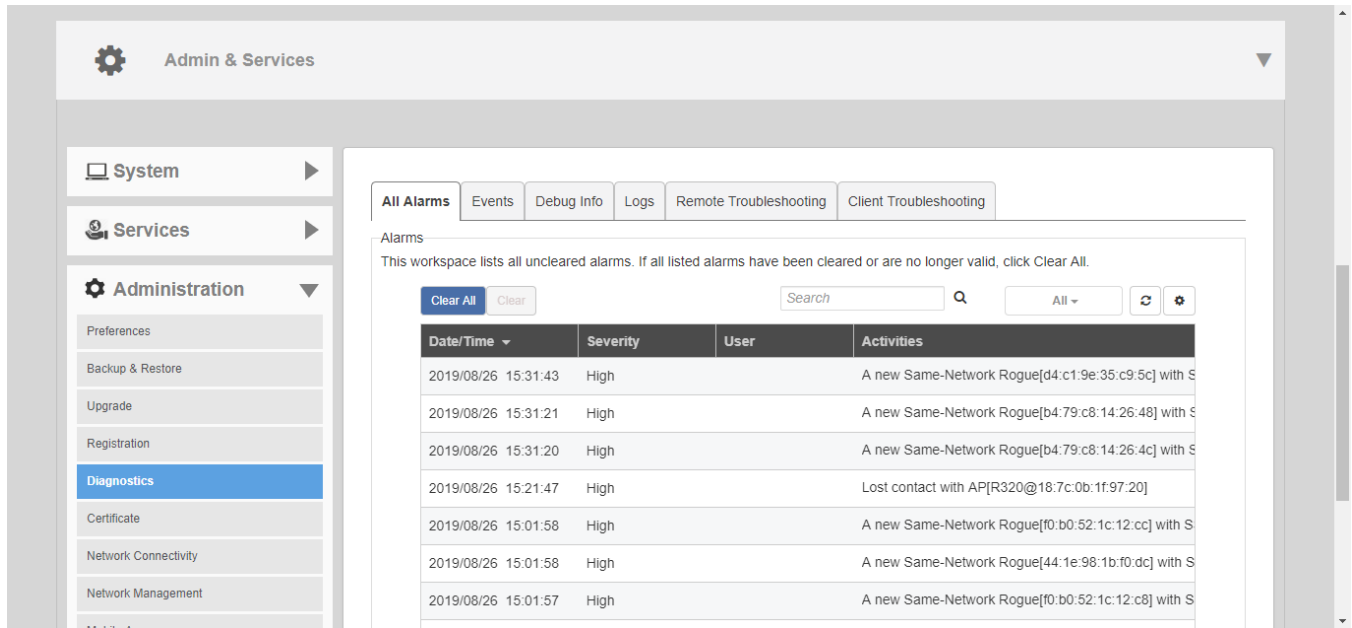
The *All Alarms* page displays a list of all recent alarms. Alarms include important events such as when an AP loses contact with the Unleashed Master AP, a rogue AP is detected, an authentication server becomes unreachable, or when an Unleashed Master/Member role change is detected.

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 315** Viewing a list of alarm event messages



### Viewing System Event Messages

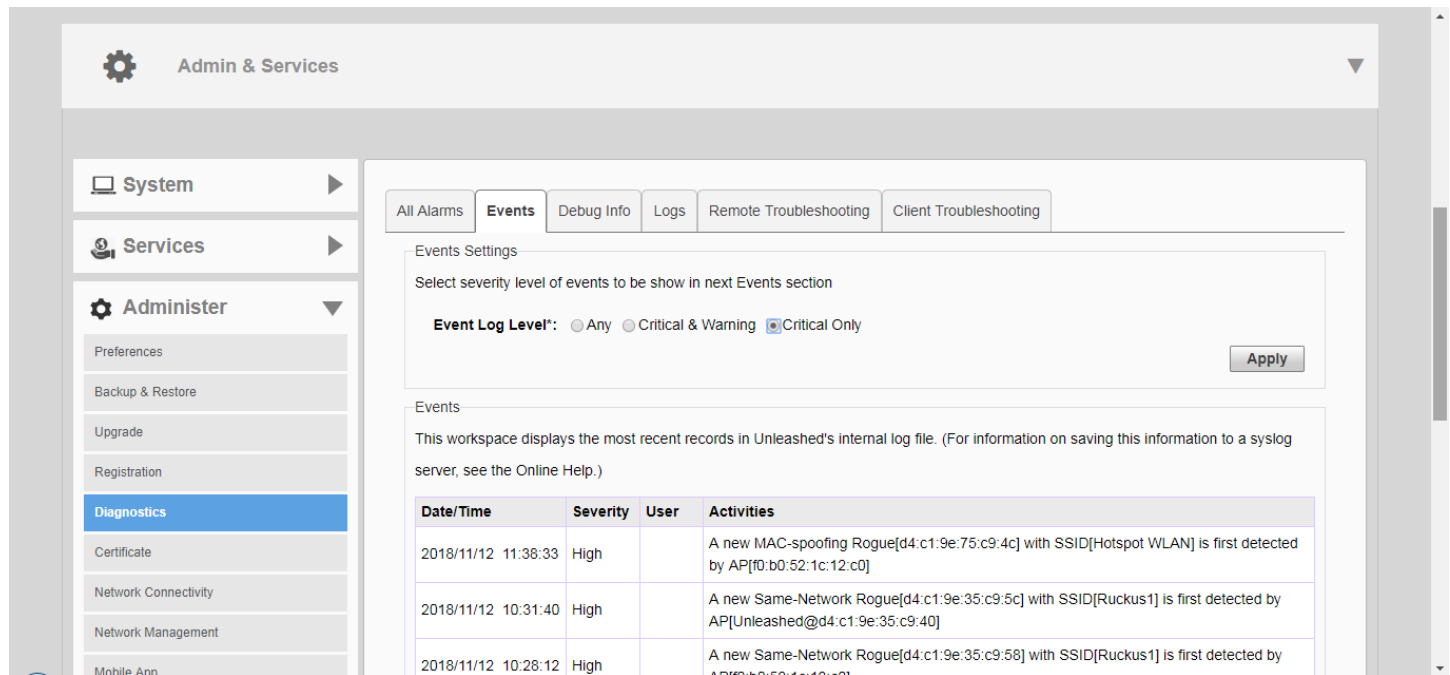
The **Diagnostics > Events** page displays the most recent records in the Unleashed Master AP's internal log file.

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 316 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.

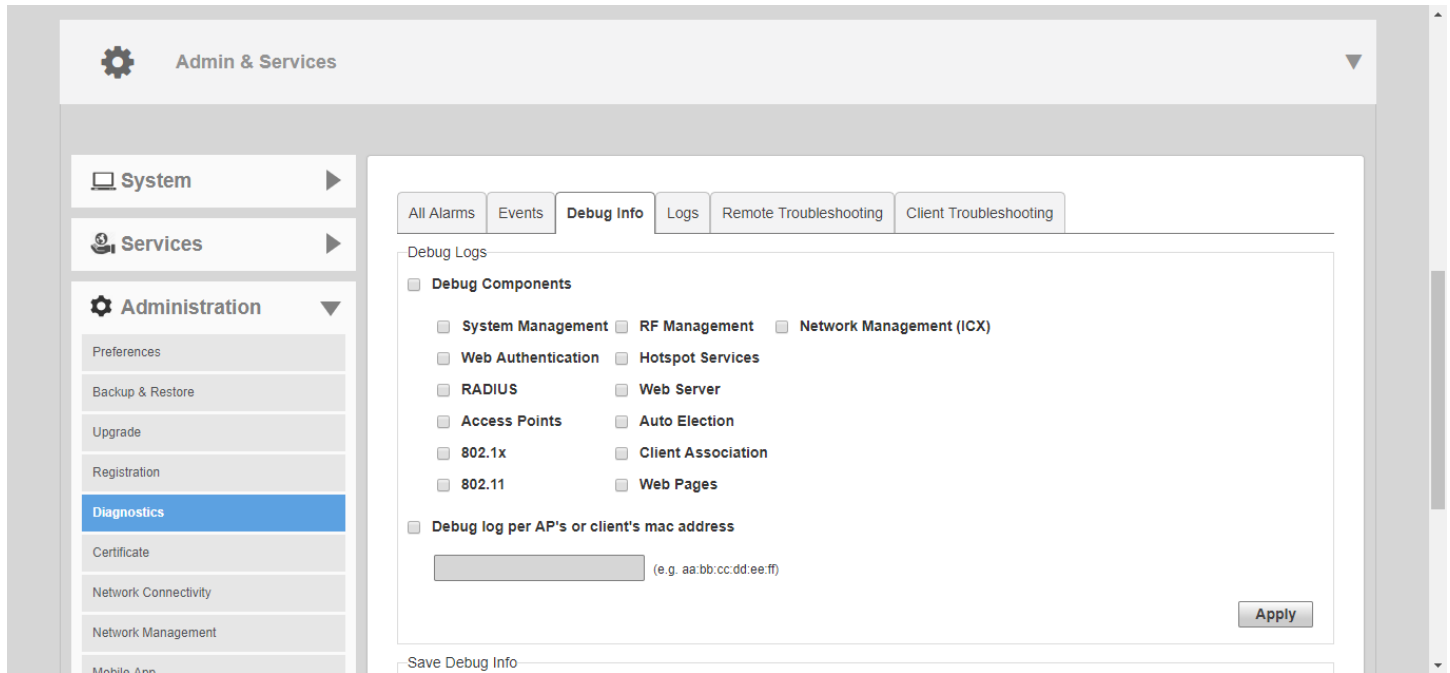
You can also save the log files using the **Save Debug Info** button. If you request assistance from Ruckus technical support, you may be asked to supply detailed debug information from Unleashed. Click the **Save Debug Info** button, and then save the file to your computer. You can then email this file to Ruckus Support to assist with troubleshooting.

### NOTE

The Unleashed Master AP's log files also contain all of the member APs' support info.

You can also allow the Unleashed Master 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 Unleashed 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).

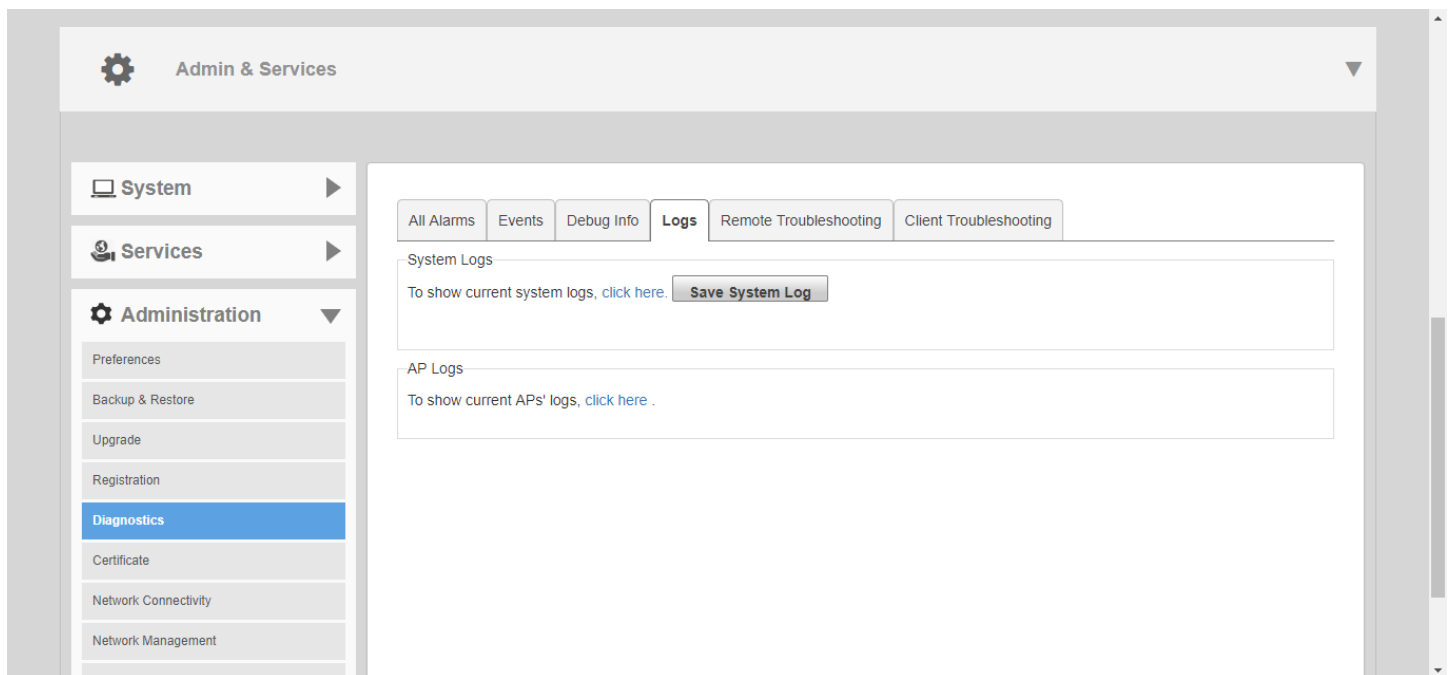
FIGURE 317 The Debug Info page



### *Saving System Logs to Your Computer*

The **Admin & Services > Administration > Diagnostics > Logs** page provides an option to view the AP's current system logs and an option to save the current log file as a .tar file to a local computer.

FIGURE 318 The Logs page



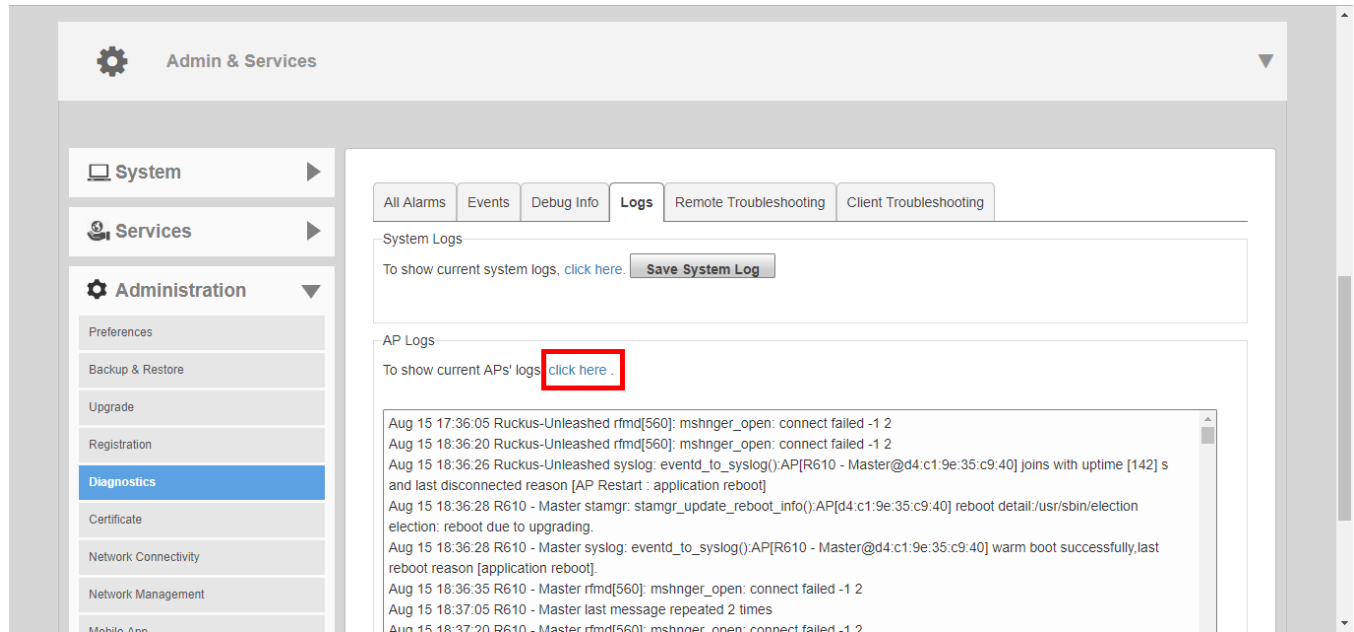


## Viewing Current AP Logs

Use the *AP Logs* link to display a list of recent AP activity logs from the web interface and save the log file for troubleshooting analysis.

1. Go to *Admin & Services > Administration > Diagnostics > Logs*, and locate the AP Logs section.
2. Click the **“Click Here”** link next to *“To show current APs' logs...”* to view the log contents.
3. To save, select the text in the text box and copy/paste it into a text editor.

**FIGURE 319** Click the link to display current AP logs



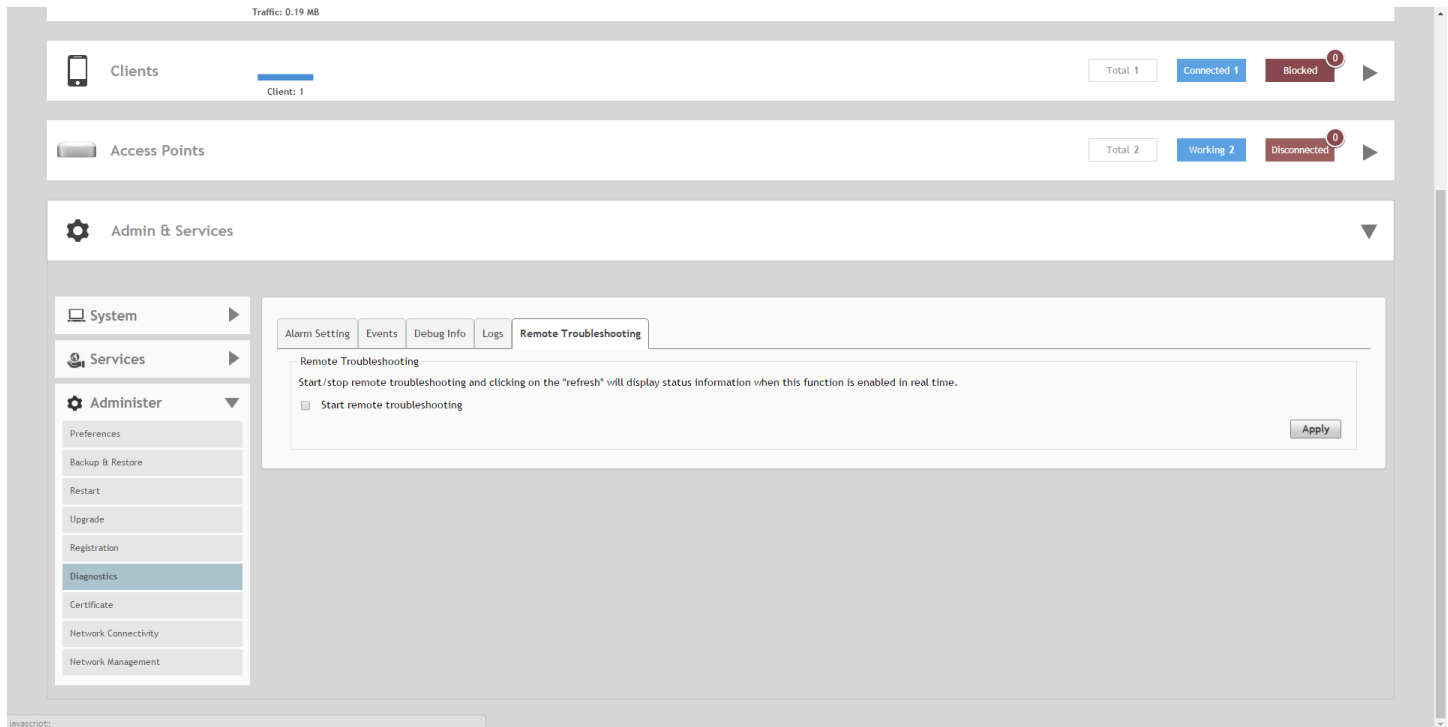
## Enabling Remote Troubleshooting

The Remote Troubleshooting feature allows Ruckus support personnel to connect directly to an Unleashed network deployed at a customer's site for troubleshooting purposes.

### NOTE

Do not enable this feature unless instructed to do so by Ruckus Support.

FIGURE 320 Remote Troubleshooting



### 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.

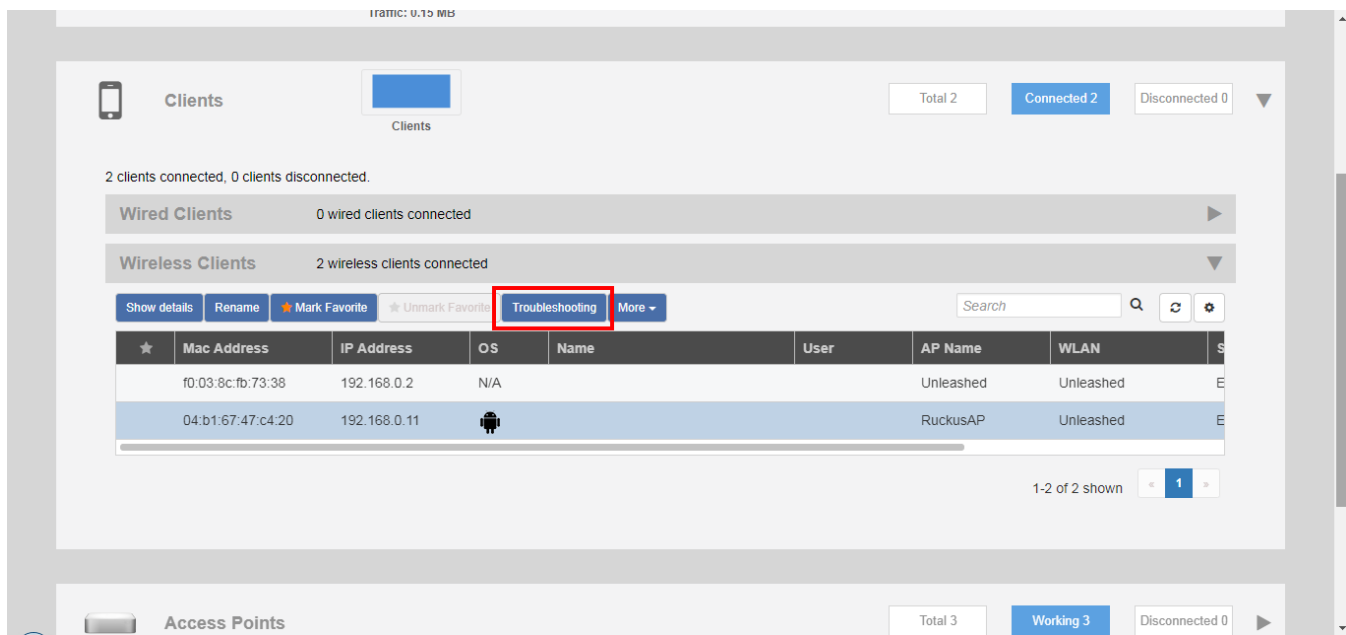
**NOTE**

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**.

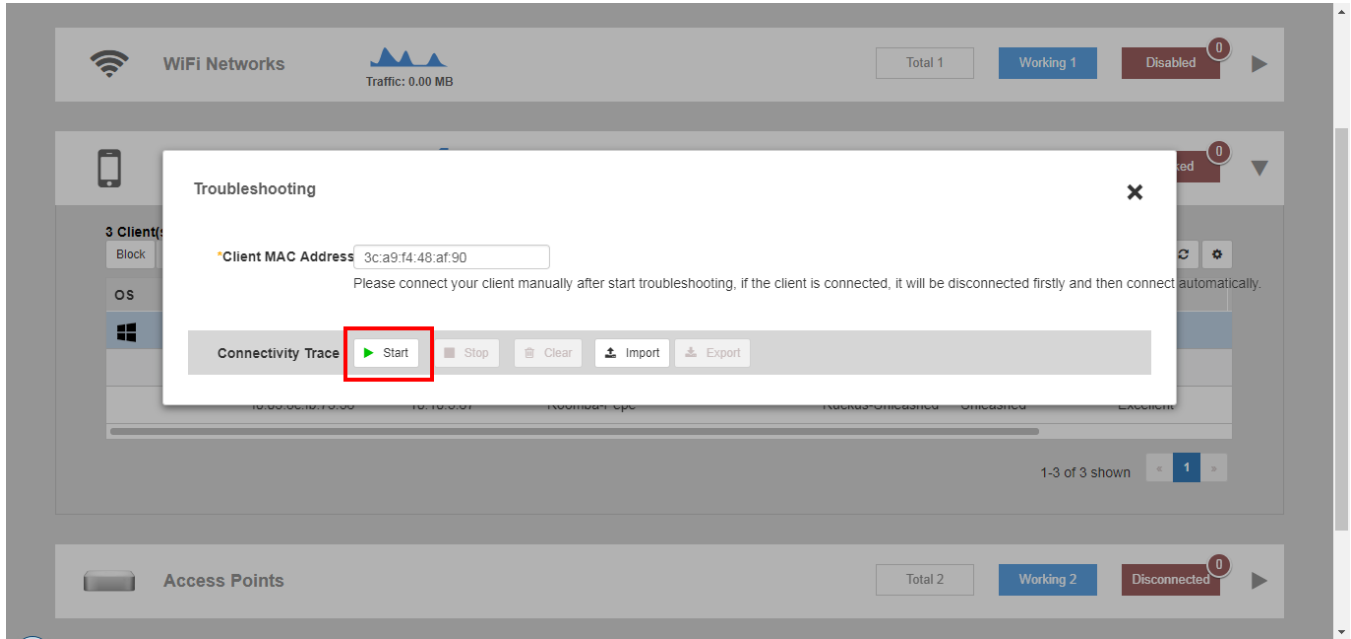
**FIGURE 321** Click Troubleshooting to perform client connectivity trace



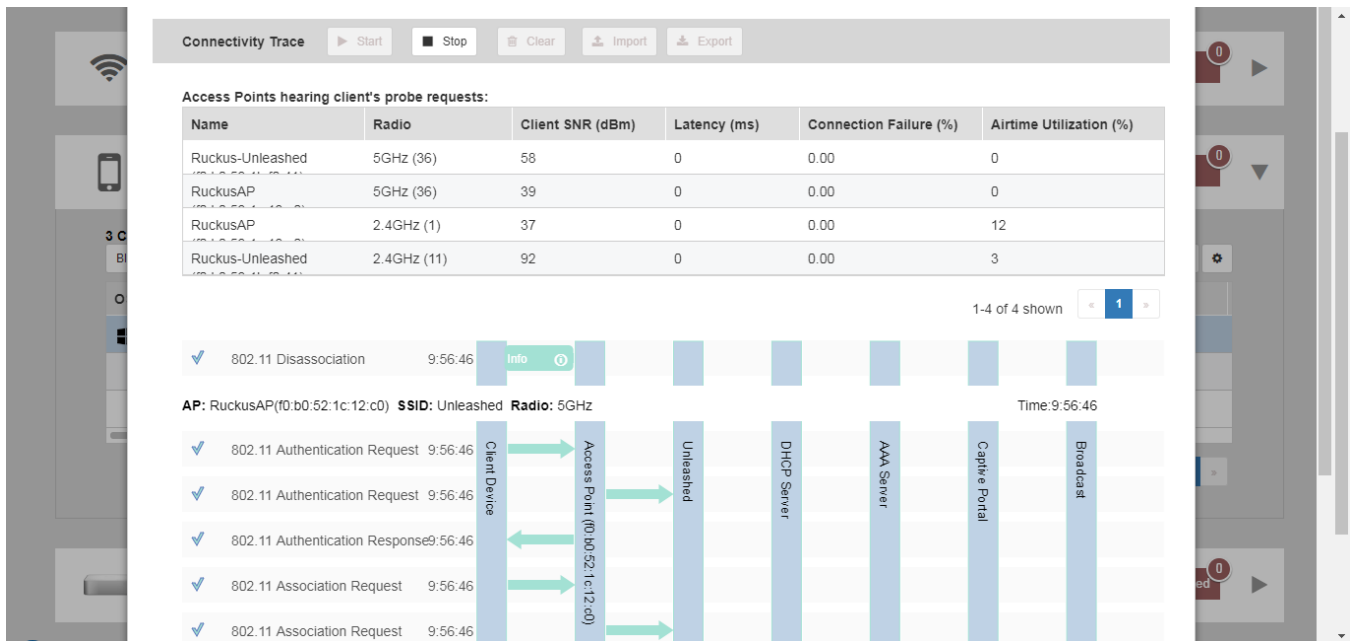
The *Troubleshooting* screen appears.

3. In *Connectivity Trace*, click the **Start** button to begin. The association trace begins. The page refreshes to display detailed results.

**FIGURE 322** Click Start to begin connectivity trace



**FIGURE 323** 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

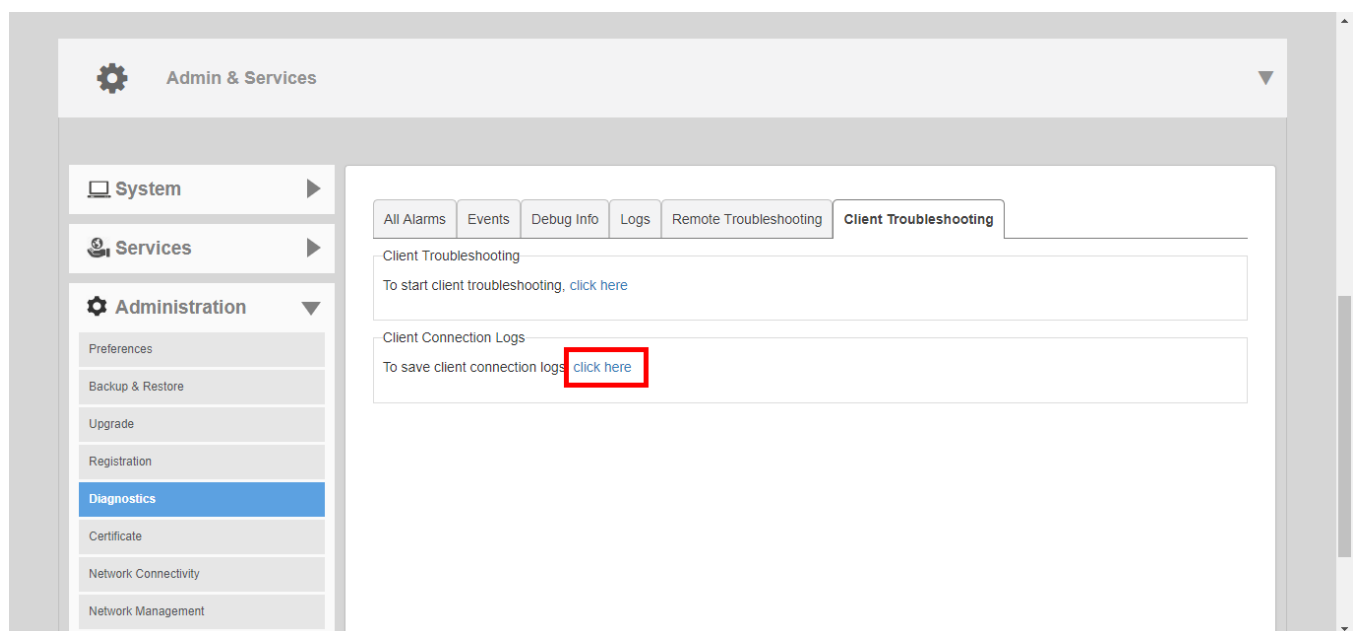
Saving client connection logs may be helpful in troubleshooting client connectivity issues.

Unleashed provides two options for saving client connection logs - download the current log file immediately from the web interface, or configure 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 324** Saving client connection logs to a local computer



## 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

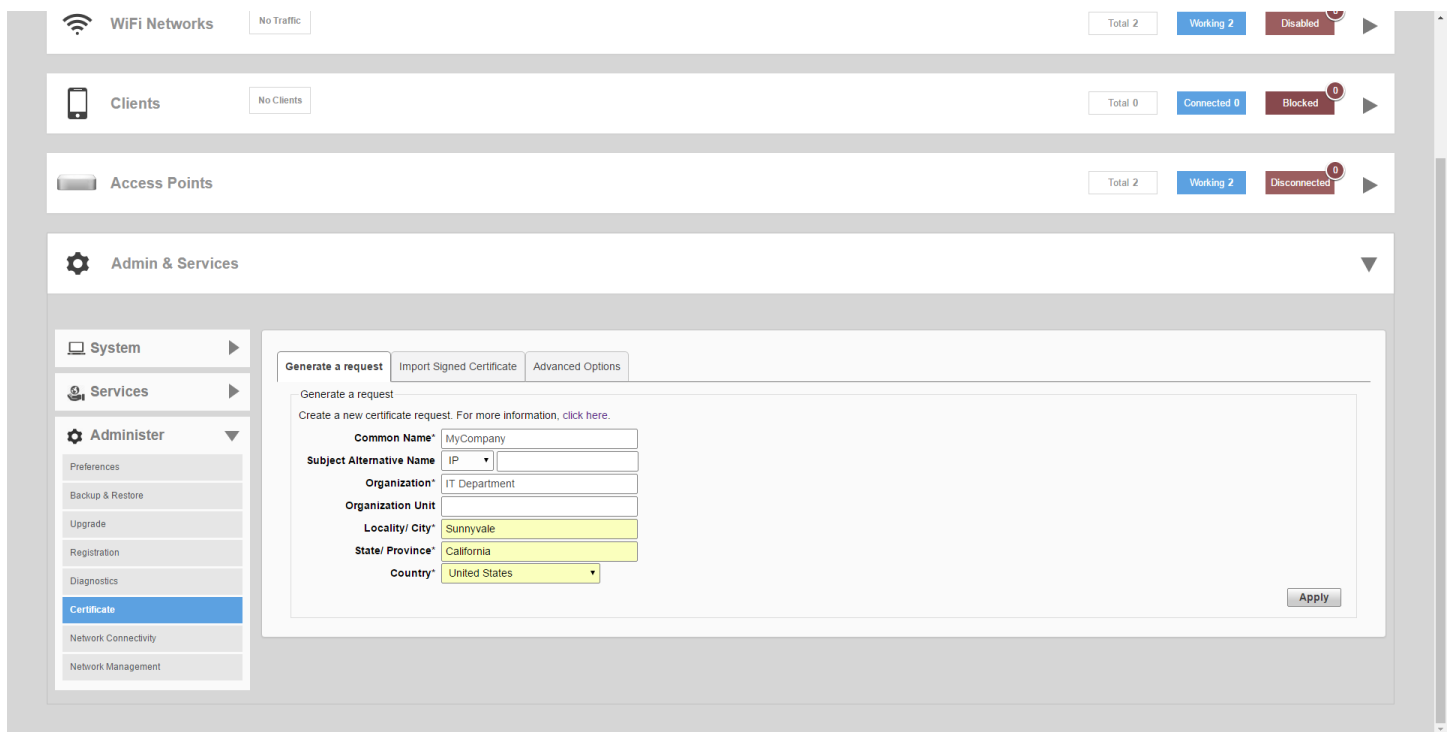
If you do not have an existing SSL certificate, you will need to create a certificate signing request (CSR) file and send it to a certificate authority (CA) to purchase an SSL certificate.

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 325 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 Unleashed Master AP's IP address (e.g., "192.168.0.2"), or a familiar name by which the Unleashed 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 Unleashed Master AP's IP address instead. However, note that some CA's may not allow this.

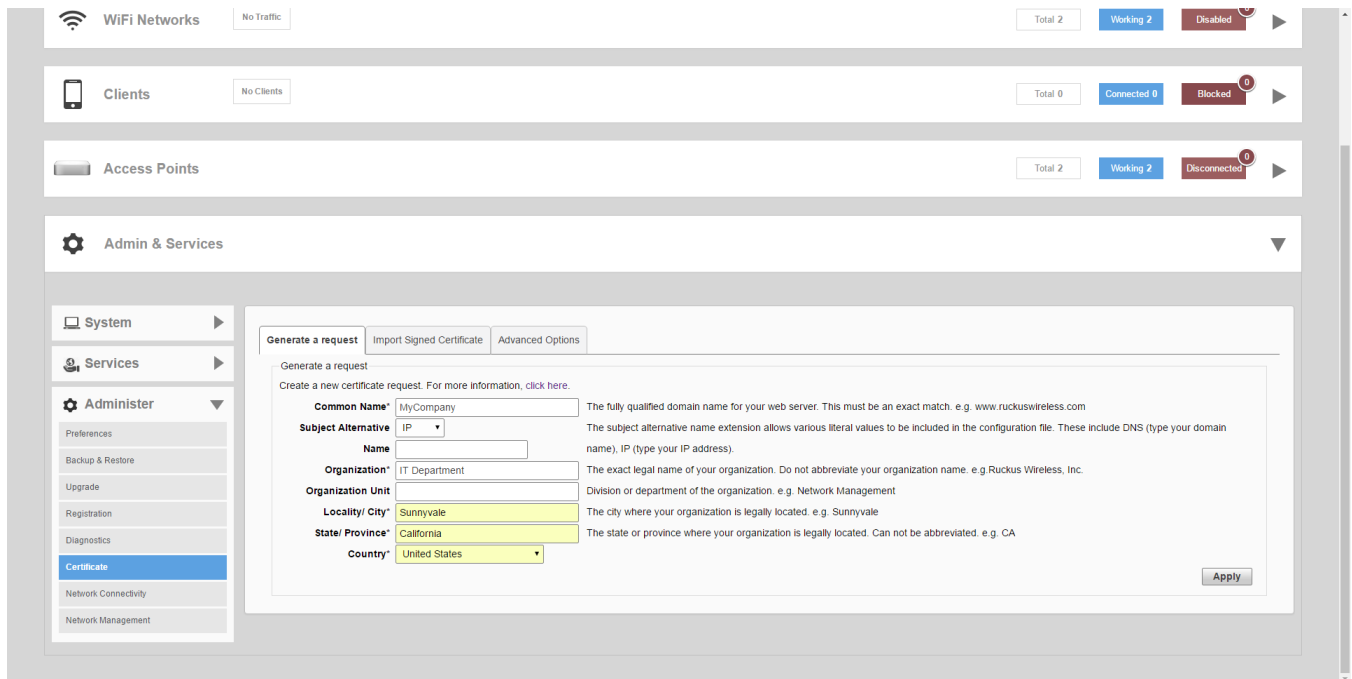
- If you wish to access the Unleashed web UI from a public network via the internet you must use a Fully Qualified Domain Name (FQDN).
- In all cases when using a familiar name there must be an appropriate private or public DNS entry to resolve the familiar name to the Unleashed AP's IP address.
- If you use a familiar name, this name will be shown in the browser's URL whenever accessing the Unleashed 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 326 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
AQUFADCBsDELMAkGA1UEBhMCVVMxFTAVBgNVBAAoTD1Z1cm1TaWduLCBJ
bmMuMR8wHQYDVQQLBgEFBQcBAQRtMGswJAYIKwYBBQUHMAGGGGh0dHA6
Ly9vY3NwLnZ1cm1zaWduLmNvbTBDEBggrBgEFBQcwoY3aHR0cDovL1NW
U1N1Y3VyZS1haWEudmVyaXNpZ24uY29tL1NWU1N1Y3VyZTIwMDUuYW1h
LmN1cm1jBuBggrBgEFBQcBDARiMGChXqBcMFowWDBWfg1pbWFNzS9naWYw
ITAfMAcGBSsOAwIaBBRLa7kolgYMu9BSOJsprEshiyEFGDAmFiRodHRw
Oi8vbG9nb3N5Z2ZkZjpc2lnbi5jb20vdnNsb2dvMS5naWYwDQYJKoZIhvcN
AQEFBQADggEBAI/S2dmm/kgPeVAl sIHmx-
751o4oq8+fwehRDBmQDaKiBvVXGZ5ZMnoc3DMYDjx0SrI91kPsn223CV
3UVBZo385g1T4iKwXgcQ7WF6QcUYOE6HK+4ZGcHermFf3fv3C1-
FcCjq+zEu8ZboUf3fWbGprGRA+MR/dDI1dTptSUG7/zWjX05jC//
0pykSlDW/q8hgO8kq30S8JzCwkqrXJfQ050N4TJtgb/
YC4gwH3BuB9wqprjUahTiK1V1-
ju9bHB+bFkMWIIMIXc1Js62Jc1WzwFgaGUS2DLE8xICQ3wU1ez8RUPGn
wSxAYtZ2N7zDxYDP2tEi05j2cXY708mR3ni0C30=
-----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 Unleashed. Refer to [Importing an SSL Certificate](#) on page 377 for instructions.



## Importing an SSL Certificate

After you receive the signed certificate from the Certificate Authority, you must import it into Unleashed.

To import a signed certificate:

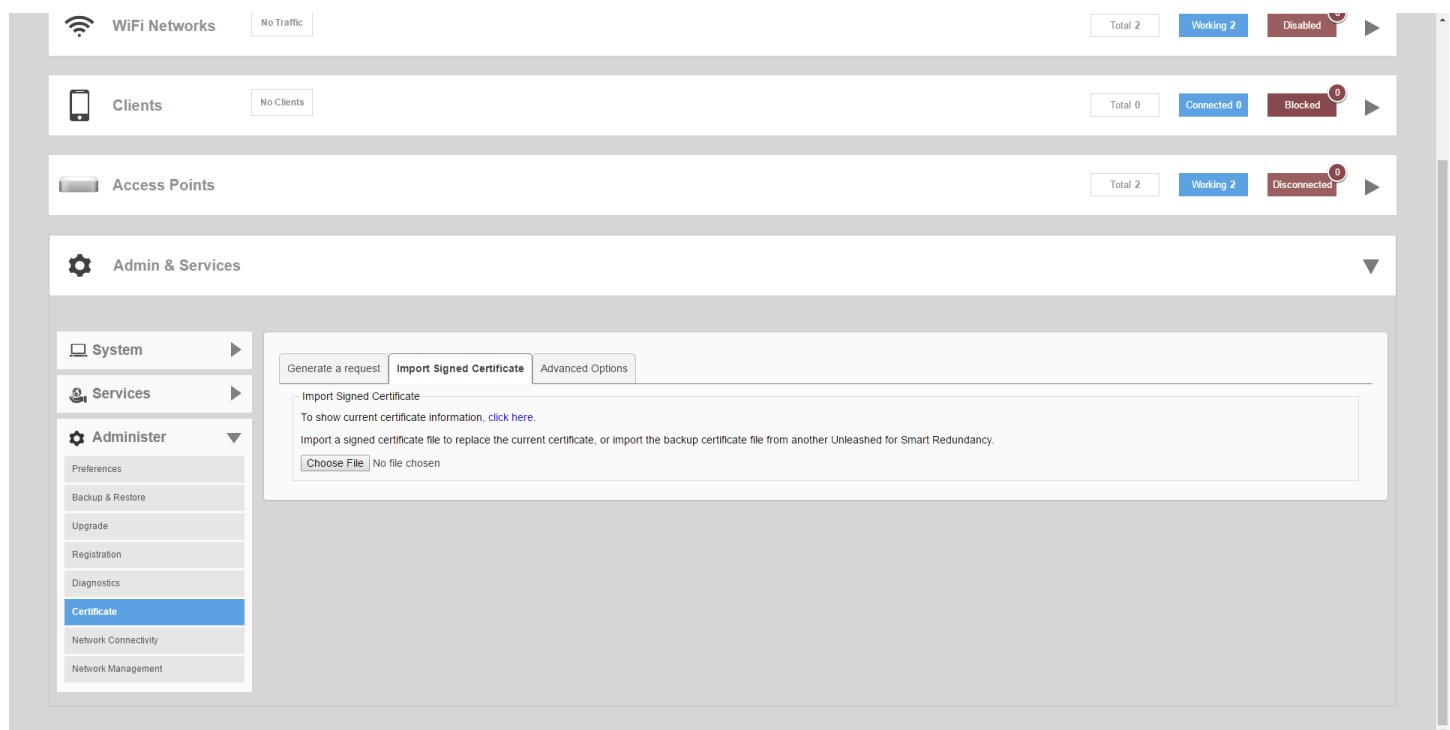
1. Click the **Browse** button and select the file that contains the certificate (in PEM format) to upload it.
2. If there are no intermediate CA certificates, then click the **Import** button to install the uploaded certificate.

### NOTE

If the certificate does not match the currently installed private key you will be prompted to upload the correct private key.

3. If your Unleashed certificate was issued by an intermediate CA, then you must also import the intermediate CA's certificate (as well as all other intermediate CA certificates in the path to the root CA). In that event, you would receive intermediate CA certificate download instructions from the certificate vendor. To import an intermediate certificate:
  - a) After selecting the end certificate, click on 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 format) to upload it.
  - d) If there are no additional intermediate certificates, click the **Import** button to install the uploaded certificate.
4. Alternatively, you can simplify this process by appending the intermediate CA certificate(s) to the Unleashed certificate file. Then, you just need to import a single file. The intermediate certificate(s) will be imported automatically. In this case, you will see multiple ---BEGIN CERTIFICATE--- and ---END CERTIFICATE--- pairs in the file.

**FIGURE 327** Import signed certificate



## SSL Certificate Advanced Options

The **Advanced Options** section allows you to perform additional certificate management functions.

These include the following:

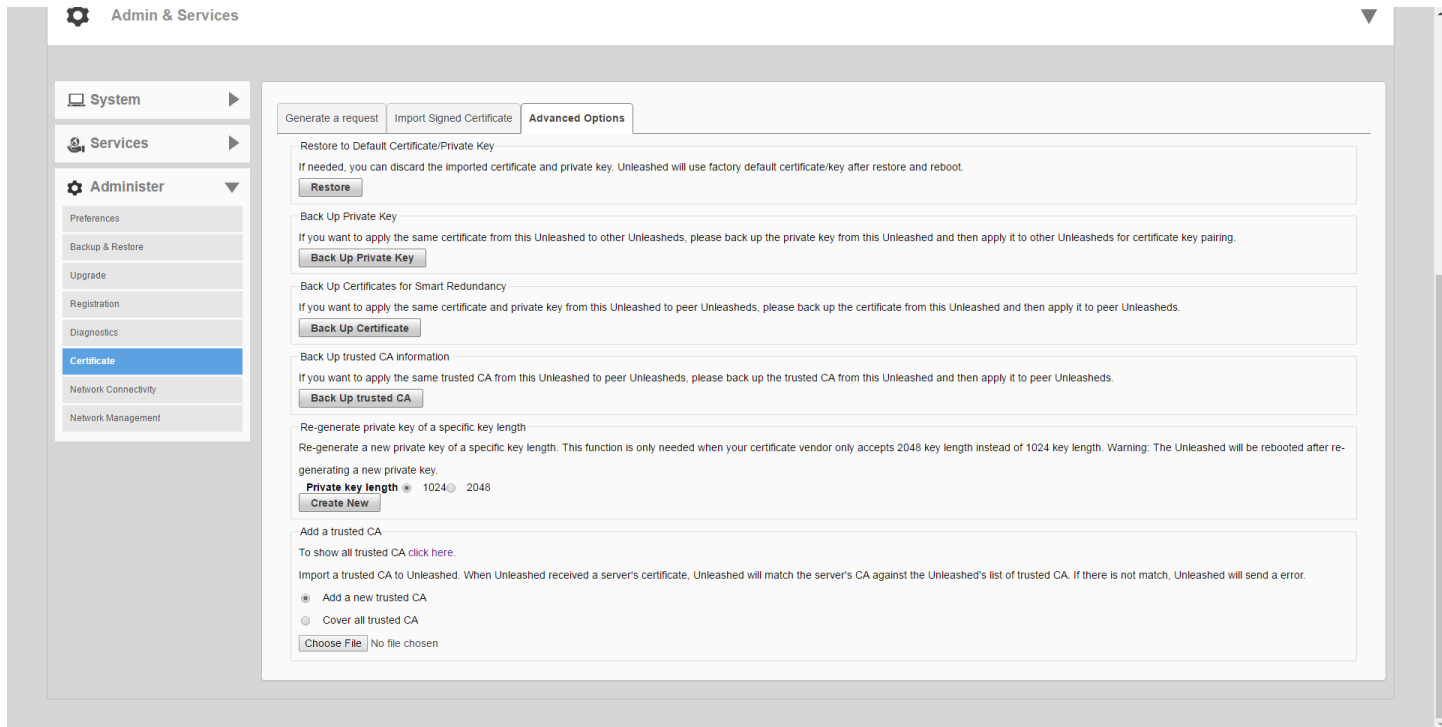
- **Restore to Default Certificate/Private Key:** This deletes any certificate and private key that has been imported, and restores the factory default certificate/private key after restore and reboot.

### 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 Authority 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

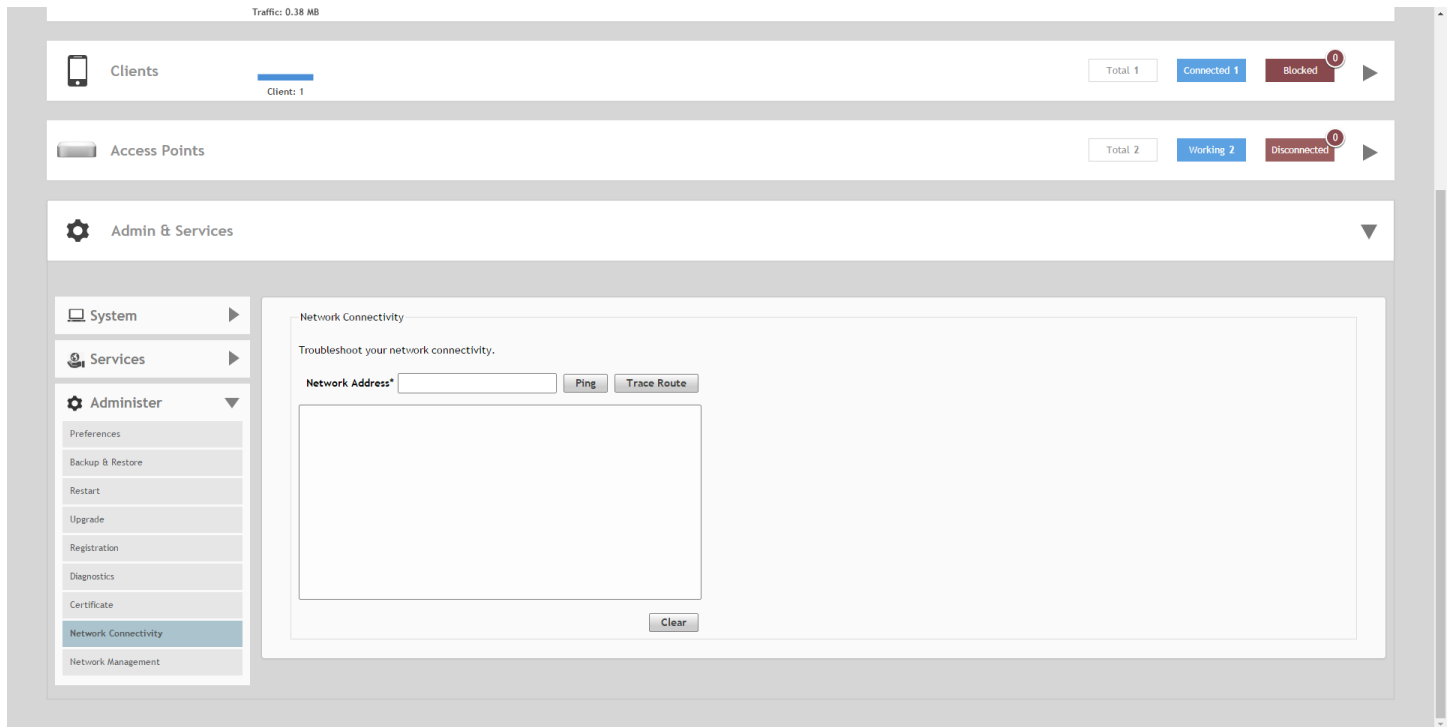
FIGURE 328 SSL Certificate Advanced Options



## 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 329 Using Ping and Traceroute to test network connectivity



## Network Management

Unleashed provides support for Simple Network Management Protocol (SNMP v2 and v3), which allows you to query system information such as system status, AP status, AP Ethernet port status, etc.

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>.

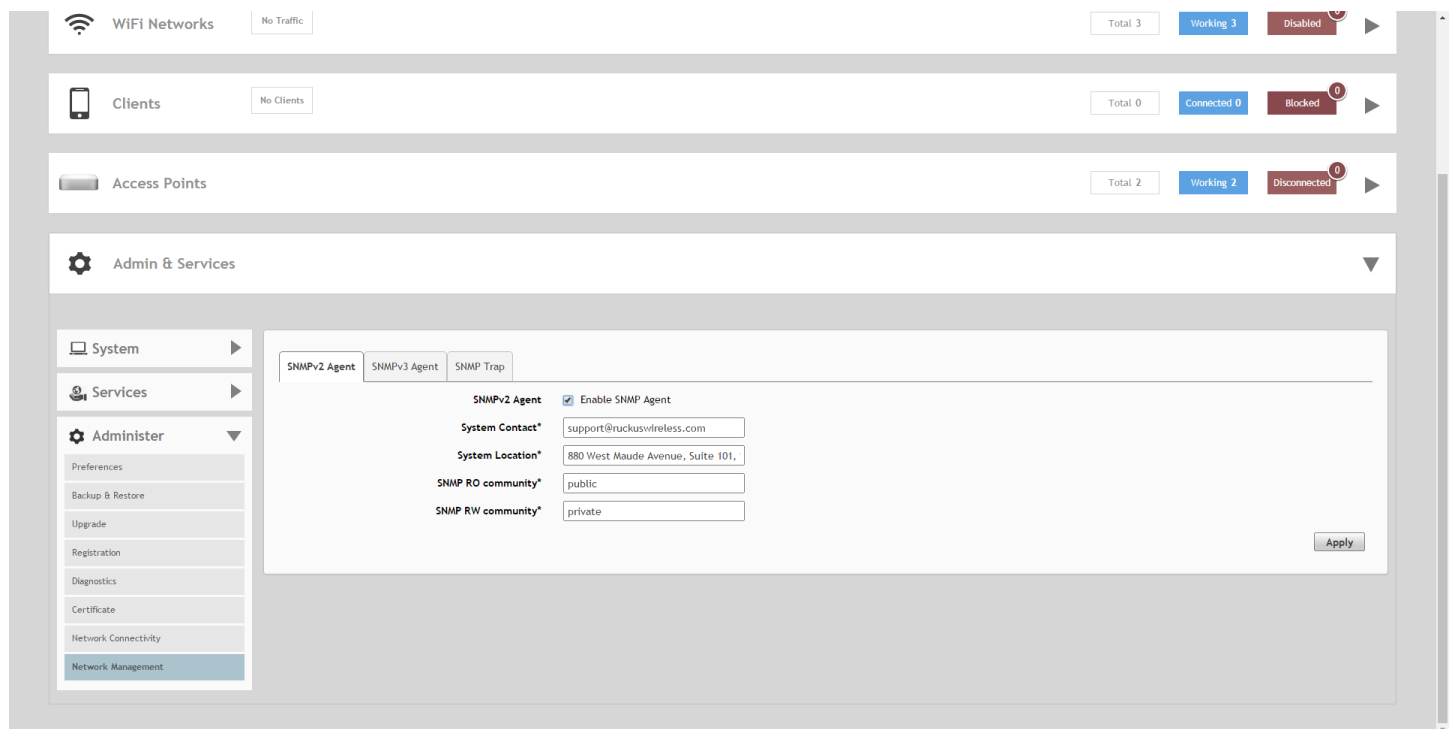
## SNMPv2

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 330 SNMPv2 Agent



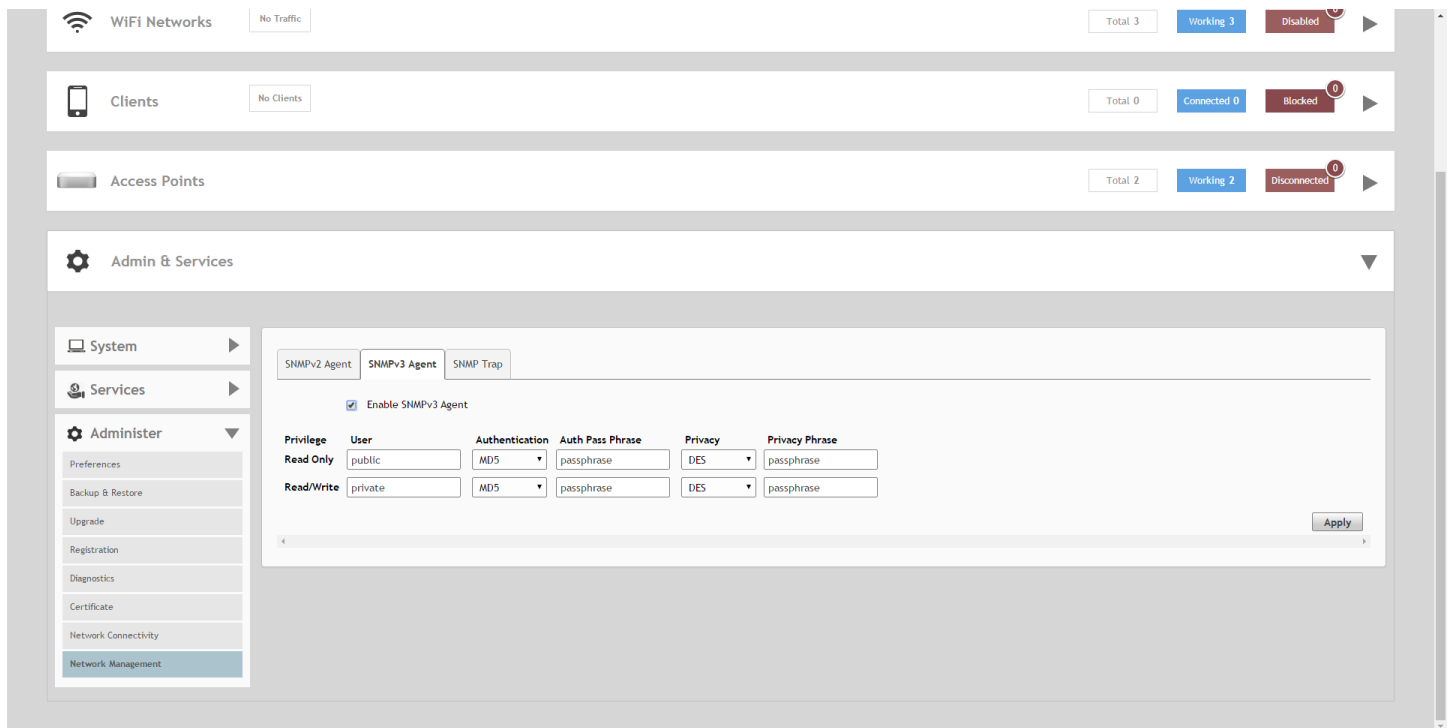
## SNMPv3

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.

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

FIGURE 331 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.

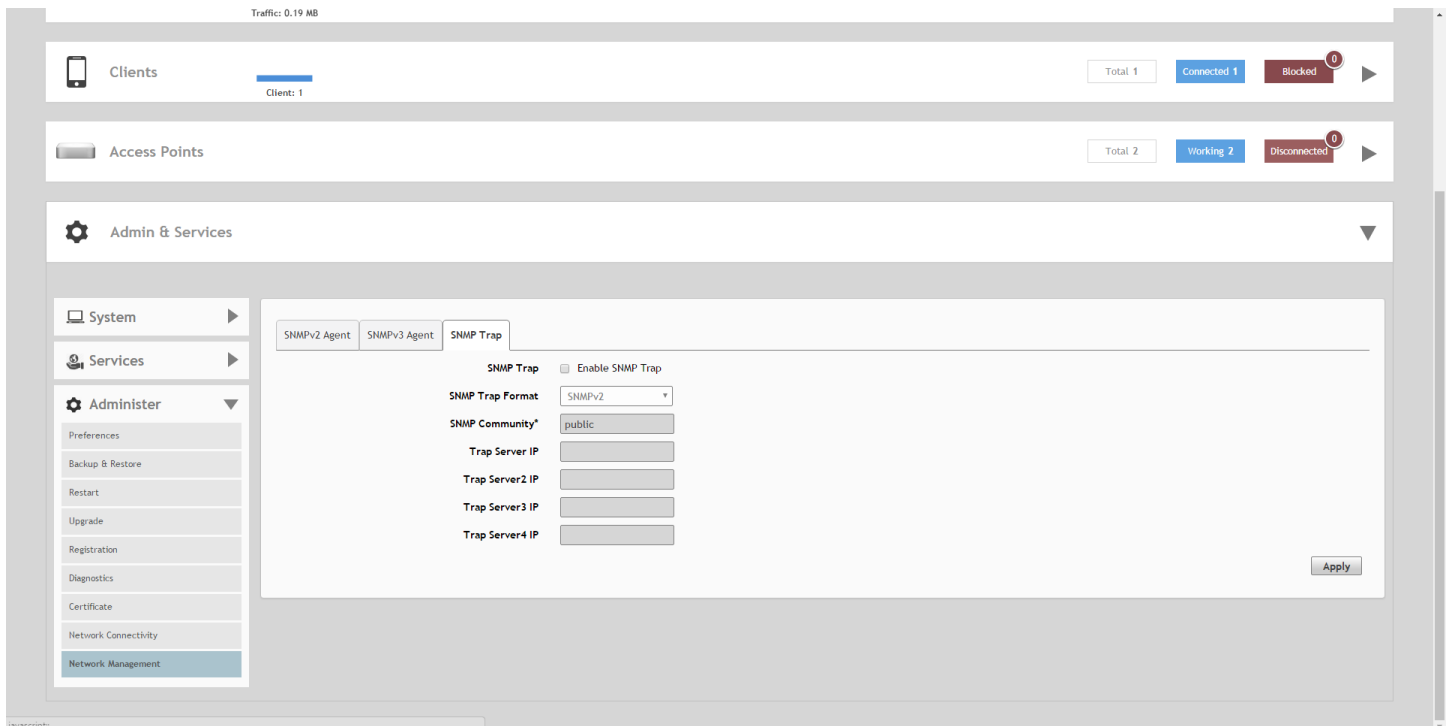
Enable this feature if you want to automatically receive notifications for AP and client events that indicate possible network issues.

To enable SNMP trap notifications:

- Go to **Admin & Services > Administer > Network Management**.
- 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 332 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:

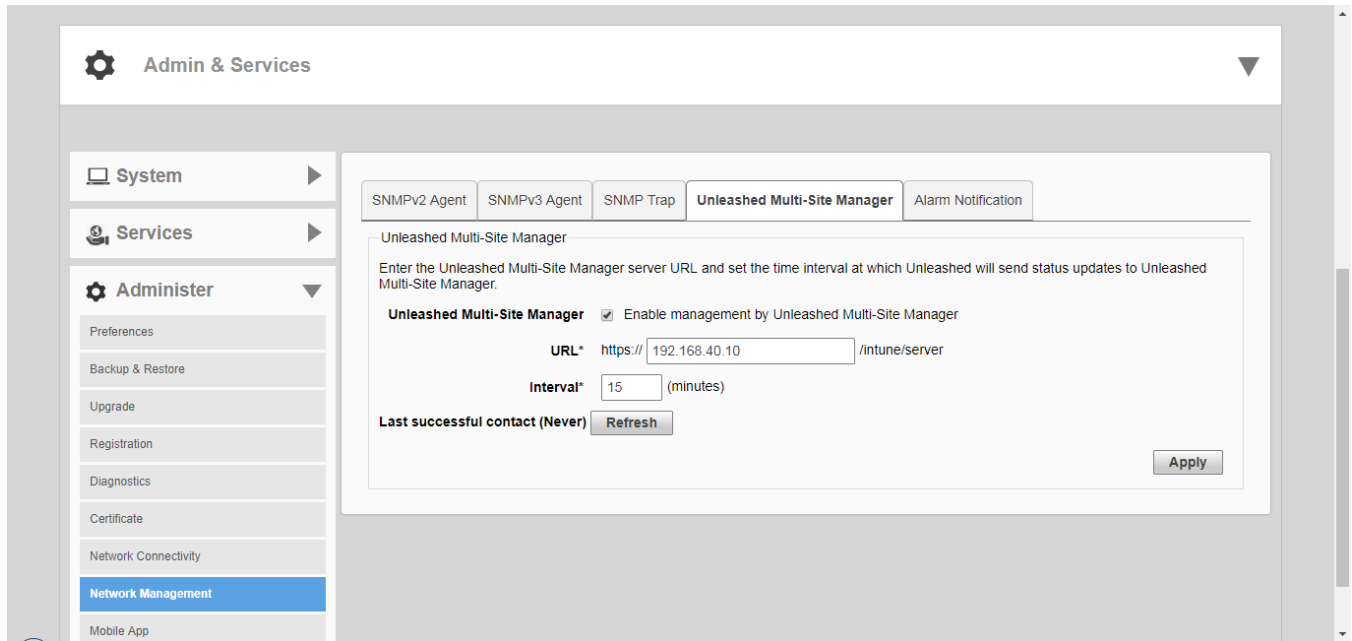
- **Monitoring:** Provides the ability to view the overall health status of all Unleashed networks, events and alarms, placement of APs on a world map, and connected client information from the dashboard.
- **Reporting:** Detailed statistics reports are available including device inventories, client 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 333** Enabling Unleashed Multi-Site Manager management



### Configuring Alarm Event Notification Settings

The Unleashed 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 via email or via the Unleashed mobile app.

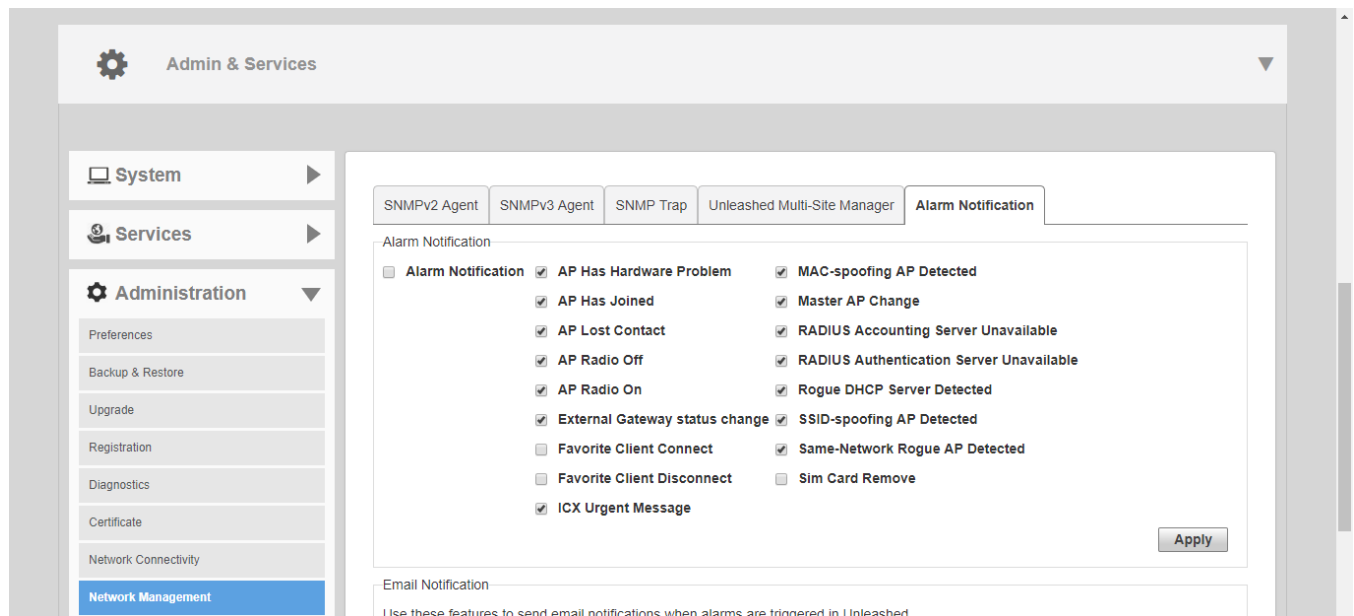
To configure alarm event notifications and email/mobile app delivery:

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 334** Alarm Notification settings



## Enabling Mobile App Remote Management

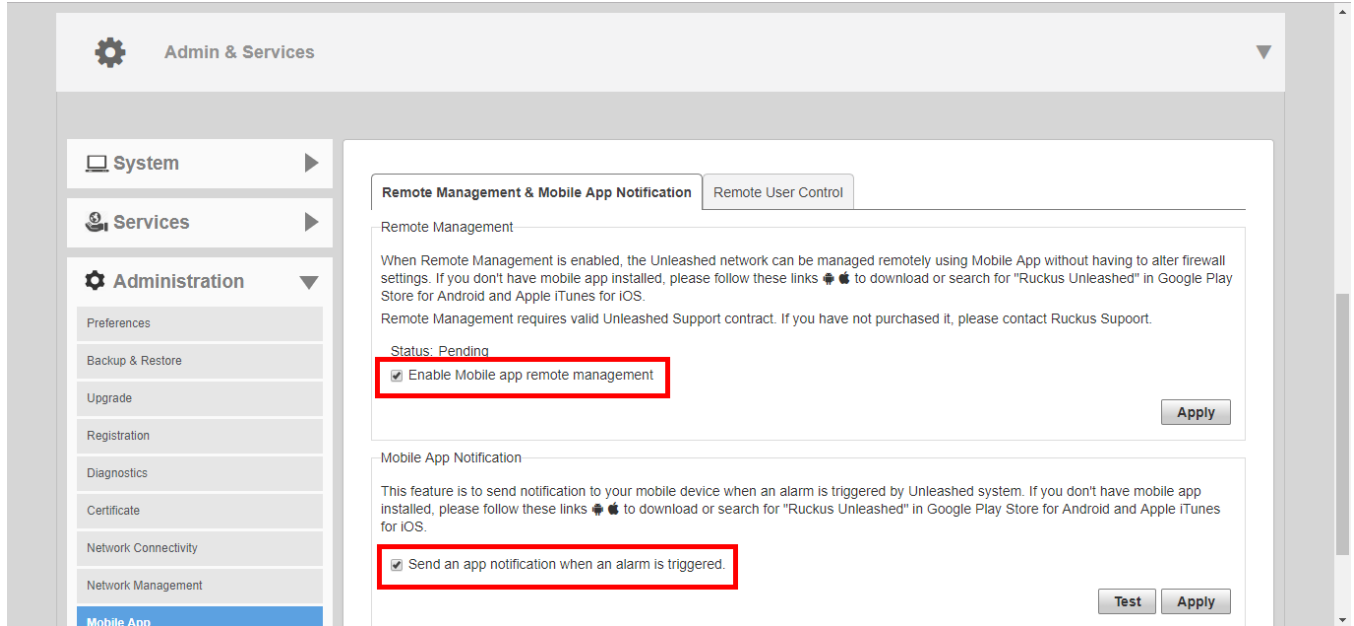
The Unleashed mobile app provides another way to manage your Unleashed network - using an Android or iOS client.

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 335** Enabling mobile app remote management

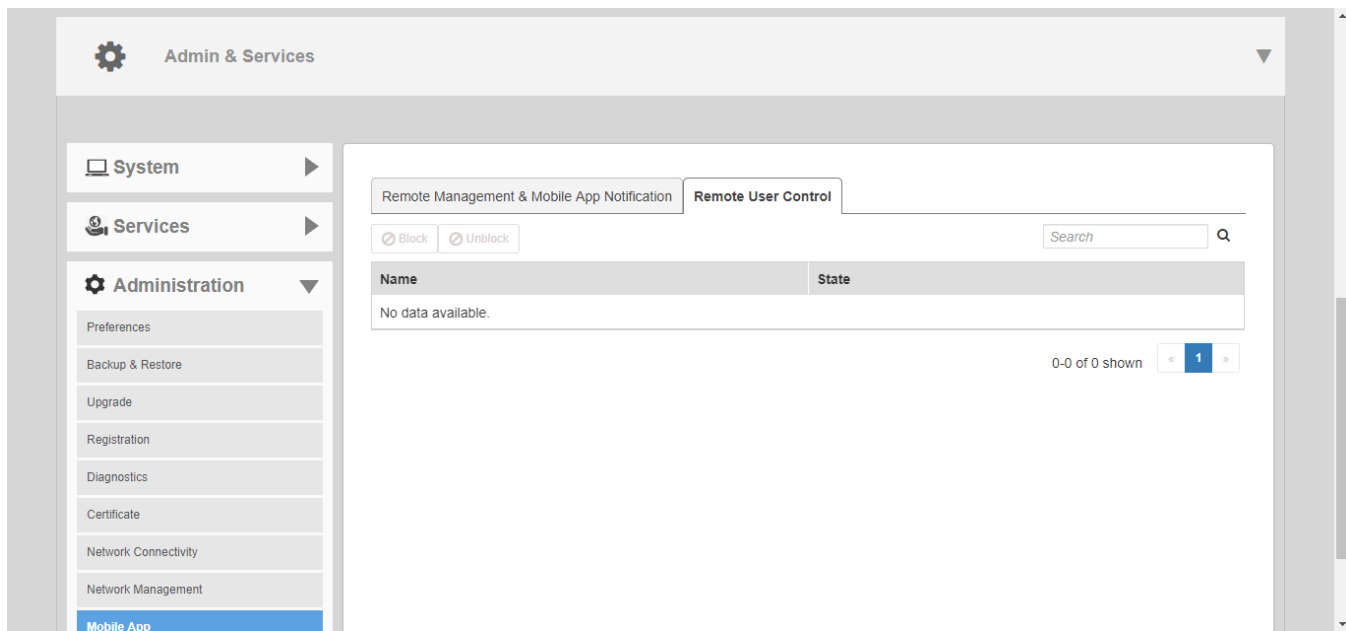


3. Optionally, enable the check box next to **Enable Mobile app remote management**, and click **Apply**.

**FIGURE 336** Remote Management

- 4. On the *Remote User Control* tab, you can view mobile app connections and block or unblock mobile app clients.

**FIGURE 337** Remote user control





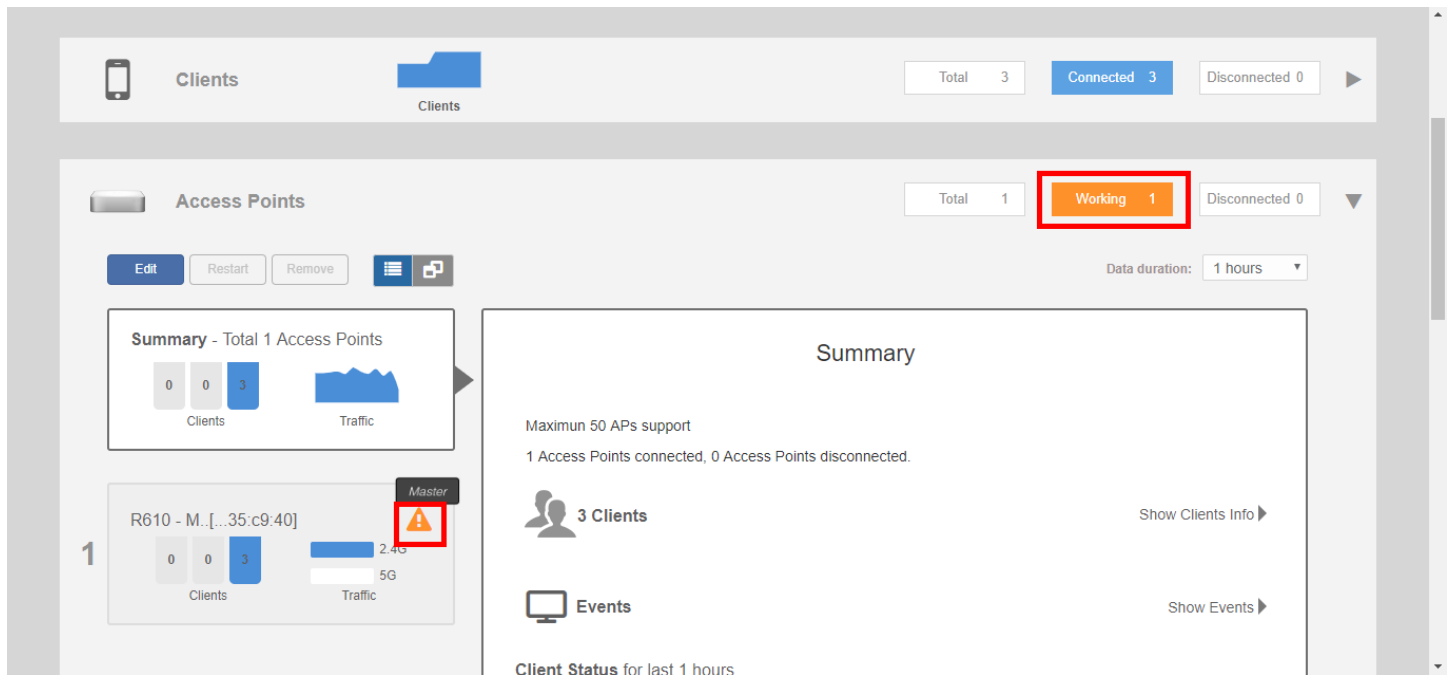
# Unleashed Access Point Power Supply Considerations

- AP Power Warnings..... 389
- Power Limitations by PoE Mode and AP Model..... 391

## AP Power Warnings

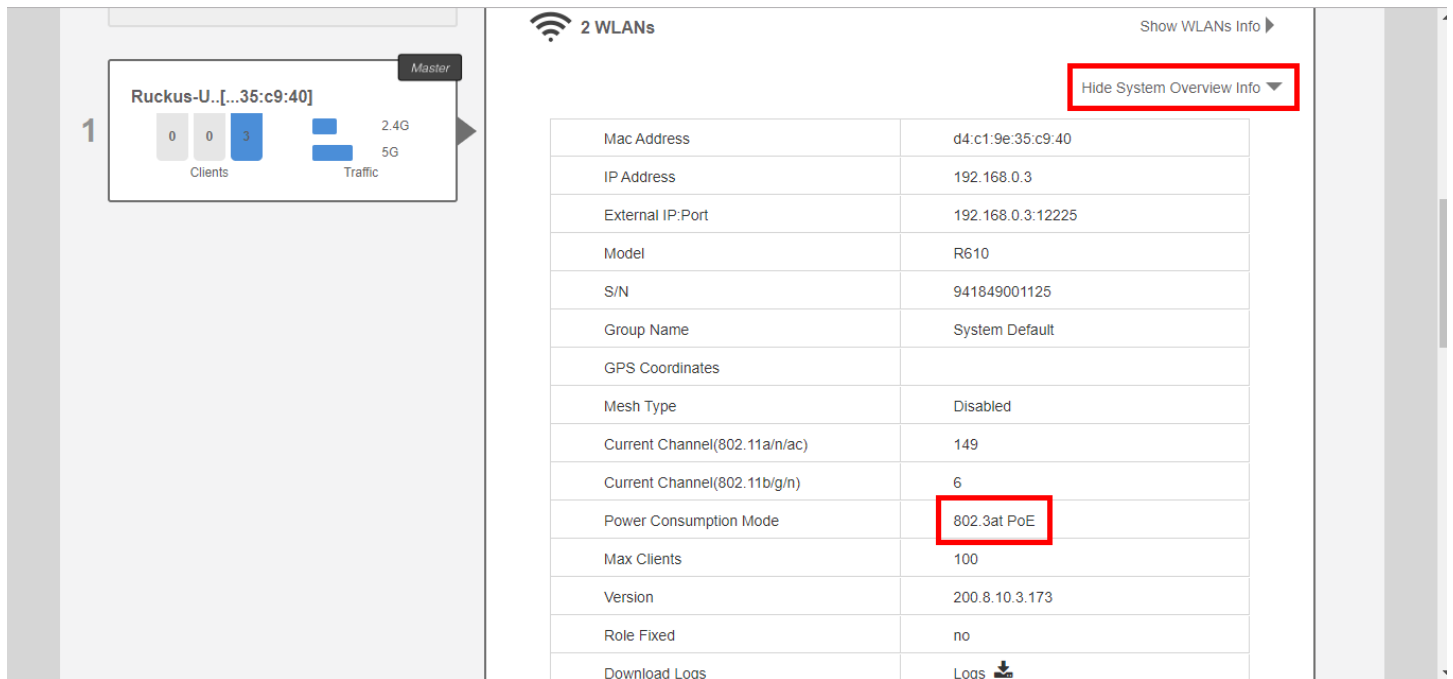
Beginning with release 200.8, the Unleashed dashboard displays warning icons when an AP is operating in reduced power mode.

**FIGURE 338** Warning icons indicate an AP is operating in reduced power mode



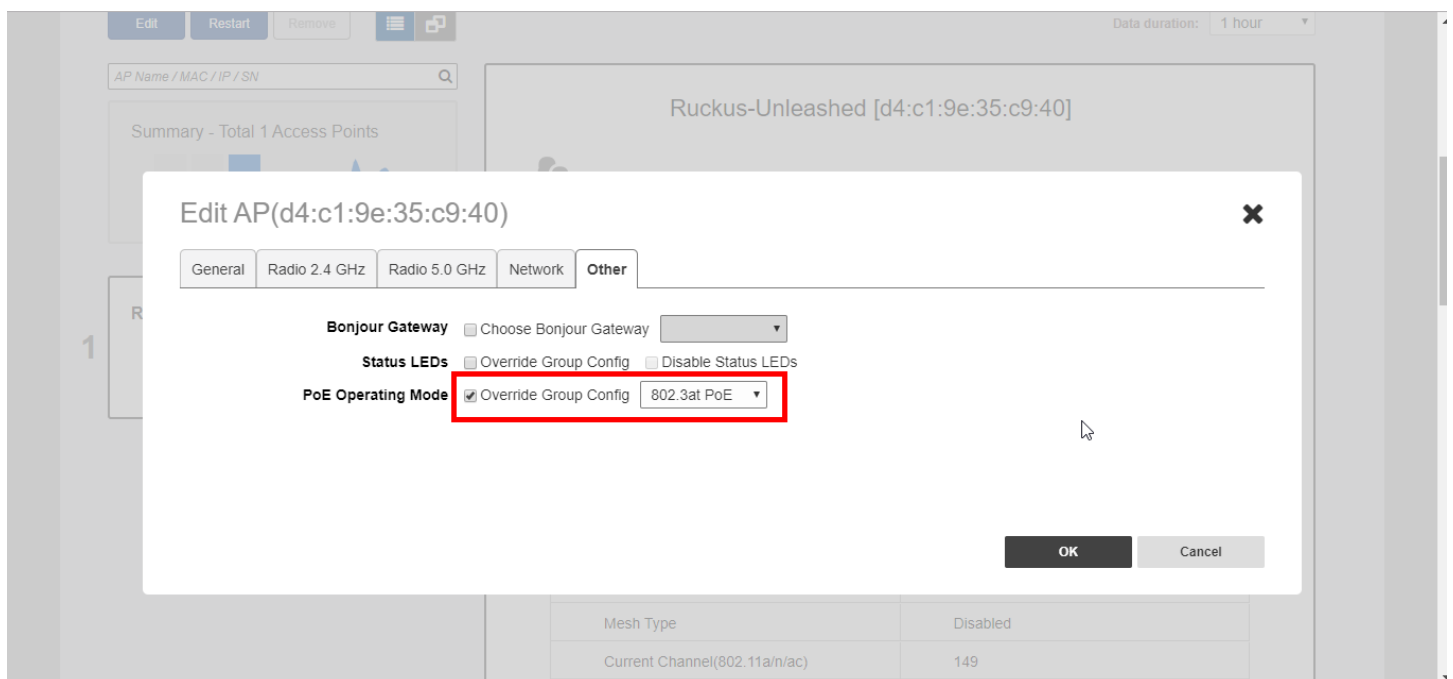
If a warning icon appears, click **Show System Overview** and locate the **Power Consumption Mode** entry. Refer to *Power Limitations by PoE Mode and AP Model* to see what limitations are in effect.

FIGURE 339 Show 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 340 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.

### R750

**TABLE 25** R750 PoE Modes

	LLDP Power Ask	2.4G Tx/Rx	5G Tx/Rx	2.5Gbps Eth	1Gbps Eth	USB	IoT
DC		4/4	4/4	Enabled	Enabled	Enabled	Enabled
802.3af		2/4	2/4	Enabled	Disabled	Disabled	Disabled
802.3at	25W	4/4	4/4	Enabled	Enabled	Enabled	Enabled
PoE injector (Model 480125A) 60W		4/4	4/4	Enabled (1Gbps speed)	Enabled	Enabled	Enabled

### R720

**TABLE 26** 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	
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 27** 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

### R610

**TABLE 28** 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

## T610

**TABLE 29** 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 30** 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



COMMScope®  
**RUCKUS**®

© 2020 CommScope, Inc. All rights reserved.  
Ruckus Wireless, Inc., a wholly owned subsidiary of CommScope, Inc.  
350 West Java Dr., Sunnyvale, CA 94089 USA  
[www.ruckuswireless.com](http://www.ruckuswireless.com)