USER GUIDE



# **RUCKUS Unleashed 200.13 User Guide**

Supporting Release 200.13

Part Number: 800-73277-001 Rev A Publication Date: October 2022

## **Copyright, Trademark and Proprietary Rights Information**

© 2022 CommScope, Inc. All rights reserved.

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

### **Export Restrictions**

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

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

### Disclaimer

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

### **Limitation of Liability**

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

#### **Trademarks**

ARRIS, the ARRIS logo, COMMSCOPE, RUCKUS, RUCKUS WIRELESS, the Ruckus logo, the Big Dog design, BEAMFLEX, CHANNELFLY, FASTIRON, ICX, SMARTCELL and UNLEASHED are trademarks of CommScope, Inc. and/or its affiliates. Wi-Fi Alliance, Wi-Fi, the Wi-Fi logo, Wi-Fi Certified, the Wi-Fi CERTIFIED logo, Wi-Fi Protected Access, the Wi-Fi Protected Setup logo, Wi-Fi Protected Setup, Wi-Fi Multimedia and WPA2 and WMM are trademarks or registered trademarks of Wi-Fi Alliance. All other trademarks are the property of their respective owners.

# Contents

Preface	9
Contacting RUCKUS Customer Services and Support	9
What Support Do I Need?	
Open a Case	
Self-Service Resources	
Document Feedback	
RUCKUS Product Documentation Resources	
Online Training Resources	
Document Conventions	
Notes, Cautions, and Safety Warnings	
Command Syntax Conventions	11
Introducing RUCKUS Unleashed	
Overview	
Network Overview	
Unleashed Dedicated Master Network Overview	
Feature Parity with ZoneDirector	
Limitations and Deviations from ZoneDirector	
RUCKUS Unleashed-Only Features	
Unleashed Access Point Physical Features	
C110	
E510	22
H320	
Н350	
H510	
H550	
M510	
R320	
R350	57
R510	
R550	
R610	
R650	
R710	
R720	
R750	
R850	
T310 Family	
T350 Family	100
T350SE	
T610 and T610s	
T710 and T710s	
Т750	
T750SE	
Setting Up an Unleashed Wi-Fi Network	
Overview of the Setup Process	129

Step 1: Unpack and Install the Unleashed Master AP	
Step 2: Configure Your Unleashed Network	
Step 2a: Setup Using the Mobile App	130
Step 2b: Setup Using a Web Browser	135
Step 2c: Setup Using the Command Line Interface	152
Step 3: Customize Your Wireless LANs	156
Step 4: Deploy Additional Unleashed Member Access Points	159
Using the Admin Interface	161
Unleashed Administration Interface Overview	
Navigating the Dashboard	
Using the Dashboard Components	
Internet	
Dedicated Master	
WiFi Networks	
Clients	
Access Points	
Switches	
Admin & Services	
Dedicated Master Configuration	
Dedicated Master Overview	
Converting an Unleashed Master AP to Dedicated Master	
Checking Whether the Current Active Master AP is an R750 or R850	
Converting an Active Master AP to Dedicated Master	
Joining a Member AP to the Dedicated Master Network	
Joining a Member AP to Dedicated Master Using Option 43 (Recommended)	
Placing a Member AP in the Same Network as Dedicated Master	
Setting the Dedicated Master IP Address in the Member AP CLI	
Dedicated Master AP or Member AP Behind NAT	
Basic NAT Topologies	
Configuration Requirements for Ports or IP Addresses for NAT Topologies	
Checking Dedicated Master Status in the Unleashed Web Interface	
Smart Redundancy Configuration	
Smart Redundancy Setup Overview	
Configuring Dedicated Master for Smart Redundancy	
Checking the Standby Dedicated Master	
Disabling Smart Redundancy	185
WLAN Configuration	
WLAN Configuration Overview	189
WLAN Usage Types	189
Creating a New WLAN	
802.1X EAP WLANs	
802.1X WLAN Survivability	
Guest WLANs	196
Deploying a Guest WLAN	196
Hotspot WLANs	
Configuring Global WLAN Settings	
Editing an Existing WLAN	
Using a QR Code to Join a Wi-Fi Network	
Deleting a WLAN	

Disabling a WLAN Temporarily	
Advanced WLAN Configuration	
Advanced WLAN Configuration Overview	
Configuring Advanced WLAN Options	
Zero-IT and DPSK Settings	
Zero-IT	
Dynamic PSK	
Enabling Zero-IT for a WLAN	
Enabling DPSK for a WLAN	
WLAN Priority Settings	
Access Control Settings	
Application Policies	
Creating an Application Control Policy	
Radio Control Settings	
Creating Separate WLANs for 2.4 GHz and 5 GHz Radios	
Other Advanced WLAN Settings	
Configuring Client Isolation Allowlists	
Bypass Apple CNA	
Access Point Configuration	280
Access Point Configuration	
Show Mesh Topology	
Show Mesh Topology	
Show Events and Alarms	
Configuring Global AP Settings	
Radio (2.4G)	
Radio (2.46) Radio (5G)	
Other	
Monitoring an Individual AP	
Show Client Info	
Show WLANs Info	
Show AP Info	
Show Ar mild	
Client Status and Traffic Graphs	
Configuring an Individual AP	
Renaming an AP	
Working with AP Groups	
Viewing AP Group Members	
Modifying the System Default AP Group	
Creating a New AP Group	
Modifying Model Specific Controls	
Configuring AP Ethernet Ports	
Restarting an AP	
Removing an AP	
ICX Switch Management	
ICX Switch Management Overview	
Requirements	
Preparing an ICX Switch for Unleashed Management	
Approving a New Switch to Join Unleashed	
Monitoring Connected ICX Switches	

Accessing the RUCKUS Switch Home Page	
Managing Switch Ports	
Backup and Restore Switch Configuration	
Upgrading ICX Switch Firmware	
Working with Clients	240
Client Management Overview	
Viewing the Clients List	
Renaming a Client	
Deleting a Client	
Permanently Blocking a Client Device	
Marking a Client as a Favorite	
Running a SpeedFlex Performance Test on a Wireless Client	
Client Connection Troubleshooting	
Marking a Client as a Legacy Device	
Adding User Accounts to the Internal User Database	
Authenticating Clients Using an External Database	
Configuring Admin & Services Settings	
Admin & Services Overview	
System Settings	
System Info Settings	
IP Settings	
Configuring the System Time	
Setting the Country Code	
Configuring User Roles	
Adding New Users to the Local Database	
Changing an Existing User Account	
Importing Users into the Local Database using CSV File	
Deleting a User Record	
Changing User Password	
Mesh Networking	
Enabling Log Delivery to Remote Syslog Server	
Services	
AAA Servers	
Access Control	
Application Recognition and Control	
Bonjour Gateway	
Dynamic PSK	
Guest Access Services	
Hotspot Services	
Radio Control	
WIPS	
URL Filtering	
Wi-Fi Calling	456
Tunnel Configuration	
Administration Settings	
Preferences	
Backup and Restore	
Upgrade	
Diagnostics	

Working with SSL Certificates	
Testing Network Connectivity	
Network Management	
Enabling Mobile App Remote Management	
Technical Support	
Unleashed Access Point Power Supply Considerations	
AP Power Warnings	
Power Limitations by PoE Mode and AP Model	
R850	
R750	
R720	501
R710	502
R650	502
R610	502
R550	502
H550	
T610	503
M510	503
Т750	503
T750SE	504
Т350с	
T350d	505
T350SE	

# Preface

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

## **Contacting RUCKUS Customer Services and Support**

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

For product support information and details on contacting the Support Team, go directly to the RUCKUS Support Portal using https://support.ruckuswireless.com, or go to https://www.commscope.com/ruckus 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 <a href="https://support.ruckuswireless.com/contact-us">https://support.ruckuswireless.com/contact-us</a> and Live Chat is also available.
- Worldwide toll number for our support organization. Phone charges will apply: +1-650-265-0903

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

### **Self-Service Resources**

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

- Technical Documentation—https://support.ruckuswireless.com/documents
- Community Forums—https://community.ruckuswireless.com
- Knowledge Base Articles—https://support.ruckuswireless.com/answers
- Software Downloads and Release Notes-https://support.ruckuswireless.com/#products\_grid
- Security Bulletins—https://support.ruckuswireless.com/security

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

## **Document Feedback**

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

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

When contacting us, include the following information:

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

For example:

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

## **RUCKUS Product Documentation Resources**

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

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

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

## **Online Training Resources**

To access a variety of online RUCKUS training modules, including free introductory courses to wireless networking essentials, site surveys, and products, visit the RUCKUS Training Portal at https://commscopeuniversity.myabsorb.com/. The registration is a two-step process described in this video. You create a CommScope account and then register for, and request access for, CommScope University.

## **Document Conventions**

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

#### **TABLE 1** Text Conventions

Convention	Description	Example
monospace	Identifies command syntax examples	<pre>device(config)# interface ethernet 1/1/6</pre>
bold	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> .
italics	Publication titles	Refer to the RUCKUS Small Cell Release Notes for more information.

## Notes, Cautions, and Safety Warnings

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

#### NOTE

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

#### ATTENTION

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



#### CAUTION

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



#### DANGER

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

## **Command Syntax Conventions**

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

Convention	Description	
bold text	Identifies command names, keywords, and command options.	
italic text	Identifies a variable.	
[]	Syntax components displayed within square brackets are optional.	
	Default responses to system prompts are enclosed in square brackets.	
{x   y   z}	A choice of required parameters is enclosed in curly brackets separated by vertical bars. You must select one of the options.	
x y	A vertical bar separates mutually exclusive elements.	
< >	Nonprinting characters, for example, passwords, are enclosed in angle brackets.	
	Repeat the previous element, for example, member[member].	
١	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.	

•	Overview	. 13
	Network Overview	
•	Feature Parity with ZoneDirector	15
	Limitations and Deviations from ZoneDirector.	
	RUCKUS Unleashed-Only Features.	
	Unleashed Access Point Physical Features	

## **Overview**

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

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

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

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

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

## **Network Overview**

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

#### NOTE

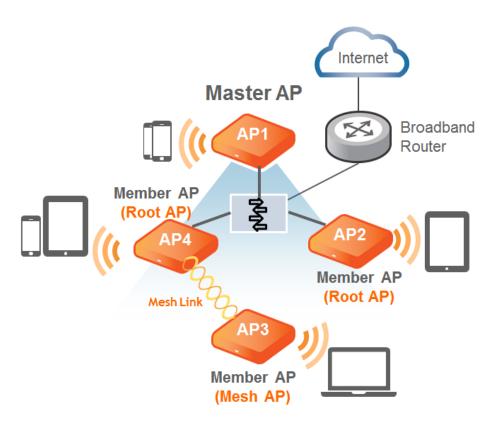
Beginning with release 200.8, the maximum capacity limit has been increased from 50 APs and 1,024 clients to 128 APs and 2,048 clients per RUCKUS Unleashed network in bridge mode (gateway mode supports up to 25 APs and 512 clients).

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

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

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

#### FIGURE 1 Basic Unleashed Network Topology



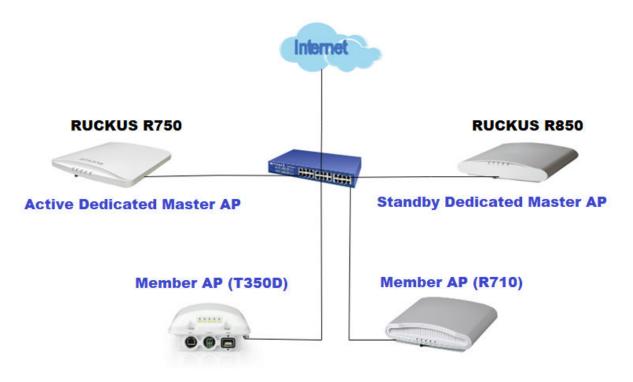
### **Unleashed Dedicated Master Network Overview**

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

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

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

#### FIGURE 2 Basic Unleashed Dedicated Master Network Topology



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

## **Feature Parity with ZoneDirector**

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

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

Feature Parity with ZoneDirector

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

## **Limitations and Deviations from ZoneDirector**

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

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

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

## **RUCKUS Unleashed-Only Features**

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

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

#### NOTE

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

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

## **Unleashed Access Point Physical Features**

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

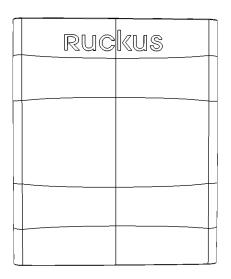
### **C110**

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

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

Introducing RUCKUS Unleashed Unleashed Access Point Physical Features

#### FIGURE 3 C110 Access Point



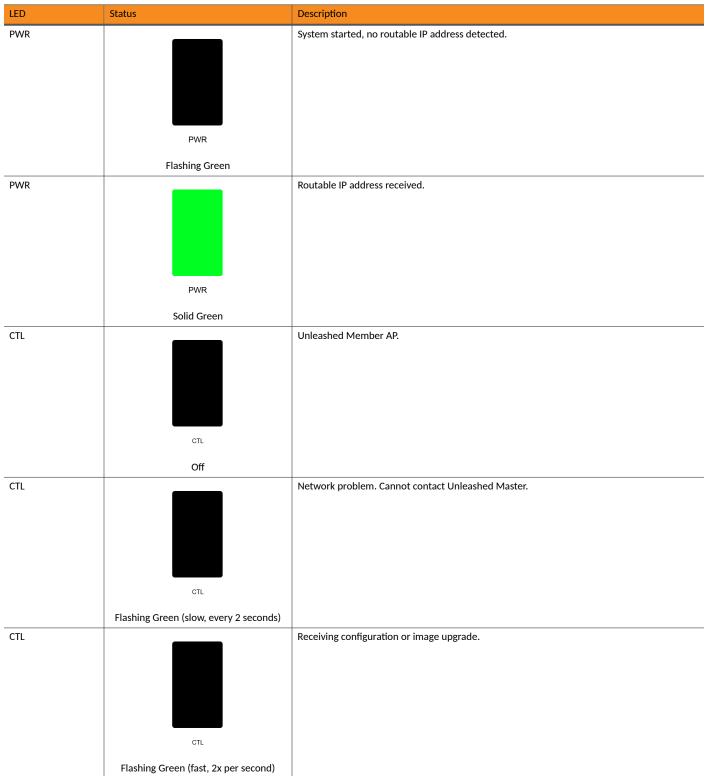
### **Rear Panel**

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

#### TABLE 2 Front Panel LEDs

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

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



Unleashed Access Point Physical Features

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

LED	Status	Description
CTL	ст. 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	24G Off	Radio is down.

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



**Unleashed Access Point Physical Features** 

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

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

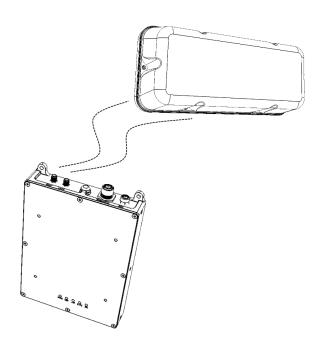
### **E510**

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

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

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

#### FIGURE 4 E510 Access Point



#### **Front Panel**

The E510 AP features five LEDs on its front panel.

#### TABLE 3 Front Panel LEDs

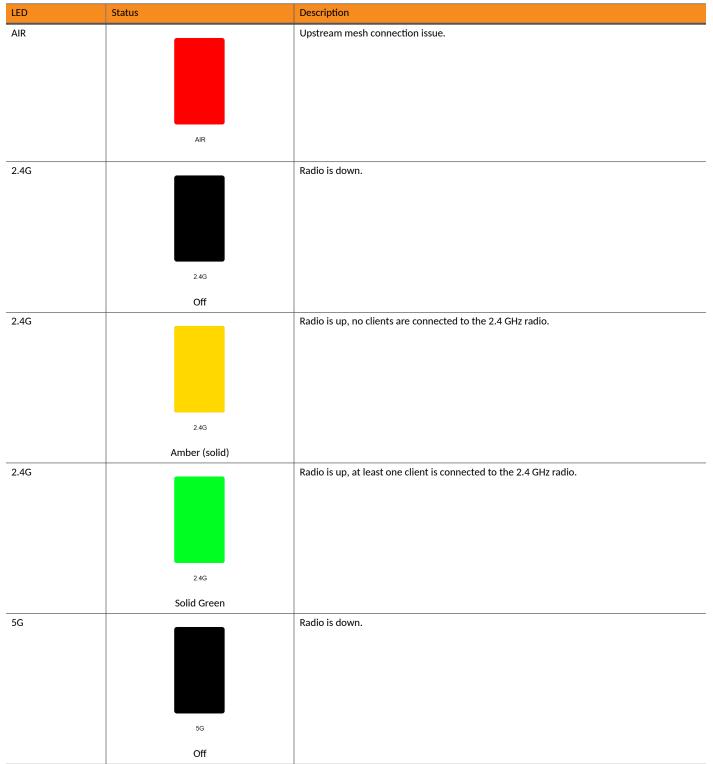
LED	Status	Description
PWR		No power connected.
	PWR	
	Off	
PWR		Boot up in process.
	PWR	
	Solid Red	
PWR		System started, no routable IP address detected.
	PWR	
	Flashing Green	
PWR		Routable IP address received.
	PWR	
CTL	Solid Green	Unleashed Member AP.
	CTL	
	Off	
	UII	

**Unleashed Access Point Physical Features** 

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

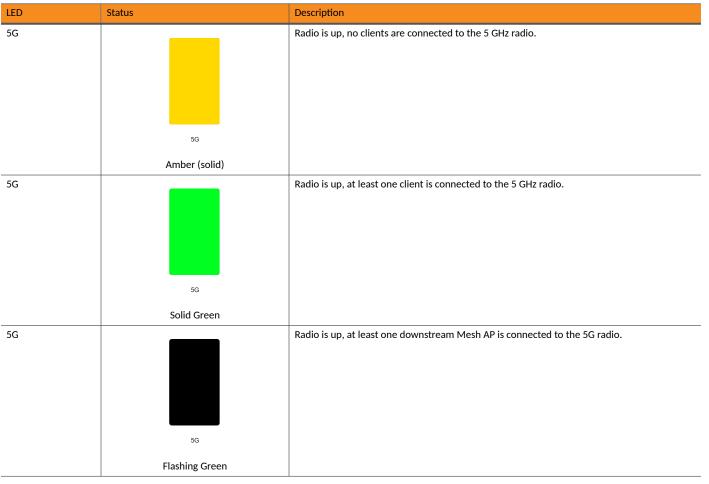
LED	Status	Description
CTL	CTL	Network problem. Cannot contact Unleashed Master.
	Flashing Green (slow, every 2 seconds)	
CTL	CTL	Receiving configuration or image upgrade.
	Flashing Green (fast, 2x per second)	
СТL	СТЬ	Unleashed Master AP.
	Solid Green	
AIR		No upstream mesh connection (Root AP).
	AIR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

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



**Unleashed Access Point Physical Features** 

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

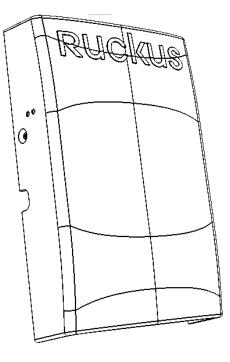


### H320

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

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

#### FIGURE 5 H320 Access Point



#### **Rear Panel**

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

#### **TABLE 4 Front Panel LEDs**

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

**Unleashed Access Point Physical Features** 

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

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

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



**Unleashed Access Point Physical Features** 

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



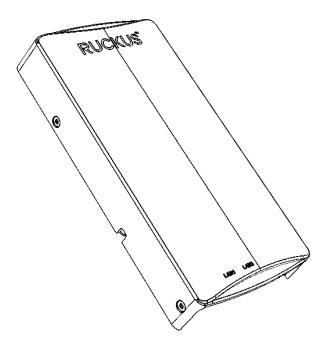
#### TABLE 4 Front Panel LEDs (continued)

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

### H350

The H350 is a Wi-Fi 6 (802.11ax) Wi-Fi access point with integrated switch in a wall-plate form factor. This section describes the physical features of the RUCKUS Unleashed H350 802.11ax Access Point.

#### FIGURE 6 H350 Access Point



#### **Rear Panel**

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

Unleashed Access Point Physical Features

#### TABLE 5 Front Panel LEDs

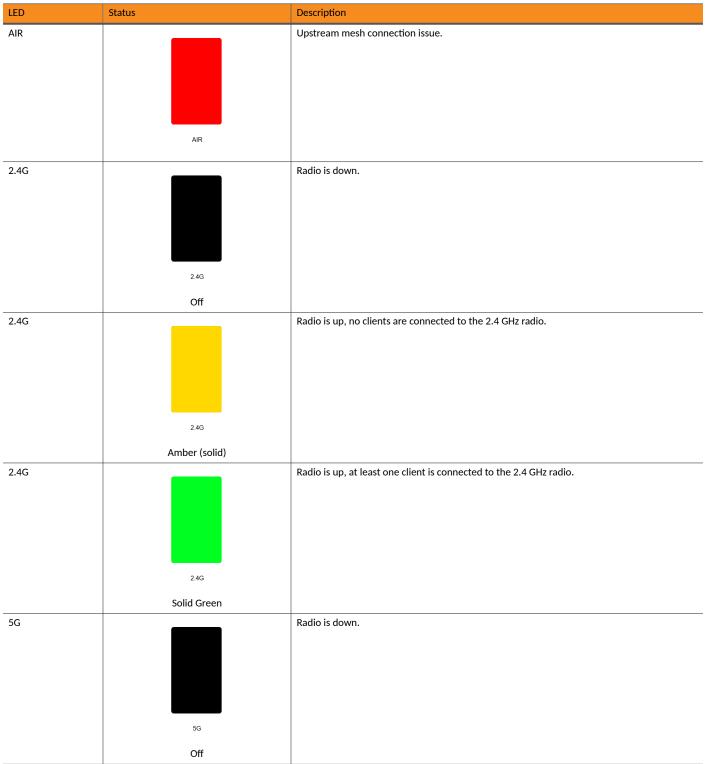
LED	Status	Description
PWR		No power connected.
	PWR	
	Off	
PWR		Boot up in process.
	PWR	
	Solid Red	
PWR		System started, no routable IP address detected.
	PWR	
	Flashing Green	
PWR		Routable IP address received.
	PWR	
	Solid Green	Unite sche d Manuferr AD
CTL		Unleashed Member AP.
	CTL	
	Off	

#### TABLE 5 Front Panel LEDs (continued)

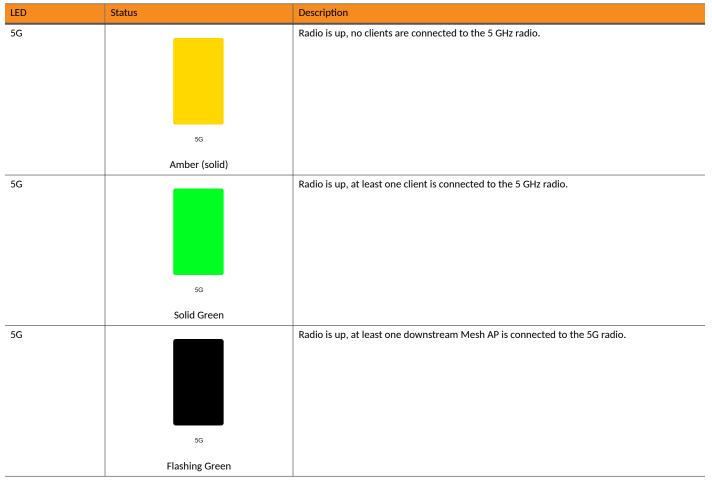
LED	Status	Description
CTL	CTL	Network problem. Cannot contact Unleashed Master.
	Flashing Green (slow, every 2 seconds)	
CTL		Receiving configuration or image upgrade.
	CTL	
	Flashing Green (fast, 2x per second)	
CTL	СТL	Unleashed Master AP.
	Solid Green	
AIR		No upstream mesh connection (Root AP).
	AIR	
	N/A	
AIR		Upstream mesh connection established (Mesh AP).
	AIR	
		1

**Unleashed Access Point Physical Features** 

#### TABLE 5 Front Panel LEDs (continued)



#### TABLE 5 Front Panel LEDs (continued)



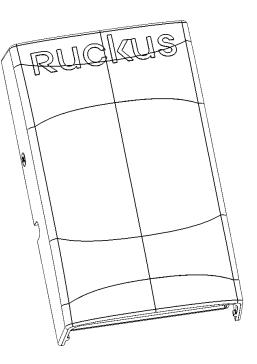
### H510

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.

Introducing RUCKUS Unleashed Unleashed Access Point Physical Features

#### FIGURE 7 H510 Access Point



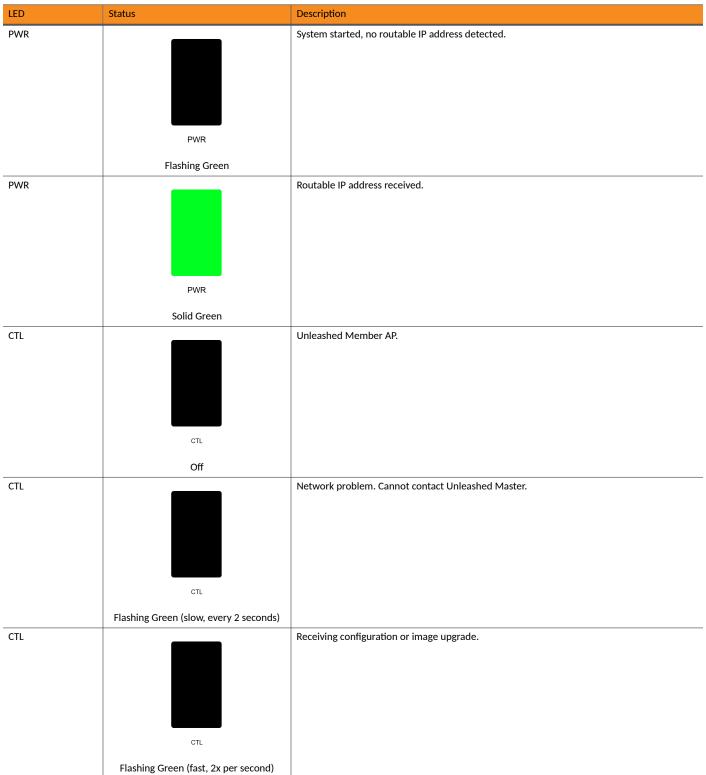
#### **Rear Panel**

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

#### TABLE 6 Front Panel LEDs

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

#### TABLE 6 Front Panel LEDs (continued)



Unleashed Access Point Physical Features

# 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)



**Unleashed Access Point Physical Features** 

### TABLE 6 Front Panel LEDs (continued)

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

# H550

The H550 is an 802.11ax Wave 2 dual-band concurrent Wi-Fi Wall Switch and IoT gateway 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 H550 802.11ax Access Point.

#### FIGURE 8 H550 Access Point



# **Rear Panel**

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

## TABLE 7 Front Panel LEDs

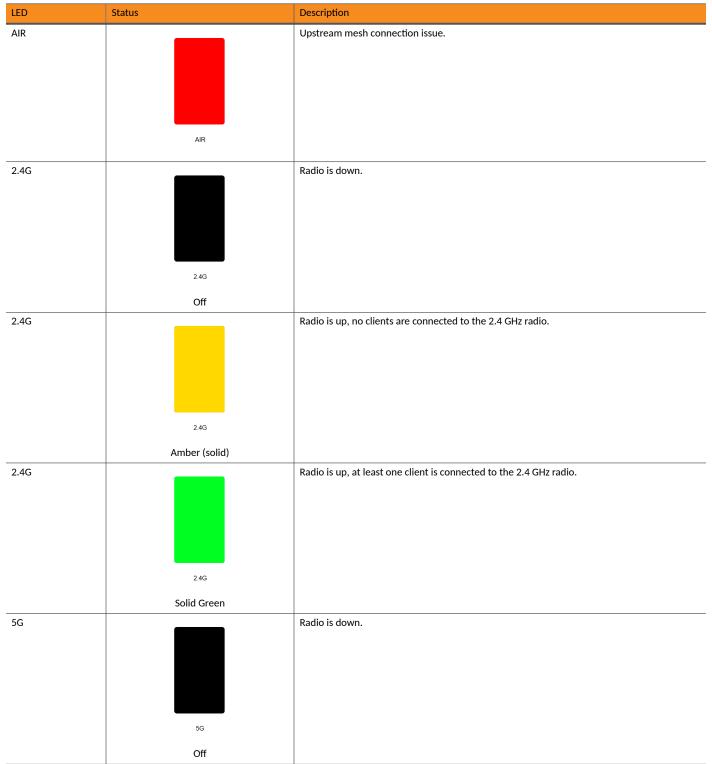
LED	Status	Description
PWR		No power connected.
	PWR	
	Off	
PWR		Boot up in process.
	PWR	
PWR	Solid Red	System started, no routable IP address detected.
	PWR	
	Flashing Green	
PWR		Routable IP address received.
	PWR	
	Solid Green	Unleashed Member AP.
CTL		Unleashed Member AP.
	CTL	
	Off	

**Unleashed Access Point Physical Features** 

# TABLE 7 Front Panel LEDs (continued)

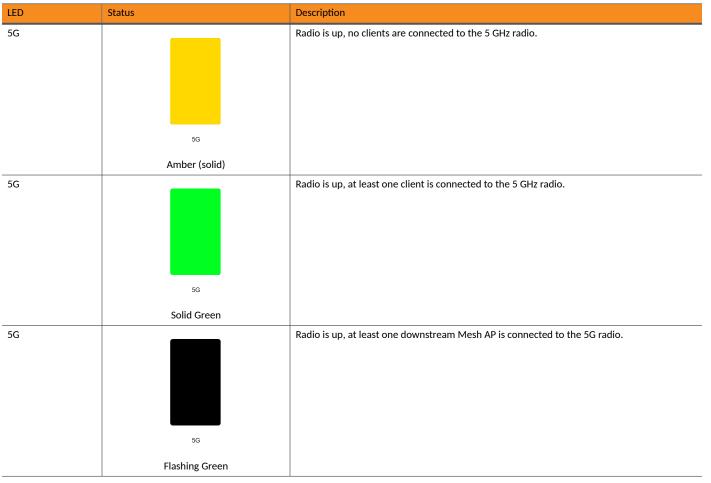
LED	Status	Description
CTL	СТL	Network problem. Cannot contact Unleashed Master.
	Flashing Green (slow, every 2 seconds)	
CTL	СТL	Receiving configuration or image upgrade.
	Flashing Green (fast, 2x per second)	
CTL		Unleashed Master AP.
	CTL	
	Solid Green	
AIR		No upstream mesh connection (Root AP).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

#### TABLE 7 Front Panel LEDs (continued)



**Unleashed Access Point Physical Features** 

#### TABLE 7 Front Panel LEDs (continued)



# M510

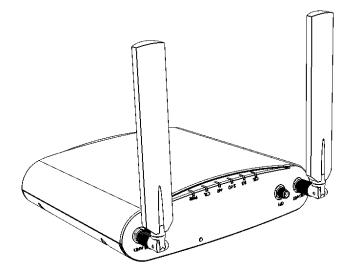
The Unleashed M510 is an 802.11ac Wave 2 Access Point with embedded LTE module for cellular backhaul. The M510 is designed for deployment in scenarios where there is no readily accessible wired connectivity for backhaul, such as in buses, taxis, or other in-vehicle deployments, or in remote locations 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 50.

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

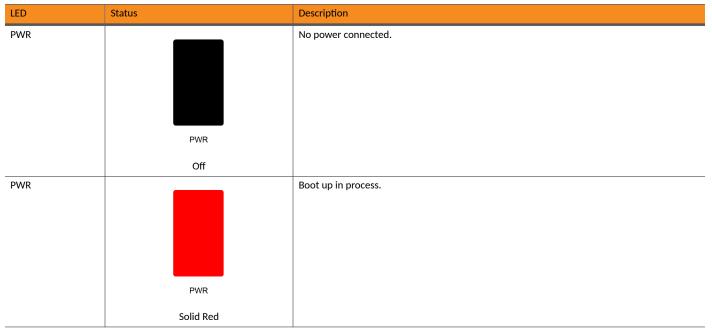
#### FIGURE 9 M510 Access Point



## **Front Panel**

The M510 AP features six LEDs on its front panel.

#### **TABLE 8 Front Panel LEDs**



**Unleashed Access Point Physical Features** 

# TABLE 8 Front Panel LEDs (continued)

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

#### TABLE 8 Front Panel LEDs (continued)



**Unleashed Access Point Physical Features** 

#### TABLE 8 Front Panel LEDs (continued)



#### TABLE 8 Front Panel LEDs (continued)

LED	Status	Description
5G	56	Radio is up, at least one downstream Mesh AP is connected to the 5G radio.
	Flashing Green	
CEL		<ul> <li>Off: No cellular connection.</li> <li>Amber: 3G connection.</li> <li>Green: 4G/LTE connection.</li> </ul>
	5G	
	Solid Green	

#### NOTE

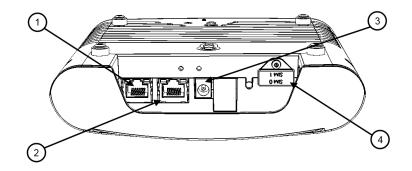
CEL LED will remain in "Off" status until the Unleashed M510 is provisioned.

# **Bottom Panel**

The bottom panel of the M510 includes the following:

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

## FIGURE 10 M510 bottom panel



**Unleashed Access Point Physical Features** 

#### TABLE 9 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 10 Behavior of Ethernet port LEDs on the M510

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

# **Deployment Considerations**

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

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

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

## Limitations

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

# M510 Configuration

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

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

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

In WAN Connection, select one of the following options:

- Ethernet (primary) with Cellular failover
- Cellular only

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

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

#### FIGURE 11 Ethernet (Primary) with Cellular failover

Qualant						
System	IP setting	Wireles	ss LAN Ad	Iministrator	Re	eview
Gateway Mode						
WAN Selection		▼				
* WAN connection	Ethernet (Primary) with cellula	ar 🗸				
* WAN Recovery	60 seconds (10-300)				POE IN	/
Timer			SIM	10	WAN	S. S. C.R.
				i futt t.	LIN WIDIPLE	
				Contraction of the local division of the loc		
			SIN		AN	
			SIM	·· ·	AN	
					AN the WAN port and	SIM slo
Cellular Radio Settings		▼		This image shows		SIM slo
Cellular Radio Settings APN for SIM 0	defaultapn	•		This image shows	the WAN port and	SIM slo
-	defaultapn defaultapn	<b>V</b>	LAN & WLAN IP AG	This image shows ddress er IP 192.168.1	the WAN port and	SIM slo
APN for SIM 0	defaultapn	▼ 	LAN & WLAN IP Ad	This image shows ddress or IP 192.168.1 hask 255.255.2	the WAN port and 0.1 55.0	SIM slo
APN for SIM 0 APN for SIM 1	defaultapn	▼ 	LAN & WLAN IP Ac * Route * Netm	This image shows ddress er IP 192.168.1 hask 255.255.2 ht IP Addresses	the WAN port and 0.1 55.0	SIM slo
APN for SIM 0 APN for SIM 1 WAN IP Address for Eth	defaultapn	▼ 	LAN & WLAN IP AG * Route * Netm LAN & WLAN Clier	This image shows ddress er IP 192.168.1 hask 255.255.2 ht IP Addresses g IP 192.168.1	the WAN port and 0.1 55.0 5 0.2	SIM slo
APN for SIM 0 APN for SIM 1 WAN IP Address for Eth O Manual	defaultapn ernet		LAN & WLAN IP AC * Route * Netm LAN & WLAN Clien * Startin	This image shows         ddress         er IP       192.168.1         aask       255.255.2         at IP Addresses         g IP       192.168.1         g IP       192.168.1	the WAN port and 0.1 55.0 5 0.2	SIM slo
APN for SIM 0 APN for SIM 1 WAN IP Address for Eth Manual * IP Address	defaultapn ernet 172.18.165.7		LAN & WLAN IP AC * Route * Netm LAN & WLAN Clien * Startin * Endin	This image shows ddress er IP 192.168.1 hask 255.255.2 ht IP Addresses g IP 192.168.1 g IP 192.168.1 192.168.1 192.168.1	the WAN port and 0.1 55.0 6 0.2 0.102	
APN for SIM 0 APN for SIM 1 WAN IP Address for Eth Manual * IP Address * Netmask	defaultapn ernet 172.18.165.7 255.255.255.0		LAN & WLAN IP AC * Route * Netm LAN & WLAN Clien * Startin * Endin Number of	This image shows         ddress         er IP       192.168.1         nask       255.255.2         nt IP Addresses         g IP       192.168.1         g IP       192.168.1         f IPs       101	the WAN port and 0.1 55.0 6 0.2 0.102	

Back

Unleashed Access Point Physical Features

#### FIGURE 12 Cellular only

1 System	2 IP setting	3 Wireless LAN	4 Administrator	5 Review
Gateway Mode				
WAN Selection		•		
* WAN connect	Cellular only	~		
Cellular Radio Setti	ngs	•		POE IN WAN
APN for SI	M 0 internet		SIM 0	
APN for SI	M 1 internet		SIM 1	
			* This image shows the V	/AN port and SIM slots
LAN & WLAN Client	t IP Addresses	V LAN &	WLAN IP Address	•
* Starting	<b>10.10.0.10</b>		* Router IP 10.10.0.1	
* Ending	<b>JIP</b> 10.10.0.30		* Netmask 255.255.0.0	
Number of				
Lease Ti	Twelve hours	~		
			Back	Next

#### 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

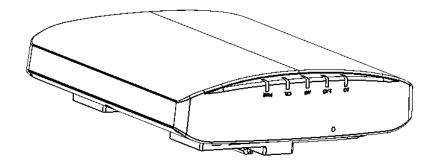
PPPoE IP address mode is not supported on Unleashed M510.

# **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 13 R320 Access Point



# **Front Panel**

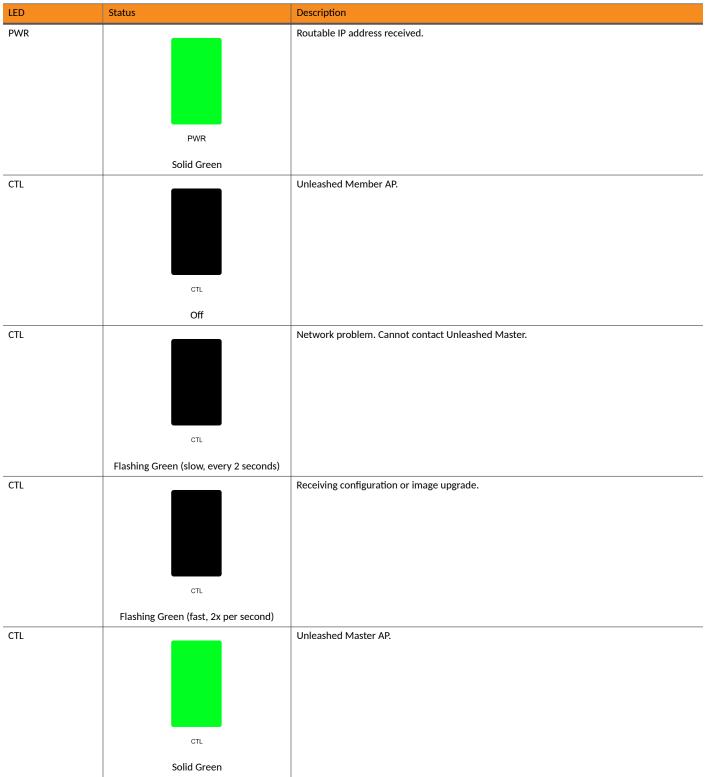
The R320 AP features five LEDs on its front panel.

#### TABLE 11 Front Panel LEDs

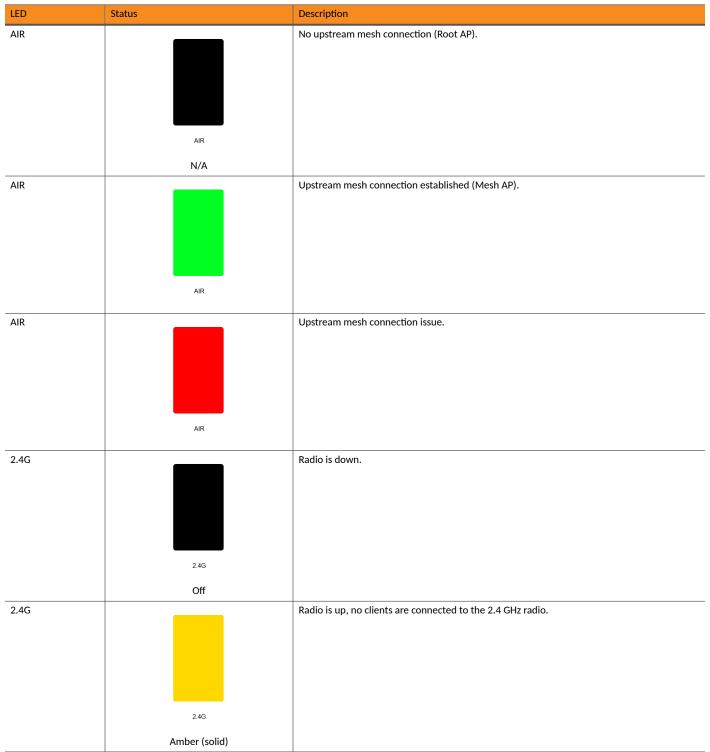
LED	Status	Description
PWR	PWR	No power connected.
	Off	
PWR	PWR Solid Red	Boot up in process.
PWR	PWR Flashing Green	System started, no routable IP address detected.

**Unleashed Access Point Physical Features** 

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

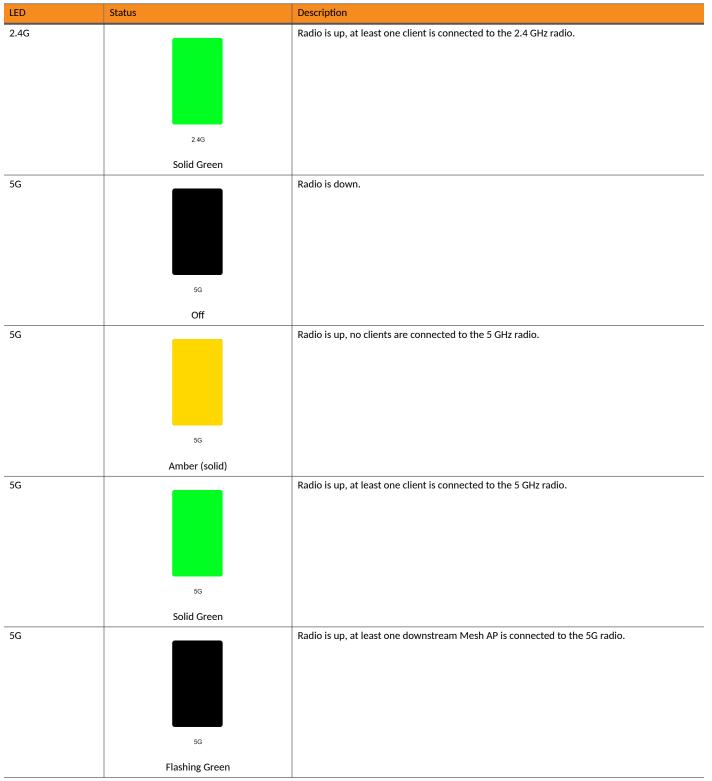


#### TABLE 11 Front Panel LEDs (continued)



**Unleashed Access Point Physical Features** 

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

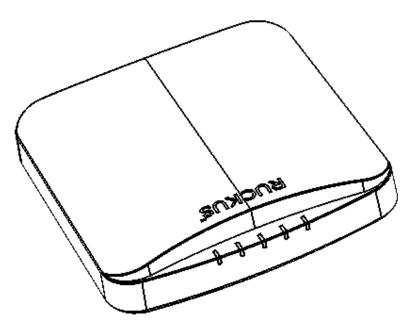


# **R350**

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

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

FIGURE 14 R350 Access Point



# **Front Panel**

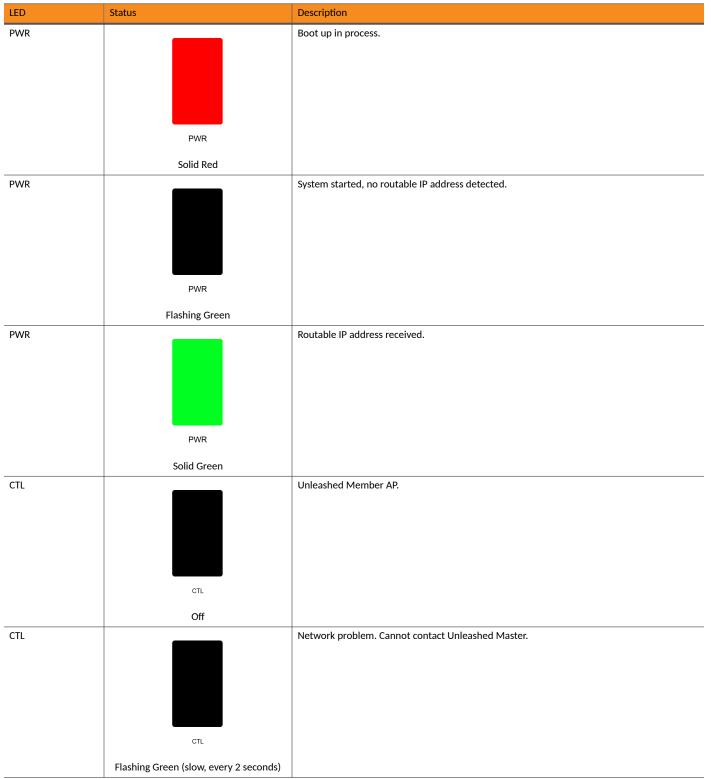
The R350 AP features five LEDs on its front panel.

### TABLE 12 Front Panel LEDs

LED	Status	Description
PWR		No power connected.
	PWR	
	Off	

**Unleashed Access Point Physical Features** 

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

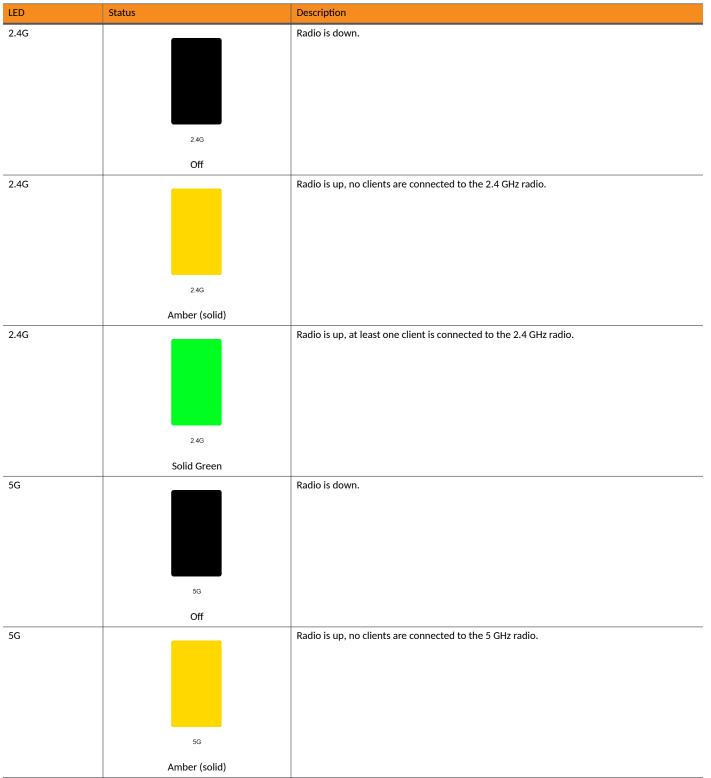


# TABLE 12 Front Panel LEDs (continued)

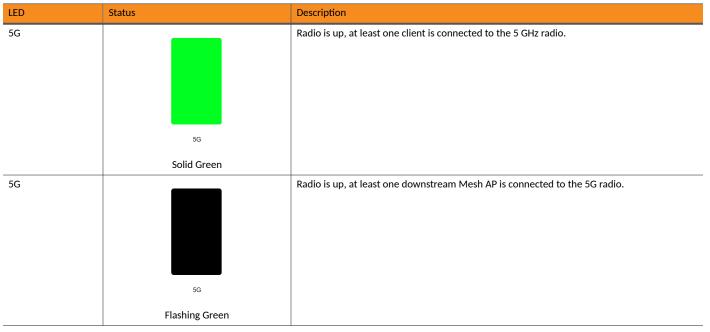
LED	Status	Description
CTL	сть Flashing Green (fast, 2x per second)	Receiving configuration or image upgrade.
CTL		Unleashed Master AP.
	CTL Solid Green	
AIR	AIR	No upstream mesh connection (Root AP).
AIR	N/A	Unstream mach connection actablished (Mach AD)
AIK	AIR	Upstream mesh connection established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

**Unleashed Access Point Physical Features** 

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



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

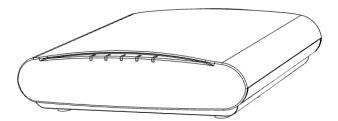


# **R510**

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

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

FIGURE 15 R510 Access Point

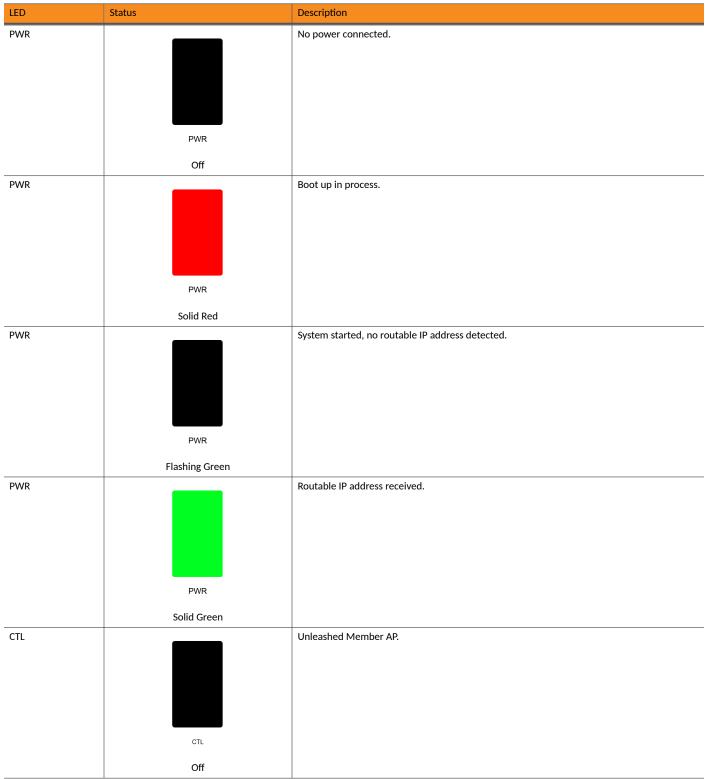


# **Front Panel**

The R510 AP features five LEDs on its front panel.

Unleashed Access Point Physical Features

### TABLE 13 Front Panel LEDs



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

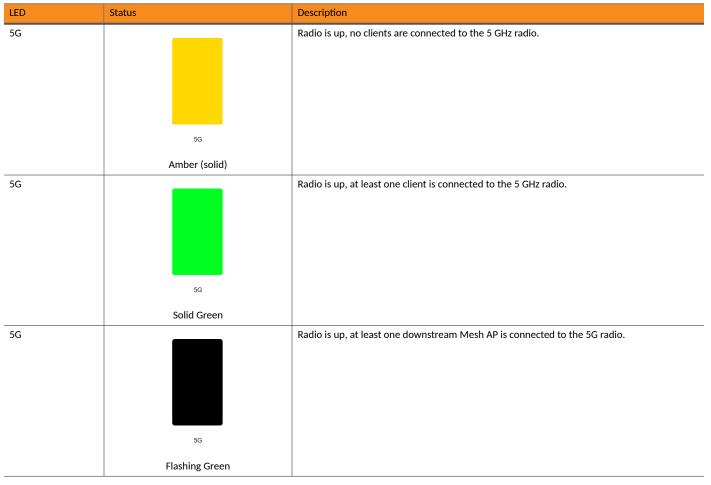
LED	Status	Description
CTL	сть	Network problem. Cannot contact Unleashed Master.
	Flashing Green (slow, every 2 seconds)	
CTL		Receiving configuration or image upgrade.
	CTL	
	Flashing Green (fast, 2x per second)	
CTL	CTL	Unleashed Master AP.
	Solid Green	
AIR		No upstream mesh connection (Root AP).
	AIR	
	N/A	
AIR		Upstream mesh connection established (Mesh AP).
	AIR	
		1

**Unleashed Access Point Physical Features** 

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



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

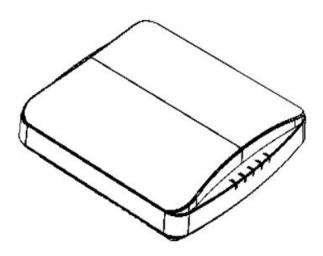


# **R550**

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

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

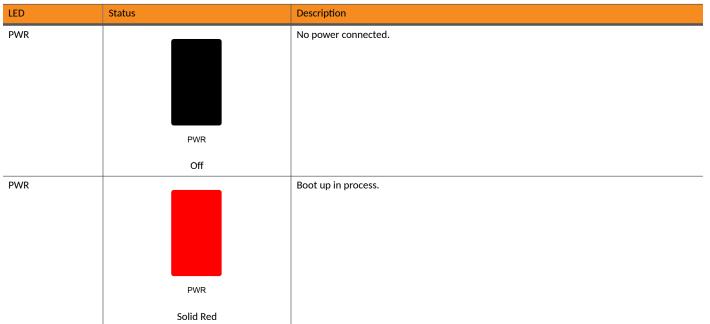
#### FIGURE 16 Unleashed R550 Access Point



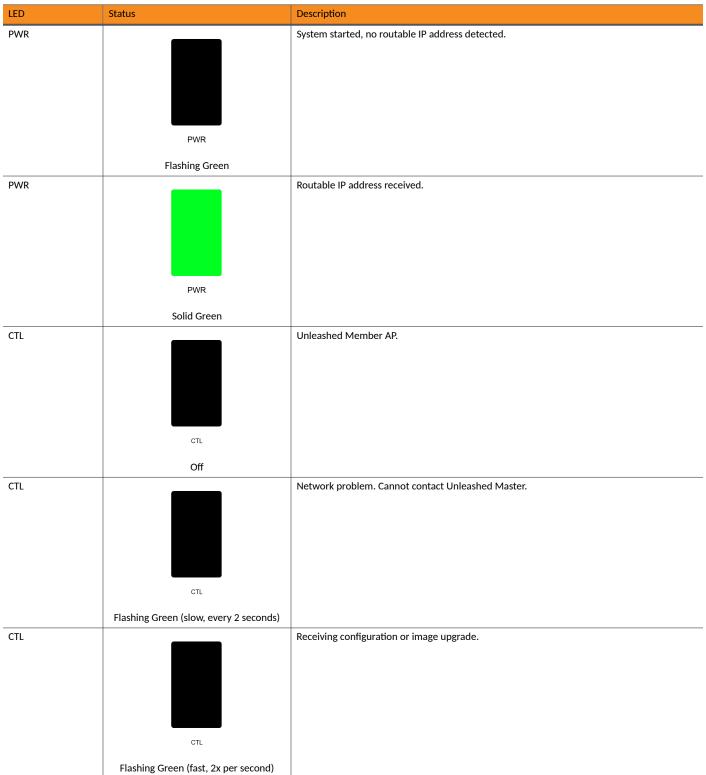
# **Front Panel**

The R550 AP features five LEDs on its front panel.

#### TABLE 14 Front Panel LEDs



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



**Unleashed Access Point Physical Features** 

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

LED	Status	Description
CTL	стL 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)



Unleashed Access Point Physical Features

### TABLE 14 Front Panel LEDs (continued)

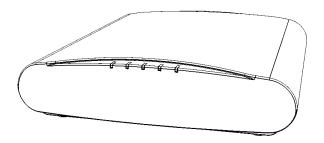
LED	Status	Description
5G		Radio is up, at least one downstream Mesh AP is connected to the 5G radio.
	5G	
	Flashing Green	

# **R610**

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

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

#### FIGURE 17 R610 Access Point



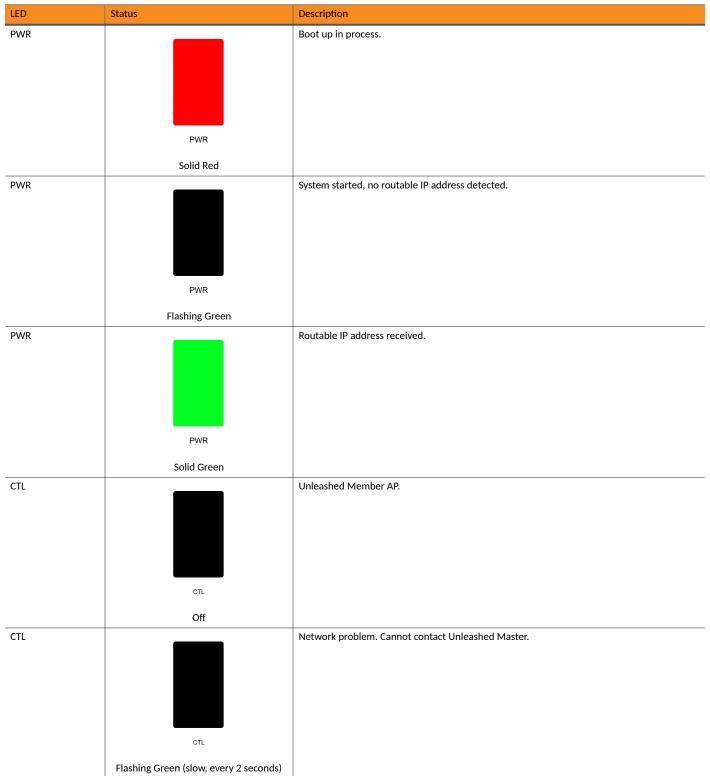
# **Front Panel**

The R610 AP features five LEDs on its front panel.

#### TABLE 15 Front Panel LEDs

LED	Status	Description
PWR		No power connected.
	PWR	
	Off	

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



Unleashed Access Point Physical Features

# TABLE 15 Front Panel LEDs (continued)

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

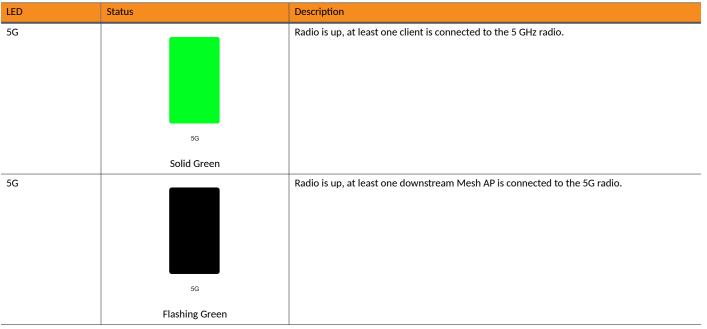
#### Introducing RUCKUS Unleashed Unleashed Access Point Physical Features

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



**Unleashed Access Point Physical Features** 

## TABLE 15 Front Panel LEDs (continued)

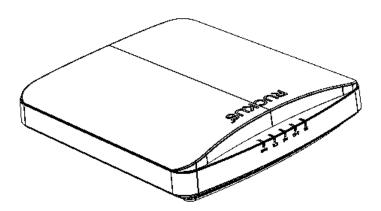


# **R650**

The Ruckus R650 is a mid-range "Wi-Fi 6" (802.11ax) dual-band indoor 4x4: 4 AP with BeamFlex+, one 2.5 Gbps PoE+ port, one 1 Gbps Ethernet port, and onboard support for IoT and BLE/Zigbee.

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

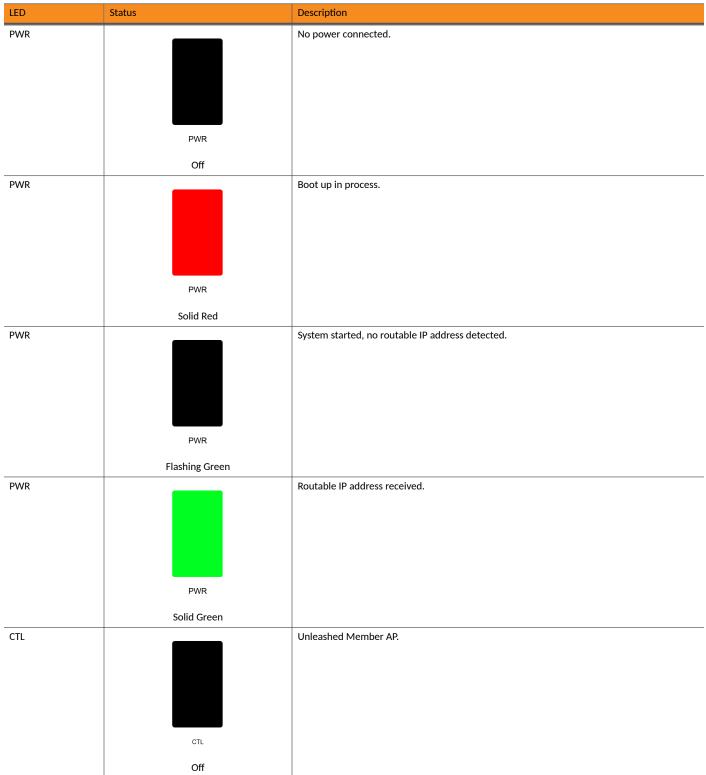
FIGURE 18 Unleashed R650 Access Point



## **Front Panel**

The R650 AP features five LEDs on its front panel.

#### TABLE 16 Front Panel LEDs

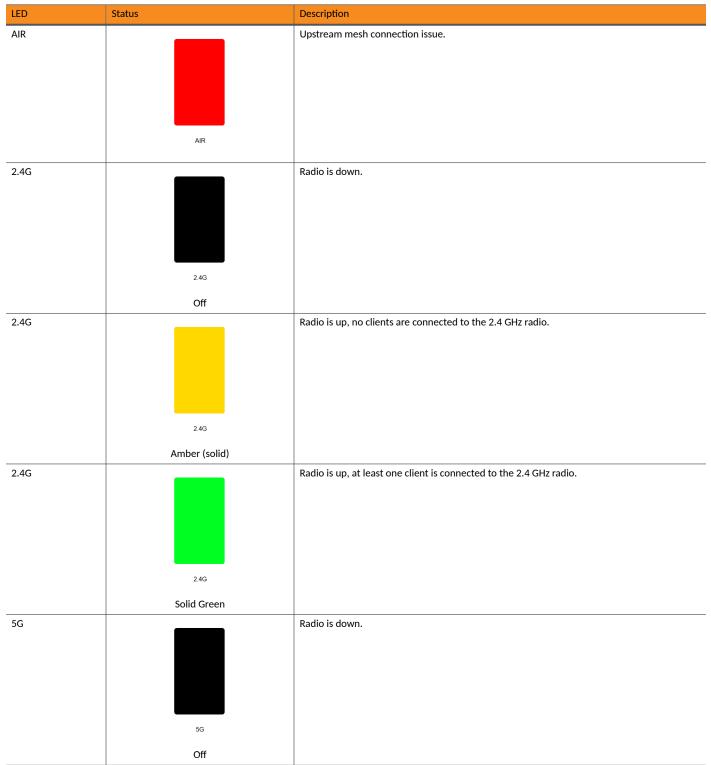


**Unleashed Access Point Physical Features** 

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

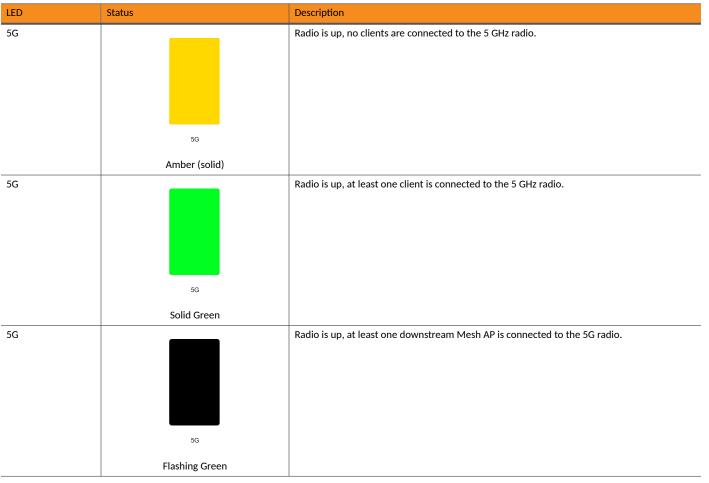
CTL     Flashing Green (slow, every 2 seconds)       CTL     Flashing Green (slow, every 2 seconds)       CTL     Flashing Green (slow, every 2 seconds)       ort.     rt.       ort.     Flashing Green (slow, every 2 seconds)       CTL     Image: state stat		Description	Status	LED
CTL     Image: CTL or true of the true of tr	Unleashed Master.	Network problem. Cannot cont		CTL
Image: CTL     Flashing Green (fast, 2x per second)       CTL     Image: CTL       Image: CTL     Image: CTL			Flashing Green (slow, every 2 seconds)	
CTL       Image: CTL       Unleashed Master AP.         ort       ort         Solid Green       Image: CTL         AIR       Image: CTL	pgrade.	Receiving configuration or imag	СТL	CTL
CTL       Image: CTL       Unleashed Master AP.         ort       ort         Solid Green       Image: CTL         AIR       Image: CTL         Image: CTL       Image: CTL			Flashing Green (fast, 2x per second)	
Solid Green       AIR       AIR       AIR       AIR       N/A		Unleashed Master AP.	сть	CTL
AIR No upstream mesh connection (Root AP).				
N/A	ot AP).	No upstream mesh connection		AIR
	shed (Mesh AP).	Upstream mesh connection est		AIR
AIR			AIR	

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



Unleashed Access Point Physical Features

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

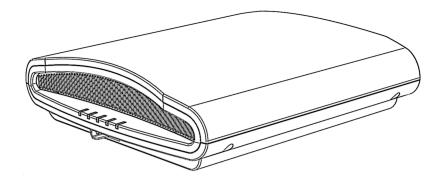


# **R710**

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

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

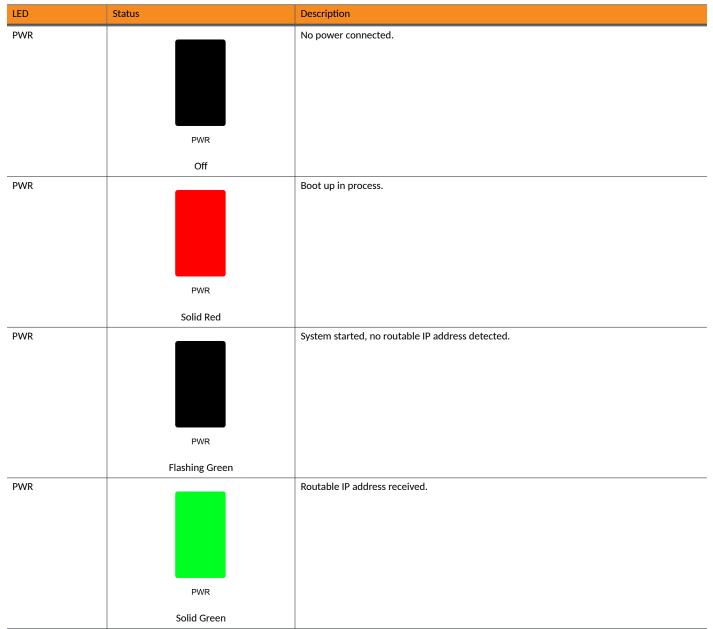
#### FIGURE 19 R710 Access Point



## **Front Panel**

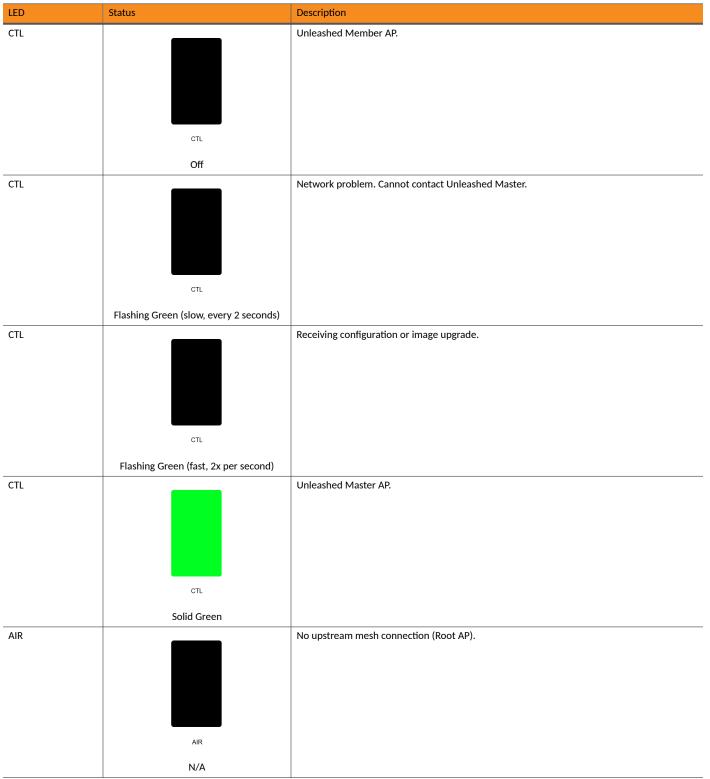
The R710 AP features five LEDs on its front panel.

#### TABLE 17 Front Panel LEDs

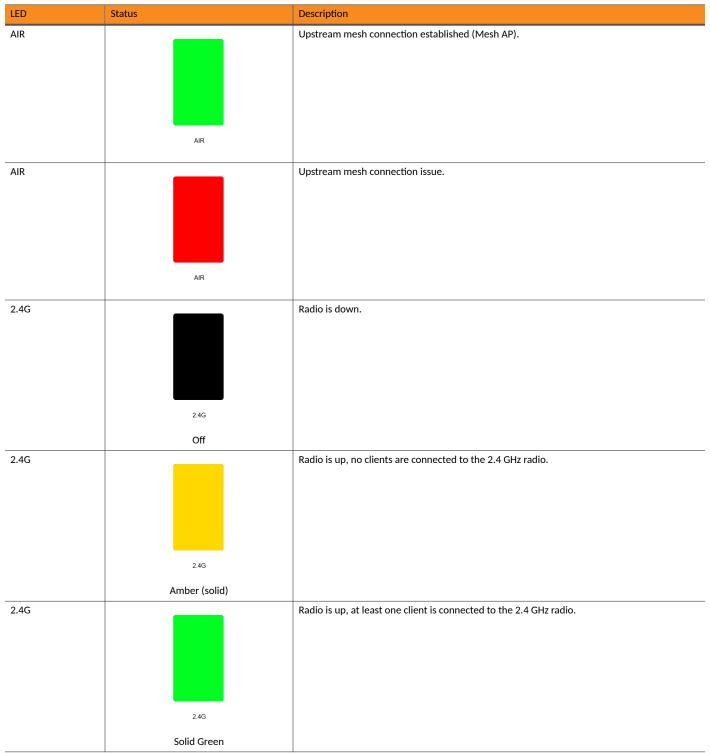


**Unleashed Access Point Physical Features** 

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

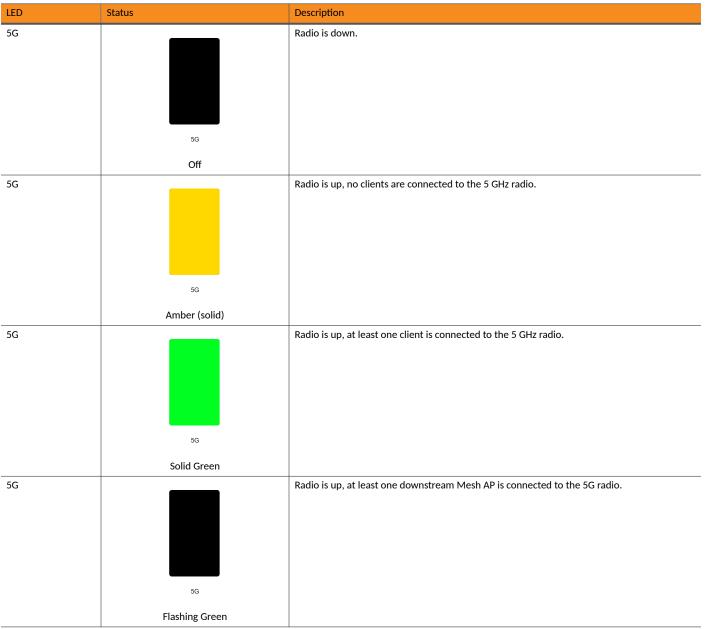


#### TABLE 17 Front Panel LEDs (continued)



**Unleashed Access Point Physical Features** 

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



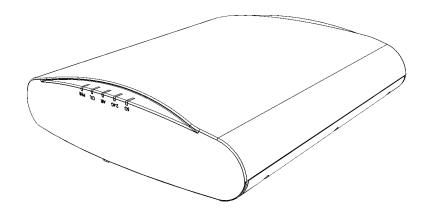
# **R720**

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

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

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

#### FIGURE 20 R720 Access Point



## **Front Panel**

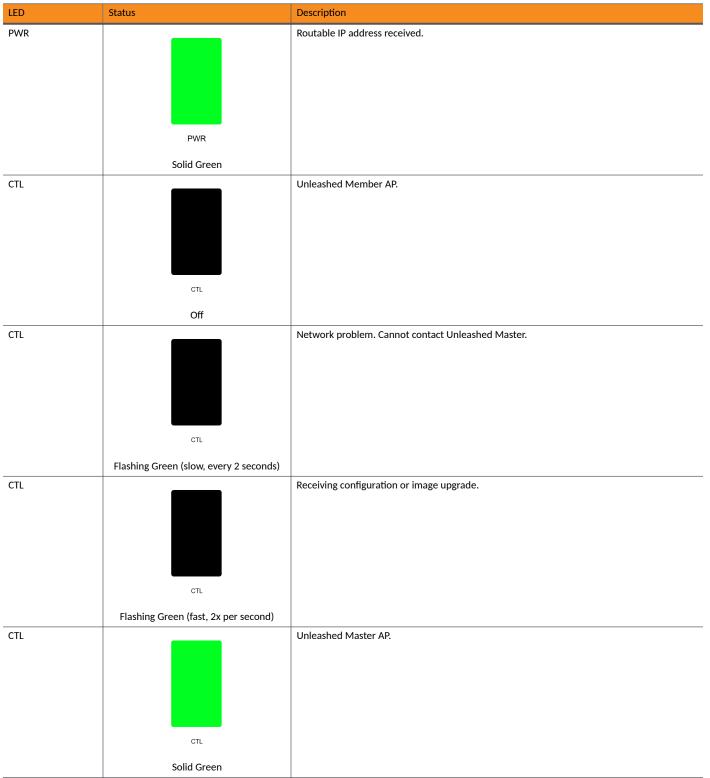
The R720 AP features five LEDs on its front panel.

#### TABLE 18 Front Panel LEDs

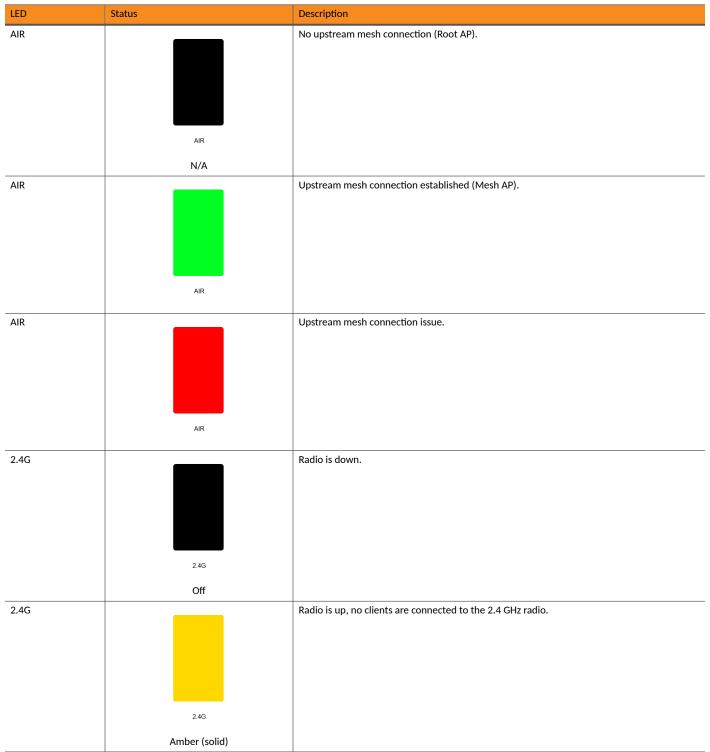
LED	Status	Description
PWR	PWR	No power connected.
	Off	
PWR	PWR Solid Red	Boot up in process.
PWR	PWR Flashing Green	System started, no routable IP address detected.

**Unleashed Access Point Physical Features** 

#### TABLE 18 Front Panel LEDs (continued)



#### TABLE 18 Front Panel LEDs (continued)



**Unleashed Access Point Physical Features** 

#### TABLE 18 Front Panel LEDs (continued)



# **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).

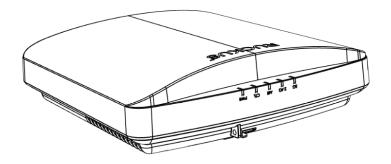
The Unleashed R750 provides advanced 11ax features such as OFDMA, MU-MIMO, 11ax power save, and WPA3. It includes a USB port and onboard IoT management chip for applications such as ZigBee, BLE (Bluetooth Low Energy) or LTE dongles, and a 2.5 GbE port that supports 802.3af, 802.3at and 802.3bt (40W) PoE, and one 1 GbE port (non-PoE).

#### NOTE

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

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

#### FIGURE 21 Unleashed R750 Access Point



## **Front Panel**

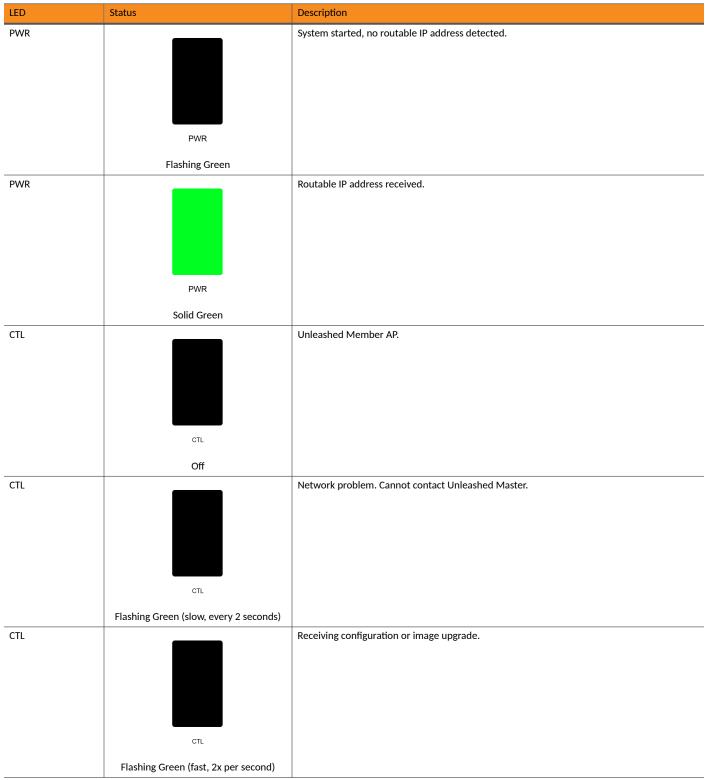
The R750 AP features five LEDs on its front panel.

#### TABLE 19 Front Panel LEDs

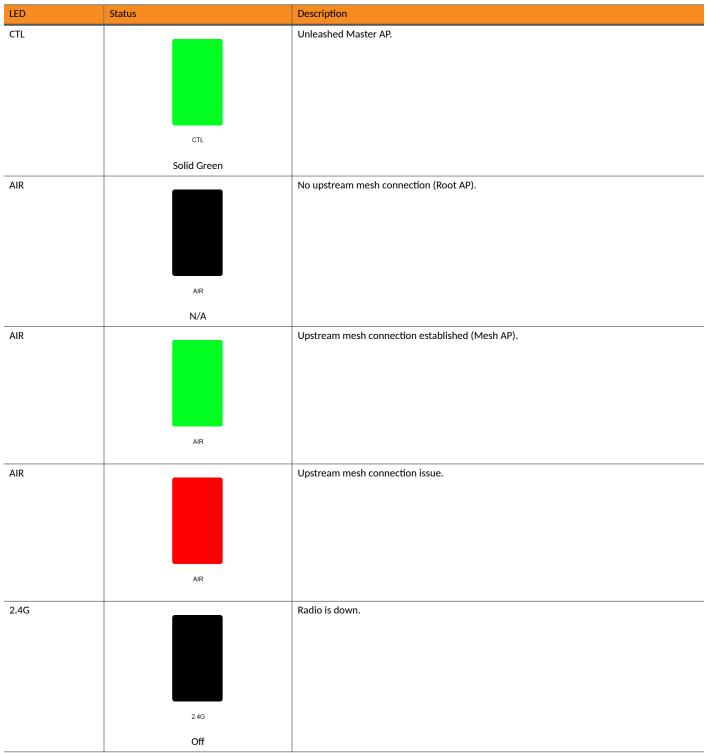
LED	Status	Description
PWR		No power connected.
	PWR	
	Off	
PWR		Boot up in process.
	PWR	
	Solid Red	

**Unleashed Access Point Physical Features** 

#### TABLE 19 Front Panel LEDs (continued)



#### TABLE 19 Front Panel LEDs (continued)



**Unleashed Access Point Physical Features** 

#### TABLE 19 Front Panel LEDs (continued)



#### TABLE 19 Front Panel LEDs (continued)

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

## **R850**

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

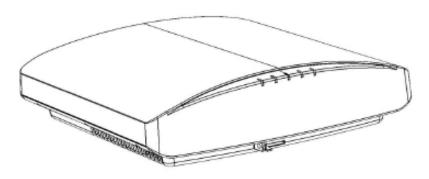
The R850 has one 5 Gbps PoE Ethernet port and one 1 Gbps port, onboard BLE and Zigbee radios for IOT applications, and a USB port for additional connectivity. The R850 will operate with PoH, uPOE and 802.3at power.

#### NOTE

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

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

#### FIGURE 22 Unleashed R850 Access Point

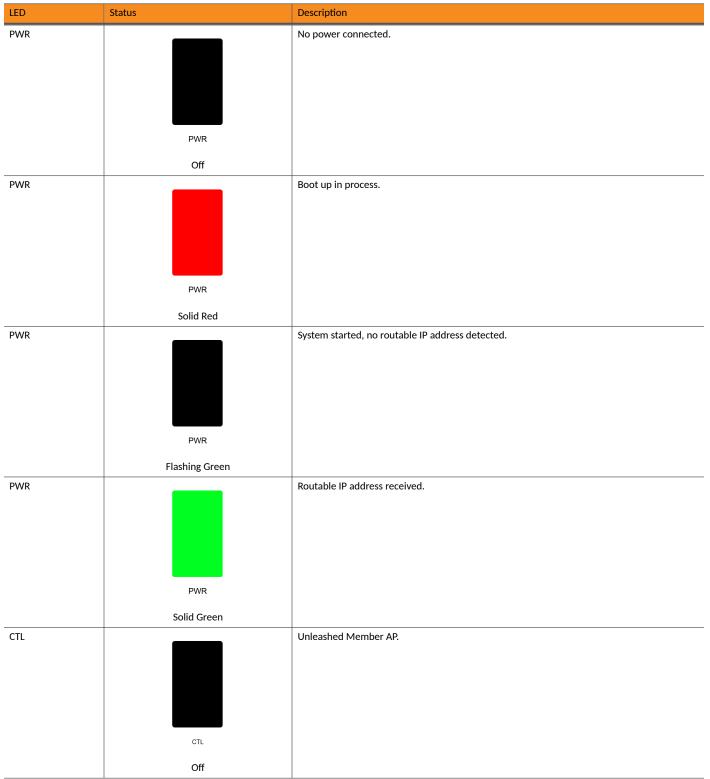


## **Front Panel**

The R850 AP features five LEDs on its front panel.

**Unleashed Access Point Physical Features** 

#### TABLE 20 Front Panel LEDs

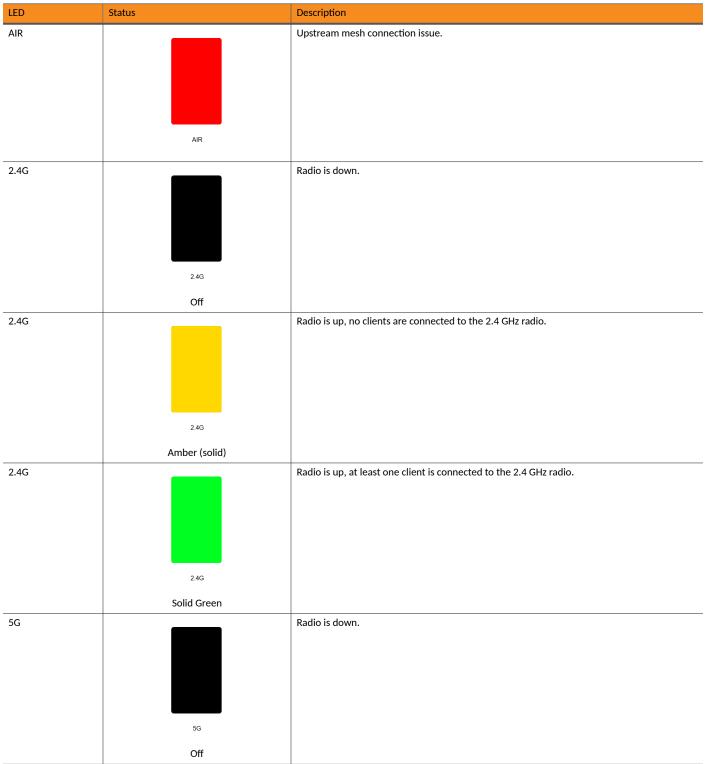


#### TABLE 20 Front Panel LEDs (continued)

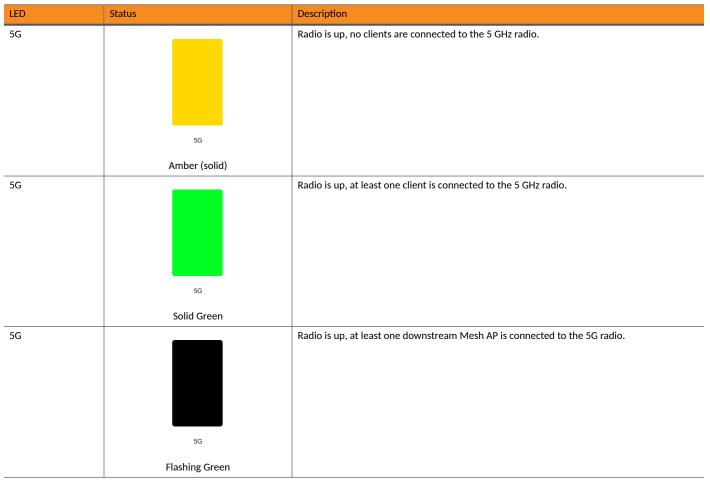
CTL     Flashing Green (slow, every 2 seconds)       CTL     Flashing Green (slow, every 2 seconds)       CTL     Image: Crt. Flashing Green (fast, 2x per second)       CTL     Flashing Green (fast, 2x per second)       CTL     Image: Crt. Flashing Green (fast, 2x per second)       CTL     Image: Crt. Flashing Green (fast, 2x per second)       CTL     Image: Crt. Flashing Green (fast, 2x per second)       CTL     Image: Crt. Flashing Green (fast, 2x per second)       CTL     Image: Crt. Flashing Green (fast, 2x per second)       CTL     Image: Crt. Flashing Green (fast, 2x per second)       CTL     Image: Crt. Flashing Green (fast, 2x per second)       CTL     Image: Crt. Flashing Green (fast, 2x per second)       CTL     Image: Crt. Flashing Green (fast, 2x per second)       CTL     Image: Crt. Flashing Green (fast, 2x per second)       CTL     Image: Crt. Flashing Green (fast, 2x per second)       CTL     Image: Crt. Flashing Green (fast, 2x per second)       CTL     Image: Crt. Flashing Green (fast, 2x per second)       CTL     Image: Crt. Flashing Green (fast, 2x per second)       CTL     Image: Crt. Flashing Green (fast, 2x per second)       CTL     Image: Crt. Flashing Green (fast, 2x per second)       Image: Crt. Flashing Green (fast, 2x per second)     Image: Crt. Flashing Green (fast, 2x per second)       Image: Crt. Flashing Green (fast, 2x per s	Description	Status	LED
CTL     Receiving configuration or image upgrade.       GTL     Flashing Green (fast, 2x per second)       CTL     Unleashed Master AP.       GTL     GTL       OTL     Solid Green       AIR     No upstream mesh connection (Root AP).	Network problem. Cannot contact Unleashed Master.	CTL	CTL
CTL     Flashing Green (fast, 2x per second)       CTL     Image: CTL       CTL     Image: CTL       Image: C		Flashing Green (slow, every 2 seconds)	
Flashing Green (fast, 2x per second)       Unleashed Master AP.         CTL       Image: CTL       Image: CTL         oru       oru       Image: CTL         Solid Green       Image: CTL       Image: CTL         AIR       Image: CTL       Image: CTL	 Receiving configuration or image upgrade.		CTL
CTL     Unleashed Master AP.       CTL     CTL       Solid Green     No upstream mesh connection (Root AP).       AIR     Image: Air Arrow		CTL	
AIR     Solid Green       AIR     Image: Air		Flashing Green (fast, 2x per second)	
Solid Green       AIR     No upstream mesh connection (Root AP).       AIR     AIR	Unleashed Master AP.		CTL
AIR No upstream mesh connection (Root AP).			
	 No upstream mesh connection (Root AP).		AIR
Ν/Δ		AIR	
		N/A	
AIR Upstream mesh connection established (Mesh AP).	Upstream mesh connection established (Mesh AP).		AIR
AIR		AIR	

**Unleashed Access Point Physical Features** 

#### TABLE 20 Front Panel LEDs (continued)



#### TABLE 20 Front Panel LEDs (continued)



# **T310 Family**

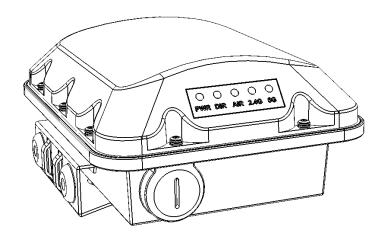
The Unleashed T310 family provides 802.11ac "Wave 2" features, including MU-MIMO, in an outdoor access point.

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

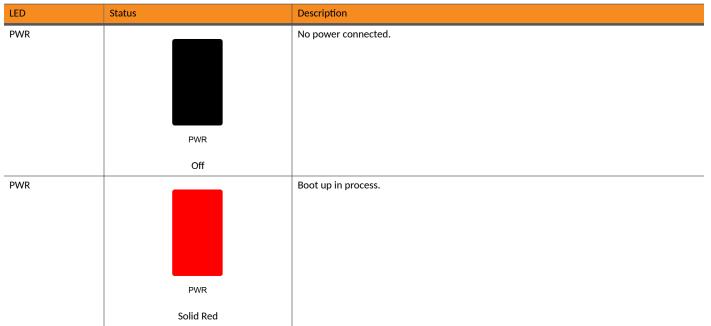
#### FIGURE 23 T310d Outdoor Access Point



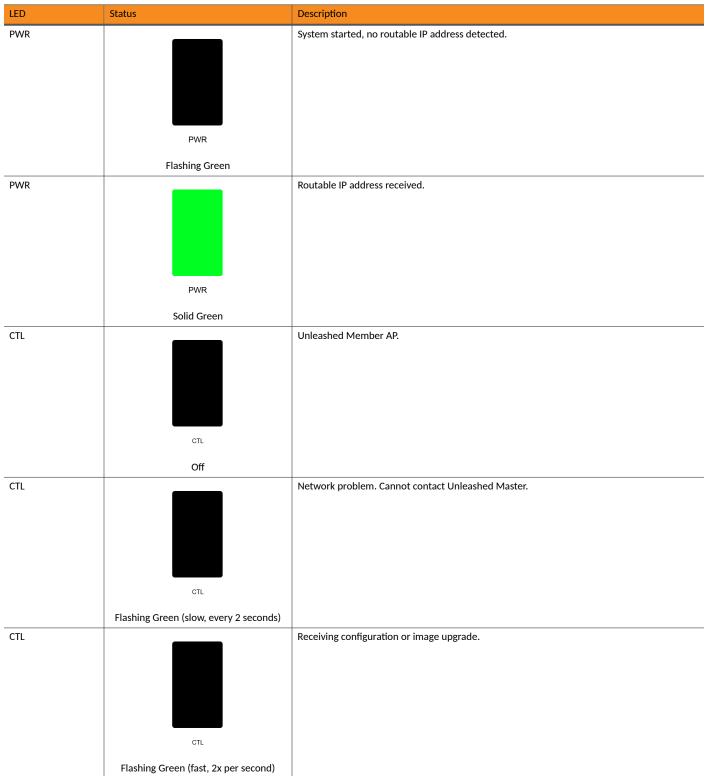
## **Front Panel**

The T310 features five LEDs on its front panel.

#### TABLE 21 Front Panel LEDs



#### TABLE 21 Front Panel LEDs (continued)



**Unleashed Access Point Physical Features** 

#### TABLE 21 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 21 Front Panel LEDs (continued)



Unleashed Access Point Physical Features

#### TABLE 21 Front Panel LEDs (continued)

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

# **T350 Family**

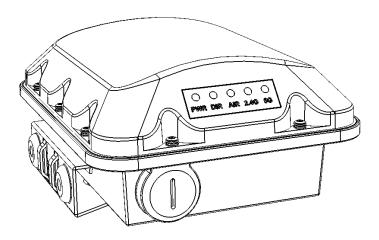
The Unleashed T350 family provides 802.11ax "Wave 2" features, including MU-MIMO, in an outdoor access point.

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

The T350 is available in four antenna variants:

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

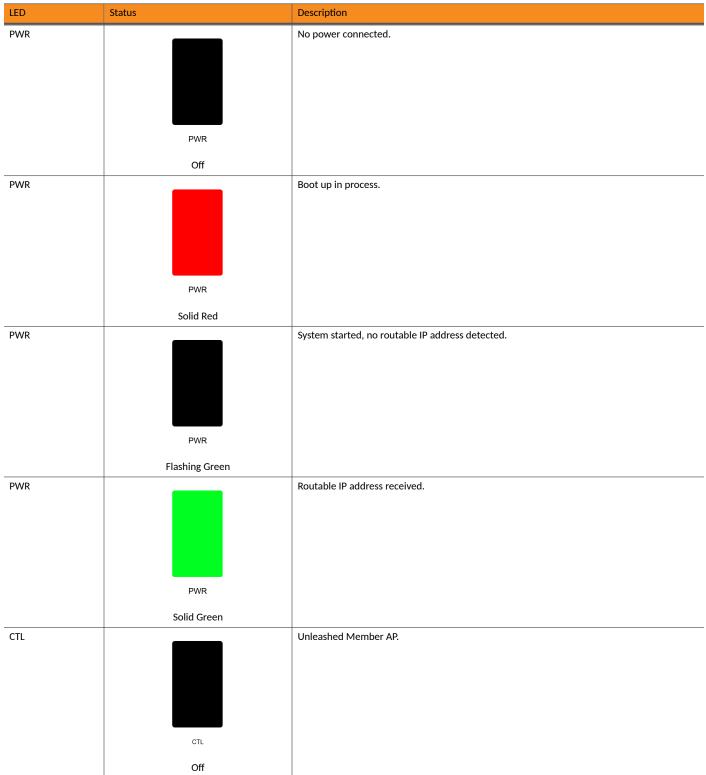
## FIGURE 24 T350d Outdoor Access Point



## **Front Panel**

The T350 features five LEDs on its front panel.

#### **TABLE 22 Front Panel LEDs**

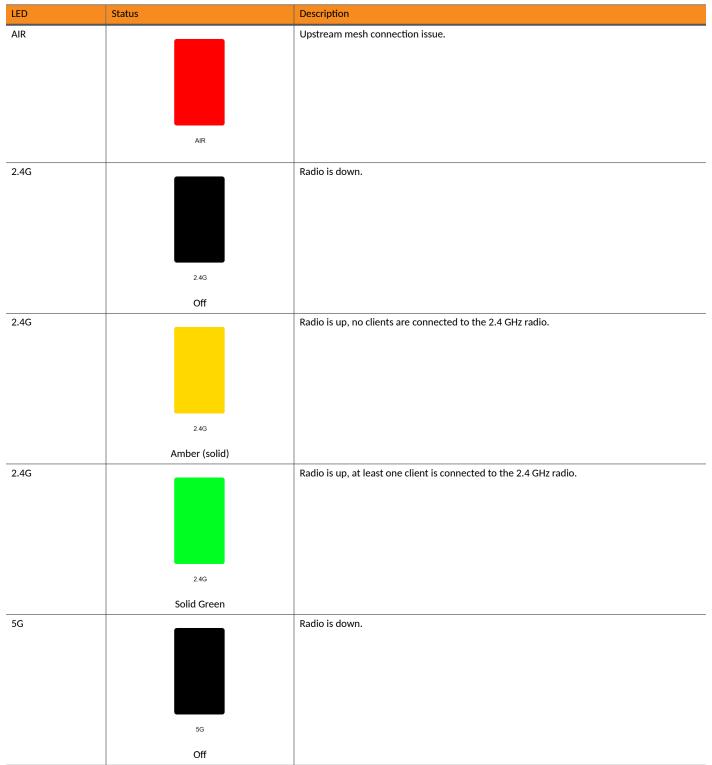


**Unleashed Access Point Physical Features** 

#### TABLE 22 Front Panel LEDs (continued)

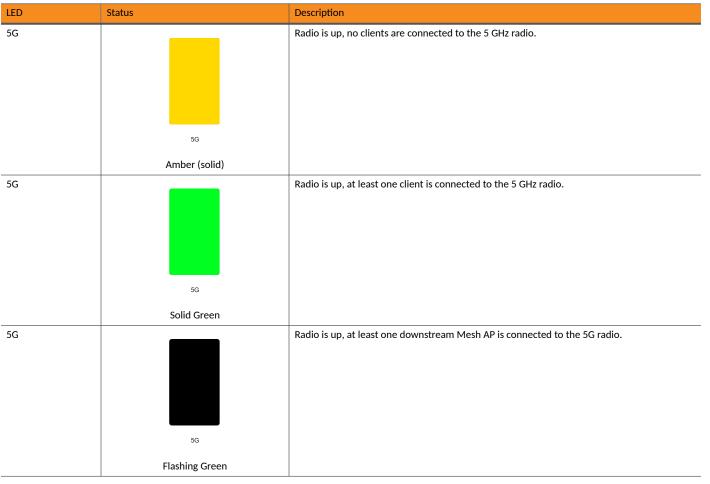
LED	Status	Description
CTL	CTL	Network problem. Cannot contact Unleashed Master.
	Flashing Green (slow, every 2 seconds)	
CTL	CTL	Receiving configuration or image upgrade.
	Flashing Green (fast, 2x per second)	
CTL	CTL	Unleashed Master AP.
AIR	Solid Green	No upstream mesh connection (Root AP).
	AIR	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

#### TABLE 22 Front Panel LEDs (continued)



**Unleashed Access Point Physical Features** 

#### TABLE 22 Front Panel LEDs (continued)



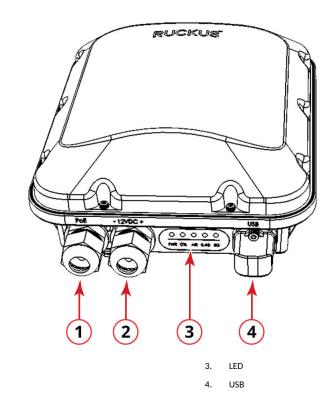
# **T350SE**

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

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

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

#### FIGURE 25 Unleashed T350SE Access Point



## **Front Panel**

12V DC

1. PoE

2.

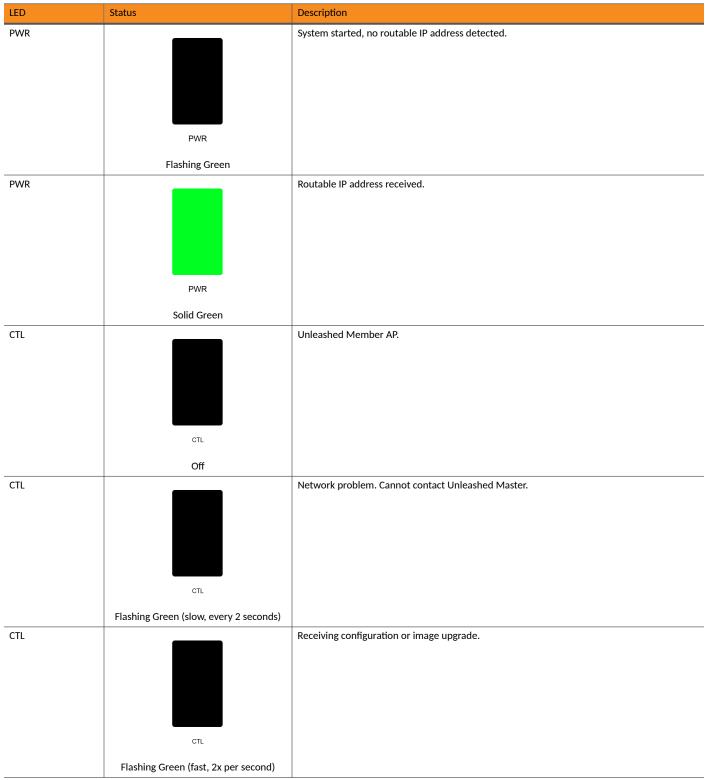
The T350SE AP features five LEDs on its front panel.

#### TABLE 23 Front Panel LEDs

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

**Unleashed Access Point Physical Features** 

#### TABLE 23 Front Panel LEDs (continued)



#### TABLE 23 Front Panel LEDs (continued)

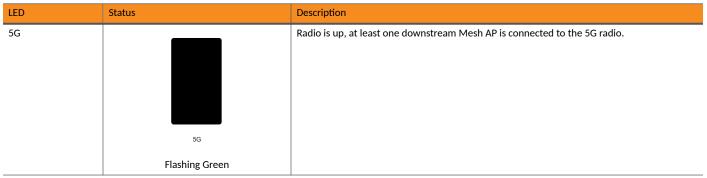


**Unleashed Access Point Physical Features** 

#### TABLE 23 Front Panel LEDs (continued)



### TABLE 23 Front Panel LEDs (continued)



## **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.

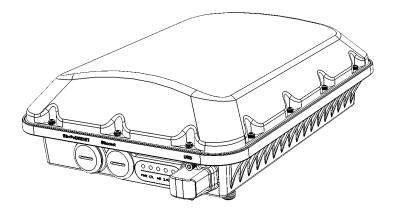
The T610 also includes a USB port for BLE Smart Beacon, Zigbee or other IoT devices.

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 26 Unleashed T610/T610s Outdoor Access Point

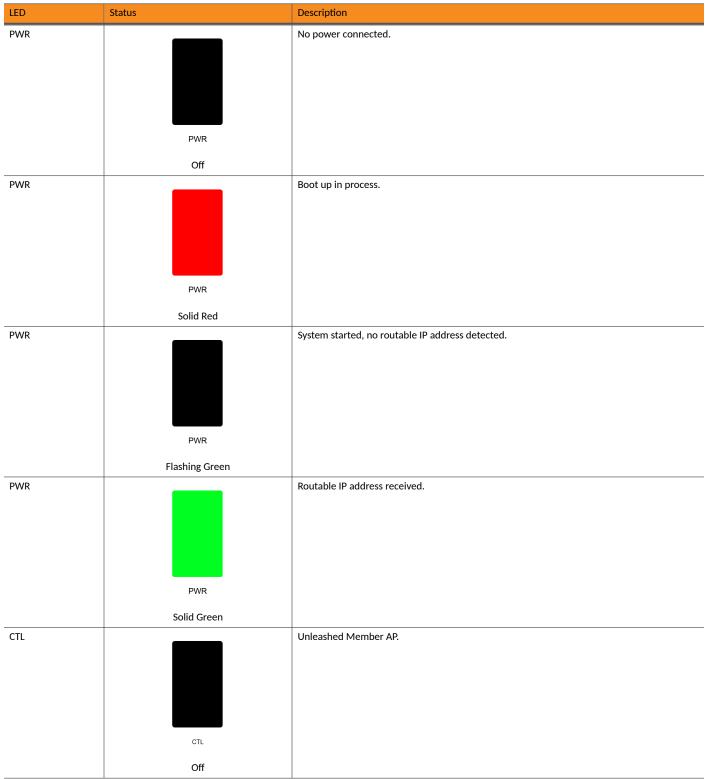


### **Front Panel**

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

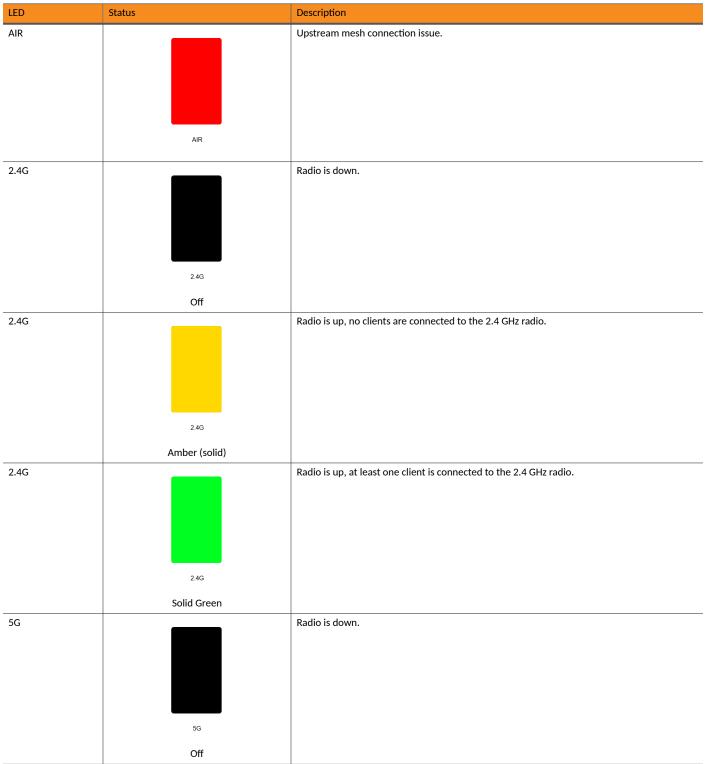
Unleashed Access Point Physical Features

### **TABLE 24 Front Panel LEDs**

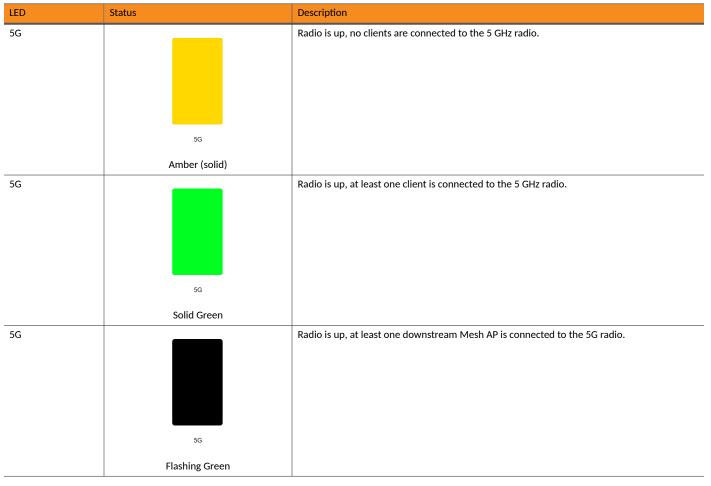


CTL Network problem. Cannot contact Ur	nleashed Master.
Flashing Green (slow, every 2 seconds)	
CTL Receiving configuration or image upg	grade.
CTL	
Flashing Green (fast, 2x per second)	
CTL Unleashed Master AP.	
CTL	
Solid Green	
AIR No upstream mesh connection (Root	: AP).
AIR	
N/A	
AIR Upstream mesh connection establish	ied (Mesh AP).
AIR	

**Unleashed Access Point Physical Features** 



### TABLE 24 Front Panel LEDs (continued)



## T710 and T710s

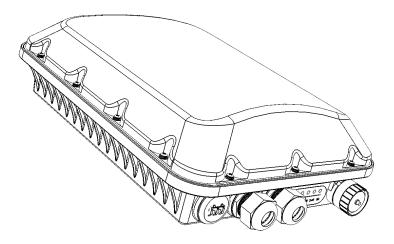
The Unleashed T710 is the first outdoor Ruckus Unleashed 802.11ac Wave 2 access point.

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

### NOTE

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

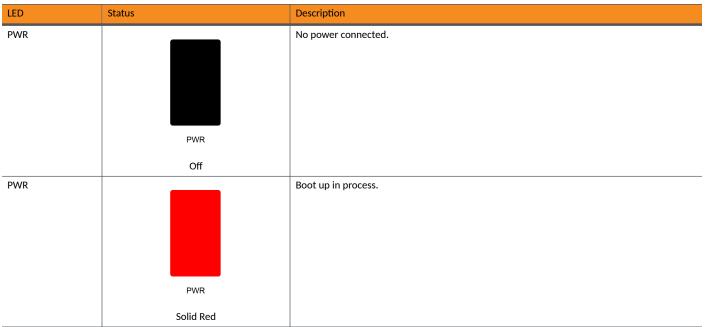
### FIGURE 27 Unleashed T710/T710s Outdoor Access Point

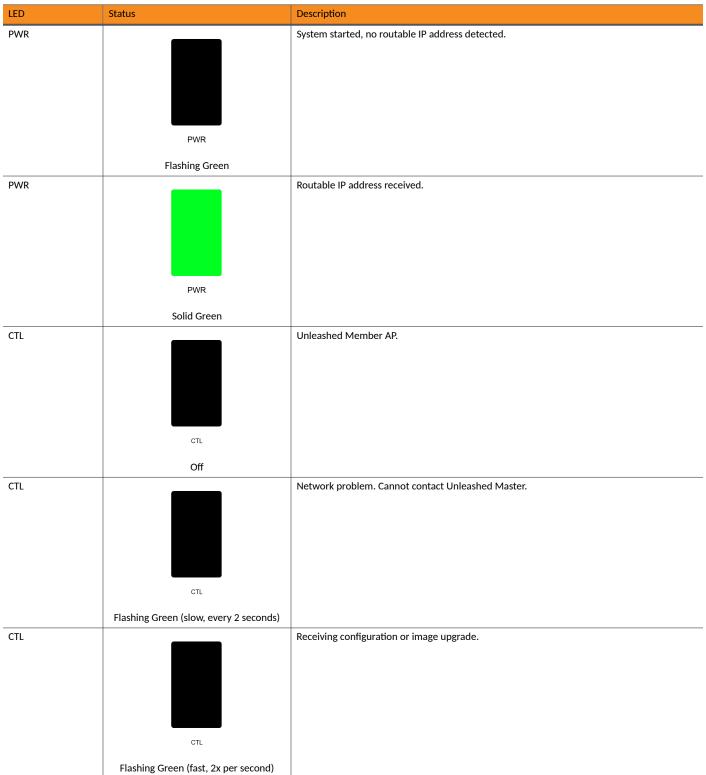


### **Front Panel**

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

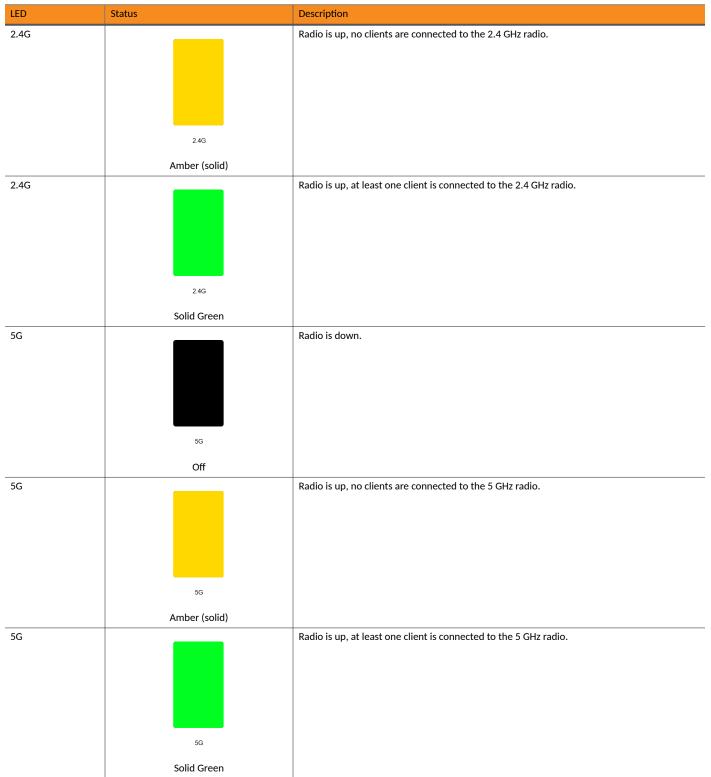
### TABLE 25 Front Panel LEDs





**Unleashed Access Point Physical Features** 

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



**Unleashed Access Point Physical Features** 

### TABLE 25 Front Panel LEDs (continued)

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

### **T750**

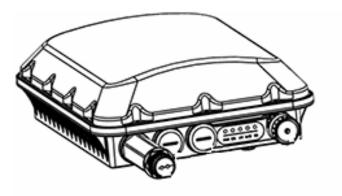
The Ruckus T750 is a high-end dual-band outdoor Wi-Fi 6 AP that supports 8 spatial streams (4x4:4 in 5GHz, 4x4:4 in 2.4GHz).

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

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

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

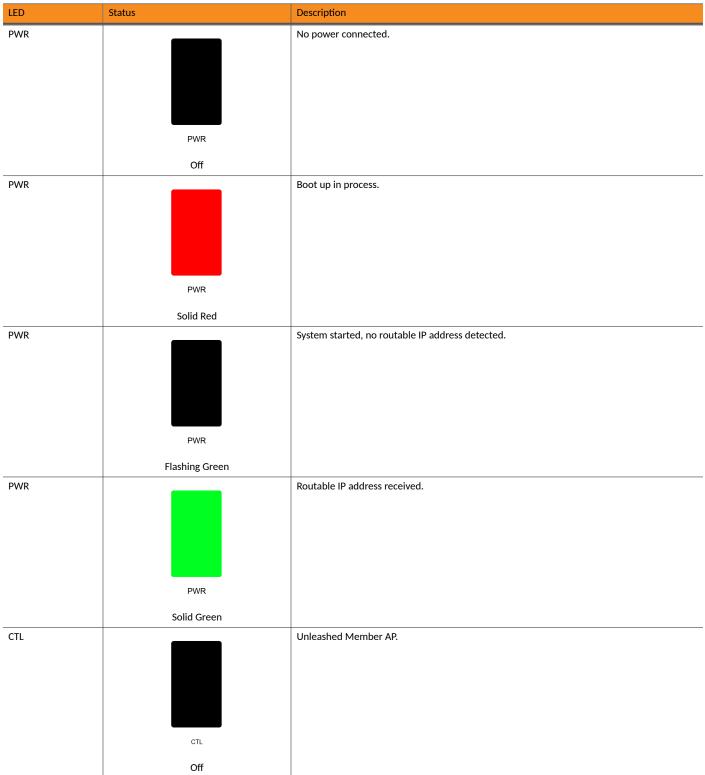
### FIGURE 28 Unleashed T750 Access Point



### **Front Panel**

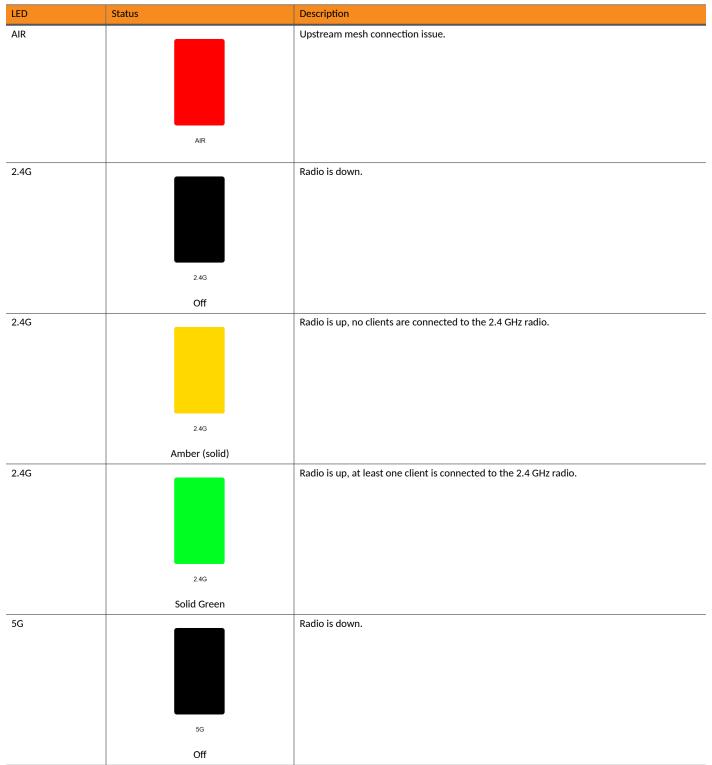
The T750 AP features five LEDs on its front panel.

### TABLE 26 Front Panel LEDs



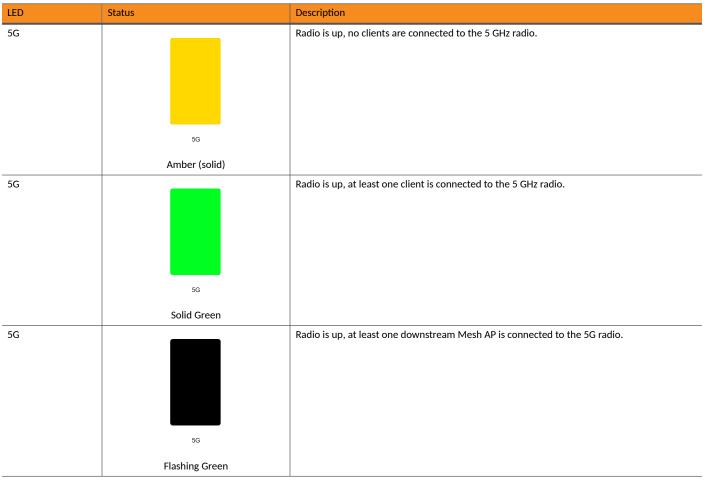
**Unleashed Access Point Physical Features** 

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



**Unleashed Access Point Physical Features** 

### TABLE 26 Front Panel LEDs (continued)



## **T750SE**

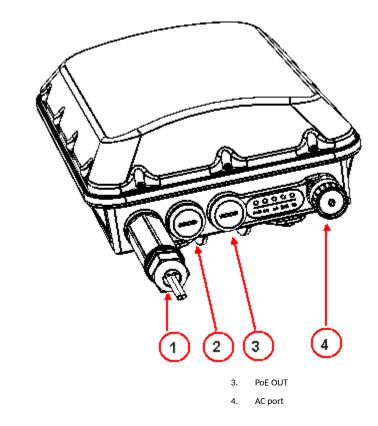
The Ruckus T750SE is a high-end dual-band outdoor Wi-Fi 6 AP with external antenna connectors that supports 8 spatial streams (4x4:4 in 5GHz, 4x4:4 in 2.4GHz).

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

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

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

FIGURE 29 Unleashed T750SE Access Point



# SFP port PoE IN

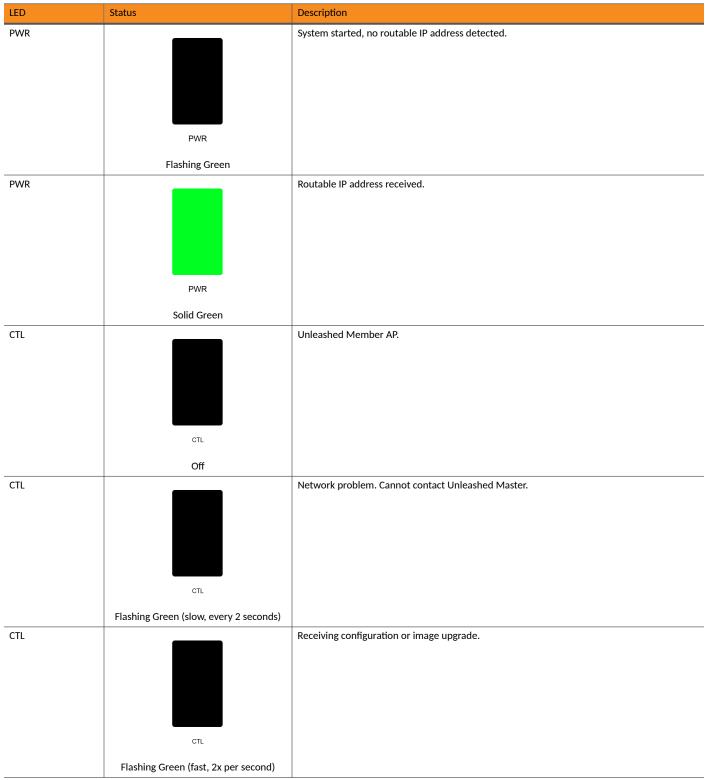
### **Front Panel**

The T750SE AP features five LEDs on its front panel.

### TABLE 27 Front Panel LEDs

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

**Unleashed Access Point Physical Features** 





**Unleashed Access Point Physical Features** 



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

# **Setting Up an Unleashed Wi-Fi Network**

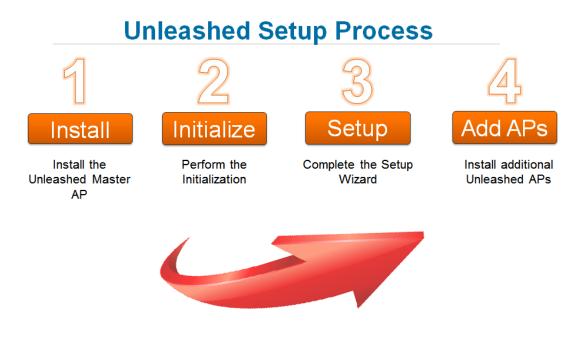
•	Overview of the Setup Process	129
•	Step 1: Unpack and Install the Unleashed Master AP	. 130
•	Step 2: Configure Your Unleashed Network	. 130
•	Step 3: Customize Your Wireless LANs	. 156
•	Step 4: Deploy Additional Unleashed Member Access Points	159

# **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 130
- 2. Step 2: Configure Your Unleashed Network on page 130
- 3. Step 3: Customize Your Wireless LANs on page 156
- 4. Step 4: Deploy Additional Unleashed Member Access Points on page 159
- 5. Begin Using Your Ruckus Unleashed Network!

### FIGURE 30 Unleashed setup overview



### NOTE

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

# Step 1: Unpack and Install the Unleashed Master AP

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

### NOTE

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

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

### NOTE

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

# **Step 2: Configure Your Unleashed Network**

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

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

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

## Step 2a: Setup Using the Mobile App

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

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

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

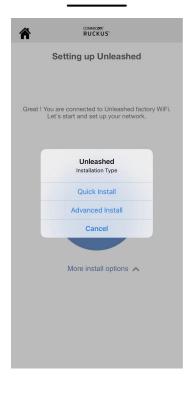
2. Launch the app, and follow the on-screen instructions to configure your RUCKUS Unleashed networks.

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

FIGURE 31 RUCKUS Unleashed Mobile App for iOS and Android

	Unleashed Home	
Ŕ	Typical Install Most commonly deployed configuration.	(
	OR	
	Gateway Install	
ප	Unleashed AP acts as gateway for both wired & wireless devices.	
	Manage Network	
	Helps to manage your Unleashed network.	

Version: 6.90.1

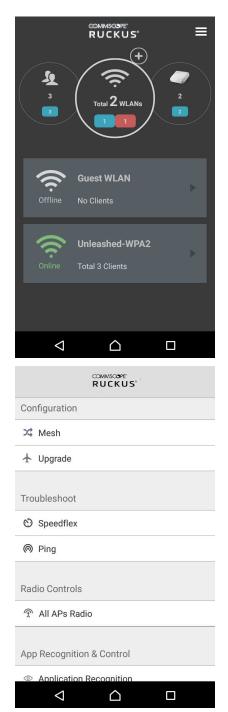


To configure RUCKUS Unleashed, in the **Wireless LAN** page, enter WLAN name, password, and the country where the AP is located, and click **Next**. In the **Administration** page, enter admin username and password, and click **Finish**.

Configure Unleashed Wireless LAN	
Step 1 Step 2	
WLAN Name Ruckus-Wireless 1	8
WLAN Password	
Country where AP is located US	
Back Next	
COMMSCOPE	
comiscore RUCKUS	
Configure Unleashed	
Configure Unleashed Administration	
Configure Unleashed Administration Step 1 Step 2	0
Configure Unleashed Administration Step 1 Step 2 Admin Username admin	©
Configure Unleashed Administration Step 1 Step 2 Admin Username admin	
Configure Unleashed Administration Step 1 Step 2 Admin Username admin	
Configure Unleashed Administration Step 1 Step 2 Admin Username admin	
Configure Unleashed Administration Step 1 Step 2 Admin Username admin	
Configure Unleashed Administration Step 1 Step 2 Admin Username admin	
Configure Unleashed Administration Step 1 Step 2 Admin Username admin	
Configure Unleashed Administration Step 1 Step 2 Admin Username admin	

COMISSIONE RUCKUS'
Configuring Unleashed
Customization in progress 3m 43s remaining
RUCKUS'
<b>O</b>
Congratulations! Your Unleashed network is ready to use !
Test your WiFi Speed !
Manage Network

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



# Step 2b: Setup Using a Web Browser

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

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

### NOTE

Only R750 AP or R850 AP support Dedicated Master mode.

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

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



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

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

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

### FIGURE 34 Security Warning (Chrome)

Your connection is not private	
Attackers might be trying to steal your information from <b>192.168.40.1</b> . passwords, messages, or credit cards). NET::ERR_CERT_AUTHORITY_INVALID	
Automatically report details of possible security incidents to Google. <u>Privacy</u>	policy
Advanced	Back to safety

3. In response to the security warning, complete one of the following processes:

- Click I Understand the Risks > Add Exception... > Confirm Security Exception (Firefox)
- Click Advanced > Proceed to [IP address] (unsafe) (Chrome)
- Click Continue to this website (not recommended) (Internet Explorer)

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

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

### FIGURE 35 Installation Page

This is the most straple and quick way to install     (internal Gateway: Disabled; Mesh: Disabled;     Wireless LAN     • Name (ESSID):     • Name (ESSID):     • Administrator     • Administrator     • Country Code:     • Initied States      Provide more advanced options to install
Name (ESSID): Ruckus-Wireless 1     Passphrase:      Administrator      Admin Username: admin     Password:      Admin Username: admin     Password:      Country Code: United States
Admin Username: admin     Password:      Ø     If a Ruckus ICX switch is managed by Unleashed hen it will use the same login credentials as provided above.     Country Code: Unled States

### NOTE

Click **Custom Install** for other installation options. For more information, refer to Advanced Install on page 138 and UMM Install on page 148. For information on **Local Upgrade** options, refer to Installation with Local Upgrade on page 150.

### **Advanced Install**

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

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

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

### NOTE

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

c) If you want to enable Mesh networking for your Unleashed network, select the **Mesh** check box. Refer to Mesh Networking on page 397 for more information.

### NOTE

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

### NOTE

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

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

### NOTE

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

### e) Click Next to continue.

### FIGURE 36 Setup Wizard: System Page

System	IP setting	Wireless LAN	Administrator	Review
Version	<b>1:</b> 200.13.6.1.190			
* Name	a: Ruckus-Unleashed	-Dedica Name your sy characters ex	stem 32 characters max using a cluding space.	alphanumeric
• Country Code	a: United States	✓ Select the rep	gulatory country code for the Uni-	eashed Network.
Mes	n: 🔽	Select this ch	eck box to enable Mesh for the	Unleashed Network.
* Mesh Name (ESSID	): Mesh-4119720017	55-736 Each mesh-e mesh WLAN	nabled Unleashed requires a uni- for the backbone traffic.	que name(SSID) for t
Mesh Passphrase	: nHkmsrLIX9ok3tD_	L3TPwx Generate		
Dedicated Maste	r: 🗹	Network, The	reck box to enable Dedicated Ma radio function of Dedicated Mast vice cannot be provided.	aster for the Unleash ter AP will be disable

- Step 2: Configure Your Unleashed Network
  - 3. On the **IP Setting** page, select whether the AP will serve as a gateway using one Ethernet port as a WAN port (connected to a cable or DSL modem, PPPoE connection, and so on), and the other as a LAN port.

### NOTE

If your modem or router already provides gateway functionality, do not enable Gateway mode on the Unleashed Master AP. For more information, refer to Gateway Mode on page 374.

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

### NOTE

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

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

### NOTE

Optionally, if a manual IP address is configured, you can enable the built-in DHCP Server to provide IP addresses to clients on the Unleashed subnet. For more information, refer to DHCP Server on page 380.

### FIGURE 37 Setup Wizard: IP Setting Page

System	IP setting	Wireless LAN	Administrator	Review
WAN IP Address		¥		
🔿 Manual	OHCP			
• IP Address	192.172.10.225			
* Netmask	255.255.255.0			
* Gateway	192.172.10.1			
Primary DNS Server	137.117.0.1			
Secondary DNS Server	8.8.4.4			
Access VLAN	1			

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

### NOTE

The default value of the access VLAN ID is 1.

d) If Gateway mode is enabled, select whether to assign a manual IP address or allow the system to obtain an IP address automatically using DHCP or PPPoE for the WAN port, and configure the local subnet settings for the LAN port. Under **Standby WAN Port**, select whether to assign a manual IP address or allow the system to obtain an IP address automatically using DHCP. The default is **DHCP** (Dynamic). For more information on Gateway mode, refer to Gateway Mode on page 374.

### NOTE

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

### FIGURE 38 Enabling Gateway Mode

1	2	-3-	4		-5	
System	IP setting	Wireless LA	N Adminis	strator	Review	
Cateway Mode						
	AMCKMS.					
WAN Port		▼ LA	N & WLAN Client IP A	ddresses	▼	
WAN Port	PORT 3 V		* Starting IP	10.106.0.2		
		DΕ	* Ending IP	10.106.7.209		
	172.172.10.186		Number of IPs	2000		
	255.255.255.0		Lease Time	Twelve hours	~	
	172.172.10.1	1	Primary DNS Server	137.117.0.1		
* Primary DNS Server	137.117.0.1	Sec	ondary DNS Server	8.8.8.8		
Secondary DNS Server	8.8.8.8					
Standby WAN Port ()		► LA	N & WLAN IP Address		•	
WAN Port	PORT 4 V		* Router IP	10.106.0.1		
🔿 Manual	O DHCP		* Netmask	255.255.0.0		
* IP Address	10.223.4.106					
* Netmask	255.255.254.0					
* Gateway	10.223.5.254					
* Primary DNS Server	10.10.10.190					

e) Click Next to continue.

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

### NOTE

WPA2 is highly recommended for the highest level of security.

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

### FIGURE 39 Setup Wizard: Wireless LAN Page

1	2	3	4	-5
System II	P setting Win	eless LAN Admi	inistrator	Review
* Name (ESSID): Password Protect (WPA2):		Name your own wireless LA LAN list. It will be shown as It is highly recommended se LAN. So only authorized us between 8 and 64 character		

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

### FIGURE 40 Setup Wizard: Administrator Page

System       IP setting       Wreless LAN       Administrator       Review         • Admin Username:       Idmin       Interface and the following password will permit admin access two bin furfaces and the following password will permit admin access two bin furfaces and the following password will permit admin access two bin furfaces and the following password will permit admin access the bin bin furface and the following password will permit admin access the bin bin furface and the following password will permit admin access the bin bin furface and the following password will permit admin access the bin bin furface and the following password will permit admin access the bin bin furface and the bin	<ul> <li>Admin Username: admin</li> <li>This username and the following password will permit admin access to web interface after the set up is done.</li> <li>Password: </li> <li>Confirm Password: </li> <li>Confirm Password: </li> <li>Confirm Password: </li> <li>Enter the above password again.</li> <li>Password Recovery:</li> <li>Security Email: example@mail.com</li> <li>The will be used to reset forgotten password</li> <li>What is your mother's ma </li> </ul>	1	2	<u>a</u>	5
Password:      ·····     Password:      The password can only contain between 4 and 32 characters and cannot have      or      Sconfirm Password:      ····     Password Recovery:      ···     Security Email:      example@mail.com     The will be used to reset forgotten password     The will be used to reset forgotten password     The will be used to reset forgotten password	<ul> <li>Password: The password can only contain between 4 and 32 characters and cannot have "" or "5(" and no spaces are allowed.</li> <li>Confirm Password: Confirm Password can only contain between 4 and 32 characters and cannot have "" or "5(" and no spaces are allowed.</li> <li>Confirm Password: Contain between 4 and 32 characters and cannot have "" or "5(" and no spaces are allowed.</li> <li>Confirm Password: Contain between 4 and 32 characters and cannot have "" or "5(" and no spaces are allowed.</li> <li>Enter the above password again.</li> <li>Password Recovery:</li> <li>Security Email: example@mail.com</li> <li>The will be used to reset forgotten password</li> <li>The will be used to reset forgotten password</li> </ul>	System IF	P setting Wire	eless LAN Administrator	Review
Confirm Password:     Inter the above password again.     Password Recovery:     ✓     Security Email: example@mail.com     The will be used to reset forgotten password     Security Question:     What is your mother's ma      The will be used to reset forgotten password	Confirm Password:          ····				
Security Email: example@mail.com     The will be used to reset forgotten password     Security Question: What is your mother's ma      The will be used to reset forgotten password	Security Email: example@mail.com     The will be used to reset forgotten password     Security Question: What is your mother's ma      The will be used to reset forgotten password	* Confirm Password:	••••• Ø		wed.
		* Security Email:	example@mail.com		

### Setting Up an Unleashed Wi-Fi Network

Step 2: Configure Your Unleashed Network

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

### FIGURE 41 Setup Wizard: Review Page

System	IP setting	Wireless LAN	Administrator	Review
Review the inform	nation below	and click Finish to configure		
System Name	a	Ruckus-Unleashed-Dedicated		
Country Code	a (	United States		
Internal Gateway	, 1	Disabled		
IP Mode	a	Dynamic (DHCP)		
IP setting	,	192.172.10.225		
Wireless LAM	•	Ruckus-Wireless 1		
Admin Username	a) II	admin		
Admin Passwore	<b>i</b>	show password		
Password Recovery	,	Disabled		
Mesl	n (	Mesh-411972001755-736		
Dedicated Maste	e ()	Enabled		
System Time		System time will be automatically set. Your current PC time is 2022/7/11 15	30.03)	

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

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

#### NOTE

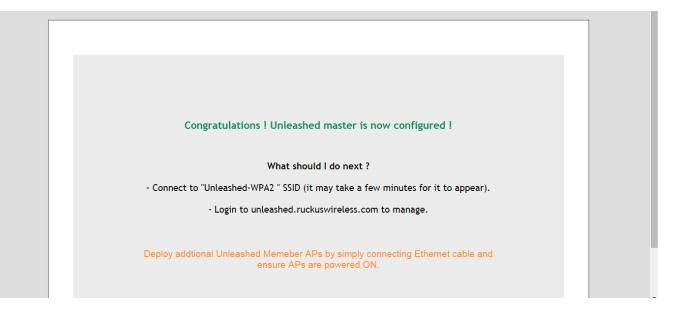
Do not disconnect power or network cables during this process, and do not click Back or Refresh in your web browser.

#### FIGURE 42 Configuring System Settings & Rebooting Page

Configuring system settings & rebooting. It may take few minutes.	
WARNING	
- Do not power off or reboot AP	
- Do not refresh browser or hit browser back.	

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

#### FIGURE 43 Congratulations! Page



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

#### FIGURE 44 Login Page

RUCKUS'	Have you tried new Undesthed mobile app ? (ROS & Android)
Unleashed	
Username Password	
Forget password?	
Unleash	

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

#### FIGURE 45 Unleashed Dashboard

RUCKUS COMMECCIE UNLEASHED	System Name: Dedicated Unleashed	Up Time: 29d 5h 43m	admin Log Ou
Internet		Connected	► F
Cedicated Master		Enabled	SR Connected
📚 WIFi Networks		Total 1 Working	1 Disabled 0
Clients Clients		Total 0 Connected	0 Disconnected 0
Access Points		Total 2 Working	2 Disconnected 0
Switches		Total 0 Working	0 Disconnected 0
Admin & Services			Þ

10. Continue to Step 3: Customize Your Wireless LANs on page 156.

#### Setting Up an Unleashed Wi-Fi Network

Step 2: Configure Your Unleashed Network

### **UMM** Install

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

To enable UMM easy deployment:

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

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

#### FIGURE 46 UMM Install

Unleashed Installation		
O Advanced Install	This is the most typical way to ins	stall if one do not want to use UMM
UMM Install	Use image from UMM to install a	n Unleashed network
* UMM Domain/IP:	10.10.13.17	UMM address from where the Unleashed Network can retrieve configuration
* Config Template Name:	UMM Template 1	Configuration template pre-stored in UMM for the Unleashed Network
* System Name:	Ruckus-Unleashed	Name your system 32 characters max using alphanumeric characters excluding space.
		Back Next

#### FIGURE 47 Contacting UMM for Easy Deployment

Contacting UMM (10.200.3.4) for easy deployment. It may take a few minutes.
Pulling configuration template from UMM
WARNING
- Do not power off or reboot the AP.
Cancel

#### Installation with Local Upgrade

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

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

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

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

#### FIGURE 48 Local Upgrade - Installation Page

This is the most simple and quick way to install (Internal Gateway: Disabled; Mesh: Disabled)
hrase:
word:
Provide more advanced options to install

#### FIGURE 49 Choose Local Image File to Upgrade

Local Upgrade			
System In	fo		
	IP Address:	192.168.0.1	
	Subnet Mask:	255.255.255.0	
	Gateway:	192.168.0.1	
	DNS servers:	,	
	AP Model:	R320	
	AP Serial Number:	481809000088	
	Current Software Version:	200.8.10.3.118	
Select ima			
	Local File Name: Choose File I o file chooser		
	WARNING:Upgrading the firmware could take a few the time.Please do NOT remove power from your AP		

### Step 2c: Setup Using the Command Line Interface

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

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

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

#### NOTE

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

The Unleashed CLI Wizard Configuration Tool starts automatically.

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

#### Configure Unleashed AP to Bridge Mode

```
Please login: super
Password: ******
Welcome to Ruckus Wireless Unleashed CLI Setup Wizard
Would you like to start the Setup Wizard? [yes/no]: yes
Enter the way of installation. 1. easy-deployment installation 2. local wizard [1/2] 2
Enter Administrative User Name (32 characters max) [admin]:
admin
Enter Administrator Password (4-32 characters):
*****
Re-enter Administrator Password (4-32 characters):
*****
Enter System Name (32 characters max) [Ruckus-Unleashed]:
Unleashed
Enter Country Code (or 'help' to show the list) [US]: US
Enable Mesh [yes/NO]? no
Enable Gateway Mode [yes/NO]? no
Enable Dedicated Master [yes/NO]? no
Enter WAN IP type [1]:
     1: DHCP Mode;
     2: Manual Mode;
1
Enter Access VLAN [1]: 1
Enable WLANs [YES/no]? yes
Enter Wireless LAN (ESSID, 1-32 characters) [Ruckus-Wireless 1]:
Unleashed-SSID
Is it an Open WLAN [yes/NO]? no
Enter the WPA2 Passphrase (8-63 characters): *******
Re-enter the WPA2 Passphrase (8-63 characters):
******
Please review the following settings:
System Name=
                            Unleashed
Administrator Name=
                            admin
Country Code=
                            US
                            Disable
Mesh Supported=
Gateway Mode Supported=
                            Disable
Dedicated Master Supported= Disable
IPv4 Mode=
                            DHCP
Access VLAN=
                            1
WLAN ESSID=
                            Unleashed-SSID
Wireless Authentication=
                            WPA2_PSK
Done with the Setup Wizard [yes/no]? yes
Save the configuration ...
It will take a few minutes to complete, do not power off the AP! This AP will reboot automatically.
```

Welcome to Ruckus Unleashed Network Command Line Interface

Step 2: Configure Your Unleashed Network

ruckus>

#### **Configure Unleashed AP in Dedicated Mode**

Please login: super Password: \*\*\*\*\*\*\*

Welcome to Ruckus Wireless Unleashed CLI Command Line Interface

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

Enter the way of installation:

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

2. local wizard

please enter 1 or 2: 2

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

Re-enter Administrator Password (4-32 characters): \*\*\*\*\*

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

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

Enable Mesh [yes/NO]? yes

Enable Gateway Mode [yes/NO]?

Enable Dedicated Master [yes/NO]? yes

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

Enter Access VLAN [1]: 1

Enable WLANs [YES/no]?

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

\*\*\*\*\*\*\* Please review the following settings: System Name= Unleashed

Administrator Name= admin Country Code= US Mesh Supported= Enable Gateway Mode Supported= Disable Dedicated Master Supported= Enable IPv4 Mode= DHCP Access VLAN= 1 WLAN ESSID= Dedicated-SSID Wireless Authentication= WPA2 PSK

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

Save the configuration ...

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

Welcome to Ruckus Unleashed Network Command Line Interface ruckus>

#### **Configure Unleashed AP to Gateway Mode**

```
Please login: super
Password: ******
Welcome to Ruckus Wireless Unleashed CLI Setup Wizard
Would you like to start the Setup Wizard? [yes/no]: yes
Enter the way of installation. 1. easy-deployment installation 2. local wizard [1/2] 2
Enter Administrative User Name (32 characters max) [admin]:
admin
Enter Administrator Password (4-32 characters):
****
Re-enter Administrator Password (4-32 characters):
****
Enter System Name (32 characters max) [Ruckus-Unleashed]:
Unleashed-Gateway
Enter Country Code (or 'help' to show the list) [US]: US
Enable Mesh [yes/NO]? no
Enable Gateway Mode [yes/NO]? yes
Enter AP R510 WAN Port:
    1: port1, eth0, UP:
2: port2, eth1, DOWN:
1
Enter WAN IP type [1]:
     1: DHCP Mode;
     2: Manual Mode;
     3: PPPOE Mode;
1
Enter LAN & WLAN IP Address [10.106.0.1]:
192.168.1.1
Enter LAN & WLAN IP Netmask [255.255.0.0]:
255.255.255.0
Enter Client Starting IP Address [10.106.0.2]:
192.168.1.2
Enter Client Ending IP Address [10.106.7.209]:
192.168.1.200
Enter Lease Time [2]:
    1: 6 hours;
    2: 12 hours;
    3: 1 day;
    4: 2 days;
    5: 1 week;
    6: 2 weeks;
1
```

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

Please review the following System Name= Administrator Name= Country Code= Mesh Supported= Gateway Mode Supported= WAN Port= IPv4 Mode= LAN Port IPv4 Address Info= Client Starting IPv4= Client Ending IPv4= Lease Time= WLAN ESSID=	Unleashed-Gateway admin US Disable Enable port1 eth0 UP DHCP
WLAN ESSID= Wireless Authentication=	Unleashed-SSID WPA2 PSK

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

Save the configuration ...

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

Welcome to Ruckus Unleashed Network Command Line Interface ruckus>

## **Step 3: Customize Your Wireless LANs**

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

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

To customize an existing wireless LAN:

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

FIGURE 50 Click the Wi-Fi networks section to expand

Ţ,	WiFi Networks	Total 1 Working 1 Disabled 0
	Create Edit Disable Delete	Data duration: 1 hours •
	Summary - Total 1 WiFi Networks	Summary
	Clients Traffic	1 WiFi Networks enabled, 0 WiFi Networks disabled.
	Unleashed	5 Clients Show Clients Info
1	0 0 5 Clients Traffic	Client Status for last
		5

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

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

WiFi Network      Create      Edt	S Traffic: 0.01 MB		Total 1	Working 1 Data duration:	Disabled 0	•
Summary - Total 1 Wi	Fi Networks	Summary 1 WiFi Networks enabled, 0 WiFi Networks disabled.				
Unleashed 0 0 5 Clients Traffic		5 Clients Client Status for last	ate 📕 Poor	Show Clier	its Info 🕨	
		5				

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

#### NOTE

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

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

#### FIGURE 52 Editing an existing WLAN

Create	Edit Disable Delete		Data duration: 1 hours 🔻
	Euit WLA	4	×
Clier		<ul> <li>Name: Unleashed</li> <li>Isage Type:          <ul> <li>Standard for most regular wireless network usage</li> <li>Guest Access guest access policies and access control will be applied</li> </ul> </li> </ul>	Clients Info 🕨
Unleashed 1 0 0	Authenticati 5 Encrypti	Hotspot Service known as WISPr      MAthod:      Open      802.1X EAP      MAC Address      Method:      WPA2      WPA3      WPA3-Mixed      OWE      None	
		Password:     Show password       ing Server:     Disabled     •       Send Interim-Update every     10     minutes	
	Show Advanced C	ptions ► oĸ	Cancel
		13:08 13:09 13:10 13:11 13:12 13:13 13:14	13:15 13:16 13:17
		Traffic for last	

Congratulations! Your Unleashed network is now configured and ready for use. You may now proceed to Step 4: Deploy Additional Unleashed Member Access Points on page 159.

## **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	161
•	Navigating the Dashboard	161
•	Using the Dashboard Components	. 162

## **Unleashed Administration Interface Overview**

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

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

## **Navigating the Dashboard**

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

#### FIGURE 53 RUCKUS Unleashed Dashboard

	UCKUS IMSCOPE UNLEASHED		3	System Name: Dedicated-Unleashed	Y	Up Time: 29d 5h 43m	(	2) 🛔	Help Log Out
	Internet						Connected		►
	Dedicated Master						Enabled	SR Connected	Þ
<b>(</b> (t·	WiFi Networks	Traffic: 0.00 MB				Total 1	Working 1	Disabled 0	Þ
۵	Clients	Clients				Total 0	Connected 0	Disconnected 0	Þ
	Access Points					Total 2	Working 2	Disconnected 0	Þ
	Switches					Total 0	Working 0	Disconnected 0	Þ
ø	Admin & Services								►

#### **TABLE 28** Dashboard Components

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

#### TABLE 28 Dashboard Components (continued)

Number	Component	Description
3	Network Components	Provide general overviews of each component. Click any of the components to expand for more detailed information and configuration options. Refer to Using the Dashboard Components on page 162.

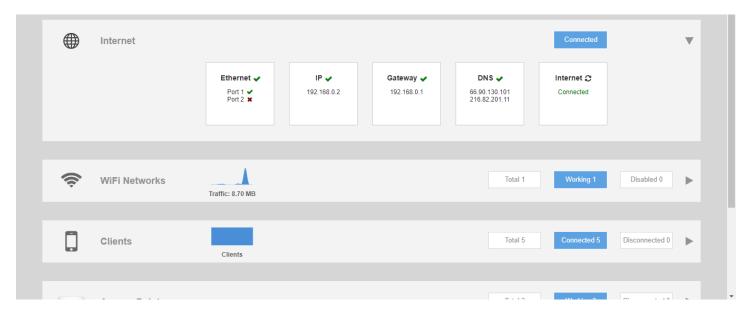
## **Using the Dashboard Components**

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

### Internet

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

#### **FIGURE 54 Internet Component**



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

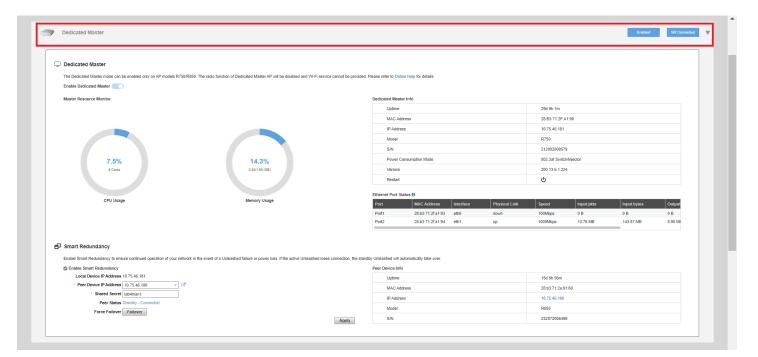
### **Dedicated Master**

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

#### NOTE

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

#### FIGURE 55 Dedicated Master Component

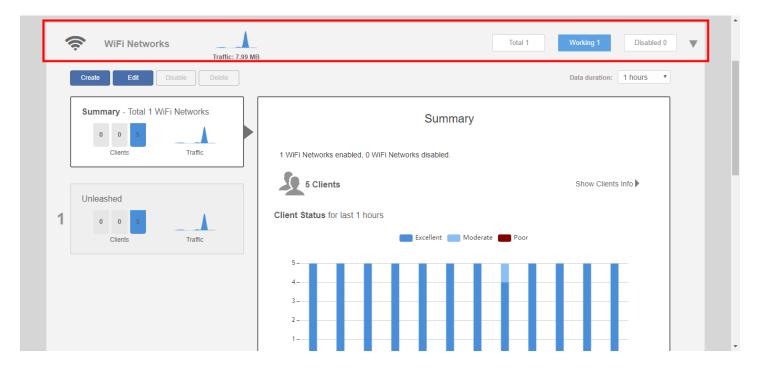


### **WiFi Networks**

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

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

#### FIGURE 56 WiFi Networks Component



### **Clients**

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

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

#### **FIGURE 57 Clients Component**

	Clients						
5 clients connected, 0 clients disc	connected.						
Wired Clients	0 wired clients connect	ted					
Wireless Clients	5 wireless clients con	nected					▼
Show details Rename  🖈 Ma	ark Favorite 🛛 🖈 Unmark	Favorite	oubleshooting More -		Search	Q	•
★ Mac Address	IP Address	os	Name	User	AP Name	WLAN	s
c8:3a:6b:db:1a:3e	192.168.0.6	N/A	Roku		Unleashed	Unleashed	E
88:71:e5:a8:7a:d3	192.168.0.14	N/A			Unleashed	Unleashed	E
48:a4:72:9f:13:bb	192.168.0.10		LP-JFILES		Unleashed	Unleashed	E
f0:03:8c:fb:73:38	192.168.0.4	N/A	Roomba-3143C90C41834720		RuckusAP	Unleashed	E
04:b1:67:47:c4:20	192.168.0.8	÷	Xiaomi Mi A1		Unleashed	Unleashed	E

### **Access Points**

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

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

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

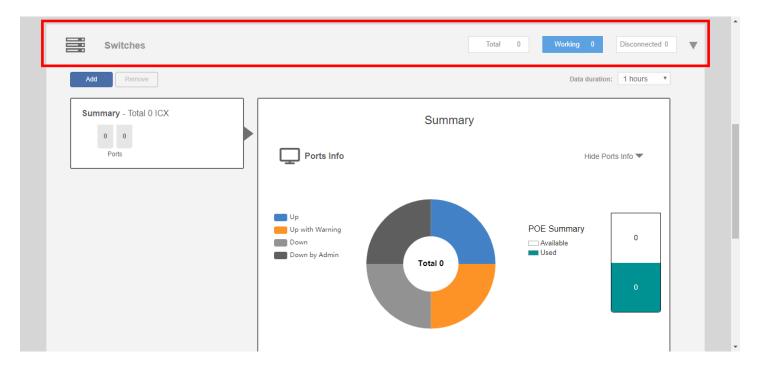
#### FIGURE 58 Access Points Component

	Edit Restart Remove	Data duration: 1 h	ours 🔻
	Summary - Total 3 Access Points	Summary	
	Clients Traffic	Maximun 25 APs support 3 Access Points connected, 0 Access Points disconnected.	
	Master Unleashe[35:c9:40]	Mesh Status :Enabled Show Mesh Topology	•
1	0 0 4 2.4G 5G Clients Traffic	5 Clients Show Clients Info	•
		Client Status for last 1 hours	
	Mesh RuckusAP[1c:12:c0]	Excellent 📒 Moderate 🛑 Poor	

### **Switches**

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

#### FIGURE 59 Switches Component



### **Admin & Services**

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

#### FIGURE 60 Admin & Services Component

🛄 System	System Info	
System Info	Name* Unleashed	
IP Settings	System Version         200.7.10.2.294           Unleashed ID         un9418490011251546969169799         Generate	
System Time	Comeasieu ib unatiotadu 112010400001201040300 Todataal Generate	
Country Code	Preferred Master	
Roles	Preferred Master No Preference 🔻	
Users	Upon applying this change, the selected AP will become a Master AP if it's not a Master AP currently and the	
Mesh	previous Master AP will be rebooted to become a Member AP. As a result, there may be a brief network disruption.	
	Apply	
Services	Email Server	

# **Dedicated Master Configuration**

<ul> <li>Dedicated Master Overview</li></ul>	
	169
	169
Joining a Member AP to the Dedicated Master Network	171
Dedicated Master AP or Member AP Behind NAT	174
Checking Dedicated Master Status in the Unleashed Web Interface.	175
Smart Redundancy Configuration	175

## **Dedicated Master Overview**

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

#### NOTE

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

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

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

## **Converting an Unleashed Master AP to Dedicated Master**

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

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

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

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

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

For more information, refer to Designating a Preferred Master AP on page 366.

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

Converting an Unleashed Master AP to Dedicated Master

#### FIGURE 61 Warning Message

Dedicated Master	
The Dedicated Master mode can only be enabled on AP models R750/R850, the radio function of Dedicated Master AP will be disabled and Wi-Fi service can provided, please refer to Online Help for details.	ot be
Warning: Current Master AP does not support the Dedicated Master mode, please go to "System into -> Preterred Master' to select the specified AP model as Preterred Master:	
Enable Dedicated Master	

### **Converting an Active Master AP to Dedicated Master**

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

FIGURE 62 Enabling Dedicated Master Mode

Dedicat	d Master				
_					
	ted Master mode can only be enabled on AF lease refer to Online Help for details.	P models R750/R850, the radio	function of Dedicated Master AP v	rill be disabled and Wi-Fi service	cannot be
Enable D	dicated Master				

The system displays the following warning message:

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

#### FIGURE 63 Warning Message: Enabling Dedicated Master

Access Points	Τα	otal 1	Working 1	Disconnected 0	•
Dedicated Master	?	H	Disabled	SR Disabled	v
The Dedicated Master mode can only be provided, please refer to Online Help for a Enable Dedicated Master	Enabling Dedicated Master will reboot the AP. Once enabled, it cannot be disabled unless restoring the Unleashed to factory settings. Do you want to continue? Yes No	(iii be disable	d and Wi-Fi service	cannot be	

2. Click Yes to reboot the AP.

## Joining a Member AP to the Dedicated Master Network

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

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

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

#### NOTE

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

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

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

#### FIGURE 64 Member AP Joining Dedicated Master Using Option 43

Access Point Policies
Approval Z Automatically approve all join requests from APs. (To enhance wireless security,
deactivate this option. This means you must manually "allow" each newly discovered AP.)
Dedicated Master Discovery Policy <ul> <li>Use DHCP OPTION 43 or auto discovery on same subnet (AP settings will be ignored)</li> </ul>
Configure Primary and Secondary Unleashed Settings to AP(IP or domain name is
acceptable)
* Primary Unleashed Addr
Secondary Unleashed Addr
Keep AP's Primary and Secondary Unleashed Settings
Management VLAN () Keep AP's setting () VLAN ID
* Tunnel MTU 1500 (To limit the maximum transmission unit size between Unleashed and AP, range:
850 ~ 1500)
Auto Recovery AP reboots if disconnected from Unleashed for more than 30 Minutes.
Apply

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

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

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

The member AP automatically joins Dedicated Master.

### Placing a Member AP in the Same Network as Dedicated Master

#### NOTE

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

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

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

#### FIGURE 65 Placing Member AP in Same Network as Dedicated Master

Access Point Policies
Access Forner Forces
Approval 🗹 Automatically approve all join requests from APs. (To enhance wireless security,
deactivate this option. This means you must manually "allow" each newly discovered AP.)
Dedicated Master Discovery Policy <ul> <li>Use DHCP OPTION 43 or auto discovery on same subnet (AP settings will be ignored)</li> </ul>
Configure Primary and Secondary Unleashed Settings to AP(IP or domain name is
acceptable)
* Primary Unleashed Addr
Secondary Unleashed Addr
Keep AP's Primary and Secondary Unleashed Settings
Management VLAN () Keep AP's setting () VLAN ID
* Tunnel MTU 1500 (To limit the maximum transmission unit size between Unleashed and AP, range:
850 ~ 1500)
Auto Recovery AP reboots if disconnected from Unleashed for more than 30 Minutes.
Apply

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

### Setting the Dedicated Master IP Address in the Member AP CLI

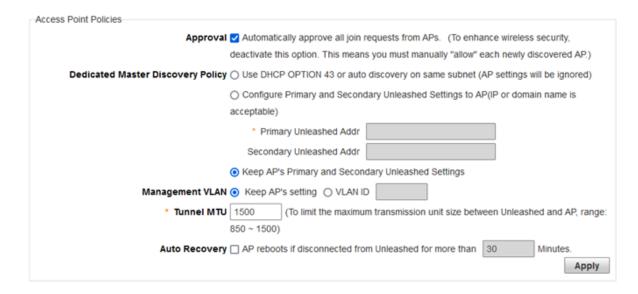
#### NOTE

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

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

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

#### FIGURE 66 Maintaining the Unleashed Settings of the AP



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

```
rkscli: set director ip 192.168.80.13 192.168.80.8
** Please reboot for this change to take effect
OK
```

After reboot, the member AP automatically joins Dedicated Master.

## **Dedicated Master AP or Member AP Behind NAT**

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

### **Basic NAT Topologies**

You can follow three basic NAT topologies:

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

### **Configuration Requirements for Ports or IP Addresses for NAT Topologies**

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

- Member AP behind NAT: Port configuration is not required.
- Dedicated Master AP behind NAT:
  - UDP port 12222, 12223, 60000 and TCP port 443 are configured to the private IP address of the Dedicated Master AP in the NAT mapping table.

- The member AP must connect to the WAN IP address of NAT by Layer 3 (that is, the public IP address in the NAT mapping table of the Dedicated network).
- Both Dedicated Master AP and Member AP behind NAT:
  - UDP port 12222, 12223, 60000 and TCP port 443 are configured to the private IP address of the Dedicated Master AP in the NAT mapping table.
  - The member AP must connect to the WAN IP address of NAT by Layer 3 (that is, the public IP address in the NAT mapping table of the Dedicated network).

## **Checking Dedicated Master Status in the Unleashed Web** Interface

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

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

#### FIGURE 67 Dedicated Master and Smart Redundancy Information

Dedicated Master						
The Dedicated Master mode can only be enabled on AP mo	idels R750/R850, the radio function of Dedicated M	er AP will be disabled and WI-FI service cannot be prov	ided, please refer	to Online Help for details.		
Enable Dedicated Master						
Master Resource Monitor		Dedicated Master Info				
		Uptime		20m 57s		
		MAC Address		C8:03:F5:2C:82	50	
		IP Address	IP Address		192.168.80.13	
	Model		R850			
		SN		982072000717		
1.0%	12.4%	Power Consumption Mode		802 3bt5 Switch/	njector	
	0.21/1.66 (56)	Version		200.13.6.1.193		
		Restart		¢		
CPU Usage	Memory Usage	Ethernet Port Status () Port MAC Address	Interface	Physical Link	Speed	Input
		Port 08.03.15.20.82.53	eth0	down	100Mbps	0.8
		Port2 c8:03:15:2c:82:54	eth0	up	2500Mbps	128.66
						18.00.000
Smart Redundancy						
Enable Smart Redundancy to ensure continued operation of	f your network in the event of a Unleashed failure	over loss. If the active Unleashed loses connection, the	standby Unleashe	ed will automatically take o	ver.	
Enable Smart Redundancy		Peer Device Info				
Local Device IP Address 192.168.80.13		Uptime		N/A.		
* Peer Device IP Address 192.168.80.8	-	MAC Address		NA		
Peer Status Disconnected		IP Address		192.168.80.8		
		Model		NA		

## **Smart Redundancy Configuration**

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

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

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

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

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

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

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

### **Smart Redundancy Setup Overview**

Complete the following steps to set up Smart Redundancy.

- 1. Install the Dedicated Unleashed Master AP. Refer to Setting Up an Unleashed Wi-Fi Network on page 129.
- 2. Configure the Dedicated Unleashed Master AP. Refer to Configuring Dedicated Master for Smart Redundancy on page 176.
- 3. Set up Smart Redundancy with the following components:
  - Member R750 AP or R850 AP
  - Other Dedicated Master
- 4. Check Smart Redundancy status. Refer to Checking the Standby Dedicated Master on page 184.

### **Configuring Dedicated Master for Smart Redundancy**

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

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

#### Smart Redundancy Setup Through Auto Mode

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

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

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

#### FIGURE 68 Enabling Smart Redundancy: Auto Mode

#### Smart Redundancy

Enable Smart Redundancy to ensure continued operation of your network in the event of a Unleashed failure or power loss. If the active Unleashed loses connection, the standby Unleashed will automatically take over.

Enable Smart Redundancy	Peer Device Info		
Local Device IP Address 192.168.184.127	Uptime	N/A	
* Peer Device IP Address 192.168.183.126 *	MAC Address	N/A	
Peer Status N/A	IP Address	N/A	
	Model	N/A	
Apply	S/N	N/A	

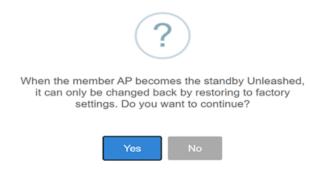
4. From the Peer Device IP Address list, select the IP address of the member R750 AP or R850 AP.

#### NOTE

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

5. Click Apply. A confirmation message is displayed.

#### FIGURE 69 Confirmation Message for Selecting Peer Device



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

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

#### FIGURE 70 Checking Smart Redundancy Status

'n	RU RU	UNLEASHED	URL Filtering License	Unleashed mobile app	is now available !	Ruckus-Unleashed	Up Time: 6m 33s	admin	Help Log Out
		Internet					Connected		•
		Dedicated Master					Enabled	SR Connected	▶
Ð	Smart	Redundancy							
		Smart Redundancy to ensure conti Unleashed will automatically take		network in the event	of a Unleashed failu	re or power loss. If t	he active Unleashed lose	es connection	i, the
	🖾 Enab	ele Smart Redundancy		F	eer Device Info				

Enable Smart Redundancy	Peer Device Info	Peer Device Info		
Local Device IP Address 192.168.183.126	Uptime	4m 57s		
* Peer Device IP Address 192.168.184.127 *	MAC Address	28:b3:71:21:59:30		
* Shared Secret ruckus	IP Address	192.168.184.127		
Peer Status Standby - Connected	Model	R750		
Force Failover Failover				
App	sly S/N	212002008421		

#### NOTE

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

#### NOTE

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

#### NOTE

Smart Redundancy supports synchronization of SSL certificate.

#### NOTE

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

#### NOTE

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

#### Smart Redundancy Setup Through Manual Mode

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

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

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

#### NOTE

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

#### FIGURE 71 Enabling Smart Redundancy: Manual Mode

#### Smart Redundancy

Enable Smart Redundancy to ensure continued operation of your network in the event of a Unleashed failure or power loss. If the active Unleashed loses connection, the standby Unleashed will automatically take over.

N/A N/A N/A

N/A

Enable Smart Redundancy			Peer Device Info	
Local Device IP Address	192.168.183.126		Uptime	
Peer Device IP Address	192.168.184.127 -	]	MAC Address	
* Shared Secret	ruckus		IP Address	
Peer Status	N/A		Model	
			Model	
		Apply	S/N	

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

#### NOTE

The versions of local and peer devices must match.

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

1

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

#### FIGURE 72 Syncing Configuration Between Local and Peer Devices

#### Smart Redundancy

Enable Smart Redundancy to ensure continued operation of your network in the event of a Unleashed failure or power loss. If the active Unleashed loses connection, the standby Unleashed will automatically take over.

Peer Device Info

Enable Smart Redundancy	
Local Device IP Address	192.168.183.126
* Peer Device IP Address	192.168.184.127 *
* Shared Secret	ruckus
Peer Status	Pending
Smart Redundancy is configuration to syncl	s not fully operational yet. Select which correct hronize.
Sync to peer	(last updated on 2022/07/12 17:37:18)
Sync from peer	(last updated on 2022/07/12 17:41:49)

Feel Device Into	
Uptime	1m 29s
MAC Address	28:b3:71:2f:59:30
IP Address	192.168.184.127
Model	R750
S/N	212002008421

Apply

- 12. Choose one of the following options:
  - Click **Sync to peer** on the primary Dedicated Master. A confirmation message is displayed.

#### FIGURE 73 Confirmation Message: Sync to Peer

?
Unleashed will reboot and all lost. It may take a few minutes.

Yes

Click Yes to proceed.

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

• Click Sync from peer on the primary Dedicated Master.

A confirmation message is displayed.

FIGURE 74 Confirmation Message: Sync from Peer

1		1
1	2	
	-	
1	_	/

Please note current Unleashed will reboot and all configuration will be lost. It may take a few minutes.



Click Yes to proceed.

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

NOTE

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

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

The secondary Dedicated Master enters the standby mode.

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

#### FIGURE 75 Checking the Status of Smart Reducdancy

M RI	UCKUS' MISCOPE UNLEASHED	URL Filtering License	K > leashed mobile app is now a IOS & Android	System Name: Ruckus-Ur vailable !	leashed Up Time: 6m 33s	admin	Help Log Out
	Internet				Connected		Þ
	Dedicated Master				Enabled	SR Connected	) ►
-							

#### Smart Redundancy

Enable Smart Redundancy to ensure continued operation of your network in the event of a Unleashed failure or power loss. If the active Unleashed loses connection, the standby Unleashed will automatically take over.

Enable Smart Redundancy	Peer Device Info		
Local Device IP Address 192.168.183.126	Uptime	4m 57s	
* Peer Device IP Address 192.168.184.127 * C	MAC Address	28:b3:71:2f:59:30	
* Shared Secret ruckus	IP Address	192.168.184.127	
Peer Status Standby - Connected Force Failover Failover	Model	R750	
Apply	S/N	212002008421	

#### NOTE

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

#### NOTE

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

#### NOTE

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

#### NOTE

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

#### NOTE

Smart Redundancy supports synchronization of SSL certificate.

#### NOTE

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

#### NOTE

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

#### Smart Redundancy Setup Through the Command Line Interface

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

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

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

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

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

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

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

g <sup>a</sup> login as:
g. Please login: admin
Password:
Welcome to Ruckus Unleashed Network Command Line Interface
ruckus> ena
ruckus# config
You have all rights in this mode.
ruckus(config)# system
ruckus(config-sys)# smart-redundancy
ruckus(config-sys-smart-redundancy)# peer-addr 192.168.183.126
The command was executed successfully. To save the changes, type 'end' or 'exit'.
ruckus(config-sys-smart-redundancy)# secret ruckus
The command was executed successfully. To save the changes, type 'end' or 'exit'.
ruckus(config-sys-smart-redundancy)
The smart redundancy settings have been updated.
Your changes have been saved.
ruckus(config-sys)# smart-redundancy
ruckus(config-sys-smart-redundancy)# show
Smart Redundancy:
Status= Enabled
Local Connect Status= Disconnected
Peer IP Address = 192.168.183.126
Peer Connect Status = Disconnected
Shared Secret= ruckus
ruckus(config-sys-smart-redundancy)#
idekus (config-sys-smart-fedundancy) #

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

#### NOTE

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

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

### **Checking the Standby Dedicated Master**

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

#### FIGURE 78 Opening the Standby Dedicated Master Web Interface

#### B Smart Redundancy

Enable Smart Redundancy to ensure continued operation of your network in the event of a Unleashed failure or power loss. If the active Unleashed loses connection, the standby Unleashed will automatically take over.



The standby mode information is displayed.

#### FIGURE 79 Standby Dedicated Master Information

COMMSCO	<i>n</i>	UNLEASHED				ayı	stem Name: Ruckus-Unleashed	Up Time: 58m 39s	admin
	Sm	art Redun	dancy						
	This U	Inleashed is runnin	g on the st	andby mode with only	limited configuration	n change allowed, please ac	cess the Dedicated Master for full	netowrmk managment	
		General Info	IP Info	Diagnostics					
				System Version:	200.13.6.1.177				
				Unleashed ID:	un2019020000221	657614358463			
				Cluster Status:	Connected Dis	connect			
				MAC:	28:83:71:2F:59:30				
				Model:	R750				
				S/N:	212002008421				
		Ethernet Po	ort Status	0					
		Port		MAC Address	Interface	Physical Link	Speed I	nput pkts	
		Post!		28.52.74.26.60.22	oth0	down	100Mbaa 0	P	

### **Disabling Smart Redundancy**

You can disable Smart Redundancy using the following options:

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

#### Disabling Smart Redundancy from the Primary Dedicated Master

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

1. Clear the Enable Smart Redundancy check box.

#### FIGURE 80 Disabling Smart Redundancy from the Primary Dedicated Master

#### Smart Redundancy

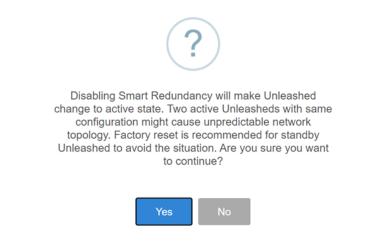
Enable Smart Redundancy to ensure continued operation of your network in the event of a Unleashed failure or power loss. If the active Unleashed loses connection, the standby Unleashed will automatically take over.

Enable Smart Redundancy		Peer Device Info	
Local Device IP Address 192.168.183.126		Uptime	2h 15m
* Peer Device IP Address 192.168.184.127	C.	MAC Address	28:b3:71:2f:59:30
* Shared Secret ruckus		IP Address	192.168.184.127
Peer Status Standby - Connected		ir Address	102.100.104.121
Force Failover Failover		Model	R750
	Apply	S/N	212002008421

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

A confirmation message is displayed.

#### FIGURE 81 Confirmation Message: Disabling Smart Redundancy



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

#### FIGURE 82 Checking Smart Redundancy Status After Disabling

Dedicated Master			Enabled SR Disabled
P Smart Redundancy			
Enable Smart Redundancy to ensure continued operation of your standby Unleashed will automatically take over.	network in the event of	of a Unleashed failure or power loss	s. If the active Unleashed loses connection, the
Enable Smart Redundancy	P	eer Device Info	
Local Device IP Address 192.168.183.126		Uptime	N/A
* Peer Device IP Address 192.168.184.127		MAC Address	N/A
* Shared Secret ruckus		IP Address	N/A
Peer Status N/A			
		Model	N/A
		S/N	N/A

#### **Disabling Smart Redundancy from the Standby Dedicated Master**

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

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

#### FIGURE 83 Disabling Smart Redundancy from the Standby Dedicated Master

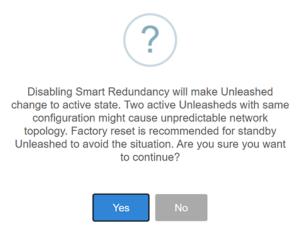
#### Smart Redundancy

General Info	IP Info	Diagnostics					
		System Version:	200.13.6.1.177				
		Unleashed ID:	un2019020000221657614358463				
Cluster Status:			Connected Disconnect				
MAC:			28:83:71:2F:59:30				
		Model:	R750				
		S/N:	212002008421				
Ethernet Po	ort Status	0					
Port		MAC Address	Interface	Physical Link	Speed	Input pkts	
Port1		28:b3:71:2f:59:33	eth0	down	100Mbps	0 B	
Port2		28:b3:71:2f:59:34	eth1	up	100Mbps	41.08 KB	

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

A confirmation message is displayed.

FIGURE 84 Confirmation Message: Disabling Smart Redundancy



3. Click Yes to confirm.

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

# **WLAN Configuration**

•	WLAN Configuration Overview	
•	WLAN Usage Types	189
•	Creating a New WLAN	190
•	802.1X EAP WLANs	193
•	Guest WLANs	196
•	Hotspot WLANs	261
•	Configuring Global WLAN Settings	262
•	Editing an Existing WLAN	
•	Using a QR Code to Join a Wi-Fi Network	264
•	Deleting a WLAN	265
•	Disabling a WLAN Temporarily	266

## **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 196.
- 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 434.

## **Creating a New WLAN**

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

1. In the WiFi Networks component, click Create.

#### FIGURE 85 Creating a New WLAN

((t·	WiFi Networks	Total	1 Working 1 Disabled 0
Cre	eate Edit More -		Data duration: 1 hour
s	ummary - Total 1 WiFi Networks	Summary	
	Clients Traffic	WIFI Networks enabled, 0 WIFI Networks disabled.	
1:	s-wpa	0 Clients	Show Clients Info
1	0 0 0 Clients Traffic	lient Status for last 1 hour 💼 Excellent 💼 Moderate 💼 Poor	
		5-	

The Create WLAN page is displayed.

#### FIGURE 86 New WLAN Settings

* Name:	!20011
Usage Type:	<ul> <li>Standard For most regular wireless network usage</li> </ul>
	O Guest Access Guest access policies and access control will be applied
	O Hotspot Service Known as WISPr
Authentication Method:	Open O 802.1X EAP O MAC Address
Encryption Method:	WPA2 O WPA3 O WPA2/WPA3-Mixed O OWE O None
* Password:	Show password Show QR Code
	$\hfill \ensuremath{\square}$ Allow Legacy Devices to connect to this WLAN by previous password.
	It only works for online Legacy Devices.
Accounting Server:	Disabled V +
	Send Interim-Update every 10 minutes
Show Advanced Options	
	OK Cancel

2. Enter a Name for this wireless network.

- 3. Select the WLAN **Usage Type** from the following options:
  - Standard: Use this WLAN type for most regular wireless network usage.
  - Guest Access: Guest access policies and access controls will be applied. For more information, refer to Guest WLANs on page 196.

#### NOTE

As of Unleashed 200.7, Social Media WLANs are a subset of guest WLANs, and are configured using the guest WLAN settings. Social Media WLANs require a visitor to log in using a social media account before being granted Internet access. For more information, refer to Social Media WLANs on page 240.

- Hotspot Service: Use this WLAN type for a Hotspot (also known as WISPr) WLAN. To deploy a Hotspot WLAN, you must first configure a Hotspot Service. For more information, refer to Hotspot Services on page 434.
- 4. For Authentication Method, select one of the following options:

#### NOTE

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

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

#### NOTE

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

- 5. For **Encryption Method**, select one of the following options:
  - WPA2: Encrypts traffic using the WPA2 standard. The WPA2 encryption method complies with the 802.11i security standard. Announced in 2004, WPA2 encryption remains mandatory for all new products that bear the Wi-Fi trademark.
  - WPA3: You can enable 802.11r FT roaming for open authentication and WPA3 encryption. Announced in January 2018, the WPA3 standard replaces WPA2 with several security enhancements.
  - WPA2/WPA3-Mixed: Allows mixed networks of WPA2- and WPA3-compliant devices. SAE FT and AKM PSK SHA256 is supported for Open authentication + WPA2/WPA3-Mixed encryption. Enable 802.11r FT Roaming is configurable for open authentication and WPA2/WPA3-Mixed encryption and 802.1X EAP authentication + WPA2/WPA3-Mixed encryption under Advanced Options > Radio Control. Refer to Radio Control Settings on page 282 for more information.
  - **OWE**: Opportunistic Wireless Encryption (OWE) provides encrypted communications for open networks.
  - None: No encryption; communications are sent in clear text.

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

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

#### FIGURE 87 Displaying QR Code Page

#### Do you want to print the QR code for this Wi-Fi?

WiFi Name: 1s-wpa Password: 23456789

#### 1. How to use QR code?

You can print and share it to your users, and ask them to open the camera on the smartphone and hold it over the Code. A notification should pop up and connect them to the wireless network automatically. If this does not work, check the smartphone settings and make sure that the QR Code scanning feature is enabled. If it is still not working, then you may need to manually connect to the WiFi

2. How can I regenerate the QR code later?

You can go to WiFi Networks page and select your WiFi, click the "More" button and then click "Show QR Code" from the dropdown list, a QR code page should pop up.

Save Print

x

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

This option is available only for wireless clients that are marked as legacy devices in the **Clients** > **Wireless Clients** page. For more information, refer to "Marking a Client as a Legacy Device". If the **Allow Legacy devices to connect to this WLAN by previous password** check box is selected, under **Advanced Options** > **Zero-IT & DPSK**, **Dynamic PSK** is selected as **Internal**. You can change the password and Unleashed generates DPSK keys for all connected legacy devices with the previous password of the WLAN. For more information about internal DPSK, refer to **Enabling DPSK for a WLAN** on page 271. You can view all the generated DPSK keys in the **Admin & Services** > **Services** > **Dynamic PSK** > **Generated Dynamic PSKs** page.

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

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

#### NOTE

Alternatively, you can create AAA servers on the Admin & Services > Services > AAA Servers page. For more information, refer to AAA Servers on page 408.

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

#### NOTE

For advanced WLAN configuration options, refer to Advanced WLAN Configuration on page 267.

## 802.1X EAP WLANs

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

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

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

### 802.1X WLAN Survivability

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

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

#### NOTE

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

To configure WLAN Survivability for 802.1X WLAN clients:

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

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

FIGURE 88 Enable	802.1X WLAN	survivability
------------------	-------------	---------------

€	Internet			Connected		•
		Create WLAN		×		
	WiFi Networ		EAP Survivability		Disabled 0	T
	Create Edit		Standard for most regular wireless network usage     Guest Access guest access policies and access control will be applied		ation: 1 hour 🔻	
Γ	Summary - Total 1 \	Authentication Method:	O Hotspot Service known as WISPr O Open O 802.1X EAP MAC Address			
	0 0 4	Encryption Method: Authentication Server:				
L	Clients	WLAN Survivability:				
1	Unleashed 0 0 4 Clients	Accounting Server:	Cache time 15 hours Disabled		ow Clients Info 🕨	
		Show Advanced Options	<b>OK</b> Can	cel		
			4		T	Ţ

- 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 log in using an existing social media account to access the wireless network.
- Authentication with shared key: Any client can connect using the same shared password.
- Authentication with unique key (Guest Pass): Guest Pass keys must be generated for each guest, either by an 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**

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

Complete the following steps to deploy a guest WLAN.

1. Go to Wi-Fi Networks > Create.

#### 2. Type a **Name** for the guest WLAN.

	Create WLAN	×		Þ
	* Name:			
		Standard For most regular wireless network usage     Guest Access     Guest access policies and access control will be applied		•
	Onboarding Portal:	O Hotspot Service Known as WISPr Enable Zero-IT device registration from the Guest Portal	Data duration: 1 hour 🗸	
	Guest Authentication:	$\textcircled{\sc 0}$ Guest Pass and Social Login $\bigcirc$ Social Login only $\bigcirc$ None		
	Guest Password:	Unique password for each guest		
Fo		Please go to the following link and log in as guest pass admin to create unique password https://unleashed.ruckuswireless.com/guestpass or https://192.172.10.233/guestpass		
		O Single shared password among all guest	Show Clients Info 🕨	
	Guest Friendly Key:	C Enable The key will include only numbers		
	Grace Period: Allow users to reconnect without re-authentication for 480 r	Allow users to reconnect without re-authentication for 480 minutes	Excellent Moderate Poor	
	Authentication Method:	Open 0802.1X EAP MAC Address		
	Encryption Method:	○ WPA2 ○ WPA3 ○ WPA2/WPA3-Mixed ○ OWE		
	Accounting Server:	Disabled		

#### FIGURE 89 Creating a New Guest WLAN

- 3. For Usage Type, select Guest Access.
- 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 209.
- 5. For Guest Authentication, select Guest Pass and Social Login (allows social media login and Guest Pass), Social Login only (social media login only), or None (no password required).

- 6. For Guest Password, if you selected Guest Pass and Social Login in the previous step, choose one of the following options:
  - Unique password for each guest: Guest Passes must first be generated, in batch or individually, for each visitor before they will be able to log in using a Guest Pass. For more information, refer to Working with Guest Passes on page 214.
  - 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 90 Selecting a Single Shared Password or Unique Password for Each Guest

	Create WLAN	×		►
	* Name: Usage Type:	O Standard For most regular wireless network usage	Total 10 Working 10 Disabled 0	
	Onknowling Postal	Guest Access Guest access policies and access control will be applied     Hotspot Service Known as WISPr     Enable Zero-IT device registration from the Guest Portal	Data duration: 1 hour 🗸	
	Guest Authentication:	Guest Pass and Social Login      Social Login only      None		
2	Guest Password:	Unique password for each guest Please go to the following link and log in as gue t pass admin to create unique password https://unleashed.ruckuswireless.com/guestpass Single shared password among all guest	Show Clients Info 🕨	
		C Enable The key will include only numbers		
		Allow users to reconnect without re-authentication for 480 minutes     Open 802.1X EAP MAC Address	Excellent Moderate Poor	
	Encryption Method: Accounting Server:	O WPA2 O WPA3 O WPA2/WPA3-Mixed O OWE		

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

#### NOTE

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

#### NOTE

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

- 8. For Grace Period, enter a value in minutes to allow users to reconnect without re-authentication. Clear the check box to disable the grace period.
- 9. 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.

- 10. For **Encryption Method**, select one of the following options:
  - WPA2: Encrypts wireless traffic with WPA2 encryption. If this option is selected, users will still be required to enter the WPA2 passphrase to access the open guest WLAN, even with **None** selected as the guest authentication type.
  - WPA3: Announced in January 2018, the WPA3 standard replaces WPA2 with several security enhancements.
  - WPA2/WPA3-Mixed: Allows mixed networks of WPA2- and WPA3-compliant devices.
  - OWE: Opportunistic Wireless Encryption (OWE) provides encrypted communications for open networks.
  - None: Without encryption, anyone can access this WLAN with no passphrase or Guest Pass login required. (Guests may still be required to visit a captive portal landing page, if configured.)
- 11. For Accounting Server, select an accounting server from the list or click the + icon to create a new RADIUS accounting server entry.
- 12. (Optional) Click **Show Advanced Options**, and configure any advanced options, such as restricted subnet access, WLAN priority, access controls, application visibility, and so on. Refer to Advanced WLAN Configuration on page 267 for more information.
- 13. Click Next.

14. Customize the guest WLAN by configuring the following options: social media login options, Guest pass self-service, redirection, terms and conditions, and captive portal appearance.

#### FIGURE 91 Configuring the Guest WLAN

4	🔶 WiFi Netwo	Edit WLAN	×			^
	Create Edit Summary - Total 2 0 0 3	Social Media Logins:	FacebookWiFi Google/Google+ LinkedIn Microsoft WeChat	ura	tion: 1 hour *	
	Clients		Enable guestpass self service     Effective from first use Expire new guest passes if not used within 7 days	iho	w Clients Info ▶	
1	0 0 3 Clients	User Redirection URL:	Effective from the creation time     Redirect to website user intends to visit     Redirect user to this website			
		Terms and Conditions:	Show terms and conditions Edit			
2	web auth wian		Insert WiFi4EU snippet in head tag of Portal page Click on edit area to change each part of captive portal & preview to check the result			

- Social Media Logins: Allow users to log in using their social media accounts. Refer to Social Media WLANs on page 240.
- Guest Pass Self-Service: Allow users to self-authenticate their clients to your guest WLAN using a Guest Pass generated automatically for each guest user. For more information, refer to Guest Pass Self-Service on page 216.
- Validity Period: Click Effective from first use to make the Guest Pass valid on first use or click Effective from the creation time to make the Guest Passes valid from the time they are created. If you select Effective from first time, enter a value for the number of days after which the Guest Passes will expire if not used.
- User Redirection URL: Click Redirect to website user intends to visit to redirect to the website the user intended to visit after successful login or click Redirect user to this website to redirect the user to a specified URL. If you select Redirect user to this website, enter the URL of the website in the field.
- **Terms and Conditions**: Choose whether to display the terms and conditions before guests can access your network. You can also edit the default terms and conditions by clicking **Edit**, and replacing the default text with any text you choose.
- Language: Select the check box to change the language of the Unleashed web user interface.

#### NOTE

The **Language** option is available only when the system language is non-English. By default, the **Language** option is selected. In the Guest portal page, the **English (EN)** toggle switch will be displayed. Toggle the switch to change the language. When the **Language** check box is cleared, the toggle switch will not be displayed in the Guest portal page.

• Insert WiFi4EU Snippet: Insert a WiFi4EU snippet in the head tag of the web authentication portal page. This allows the WLAN to be used by members of the WiFi4EU "digital single market" for EU member states.

#### FIGURE 92 Inserting a WiFi4EU Snippet

	Summary - Total 2	Terms and Conditions: Show terms and conditions Edit	
		Insert WiFi4EU Snippet: @ Insert WiFi4EU snippet in head tag of Portal page	
		Network Identifier test123	
		Portal Language English v	how Clients Info
		Enable self-test modus	
		Customize Captive Portal: Click on edit area to change each part of captive portal & preview to check the result	
1			
2	web auth wlan		
	Clients		25 15:40

- **Customize Captive Portal**: Customize the banner, background image, background color, logo, welcome message, and opacity level. Click **Preview** to preview your changes.
- 15. Click **OK** to save your changes.
- 16. The next screen prompts you to begin the configuration for email and SMS delivery of Guest Passes. Click **Yes** to configure email and SMS settings, or click **No** to skip this step.

You can configure these settings later from the Admin & Services page, if you prefer. Refer to Configuring Email Server Settings on page 202 for more information.

#### FIGURE 93 Configuring Email and SMS Delivery Settings

🔶 WiFi Netwo	orks Traffic: 0.09 MB	Total 2 Normal 2 Disabled
Use Create Create Summary (2 V Clients	Do you want to send an email or SMS of the Guest Pass to your guests?	Yes No
Gue 1 Clients	ast-WLAN-1 2 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	25 17:26 17:27 17:28 17:29 17:30

#### **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 94 Email Server settings

Services		Apply	
Administration	►	Switch Approval  Approval  Automatically approve all join requests from switches.  Apply	
		Email Server	
		From Email Address test@example.com	
		SMTP Server Name smtp.example.com	
		SMTP Server Port 587	
		SMTP Authentication Username username	
		SMTP Authentication Password	
		Confirm SMTP Authentication Password	
		B 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	

#### **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 95 Configuring SMS settings

	SMTP Encrypt	and options	Test Apply
-SMS S	ettings		
✓ En.	able SMS Server		
e (	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	
۲	Twilio account information	n	
	Account SID	[register a new Twilio account]	
	Auth Token		
	From PhoneNumber		
0	Clickatell account informa	ation	
	User Name	[register a new Clickatell account]	
	Password		
	API Id		
	From PhoneNumber		
0	Customized Server		
	Method	GET T	
	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 96 Optionally Configuring a Guest Pass Operator Now

🔶 WiFi Netv		X Disabled
	Do you want to create Guest Pass Operator now?	
Use	Yes No Later	t(s) Info 🕨
Summary (2 V	To create it later these are steps: 1. Go to 'System & Admin -> Roles -> Create New' , select the WLAN(s) and check 'Allow Guest Pass Generation' for seleced WLAN(s).	
Clients	<ol> <li>Go to 'System &amp; Admin -&gt; Users -&gt; Create New', create a new user (for operator) and attach the above role to the user.</li> <li>Guest pass operator can login to https://unleashed.ruckuswireless.com/guestpass or https://192.168.40.20/guestpass using</li> </ol>	
Gu 1	above user credentials.	
Clients	No Traffic 0, 17.60, 17.61, 17.52, 17.61, 17.65, 17.64	17.57 17.59

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 97 Create Guest Pass Operator - Step 1

Guest Pass Operator	Step 1 - Create Role create a role for guest pass operator, essentially assign any other guest WLAN this user can guest pass for.	() () () () () () () () () () () () () (
* Name: Guest Pass Operator Description:	description of the role	
Group Attributes:	this is used by other AAA servers to authenticate the user	
Available WLAN's :	*Selected WLAN's :(0)	cted 0
	◆	cted 0

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 98 Moving WLANs from Available to Selected

	* Name: Gue Description:	t Pass Operator unique name for this role description of the role this is used by other AAA servers to	
	Available WLAN's :	authenticate the user	cted 0
•			cted 0

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 99 Create Guest Pass Operator - Step 2

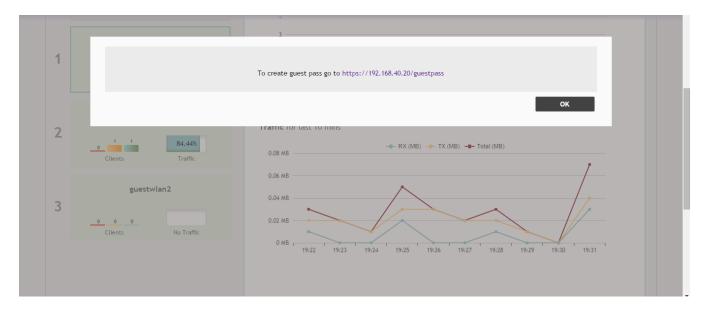
1	Guest Pass Operator	3 Step2-Create User create a role for guest pass operator, essentially assign any other guest whan this user can guest pass for.
2	*User Name: Full Name: *Password	unique name for the user full name for the user
3		Back         Finish         Cancel           19:19         19:20         19:21         19:22         19:24         19:25         19:26         19:27         19:28
		19:19 19:20 19:21 19:22 19:23 19:24 19:25 19:26 19:27 19:28

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

#### NOTE

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

FIGURE 100 Guest pass operator created, to create a guest pass go to URL



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 101 Configuring guest Restricted Subnet Access

	Restr	icted Sul	onet Access	WLAN	Priority Access C	control Radio Control	Others				
	conr conf	nected. If igure up t	there are other	subnets ess rules	on which you want	o which Unleashed and i to block or allow guest us lest access rules are prio	sers, you can cr	eate and	are		
		Order	Description	Туре	Source Address	Destination Address	Application	Protocol	Sc		
		1		Deny	Any	location.host	Any	Any	An		
		2		Deny	Any	10.0.0/8	Any	Any	An		
		3		Deny	Any	172.16.0.0/12	Any	Any	An	09:15	
		4		Deny	Any	192.168.0.0/16	Any	Any	An		
		Create Nev	v Delete 🔳	Advance	d Options						
	4								•		
							Next	Ca	icel	d 3 Disconnec	
Clients			lients							d 3 Disconnec	

#### 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 214.
- 6. Click **Next** to continue to the next guest WLAN configuration page.

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

#### NOTE

For information on these settings, see Deploying a Guest WLAN on page 196.

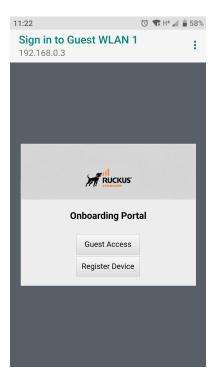
#### FIGURE 102 Enabling Onboarding Portal

Summary - Total 1 W	iFi Networks	Summary	
Clients	Create WLAN	×	
Unleashed		Guest WLAN  Standard for most regular wireless network usage Guest Access guest access policies and access control will be applied	Clients Info 🕨
	Onboarding Portal	Hotspot Service known as WISPr     Enable Zero-IT device registration from the Guest Portal     Guest Pass + Device Registration     Device Registration	
	Guest Authentication:	Guest Pass and Social Login      Social Login only      None	
	Guest Password:	Unique password for each guest     Please go to the following link and log in as guest pass admin to create unique password     https://unleashed.ruckuswireless.com/guestpass & https://192.168.0.2/guestpass     Single shared password among all guest	
	Validity Period	Effective from first use Expire new guest passes if not used within 7 days     Effective from the creation time	09:20
	Grace Period	Allow users to reconnect without re-authentication for 480 minutes	
	Authentication Method:	Open      802.1X EAP      MAC Address	

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:

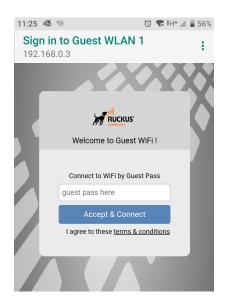
- **Guest Access**: Connect this device to a guest WLAN.
- Register Device: Download a Zero-IT activation file to register this device for access to one or more internal WLANs.

FIGURE 103 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.

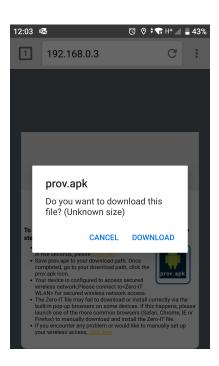
#### FIGURE 104 Guest Access Welcome Page



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

FIGURE 105 Activating the Device Using the WLAN Connection Activation Screen, and Downloading Activation File

11:48	o <u>₹</u>	ଷ ‡⊽⊿	<b>49</b> %
2	<b>b</b> https://192.168.0.3	G	:
L	WLAN Connection Activ	ation	
L	Username		
L	Password Log In		1
			l
12:01	0	• 🗣 H+ ⊿	44%
3	192.168.0.3	G	•
l			
	ecure WLAN Configuratior tup your wireless network connectior		se



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



#### Working with Guest Passes

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

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

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

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

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

#### NOTE

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

#### **Generating a Guest Pass**

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

Complete the following steps to generate a guest pass.

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

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

#### FIGURE 107 Creating a Guest Pass

Create Guest Pass	s <b>X</b>
Number of Guest Passes:	Single     Multiple     (2-100)     By Profile     To download sample profile click here
* Guest Name	
* Guest WLAN:	No guest wlan
* Valid for:	1 Days 🗸
Guest Email:	
Guest Phone:	Phone Number
Advanced <del>▼</del> Enable Session Timeout:	Mins
Enable Shared Pass:	2 guests 🗸
	Generate Cancel

- 3. For **Number of Guest Passes**, select one of the following options:
  - Single: Generate a single guest pass. Refer to Generating and Delivering a Single Guest Pass on page 225.
  - Multiple: Generate multiple guest passes. Refer to Generating and Printing Multiple Guest Passes at Once on page 230.
  - By Profile: Import a guest pass profile. Refer to Creating a Guest Pass Profile on page 232.
- 4. Enter the guest name.
- 5. For **Guest WLAN**, select the WLAN for which the guest pass will be issued. To create a guest WLAN, refer to Deploying a Guest WLAN on page 196.
- 6. In Valid For, enter a number and select a time interval (Hours, Days, or Weeks) for which the guest pass will remain valid.
- (Optional) Enter a guest email address and guest phone number. If these options are entered, and the email server and SMS delivery method have been configured (from Admin & Services > System > System Info), you can deliver the guest pass to the guest using email or SMS.
- 8. (Optional) Under Advanced Options, configure the following options:
  - Enable Session Timeout: Select the check box and select a time interval (Minutes, Hours, Days, or Weeks) after which guests are required to log in again. If Session Timeout is disabled, the connected users are not required to log in again until the guest pass expires.
  - Enable Shared Pass: Allow multiple users to share a single guest pass.
- 9. Click Generate to create the guest pass.

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

#### **Guest Pass Self-Service**

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

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

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

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

#### **Enabling Guest Pass Self-Service**

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

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

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

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

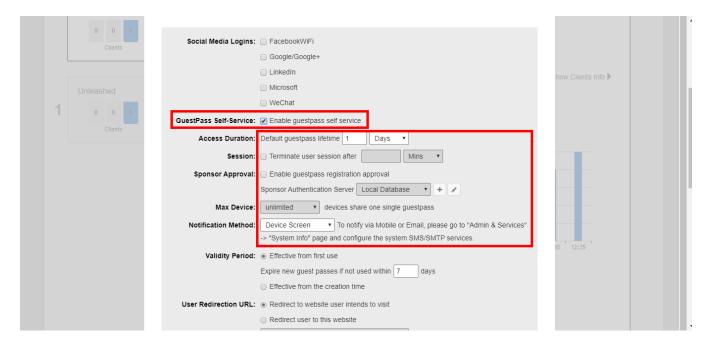


FIGURE 108 Select Enable Guest Pass Self Service

- 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 217.)
  - Notification Method: Select whether the guest pass will be delivered via email, SMS, or displayed directly on the device screen. When Sponsor Approval is selected, the Device Screen option is not allowed.
- 6. Click **OK** to save your changes.

Requiring Sponsor Approval for Self-Service Guest Pass Authentication

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

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

#### NOTE

If using sponsor approval, RUCKUS Unleashed must be configured with your SMTP settings for email delivery, or with a valid Twilio or Clickatell account to deliver guest passes through SMS. Refer to Customizing the Guest Pass Email Content on page 239 and Customizing the Guest Pass SMS Content on page 240 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 109 Enabling Sponsor Approval for Guest Pass Self-Service

	Unleashed		LinkedIn		
1	0 0 5		Microsoft		
			WeChat		
		GuestPass Self-Service:	Enable guestpass self service		
		Access Duration:	Default guestpass lifetime 1 Days		
	Guest WLAN 2	Session:	Terminate user session after     Mins		
2	0 0 0	Sponsor Approval:	Enable guestpass registration approval		
	Clients		Sponsor Authentication Server Local Database 🔻 🗭		
			Default Sponsor Email sponsor@example.com	35 12:40	
		Max Device:	1 • devices share one single guestpass		
		Notification Method:	Mobile   To notify via Mobile or Email, please go to "Admin & Services"		
			-> "System Info" page and configure the system SMS/SMTP services.		
		Validity Period:	<ul> <li>Effective from first use</li> </ul>		
			Expire new guest passes if not used within 7 days		
			<ul> <li>Effective from the creation time</li> </ul>		
		User Redirection URL:	<ul> <li>Redirect to website user intends to visit</li> </ul>		
			<ul> <li>Redirect user to this website</li> </ul>		
		Terms and Conditions:	Show terms and conditions Edit		

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.

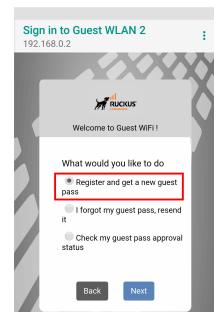
## FIGURE 110 Requesting Help with a Guest Pass

<b>Sign in</b> 192.168	to Guest WLAN 2 .0.2	:
		X
	Welcome to Guest WiFi !	
	Connect to WiFi by Guest Pass guest pass here	
	Connect Help with a guest pass	
	V M	

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

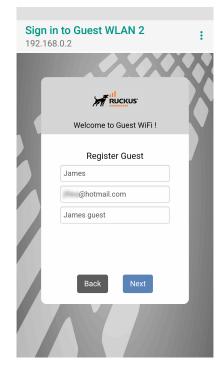
1. On the What would you like to do screen, select Register and get a new guest pass, and click Next.

FIGURE 111 Requesting a New Guest Pass



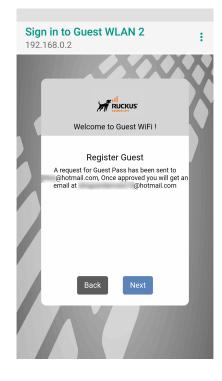
2. Enter a username, an email address or phone number to which the guest pass key will be sent, and the sponsor's email address, and click **Next**.

FIGURE 112 Registering as a Guest



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

### FIGURE 113 Guest Pass Request Submitted Message



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

## FIGURE 114 Sponsor Accept Email

Dear Sponsor/Admin,

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

 https://192.168.0.2/user/sponsor login.jsp?

 email=GKGGGJGMGFHDEAGIGPHEGNGBGJGMCOGDGPGN&user=HDGMGJGOGHHDGBGOGEGBHCHCGPHHHDDBDAEAGIGPHEGNG

 BGJGMCOGDGPGN&ssid=EHHFGFHDHECAFHEMEBEOCADC

 Name:
 @hotmail.com

 Mobile No:

 Email:
 @hotmail.com

 SSID: Guest WLAN 2

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

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

## NOTE

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

FIGURE 115 Sponsor/Approver Login Page

RUCKUS.	
Sponsor /Approver Authentication	
Log in	

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

## FIGURE 116 Guest Pass Approval

			GuestPass Approval			
		Gu	est access registration pending appr	oval:		
-	UserName	Mobile	Email	Wlan	Request-time	Duration
•	@hotmail.com	n	@hotmail.com	Guest WLAN 2	2018/12/17 13:40	1 da
	Approve			F	Reject	

FIGURE 117 Guest Pass Approved Message



 $\frown$ 

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

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

#### FIGURE 118 Guest Pass Activation Email Message

Greetings, @hotmail.com You have been granted access to the company wireless network Your guest pass key is DMBXV-PHIQM This guest pass is valid antil 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:

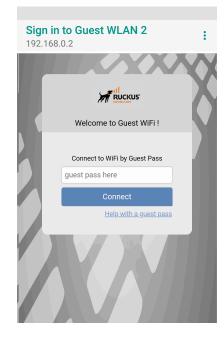
Finding the Wireless "Guest" Network

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

#### FIGURE 119 Entering Guest Pass Code



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

## **Controlling Guest Pass Generation Privileges**

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

In order to change the guest pass generation privileges for a group of users, refer to Configuring User Roles on page 390.

For more information on creating a Guest Pass Operator role, refer to Creating a Guest Pass Operator on page 205.

#### **Generating and Delivering a Single Guest Pass**

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

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

#### NOTE

For instructions on how to generate multiple guest passes, refer to Generating and Printing Multiple Guest Passes at Once on page 230.

#### NOTE

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

Complete the following steps to generate a single guest pass.

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

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

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

## NOTE

The user generating the guest pass must have guest pass generation privileges, as described in Controlling Guest Pass Generation Privileges on page 225.

## FIGURE 120 Requesting a Guest Pass

Request a Guest Pass	
Username Password	
Log In	

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

- 3. On the **Guest Information** page, fill in the following options:
  - **Creation Type**: Click **Single** to generate a single guest pass. To generate multiple guest passes in batch, refer to Generating and Printing Multiple Guest Passes at Once on page 230.
  - Full Name: Enter the name of the guest user for whom you are generating the guest pass.
  - Valid for: Enter a number in the Valid for field and select a time unit (Hours, Days, or Weeks) to specify the time period when the guest pass will be valid.
  - WLAN: Select the WLAN for this guest (typically, a guest WLAN).
  - Email: (Optional) Enter the email address for this user.
  - Phone Number: (Optional) Enter a phone number for this user.
  - Key: Leave as is if you want to use the random key that RUCKUS Unleashed generates. If you want to use a key that is easy to remember, delete the random key, and enter a custom key. For example, if RUCKUS Unleashed generated the random key OVEGS-RZKKF, you can change it to "joe-guest-key". Customized keys must be from 1 through 16 ASCII characters in length.

#### NOTE

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

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

#### FIGURE 121 Creating a Single Guest Pass

	Guest Information
Key Remarkc (Max length is 64 Sharable	I     Days       Guest WLAN 1       +001-4001234567       RHW/RC-RBZSF       I       •       1       •
	Next > or Show existing guest castes

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

## FIGURE 122 Guest Pass Generated Page

RUG	CKUS	
Guest Pass G	enerated	
Here is the generated guest pass for <b>Bob Marley</b>	RHWRC-RBZSF	
This guest pass is valid for 1 days once be activated before 12/25/2018, 9:58 Email SMS C Defaul		
Create another		

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

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

# FIGURE 123 Sending Guest Pass Key through Email Entered on the Guest Information Screen

RUCKUS.	
Guest Pass Generated	
Here is the generated guest pass for Bob Marley	
 This guest pass is valid for 1 days once activated, and has to be activated before 12/25/2018, 9:58:09 AM.	
Email SMS C Default Print Instructions sending email to boo@example.com Create another Guest Pass	

#### FIGURE 124 Sample Guest Pass Printout

	nnecting as a Guest the Corporate Wireless Network
	ings, Bob Marley
	angs, but marries
	quest pass key is RHWRC-RBZSF
	suest pass is valid for 1 days once activated, and has to be activated before 12/25/2018, 9:58:09 AM
Conne	ect your wireless-ready PC to this network: Guest WLAN 1, as detailed in the instructions printed below.
Befor	e you start, please review the following requirements.
	uirements • A wireless-network-ready computer • The corporate "guest" network name • The guest pass (a text "key")
Con Using	necting 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.
Find	ling 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.
з	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.
	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.
Log	aina 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.
з	When the Unleashed WebUI "Guest Pass" page appears, enter the text of your guest pass key (by typing or pasting) and click Login.
	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.
Imn	nortant

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 230.

#### Generating and Printing Multiple Guest Passes at Once

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

#### NOTE

For instructions on how to generate a single guest pass, refer to Generating and Delivering a Single Guest Pass on page 225.

#### NOTE

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

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

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

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

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

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

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

#### NOTE

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

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

#### FIGURE 125 Generating Multiple Guest Passes

Creation Type       Single Multiple         Valid for * <ul> <li>Days</li> <li>WLAN *</li> <li>Guest WLAN 1 *</li> <li>Number</li> <li>or specified by profile below</li> <li>Profile (*.csv)</li> <li>Choces File No file chosen</li> <li>To download sample profile, elcichares</li> <li>Sharable</li> <li> <ul> <li>I *</li> <li>Quest share a single guest pass</li> <li>Session</li> <li>Terminate user session after</li> <li>Mins *</li> <li>Next &gt;</li> <li>or Show ensiting quest passes</li> </ul></li></ul>		
Creation Type Valid for * Days • WLAN * Guest WLAN 1 • Number 5 or specified by profile below Profile (*.csv) Choose File No file chosen To download sample profile, click here Sharable 1 • guests share a single guest pass Session Terminate user session after Mins •		
Valid for * 1 Days • WLAN Guest WLAN 1 • Number 5 or specified by profile below Profile (*.csv) Choose File No file chosen To download sample profile, click here Sharable 1 • guests there a single guest pass Session Terminate user session after Mins •		Guest Information
Next > or Show existing quest calles	Valid WL Nur Profile (* Shat	t for * 1 Days • LAN * Guest WLAN 1 • * Source File No file chosen To download sample profile, <u>clickhere</u> trable 1 • guests share a single guest pass

#### NOTE

If you want to be able to identify the guest pass users by their names (for example, for monitoring or auditing purposes in a hotel setting), click **Choose File**, and upload a guest pass profile instead. Refer to Creating a Guest Pass Profile on page 232 for more information.

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

FIGURE 126 Multiple Guest Passes Generated

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

A new browser page appears and displays the guest pass instructions and the **Print** dialog box is displayed.

7. Select the printer that you want to use and click **Print** to print the guest pass instructions.

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

#### **Creating a Guest Pass Profile**

Complete the following steps to create a Guest Pass profile.

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

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

## FIGURE 127 Downloading a Sample Profile

Guest Information
Creation Type O Single Multiple
Valid for * 1 Days V
WLAN Guest WLAN 1 T
Number 5 or specified by profile below
Profile (*.csv) Choose File No file chosen To download sample profit click here
Sharable 1 guests share a single guest pass
Session Terminate user session after Mins 🔻
Next > or <u>Show existing guest passes</u>

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

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

#### FIGURE 128 Editing the CSV File in a Spreadsheet Application

	Α	В	С	D	E	F	G
1	#Guest Name (Must)	Remarks	Key (Empty implies random key)	Email Address	Phone Number		
2	Batch-Guest-1	Batch generation	ΑΑΑΑΑΑΑ	someone@example.com	14081234567		
3	Batch-Guest-2	Batch generation	AAAAAAB	someone1@example.com			
4	Batch-Guest-3	<b>Batch generation</b>		someone2@example.com			
5	Batch-Guest-4	Batch generation		someone3@example.com			
6	Batch-Guest-5	<b>Batch generation</b>		someone4@example.com			
7							
8							
9							
10							
11							
12							
13							
14							
15							
16							
17							
18							
19							
20							
21							
22							
	<ul> <li>→ batch_g</li> </ul>	uestpass_sample	÷				•

6. Return to the **Guest Information** page, and complete step 3 through step 7 in Generating and Printing Multiple Guest Passes at Once on page 230 to upload the guest pass profile and generate multiple guest passes.

FIGURE 129 Importing Batch Generation CSV File	FIGURE	129 lm	porting	Batch	Generation	CSV	File
--	--------	--------	---------	-------	------------	-----	------

Guest Information reation Type Single Muttiple Valid for 1 Days V WLAN Guest WLAN 1 V Number Single Specifies by profile below troffile ('.csv) Choose File of file chosen O starable 1 V guests share a single guest pass
Session Terminate user session after Mins T Next > or Show existing quest bases

## **Monitoring Generated Guest Passes**

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

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

## FIGURE 130 Viewing generated Guest Passes

<u>⊇</u> System	Gues	t Pass Generatio	on Gue	est Pass Print	out Customization	Email	SMS			
Convision										
Services	G	est Pass Generat	ion							
AA Servers	Au	thenticated users	can gene	erate guest pa	asses at the URL sho	own belov	W.			
ccess Control	G	iest Pass Genera	ation UR	L https://192	.168.0.2/guestpass					
oplication Recognition & Control		Authenticatio	on Serve	er Local Dat	abase	•				
										Apply
Bonjour Gateway										
	- 0.0	min Concrated C	neet Daei							
mamic PSK		min Generated G			es. Vou can review t	he quest	nasses generate	d for your up	ars. You may also remo	ve them if
vnamic PSK uest Access Service	Th				es. You can review t	he guest	passes generated	d for your use	ers. You may also remo	ve them if
	Th	ese tables list the cessary.	generate	ed guest pass		he guest				
uest Access Service	Th	ese tables list the	generate		es. You can review t Email	he guest	passes generated Phone Number			ve them if Expires
lest Access Service htspot Services Idio Control	Th	ese tables list the cessary.	generate	Key						Expires
uest Access Service htspot Services adio Control		ese tables list the cessary. Guest Name Bob Marley	generate Role Default	Key RHWRC- RBZSF	Email		Phone Number +001-		Create Time 2018/12/18 09:58:09	Expires 2018/12/25
uest Access Service		ese tables list the cessary. Guest Name Bob Marley	generate Role	Key RHWRC- RBZSF	Email		Phone Number +001- 4081234567	Remarks	Create Time	Expires 2018/12/25

## **Creating a Custom Guest Pass Printout**

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

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

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

To create a custom guest pass printout:

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

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

## FIGURE 131 Guest Pass Printout Customization

Clients	No Clients				Total 0	Connected 0	Blocked	►
Access Points					Total 2	Working 2	Disconnected	►
Admin & Services								▼
System	Edit this field to	out Customization	tout Customization Email SMS and of email notifications to guests. The message body may have up annolo_ctick have	to 8,000 characters.The variables (GUEST NAME), (GUEST	PASS), (EXPIRED TI	ME) and (WLAN NAM	AE) must be part of	_
Application Recognition & Control		Name	Description	Actions				
Bonjour Gateway	•	Default	Guest Pass Printout in English	Edit Clone Prev				
DHCP Server		French	Guest Pass Printout in French	Edit Clone Prev	iew			
Dynamic PSK	Create New					Del	ete 🛛 1-2 (2) 🔾	
Guest Access Service	Search terms		Include all terms Include any of these terms					
Hotspot Services								
Radio Control								
WIPS								
111-3								
🌣 Administer 🕨 🕨								

- 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 <u>Guest Pass Printout Tokens</u> on page 238.

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

	Guest Access Service Guest Pass Generation Guest Pass Printout Customization Email SMS
🗿 Serv	
AAA Server	Create New
Access Con	Name*
Application	Description
Bonjour Ga	Instruction Printout Import an HTML file for Instruction Printout
DHCP Serve	Choose File No file chosen
Dynamic PS	
Guest Access	Delete @1-2 (2) @
Hotspot Servic	Search terms
notspot servic	

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

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

#### **Guest Pass Printout Tokens**

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

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

#### TABLE 29 Tokens that you can use in the guest pass printout (continued)

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

#### **Customizing the Guest Pass Email Content**

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

#### NOTE

To allow Unleashed to deliver guest passes via email, you must first configure an email account (and its SMTP settings) from which Unleashed will send the emails. For information on configuring the email server, see Configuring Email Server Settings on page 202.

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 133 Customize guest pass email content

Admin & Servi	Ces
🛄 System	
	Guest Pass Generation         Guest Pass Printout Customization         Email         SMS
Services	Customize The Email Content
AAA Servers	You can customize individual email content. The maximum allowable size is 8KB. There must leave in four pairs parentheses and
	cannot be nested. The value of variables in the parenthese cannot be changed. To download a sample, click here
Access Control	
Application Recognition & Control	Greetings, (GUEST NAME)
Bonjour Gateway	You have been granted access to the company wireless network
	Your guest pass key is: (GUEST PASS)
Dynamic PSK	This guest pass is valid until (EXPIRED TIME)
Guest Access Service	Connect your wireless-ready device to this network: (WLAN NAME), as detailed in the instructions printed below.
Hotspot Services	Please follow the instruction below:
Radio Control	Finding the Wireless "Guest" Network
	1 Find "Guest" SSID on device.
WIPS	2 Select the "Guest" SSID and and click Connect.

#### **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 202.

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 134 Customize guest pass SMS content

	ervices						
🛄 System							
Services	•	Guest Pass Generation	Guest Pass Printout Customization	Email	SMS		
AAA Servers		You can customize	individual sms content. The maximum	allowable	size is '	160B. There must leave in three pairs parentheses and	
Access Control		cannot be nested. The 'WLAN NAME' in the first parenthese, the 'GUEST PASS' in the second parenthese and the the third parenthese. To download a sample, click here					
Application Recognition & Contro	A	the third parentness	e. To download a sample, click here				
Bonjour Gateway		SSID: (WLAN NAI Passcode: (GUES					
Dynamic PSK		Expires on (EXPIR					
Guest Access Service							
Hotspot Services							
Radio Control							

## 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 242
- Google/Google+ on page 242
- LinkedIn on page 252
- Microsoft Live on page 256

### • WeChat on page 260

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 135 Creating a Social Media WLAN

					· · · · · · · · · · · · · · · · · · ·
	Summary - Total 1 V		social-media         Standard for most regular wireless network usage         Guest Access guest access policies and access control will be applied         Hotspot Service known as WISPr		
		Onboarding Portal	Enable Zero-IT device registration from the Guest Portal		
		Guest Authentication:	Guest Pass and Social Login Social Login only None	Client(s) Info ▶	
1	0 0 1 Clients	Guest Password:	Unique password for each guest     Please go to the following link and log in as guest pass admin to create unique password     https://unleashed.ruckuswireless.com/guestpass & https://192.168.0.4/guestpass		
			<ul> <li>Single shared password among all guest</li> </ul>		
		Validity Period	Effective from first use     Expire new guest passes if not used within 7 days     Effective from the creation time		
		Grace Period	✓ Allow users to reconnect without re-authentication for 480 minutes		
		Authentication Method:	Open      802.1X EAP      MAC Address		
		Encryption Method: Accounting Server	<ul> <li>○ WPA2 ● None</li> <li>□Disabled ▼ +</li> <li>Send Interim-Update every 10 minutes</li> </ul>	13:35	

WLAN Configuration Guest WLANs

#### FIGURE 136 Select social media logins

	🛜 WiFi Networ			Disabled 0
	Create Edit	Create WLAN	×	ation: 1 hour V
	Create	Social Media Logins:	🗌 FacebookWiFi	
	Summary - Total 1 \		Google/Google+	
			Linkedin     Microsoft	
	Clients		WeChat	
		GuestPass Self-Service:	Enable guestpass self service	ow Clients Info 🕨
		Validity Period:	Effective from first use	
1			Expire new guest passes if not used within 7 days  Effective from the creation time	
		User Redirection URL:	Redirect to website user intends to visit	
			Redirect user to this website	
		Terms and Conditions:	Show terms and conditions Edit	
		Insert WiFi4EU Snippet:	Insert WiFi4EU snippet in head tag of Portal page	
		Customize Captive Portal:	Click on edit area to change each part of captive portal & preview to check the result	

## Facebook Wi-Fi

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

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

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

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

#### Google/Google+

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

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

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

#### Select Enable HTTPS or Enable HTTP.

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

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

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

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

## FIGURE 137 Logging in Using Google ID

Create WLAN	×
Social Media Logins: 🗌 FacebookWiFi	
✓ Google/Google+	
Use my own client ID	
Input existing client ID/password or click here to generate one	
Enable HTTPS      C Enable HTTP	
* Google Client ID: Client ID	
* Client Password: Password .	
Only allow users from following hosted domains	
□ Microsoft	
□ WeChat	

#### OAuth Setup Procedure for Google+ Social Media Login

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

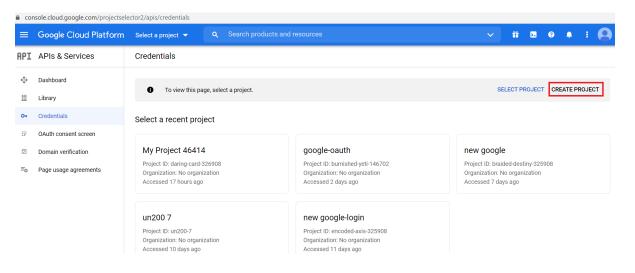
Complete the following steps to create a project ID in the Google Developers Console.

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

#### NOTE

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

#### FIGURE 138 Creating a New Project on the Google OAuth Console



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

## FIGURE 139 Entering the Project Name

≡ Goo	ogle Cloud Platform	٩	Search products and resources	
New Pro	ject			
	You have 19 projects remaining in your quo delete projects. <u>Learn more</u> MANAGE QUOTAS	ta. Requ	lest an increase or	
Project nar unleased-1 Project ID:		IT	0	
Locatio	on * Janization		BROWSE	
CREATE	CANCEL			

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

FIGURE 140 Configuring OAuth Consent Screen

≡	Google Cloud Platform	unleased-test < Q Search products and resources			
API	APIs & Services	OAuth consent screen			
<>	Dashboard	Choose how you want to configure and register your app, including your			
Ш	Library	target users. You can only associate one app with your project.			
0-	Credentials	User Type			
92	OAuth consent screen	🔿 Internal 🕜			
~	Domain verification	Only available to users within your organization. You will not need to submit your app for verification. Learn more about user type			
≡¢	Page usage agreements	● External ②			
		Available to any test user with a Google Account. Your app will start in testing mode and will only be available to users you add to the list of test users. Once your app is ready to push to production, you may need to verify your app. Learn more about user type			
		CREATE			
		Let us know what you think about our OAuth experience			

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

## FIGURE 141 Entering App Information

API	APIs & Services	Edit app registration
¢.	Dashboard	1 OAuth consent screen — 2 Scopes — 3 Test users — 4
ш	Library	
0-	Credentials	App information
92	OAuth consent screen	This shows in the consent screen, and helps end users know who you are and contact you
	Domain verification	App name *
≡¢	Page usage agreements	oauth-test
		The name of the app asking for consent
		User support email * vicky.f.zhang@gmail.com
		For users to contact you with questions about their consent
		App logo BROWSE
		Upload an image, not larger than 1MB on the consent screen that will help users recognize your app. Allowed image formats are JPG, PNG, and BMP. Logos should be square and 120px by 120px for the best results.

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

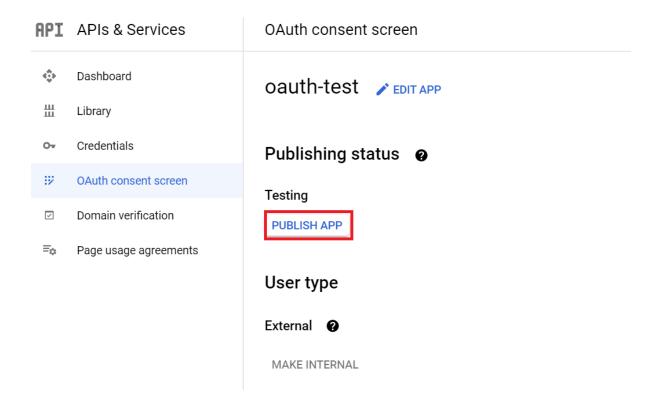
## FIGURE 142 Entering Developer Contact Information

0-	Credentials	Provide users a link to your home page
92	OAuth consent screen	Application privacy policy link
7	Domain verification	Provide users a link to your public privacy policy
≡¢	Page usage agreements	Application terms of service link
		Provide users a link to your public terms of service
		Authorized domains (2) When a domain is used on the consent screen or in an OAuth client's configuration, it must be pre-registered here. If your app needs to go through verification, please go to the <u>Google Search</u> <u>Console</u> to check if your domains are authorized. <u>Learn more</u> about the authorized domain limit.
		Developer contact information
<۱		Email addresses * someone@test.com  These email addresses are for Google to notify you about any changes to your project.

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

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

## FIGURE 143 Publishing the App



In the Push to production dialog box, click Confirm.

# Push to production?

Your app will be available to any user with a Google Account.

You do not need to submit your app for verification. If you change your app's configuration in the future, like adding more than 10 domains, uploading a logo, or requesting sensitive or restricted scopes, you will need to <u>submit for</u> verification.

CANCEL	CONFIRM

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

FIGURE 144 Changing the Publishing Status

<>	Dashboard	oauth-test 🧪 EDIT APP
ш	Library	
0-	Credentials	Verification Status
92	OAuth consent screen	Verification not required
$\checkmark$	Domain verification	Your consent screen is being shown, but your app has not been reviewed so your users may not see all of your information, and you will not be able to
≡¢	Page usage agreements	request certain OAuth scopes. Learn more
		Publishing status  In production BACK TO TESTING User type
		External 😧

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

FIGURE 145 Creating Credentials: OAuth Client ID

API	APIs & Services	Credentials	+ CREATE CREDENTIALS			
< <b>\$</b> }	Dashboard	Create credentials to ac	API key Identifies your project using a simple API key to check quota and access			
岀	Library	A Remember t	OAuth Client ID Requests user consent so your app can access the user's data		CONFIGURE CO	NSENT SCREEN
0+	Credentials		Service account			
92	OAuth consent screen	API Keys	Enables server-to-server, app-level authentication using robot accounts			
7	Domain verification	Name	Help me choose	rictions	Key	Actions
≡o	Page usage agreements	No API keys to displa	Asks a few questions to help you decide which type of credential to use			
		OAuth 2.0 Client II	Ds			
		Name	Creation date 🔸	Туре	Client ID	Actions
		No OAuth clients to di	splay			
		Service Accounts			Manag	e service accounts
		Email	Name 🕇			Actions
		No service accounts to	o display			

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

#### NOTE

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

## FIGURE 146 Selecting Web Application and Entering Authorized Redirect URI

API	APIs & Services	← Create OAuth client ID
<. *	Dashboard	A client ID is used to identify a single app to Google's OAuth servers. If your app runs o
Ш	Library	multiple platforms, each will need its own client ID. See <u>Setting up OAuth 2.0</u> for more information. <u>Learn more</u> about OAuth client types.
0+	Credentials	Application type * Web application
:2	OAuth consent screen	
$\checkmark$	Domain verification	Name * Web client 1
≡¢	Page usage agreements	The name of your OAuth 2.0 client. This name is only used to identify the client in the console and will not be shown to end users.
		The domains of the URIs you add below will be automatically added to your OAuth consent screen as authorized domains.
		Authorized JavaScript origins  For use with requests from a browser
		Authorized redirect URIs @
		For use with requests from a web server
		URIs *
		https://unleashed.ruckuswireless.com/user/auth.jsp
		+ ADD URI

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

FIGURE 147 OAuth Client ID and Client Secret

# OAuth client created

The client ID and secret can always be accessed from Credentials in APIs & Services



OAuth is limited to 100 <u>sensitive scope logins</u> until the <u>OAuth</u> <u>consent screen</u> is verified. This may require a verification process that can take several days.

Your Client ID 195963350142-14s5og8ifeo5epbtpj57mpoma7ictq8p.apps.gc

Your Client Secret yi-4t2rRHiJLUCbh466\_S-F9

ΟΚ

Ē

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

## LinkedIn

To configure a LinkedIn social media WLAN, you must first configure an application on the LinkedIn developer apps website. Refer to the following URL for the LinkedIn developer network: https://www.linkedin.com/developer/apps for more information.

### OAuth Setup Procedure for LinkedIn Social Media Login

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

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

### FIGURE 148 LinkedIn My Applications

linkedin.com/developers/apps	0-7
in DEVELOPERS Products Docs and tools ▼ Resources ▼ My apps ▼	<b>P</b>   <b>D</b>
My apps	Create app
Zd&unleashed-test         Client ID: 86/8aah01m29/0         Created: Aug 16, 2021         Ruckus Networks         Not verified	□ Leave Feedback
About Help Center Privacy And Terms 🗸 Developer Legal 🛩 Linked in Linked in Corporation © 2021	

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

### FIGURE 149 Creating a New LinkedIn Application

Create an app	
App name *	
unleashed-oauth test1	
inkedIn Page*	
${\mathbb D}$ This action can't be undone once the app is saved.	
Ruckus Networks	
Information Technology & Services; 501-1000 employees	
The LinkedIn Page you select will be associated with your app. Verification can be done by a Page Admin. Learn more	
Privacy policy URL	
Begin with http:// or https://	
COMMEXANT RUCKUS' Upload a logo quare image recommended. At least one dimension should be at least 100p.c.	
egal agreement Vhen you develop on our platform, you are agreeing to be bound by our API Terms of Use.	
✓ I have read and agree to these terms	
	Cancel Create ap

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

FIGURE 150 LinkedIn Authentication Keys

RUCKUS'		Dauth test1 71199pyy   Created	d: Aug 26, 2021	
Settings	Auth	Products	Analytics	Team members
Applicat	tion crede	ntials		
	ication ke	ys		
Client ID: 862vsu7	71199руу			
Client Se	cret:			
ha9UO\	/gaYtwWPZ	3ј 🖌	3	

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

### NOTE

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

### FIGURE 151 Entering the Authorized Redirect URI

OAuth 2.0 settings	
Token time to live duration Access token: <b>2 months</b> (5184000 seconds)	
Authorized redirect URLs for your app	
http://unleashed.ruckuswireless.com/user/auth.jsp + Add redirect URL	
	Cancel Update

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

FIGURE 152 Sharing and Signing with LinkedIn

RUCKUS'	eashed-oauth test1 ht ID: 862vsu7ll99pyy Creat	ed: Aug 26, 2021		
Settings	Auth Products	Analytics	Team members	
<b>Products</b> Additional a	vailable products			
١	Marketing Develop Build marketing exper View docs 🗗 📔 View o		the right audiences	Select
	Share on LinkedIn Amplify your content I View docs 🖸 📔 View e	oy sharing it on l	LinkedIn	Select
0=	Sign In with Linked Let users easily sign in		ssional identity	Select

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

### FIGURE 153 Checking the Permissions Added for Linkedin Login

#### OAuth 2.0 scopes

- Scopes define what your app can do on a user's behalf.
- The OAuth consent screen will display descriptions to end users as they are seen below. Some variation may occur if your app has a custom OAuth experience.

r emailaddress
-
Use the primary email address associated with your LinkedIn account
ose the printing entail dealess associated with your Entream account
r_liteprofile
•
Use your name and photo
w member social
w_member_social
Create, modify, and delete posts, comments, and reactions on your behalf
create, modify, and delete posts, comments, and reactions on your behalf

### **Microsoft Live**

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

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

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

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

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

### 2. Click New Registration.

### FIGURE 154 Create a new app registration

Microsoft Azure	arphi Search resources, services, an	nd docs (G+/)	. Q	Q 🗇	? 🙂	сом	мѕсор
ome > App registrations							
op registrations							х
New registration 🌐 Endpoints 🤌 Troubleshooting	♡ Got feedback?						
Welcome to the new and improved App registrations (now Gener	rally Available). See what's new $ ightarrow$						
Still want to use App registrations (Legacy)? Go back and tel							
<sup>5</sup> Start typing a name or Application ID to filter these results							
Start typing a name or Application ID to filter these results isplay name		Application (client) ID			eated On	Certificates & secrets	
<ul> <li><sup>2</sup> Start typing a name or Application ID to filter these results</li> <li><b>Isplay name</b></li> <li>JaïTheBot</li> </ul>		013037d2-c9de-4f6f-916a-016349528		7/	17/2019	🕑 Current	
O Start typing a name or Application ID to filter these results       Display name       JaiTheBot       SalesforceChatBot				7/			
<sup>2</sup> Start typing a name or Application ID to filter these results <b>isplay name</b> JaiTheBot		013037d2-c9de-4f6f-916a-016349528	)e8	7/	17/2019	🕑 Current	
<ul> <li><sup>2</sup> Start typing a name or Application ID to filter these results</li> <li>isplay name</li> <li>JaiThe8ot</li> <li>SalesforceChatBot</li> </ul>		013037d2-c9de-4f6f-916a-016349528 0eaa2afc-cc97-4006-838f-757e8965b0	)e8 307d	7/ 2/4 4/	17/2019 8/2018	<ul> <li>Current</li> <li>Current</li> </ul>	
<sup>O</sup> Start typing a name or Application ID to filter these results <b>Display name</b> M JaiTheBot SA SalesforceChatBot AB Azure Bridge		013037d2-c9de-4f6f-916a-016349528 Oeaa2afc-cc97-4006-838f-757e8965b0 3474f3da-b195-448d-a469-dc729e473	0e8 307d ia2c	7/* 2/4 4/* 8/5	17/2019 8/2018 19/2019	<ul> <li>Current</li> <li>Current</li> <li>Current</li> </ul>	
Start typing a name or Application ID to filter these results       Display name       M       JaiTheBot       SA       SalesforceChatBot       A       HO       HotelBot		013037d2-c9de-4f6f-916a-016349528 Oeaa2afc-cc97-4006-838f-757e8965b0 3474f3da-b195-448d-a469-dc729e473 f5151b87-a998-41d5-8939-76fb66035	0e8 307d ia2c 214	7/ 2/4 4/ 8/3 1/	17/2019 8/2018 19/2019 80/2017	<ul> <li>Current</li> <li>Current</li> <li>Current</li> <li>Current</li> </ul>	

- 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 155).

- 5. In **Redirect URI:**, provide a valid redirect callback URL, for example:
  - HTTPS://unleashed.ruckuswireless.com/user/auth.jsp (see Figure 155).

### 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 155 Register an Application configuration settings

	Microsoft Azure	➢ Search resources, services, and docs (G+/)	Ð	Q		$\odot$	jay.files@commscope.c соммясоре
Hon	ne > App registrations > Register an application						
Re	gister an application						×
Sup	pported account types						•
Who	o can use this application or access this API?						
0	Accounts in this organizational directory only (CommScope only - Single t	enant)					
0	Accounts in any organizational directory (Any Azure AD directory - Multite	nant)					
۲	Accounts in any organizational directory (Any Azure AD directory - Multite	nant) and personal Microsoft accounts (e.g. Skype, Xbox)					
Help	o me choose						
Red	lirect URI (optional)						
	Il return the authentication response to this URI after successfully authentic qed later, but a value is required for most authentication scenarios.	ating the user. Providing this now is optional and it can be					
_							
W	eb	n/user/auth.jsp 🗸					
							*
By p	roceeding, you agree to the Microsoft Platform Policies 🖄						
	Register						

### 6. Click **Register**.

Þ

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 156 Take note of Application (Client) ID

	,P Search resources, services, and docs (G+,)	🚬 💀 🖓 🎯 ? 🙄 соммиссом	.0
Home > App registrations > OAuth 2.0			
OAuth 2.0		×	? ×
,O Search (Ctrl+/) «	Delete     Endpoints		
R Overview	Got a second? We would love your feedback on Microsoft identity platform (previou	sly Azure AD for developer). $ ightarrow$	
Quickstart	Display name : OAuth 2.0	Supported account types : My organization only	- î
	Application (client) ID: 05bf2dd7-3cd0-4f5f-8434-c1876fa4a898	Redirect URIs : 1 web, 0 public client	- 1
Manage	Directory (tenant) ID : 31472f81-8fe4-49ec-8bc3-fa1c295640d7	Application ID URI : Add an Application ID URI	- 1
📰 Branding	Object ID : dd617cca-b61a-47c6-87a2-7e54cfc2af0b	Managed application in : OAuth 2.0	- 1
Authentication		8	_
Ŷ Certificates & secrets	Welcome to the new and improved App registrations. Looking to learn how it's chan	nged from App registrations (Legacy)? Learn more	
API permissions	C.II.ADI	Description of the second s	
Expose an API	Call APIs	Documentation	- 1
Cowners		Microsoft identity platform Authentication scenarios	- 1
Roles and administrators (Previ		Authentication libraries	
	🗵 💿 🐅 🥨	Code samples Microsoft Graph	
🛄 Manifest		Glossary Help and Support	
Support + Troubleshooting	Build more powerful apps with rich user and business data from Microsoft services and your own company's data	nely and support	
Troubleshooting	sources.		
New support request	View API permissions		-

- 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 157 Take note of Client Secret

Client secrets

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

+ New client secret			
Description	Expires	Value	Copy to clipboard
secret1	8/18/2021	4j5w_LW-NC.7KTM612ch.e2.zo4Yfp-2bo	0

- 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 156.
  - Client Password: The client secret described in Figure 157.

FIGURE 158 Create WLAN configuration screen - Microsoft Social Media Login

Create WLAN		
Social Media Logins:	☐ FacebookWiFi	
	Google/Google+	
	🗌 LinkedIn	
	✓ Microsoft	
	Input existing client ID/passv	vord or click here to generate one
	● Enable HTTPS ○ Enabl	e HTTP
	* Microsoft Client ID:	Client ID
	* Client Password:	Password
	□ WeChat	
GuestPass Self-Service:	Enable guestpass self service	
Validity Period:	<ul> <li>Effective from first use</li> </ul>	
	Expire new guest passes if not us	sed within 7 days
	$\bigcirc$ Effective from the creation tim	e

### WeChat

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

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

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

#### Connecting to a WeChat WLAN

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

To connect to a WeChat WLAN:

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

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

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

### **Guest Access Walled Garden**

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

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

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

### FIGURE 159 Enter domain name or IP addresses to allow access to unauthenticated users

Grace Period	: Allow users to reconnect without	out re-authentication for 480 m	ninutes		•
Authentication Method	:      Open      802.1X EAP      MA	C Address			
Encryption Method	: OWPA2 OWPA3 OWPA2/W	PA3-Mixed 🔘 OWE 💿 None			
Accounting Server	r: Disabled •	+			
	Send Interim-Update every 10	minutes			
ide Advanced Options 🔻					
Restricted Subnet Access	WLAN Priority Access Control	Radio Control Walled Garder	n Others		
Unauthenticated users are	allowed to access the following dest	tinations:			
.g. *.mydomain.com,mydon	nain.com, *.mydomain.*,192.168.1.1:80	), 192.168.1.1/24 or 192.168.1.1:80/2	24)		
Order	Destination Address	Action			
1 🔻	*.mydomain.com	Save Ca	ancel		
Create New Delete					
				1	
		Next	Cancel		

## **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 434.

# **Configuring Global WLAN Settings**

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

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

### FIGURE 160 Configuring Global Settings for All WLANs

	Internet		Connected	►
((t.	WiFi Networks	Traffic: 0.50 MB	Total 1 Working 1 D	lisabled
Crea		1 hour 🔻	1 WiFi Network(s) enabled, 0 WiFi Network(s) disabled. Please select one of the WiFi Network to see details.	
Su	Immary (1 WiFi Network in	total)	3 Client(s) Show Clier	nt(s) Info 🕨
	Clients Tra	affic	Client Status for last 1 hour	
Un	leashed		Excellent Moderate Poor	
1			4	

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

### NOTE

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

• Users: Create new users on the internal database.

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

### FIGURE 161 Global Configuration Settings for All WLANs

Create        Create   <		Global Configuration	×		
Create Control of the Configuration of users' wireless settings. Ask users to connect their wireless devices to either wireless devices to either wireless devices to either wireless devices to either database and run the Zero-IT Activation WLAN/SSID, and then have them go to the Activation URL shown below. After they downood and run the Zero-IT Activation application, their wireless devices will be configured automatically for WLANs that support Zero-IT Activation. Activation URL: https://192.168.0.4/activate Authentication Server Cocal Database   Apply Cancel  Clients  Client(s)	🗢 Wifi N	Zero-IT Activation Default Web Portal Logo Users			
Clients Cancel		wired network or dedicated activation WLAN/SSID , and then have them go to the Activation URL shown below. After they download and run the Zero-IT Activation application, their wireless devices will be configured automatically for WLANs that support Zero-IT Activation. Activation URL: https://192.168.0.4/activate		1 hour V	
		Apply C	Cancel		
		1 Client(s)		nfo 🕨	

## **Editing an Existing WLAN**

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

### FIGURE 162 Click Edit to edit an existing WLAN

WiFi Networks	Traffic: 0.01 MB	Total     1     Disabled     0       Data duration:     1 hours     •	
Summary - Total 1 WiF	i Networks	Summary 1 WiFi Networks enabled, 0 WiFi Networks disabled.	
Unleashed 0 0 5 Clients	Traffic	Show Clients Info       Client Status for last   Excellent  Moderate  Poor	
		5	

### FIGURE 163 Modify WLAN settings

	Create Edit	Disable Delete		ata duration: 1 hours 🔻	^
	Summary - Total 1 V	Edit WLAN	×		
			Unleashed  Standard for most regular wireless network usage	Clients Info 🕨	
	Unleashed	Authentication Method:	Guest Access guest access policies and access control will be applied     Hotspot Service known as WISPr     Open    802.1X EAP    MAC Address		
1	0 0 5 Clients		WPA2 WPA3 WPA2/WPA3-Mixed OWE None      Show password		
		Accounting Server:	Disabled		
		Show Advanced Options	<b>OK</b> Cancel		
			13:08 13:09 13:10 13:11 13:12 13:13 13:14 13:15 1	3:16 13:17	
		т	Traffic for last		

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

## Using a QR Code to Join a Wi-Fi Network

Instead of entering a Wi-Fi password manually, you can join a Wi-Fi network using a QR code.

Complete the following steps to join a Wi-Fi network using a QR code.

1. From the Unleashed Dashboard, expand the Wi-Fi Networks and select More > Show QR Code.

### FIGURE 164 Joining a WLAN Using a QR Code

4	WiFi Networks		Total 1 Working 1 Dis	abled 0	•
1	Create Edit More -		Data duration: 11	nour 🗸	
	Disable Summary - Total 1 Delete Show QR Code	Summary			
l	Clients Traffic	1 WiFi Networks enabled, 0 WiFi Networks disabled.			
	1s-wpa	0 Clients	Show Clients	Info 🕨	
1	0 0 0 Clients Traffic	Client Status for last 1 hour	r		
		5-			
		4-			

#### 2. In the **QR Code** page, click **Print** to print the QR code or scan the QR code using a smartphone camera.

#### FIGURE 165 QR Code Page

Do you want to print the QR code for this Wi-Fi network?

#### 1. How to use Wi-Fi QR code?

You can print and share it to your users, and ask them to open the camera app on the smartphone and hold it over the Code. A notification should pop up and connect them to the wireless network automatically. If this did not work, check the smartphone settings and make sure that the QR Code scanning feature is enabled. If it still not working, then you may need to ask your user to download a third-party QR Code scanner from smartphone app store.

#### 2. How can I regenerate the QR code later?

You can to to WiFI Networks page and select your WiFI, click the "More" button and then click "Show QR Code" from the dropdown list, a QR code page should pop up.



Print

The Show QR Code option is not supported across all WLAN types. Refer to the following table for more information.

### TABLE 30 QR Code Support for WLAN Types

WLAN Type	QR Code Support
Open/None	Yes
Open WPA2	Yes
Open WPA3	No
Open WPA2/WPA3-Mix	No
Open OWE	No
802.1x + WPA2	No
802.1x + WPA3	No
802.1x + WPA2/WPA3-Mix	No
MAC + WPA2	Yes
MAC + WPA3	No
MAC + WPA2/WPA3-Mix	No
MAC + None	Yes

## **Deleting a WLAN**

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

### FIGURE 166 Deleting a WLAN

奈 WiFi Networks			Total 1 Working 1 Disabled 0
Create Edit More •			Data duration: 1 hour ~
Summary - Total 1 0 0 0 Show QR Code		Ruckus-Wireless 1	
Clients Traffic	0 Clients		Show Clients Info 🕨
Ruckus-Wireless 1	Client Status for last 1 hour 5	Excellent 🔜 Moderate 📟 Poor	

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

# **Disabling a WLAN Temporarily**

Complete the following steps to temporarily disable a WLAN:

- 1. In the Wi-Fi Networks section, select the WLAN that you want to disable, and click More > Disable.
- 2. Click **OK** when prompted to disable the selected WLAN.
- 3. Click Enable to re-enable the WLAN.

### FIGURE 167 Disabling a WLAN Temporarily

奈 WiFi Networks		Total	1 Working 1 Disabled 0
Create Edit More -			Data duration: 1 hour
Summary - Total 1 Delete 0 0 0 Show QR Code		Ruckus-Wireless 1	
Clients Traffic	0 Clients		Show Clients Info
1 Ruckus-Wireless 1	Client Status for last 1 hour	Excellent Moderate Poor	

# **Advanced WLAN Configuration**

•	Advanced WLAN Configuration Overview	267
	Configuring Advanced WLAN Options	
	Zero-IT and DPSK Settings	
	WLAN Priority Settings	
	Access Control Settings	
	Application Policies	
•	Radio Control Settings	282
•	Other Advanced WLAN Settings	284

## **Advanced WLAN Configuration Overview**

The WLAN Advanced options include settings such as Zero-IT and Dynamic PSK options, WLAN priority, VLAN, access controls, rate limiting, application policies, URL filtering controls, radio controls and other advanced settings.

The advanced WLAN options available vary depending on the authentication and encryption methods chosen as well as the WLAN usage type.

# **Configuring Advanced WLAN Options**

To edit the advanced options for a WLAN:

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

2. Click the arrow next to Show advanced options to expand the advanced options section.

### Create WLAN × \* Name: Usage Type: Standard for most regular wireless network usage O Guest Access guest access policies and access control will be applied Hotspot Service known as WISPr Authentication Method: Open 802.1X EAP MAC Address Encryption Method: O WPA2 O WPA3 O WPA2/WPA3-Mixed O OWE None Web Authentication: Enable captive portal/Web authentication (Users will be redirected to a Web portal for authentication before they can access the WLAN.) Clients Info 🕨 Accounting Server: Disabled • + ø Send Interim-Update every 10 minutes Unleashed Show Advanced Options > ок Cancel

### FIGURE 168 Click Show Advanced Options

### FIGURE 169 WLAN advanced options

l	Jnleashed	Accounting Server	WLAN.) Disabled		Clients Info ▶	*
1	Clients	AN Priority Access Con	atrol Radio Control Others			
2	Guest WLAN 1	Hide SSID : ( Access VLAN : ( Max Clients : /	<ul> <li>High Low</li> <li>Hide SSID in Beacon Broadcasting (Closed System)</li> <li>Enable Dynamic VLAN</li> <li>Allow up to 100 clients per AP radio</li> <li>Always on Always off Specific</li> </ul>		12:30	
		0.	<b>ок</b> .4 м8 -	Cancel		

- 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 269.
  - WLAN Priority: Contains options for setting the WLAN's priority level, WLAN visibility, VLAN, max clients and service schedule. See WLAN Priority Settings on page 276.
  - Access Control: Contains options for configuring Call Admission Control, rate limiting, access controls, application visibility policies and URL filtering. See Access Control Settings on page 277.
  - **Radio Control**: Contains options for configuring radio settings including 802.11k radio resource management, Background Scanning, load balancing and band balancing. See Radio Control Settings on page 282.
  - **Others**: Contains options for configuring force DHCP, inactivity timeout, wireless client isolation, and enabling the Apple CNA bypass feature. See Other Advanced WLAN Settings on page 284.
- 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 170 Enabling Zero-IT for a WLAN

Unleashed 1 0 0 7	Password:     Show password     Clients Info ▶       Accounting Server:     Disabled     ▼       Send Interim-Update every     10     minutes	
	Hide advanced options ▼          Zero-IT & DPSK       WLAN Priority       Access Control       Radio Control       Others	
	Zero-IT Activation <sup>™</sup> :  Enable Zero-IT Activation WLAN users are provided with wireless configuration installer after they log in. Dynamic PSK <sup>™</sup> :  Disable  Internal  External	
	OK Cancel	

### **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 271 for more information).
- 6. Click **OK** to save.

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

### **Enabling DPSK for a WLAN**

Complete the following steps to enable DPSK for a WLAN.

- 1. Expand the Wi-Fi Networks section, and click Create to configure a new WLAN (or Edit for an existing WLAN).
- 2. For Usage Type, select Standard.
- 3. For Authentication Method, select Open.
- 4. For Encryption Method, select WPA2.
- 5. Click Show advanced options and select the Zero-IT & DPSK tab.
- 6. For **Dynamic PSK**, choose one of the following options:
  - Internal: Use the internal database for client authentication.
  - External: Use an external AAA (RADIUS) server for client authentication.

7. If using an external RADIUS server for authentication, select the authentication server from the list and click **OK** to save.

Unleashed	Encryption Method:  WPA2  None  Accounting Server:  Disabled	Clients Info 🕨	•
1 Clients	Hide advanced options ▼       Zero-IT & DPSK     WLAN Priority     Access Control     Radio Control     Others       Dynamic PSK <sup>TM</sup> :     O Disable     Internal     External       Authentication Server     RADIUS 1     ▼	08:40	
	OK Cancel		•

If using an internal database, continue with the following steps.

- 8. For **DPSK Type**, select one of the following options:
  - Secure D-PSK: Includes almost all printable ASCII characters, including periods, hyphens, dashes, and so on. This option is more secure; however it may be difficult to use for mobile clients whose keyboards may not contain the entire set of printable ASCII characters.
  - Mobile Friendly D-PSK: Select this option if this WLAN is used for mobile clients. This range of characters is limited to lowercase letters, uppercase letters, and numbers that makes it easier for users to input the DPSK when activating a mobile client to a Zero-IT WLAN. (You may also want to limit the DPSK length to 8 characters for the convenience of your mobile client users.)
  - User Friendly D-PSK: This option includes numbers only. By default, the DPSK length is set to 8 characters automatically and the maximum DPSK length is 62 characters.

### NOTE

All generated DPSK keys (only numbers) must also be unique within the same WLAN and MAC address (bound or unbound).

- 9. For DPSK Length, enter a PSK passphrase length (from 8 through 62 characters).
- 10. **Expire D-PSK**: Set the time interval from when the DPSK must expire. For **Validity Period**, select whether the DPSK expiration period will start from first use or the creation time.
- 11. Limit D-PSK: By default, each authenticated user can generate multiple DPSKs. Select this option to limit the number of DPSKs that each user can generate across multiple devices (1 through 4).
- 12. Shared D-PSK: Enable this option to allow a single user to share a single DPSK across multiple devices. By default, each DPSK is unique and mapped to a single MAC address; the Shared D-PSK option allows the administrator to override this rule and allow a user to share a single DPSK across multiple devices.
- 13. Click **OK** to save your changes.

This WLAN is now ready to authenticate users using DPSKs once their credentials are verified against either the internal database or an external AAA server.

### FIGURE 172 Using the Internal Database for DPSK Authentication

Zero-IT & DPSK	WLAN Priorit	y Access Control	Radio Control	Others		
Zero-IT Act	ivation <sup>TM</sup> : 🗹	Enable Zero-IT Activa	ation			
	WL	AN users are provided	with wireless confi	guration installer after they log in.		
Dynami	ic PSK™ : ○	Disable 💿 Internal (	⊖ External			
	All	generated D-PSK of	the WLAN could b	be removed if configurations related to D	PSK	
	are	changed,for more de	etail, please refer	to help document.		
DF	SK Type : 🔿	Secure D-PSK The k	ey will include near	rly all printable ASCII characters.		
	0	O Mobile Friendly D-PSK The key will include numbers, lower case and upper case letters.				
	۲	User Friendly D-PSK	The key will only i	nclude numbers.		
DPS	K Length : 8	character pass	phrase.			
Exp	ire D-PSK Set	t when the D-PSK sho	ould expire Unlin	nited 🗸		
	Val	idity Period:  Effect	tive from first use	O Effective from creation time		
Lii	mit D-PSK	Limit D-PSK generati	on per user to 1	devices.		
	Cu	rently allow 1~4 device	es per user.			
Shar	red D-PSK 🗌	Enable one D-PSK to	share with 2	devices(2~2048).		

#### NOTE

For information on DPSK management and batch generation, refer to Dynamic PSK on page 426.

### DPSK Functionality for Legacy and Non-Legacy Devices

The following use cases apply to DPSK functionality for legacy and non-legacy devices:

- If you change the name of the WLAN SSID, Unleashed deletes all the DPSKs of legacy and non-legacy devices.
- If Dynamic PSK is changed from Internal to External or Disable, Unleashed deletes all the DPSKs of legacy and non-legacy devices.
- If DPSK Validity Period or Shared DPSK options are changed, Unleashed deletes all the DPSKs of non-legacy devices only.
- If Allow Legacy Devices to connect to WLAN by previous password is disabled, Unleashed deletes DPSKs of legacy devices only.
- If the legacy device is unmarked, Unleashed deletes the DPSK of this legacy device.
- If the legacy device is deleted from the UI, Unleashed does not delete the DPSKs of this legacy device.

### Using External DPSK with RADIUS Authentication

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

The external DPSK feature allows customers to exceed the maximum number of DPSKs that can be stored on the controller, and provides the option to store and manage DPSKs on the AAA server for distribution to multiple controllers.

To enable external DPSK using an external authentication server:

- 1. Go to WiFi Networks > Create/Edit WLAN > Advanced Options > Zero-IT & DPSK.
- 2. In Dynamic PSK, select External.
- 3. In Authentication Server, select or create an AAA server entry.
- 4. Click OK.

### **FIGURE 173 External DPSK**

Encryption Method:  WPA2  WPA3  WPA2/WPA3-Mixed  OWE  None Accounting Server: Disabled  V +  Send Interim-Update every 10 minutes			•
Hide Advanced Options ▼           Zero-IT & DPSK         WLAN Priority         Access Control         Radio Control         Others		11:10	
Dynamic PSK <sup>TM</sup> : Obiable Interna External Authentication Server Ruckus RADIUS T +			
		63	
		11:10	
ок	Cancel		

- 5. The controller will send Access-Request messages to the RADIUS server with following attributes: Ruckus-SSID, Ruckus-BSSID, User-Name, Ruckus-Dpsk-Params.
- 6. The AAA server sends back a RADIUS Access-Accept or Access-Reject message with the following attributes: Access-Accept: Calling-station-id, Tunnel-Type, Tunnel-Medium-Type, Tunnel-Private-Group-Id, MS-MPPE-Recv-Key, Session-Timeout, Ruckus-User-Groups, User-Name. The MS-MPPE-Recv-Key is mandatory.

### NOTE

If the User-Name attribute is empty in the Access-Accept packet of external Radius server, the column User in the web UI uses the User-name attribute from the Access-Request packet of Unleashed.

7. The AAA server generates a DPSK key (PMK) for each wireless station. This key is encrypted and entered in the attribute MS-MPPE-Recv-Key: PMK = PBKDF2\_SHA1(PassPhrase, Wlan-SSID, Wlan-SSID-Len, 4096, 32). See RFC2548 Chapter 2.4.3.

### NOTE

The WLAN-SSID attribute will exist in the authentication request. The AAA server can use this value to generate the PSK or the AAA server can be pre-configured with WLAN-SSID value.

- 8. The AAA server calculates the wireless station's Pairwise Transient Key (PTK) from the Ruckus-Dpsk-Params attribute (AKM Suite, Cipher, Anonce, EAPOL-Key-Frame) in the Access-Request message and generates the PMK key, and finally verifies the Key MIC of the station. If it matches, the RADIUS server will send back an Access-Accept message with the MS-MPPE-Recv-Key attribute.
- 9. With the DPSK keys generated managed by the AAA server, the controller's internal max DPSK limits are avoided and an unlimited number of DPSKs can be generated.

### **External DPSK RADIUS Attribute Value Pairs**

The RADIUS Attribute Value Pairs (AVP) and Vendor Specific Attributes (VSA) used in external DPSK generation are listed in the following table.

The following parameters are used in access-request messages.

### TABLE 31 Access-Request message parameters

	Parameter	AVP / VSA name	Comment
1	SSID	Ruckus-SSID	Since DPSK passphrases are bound to SSIDs, it's expected that AAA server will have the PMK lists indexed by SSID value.
2	UE's MAC address	User-Name	This AVP chosen for backward compatibility with MAC Authentication use case. The AAA server can override this value with a real (human or account) user-name when User-Name AVP is included in an Access-Accept or Access-Reject message.
3	AP's BSSID	Ruckus-BSSID	Note: the AAA Interface Document needs to be updated. Currently it states, "BSSID for each WLAN in each radio"; however, only a single BSSID (the one the client has associated with) is included in the VSA.
4	Anonce	Ruckus-DPSK-params	This is a new Ruckus VSA, defined below.
5	Snonce	Ruckus-DPSK-params	The Snonce is parsed from the EAPOL Key Frame field of Ruckus-dpsk- params.
6	MIC	Ruckus-DPSK-params	The MIC is parsed from the EAPOL Key Frame field of Ruckus-dpsk-params.
7	4WHS-M2 EAPOL Key frame	Ruckus-DPSK-params	The EAPOL-Key-Frame is used for the MIC calculation.
8	Cipher	Ruckus-DPSK-params	If the UE has negotiated TKIP-based encryption (this would be a really old device), then the key integrity algorithm is different than AES (Advance Encryption Standard, the encryption algorithm currently in use). In this case, AAA server also has to use the same algorithm as the UE in order to properly identify the PMK. TKIP is indicated according to the Cipher octet (see below). Note that two different integrity algorithms are used: HMAC-SHA1 ands HMAC-MD5.
9	AKM Suite	Ruckus-DPSK-params	The use of the AES key integrity and key hierarchy is indicated by the AKM Suite value. If the UE has negotiated FT encryption (FT - fast transition, aka 802.11r), generating the PTK from the PMK uses a different algorithm than AES. In this case, AAA server also has to use the same algorithm as the UE in order to properly identify the PMK. The AKM Suite value indicates whether FT is used.

The following parameters are used in access-accept/access-reject messages.

	Parameter	RADIUS AVP or VSA name	Mandatory / Optional	Comment
1	MS-MPPE-Recv-Key	MS-MPPE-Recv-Key	Mandatory	Included whenever the AAA server has found a matching PMK (for either bound or unbound case).
2	PMK-time	Session-Timeout	Mandatory	Included whenever the AAA server has found a matching PMK, this is PMK expired time for the controller. Its range could be 0-14400 minutes.
3	User-name	User-name	Optional	Included if admin desires the username to be included in syslog events generated by the controller.
4	VLAN assignment	The following triplet of AVPs: 1. Tunnel-Type 2. Tunnel-Medium-Type 3. Tunnel-Private-Group-Id	Optional	<ul> <li>Included if admin requires dynamic VLAN assignment. Note: the Tag field in all three AVPs is set to the same value (see RFC-2868).</li> <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 "<vlan id="">". VLAN ID has a value between 1 and 4094 and is encoded as a string (see RFC-3580).</vlan></li> </ul>
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:

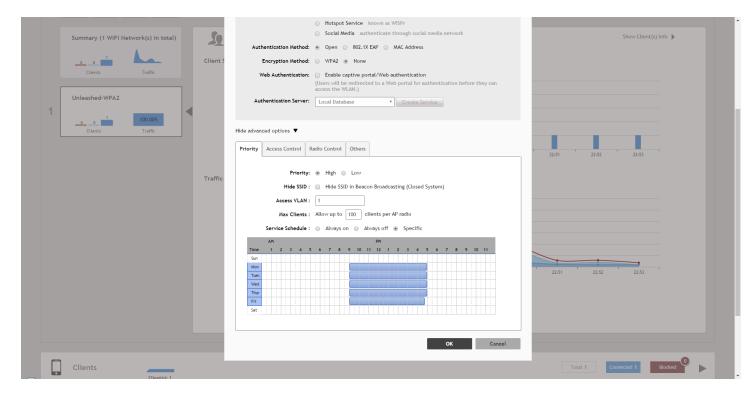
- **Priority**: Set the priority of this WLAN to *Low* if you would prefer that other WLAN traffic takes priority. For example, if you want to prioritize internal traffic over guest WLAN traffic, you can set the priority in the guest WLAN configuration settings to "Low." By default, all WLANs are set 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 386.

### FIGURE 174 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 413.
- 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 417 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 279.
- 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 450.
- WiFi Calling: Wi-Fi Calling is a service for Android and iOS smartphones that allows clients to make and receive voice phone calls over a Wi-Fi connection. For more information, see Wi-Fi Calling on page 456.

Zero-IT & DPSK       WLAN Priority       Access Control       Radio Control       Others         Call Admission Control:       Enforce CAC when CAC Is enabled on the radio         Rate Limit:       Per STA rate limiting will not work if SSID rate limiting is enabled.       13:35         Per Station Uplink       DISABLE • mbps (0.1~200.0)       Per Station Downlink       DISABLE • mbps (0.1~200.0)         Per Station Downlink       DISABLE • mbps (0.1~500.0)       Enable Per SSID Uplink       0       mbps (0.1~500.0)         Enable Per SSID Downlink       0       mbps (0.1~500.0)       Enable Per SSID Downlink       0       mbps (0.1~500.0)         Access Control:       Layer2 MAC ACL :       No ACL • • • •       •       •       •         Layer3/4 ACL :       No ACL • • • •       •       •       •       •       •         Device Policy :       No ACL • • • •       • <t< th=""></t<>
Rate Limit: Per STA rate limiting will not work if SSID rate limiting is enabled.   Per Station Uplink DISABLE • mbps (0.1~200.0)   Per Station Downlink DISABLE • mbps (0.1~200.0)   Enable Per SSID Uplink 0   mbps (0.1~500.0)   Enable Per SSID Downlink   Ombps (0.1~500.0)   Access Control:   Layer2 MAC ACL :   No ACL • • •   Device Policy :   No ACL • • •   Application Visibility:   Enable   Apply Policy Group :
Image: Single interview       Image: Single interview
Per Station Uplink       DISABLE * mbps (0.1~200.0)         Per Station Downlink       DISABLE * mbps (0.1~200.0)         Enable Per SSID Uplink       0         mbps (0.1~500.0)       Enable Per SSID Downlink         Access Control:       Layer2 MAC ACL :         No ACL *       *         Device Policy :       No ACL *         Application Visibility:       Enable         Apply Policy Group :       No_Policy *
Enable Per SSID Uplink 0 mbps (0.1~500.0)   Enable Per SSID Downlink 0 mbps (0.1~500.0)   Access Control: Layer2 MAC ACL : No ACL · + · · Layer3/4 ACL : No ACL · + · Device Policy : No ACL · + · Application Visibility: Enable Apply Policy Group : No_Policy · + ·
□ Enable Per SSID Downlink 0 mbps (0.1~500.0)   Access Control: Layer2 MAC ACL : No ACL ✓ +    Layer3/4 ACL : No ACL ✓ +    Device Policy : No ACL ✓ +    Application Visibility: □ Enable   Apply Policy Group : No_Policy ✓ +
Access Control: Layer2 MAC ACL : No ACL · + / Layer3/4 ACL : No ACL · + / Device Policy : No ACL · + / Application Visibility: Enable Apply Policy Group : No_Policy · + /
Layer3/4 ACL : No ACL V + P Device Policy : No ACL V + P Application Visibility: Enable Apply Policy Group : No_Policy V + P
Device Policy : No ACL    Application Visibility: Enable   Apply Policy Group : No_Policy
Application Visibility: Enable Apply Policy Group : No_Policy  +
Apply Policy Group : No_Policy V +
URL Filtering:  Enable
URL Filtering Profile : V + V
Wi-Fi Calling:  Enable
OK Cancel

### FIGURE 175 Advanced WLAN settings - Access Control configuration

# **Application Policies**

For instructions on configuring Application Control Policies, see Creating an Application Control Policy on page 279.

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 419.

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.

de Advanced Options 🔻				*
Zero-IT & DPSK WLAN Priority Access Control	Radio Control Others			
Call Admission Control: Enforce CAC when CA	C is enabled on the radio		10:00	
Rate Limit: Per STA rate limiting will	ot work if SSID rate limiting	g is enabled.		
Per Station Uplink	Disabled •	]		
Per Station Downlink	Disabled •			
🗌 Enable Per SSID Upli	nk 0	mbps (0.1~200.0)		
Enable Per SSID Dow	nlink 0	mbps (0.1~200.0)		
Access Control: Layer2 MAC ACL :	lo ACL 🔻 🕇 🖋			
Layer3/4 ACL :	lo ACL 🔻 🕇 🖋			
Device Policy :	lo ACL 🔻 🕇			
Application Visibility: 🖉 Enable				
Apply policy group :	Block Facebo 🔹 🕇	·		
URL Filtering: Enable				
URL Filtering Profile :	• •	Ø	10:00	
		OK Cancel		

FIGURE 177 Creating an Application Control Policy for a specific website

New A	Create Application	on Policy Rule		×	×	
	*Rule Type:	Denial Rules	•			
* N	*Application Type:	System Defined	•			
De	*Application:	Web	Facebook	~		
CI						
No			ок	Cancel		
			0-0 0	or u snown		
				OK Canc		

# **Radio Control Settings**

The [Edit WLAN] > Advanced Options > Radio Control tab provides options for configuring radio settings for the WLAN, such as load balancing, band balancing, fast BSS transition and radio resource management.

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

- Fast BSS Transition: (Disabled by default) The Fast BSS Transition feature uses messages and procedures defined in 802.11r to allow continuous connectivity for wireless devices in motion, with fast and secure handoffs from one AP to another. A fast BSS transition is a BSS transition in the same mobility domain that establishes the state necessary for data connectivity before the re-association rather than after the re-association. In this way, clients that support the 11r standard (including iOS devices) can achieve significantly faster roaming between APs.
- Radio Resource Management: (Disabled by default) Radio Resource Management utilizes 802.11k Neighbor Reports, which are sent by the AP to inform clients of the preferred roaming target AP. The client sends 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.

This option allows you to create separate WLANs on the two radios. For example, you could create a "2.4G" WLAN with the *Enable WLAN* on feature set to **2.4 GHz only**, and a "5G" WLAN with the feature set to **5 GHz only**.

For more information, see Creating Separate WLANs for 2.4 GHz and 5 GHz Radios on page 283.

### FIGURE 178 Radio Control options

Driarity Assass Control
Priority Access Control
Wireless Med Managemen

### **Creating Separate WLANs for 2.4 GHz and 5 GHz Radios**

Use the "Enable WLAN on" option to configure 2.4 or 5 GHz radio service on/off for the WLAN. This allows you to create two separate WLANs that each operates on one or the other of the 2.4 or 5 GHz radios.

In some scenarios, it may be preferable to deploy a separate WLAN/SSID for each radio; one 2.4 GHz SSID and one 5 GHz SSID. In this way, you can ensure that all 2.4 GHz-only devices connect to the 2.4 GHz WLAN only, while 5 GHz-capable devices are allowed to connect to the 5 GHz WLAN.

- 1. Create the 2.4 GHz WLAN.
- 2. Go to WiFi Networks > Create > Advanced Options > Radio Control.
- 3. In Enable WLAN on, select 2.4 GHz only.
- 4. Click **OK** to save.
- 5. Create the 5 GHz WLAN.
- 6. Go to WiFi Networks > Create > Advanced Options > Radio Control.
- 7. In Enable WLAN on, select 5 GHz only.

8. Click **OK** to save.

FIGURE 179 Use the "Enable WLAN on" option to configure 2.4 or 5 GHz radio service on/off for the WLAN

Clients		isabled V + P nd Interim-Update every 10 minutes	•
Hide	e Advanced Options 🔻		
W	LAN Priority Access Control	Radio Control Others	
	Wireless Media Rad	dio Resource Management :  Enable 802.11k Neighbor-list Report	
	Management: Rec	commended to enable 802.11k Neighbor-list Report for assistant.	
	Bac	ckground Scanning : Z Enable	
	(All r	radios will perform background scanning)	
	Loa	ad Balancing :      Enable	
	(App	plies to this WLAN only.it may not be active on other WLANs)	
	Ban	nd Balancing : D Enable	
	Appl	plies to this WLAN only. Band Balancing might be enabled on other WLANs	
	802	2.11d :	
		Support for 802.11d (only applies to radios configured to operate in 2.4 GHz band)	
	Ena	able WLAN on : 2.4 GHz only  All Radios	
		2.4 GHz only OK Cancel 13:50	
		5 GHz only	Ŧ

9. To verify that only 2.4 GHz devices are connected to the 2.4 GHz WLAN and 5 GHz devices are connected to the 5 GHz WLAN, expand the **Clients** section and view the list of connected wireless clients. Check the WLAN and *Radio* columns to view connection status.

# **Other Advanced WLAN Settings**

The **Others** tab provides the following options:

- Force DHCP: (Disabled by Default.) Enable this option to force clients to obtain a valid IP address from DHCP within the specified number of seconds. 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 (from 1 through 500 minutes).
- Wireless Client Isolation: Select the level of client isolation you want to enforce:
  - **Isolate wireless client traffic from other clients on the same AP**: Enables client isolation on the same Access Point (clients on the same subnet but connected to other APs will still be able to communicate).
  - Isolate wireless client traffic from all hosts on the same VLAN/subnet: Prevents clients from communicating with any host on the same subnet or VLAN other than those listed on the client isolation allowlist. If this option is chosen, you must select a allowlist from the drop-down list. (Refer to Configuring Client Isolation Allowlists on page 286.)
- **Bypass Apple CNA Feature**: With Bypass Apple CNA enabled, captive portal (web-based authentication) login must be performed by opening a browser to any unauthenticated page (HTTP) to get redirected to the login page. (Refer to Bypass Apple CNA on page 287).
- **Tunnel Mode**: Select this check box if you want to tunnel the WLAN traffic back to Dedicated Master. Tunnel mode enables wireless clients to roam across different APs on different subnets. If the WLAN has clients that require uninterrupted wireless connection (for example, VoIP devices), RUCKUS recommends enabling tunnel mode.

### NOTE

When tunnel mode is enabled on a WLAN, multicast video packets are blocked on that WLAN; however, multicast voice packets are allowed.

- **DTIM Interval**: Configure the Delivery Traffic Indication Message (DTIM) interval to control how often DTIM messages are transmitted. This setting affects the frequency of data transmissions per broadcast beacon. Setting the DTIM interval to a lower value results in more frequent DTIM messages, which can prevent mobile devices from going into power save mode, thereby increasing battery consumption.
- Directed MC/BC Threshold: 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 the syslog server (refer to Client Connection Troubleshooting on page 359):
  - Send traffic flow data to syslog server: RUCKUS Unleashed sends client flow data only to the syslog server.
  - Send connection records to syslog server: RUCKUS Unleashed sends client connection event logs only to the syslog server.
- Wifi6: (Optional) Enable wifi6. (Disabled by Default).

### FIGURE 180 Configuring Other Advanced WLAN Settings

Zero-IT & DPSK	WLAN Priority	Access Control Radio Control Others					
	Force DH0	<ul> <li>P: Enable Force DHCP. Disconnect client if client does not obtain valid IP address in 10 seconds.</li> </ul>					
	Inactivity Timeo	ut: Terminate idle user session after 5 minute(s)					
Wirel	ess Client Isolatio	n: Isolate wireless client traffic from other clients on the same AP.					
	Isolate wireless client traffic from all hosts on the same VLAN/subnet.						
		No AllowList 🗸 🖌					
		(Requires allowlist for gateway and other allowed hosts.)					
	Tunnel Mo	le: 🗹 Tunnel WLAN traffic to Unleashed					
		(Recommended for VoIP clients and PDA devices.)					
	DTIM Interv	1 (1-255) Defines the frequency of beacons that will include a DTIM					
		(0-128) Defines the client count at which an AP will stop converting					
Directe	d MC/BC Thresho	group-addressed data traffic to unicast					
Cli	ient Traffic Loggiı	g: 🗹 Send traffic flow data to syslog server					
		Send connection records to syslog server					
		also available for download at Client Connection Logs section of Admin & Servic > Administration-> Diagnostics -> Client Troubleshooting tab					

### **Configuring Client Isolation Allowlists**

When Wireless Client Isolation is enabled on a WLAN, all communication between clients and other local devices is blocked at the access point.

To prevent clients from communicating with other nodes, the access point drops all ARP packets from stations on the WLAN where client isolation is enabled and which are destined to IP addresses that are not part of a per-WLAN allowlist.

You can create exceptions to client isolation (for example, allowing access to a local printer) by creating client isolation allowlists.

Complete the following steps to configure a client isolation allowlist:

- 1. Go to Wi-Fi Networks > Advanced Options > Others.
- 2. Under Wireless Client Isolation, select both the options:
  - Isolate wireless client traffic from other clients on the same AP
  - Isolate wireless client traffic from all hosts on the same VLAN/subnet
- 3. Click Create Allowlist.
- 4. Enter a name and a description (optional) for the allowlist.
- 5. Auto Allowlist is enabled by Default, which allows the APs to auto-discover gateway devices and add them to the isolation allowlist.
- 6. Under Rules, click Create New to create multiple device-specific rules for each device to be allowlisted. For each rule, enter the following:
  - **Description**: Description of the device.
  - MAC Address: Enter the MAC address of the device.
  - IPv4 Address: Enter the IP address of the device.
- 7. Click Save to save the rule you created.
- 8. To change the order in which rules are implemented, select the order from the drop-down menu in the **Order** column. You can also edit or clone rules from the **Action** column. To delete a rule, select the check box next to the rule and click **Delete**.
- 9. Click **OK** to save the allowlist.

### FIGURE 181 Creating a Client Isolation Allowlist

Creat	e New						×
	* Name						
	Description						
	Auto Allowlist	🛛 APs will auto	-discover gateway	devices and add then	to the isolation allowl	ist	
	Datas	Order	Description	MAC Address	IPv4 Address	Action	
	Rules Create New Delete						
					ок	Cance	el
		⊖ Single	shared password	among all guest			
	Guest Friendly	Key: 🖾 Enable	e The key will inclu				
	Grace Pe	eriod: 🖪 Allow	users to reconnect	without re-authenticat	ion for 480 minute	es	

### **Bypass Apple CNA**

Some Apple iOS and OS X clients include a feature called Captive Network Assistant (Apple CNA), which allows clients to connect to an open captive portal WLAN without displaying the login page.

When a client connects to a wireless network, the CNA feature launches a pre-browser login utility and it sends a request to a success page on the Apple website. If the success page is returned, the device assumes it has network connectivity and no action is taken. However, this login utility is not a fully functional browser, and does not support HTML, HTML5, PHP or other embedded video. In some situations, the ability to skip the login page for open WLANs is a benefit. However, for other guest or public access designs, the lack of ability to control the entire web authentication process is not desirable.

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

To enable Apple CNA bypass, use the following procedure:

- 1. Expand the WiFi Networks component and select the WLAN you want to configure, then click Edit.
  - Select one of the following WLAN usage types:
  - Standard Usage with Web Auth enabled
  - Guest Access (including Social Media)
  - Hotspot (WISPr)
- 2. Click Show Advanced Options.
- 3. Click the **Others** tab.
- 4. Select the Enable check box next to Bypass Apple CNA Feature.
- 5. Click **OK** to save your changes.

### FIGURE 182 Enable Bypass Apple CNA feature

Hide advanced options ▼	
Restricted Subnet Access WLAN Priority Access Control Radio Control Others	
Force DHCP : Enable Force DHCP, disconnect client if client does not obtain valid IP in	
10         seconds.           Inactivity Timeout : Terminate idle user session after         1	12:20
Wireless Client Isolation	
No AllowList	
(Requires allowist for gateway and other allowed hosts.)  Bypass Apple CNA @ Enable Feature:	d 2 Disconnected 0
DTIM Interval 1 (1-255) Defines the frequency of beacons that will include a DTIM	
Directed MC/BC 5 (0-128) Defines the client count at which an AP will stop converting group Threshold addressed data traffic to unicast	
Access Point	3 Disconnected 0
Next Cancel	
Admin & Services	•

# **Access Point Configuration**

•	Access Point Configuration Overview	289
•	Show Mesh Topology	290
•	Show Client Info	291
•	Show Events and Alarms	293
•	Configuring Global AP Settings	294
	Monitoring an Individual AP	
•	Configuring an Individual AP	307
•	Working with AP Groups	311
•	Restarting an AP	327
	Removing an AP	

## **Access Point Configuration Overview**

The Access Points component provides tools for monitoring and configuring all Unleashed APs at once, configuring each AP individually, or configuring multiple groups of APs with a set of common custom settings.

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 oneminute 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 183 Access Points Component

Access Points	Total 4 Working 3 Disconnected
Edit Restart Remove	Data duration 1 hour •
Summary - Total 4 Access Points	Summary
Clients Traffic	Maximun 25 APs support 3 Access Points connected, 1 Access Points disconnected.
Master Unleashe[35:c9:40]	Mesh Status :Enabled Show Mesh Topology
1 0 0 3 2.4G 5G Clients Traffic	Show Clients Info
Mesh	Client Status for last 1 hour
RuckusAP[1c:12:c0]	Excellent Moderate Poor
2 0 0 0 2.4G 5G Clients Traffic	5

# **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.

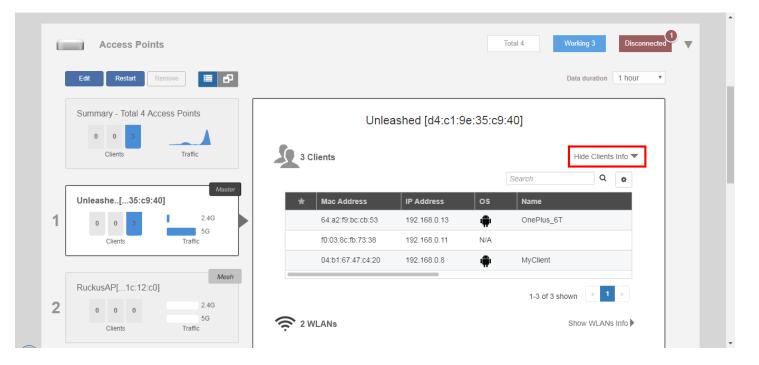
#### FIGURE 184 Mesh Topology

	Access Points				Total 4	Working 3 Di	sconnected
	Edit Restart Remove					Data duration 1 ho	ur 🔻
	Summary - Total 4 Access Points		S	ummary			
	Clients Traffic	Maximun 25 APs suj 3 Access Points con	oport nected, 1 Access Points di	sconnected.			
	Master Unleashe[35:c9:40]	Mesh Status :Ena	bled			Hide Mesh Topology '	-
1	0 0 3 2.4G	Tree	Access Points	Signal	Description	Channel	
	Clients Traffic	<b>□ ↓3</b>	d4:c1:9e:35:c9:40			36	
		e "P	f0:b0:52:1c:12:c0	41		36	
	Mesh	¥., -	f0:b0:52:1b:f0:40	49		36	
	RuckusAP[1c:12:c0]						

# **Show Client Info**

Click this link to display the currently connected clients list.

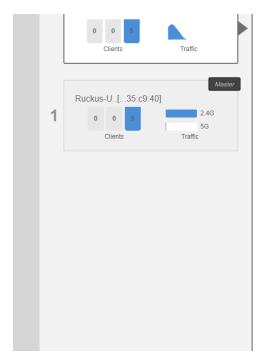
#### FIGURE 185 Client Info summary



## **Show Events and Alarms**

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

#### FIGURE 186 Show/hide Events & Alarms



Maximun	128 APs and 10 AP grou	ps support	
1 Access	Points connected, 0 Acce	ess Points disconnecte	d.
5	Clients		Show Clients Info
Events	vents & Alarms		Hide Events & Alarms 🔻
			Search Q 2 0
	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] wit

# **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 187 Click Edit to configure AP global settings

	Access Points					Total 4	/orking 3	Di	isconnected	<b>P</b> ,
	Edit Restart Remo	ove 🔳 🗗				E	Data duration	1 ho	our 🔻	
Summary - Total 4 Access Points				Summar	y					
	Clients	Traffic	Maximun 25 APs support							
Ľ			3 Access Points connected, 1 Acces	s Points disconnected						
	Unleashe[35:c9:40]	Master	Mesh Status :Enabled			Sho	ow Mesh Top	oology		
1	0 0 3 Clients	2.4G 5G Traffic	3 Clients				Hide Clien	ts Info	•	
						Search	Q	•		
		Mesh	★ Mac Address	IP Address	os	Name				
	RuckusAP[1c:12:c0]		64:a2:f9:bc:cb:53	192.168.0.13		OnePlus_6T			·	
2	0 0 0	2.4G	f0:03:8c:fb:73:38	192.168.0.11	π N/A	_				
	Clients	5G Traffic	04:b1:67:47:c4:20	192.168.0.8		MyClient				

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

## Radio (2.4G)

You can select or clear channels from which to choose during the automatic channel selection process or select a specific channel on which to operate, or enable **Call Admission Control** or **Spectralink Compatibility** for this radio.

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

#### FIGURE 188 System Default AP Group: 2.4 GHz Radio Configuration

General	Radio 2.4 GHz	Radio 5.0 GH	Hz Network	Other								
	Rad	io 2.4 GHz 🗌	Override Grou	p Config	1 2	<b>v</b> 3 <b>v</b> 4	<b>7</b> 5 7	6 🗹 7	89	<b>1</b> 0	11	
	Char	nelization	Override Grou	p Config	Auto	$\sim$						
		Channel 🗌	Override Grou	p Config	Auto	$\sim$						
		TX Power	Override Grou	p Config	Auto	$\sim$						
	Call Admissio	on Control	Override Grou	p Config	Off		$\sim$					
	WLA	N Service	Override Grou	p Config	Disable	~						
	Protec	tion Mode	Override Grou	p Config	RTS/CTS	$\sim$						

## Radio (5G)

You can select or clear channels from which to choose during the automatic channel selection process or select a specific channel on which to operate, or enable **Call Admission Control** or **Spectralink Compatibility** for this radio.

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

#### FIGURE 189 System Default AP Group: 5 GHz Radio Configuration

General	Radio 2.4 GHz	Radio 5.0 GHz	Network	Other	r
					☑ 36 ☑ 40 ☑ 44 ☑ 48 ☑ 52 ☑ 56 ☑ 60 ☑ 64 ☑ 100 ☑ 104
	Radio	5.0 GHz 🗌 C	verride Grou	p Config	fig 💟 108 💟 112 💟 116 💟 120 💟 124 💟 128 💟 132 💟 136 🗌 140
					🗌 144 🗹 149 🗹 153 🗹 157 🔽 161
	Chann	elization 🔽 C	verride Grou	p Config	fig Auto V
		Channel 🔽 C	verride Grou	p Config	fig 48 ~
	T	X Power 🗌 C	verride Grou	p Config	fig Full V
	Call Admission	Control 🗌 C	verride Grou	p Config	fig Off 🗸
	WLAN	I Service 🛛 🖓	verride Grou	p Config	fig Enable V

### Other

The Access Points > Summary > Edit > Other page provides the following options:

- **Preferred Master**: Select a specific AP to be the Master AP and, if the preferred Master AP reboots, it will resume the role of Master AP again once it rejoins the Unleashed network. By default, there is no preference as to which AP should become the Master AP; the first AP that is deployed automatically becomes the Master AP. Using the Preferred Master setting, users can configure one AP to have priority. Any (non-mesh) AP can become the Master if the preferred Master is offline, but when the Preferred Master comes back online, it will assume the Master role again.
- Model Specific Control: Select which AP model to configure from the drop-down list. The options below can be configured independently for each Unleashed AP model. See Modifying Model Specific Controls on page 297.

#### FIGURE 190 Configuring other AP settings

	Edit AP Group	×	ŕ
l	* Name System Default		
1	Radio B/G/N(2.4G)     Radio A/N/AC(5G)     Other		
	Model Specific Control     C110     •       Max Clients     Allow Max 100     clients to associate with this AP       Status LEDs     Disable Status LEDs		
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 191 Model Specific Controls

	Edit AP Group	×	ſ
	* Name System Default		
1	AP Assign WLAN Assign Radio B/G/N(2.4G) Radio A/N/AC(5G) Other Model Specific Control H320  Max Clients Allow Max 100 clients to associate with this AP Status LEDs Disable Status LEDs		
	Port Setting Edit Port Setting		

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 321 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 499.

#### FIGURE 192 PoE Operating Mode

	* Name System Default		
	Radio B/G/N(2.4G) Radio A/N/AC(5G)	Other	
1	Model Specific Control	R720 •	
	Max Clients	Allow Max 100 clients to associate with this AP	
	Status LEDs	Disable Status LEDs	
	PoE Operating Mode	802.3at+ PoE v	
2		Auto	
~		802.3af PoE	
		802.3at PoE	
		802.3at+ PoE	
3			
5			

#### **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 193 Select model and enable the option "Disable Status LEDs"

	Edit AP Group	×	•
	* Name System Default		
1	Radio (2.4G)     Radio (5G)     Other	]	h
	Model Specific Control R610  Max Clients Allow Max 100  clients to associate with this AP		
	Status LEDs     Image: Comparison of the status lebs       PoE Operating Mode     Auto     ▼		

# **Monitoring an Individual AP**

Click one of the AP boxes in the Access Points component to monitor and configure that specific AP individually.

You can edit, restart, or remove an AP from the network from the individual AP monitoring page. The individual AP monitoring page also includes graphs displaying signal quality and traffic statistics, and links to more detailed information on the AP and its connected clients.

#### **FIGURE 194 Viewing Individual APs**

Access Points		Total 4 Working 3 Disconnected
Edit Restart Remove 🗮 🗗		Data duration 1 hour
Summary - Total 4 Access Points	Unleashed [d4:c1:9	e:35:c9:40]
Master	5 clients	Search Q &
Unleashe[35:c9:40]	Mac Address         IP Address           64:a2:f9:bc:cb:53         192.168.0.13	OS Name OnePlus_6T
Clients Traffic	f0:03:8c:fb:73:38 192.168.0.11 04:b1:67:47:c4:20 192.168.0.8	N/A MyClient
Mesh           RuckusAP[1c:12:c0]           2         0         0         2.46		1-3 of 3 shown
Clients Traffic	🔶 2 WLANS	Show WLANs Info 🕨

The individual AP monitoring screen contains the following elements:

- Edit: Click this button to configure an AP individually.
- Restart: Click this button to restart the AP.
- Approve: If auto-approval is disabled, click this button to approve the AP and allow it to join the network.
- Remove: Click this button to remove this AP from the network.
- Show Clients Info: Click this link to display a list of clients currently connected to the AP. Details for each client include MAC address, IP address, OS, Host Name, MAC address of the AP to which the client is currently connected, WLAN name, Signal Strength indicator, Auth status, and duration online.
- Show AP Info: Click this link to display AP-specific information including MAC address, IP address, external IP and port number, model name, serial number, and firmware version.
- Client Status: Displays a breakdown of client numbers by signal quality (Excellent, Moderate, or Poor) over time, in one-minute intervals.
- Traffic: Displays the total traffic (Tx + Rx) on the AP radio in one-minute intervals.

### **Show Client Info**

Click the Show Client Info link to display a list of clients connected to this AP.

#### FIGURE 195 Show Client Info from AP page

							Disconnected	
Edit Restart Remove					Di	ata duration	1 hour 🔻	
Summary - Total 4 Access	Points	Unlea	ashed [d4:c1:9	e:35:c9:	40]			
0 0 3 Clients	Traffic	3 Clients			Г	Hide Clients	s Info 🔻	
	Master				Search	۹	•	
Unleashe[35:c9:40]	Master	★ Mac Address	IP Address	os	Name			
1 0 0 3	2.4G	64:a2:f9:bc:cb:53	192.168.0.13	<b>.</b>	OnePlus_6T			
Clients	5G Traffic	f0:03:8c:fb:73:38	192.168.0.11	N/A				
		04:b1:67:47:c4:20	192.168.0.8	÷.	MyClient			
	Mesh							

### **Show WLANs Info**

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

#### FIGURE 196 Showing WLAN Information for an Individual AP

1	Access Points					Fotal 3 Working 3	Disconnected 0
	Edit Restart Remo	ove 🔳 🗗				Data duration:	1 hours V
	Summary - Total 3 Acces	s Points		Unleashed [d4	4:c1:9e:35:c9:	40]	
	Clients	Traffic	1 Clients			Show Clients Ir	nfo 🕨
ſ	Unleashe[35:c9:40]	Master	🤶 4 WLANS			Hide WLANs Ir	nfo 🔻
1		2.4G	Name/ESSID	BSSID	Radio	State	
1	0 0 1	5G	Unleashed	d4:c1:9e:35:c9:48	802.11b/g/n	Up	
l	Clients	Traffic	Guest WLAN 1	d4:c1:9e:75:c9:48	802.11b/g/n	Up	
		Mesh	Unleashed	d4:c1:9e:35:c9:4c	802.11a/n/ac	Up	
	RuckusAP[1b:f0:40]		Guest WLAN 1	d4:c1:9e:75:c9:4c	802.11a/n/ac	Up	
2	0 0 0	2.4G 5G				1-4 of 4 shown < 1	

## **Show AP Info**

Click **Show AP Info** to display detailed information on this AP. The AP info page displays general information about the AP, including the radio channels in use, Mesh type, maximum number of clients, and firmware version. The **Save Logs** and **Speed Test** buttons are also available.

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

#### NOTE

Speed Test option is displayed for member APs only.

#### NOTE

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

#### FIGURE 197 Showing AP Information for an Individual AP

	0 0 3 Clients	Traffic	3 Clients		Show Clients Info 🕨	*
			2 WLANS		Show WLANs Info 🕨	
	Ruckus-U[35:c9:40]	Master			Hide AP Info 🔻	
1	0 0 3	2.4G 5G	Device Name	Ruckus-Unleashed		
	Clients	Traffic	Status	Connected		
			Uptime	5m 9s		
			Description			
			Location			
			Mac Address	d4:c1:9e:35:c9:40		
			IP Address	192.168.0.14		
			Model	R610		
			S/N	941849001125		
			Group Name	System Default		
			GPS Coordinates			
			Mesh Type	Disabled		
			Current Channel(802.11a/n/ac)	157		
				_		· ·

For **Download Logs**, you can click **Support Logs** to save AP support log as a .txt file, and click **AP Dump Logs** to save the AP dump log as a .tar file on your computer.

#### NOTE

AP Dump Logs and Download buttons are displayed only when an AP reboots unexpectedly.

#### FIGURE 198 Download Logs

GPS C	oordinates			
Mesh T	ype		C	Disabled
Current	Channel(802.11a/n/ac/a	ix)	1	161
Current	Channel(802.11b/g/n/ax	;)	1	11
LACP/L	AG		E	Disabled
Power	Consumption Mode		8	302.3af Switch/Injector
Max Cli	ents		1	100
Version			2	200.10.10.5.88
Fixed N	lember Role		г	10
Downlo	ad Logs		S	Support Logs 🛓 AP dump Logs 🛓
Ethernet Port	Status 🚯			
Port	Interface	Logic Link	Physical Link	Label
Port1	eth0	Down	Down	10/100/1000 Port1
Port2	eth1	Up	Up 1000Mbps ful	II 100/1000/2500 PoE Port2

The table under **Ethernet Port Status** displays the current link status of the Ethernet ports on the AP. Hover over the "i" icon to display an illustration of the physical port locations on the AP.

#### FIGURE 199 Ethernet Port Status

Ethernet Port S	itatus 📵				
Port	Interface	Logic Link	Physical Link	Label	
Port1	eth0	Down	Down	10/100/1000 Port1	
Port2	eth1	Up	Up 1000Mbps full	100/1000/2500 PoE Port2	
Radio (	re to capture wireless   ) 2.4GHz • 5GHz al Mode (Capture a lim ve to file) or[	nited snapshot on each A	P, then Stop 'from one IP	al files or stream them to Wireshark.	
Start Neighbor APs					
Access Point				Channel	SNR
No data availab	le				

The Packet Capture section displays radio channels and capture modes. For more information, refer to Capturing Remote Packets on page 480.

#### FIGURE 200 Packet Capture

k         Physical Link         Label           Down         10/100/1           Up 1000Mbps full         100/1000	Logic Link Down Up	Interface eth0	Port Port1
			Port1
Up 1000Mbps full 100/1000	Up		
		eth1	Port2
kets to/from one IP	imited snapshot on ea	ature to capture wireless lio 0 2.4GHz	Radii L and S C C C C C C C C C C C C C

The Neighbor APs section displays channel, path score, and SNR of nearby APs.

#### FIGURE 201 Neighbor APs

#### **Neighbor APs**

Access Point	Channel	SNR	Path Score (status)
4c:b1:cd:18:e8:60	149	51 dB	666
d8:38:fc:33:ae:f0	44	65 dB	669

The Radio information section provides channel and transmission details on the AP's 2.4 GHz and 5 GHz radios.

#### FIGURE 202 Radio information

Radio 80	02.11b/g/n	802.11a/n/ac 💌
Current Channel 6	5	157
Config Channel A	Auto	Auto
Channelization 2	20	80
WLAN Service	Enabled	Enabled
Background Scanning E	Enabled	Enabled
TX Power F	Full	Full
# of Authorized Client 3 Devices	3	0
% Retries/% Drops 0	0.0140/0.00	0.00/0.00
% Non-unicast 0	0.383	0.00
Packets/Bytes RX 5	5.9K/491K	0/0
Packets/Bytes TX 1	14K/17M	1.4K/323K
Wians Data Packets/Bytes RX 1	1.7K/351K	0/0
Wians Data Packets/Bytes TX 2	2.7K/2.5M	0/0
Noise Floor -9	97	-104
PHY Errors 2	2	0
% AirTime (total/busy/RX/TX) 5	5.0/0.0/4.5/0.5	4.0/0.5/3.5/0.0
Available Channel 1	1,2,3,4,5,6,7,8,9,10,11	36,40,44,48,149,153, 157,161
Block Channel		165

### **Show Events and Alarms**

Click Show Events and Alarms to view lists of event and alarm messages for this AP.

#### FIGURE 203 Show AP-specific Events & Alarms

Ever	Alarms		
			Search Q 2
	Date/Time 👻	Severity	Activities
	2020/03/17 10:56:05	High	A new Same-Network Rogue[f0:b0:52:1b:f0:48] wi
	2020/03/17 10:56:04	High	A new Same-Network Rogue[f0:b0:52:1b:f0:4c] wif
	2020/03/17 10:50:37	High	A new Same-Network Rogue[44:1e:98:1b:f0:dc] w
	2020/03/17 10:50:36	High	A new Same-Network Rogue[44:1e:98:1b:f0:d8] w
	2020/03/17 10:49:34	High	A new Same-Network Rogue[f0:b0:52:1c:12:c8] wi
	2020/03/17 10:49:33	High	A new Same-Network Rogue[f0:b0:52:1c:12:cc] wi
	2020/03/17 10:38:49	High	A new Same-Network Rogue[b4:79:c8:14:26:48] w
	2020/03/17 10:38:48	High	A new Same-Network Rogue[b4:79:c8:14:26:4c] w
	2020/03/17 10:35:48	High	A new Same-Network Rogue[d4:c1:9e:35:c9:58] w
	2020/03/17 10:35:47	High	A new Same-Network Rogue[d4:c1:9e:35:c9:5c] w

.

## **Client Status and Traffic Graphs**

The Client Status and Traffic graphs provide a graphical display of the number and signal quality of connected clients and transmit/receive traffic over the last hour.

#### FIGURE 204 Client status and traffic graphs



# **Configuring an Individual AP**

To configure a specific AP, from the dashboard, Access Points, click the AP you want to configure, and click Edit.

#### FIGURE 205 Configuring an AP

Access Points		Total 4 Working 3 Disconnected
Edit Restart Remove 🔳 🗗		Data duration 1 hour •
Summary - Total 4 Access Points	Unleashed [d4:c	1:9e:35:c9:40]
Clients Traffic	3 Clients	Show Clients Info
Master Unleashe[35:c9:40]	🔶 2 WLANS	Show WLANs Info 🕨
1 0 0 3 2.4G Clients Traffic	Client Status for last 1 hour	Show System Overview Info
Mesh RuckusAP[1c:12:c0]	Excellent	Moderate Poor
2 0 0 0 2.4G Clients Traffic	5	

#### FIGURE 206 Editing an AP's Configuration Settings

Access Points	Total 4 Working 3 Disconnected
Edit Restart Remove 🔳 🗗	Data duration 1 hour •
s Edit AP(d4:c1:9e:35:c9:40)	×
General Radio B/G/N(2.4G) Radio A/N/AC(5G) Network Other	
* MAC Address d4:c1:9e:35:c9:40	
Device Name     Unleashed     Description	
1 Location	
GPS Coordinates Latitude: (example: 37.3881398,-122.0258633)	Longitude:
	OK Cancel
R	on current
<b>2</b> 0 0 0 24G 5G 4-	
Clients Traffic 3	

In general, the settings available on the **Edit AP** page for an individual AP are the same as those for global AP settings (refer to Configuring Global AP Settings on page 294). Configuring these settings for an individual AP overrides the global AP settings.

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

- General: Configure the device name of the AP, the description, location, and GPS coordinates.
- Radio B/G/N (2.4G): Enable or disable WLAN service for this radio.
- Radio A/N/AC (5G): Enable or disable WLAN service for this radio.

#### NOTE

For the country code "US", 11ax and 11ac APs support channel 144. For the country codes "UK" and "JP", only 11ax APs support channel 144.

Network: Configure a manual (static) IP address, or allow the AP to obtain an IP address using DHCP.

#### NOTE

You cannot configure the IP address settings for the current Master AP from the **Network** tab. You must go to **Admin & Services** > **System** > **IP Settings** to change the IP settings of the Master AP.

• Other: Designate this AP to serve as a Bonjour Gateway AP (refer to Bonjour Gateway on page 423), enable or disable the status LEDs of the AP, or override the PoE operating mode settings of the AP group, and configure a specific PoE power mode for this AP.

#### FIGURE 207 Configuring an AP with a Static IP Address from the AP's Edit > Network tab

				Total 4	Working 3	Disconnected
Edit	Restart Remove					hour
s	Edit AP(f0:b0:52:1c:12:	c0)				×
	General Radio B/G/N(2.4G) Radio	A/N/AC(5G) Network Othe	r			
	IP Mode	Override Group Config	IPv4 only v			
	Device IP Settings	IPv4	Manual O DHCP O Keep AP's setting	g		
U		IP Address *	192.168.0.17			
1		Netmask *	255.255.255.0			
		Gateway *	192.168.0.1			
		Primary DNS Server	66.90.130.101			
		Secondary DNS Server	216.82.201.11			
R						
2				ок	Cancel	
	Clients Traffic	3 -				
		2				
	Mesh					

#### FIGURE 208 Other AP Settings

54 0		
Edit	AP(d4:c1:9e:35:c9:40)	×
Gene	ral Radio 2.4 GHz Radio 5.0 GHz Network Other	
	Bonjour Gateway Choose Bonjour Gateway 🔹	
	Status LEDs 🔲 Override Group Config 📄 Disable Status LEDs	
	PoE Operating Mode Override Group Config Auto	
R		
1		
		OK Cancel
		on ounder

## **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 209 Renaming an AP

	Traffic: 0.03 MB			
Clients	Clients			3 Disconnected 0
	d4:c1:9e:35:c9:40) adio 2.4 GHz Radio 5.0 GHz	etwork Other		×
	* MAC Address d4:c1 * Device Name R610			1
5	Description Location GPS Coordinates	Longitude:		
R	(examp	37.3881398,-122.0258633)	ок	Cancel
1 0 0 S Clients	5G Traffic	Client Status for last 1 hours		

# **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 210 Set View Mode to AP Group

Access Points	Total	3 Working 3 Disconnected 0
Edit Restart Remove		Data duration 1 hour •
Summary - Total 3 Access Pointss	Summary	
Clients Traffic	3 Access Point(s) connected, 0 Access Point(s) disconnected.	
Master Unleashe[35:c9:40]	Mesh Status :Enabled	Show Mesh Topology
1 0 0 2 2.4G Clients Traffic	2 Client(s)	Show Client(s) Info
Mesh RuckusAP[1c:12:c0]	Client Status for last 1 hour	
2 0 0 0 2.4G 5G Clients Traffic	Excellent 🗾 Moderate 📟 Poo	۲

## **Viewing AP Group Members**

Select an AP group to view details on all APs that are members of the AP group.

To view AP group membership:

1. Go to Access Points and click the Group View button.

You can view details of each member of the AP group, including its MAC address, IP address, Device Name, Model number, Status, Mesh Mode, Channel, and Serial Number.

2. In the AP table, click on the MAC address of the AP to view the AP detail page of each AP.

#### NOTE

By default, only AP group view is displayed if there are more than 25 APs in the network.

#### FIGURE 211 Viewing Members of an AP Group

G	Access Points								Total	1 Working	1 Disconnected 0	•
	Create Edit Remove										Data duration: 1 hour	
	Summary - 2 AP Groups		APs Total 1			Sys	tem Default				Hide Access Points 💌	
1	System Default		Mac Address	IP Address	Device Name	Mo	del	Status		Q Search Mesh Mode	•	
	Clients Traffic		94:16:65:14:c8:51	10.106.0.1	AP_aa:bb:cc:dd:	ee:ff r71	D	Connected		Disabled 1-1 of 1 sl	11 (11b/g/n-	
2	test1 0 0 0 Clients Traffic	((t-	WLANS Total 3							Q Search	Hide WLANs Info 🔻	
			Name	ESSID	Authentication	Encryption	Description					
			123	123	open	none	123					
			test	test	open	wpa23-mixed	test					
			_SeanSeantest1	_SeanSeantest1	open	wpa2	_SeanSeantest1					
										1-3 of 3 sl	nown < 1 >	
		<u>.</u>	Clients Total 0								Hide Clients Info 🔻	
										Q Search	•	

### 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.

Access Points				Total 3	Working 3	Disconnected 0	▼
Create Edit Remove 🛅 🗗					Data duration	1 hour 🔻	
Summary - Total 1 AP Group		Syster	n Default				
	3 AP(s)				Hide Access	Point	
System Default				Search	Q	٥	
	Mac Address	IP Address	Device Name		Status		
Clients Traffic	f0:b0:52:1c:12:c0	192.168.0.17	RuckusAP		Connected (Mesh	n AP, 1	
	d4:c1:9e:35:c9:40	192.168.0.4	Unleashed		Connected (Root	AP)	
	f0:b0:52:1b:f0:40	192.168.0.9	RuckusAP		Connected (Mesh	1 AP, 1	
				1-3 of	3 shown < 1	2	

FIGURE 212 Clicking Edit to Configure the AP Group

The Edit AP Group form appears.

- 3. Assign APs to or from this AP group using the left and right arrows on the AP Assign tab.
- 4. Assign WLANs to or from this AP group using the left and right arrows on the WLAN Assign tab.

.

- 5. On the *Radio B/G/N* (2.4*G*) and *Radio A/N/AC* (5*G*) tabs, modify any of the following settings that you want to apply to the System Default AP group.
  - Channel Range: To limit the available channels for 2.4 GHz, 5 GHz Indoor and 5 GHz Outdoor channel selection, deselect any channels that you do not want the APs to use.

NOTE

For country codes "US", "UK", and "JP", channel 144 is supported if DFS channel is enabled.

- **Channelization**: Select Auto, 20MHz or 40MHz channel width for the 2.4 GHz radio, or Auto, 20, 40, or 80 MHz channel width for the 5 GHz radio.
- **Channel**: Select Auto or manually assign a channel for the 2.4 GHz or 5 GHz radio.
- **TX Power**: Allows you to manually set the transmit power on all 2.4 GHz or 5 GHz radios (default is Auto).

Max = max allowable Tx power according to country regulations

Min = 0dBm per chain for 11n APs, 2dBm per chain for 11ac APs

- Call Admission Control: (Disabled by default). Enable Wi-Fi Multimedia Admission Control (WMM-AC) to support Polycom/ Spectralink VIEW certification.
- WLAN Service: This option allows users to disable WLAN service on the 2.4 or 5 GHz radios on all APs in the AP group.
- Protection Mode: If you activate Protection Mode, you control how 802.11 devices know when they should communicate with another device. The use of RTS/CTS (Request to Send/Clear to Send) reduces collisions and increases the performance of the network if hidden stations are present. However, RTS/CTS (and CTS-only) introduce overhead and may in fact reduce overall performance in some situations. Through the proper use of RTS/CTS and CTS-only, you can fine-tune the operation of your wireless LAN depending on the physical operating environment.
  - **CTS-only**: Choose this option to force all destination devices to acknowledge their ability to receive data when a transmission is initiated. Use this option for compliance with the Wi-Fi Alliance certification.
  - RTS/CTS: Choose this option to force both sending and receiving devices to confirm a data exchange on both ends before proceeding.
  - None: Choose this option to disable both RTS and CTS acknowledgment.
- 6. On the Other tab, modify settings for all APs of a specific model in the System Default AP group. For more information on model-specific controls, see Modifying Model Specific Controls on page 297.
  - 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 499.
    - Port Setting: Refer to Configuring AP Ethernet Ports on page 321 for more information on configuring AP-specific Ethernet port settings.

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

#### FIGURE 213 Configuring AP Group Settings

Edit AP Grou	р								
* Name	System Default								
Radio (2.4G)	Radio (5G) Other								
	Radio 2.4 GHz	<b>1</b> 2	<b>v</b> 3	4 🖬 5	67	8 2	9 🗹 10	✓ 11	
	Channelization	Auto	$\checkmark$						
	Channel	Auto	$\checkmark$						
	TX Power	Auto	$\sim$						
Ca	all Admission Control	Off		~					
	WLAN Service	Disable	$\sim$						
	Protection Mode	RTS/CTS	~						

## **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 214 Creating a New AP Group

Access Points		Total 3 Working 3 Disconnected 0
Create Edit Remove		Data duration 1 hour •
Summary - Total 1 AP Group	Summary	
0 0 2 Clients Traffic	3 Access Point(s) connected, 0 Access Point(s) disconnected.	
System Default	Mesh Status :Enabled	Show Mesh Topology
Clients Traffic	2 Client(s)	Show Client(s) Info
	Client Status for last 1 hour	
	Excellent Moderate	Poor
	5	

The Create AP Group form appears.

- 2. Assign APs to or from this AP group using the left and right arrows on the Step 1 Assign APs screen.
- 3. Assign WLANs to or from this AP group using the left and right arrows on the Step 2 Assign WLANs screen.

- 4. On the Radio B/G/N (2.4G) and Radio A/N/AC (5G) tabs, modify any of the following settings that you want to apply to the group:
  - **Channel Range**: To limit the available channels for 2.4 GHz, 5 GHz Indoor and 5 GHz Outdoor channel selection, deselect any channels that you do not want the APs to use.
  - Channelization: Select Auto, 20MHz or 40MHz channel width for the 2.4 GHz radio, or Auto, 20, 40, or 80 MHz channel width for the 5 GHz radio.
  - **Channel**: Select Auto or manually assign a channel for the 2.4 GHz or 5 GHz radio.
  - TX Power: Allows you to manually set the transmit power on all 2.4 GHz or 5 GHz radios (default is Auto).

Max = max allowable Tx power according to country regulations

Min = 0dBm per chain for 11n APs, 2dBm per chain for 11ac APs

- Call Admission Control: (Disabled by default). Enable Wi-Fi Multimedia Admission Control (WMM-AC) to support Polycom/ Spectralink VIEW certification.
- WLAN Service: This option allows users to disable WLAN service on the 2.4 or 5 GHz radios on all APs in the AP group.
- Protection Mode: Protection Mode allows control over how 802.11 devices know when they should communicate with another device. The use of RTS/CTS (Request to Send/Clear to Send) reduces collisions and increases the performance of the network if hidden stations are present. However, RTS/CTS (and CTS-only) introduce overhead and may in fact reduce overall performance in some situations. Through the proper use of RTS/CTS and CTS-only, you can fine-tune the operation of your wireless LAN depending on the physical operating environment.
  - **CTS-only**: Choose this option to force all destination devices to acknowledge their ability to receive data when a transmission is initiated. Use this option for compliance with the Wi-Fi Alliance certification.
  - **RTS/CTS**: Choose this option to force both sending and receiving devices to confirm a data exchange on both ends before proceeding.
  - None: Choose this option to disable both RTS and CTS acknowledgment.

- 5. On the Other tab, modify any of the following settings that you want to apply to the System Default AP group:
  - Model Specific Control: Select the AP model to which the settings will apply. For more information, see Modifying Model Specific Controls.
  - Max Clients: Set the maximum number of clients that can associate per AP. Note that different AP models have different maximum client limitations.
  - Status LEDs: When managed by ZoneDirector, you can disable the external LEDs on certain AP models. This can be useful if your APs are installed in a public location and you don't want to draw attention to them.
  - **PoE Operating Mode**: Options vary depending on AP model selected in Model Specific Control. For a list of PoE operating modes by AP model, refer to *Unleashed Access Point Power Supply Considerations*.
  - Port Setting: Refer to Configuring AP Ethernet Ports for more information on configuring AP-specific Ethernet port settings.

#### FIGURE 215 Create new AP group

			×
Create AP Group	Step 1-Assign APs Select the APs that need to be part of this	AP group.	
* Name	AP Group 2		
Select APs			
	Available APs from System Default	Selected APs for this Group	
	search here Q	[search here Q]	
	Unleashed (d4:c1:9e:35:c9:40)	✗ RuckusAP (f0:b0:52:1c:12:c0)	
	RuckusAP (f0:b0:52:1b:f0:40)		
		<b>•</b>	

### **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 216 Model Specific Controls

	Edit AP Group	×	ſ
	* Name System Default		
1	AP Assign WLAN Assign Radio B/G/N(2.4G) Radio A/N/AC(5G) Other Model Specific Control H320  Max Clients Allow Max 100 clients to associate with this AP Status LEDs Disable Status LEDs		
	Port Setting Edit Port Setting		

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 321 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 499.

#### FIGURE 217 PoE Operating Mode

	* Name System Default		•
	Radio B/G/N(2.4G) Radio A/N/AC(5G)	Other	
1	Model Specific Control	R720 •	
	Max Clients	Allow Max 100 clients to associate with this AP	
	Status LEDs	Disable Status LEDs	
	PoE Operating Mode	802.3at+ PoE 🔻	
2		Auto	
~		802.3af PoE	
		802.3at PoE	
		802.3at+ PoE	
0			
3			
			-

### **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 218 Configuring AP Ethernet Ports - H510

	Radio (2.4G) Radio (5G) Othe	er			
					A
_	Model Specific Cont	trol H510 v			
	Max Clie	Allow Max 100 clients to	associate with this AP		
	Status LE	Disable Status LEDs			
	Port Sett	ting			
	Port Enable DHCP_Opt82	Туре	VLA	AN	
-	LAN1 🖉 🗌	Trunk Port • Untag ID 1	Members 1-4094 Gues	st VLAN Enable Dynamic VLAN	Disable
	LAN2 🕑 🔲	Trunk Port   Untag ID  1	Members 1-4094 Gues	st VLAN Enable Dynamic VLAN	Disable
	LAN3 🕑 🗌	Trunk Port   Untag ID 1	Members 1-4094 Gues	st VLAN Enable Dynamic VLAN	Disable
	LAN4 🕑 🔲	Trunk Port   Untag ID 1	Members 1-4094 Gues	st VLAN Enable Dynamic VLAN	Disable
	LAN5 🥑 🗌	Trunk Port   Untag ID 1	Members 1-4094 Gues	st VLAN Enable Dynamic VLAN	Disable

#### FIGURE 219 Configuring AP Ethernet Ports - H350

Radio (2.4G) Radio (5G) Other											
Model Specific Control		~									
Max Clients Allow Max 100 clients to associate with this AP											
Status LEDs Disable Status LEDs											
Port Setting	Untag ID	Members	Guest VLAN	Rate Limiting Uplink	Rate Limiting Downlink	802.1x					
	4094	4094	5	5 v mbps	2 v mbps	Authenticator					
	1	1-4094		Disabled	Disabled	Supplicant					
	1	1-4094		2	Disabled	Disabled					
				3							
	•			5		•					
	,	Authenticat	ion Server te	st- i	~						
		Account	ing Server No	one	¥	•					

11. In Rate Limiting Uplink and Rate Limiting Downlink, select a value starting from 1 through 500 (Mbps).

#### NOTE

Memory type of 11ax and cypress is 500 Mbps, and other APs (QCA, dakota, mips) is 200 Mpbs.

NOTE

Rate Limit supports maximum of 100 clients per WLAN. If the number of clients is more than 100, it will run out of memory of AP.

- 12. In **802.1X**, select whether the port will be used as an 802.1X Supplicant, Authenticator (port-based or MAC-based), or whether 802.1X is disabled on the port. AP Ethernet ports can be individually configured to serve as either an 802.1X supplicant (authenticating the AP to an upstream authenticator switch port), or as an 802.1X authenticator (receiving 802.1X authentication requests from downstream supplicants). A single port cannot provide both supplicant and authenticator functionality at the same time.
  - Disabled: 802.1X authentication is disabled for this port.
  - **Supplicant**: This port authenticates itself to an upstream Authenticator port.
  - Authenticator (Port-Based): This port accepts auth requests from downstream stations. In Port-based mode, only a single MAC host must be authenticated for all hosts to be granted access to the network.
  - Authenticator (MAC-Based): This port accepts auth requests from downstream stations. In MAC-based mode, each MAC host is individually authenticated. Each newly-learned MAC address triggers an EAPOL request-identify frame.

For more information on port based 802.1X, see Using Port Based 802.1X.

13. In **Authenticator** (options appear if any port is configured as an Authenticator), select an **Authentication Server** and **Accounting Server** against which to authenticate clients from the drop-down list.

Optionally, **Enable MAC authentication bypass (Use device MAC address as username and password)** to allow specific devices to bypass 802.1X authentication.

- 14. In **Supplicant** (options appear if any port is configured as a Supplicant), select the supplicant authentication method:
  - MAC Address: Use the station's MAC address as the user name and password.
  - User Name and Password: Enter the login info for authenticating this supplicant port to an upstream authenticator port.

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

#### FIGURE 220 H510 Port Settings: Enable, DHCP Option 82, Port Type, and VLAN Untag ID

* Name	Syste	m Default								
Radio B/G/N(2.4G	) Radi	io A/N/AC(5G)	Other							
Mod	N S		H510  Allow Max 100 Disable Status		issociate	with this AP				l
Port		DHCP Opt82	Туре					VLAN		
LAN1	-		Access Port •	Untag ID	1	Members	1	Guest VLAN	Enable Dynamic VLAN	C .
LAN2	4		Access Port •	Untag ID	1	Members	1	Guest VLAN	Enable Dynamic VLAN	
LAN3	1		Access Port 🔹	Untag ID	1	Members	1	Guest VLAN	Enable Dynamic VLAN	C .
LAN4	4		Access Port 🔻	Untag ID	1	Members	1	Guest VLAN	Enable Dynamic VLAN	C
LAN5	1		Trunk Port 🔹	Untag ID	1	Members	1-4094	Guest VLAN	Enable Dynamic VLAN	C
Authenticator		tication Server	None  Acco	unting Serve Jse device N			ame and p	assword)		

FIGURE 221 H510 Port Settings: Guest VLAN, Dynamic VLAN and 802.1X

	* Name	System Defau	ılt								
Radi	io B/G/N(2.4G)	Radio A/N/A	C(5G)	Other							
		_									<b>^</b>
ol	H510	•									
ts	Allow Max 100	clients to a	ssociate v	with this AP							
Ds	Disable Status	LEDs									
	Disable Status	LEDS									
٦g	_	LEDs									L
	Туре	_		1		VLAN			802.1X		L
ng	Access Port	▼ Untag ID	1	Members	1	Guest VLAN	Enable Dynamic VLAN		Disabled	Ŧ	l
٦g	Туре	_	1	{	1	1	Enable Dynamic VLAN Enable Dynamic VLAN			<b>T</b>	l
٦g	Access Port	▼ Untag ID	<u> </u>	Members		Guest VLAN		- 4	Disabled	* * *	ļ
٦g	Access Port Access Port	▼ Untag ID ▼ Untag ID	<u> </u>	Members	1	Guest VLAN Guest VLAN	Enable Dynamic VLAN	4	Disabled Authenticator (Port-Based)	_	ļ
ng	Access Port Access Port Access Port	▼ Untag ID ▼ Untag ID ▼ Untag ID	<u> </u>	Members Members Members	1	Guest VLAN Guest VLAN Guest VLAN	Enable Dynamic VLAN Enable Dynamic VLAN	     	Disabled Authenticator (Port-Based) Authenticator (MAC-Based)	_	ł
ng Opt82	Access Port Access Port Access Port Access Port Access Port Trunk Port	Untag ID Untag ID Untag ID Untag ID Untag ID Untag ID	1 1 1 1	Members Members Members Members	1 1 1	Guest VLAN Guest VLAN Guest VLAN Guest VLAN	Enable Dynamic VLAN Enable Dynamic VLAN Enable Dynamic VLAN	     	Disabled Authenticator (Port-Based) Authenticator (MAC-Based) Authenticator (MAC-Based)	_	

#### FIGURE 222 H510 Authenticator and Supplicant Settings

-			
1	* Name	System Default	
	Radio B/G/N(2.4G)	Radio A/N/AC(5G) Other	
	LAIN4 LAN5	Access Port      Untag ID      Members     Guest VLAN     Enable Dynamic VLAN     Trunk Port     Untag ID     Members     1-4094     Guest VLAN     Enable Dynamic VLAN	
	Authenticator	Authentication Server None  Accounting Server None  Ac	
	Supplicant	MAC Address (Use MAC Address of AP as User Name and Password)     User Name     Password	
	Marine Cer	PORT 2	

## **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 frontbottom ports are enabled as Access Ports by default, and whose rear port is a Trunk Port and is non-configurable).

If configured as an Access Port, all untagged ingress traffic is sent to the configured Untag VLAN, and all egress traffic is sent untagged. If configured as a Trunk Port, all untagged ingress traffic is the configured Untag VLAN (by default, 1), and all VLAN-tagged traffic on VLANs 1-4094 will be seen when present on the network.

The default Untag VLAN for each port is VLAN 1. Change the Untag VLAN to:

- Segment all ingress traffic on this Access Port to a specific VLAN
- Redefine the Native VLAN on this Trunk Port to match your network configuration

### Trunk Ports

Trunk links are required to pass VLAN information between switches. Trunking is a function that must be enabled on both sides of a link. If two switches are connected together, for example, both switch ports must be configured as trunk ports. The Trunk port is a member of all the VLANs that exist on the AP/switch and carries traffic for all VLANs between switches.

For a Trunk port, the VLAN Untag ID field is used to define the native VLAN - the VLAN into which untagged ingress packets are placed upon arrival. If your network uses a different VLAN as the native VLAN, configure the AP Trunk port's VLAN Untag ID with the native VLAN used throughout your network.

#### **Access Ports**

Access ports provide access to the network and can be configured as members of a specific VLAN, thereby separating the traffic on these ports from traffic on other VLANs.

All Access Ports are set to Untag (native) VLAN 1 by default. This means that all Access Ports belong to the native VLAN and are all part of a single broadcast domain. When untagged frames from a client arrive at an AP's Access Port, they are given an 802.1Q VLAN header with "1" as their VLAN ID before being passed onto the wired network.

When VLAN 1 traffic arrives destined for the client, the VLAN tag is removed and it is sent as plain (untagged) 802.11 traffic. When any tagged traffic other than VLAN 1 traffic arrives at the same Access Port, it is dropped rather than forwarded to the client.

To remove ports from the native VLAN and assign them to specific VLANs, select Access Portand enter any valid VLAN ID in the VLAN IDfield (valid VLAN IDs are 2-4094).

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

#### TABLE 33 Access Ports with VLANs configured

VLAN Settings	Incoming Traffic (from the client)	Outgoing Traffic (to the client)
Access Port, Untag VLAN 1	All incoming traffic is native VLAN (VLAN 1).	All outgoing traffic on the port is sent untagged.
Access Port, Untag VLAN [2-4094]	All incoming traffic is sent to the VLANs specified.	Only traffic belonging to the specified VLAN is forwarded. All other VLAN traffic is dropped.

#### **General Ports**

General ports are user-defined ports that can have any combination of up to 20 VLAN IDs assigned. General ports function similarly to Trunk ports, except that where Trunk ports pass all VLAN traffic, General ports pass only the VLAN traffic that is defined by the user.

To configure an AP Ethernet port as a General port, select General Port and enter multiple valid VLAN IDs separated by commas or a range separated by a hyphen.

#### NOTE

You must also include the Untag (native) VLAN ID in the Members field when defining the VLANs that a General port will pass. For example, if you enter 1 as the Untag VLAN ID and want the port to pass traffic on VLANs 200 and 300, you would enter: **1,200,300**.

### Using Port Based 802.1X

802.1X authentication provides the ability to secure the network and optionally bind service policies for an authenticated user.

## NOTE

802.1X port settings are unavailable when mesh mode is enabled.

802.1X provides logical port control and leverages the EAP authentication and RADIUS protocols to allow the network policy to be effectively applied in real time, no matter where the user connects to the network.

AP Ethernet ports can be individually configured to serve as either an 802.1X supplicant (authenticating the AP to an upstream authenticator switch port), or as an 802.1X authenticator (receiving 802.1X authentication requests from downstream supplicants). A single port cannot provide both supplicant and authenticator functionality at the same time.

If port based 802.1X is enabled on any ports, you can monitor connected wired clients by expanding the **Clients** Dashboard component and clicking **Wired Clients** to display a list of authenticated 802.1X wired clients.

#### FIGURE 223 Monitor currently connected 802.1X wired clients

	WiFi Networks	Traffic: 0.09 MB			Total 1	Working 1	Disabled 0	•
	Clients				Total 1	Connected 1	Disconnected 0	•
1 clients co	onnected, 0 clients disconn	Clients						
Wired	Clients 0 w	rired clients connected					▼	
This table	e lists all currently connecte	d 802.1X wired client devices. O	only those devices with a status of "a	uthorized" are permi	tted access to the	network.		
Show de					Sea	irch	Q 2 0	
Mac Ad	ddress User/IP		Access Point	VLAN		Status	;	
			No data available.					
						0-0 of 0 show	n « 1 »	
Wirele	ess Clients 1 w	vireless 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 224 Click Restart to reboot a single AP

6	Access Points		Total 4 Working 3 Disconnected
1	Edit Restart Remove 🧮 🗗		Data duration 1 hour
	Summary - Total 4 Access Points	RuckusAP [f0:	b0:52:1c:12:c0]
	Clients Traffic	0 Clients	Show Clients Info
	Master Unleashe[35:c9:40]	2 WLANS	Show WLANs Info
1	0 0 3 2.4G 5G Clients Traffic	Client Status for last 1 hour	Show System Overview Info
ſ	RuckusAP[1c:12:c0]	Excellent	Moderate Poor
2	0 0 0 2.4G 5G Clients Traffic	5	

#### 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 225 Removing an AP

6	Access Points	Total 4 Working 3 Disconnected
1	Edit Restart Remove 🗮 🗗	Data duration 1 hour
	Summary - Total 4 Access Points	RuckusAP [f0:b0:52:1c:12:c0]
	Clients Traffic	0 Clients Show Clients Info
	Master Unleashe[35:c9:40]	Image: Show WLANs Info
1	0 0 3 2.4G 5G Clients Traffic	Show System Overview Info
ſ	Mesh	Excellent Moderate Poor
2	RuckusAP[1c:12:c0]	5
l	Clients Traffic	3

# **ICX Switch Management**

•	ICX Switch Management Overview	. 331
	Preparing an ICX Switch for Unleashed Management	
	Approving a New Switch to Join Unleashed	
	Monitoring Connected ICX Switches	
•	Managing Switch Ports	340
	Backup and Restore Switch Configuration	
	Ungrading ICX Switch Firmware	

## **ICX Switch Management Overview**

Beginning with Unleashed release 200.8, the administrator can monitor and manage Ruckus ICX switches and routers in the ICX 7000 series and above. Unleashed can manage up to 8 switches at a time.

ICX switch management allows you to monitor status, view usage statistics, and perform basic management operations including configuration backup and firmware management.

The following capabilities are supported:

- ICX switch registration and authentication
- Switch inventory (including model, firmware version, and last backup)
- Health and performance monitoring (status, traffic stats, errors, clients) with alarms
- Switch configuration file backup and restore
- Firmware upgrades

## **Requirements**

#### NOTE

For more information on ICX device capabilities and configuration, refer to the Ruckus FastIron documentation set available at the following URL:

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

The following items are required to manage ICX devices:

- The ICX switch must be running FastIron software version 08.0.90 or higher.
- The Unleashed Master AP's IP address must be reachable by the ICX device through the Management interface or through router interfaces.
- ICX devices will be automatically discovered by the Unleashed Master. If automatic switch approval is enabled, all ICX switches discovered on the network will be listed in the Switches dashboard component. To disable automatic approval, go to Admin & Services > System > System Info > Switch Approval and disable the Approval option.

ICX devices running either router or switch images can be managed by Unleashed.

#### **ICX Switch Management**

Preparing an ICX Switch for Unleashed Management

#### FIGURE 226 Switch auto approval

🛄 System	•	System Info
System Info		Name* Ruckus-Unleashed
IP Settings		System Version 200.8.10.3.94
-		Unleashed ID un9418490011251563205223! Generate
System Time		Apply
Country Code		Preferred Master
Roles		Preferred Master No Preference
Users		Upon applying this change, the selected AP will become a Master AP if it's not a Master AP currently and the previous Master AP will be rebooted to become a Member AP. As a result,
Mesh		there may be a brief network disruption.
		Apply
		Switch Approval
Services		Approval <i>A</i> utomatically approve all join requests from switchs.
		Apply

## **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@ICX7	150-C12-Switch#s	how lldp neighbo	rs	
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@ICX7	150-C12-Switch#			

9. Additionally, you can verify whether the AP can receive LLDP information from its neighbors using the AP CLI. To check the AP's LLDP info, use the following command:

```
ruckus(ap-mode)# get lldp neighbors
    _____
LLDP neighbors:
      _____
Interface: eth0, via: LLDP, RID: 1, Time: 3 days, 02:55:58
 Chassis:
   ChassisID: mac 78:a6:e1:2e:03:ce
             ICX7150-C12-Switch
Not received
   SysName:
   SysDescr:
   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: yesAdv:100Base-TX, HD: yes, FD: yesAdv:100Base-TX, HD: yes, FD: yesAdv: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.

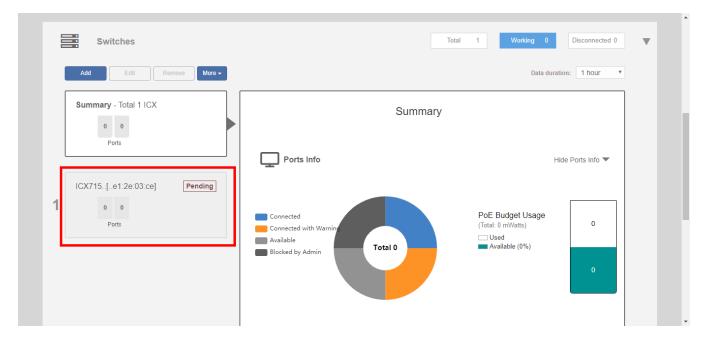
## **Approving a New Switch to Join Unleashed**

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 227 Select a switch that is pending approval



#### NOTE

RUCKUS Unleashed does not recognize older versions of ICX switches and displays the following warning message: "Unleashed system only supports ICX firmware version 08.0.90 or later."

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

## FIGURE 228 Click Approve

Switches	Total 1 Working 0 Disconnected 0
Add Edit Remove More +	Data duration: 1 hour
Summary - Total 1 ICX	* Unleashed system only supports ICX firmware version 06.0.90 or later.
0 0	ICX Switch is Pending to join
Ports	Device Name: ICX7150-C12-Switch
ICX715[e1:2e:03:ce] Pending	MAC Address: 78:a6:e1:2e:03:ce
	IP Address: 192.168.0.24
Ports	Pending for approval.

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.

	Switches	Total 1 Working 0 Disconnected 0	T
	Add Edit Remove More -	Data duration: 1 hour	
	0 0 Ports	ICX Switch is Pending to join	
		Device Name: ICX7150-C12-Switch	
1	ICX715[e1:2e:03:ce] Pending	MAC Address: 78:a6:e1:2e:03:ce IP Address: 192.168.0.24 Unable to login to this switch with default credential, please provide admin user	
	Ports	name & password of this switch to continue	

FIGURE 229 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 230 Enter admin user name and password for switch authentication

Add Edit Remove M	ve •	Data duration: 1 hour •
Summary - Total 1 ICX	Approve Switch Join Unleashed	join
	Admin Name admin Password Ø	
ICX715[e1:2e:03:ce] Pendin	OK Cancel	
Ports	Continue	se provide admin user nue

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 231 ICX switch connecting

Switches	Total 1 Working 0 Disconnected 0	▼
Add Edit Remove More	Data duration: 1 hour	
Summary - Total 1 ICX	* Unleashed system only supports ICX firmware version 08.0.90 or later.	
0 0 Ports	ICX Switch is Connecting	
	MAC Address: 00:00:00:00:00	
ICX715[00:00:00] Connecting	IP Address: 192.168.0.24	
1 0 0 Ports	Name: ICX7150-C12-Switch	

## **Monitoring Connected ICX Switches**

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

The following details are displayed when the links are expanded:

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

#### FIGURE 232 Selecting a Switch to Monitor Details

Switches	Total 3 Working 1 Disconnected 0	▼
Add Edit Remove	Data duration: 1 hours 🔻	
Summary - Total 3 ICX	ICX7150-24P-Switch [d4:c1:9e:45:16:e0] To manage the ICX switch click here.	
Stack [d4:c1:9e:45:16:e0] 4 82 Ports	Ports Info Show Ports Info  Kealth Show Health	
2 0 0 Ports	Events & Alarms Hide Events & Alarms	

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 233 Monitoring Switch Health Details

Ports	W Health	Hide Health 🔻
	20%	time: 11/26 10:55:10 avg: 1 %
	0% 11/26 10:20:34 11/26 10:30:30 11/26 10:40:22 11/26 10:50:14 11/2 Memory Usage: 42% 100% 80% 60%	6 11:00:06 11/26 11:09:58

Click Show Events & Alarms to expand the section and view switch event and alarm lists.

FIGURE 234 Viewing Switch Event and Alarm Lists

Frents & Alarms     Events & Alarms     Events & Alarms     Events & Alarms     Search     Q     Date/Time - Severity   Activities   202001/23 17:02:20   High   ICX [78:a6:e1:2e:03:ce] joins.     1:1 of 1 shown		1-1 of 1 shown
Events       Alarms         Search       Q         Date/Time -       Severity         Activities         2020/01/23       17:02:20         High       ICX [78:a6:e1:2e:03:ce] joins.	Health	Show Health
Date/Time ~         Severity         Activities           2020/01/23 17:02:20         High         ICX [78:a6:e1:2e:03:ce] joins.		Hide Events & Alarms 💌
2020/01/23 17:02:20 High ICX [78:a6:e1:2e:03:ce] joins.		Search Q 2
1-1 of 1 shown		
		1-1 of 1 shown

## Accessing the RUCKUS Switch Home Page

To access the RUCKUS switch home page from within Unleashed without manual login, click the **To manage the ICX switch, click here** link. Enter the user name and password, and click **Login** to log in to the RUCKUS switch home page.

### FIGURE 235 Logging In to the RUCKUS Switch Home Page

Ruckus Switch WebUI	
UserName	
Password	
	Login
	_
	_

NOTE

- Access to the RUCKUS switch home page is supported only for ICX firmware version 9.0.0 or later.
- Access to the RUCKUS switch home page redirection is available only when an ICX switch is connected.
- You can extend the available redirection window time. The standard available redirection window time is 10 minutes.

## **Managing Switch Ports**

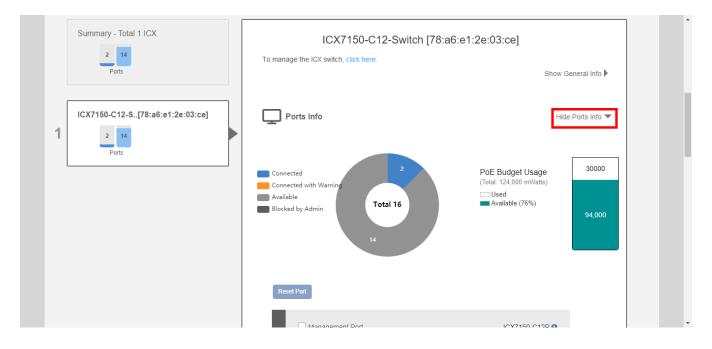
The "Ports Info" link expands to display information on overall switch status such as the number of ports used and available and PoE power budget usage. Individual switch ports can be managed by selecting the specific port from the switch port diagram or from the port list table below.

To manage ICX switch ports:

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

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

### FIGURE 236 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 237 Select a switch port to display details on that port

Reset Port				94,000	
Constant Port	11		(7150-C12P )		
Port Name GigabitEthernet1/1/1	MAC Address 78:a6:e1:2e:03:ce	Search Port Number 1/1/1	Hide Port Lis Q 2 Link Status down		

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

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

## FIGURE 238 Resetting a switch port

14 Reset Port				94,000	^
(automotion for the second sec			X7150-C12P 0		ľ
Port Name GigabitEthernet1/1/1	MAC Address 78:a6:e1:2e:03:ce	Search Port Number 1/1/1	Hide Port Lis Q 2 Link Status down		Ţ

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

FIGURE 239 Viewing a port's traffic statistics and LLDP neighbors

OK	OK		rx: 4.87G total: 257.8	) 900		
	11/26 09:26:18				) 11/26 1	
me Remote MAC Device Types Remote Port	lame	Remote MAC	Devi	ice Types	R	emote P
ckus-Unleashed d4:c1:9e:35:c9:40 bridge   wlanAccessPoint   eth0	Ruckus-Unleashed	d4:c1:9e:35:c9:4			Point   et	h0

## **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 240 Backup Switch Configuration

Switches		Total 1 Working 1 Disconnected 0
Add Edit Remove More -		Data duration: 1 hour
Summary - Total 1 ICX Back up Restore	ICX7150-C12-Switch [78:	a6:e1:2e:03:ce]
2 14 Ports ICX7150-C12-S[78:a6:e1:2e:03:ce] 2 14	To manage the ICX switch, click here.	Show General Info ► Hide Ports Info ▼
Ports	Connected Connected with Warning Available Blocked by Admin	PoE Budget Usage (Total: 124,000 mWatts) Used Available (75%) 94,000

- 3. When finished, the backup file is created as a .txt file that can be saved to your local computer.
- 4. Save the backup file to a convenient location.

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

#### Disconnected 0 Switches Total 1 More 🗸 Data duration: 1 hour Ŧ Upgrade Summary - Total 1 ICX Back up ICX7150-C12-Switch [78:a6:e1:2e:03:ce] Restore վհղ 2 14 To manage the ICX switch, click here. Ports Show General Info 🕨 ICX7150-C12-S..[78:a6:e1:2e:03:ce] Ports Info Hide Ports Info 🔻 1 2 30000 PoE Budget Usage (Total: 124,000 mWatts) Connected Connected with Warn Used Available (76%) Available Total 16 Blocked by Admin 94,000

FIGURE 241 Restore Switch Configuration

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

FIGURE 242 Restore Configuration from Backup File

Switches	Total 1 Working 1 Disconnected 0
Add Edit Remove	More - Data duration: 1 hour •
Summary - Total 1 ICX	Restore X
2 14 Ports	Local File Name icx_config_mac_78a6e12e03ce_20191101_155955.bt (775 bytes) Cancel Show General Info I
ICX7150-C12-S[78:a6:e1:2e:/	
1 2 14	Restore     Cancel
Ports	Connected 2 PoE Budget Usage 30000
	Connected with Warning (Total: 124,000 mWatts) Available Used Blocked by Admin Total 16 Available (76%)
	94,000

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 243 Switch Restore Warning

			7
		Data duration: 1 hour •	
Summary - Total 1 ICX Res	?	¥ ;e] zel Show General Info ▶	
ICX7150-C12-S[78:a6:e1:2e:1	Please note that Master AP currently connects to this ICX switch, restore this switch may cause a power outage in the Unleashed network, are you sure want to continue?	Hide Ports Info 💌	
	Yes No Connected with Warning Available Blocked by Admin	PoE Budget Usage (Totat: 124,000 mWatts) Used Available (76%) 94,000	

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

### FIGURE 244 Switch Restore in Process

Switches	Total 1 Working 1 Disconnected 0
Add Edit Remove More -	Data duration: 1 hour •
Summary - Total 1 ICX	* Unleashed system only supports ICX firmware version 06.0.90 or later.
2 14 Ports	ICX Switch is Restoring
	Device Name: ICX7150-C12-Switch
ICX715[e1:2e:03:ce] Restoring	MAC Address: 78:a6:e1:2e:03:ce
1 2 14	IP Address: 192.168.0.24
Ports	This ICX switch is restoring, and the Unleashed network may reboot and go
FUIS	temporarily out of service during this period.It may take at least 10 minutes. Please DO NOT power off or reboot the switch.

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 245 Rebuilding Unleashed Network

Rebuilding the Unleashed Network. It may take a few minutes. WARNING - Do not power off or reboot the AP. - Do not refresh your browser or hit the browser's back button.
WARNING - Do not power off or reboot the AP.
- Do not power off or reboot the AP.

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 246 Upgrading an ICX switch

Access Points		Total 1 Working 1 Disconnected 0
Switches	9 More -	Total 1 Working 1 Disconnected 0  Data duration: 1 hour
Summary - Total 1 ICX	Upgrade Back up	
2 14	Restore ICX7150-C12-S	Switch [78:a6:e1:2e:03:ce]
Ports		Show General Info 🕨
ICX7150-C12-S[78:a6:e1:2e:	03:ce] Dorts Info	Hide Ports Info 💌
1 2 14 Ports		
	Connected	2 PoE Budget Usage 30000

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

## FIGURE 247 Choose upgrade image file

	Upgrade	×	
Switches	Local File Name Choose File No file choosen	Data duration:	•
Summary - Total 1 ICX			
2 14 Ports		Cancel Show General Info 🕨	
ICX7150-C12-S[78:a6:e1:2e:0	13:ce] Ports Info	Hide Ports Info ▼	

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

### FIGURE 248 Upgrade warning message

Add Edit Remove	Jpg L	Working 1 Disconnected 0 Data duration: 1 hour •
	Please note that Master AP currently connects to this ICX switch, upgrade this switch may cause a power outage in the Unleashed network, are you sure want to continue?	e]
	Yes No	Show General Info 🕨
	Ports Info	Hide Ports Info 🔻

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

#### FIGURE 249 Verify switch version

Add Edit Remove More - Summary - Total 1 ICX	ICX7150-C12-Sw To manage the ICX switch, click here.	vitch [78:a6:e1:2e:03:ce]	
	Name	ICX7150-C12-Switch	
ICX7150-C12-S[78:a6:e1:2e:03:ce]	MAC Address	78:a6:e1:2e:03:ce	
2 14	IP Address	192.168.0.24	
Ports	Model	ICX7150-C12P	
	State	Connected	
	Gateway	192.168.0.1	
	Version	SPS08091	
	Serial Number	FEK3231N175	
	Last Seen	2019/11/01 12:50:52	
	Up Time	1h 32m	

# **Working with Clients**

•	Client Management Overview	349
•	Viewing the Clients List	
•	Renaming a Client	351
•	Deleting a Client	353
•	Permanently Blocking a Client Device	353
•	Marking a Client as a Favorite	354
•	Running a SpeedFlex Performance Test on a Wireless Client	355
•	Client Connection Troubleshooting	359
•	Marking a Client as a Legacy Device	361
•	Adding User Accounts to the Internal User Database	361
•	Authenticating Clients Using an External Database	362

## **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 250 Viewing the currently connected Clients list

	Hame: 0.14 MB					
Clients	Clients			Total 3	Connected 3	sconnected 0
3 clients connected, 0 clients d	isconnected.					
Wired Clients	0 wired clients connected					•
Wireless Clients	3 wireless clients connected					▼
Show details Rename 🖈	Mark Favorite 🔒 🖈 Unmark Favorite	Troubleshooting More -		Search	Q	<b>2 ◊</b>
★ Mac Address	IP Address OS	Name	User	AP Name	WLAN	s
64:a2:f9:bc:cb:53	192.168.0.13	OnePlus_6T		Unleashed	Unleashed	E
f0:03:8c:fb:73:38	192.168.0.11 N/A			Unleashed	Unleashed	E
04:b1:67:47:c4:20	192.168.0.8			RuckusAP	Unleashed	E
					1-3 of 3 shown	1 >
						-

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 251 Click Show Details to view client details

Clients	Clients			Total 3	Connected 3	isconnected 0
3 clients connected, 0 clients dis	sconnected.					
Wired Clients	0 wired clients connected					
Wireless Clients	3 wireless clients connected					▼
Show details Rename 🔺 N	Mark Favorite 🗙 Unmark Favorite	Troubleshooting More -		Search	Q	<b>2 ♦</b>
★ Mac Address	IP Address OS	Name	User	AP Name	WLAN	s
64:a2:f9:bc:cb:53	192.168.0.13	OnePlus_6T		Unleashed	Unleashed	E
f0:03:8c:fb:73:38	192.168.0.11 N/A			Unleashed	Unleashed	Е
04:b1:67:47:c4:20	192.168.0.8			RuckusAP	Unleashed	E
					1-3 of 3 shown	( 1 )

## FIGURE 252 Viewing details on a specific client

Wireless Cli	lient Details		×
Show Details	Name	Value	Q 2 ¢
★ Mac.	Host Name	OnePlus6T	WLAN
c8:3a	OS Vendor Type	Android	eashed Unleast
0c:91	Device Model	Android	eashed Unleast
f0:03	IP Address	192.168.0.6	eashed Unleast
c0:ee	MAC	c0:ee:fb:55:a7:0f	eashed Unleast
	WLAN	Unleashed	
	AP Name	Ruckus-Unleashed	vn « 1 »
	AP MAC	d4:c1:9e:35:c9:40	
	Received from client	0 pkts / 0 bytes	
	Transmitted to client	0 pkts / 0 bytes	
Acces	RSSI	0 dBm	Disconnected 0
	SNR	0 dB	
	Health	Excellent	
Switch	BSSID	d4:c1:9e:35:c9:4c	Disconnected 0
	VIAN	1	

## **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 253 Rename a client

3 clients connected, 0 clients	disconnected.						
Wired Clients	0 wired clients connect	ed					•
Wireless Clients	3 wireless clients conne	ected					▼
Show details Rename	Mark Favorite 🔺 Unmark F	avorite Trouble	shooting More 🗸		Search	Q	2 🔷
* Mac Address	IP Address	os	Name	User	AP Name	WLAN	s
64:a2:f9:bc:cb:53	192.168.0.13	÷.	OnePlus_6T		Unleashed	Unleashed	E
f0:03:8c:fb:73:38	192.168.0.11	N/A			Unleashed	Unleashed	E
04:b1:67:47:c4:2	0 192.168.0.8	<b>.</b>			RuckusAP	Unleashed	E
						1-3 of 3 shown	« <b>1</b> »

The Rename Client dialog appears.

3. Enter the New Name, and click OK.

#### FIGURE 254 Enter new client name

3 clients connected, 0 clients o	0 wired clie	RenameClien	t	×			
	o wired clie	Renameonen	L	^			
	3 wireless c		I be reported in this page even if it is disc				▼
Show details Rename	Mark Favorite		ed. You can have up to 520 renamed clie set to original if apply the empty new nam			Q	0
★ Mac Address	IP Add	CurrentName:			ame	WLAN	s
64:a2:f9:bc:cb:53	192.168	* New Name: M	lyClientName		shed	Unleashed	E
f0:03:8c:fb:73:38	192.168				shed	Unleashed	
04:b1:67:47:c4:20	D 192.168				lsAP		
			ок	Cancel			_

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

FIGURE 255 New name appears in Host Name

3 clients connected, 0 clients dis-	connected.					
Wired Clients	0 wired clients connected					
Wireless Clients	3 wireless clients connected	t				▼
Show details Rename 🛉 M	iark Favorite 🛛 🚖 Unmark Favorit	e Troubleshooting More 🗸		Search	Q	2 0
★ Mac Address	IP Address C	DS Name	User	AP Name	WLAN	s
64:a2:f9:bc:cb:53	192.168.0.13	OnePlus_6T		Unleashed	Unleashed	E
f0:03:8c:fb:73:38	192.168.0.11 N	I/A		Unleashed	Unleashed	E
04:b1:67:47:c4:20	192.168.0.8	MyClientName		RuckusAP	Unleashed	E
					1-3 of 3 shown	1 >

.

## **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 256 Click the Delete button to temporarily delete a client. The client will be able to reconnect.

3 clients connected, 0 clients	disconnected.						
Wired Clients	0 wired clients connect	ted					
Wireless Clients	3 wireless clients conr	nected					▼
Show details Rename	🕈 Mark Favorite 🔺 Unmark F	avorite	roubleshooting More -		Search	Q	2 0
* Mac Address	IP Address	os	Name Block	User	AP Name	WLAN	s
64:a2:f9:bc:cb:5	3 192.168.0.13		OnePlus Speed Test		Unleashed	Unleashed	E
f0:03:8c:fb:73:38	3 192.168.0.11	N/A	Delete		Unleashed	Unleashed	E
04:b1:67:47:c4:2	20 192.168.0.8	-	MyClient		RuckusAP	Unleashed	E
						1-3 of 3 shown	1 >

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 353.

## **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.

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 257 Block a client to permanently prevent it from joining your network(s)

3 clients connected, 0 clients of								
Wired Clients	0 wired clients connecte	a						
Wireless Clients	3 wireless clients connect	cted						▼
Show details Rename	Mark Favorite 🛛 🖈 Unmark Fav	vorite	Troubleshooting	More 🗸		Search	Q	<b>2</b> •
★ Mac Address	IP Address	os	Name	Block	User	AP Name	WLAN	s
64:a2:f9:bc:cb:53	3 192.168.0.13	<b>.</b>	OnePlus			Unleashed	Unleashed	E
f0:03:8c:fb:73:38	192.168.0.11	N/A		Delete		Unleashed	Unleashed	E
04:b1:67:47:c4:20	0 192.168.0.8	<b>.</b>	MyClient			RuckusAP	Unleashed	E
								x <b>1</b> »

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 258 Mark Favorite

Clients	Clients				Total 3	Connected 3	Disconnected 0
3 clients connected, 0 clients disc	onnected.						
Wired Clients	0 wired clients connect	ted					•
Wireless Clients	3 wireless clients conn	ected					▼
Show details Rename 🖌 🛉 Ma	rk Favorite 🛛 🚖 Unmark F	avorite Troubleshooti	ng More 🗸		Search		۹ ۵ ۹
* Mac Address	IP Address	OS Nam	e	User	AP Name	WLAN	s
64:a2:f9:bc:cb:53	192.168.0.13	n One	Plus_6T		Unleashed	Unleashed	E
f0:03:8c:fb:73:38	192.168.0.11	N/A			Unleashed	Unleashed	E
04:b1:67:47:c4:20	192.168.0.8	📫 MyC	lient		RuckusAP	Unleashed	E
						1-3 of 3 shown	< 1 >
							0

An alarm event will be generated each time this client goes online or offline.

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

You can test the wireless throughput to a client using the SpeedFlex tool.

To do so, you will need to install and run the SpeedFlex application on the client device.

1. Expand the **Clients** menu.

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

#### FIGURE 259 Select a client and click Speed Test

Clients	Clients				Total 3	Connected 3 Dia	sconnected 0
Wired Clients	0 wired clients conner	cted					
Wireless Clients	3 wireless clients con	nected					•
Show details 🛛 Rename 🛛 📌 M	ark Favorite 🔺 Unmark	Favorite	roubleshooting More -		Search	Q	<b>2</b>
★ Mac Address	IP Address	os	Name Block	User	AP Name	WLAN	s
64:a2:f9:bc:cb:53	192.168.0.13	÷	OnePlus Speed Test		Unleashed	Unleashed	E
f0:03:8c:fb:73:38	192.168.0.11	N/A	Delete		Unleashed	Unleashed	Е
04:b1:67:47:c4:20	192.168.0.8		MyClient		RuckusAP	Unleashed	E
						1-3 of 3 shown	1 >

- 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.

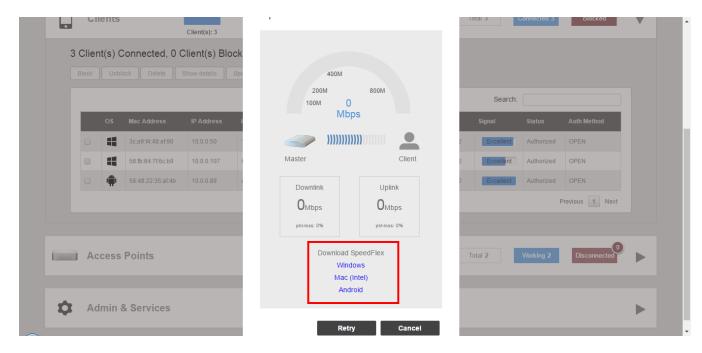
FIGURE 260 The client does not have SpeedFlex running

10.0.158 says:	×
The client[10.0.0.50] does not have SpeedFlex running. Click the OK button download the SpeedFlex application for the client's operating system, and then send it to the wireless client user for installation. Instruct the user to double-click SpeedFlex.exe to start the application. After SpeedFlex is installed and running on the client, run the SpeedFlex test again from the Unleashed Web interface.	
Prevent this page from creating additional dialogs.	
ОК	]

.

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

#### FIGURE 261 Download SpeedFlex



6. Install and run the application.

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

## FIGURE 262 Click Retry

3 Clie Block			Client(s) Bloc	 м	800M 0 bps					
				 Master	Client		Search			
	os	Mac Address	IP Address	master	Onerit		Signal	Status	Auth Method	
		3c:a9:f4:48:af:90	10.0.0.50	 Downlink	Uplink	2	Excellent	Authorized	OPEN	
		58:fb:84:7f:6c:b9	10.0.0.107	OMbps	OMbps	2	Excellent	Authorized	OPEN	
		58:48:22:35:af.4b	10.0.0.89	pkt-loss: 0%	pkt-loss: 0%	2	Excellent	Authorized	OPEN	
				Downloa	d SpeedFlex			F	Previous 1 Next	
		s Points		Ma	ndows c (Intel) idroid		al 2	Working 2	0	

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

### FIGURE 263 SpeedFlex results

	Connected, 0 (	Client(s): 3 Client(s) Block Show details Spe	80M 40M 20M 4 Mb		Total 3	Connected 3	Blocked	
OS	Mac Address	IP Address H	Master	Client	Search	h: Status	Auth Method	
		10.0.50	Downlink	Uplink	2 Excellent	Authorized	OPEN	
	58:fb:84:7f:6c:b9	10.0.0107	96 <sub>Mbps</sub>	4 <sub>Mbps</sub>	2 Excellent	Authorized	OPEN	
•	58:48:22:35:af:4b	10.0.89 a	pkt-loss: 2%	pkt-loss: 0%	2 Excellent	Authorized	OPEN	
							Previous 1 Next	

## **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 264 Click Troubleshooting to perform client connectivity trace

	TRATTIC: U.15 MIB		
Clients	Clients	Total 2	Connected 2 Disconnected 0
2 clients connected, 0 clients disco	onnected.		
Wired Clients	0 wired clients connected		•
Wireless Clients	2 wireless clients connected		▼
Show details Rename 🔺 Mar	k Favorite 🔹 Unmark Favorite Troubleshooting More	Sear	ch Q 2 0
★ Mac Address	IP Address OS Name	User AP Name	WLAN S
f0:03:8c:fb:73:38	192.168.0.2 N/A	Unleashed	Unleashed E
04:b1:67:47:c4:20	192.168.0.11 📫	RuckusAP	Unleashed E
			1-2 of 2 shown
Access Points		Total 3	Working 3 Disconnected 0

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 265 Click Start to begin connectivity trace

	Troubleshooting	×ed
3 Client(: Block	*Client MAC Address 3c:a9:f4:48:af:90 Please connect your client manually after start troubleshooting, if 1	c o
4	Connectivity Trace Start Stop Clear Limport Limport	
	ноголосно, голоо но, голого наронност сус	1-3 of 3 shown

### FIGURE 266 Connectivity trace in progress

Access Points hearing	client's probe requests	:				
Name	Radio	Client SNR (dBm)	Latency (ms)	Connection Failure (%)	Airtime Utilization (%)	
Ruckus-Unleashed	5GHz (36)	58	0	0.00	0	
RuckusAP	5GHz (36)	39	0	0.00	0	
RuckusAP	2.4GHz (1)	37	0	0.00	12	
Ruckus-Unleashed	2.4GHz (11)	92	0	0.00	3	۰
✓ 802.11 Disassoci	ation 9:56:46	Info 💽			1-4 of 4 shown < 1 >	
✓ 802.11 Disassoci AP: RuckusAP(f0:b0:52:					1-4 of 4 shown	
AP: RuckusAP(f0:b0:52:	1c:12:c0) <b>SSID:</b> Unleash ation Request 9:56:46	Radio: 5GHz	Unleas	AAA S	Time:9:56:46	
AP: RuckusAP(f0:b0:52:	1c:12:c0) <b>SSID:</b> Unleash ation Request 9:56:46	Clent	Unleashed	AAA Serrer		
<ul> <li>AP: RuckusAP(f0:b0:52:</li> <li>✓ 802.11 Authentic</li> <li>✓ 802.11 Authentic</li> </ul>	1c:12:c0) <b>SSID:</b> Unleash ation Request 9:56:46	Radio: 5GHz	Unleashed	AAA Server	Time:9:56:46	

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

# Marking a Client as a Legacy Device

Designating a wireless client as a legacy device provides a way to change a password, but allows original connected wireless devices to continue using the previous password. On a large-scale deployment, marking a wireless client as a legacy device is effective because the customer is not required to change the passwords on all the connected wireless devices.

Complete the following steps to mark a wireless client as a legacy device.

- 1. From the Unleashed dashboard, expand the Clients component.
- 2. Under Wireless Clients, select a client from the list and click Mark Legacy.

#### FIGURE 267 Marking a Client as a Legacy Device

	Mark Favorite Ma	rk Legacy Troubleshooting	More 🗸		
Favorite	Legacy Device	Mac Address	IP Address	Status	os
Yes	Yes	28:16:ad:b4:71:de	192.168.10.245	Authorized	
Yes	Yes	38:f9:d3:34:07:95	192.168.10.252	Authorized	Ś
Yes	Yes	34:36:3b:cd:eb:b0	192.168.10.250	Authorized	Ś
No	No	8e:3a:13:f0:05:7b	192.168.10.153	Authorized	Ś
No	Yes	7a:e2:d9:66:68:39	192.168.10.152	Authorized	÷.
Yes	Yes	24:11:45:b7:c2:92	192.168.10.164	Authorized	Ś
Yes	Yes	92:c6:e3:66:2d:ae		Disconnected	Ś
Yes	Yes	16:8f:0b:00:b0:9e		Disconnected	Ŵ
No	Yes	ca:50:f9:69:58:ca		Disconnected	N/A
No	Yes	96:76:53:3a:17:d4		Disconnected	N/A

The devices marked as legacy devices are allowed to connect to the WLAN with the previous password. For more information, refer to "Creating a New WLAN".

3. (Optional) Select a client and click **More** > **Unmark Legacy** to unmark the wireless client.

# **Adding User Accounts to the Internal User Database**

- 1. Go to Admin & Services > System > Users and click Create New.
- 2. Enter a User Name, optional Full Name, Password, Confirm Password, and select a Role for this user.

**Working with Clients** Authenticating Clients Using an External Database

3. Click **OK** to create the new user.

#### FIGURE 268 Creating a new User on the Internal User Database

<b>System</b>		ar Database (on Liniaashad)				
	Create New				so click the Print	
	* Username				Q 2	¢
	Full Name					
	* Password					
Users	* Confirm Password Role	Default •	+ /		IOWN « 1	
				ок	Cancel	
Services					_	

# **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 408.

# **Configuring Admin & Services Settings**

•	Admin & Services Overview	. 363
•	System Settings	.363
	Services	
•	Administration Settings	. 459

# **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 363
- Services on page 407
- Administration Settings on page 459

# **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 269 Click Admin & Services, and expand the System tab to configure system settings

🖵 System					
System Info	System		* Ruckus-Unleashed	]	
		System Versior	1 200.9.10.4.43		
IP Settings		Unleashed IE	un9418490011251572982362879	Generate Copy	
System Time					Apply
Country Code	Preferre	d Master			
Roles		oplying this change, the Preferred Maste			
Users		r AP, the selected Secondary AP will be on when changing Master AP.	come Master once Preferred Master Is	down. Please note there may	/ be a brief network
Mesh		Primary Preferred Maste	Ruckus-Unleashed[R610 - ( V		
		Secondary Preferred Master	r No Preference v		
		Disable WLAN service on Master A	P 🔽 If the Unleashed Network contains 3 or r	more connected APs, the Master AF	P will not
			provide WiFi service		Apply

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

🛄 System	T	System Info
System Info		Name <sup>*</sup> Ruckus-Unleashed
IP Settings		System Version 200.9.10.4.43
System Time		Unleashed ID un9418490011251572982362879 Generate Copy
Country Code		Apply
		Preferred Master Upon applying this change, the Preferred Master AP will become the Master AP and the previous Master AP will be rebooted to become a
Roles		Member AP, the selected Secondary AP will become Master once Preferred Master is down. Please note there may be a brief network
Users		disruption when changing Master AP.
Mesh		Primary Preferred Master Ruckus-Unleashed[R610 - ( *
		Secondary Preferred Master No Preference v
		Disable WLAN service on Master AP 🗹 If the Unleashed Network contains 3 or more connected APs, the Master AP will not
		provide WiFi service Apply
🕘 Services		

## 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.

#### **Configuring Admin & Services Settings** System Settings

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 271 Generating a new Unleashed ID for use in remote management

🖵 System	•	System Info
System Info		Name* Ruckus-Unleashed
IP Settings		System Version 200.9.10.4.43
-		Unleashed ID un9418490011251572982362879 Generate Copy
System Time		Apply
Country Code		Preferred Master
Roles		Upon applying this change, the Preferred Master AP will become the Master AP and the previous Master AP will be rebooted to become a Member AP, the selected Secondary AP will become Master once Preferred Master is down. Please note there may be a brief network
Users		disruption when changing Master AP.
Mesh		Primary Preferred Master Ruckus-Unleashed[R610 - C T
		Secondary Preferred Master No Preference 🔻
		Disable WLAN service on Master AP 🗹 If the Unleashed Network contains 3 or more connected APs, the Master AP will not
Services		provide WiFi service Apply

## **Designating a Preferred Master AP**

The Preferred Master settings allow an administrator to manually designate the primary and secondary preferred Master APs.

By default, there is no preference as to which AP should become the Master AP. The first AP that is deployed automatically becomes the Master AP. If the Master AP goes offline for any reason, any other Ethernet-connected member AP can take over the role of the Master AP.

By using the Preferred Master option, the administrator can designate the APs that will have a priority as the Master AP.

Complete the following steps to configure the primary and the secondary preferred Master APs.

1. Go to Admin & Services > System > System Info.

2. Under Preferred Master, from the Primary Preferred Master list, select a primary preferred Master AP.

The Primary Preferred Master list displays the best Master AP at the top of the list. The recommended best Master AP is displayed in

green and is indicated by a 🗳 ("thumbs up" symbol), as shown in the following figure and you can choose this AP as the primary preferred Master.

#### FIGURE 272 Designating APs as the Preferred Masters

🛄 System 🛛 🔻 🔻	System Info
System Info	Name* Ruckus-Unleashed
IP Settings	System Version 200.9.10.4.151
-	Unleashed ID un9418490011251572982362879 Generate Copy
System Time	Apply
Country Code	Preferred Master
Roles	Upon applying this change, the Primary Preferred Master AP will become the Master AP and the previous Master AP will be rebooted to
	become a Member AP, the selected Secondary Preferred Master will become Master once Primary Preferred Master is down. Please note
Users	there may be a brief network disruption when changing Master AP.
	there may be a brief network disruption when changing Master AP.
	there may be a brief network disruption when changing Master AP.  Primary Preferred Master R710-M[R710 - ec:8c:a2:26:52
Mesh	there may be a brief network disruption when changing Master AP.  Primary Preferred Master R710-M[R710 - ec:8c:a2:26:52  Secondary Preferred Master No Preference Disable WLAN service on Master AP OR10-2[R710 - 58:b6:33:3b:ed:20] pe connected APs, the Master AP will not
Users Mesh Services	there may be a brief network disruption when changing Master AP.  Primary Preferred Master R710-M[R710 - ec:8c:a2:26:52  Secondary Preferred Master No Preference Disable WLAN service on Master AP OR10-2[R710 - 58:b6:33:3b:ed:20] R710-1[R710 - 38:ff:36:38:81:50] R710-4[R710 - ec:8c:a2:26:52:a0]  Apply
Mesh	there may be a brief network disruption when changing Master AP.  Primary Preferred Master R710-M[R710 - ec:8c:a2:26:52  Secondary Preferred Master No Preference Disable WLAN service on Master AP OR10-2[R710 - 58:b6:33:3b:ed:20] e connected APs, the Master AP will not R710-1[R710 - 38:ff:36:38:81:50] R710-M[R710 - ec:8c:a2:26:52:a0] Apply T710s[T710s-74:3e:2b:31:98:60]
Mesh	there may be a brief network disruption when changing Master AP.         Primary Preferred Master       R710-M[R710 - ec:8c:a2:26:52 ]         Secondary Preferred Master       No Preference         Disable WLAN service on Master AP
Mesh	there may be a brief network disruption when changing Master AP.  Primary Preferred Master R710-M[R710 - ec:8c:a2:26:52  Secondary Preferred Master No. Dreference Disable WLAN service on Master AP 0 R710-2[R710 - 56:b6:33:3b:ed:20] R710-2[R710 - 36:ff:36:38:81:50] R710-1[R710 - ec:8c:a2:26:52:a0] R710-1[R710 - ec:8c:a2:26:52:a0] Switch Approval Approval T710s[T710S - 74:3e:2b:31:96:60] R610[R610 - ec:8c:a2:0c:41:c0] T610-1[T610 - ec:8c:a2:13:ca:40] Switches.
Mesh	there may be a brief network disruption when changing Master AP.         Primary Preferred Master       R710-M[R710 - ec:8c:a2:26:52 ]         Secondary Preferred Master       No Preference         Disable WLAN service on Master AP

3. From the Secondary Preferred Master list, select a secondary preferred Master AP.

When the primary preferred Master AP is offline, the secondary preferred Master AP assumes the role of the Master AP. When the primary preferred Master AP returns online, it rejoins the Unleashed network and resumes the role of the Master AP again.

## **Disabling WLAN Service on the Master AP**

Because the Master AP has to perform a number of tasks at once, it may be useful in some scenarios to reduce the compute load on the Master AP by disabling its WLAN service and allow the Master to focus on controller functions.

To disable WLAN service on the Master AP to allow it to focus on controller functions:

- 1. Go to Admin & Services > System > System Info.
- 2. In the Preferred Master section, deselect the Enable WLAN service on Master AP option.

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

#### NOTE

This feature will only take effect when the Unleashed network contains at least three other connected APs to provide WLAN service.

#### FIGURE 273 Disabling Master AP WLAN service

Name* Ruckus-Unleashed
System Version 200.9.10.4.151
Unleashed ID un9418490011251572982362879 Generate Copy
Apply
Preferred Master
Upon applying this change, the Primary Preferred Master AP will become the Master AP and the previous Master AP will be rebooted to
become a Member AP, the selected Scondary Preferred Master will become Master once Primary Preferred Master is down. Please note
there may be a brief network disruption when changing Master AP.
Primary Preferred Master Ruckus-Unleashed[R610 - ( >
Secondary Preferred Master No Preference V
Disable WLAN service on Master AP 🗹 If the Unleashed Network contains 3 or more connected APs, the Master AP will not
provide WiFi service
Apply
Switch Approval
Approval Z Automatically approve all join requests from switches.
Apply

## **Configuring Global Access Point Policies**

The Access Point Policies settings allow you to define how new APs are detected and approved for use in WLAN coverage, as well as policies on Dedicated Master discovery and communicating with the Dedicated Master.

Complete the following steps to review and revise the general AP policies.

1. Go to Admin & Services > System > System Info.

- 2. Review the current settings under Access Point Policies. You can change the following settings:
  - **Approval**: This option is enabled by default, which means that all join requests from any RUCKUS AP will be approved automatically. If you want to manually review and approve the joining of new APs to the WLAN, clear the **Approval** check box.
  - **Dedicated Master Discovery Policy**: If you have multiple Dedicated Masters on the network and want specific APs to join a specific Dedicated Master, you can limit Dedicated Master discovery. Ensure that Dedicated Master setup is completed.

Select one of the following options:

- Use DHCP OPTION 43 or auto discovery on same subnet (AP settings will be ignored): Add the Option 43 setting under DHCP server in the Linux DHCP server.

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

- Configure Primary and Secondary Unleashed Settings to AP: Enter the IP addresses (or FQDNs) of the primary and secondary Dedicated Master units to which you want APs to join. APs will first attempt to join the primary Dedicated Master. If they cannot find or are unable to join the primary Dedicated Master, they will attempt to join the secondary Dedicated Master. If still unsuccessful, APs will stop attempting for a brief period of time, and then they will restart the joining process. They will repeat this process until they successfully join either the primary or secondary Dedicated Master.

#### NOTE

If you have two Dedicated Masters, RUCKUS recommends using Smart Redundancy. For information on Smart Redundancy configuration, refer to Smart Redundancy Configuration on page 175.

- Management VLAN: You can enable the Dedicated Master management VLAN if you want to separate management traffic from regular network traffic. The following options are available:
  - **Keep AP's setting**: Select this option if you want to preserve the Management VLAN settings as configured on the AP. Note that the Management VLAN on the AP is disabled by default.
  - VLAN ID: Select this option and enter a valid VLAN ID to segment management traffic into the specified VLAN. Valid VLAN IDs are from 1 through 4094.
- **Tunnel MTU**: Use this field to set the Maximum Transmission Unit for tunnel packets between a Dedicated Master and the APs. The MTU is the size of the largest protocol data unit (in bytes) that can be passed. Supported MTU values range from 850 through 1500 (the default is 1500).
- Auto Recovery: Set an AP auto-recovery time in minutes, after which APs will reboot in attempt to reconnect to Dedicated Master. Default is 30 minutes.

3. Click Apply to save and apply your settings.

#### FIGURE 274 Configuring Global AP Policies

ystem Info		Name* Dedicated-Unleashed
Settings		System Version 200 13 6.1 224
ystem Time		Unleashed ID un2320720064691656261275542 Generate Copy Apply
ountry Code		Access Point Policies
oles		Approval 🗹 Automatically approve all join requests from APs. (To enhance wireless security, deactivate this option. This means you must manually "allow" each newly discovered AP.)
sers		Dedicated Master Discovery Policy   Use DHCP OPTION 43 or auto discovery on same subnet (AP settings will be ignored)
lesh		<ul> <li>Configure Primary and Secondary Unleashed Settings to AP(IP or domain name is acceptable)</li> </ul>
		Primary Unleashed Addr
	_	Secondary Unleashed Addr
Services		Keep AP's Primary and Secondary Unleashed Settings
	_	Management VLAN   Keep AP's setting  VLAN ID
Administration	•	* Tunnel MTU 1500 (To limit the maximum transmission unit size between Unleashed and AP, range: 850 ~ 1500)
		Auto Recovery A Perboots if disconnected from Unleashed for more than 30 Minutes.

### **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 275 Enable automatic approval of ICX switches

Country Code	Preferred Master
	 Preferred Master Upon applying this change, the Primary Preferred Master AP will become the Master AP and the previous Master AP will be rebooted to
Roles	become a Member AP, the selected Secondary Preferred Master AP will become Master AP and the previous Master AP will be rebooled to become a Member AP, the selected Secondary Preferred Master will become Master once Primary Preferred Master is down. Please note
Users	there may be a brief network disruption when changing Master AP.
Mesh	Primary Preferred Master Ruckus-Unleashed[R610 - ( >
	Secondary Preferred Master No Preference ~
	Disable WLAN service on Master AP 🗌 If the Unleashed Network contains 3 or more connected APs, the Master AP will not
Services	provide WiFi service
	Apply
Administration	Switch Approval
	Approval 🛛 Automatically approve all join requests from switches.
	Approval Z Automatically approve all join requests from switches.
	Approval 🛛 Automatically approve all join requests from switches.
	Approval Z Automatically approve all join requests from switches.
	Approval Z Automatically approve all join requests from switches.
	Approval        Automatically approve all join requests from switches.         Email Server
	Approval Z Automatically approve all join requests from switches.  Apply  Email Server  From Email Address
	Approval Z Automatically approve all join requests from switches.  Apply  Email Server  From Email Address SMTP Server Name

## **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.

	Apply	
►	Switch Approval           Approval         Automatically approve all join requests from switches.           Apply	
	Email Server	
	_	
	From Email Address test@example.com	
	SMTP Server Name smtp.example.com	
	SMTP Server Port 587	
	SMTP Authentication Username username	
	SMTP Authentication Password	
	Confirm SMTP Authentication Password	
	B 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	
	•	Switch Approval       Approval @ Automatically approve all join requests from switches.       Apply         Email Server       @ Enable Email Server       @ Enable Email Server Name @smp.example.com         SMTP Server Name @smp.example.com       SMTP Server Pott 587         SMTP Authentication Username @sename       SMTP Authentication Password         BMTP Authentication Password       BMTP 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

#### FIGURE 276 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 277 Configuring SMS settings

	Test Apply
SMS Settings	
✓ Enable SMS Serve	er
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
<ul> <li>Twilio account</li> </ul>	information
Account SID	[register a new Twilio account]
Auth Token	
From PhoneN	umber
Clickatell acco	unt information
User Name	[register a new Clickatell account]
Password	
APIId	
From PhoneN	umber
Customized Se Method	
	GET
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 want to update the IP address and DNS server settings of your Master AP, complete the following steps.

#### NOTE

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

Complete the following steps to change the IP address settings:

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

#### NOTE

Upon enabling Gateway mode, all devices will reboot immediately. Refer to Gateway Mode on page 374.

- 3. Under WAN IP Address, select one of the following options:
  - Manual: If you select Manual, enter the correct information in the active fields (IP Address, Netmask, Gateway, Primary DNS Server, Access VLAN are required).
  - DHCP: If you select DHCP, enter the access VLAN ID.

#### NOTE

The default value of the access VLAN ID is 1.

- 4. Click Apply to save your settings. You will lose connection to the Master AP.
- 5. To log in again to the web interface, use the newly assigned IP address in your web browser or use the Universal Plug and Play (UPnP) application to rediscover the Master AP.

#### FIGURE 278 Configuring Device IP Address Settings

System	•	IP Settings	Management Interface	DHCP Assigned Address	DHCP Reserved Address	Management Access Control		
System Info				1				
IP Settings		IP Se	-	c network addressing, click "	Janual" and make the correc	t entries. If you click "DHCP", no	"Manual" entries are needed.	
System Time			AN IP Address	5.	-			
Country Code			Manual	DHCP	•			
Roles			* IP Address 10					
Users			* Netmask 25	5.255.255.0				
Mesh			* Gateway 10	75.46.254				
	_	•	Primary DNS Server 10	10.10.10				
Services	•	Sec	condary DNS Server 10	.10.10.190				
	_		* Access VLAN 1					

#### **Gateway Mode**

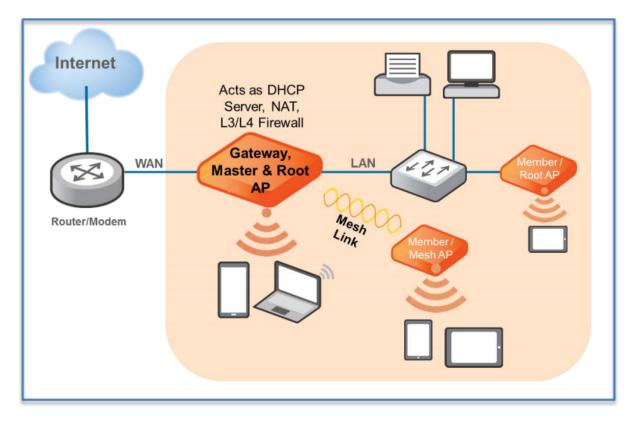
Gateway mode provides a solution for small and midsize business (SMB) customers who want to provide private IP addresses for clients and do not have an existing gateway router, or who connect to their Internet service provider (ISP) over PPPoE. Enabling Gateway mode provides Network Address Translation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

Only the H350 AP and the H550 AP support dual WAN ports, where one Ethernet port is configured as the active WAN port and the other Ethernet port is configured as the standby WAN port for the RUCKUS Unleashed gateway. At any given point, only one Ethernet port acts as the active WAN port. The traffic moves through the active WAN port. If the active WAN port fails, the traffic is automatically switched to the standby WAN port until the active WAN port recovers.

#### NOTE

If Gateway mode is enabled, the maximum number of APs in a RUCKUS Unleashed network is 25, even if the Master AP can otherwise support more APs.

#### FIGURE 279 Gateway Mode Topology



Gateway functionality can be restored with minimum user intervention when a Gateway Master AP is out of service. If the Gateway Master AP goes down, simply replace it with one of the member APs and connect the uplink Ethernet cable to the WAN port, and the member AP will become the new gateway.

If the gateway recovery mechanism does not work, you can still access the web interface of the new Master AP to configure it manually.

#### **Configuring Gateway Mode**

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

Complete the following steps to configure the Master AP as a gateway:

1. Go to Admin & Services > System > IP Settings.

2. Under IP Settings, enable the Gateway Mode option and configure the WAN and LAN IP address settings.

#### NOTE

Alternatively, in the factory default state, you can connect to the Master AP and perform the initial setup as described in step 2b - Setup Using a Web Browser. On the second wizard screen (**Management IP**) select **Enabled** in **Gateway Mode**. Refer to Advanced Install on page 138 for more information.

### FIGURE 280 Enabling Gateway Mode

🛄 System	•	IP Settings DHCP Client List Rese	rve DHCP Client IPs			
System Info		IP Settings				
IP Settings		If Unleashed was assigned static netw entries are needed.	ork addressing, click "Manua	al" and make the correct ent	ries. If you click "DHCP", no "Manu	ial"
System Time		Warning: Upon enabling Gateway, all o	devices will reboot immediate	ely.		
Country Code		Gateway Mode				
Roles		WAN Selection	▼	LAN & WLAN IP Addres	is v	•
Users		WAN Port PORT 2	•	* Router IP	10.106.0.1	
Mesh		***	19 \$	* Netmask	255.255.0.0	
Wesh		A	1 - 1			
		Process Proces	PORT 2			

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

FIGURE 281 Configuring WAN, Standby WA	N, and LAN & WLAN IP Addresses
--	--------------------------------

WAN Port			LAN & WLAN Client IP	Addresses	
WAN Port	PORT 1	~	Starting IP	10.106.0.2	
⊖ Manual	DHCP		* Ending IP	10.106.7.209	
* IP Address	10.223.38.237		Number of IPs	2000	
* Netmask	255.255.255.0		Lease Time	Twelve hours	~
* Gateway	10.223.38.254		Primary DNS Server	10.10.10.190	
* Primary DNS Server	10.10.10.190		Secondary DNS Server	10.10.10.10	
Secondary DNS Server	10.10.10.10				
Standby WAN Port 1			LAN & WLAN IP Addres	s	
WAN Port	Disabled	~	* Router IP	10.106.0.1	
Manual	C	DHCP	• Netmask	255.255.0.0	
* IP Address					
Netmask					
Gateway					
* Primary DNS Server					
Secondary DNS Server					

- 4. Configure how the WAN (uplink) port obtains its IP address:
  - DHCP (Dynamic): When DHCP (Dynamic) is selected, the WAN port is assigned an IP address automatically.
  - Manual (Static): When Manual (Static) is selected, enter an IP address, netmask, gateway address, and primary DNS server addresses in the required fields, and (optionally) enter the secondary DNS server address.
  - PPPoE: When PPPoE is selected, enter the PPPoE username and PPPoE password in the fields provided.
- 5. Configure local subnet settings for the LAN port:
  - LAN & WLAN Client IP Addresses
    - Starting IP and Ending IP: Enter the first and last IP addresses that will be issued in this scope.
    - Number of IPs: Enter the total number of addresses in this scope.
    - Lease Time: Select a duration for IP address lease time from the list.
    - Primary DNS Server and Secondary DNS Server: Enter the primary and secondary DNS server addresses.
  - LAN & WLAN IP Address
    - Router IP: Enter the IP address for the LAN port.
    - Netmask: Enter the netmask.

- 6. Designate which port will be the standby WAN (uplink) port and configure how the standby WAN port obtains its IP address:
  - DHCP (Dynamic): When DHCP (Dynamic) is selected, the WAN port is assigned an IP address automatically.
  - Manual (Static): When Manual (Static) is selected, enter an IP address, netmask, gateway address, and primary DNS server address in the required fields, and (optionally) enter the secondary DNS server address.

#### NOTE

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

7. Click **Apply**. Once setup is complete, the Gateway AP will begin providing DHCP and NAT service for clients, and clients will be assigned IP addresses from the DHCP scope that you configured.

#### **Gateway Mode Limitations and Considerations**

There are several important limitations and factors to consider when enabling gateway mode.

- All Unleashed AP models with multiple Ethernet ports support gateway mode. If your network's WAN bandwidth is higher than 100 Mbps, Ruckus recommends using 802.11ac Wave 2 or later APs (such as R510, R610, R710, R720) to enjoy the fastest internet access experience.
- The Master AP acts as the gateway for both wired and wireless clients.
- The gateway AP provides IP addresses and performs NAT (routing) functions in addition to serving as the Unleashed Master AP, and servicing wireless clients. For this reason, it is preferable to use an AP with higher CPU/memory resources, especially 802.11ac Wave 2 or later APs (e.g., R510, R610, R710, R720) as the Gateway AP, if possible.
- If gateway mode is enabled, the maximum number of APs in an Unleashed network is 25, even if the Master AP could otherwise support more.
- No VLAN support in gateway mode.
- Bonjour Gateway is not supported in gateway mode (no VLANs).
- When Mesh is enabled in gateway mode, and when the WAN IP address is obtained via PPPoE, the Master AP cannot be part of a Mesh tree. However, Mesh can still be enabled and any member AP can be a Root AP or Mesh AP.
- The WAN and LAN IP addresses must be in different IP subnets, and the address ranges may not overlap.
- If gateway mode is enabled, redundancy is disabled. This means that if the Master (gateway) AP goes offline for any reason, a member AP will not be able to take over and become the new Master.

#### Configuring M510 as Unleashed Master in Gateway Mode

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

To configure the M510 LTE WAN connection settings:

1. Go to Admin & Services > System > IP Settings.

- 2. IN WAN connection, select one of the following options:
  - Ethernet (Primary) with cellular failover: M510 in Gateway Mode with the Ethernet port as the WAN port and the LTE connection as the backup WAN port, only one of which can be active at any time. If the Ethernet connection goes down, the LTE connection becomes active to provide a backup internet uplink.
  - Cellular only: M510 configured as Master AP in Gateway Mode with an LTE connection as the uplink WAN port.

#### FIGURE 282 Select WAN uplink connection mode

Admin & S	ervices	T
🛄 System		
System Info	IP Settings DHCP Client List Preserve DHCP Client IPs	
IP Settings	IP Settings If Unleashed was assigned static network addressing, click "Manual" and make the correct entries. If you click "DHCP", no entries are needed.	"Manual"
System Time	✓ Gateway Mode	
Country Code	WAN Selection	
Roles	* WAN connection Ethernet (Primary) with cel	
Users	* WAN Recovery Time Ethernet (Primary) with cellular failover Cellular only POE M	•
Mesh		
Services	Sim1 Lan	
Administer	* This image shows the WAN port and SIN	1 slots
	Cellular Radio Settings 🛛 🗸 LAN & WLAN IP Address	<b>V</b>

- 3. In WAN Recovery Timer, enter a value in seconds after which failover to LTE uplink will occur.
- 4. In **Cellular Radio Settings**, enter the Access Point Name for each SIM card. The APN identifies the mobile network operator and the data network that the client intends to connect to.
- 5. If the Ethernet (Primary) with cellular failover option is selected, configure the WAN IP Address for Ethernet settings:
  - Manual: Enter IP address, Netmask, Gateway and DNS addresses according to your network configuration.
  - **DHCP**: Automatically assign WAN IP address from a DHCP server on the network.

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

#### FIGURE 283 M510 Cellular Radio Settings

	Users Mesh		* WAN Recovery limer	40 seconds (10-300)				
	Services	►			SIM 1	LAN		
	Administer	►			* This image :	shows the WAN port and	SIM slots	
			Cellular Radio Settings		LAN & WLAN IP Addres	s	•	
			APN for SIM 0	defaultapn	* Router IP	10.10.0.1		
			APN for SIM 1	defaultapn	* Netmask	255.255.0.0		
					-			
			WAN IP Address for Eth	nernet T	LAN & WLAN Client IP	Addresses	•	
			🔵 Manual	DHCP	* Starting IP	10.10.0.10		
			* IP Address	192.168.0.1	* Ending IP	10.10.0.30		
			* Netmask	255.255.255.0	Number of IPs	21		
			* Gateway	192.168.0.1	Lease Time	Twelve hours	•	
			* Primary DNS Server					
			Secondary DNS Server					
							Apply	
$\frown$								

#### **DHCP Server**

RUCKUS Unleashed provides a built-in DHCP server that you can enable to assign IP addresses to devices that are connected to the RUCKUS Unleashed network. The internal DHCP server will only assign addresses to devices that are on its own subnet and part of the same VLAN.

#### NOTE

Before you can enable the built-in DHCP server, the Master AP must be assigned a manual (static) IP address. If you configured RUCKUS Unleashed to obtain its IP address from another DHCP server on the network, the options for the built-in DHCP server will not be visible on the *IP Settings* page.

Complete the following steps to configure the built-in DHCP server:

- 1. Go to Admin & Services > System > IP Settings.
- 2. Under WAN IP Address, select Manual and enter the static IP settings (IP address, netmask, gateway and DNS settings).
- 3. In LAN and WLAN Client IP Addresses, enable the DHCP Server check box.
- 4. **Starting IP**: Enter the first IP address that the built-in DHCP server will allocate to DHCP clients. The starting IP address must be on the same subnet as the IP address assigned to the Master AP. If the value that you entered is invalid, an error message appears and prompts you to let RUCKUS Unleashed automatically correct the value. Click **OK** to automatically correct the entry.
- 5. **Ending IP**: Enter the last IP address in the range that you want to allocate to requesting clients. The built-in DHCP server can allocate up to 512 IP addresses including the one assigned to the Master AP. The default value is 200.
- 6. Lease Time: Select a time period for which IP addresses will be allocated to DHCP clients. Options range from six hours to two weeks (the default is one week).

7. Enter the primary and secondary DNS server addresses.

#### NOTE

In the gateway mode, the user can customize the DNS server setting for wireless clients. If the DNS server setting is ignored, the WAN interface DNS server setting is used.

#### 8. Click Apply.

#### NOTE

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

#### NOTE

RUCKUS recommends that you only enable the built-in DHCP server if there are no other DHCP servers on the network. If you enable the built-in DCHP server, RUCKUS also recommends enabling rogue DHCP server detection. For more information, refer to Rogue DHCP Server Detection on page 449.

#### NOTE

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

#### FIGURE 284 DHCP Server Configuration

🛄 System	T IP :	Settings Management Interfa	ce DHCP Assigned Address	DHCF	Reserved Address	Management Access Co	ontrol		
System Info									
IP Settings		IP Settings If Unleashed was assigned a	static network addressing, click "	"Manual"	and make the correct er	ntries. If you click "DHC	P", no "Manu	ual" entries are needed.	
System Time		WAN IP Address			LAN & WLAN Client IP			<b>v</b>	
Country Code		Manual		•	DHCP Server	_		*	
Roles		* IP Address	-	1					
Users			255.255.255.0	-	<ul> <li>Starting IF</li> </ul>	10.75.46.182			
Mesh					* Ending IF	10.75.46.200			
		* Gateway	10.75.46.254		Number of IPs	19			
		* Primary DNS Server	10.10.10.10	]	Lease Time	Six hours	~		
🗿 Services		Secondary DNS Server	10.10.10.190	]	Primary DNS Server	10.10.10.10			
Administration	•	* Access VLAN	1	1.	Secondary DNS Server				
Administration		•			Secondary Divs Server	10.10.10.190		1	Apply

#### **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 285 DHCP Client List

🛄 System	•				
System Info		IP Settings Managemen	t Interface DHCP Client List	Preserve DHCP Client IPs	
IP settings		MAC Address	I	IP Address	
System Time		58:48:22:35:af.4b		192.168.2.243	
Country Code		3c:a9:f4:48:af:90		192.168.3.98	
Roles					Previous 1 Next
Users					
Mesh					
Services	►				
Administer	►				

#### **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 286 Create New Reserved IP Address

📃 Systen	n 🔻	IP Settings	Management Interface	DHCP Client List	Preserve DHCP Client IPs	
System Info					1	
System Tim	Create New					
Country Co	MAC Address 00:01:02 IP Address 192.168					0 (0)
Roles	Description Printer					
Users					ок	Cancel
Mesh						
Servic	es 🕨					

### FIGURE 287 Reserved IP Addresses

🛄 System		IP Settings	Management Interface	DHCP Client List	Preserve DHCP Client IPs			
System Info		IF Setunys		Driff Client List	Fleselve Drice Client Irs			
IP settings		MAC A	ddress	IP Address	Description	Actions		
System Time		00:01:0	2:03:04:05	192.168.4.30	Printer	Edit Clone		
Country Code Roles	<u>C</u>	Create New Delete @1-1 (1)@						
Users	Se	earch terms		<ul> <li>Include all terms          <ul> <li>Include</li> </ul> </li> </ul>	de any of these terms			
Mesh								
Services								
Administer								

#### **Configuring a Management Interface**

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

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

Complete the following steps to configure a Management Interface:

- 1. Go to Admin & Services > System > Device IP Settings, and click the Management Interface tab.
- 2. Select the check box next to Enable IPv4 Management Interface.
- 3. Enter an IP Address and Netmask.
- 4. (Optional) Select Enable VLAN for Management Interface and enter Access VLAN.
- 5. (Optional) Enable the check box next to **Use for RADIUS services** to use this IP address for communication with a RADIUS authentication/ accounting server. If enabled, the Master AP will send RADIUS packets through this management interface, and the RADIUS server only needs to record one IP address for the Unleashed network. Otherwise, it will record the addresses of all APs.
- 6. The **Use for SNMP** services check box is automatically enabled when a Management Interface is enabled, and this address will be used for SNMP communications, if enabled.

#### FIGURE 288 Management Interface

Admin & Services		•
System Info Pettings System Time Country Code Roles Users	IP Settings       Management Interface         Management Interface         © Enable IPv4 Management Interface         Please set the IP address in the same subnet with the device IP address if VLAN is disabled.         • IP Address         192 168.30.30         • Netmask         255 255 255.0         © Enable VLAN for Management Interface         Access VLAN         Access VLAN         193         © Use for SRADIUS services         © Use for SMM Pservices	
Mesh	Apply	1

## **Configuring a Management Access Control**

Management Access Control can be used to control access to the management interface of RUCKUS Unleashed.

When you create a management access control rule, all IP addresses and subnets other than those listed specifically listed are blocked from accessing the RUCKUS Unleashed web interface. Access can be restricted by subnet, single IP address, and IP address range.

1. Go to Admin & Services > IP Settings > Management Access Control.

#### FIGURE 289 Management Access Control Tab

Admin & Services		
□ System ▼	IP Settings Management Interface Management Access Control	
System Info	This table lists the specific IP addresses which are allowed access to the Unleashed. Click Create New 1	to add another IP address, or click Edit to make changes to an existing entry.
IP Settings	+ Create Cione Delete	Search Q 2
System Time	Name IP a	address
Country Code	No data available.	
Roles		0-0 of 0 shown
Users		
Mesh		

2. Click Create.

- 3. In the **Create New** dialog box, enter the following information:
  - a) In the Name field, enter the user name that you want to allow access to the RUCKUS Unleashed web interface.
  - b) For **Restriction**, select one of the options:
    - Single
    - Range
    - Subnet
  - c) In the IP Address field, enter a single IP address, a range of IP addresses, or a subnet based on your Restriction option.

FIGURE 290 Creating a New Management Access Control

Admin & Services		
System  ▼	Create New	×
	* Name       This       Restriction          Single          Range          Subnet       * IP Address	ke chang
	Ni Current Administrator's IP address: 10.45.237.130	icel

4. Click OK.

# **Configuring the System Time**

Many Unleashed features require that the Master AP maintains the proper system time.

Maintaining the proper time relies on periodically retrieving the time from a Network Time Protocol (NTP) server on the internet. By default, the 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.
- 2. Click **Refresh** to update the display (a static snapshot) from the internal clock.

#### 3. Enable the Use NTP to synchronize the Unleashed clock automatically option.

#### FIGURE 291 Configuring the system time

🛄 System	•	System Time
System Info		Click Refresh to update the time displayed on this page. Click Sync Time with Your PC to manually synchronize the internal Unleashed clock with your administrative PC clock.
IP Settings		Current Unleashed system time is 4/20/2020 18:40:29 Your browser's current time is 4/20/2020 13:40:29 Refresh
System Time		Use NTP to synchronize the Unleashed clock automatically
Country Code		NTP Server* ntp.ruckuswireless.com     System defined User defined
Roles		Select time zone for your location: (GMT) Western Europe Time, London, Lisbon, Casablanca 🔻
Users		Automatically adjust clock for daylight saving changes
Mesh		Sync Time with Your PC Apply
Services	•	

- 4. Configure the **NTP Server**: The default NTP server is maintained by Ruckus, and is located at *ntp.ruckuswireless.com*. If you would like to use a different NTP server, enter the DNS name or IP address from which Unleashed will sync its clock.
- 5. Select **System defined** or **User defined** time zone. By default, the system-defined time zones are listed in the adjacent drop-down menu. For information on the user-defined time zone option, see Configuring a User-Defined Time Zone on page 387.
- 6. Select time zone for your location: Choose your time zone from the list. Setting the proper time zone ensures that time stamps on log files are in the proper time zone.
- 7. Sync Time with your PC: If needed, click this to update the internal clock with the current time settings from your administration PC.
- 8. Click **Apply** to save the results of any re-synchronization or NTP server settings changes.

### Configuring a User-Defined Time Zone

The user-defined time zone option allows the admin to customize the time zone and daylight savings time start and end times.

To configure a user-defined time zone:

- 1. Go to Admin & Services > System > System Time.
- 2. Enable Use NTP to synchronize the Unleashed clock automatically, and select User Defined.
- 3. Select GMT Offset (hours and minutes) away from GMT.
- 4. Optionally, enable Daylight Saving Time (DST), and enter the DST Start and DST End dates.

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

FIGURE 292 Configuring a user-defined time zone

🛄 System	•	System Time	
System Info		Click Refresh to update the time with your administrative PC clo	he displayed on this page. Click Sync Time with Your PC to manually synchronize the internal Unleashed clock bck.
IP Settings		Current Unleashed system time	e is 4/20/2020 18:40:29 Your browser's current time is 4/20/2020 13:40:29 Refresh
System Time		<ul> <li>Use NTP to synchronize to NTP Server* ntp.ruckuswing</li> </ul>	the Unleashed clock automatically
Country Code		System defined      User	
Roles		GMT Offset	GMT -8:00 T : 00 T
Users		Daylight Saving Time	Support daylight saving time(DST)
Mesh		DST Start on the	First V Sunday V in January At 00 O'clock
		DST End on the	First V Sunday V in January At 00 O'clock
			Sync Time with Your PC Apply
Services	- <b>b</b> []		

# **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:

- 1. 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 293 The Country Code page

🛄 System	•	Country Code
System Info		Different countries have different regulations on the usage of radio channels. To ensure that Unleashed is using an authorized radio channel,
IP Settings		select the correct country code for your location.
System Time Country Code		Country Code: United States Channel Optimization:  Optimize for Compatibility  Optimize for Interoperability  Optimize for Performance Apply
Roles		
Users		
Mesh		
<b>e</b> Services	_	

## **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 34 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 294 Roles

System Info	•	Roles Use these features to add new rol	es and apply policies. You can also update existin	g roles, which are listed in this table.		
IP Settings		+ Create 🥒 Edit 🗎 Delete		Search	Q	8
System Time		Name	Description			
Country Code		Default	Allow Access to All WLANS	3		
Roles				1-1 of 1 shown	« <b>1</b>	>
Users						
Mesh						
	_					
Services						
Administration	•					

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 295 Creating a new user Role

🛄 System		
	* Name Role 1	3.
	Description	Q 2
	Group Attributes	
	Policies O Allow access to all WLANs	
	🗆 WLANs 👻	
Roles	Unleashed	hown < 1 >
Users	1-1 of 1 shown 🧉 🚺	>
	Guest Password 🔲 Allow guest pass generation	
	Administration 🔲 Allow Unleashed Administration	
	<ul> <li>Super Admin (Perform all configuration and management tasks)</li> </ul>	
Services	<ul> <li>Monitoring Admin (Monitoring and viewing operation status only)</li> </ul>	
🏚 Administrati		

# Adding New Users to the Local Database

Once the wireless network is set up, you can choose to authenticate wireless users using an external authentication server (Active Directory or RADIUS server), or to authenticate users by referring to accounts that are stored in the system's internal user database.

This section describes the procedures for managing users using the internal user database. For authentication using an external AAA server, see AAA Servers on page 408.

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.
- 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 390.
- 5. Click OK to save your settings. Be sure to communicate the user name and password to the appropriate end user.

#### FIGURE 296 The Users Page

渷 WiFi Networks	Traffic: 0.19 MB			Total 1 Normal 1	Disabled	►
Clients	Client: 1			Total 1 Connected	1 Blocked	►
Access Points				Total 2 Working	Disconnected	►
Admin & Services						▼
System 🔻	, , , , , , , , , , , , , , , , , , , ,					
System V System Info Device IP settings	This table lists all current user accounts along with bas user.	sic details. You can add, edit, or delete user accounts. You can also clic			ection Guide for the	
System Info Device IP settings System Time	This table lists all current user accounts along with bas	sic details. You can add, edit, or delete user accounts. You can also clic Full Name	k the Print button to print out the First-t Role	Actions		
System Info	This table lists all current user accounts along with bas user. User Name Create New			Actions	ection Guide for the Delete ©0-0 (0)⊖	
System Info Device IP settings System Time Country Code Roles	This table lists all current user accounts along with bas user. User Name Create New	Full Name		Actions		
System Info Device IP settings System Time Country Code Roles Users	This table lists all current user accounts along with bar user. User Name Create New Search terms * In	Full Name		Actions		

#### FIGURE 297 Creating a New User on the Internal Database

	Create New				
🛛 Syst	User Name*	bobmarley			
	Full Name	bob marley			е
rstem Info	Password*	•••••			
evice IP se	Confirm Password*	•••••			
stem Tim	Role	Default 🔹			
untry Co				OK Cancel	
oles				Delete	al-11()@
				Farata	

# **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 390.)
- 5. Click **OK** to save your changes. Be sure to communicate the relevant changes to the appropriate end user.

# Importing Users into the Local Database using CSV File

- 1. From the dashboard, select Admin & Services > System > Users.
- 2. Under Internal User Database, click More > Import to import user profiles.

You can download a sample user profile using the link in **To download a example of profile, click here**.

#### FIGURE 298 Importing Users into the Local Database

-Internal User Database (on Unlea	(shed)		
	isited)		
	me Wireless Network Cor	etails. You can add, edit, or delete user accounts. You can expection Guide for the user. You also can click the Impo ok here.	
Users can acceess https://unleas	hed.ruckuswireless.com/u	iser/user_changepass.jsp to change password.	
➡ Create 🖉 Edit 🛍 Delete	More -	Search Q	2
Username	Clone	Role	
1239	Limport	Default	

3. In the **Import User List** window, either drag-and-drop a file within the dotted area or click to upload the file.

#### FIGURE 299 Importing User List

Import User List	×
Drop file here or click to upload file	
	Cancel

## **Limitations and Considerations for CSV Import**

- A CSV file can contain a maximum of 2048 accounts at one time. A maximum of 2048 accounts are stored in the local database.
- A CSV file must use the following format: UserName,FullName,Password,RoleName.
  - Password can contain only between 4 through 32 characters, and cannot contain "<>" (angle brackets).
  - RoleName must be between 1 through 32 characters and cannot contain "< >" (angle brackets).
  - UserName must be from 1 through 32 characters in length and can consist only of alphanumeric characters, underscore (\_), and period (.), and Chinese characters.
  - FullName is not necessary.

# **Deleting a User Record**

- 1. Go to Admin & Services > System > Users.
- 2. Review the Internal User Database table.
- 3. To delete one or more records, click the check boxes next to those account records, and click the Delete button.
- 4. When the confirmation dialog box appears, click **OK** to save your settings. The records are removed from the internal user database.

#### FIGURE 300 Deleting a user from the internal database

🔶 WiFi Networks	raffic: 0.01 MB		Prevent this page from creating additional additiona	ional dialogs.	Total 1	Working 1 Di	isabled	►
Clients	Client(s): 1				Total 1	Connected 1 Bl	locked	►
Access Points					Total 2	Working 2 Disc	onnected	►
Admin & Services								•
⊇ System 🛛 🔻		tabase (on Unleashed) Il current user accounts along	with basic details. You can add, edit, or delet	e user accounts. You can also click the P	rint button to print out the First-time Wireless N	etwork Connection Guide	e for the	•
System V	This table lists al user.	ll current user accounts along				etwork Connection Guide	e for the	
System V System Info Device IP settings	This table lists al user.	ll current user accounts along User Name	Full Name	Role	Actions	etwork Connection Guide	e for the	
System  System Info Device IP settings System Time	This table lists al user. 🕑	ll current user accounts along				etwork Connection Guide	e for the	
System V System Info Device IP settings System Time Country Code	This table lists al user.	ll current user accounts along User Name	Full Name	Role	Actions		e for the	
•	This table lists al user. 🕑	ll current user accounts along User Name	Full Name	Role Default	Actions			
System Info Device IP settings System Time Country Code Roles Users	This table lists al user.	ll current user accounts along User Name	Full Name bob martey	Role Default	Actions			
System Info Device IP settings System Time Country Code Roles	This table lists al user.	ll current user accounts along User Name	Full Name bob martey	Role Default	Actions			

# **Changing User Password**

Users can change their account passwords without the aid of the administrator. Syslog maintains a record of the users who have changed their passwords, which reduces the workload of the administrator.

1. Go to https://unleashed.ruckuswireless.com/user/user\_changepass.jsp or scan the QR code to reset the password.

- 2. In the **Change your password** dialog box, enter the following information:
  - a) For Username, enter your username.

The username must be from 1 through 32 characters in length and can consist only of alphanumeric characters, underscore (\_), period (.), and Chinese characters.

b) For **Password**, enter your current password.

The password must be from 4 through 32 characters in length. The usage of a pair of special characters "< >" (angle brackets) is limited, but you can use the characters separately.

- c) For New Password, enter your new password.
- d) For **Confirm New Password**, enter your new password again.

### FIGURE 301 Changing the Password for a Local Database User

Unleashed Change your pass	word
Username	
Password	Ø
New Password	Ø
Confirm New Password	Ø
Save	

3. Click Save to save the changes.

#### NOTE

If the authentication failed three times within five minutes, the login is disabled for three minutes.

## **Mesh Networking**

### **Overview of Smart Mesh Networking**

A Smart Mesh network is a peer-to-peer, multi-hop wireless network wherein participant nodes cooperate to route packets.

In a Ruckus Smart Mesh network, the routing nodes (that is, the access points forming the network), or "mesh nodes," form the network's backbone. Clients connect to the mesh nodes and use the backbone to communicate with one another, and, if permitted, with nodes on the internet. The mesh network enables clients to reach other systems by creating a path that 'hops' between nodes.

Smart Mesh networking offers many advantages:

- Smart Mesh networks are self-healing: If any one of the nodes fails, the nodes note the blockage and re-route data.
- Smart Mesh networks are self-organizing: When a new node appears, it becomes assimilated into the mesh network.

In the Ruckus Smart Mesh network, all traffic going through the mesh links is encrypted. A passphrase is shared between mesh nodes to securely pass traffic. When deployed as a mesh network, 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 35 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.
Нор	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 398 for more information.

### **Supported Mesh Topologies**

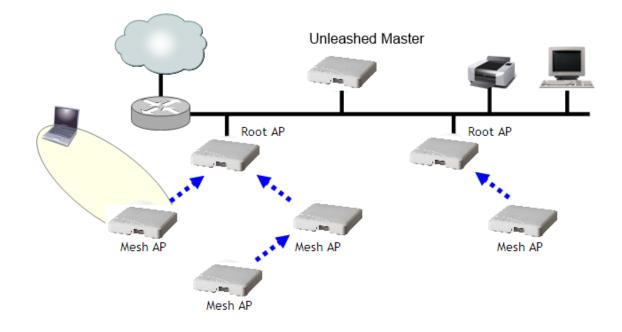
Smart Mesh networks can be deployed in three types of topologies:

- 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."

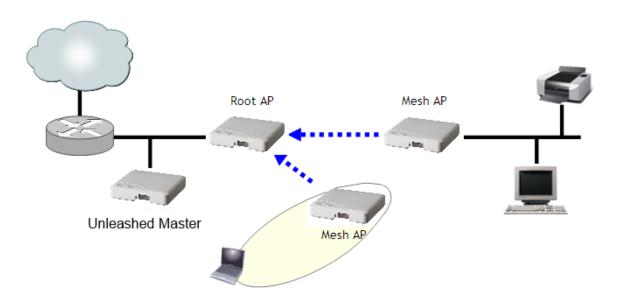
### FIGURE 302 Mesh - standard topology



#### **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 303 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.

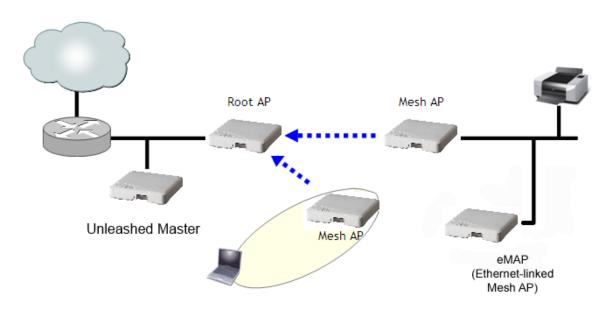
Multiple eMAPs can be connected to a single Mesh AP to, for example, bridge a wired LAN segment inside a building to a wireless mesh outdoors.

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 304 eMAP - Hybrid Mesh topology



### **Configuring Mesh Settings**

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

To configure Mesh settings, select **Enable Mesh**. Optionally, you can change the **Mesh Name (ESSID)** and the **Mesh Passphrase**, or click **Generate** to generate a new random Mesh passphrase. Under **Mesh Radio Option**, select **2.4 GHz** or **5 GHz**.

#### NOTE

Once you have enabled Mesh, you cannot disable it again without resetting the Master AP to factory defaults (see Restore to Factory Settings on page 463).

#### NOTE

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

#### NOTE

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

### NOTE

2.4-GHz mesh radio does not support Zero Touch Mesh.

### NOTE

Unleashed H320 does not support Mesh.

### FIGURE 305 Mesh Settings

□ System ▼	Mesh Settings ARP Broadcast Filter Mesh Topology Detection
System Info	Mesh Settings
IP Settings	Mesh capability allows you to deploy your access points without using wires.
System Time	Warning: Upon enabling Mesh, all Mesh capable devices will reboot immediately and you cannot disable it.
Country Code	✓ Enable Mesh
Country Code	* Mesh Name (ESSID) Mesh-111583407379
Roles	* Mesh Passphrase lagUb4TDDBTk2FeAt1byhMJ( Generate
Users	Mesh Radio Option 🔿 2.4GHz 💿 5GHz
	Zero Touch Mesh
Mesh	Zero Touch Mesh provides zero-touch onboarding of mesh APs. The new AP with the serial number you add here,
	will be automatically approved to join Unleashed Network via Zero Touch Mesh discovery.
	Pre-Approved Zero Touch Mesh APs
Services	These APs will be approved when detected. No manual approval required
• • • • • • •	Add Delete Search Q 2
Administration	AP Serial # - Status Approved on
	No data available.
	0-0 of 0 shown ( Apply

#### 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 306 Enabling Zero Touch Mesh

System	<b>•</b>	ARP Broadcast Filter	Mesh Topology Detection		
System Info		Mesh Settings			
System Time		Mesh capability allows you to deploy your Warning: Upon enabling Mesh, all Mesh c			
Country Code		Enable Mesh			
Roles		Mesh Name (ESSID) * Me			
Users		Zero Touch Mesh	VpASjVACdcvtH 4_U8yW32	enerate	
Mesh		Add Delete	s	earch Q	
0 Services	•	AP Serial #	Status	Approved on	
Gervices		No data available.			
Administer			0	-0 of 0 shown < 1 >	
Services Administer		No data available.	0	-0 of 0 shown	

### **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 307 Show Zero Touch Mesh APs

í	Access Points		Total 2 Working 2 Disconnected
	Data duration: 10 mins 💌 Edit Restart Approve Remove	2 Access Point(s) connected, 0 Access Point(s) disconnected. Please select one of the Access Points to see specific details.	
	Summary (2 Access Point(s) in total)	Mesh Status :Enabled	Show Mesh Topology 🕨
	Clients Traffic Master RuckusAP [37;b3:81]	Zero Touch Mesh Status: Enabled	Show Zero Touch Mesh Aps 🔻
1	2.46 0 0 0 56 Clients Traffic	Client(s)	Show Client(s) Info 🕨
Г	Mesh RuckusAP [1b:16:f0]	Client Status for last 10 mins	
2	2.4G 0 0 5G Clients Traffic	5 Excellent Moderale Poor	

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

### FIGURE 308 Waiting for connection

Data duration: 10		ccess Point(s) conne se select one of the Access P	cted, 0 Access Point(s) dis oints to see specific details.	connected.			
Summary (1 Access Point(s)	in total) Me	esh Status :Enabled				Show Mesl	h Topology 🕨
Clients Traffic		ero Touch Mesh Status: I	Enabled			Show Zero Touch	Mesh Aps 🔻
RuckusAP [37:b3:81]	Master Acc	ero Touch Mesh Status: H cess Points	Enabled	Model	Status		Mesh Aps 🔻
RuckusAP [37:b3:81]	2.4G Acc 5G f0.3e			Model R710	Status Waiting for connecting		

### FIGURE 309 Click Approve to allow the AP to join

	Access Points				Total 1 Work	king 1 Disconnected
	Data duration: 10 mins <b>•</b> Edt Restart Approve Remove	1 Access Point(s) connected, 0 Acces Please select one of the Access Points to see specif				
	Summary (1 Access Point(s) in total)	Mesh Status :Enabled			S	ihow Mesh Topology 🕨
	Clients Traffic Master RuckusAP [37:b3:81]	Zero Touch Mesh Status: Enabled			Show Ze	ero Touch Mesh Aps 🔻
1	2.4G	Access Points	Serial	Model	Status	Action
	5G	f0:3e:90:1b:16:f0	111604203423	R710	Disapproved	~
	Clients Traffic	Client Status for last 10 mins				Previous 1 Next

- 6. To pre-approve APs by serial number, go to Admin & Services > System > Mesh > Zero Touch Mesh, and locate the Pre-Approved Zero Touch Mesh section.
- 7. In the same section, click the **Add** button to add a new AP to the list of pre-approved Zero Touch Mesh APs.

The Input AP Serial window appears.

8. Enter the AP Serial Number of the AP to autoprovision, and click OK.

System Info	Mesh Setti	ngs			
IP Settings	Mesh capal	ility allows you to deploy your	r access points without using wires.		
System Time	Warning: L	pon enabling Mesh, all Mes	sh capable devices will reboot im	mediately.	
Country Code					
Roles	Input	AP Serial Nu	mber	×	
Users	input				
Mesh					
		AP Serial Number: 461484	4314409		dd here, will be automatically approved
0 Comrisso					
Services			ок	Cancel	0
Administer					
	461-	164814961	Pending	n/a	
				1-2 of 2 shown	1 5
					Apply

### FIGURE 310 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 311 ARP Broadcast Filter

Admin & Ser	vices						
🛄 System	T	Mesh Settings	ARP Broadcast Filter	Mesh Topology Detection	]		
System Info		ARP Broadca	st Filter				
IP Settings		ARP Broadca	st Filter is used to minimi	ze or limit the amount of broa	dcast ARPs on the network	ς.	
System Time		Enable AF	RP Broadcast Filter			Apply	-
Country Code						- 144-7 1	
Roles							
Users							
Mesh							
🕘 Services	•						
	•						

### 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 312 Mesh Topology Detection**

🛄 System	•	Mesh Settings	ARP Broadcast Filter	Mesh Topology Detection	]	
System Info		Mesh Topolog	y Detection	1		
IP Settings		The system w	ill trigger a warning even	nt when the following threshold	is exceeded.	
System Time				n with a threshold of 3	Hops	
Country Code		Enable me	esh downlinks detectio	n with a threshold of 3	Downlinks	Apply
Roles						
Users						
Mesh						

## **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.
- O(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 313 Configuring syslog settings

Passwo	b	4
API	ld	
From PhoneNumb	er	
O Customized Server		
Metho	d GET v	
UF	1.	
	Test Apply	
Log Settings		
Remote Syste	g:	
	All Syslog    All Syslog	
Equility Nam	e:Keep Original  v Priority Level:ALL v	
	Apply	
		-

# **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 314 The Admin & Services > Services page

Admin & Servi	ces						
⊒ System	Authentic	ation Servers	Test Authentication Servers Settings				
Services	This table	lists all authentic	ation mechanisms that can be used whe	enever authentication is neede	ed.		
	+ Create	🖉 Edit 🔲	Clone 🗊 Delete		Search	Q	<b>C</b>
AAA Servers	Name		Туре	IP Address		Port	
Access Control	Ruckus	AD	Active Directory	192.168.40.10	)	389	
Application Recognition & Control							
3onjour Gateway					1-1 0	f 1 shown	1
Dynamic PSK							
Suest Access Service							

## **AAA Servers**

If you want to authenticate users against an external Authentication, Authorization and Accounting (AAA) server, you will need to first configure your AAA server, then point Unleashed to the AAA server so that requests will be passed through Unleashed before access is granted. This section describes the tasks that you need to perform on the Unleashed web interface to ensure your Unleashed APs can communicate with your AAA server.

For specific instructions on AAA server configuration, refer to the documentation that is supplied with your server.

Unleashed supports two types of AAA server:

- Microsoft Active Directory
- RADIUS

A maximum of 32 AAA server entries can be created, regardless of server type.

### **Configuring AAA Servers**

Complete the following steps to configure RUCKUS Unleashed to authenticate users against an external Active Directory or RADIUS authentication server:

- 1. Go to Admin & Services > Services > AAA Servers.
- 2. In Authentication Servers, click Create New.
- 3. Enter the name for the AAA server.

- 4. Under **Type**, select the server type:
  - Active Directory: If you use a Microsoft AD server, configure the following settings:
    - **Global Catalog**: Enable Global Catalog for multi-domain AD authentication. If this option is enabled, you must also enter an Admin DN and Password so that RUCKUS Unleashed can query the Global Catalog.
    - **Encryption**: select Enable TLS encryption if you want to encrypt all authentication traffic between the client and the Active Directory server. The AD server must support TLS1.0, TLS1.1, or TLS1.2.
    - Server Address: Enter the IP address or the domain name of the AD server.
    - **Port**: The default port number (389 or 636, if you have enabled TLS encryption) should not be changed unless you have configured your AD server to use a different port.
    - Windows Domain Name: Enter a domain name for single domain authentication, or leave blank for multi-domain authentication.
  - **RADIUS**: If your authentication server is a RADIUS server, configure the following settings:
    - **Encryption**: If you want to enable encryption of RADIUS packets using Transport Layer Security (TLS), select the Enable TLS encryption check box. This allows RADIUS authentication and accounting data to be passed safely across insecure networks such as the Internet.
    - Auth Method: Choose PAP or CHAP according to the authentication protocol used by your RADIUS server.
    - Backup RADIUS: If a backup RADIUS or RADIUS Accounting server is available, enable the check box next to Backup RADIUS and additional fields appear. Enter the relevant information for the backup server and click **OK**. When you have configured both a primary and backup RADIUS server, an additional option is available in the Test Authentication Settings section to choose to test against the primary or the backup RADIUS server.
    - Server Address: Enter the IP address or the domain name of the RADIUS server (and backup RADIUS server, if enabled).
    - **Port**: The default port (1812) should not be changed unless you have configured your RADIUS server to use a different port.
    - Shared Secret: Enter a password for communication between RUCKUS Unleashed and the RADIUS server.
    - **Confirm Secret**: Repeat the shared secret.
    - Retry Policy: Enter a request timeout value (in seconds) and maximum number of retries value in the relevant fields.

### NOTE

If Backup RADIUS is disabled, enter a value for **Max Number of Consecutive Drop Packets** and **Reconnect Primary** (in minutes).

5. Click **OK** to save your AAA server entry.

### FIGURE 315 The AAA Servers Page

⊒ System	Authentication Servers	Test Authentication Servers Settings		
Services	This table lists all authenti	cation mechanisms that can be used wh	enever authentication is needed.	
AAA Servers	🕇 Create 🥒 Edit 📋	Clone Delete	Search	Q 2 🕈
Access Control	Name	Туре	IP Address	Port
Application Recognition & Control	RADIUS	RADIUS		
Bonjour Gateway			1-1	of 1 shown < 1 >
Dynamic PSK				
Guest Access Service				
Hotspot Services				

### FIGURE 316 Microsoft Active Directory Server Configuration

🛄 System	Create New		×
Services			
AAA Servers	* Name		Q 2 ¢
Access Control		Active Directory      RADIUS      RADIUS Accounting     Enable Global Catalog support	Port
Application Recognition 8	Encryption	TLS	
	* Server Address		own < 1 >
Dynamic PSK	* Port		
	Windows Domain Name	sdcqa.com domain.example.com	
			_
		ок	Cancel

### FIGURE 317 RADIUS or RADIUS Accounting Server Configuration

Create New	
Create New	×
* Name	
Туре	○ Active Directory
Encryption	□ TLS
Auth Method	● PAP ○ CHAP
Backup RADIUS	Enable Backup RADIUS support
First Server	
* Server Address	
* Port	1812
* Shared Secret	·
* Confirm Secret	
Second Server	
* Server Address	
* Port	1812
* Shared Secret	· 🖉
* Confirm Secret	·
Retry Policy	
* Request Timeout	3 seconds
* Max Number of Retries	2 times
* Max Number of	1
Consecutive Drop Packets	
<ul> <li>Reconnect Primary</li> </ul>	5 minutes
	OK Cancel

#### **Limitations on configuring AAA Servers**

- If a domain name can be resolved to more than one IP address, the first two IP addresses are used as the primary and secondary servers when the **Backup RADIUS** is disabled.
- If a domain name can be resolved to only one IP address, it is used as the primary server.
- If a domain name can resolve multiple IP addresses, only the first IP address is used as the server IP address when **Backup RADIUS** is enabled. Even if the first IP addresses of two domain names are the same, the first IP address is used as the server IP address.
- If the first two IP addresses change, the backend resolves the domain name every 2 hours and updates the AAA configuration.
- If the domain name resolution fails, the domain name is requested every 2 minutes until there is a successful resolution.

### **Testing Authentication Settings**

The **Test Authentication Settings** feature allows you to query an AAA server for a known authorized user, and return Groups associated with the user that can be used for configuring Roles within Unleashed.

After you have configured one or more authentication servers in Unleashed, perform this task to ensure that Unleashed can connect to the authentication server and retrieve the groups/attributes that you have configured for each user account.

To test the connection to the authentication server:

- 1. Go to Admin & Services > Services > AAA Servers > Test Authentication Servers Settings.
- 2. Select the authentication server that you want to use from the Test Against drop-down menu.
- 3. In User Name and Password, enter an Active Directory or RADIUS user name and password.
- 4. Click Test.

If Unleashed was able to connect to the authentication server and retrieve the configured groups/attributes, the information appears at the bottom of the page. The following is an example of the message that will appear when Unleashed authenticates successfully with the server:

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

If the test was unsuccessful, there are several possible results (other than success) that will be displayed to inform you if you have entered information incorrectly:

- Admin invalid
- User name or password invalid

These results can be used to troubleshoot the reasons for failure to authenticate users to an AAA server.

### FIGURE 318 Testing authentication server settings

-			
System		Authentication Servers Test Authentication Servers Settings	
省 Services	▼	You may test your authentication server settings by providing a user name and password here. Groups to which the user belongs will be returned and you can use them to configure the role.	
AAA Servers		Test Against Ruckus AD 🔹	
Access Control		Username user1	
Application Recognition & Control		Password 🧼	
Bonjour Gateway			est
Dynamic PSK			
Guest Access Service			
Hotspot Services			
Radio Control			
WIPS			

## **Access Control**

RUCKUS Unleashed provides several options for controlling access to your networks, including Layer 2/MAC address level Access Control Lists (ACLs), Layer 3/Layer 4/IP Address ACLs, Device Access Policies to control clients by OS type, and Client Isolation Allowlists, which are necessary when Wireless Client Isolation is enabled on a WLAN.

### FIGURE 319 Configuring Access Control

Admin & Serv	lices					
Admin & Serv	1005					
<u>⊒</u> System		L2/MAC Access Control	L3/4/IP address Access Control	Device Access Policy	Client Isolation Allow List	
Services	•	You can define L2/MAC acc devices based on their MAC	cess control lists and apply them to C addresses.	WLANs later. Set up an L	2/MAC access control list to a	allow or deny wireless
AA Servers		+ Create 🥒 Edit	Clone Delete	Allow	Search	Q 😄 🕈
Access Control		Name	Descriptio	n	Restriction	
pplication Recognition & Control		No data available.				
onjour Gateway					0-0 of 0 :	shown < 1 >
ynamic PSK						
uest Access Service						
otspot Services						
adio Control						
/IPS						
JRL Filtering						

### 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 320 Creating a Layer 2 ACL to deny specific MAC addresses

🛄 System	Create New		×
U Oystelli			
<b>G</b> Services			ow or deny wireless
	Description		
AAA Servers		Only allow all stations listed below Only deny all stations listed below	Q 2 ¢
Access Control		00:01:02:03:04:08 Create New	
Application Recognition 8	Stations	00:01:02:03:04:05 Delete	
		00:01:02:03:04:06 Delete	
		00:01:02:03:04:07 Delete	own <mark>&lt; 1</mark> >
Dynamic PSK		00:01:02:03:04:08 Delete	
		OK Cano	el

### 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 321 Configuring a Layer 3/4/IP address-based ACL

Cr	eate New						×	
	* Name	L3 /	ACL					
<u>□</u> System				ccess L3 ACL				
Services	Default Mode	Defa	ult Action i	f no rule is matched: (	Deny all by default	<ul> <li>Allow all by default</li> </ul>	ontrol list to	allow or
Giservices	Rules		Order	Description	Туре	Source Address		
			1		Allow	Any	Q	C 🕈
Access Control			2		Allow	Any		
Application Recognition 8			3 🔻	Printer	Allow	▼ 192.168.10.13		
			Create New	Delete E Advance	d Options		own	1 >
Dynamic PSK		4				÷		
						ОК Сан	icel	
							_	

### **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 322 Creating a Device Access Policy

	Create New							×	
🛄 System	* Name	don	v iOS						
Services	Description		-						ype and VLAN.
				if no rule is ma	itched: 💿 D	eny all t	oy default 🔘 Allow all	by default	Q 2 ¢
AAA Servers	Rules		Order	Description	O S/Type	Туре	Per Station Uplink	Per Station Downli	
Access Control Application Recognition 8			1	Deny iOS	Apple iOS	Deny	Disabled	Disabled	
		0	Create Nev	Delete					own < 1 >
Dynamic PSK		4						•	
								OK Cancel	

### **Configuring Client Isolation Allow Lists**

When Wireless Client Isolation is enabled on a WLAN, all communication between clients and other local devices is blocked at the Access Point.

To prevent clients from communicating with other nodes, the AP drops all ARP packets from stations on the WLAN where client isolation is enabled and which are destined to IP addresses that are not part of a per-WLAN allow list.

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

To create a Client Isolation Allow List:

- 1. Go to Admin & Services > Services > Access Control > Client Isolation Allow List.
- 2. Click Create New.
- 3. Enter a Name and optionally a description for the allowlist policy.
- 4. Auto Allowlist is enabled by Default, which allows the APs to auto-discover gateway devices and add them to the isolation allowlist.
- 5. In Rules, you can create multiple device-specific rules for each device to be allow listed.
  - **Description**: Description of the device.
  - MAC Address: Enter the MAC address of the device.
  - IPv4 Address: Enter the IP address of the device.
- 6. Click Save to save the rule you created.
- 7. To change the order in which rules are implemented, select the order from the drop-down menu in the Order column. You can also **Edit** or **Clone** rules from the **Action** column. To delete a rule, select the box next to the rule and click **Delete**.
- 8. Click **OK** to save the allow list.

#### FIGURE 323 Creating a Client Isolation Allow List

eate New					
* Nam	1e				
Descriptio	n				
Auto Allowli	st 🗹 APs will aut	o-discover gateway	devices and add then	n to the isolation allow	list
	Order	Description	MAC Address	IPv4 Address	Action
Rule	Create New	Delete			

## **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.

#### **Configuring Admin & Services Settings** Services

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 324 Application Overview page



### **FIGURE 325 Application Performance**

✓ Applications Performance for Last 1 hour	>
Uplink Throughput (88.92KB) Downlink Throughput (70.42KB) 1.5 kbps 0.9 kbps 0.6 kbps	
0 kbps 11:59 12:04 12:09 12:14 12:19 12:24 12:29 12:34 12:39 12:44 12:49 12:54 Top 10 Clients by usage Top 10 Clients by usage for last 1 hour	2 ▼

### FIGURE 326 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 279.

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.

### **Configuring Admin & Services Settings** Services

- 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 327 Application Policy**

Admin & S	ervices						
<u>⊐</u> System	►	Application Overview	Application Policy	IP based User Defined Application	Port based User Defined Application		
Services		Define application pol	icies to filter traffic by Ap	plication, then apply the policy under t	he WLAN Advanced configuration con	text.	
AA Servers	· · ·	🕇 Create 🖋 Edit	Clone 💼 Delete		Search	Q S	•
		Name		Descripti	on		
ccess Control pplication Recognition & Co		Block Facebook					
onjour Gateway	nuoi				1-1 of 1 show	n « 1	2
/namic PSK							
est Access Service							
tspot Services							
dio Control							
PS							
RL Filtering							

### FIGURE 328 Creating a new Application Policy rule

New A	Create Applicat	ion Policy Rule			×	×	
Genei	*Rule Type:	Denial Rules	¥				
* N	*Application Type:	System Defined	•				
De	*Application:	All	Facebook	-			
Rules							
Cr							
Ru							
Nc			ок	Cancel	e 1		
				U-U OT U SNOWN			
				ок			

### Applying an Application Policy to a WLAN

For instructions on applying an application policy to a WLAN, see Configuring Advanced WLAN Options on page 267.

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

🛄 Syste	m	•				
💁 Serv	Create	New				
AAA Server	Name *	Well Paid Accounting				n pie
	IP Address *	10.10.182.10				
Access Con	Netmask *	255.255.255.0				
Application	Port *	443				
Bonjour Gat	Protocol	TCP	•			1)0
Dynamic PS					OK Cancel	
Guest Access	Dervice	_				_
Hotspot Service						

### **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 330 Application Port Mapping

Admin & Se	ervices					
🛄 System	►					
o		Application Overview	Application Policy	IP based User Defined Application	Port based User Defined Application	
Services	•	User can define appl	ication port map list and	apply it to Clients later.		
AAA Servers			ame	Port Protocol	Actions	
Access Control			ane	FUIL	Actions	
Application Recognition & Cor	trol	Create New			Delete	-0 (0)
Bonjour Gateway						
Dynamic PSK		Search terms		Include all terms Include	e any of these terms	
Guest Access Service						
Hotspot Services						
Radio Control						
WIPS						

### FIGURE 331 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.

<b>‡</b> A						
🛄 System	1 🕨					
		Application Overview	Application Policy	IP based User Defined Application	Port based User Defined Application	
🥝 Serv						
AAA Server	Create New					
Access Con	Name* HTTP Proxy					
Application	Port* 8081					
	Protocol TCP	•				)0
Bonjour Gat					OK Cancel	
Dynamic PS						_
Guest Access Se	ervice					
Hotspot Services						
Radio Control						
WIPS						

## **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 332 Bonjour Gateway configuration

Admin & Serv	ices					
🛄 System		Bonjour Service				
🞱 Services	•	Enable Bonjour gateway on AP You can add new services and rules here for AP				
AAA Servers		🕂 Create 🥒 Edit 📋 Clone 🍵 Delete		Search	Q 2 0	>
Access Control		Policy	Description			
Application Recognition & Control		No data available.				
Bonjour Gateway					shown « 1 »	
Dynamic PSK				0-0 of 0	shown	
Guest Access Service					Apply	
Hotspot Services						
Radio Control						
WIPS						
URL Filtering						

### FIGURE 333 Create new Bonjour service

<u>□</u> System Cre	eate New					×	
Services		[					
		Bonjour Service Share AirPrint					Q 2 ¢
	Rules	Order	Bridge Service	From VLAN	To VLAN		
Application Recognition 8		1 •	AirPrint •	20	30		
Bonjour Gateway		Create New	Delete				
Dynamic PSK		4				+	wn <u>« 1 »</u>
							Apply
					ОК	Cancel	

**Configuring Admin & Services Settings** Services

### 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 <u>not</u> 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 334 Select Bonjour service to be deployed on an AP

Ac		Disconnected 0
E		4 hours
AP N E	Edit AP(d4:c1:9e:35:c9:40)	×
S	General Radio 2.4 GHz Radio 5.0 GHz Network Other	
	Bonjour Gateway Choose Bonjour Gateway BonjourService 🔻	
	Status LEDs Override Group Config Disable Status LEDs	
	PoE Operating Mode Override Group Config Auto	
R		
1		
	ОК Сал	ncel
	Client Status for last 1 hour	

## **Dynamic PSK**

Go to Services > Dynamic PSK to generate and manage administrator-generated DPSKs.

Only a DPSK-enabled WLAN can generate DPSKs. Refer to Enabling DPSK for a WLAN on page 271.

### FIGURE 335 Dynamic PSK Page

Admin & Serv	ices									
🖵 System		Dynamic PSK								
Services	•	Generate	Edit Export to CSV	More -				Q Search	<b>2 4</b>	
AAA Servers		DPSK ID	User	Copy Passphrase Show QR Code	Passphrase	MAC Address	WLANs	Configured VLAN	Created -	
Access Control		6	666	Delete	'?><:""{} +_)((**&^^%\$\$##	7e:fc:6d:c4:54:fe	<b>!</b> 0-00	0	2022/05/24	
Application Recognition & Control		5	555	Delete All	#tqWW9\$UNC2	96:0b:ca:10:92:cb	10-00	0	2022/05/24	
Bonjour Gateway		4	444		IQWERT###\$\$\$&&&	38:f9:d3:34:07:95	10-00	0	2022/05/24	
Dynamic PSK		2	222		Lab4man1	00:00:00:00:00:00	10-00	0	2022/05/24	
Guest Access Service									« <b>1</b> »	
Hotspot Services								1-4 of 4 shown		

### The following options are available from the **Dynamic PSK** page:

Generate: You can create DPSKs in one batch. For more information, refer to Generating DPSKs in Batch on page 429.

Edit: You can edit the DPSK user name using the Edit option.

- 1. From the DPSK table, select a DPSK entry and click **Edit**.
- 2. In the Edit dialog box, enter the new DPSK user name, and click OK.

### FIGURE 336 Editing the DPSK User Name

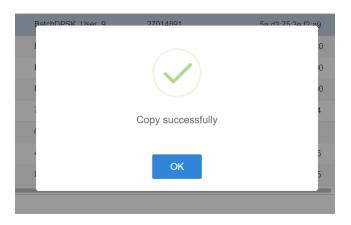
Edit				×	
•	User 555				
			ок	Cancel	
DPSK ID	User	Passphrase	MAC Address	WLANs	Config
6	666	"?><:""{} +_)((**&^^%\$\$##	7e:fc:6d:c4:54:fe	10-00	0
5	555	#tqWW9\$UNC2	96:0b:ca:10:92:cb	10-00	
	* DPSK ID 6	* User 555 DPSK ID User 6 666	* User         555           DP SK ID         User         Passphrase           6         666         "?> ""{} +_)((**&^^o\$\$\$##</td	* User 555 OK DPSK ID User Passphrase MAC Address 6 666 "?><:""{}+_)((**&^^%\$\$## 7e:fc:6d:c4:54:fe	* User         555           OK         Cancel           DP SK ID         User         Passphrase         MAC Address         WLANs           6         666         "?><:""{}]+_)((**&^^%\$\$##         7e:fc:6d:c4:54:fe         10-00

Export to CSV: Click Export to CSV to export all the generated DPSKs to a CSV file.

More: Click More to use the following options:

• Copy Passphrase: From the DPSK table, select a DPSK entry and click More > Copy Passphrase to copy a passphrase. When the confirmation message is displayed, click OK.

### FIGURE 337 Successful Copying of the Passphrase



• Show QR Code: A WLAN-supported DPSK has the Show QR Code option to join a Wi-Fi network. From the DPSK table, select a DPSK entry and, click More > Show QR Code to display the QR Code. Click Print to print the QR code or scan the QR code using a smartphone camera.

FIGURE 338 QR Code Page

Do you want to print the QR code for this Wi-Fi network?

#### 1. How to use Wi-Fi QR code?

You can print and share it to your users, and ask them to open the camera app on the smartphone and hold it over the Code. A notification should pop up and connect them to the wireless network automatically. If this did not work, check the smartphone settings and make sure that the QR Code scanning feature is enabled. If it still not working, then you may need to ask your user to download a third-party QR Code scanner from smartphone app store.

#### 2. How can I regenerate the QR code later?

You can to to WiFi Networks page and select your WiFi, click the "More" button and then click "Show QR Code" from the dropdown list, a QR code page should pop up.



Print

### **Generating DPSKs in Batch**

You can create DPSKs at once (from 1 through 50) or upload a CSV file with the custom DPSKs.

Complete the following steps to generate DPSKs.

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

### FIGURE 339 Dynamic PSK Page

	_							
System	Dynamic PSK							
🕹 Services 🛛 🔻	Generate	Edit Export to CSV More -				Q Search	2 ¢	
AAA Servers	DPSK ID	User	Passphrase	MAC Address	WLANs	Configured VLAN	Created 🕶	
Access Control	6	666	"?><:""{} +_)((**&^^%\$\$##	7e:fc:6d:c4:54:fe	10-00	0	2022/05/24 1	
Application Recognition & Control	5	555	#tqWW9\$UNC2	96:0b:ca:10:92:cb	10-00	0	2022/05/24	
Bonjour Gateway	4	444	IQWERT###\$\$\$&&&	38:f9:d3:34:07:95	10-00	0	2022/05/24	
Dynamic PSK	2	222	Lab4man1	00:00:00:00:00:00	10-00	0	2022/05/24	

- 2. Click Generate.
- 3. In the **Dynamic PSK Batch Generation** dialog box, enter the following fields:
  - Target WLAN: Select the WLAN to which the DPSKs will be applied. (Only WLANs with the DPSK enabled are listed.)
  - Number to Create: Enter the number of DPSKs you want to generate (ranging from 1 through 50; the default value is 5).
  - Dynamic VLAN ID: Enter a valid VLAN ID, ranging from 1 through 4094 (if Dynamic VLAN ID is enabled for this WLAN).
  - Upload a Profile: Refer to Uploading a Dynamic PSK Profile on page 430.

4. Click Generate to generate the requested number of DPSKs.

FIGURE 340 Generating D	PSKs Automatically
-------------------------	--------------------

rvic	Dynamic PSK B	atch Generation	×
	which contains informatio example of profile, click h Target WLAN:		
	Number to Create:	5	
	Dynamic VLAN ID:		
	or Upload a Profile:	Browse	
	To download the latest DF	PSK record generated from this page, click here	
		Generate Cancel	

You can click the click here link to download the latest DPSK record that contains the generated DPSKs.

### **Uploading a Dynamic PSK Profile**

Use the following procedure to batch generate multiple DPSKs using a CSV file that can be edited using a spreadsheet application (such as Microsoft Excel).

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

- 1. Go to Admin & Services > Services > Dynamic PSK.
- 2. Click Generate.

Look for the following message: To download an example of profile, click here.

- 3. Click the **click here** link to download a sample profile.
- 4. Save the sample batch DPSK profile (in CSV format) to your computer.

- 5. Using a spreadsheet application, open the CSV file and edit the batch dynamic PSK profile by filling out the following columns:
  - User Name: (Required) Enter the name of the user (one name per row). The length of the user name must be from 1 through 128 characters.
  - MAC Address: (Optional) If you know the MAC address of the device that the user will be using, enter it here.
  - VLAN ID: (Optional) Enter a valid VLAN ID.
  - **Passphrase**: The administrator can set the DPSK characters on their own. The DPSK length must be 8 through 62 characters. For DPSK rules, refer to DPSK Rules on page 431. If the **Passphrase** field is left empty, the system automatically generates DPSKs.

#### NOTE

The administrator is not allowed to set DPSKs using the batch method.

- 6. In the Dynamic PSK Batch Generation dialog box, click the Browse button to upload the CSV file you edited.
- 7. Click Generate to generate the custom DPSKs that you modified.

After the DPSKs have been generated, you can download the same file (with the passphrases filled in). Click the **click here** link to download the latest DPSK record generated.

#### FIGURE 341 Generating Batch Dynamic PSKs

rvic	Dynamic PSK Batch Generation	×	
	DPSK batch generation provides two facilities to create multiple Dynamic PSKs at once. You can specify the number of DPSK or upload a profile file (*.csv) which contains information necessary to create DPSKs. Once the generation is done, a result file will be downloaded for your reference. To download an example of profile click here. The maximum allowable number of DPSKs is 2048.		
	Target WLAN: 10-00 ~		
	Number to Create: 5		j
	Dynamic VLAN ID:		
	or Upload a Profile: Browse		
	To download the latest DPSK record generated from this page click here		
	Generate Cancel		
		_	

#### **DPSK Rules**

You must adhere to the following DPSK rules:

- 1. Multiple DPSKs are allowed in the same WLAN and unbound MAC address (when the MAC address is empty), but duplicate DPSKs are not allowed (shared DPSKs).
- 2. Multiple DPSKs are allowed in the same WLAN and the same bound MAC address, but duplicate DPSKs are not allowed (because the MAC address and the WLAN are used as an index in the DPSK hash table).
- 3. Multiple and duplicate (legacy device) DPSKs are allowed in the same WLAN and a different bound MAC address.

4. Multiple and duplicate DPSKs are allowed in a different WLAN, either for the same MAC address (bound) or an empty MAC address (unbound).

#### NOTE

In rules 1 and 2, if the DPSK CSV file includes the same passphrase that exists (for the same bound or unbound MAC address), Unleashed returns an error message when the administrator clicks **Upload** to import the DPSK CSV.

### FIGURE 342 Duplicate Passphrase Error

Dynamic PSK B	atch Generation	×
which contains information	provides two facilities to create multiple Dynamic PSKs at once. You can specify the number of DPSK or upload a profile file (*.csv) on necessary to create DPSKs. Once the generation is done, a result file will be downloaded for your reference. To download an here. The maximum allowable number of DPSKs is 4000.	
Target WLAN:	: 1666 ~	
Number to Create:	5	
Dynamic VLAN ID:		
or Upload a Profile:	<b>Browse</b> The passphrase 12345678 of line 2 is duplicated with line 3. System does not allow the same passphrase if MAC address is the same. Please modify the file and upload it again.	
To download the latest D	DPSK record generated from this page, click here	
	Generate Cancel	

### NOTE

If a DPSK CSV file includes the same passphrase that is existing in the same WLAN, Unleashed returns an error message when the administrator clicks **Upload** to import the DPSK CSV file and clicks **Generate**.

### FIGURE 343 Duplicate Passphrase in the Same WLAN Error

Dynamic PSK Batch Ge	neration	×
DPSK batch generation provides two fa which contains information necessary example of profile, click here. The ma Target WLAN: 1555 Number to Create: 5	cilities to create multiple Dynamic PSKs at once. You can specify the numbe	r of DPSK or upload a profile file (*.csv) for your reference. To download an
Dynamic VLAN ID: or Upload a Profile: The profile To download the latest DPSK record g	There is an error at line [2]. The passphrase "[12345678]" is duplicated with existing passphrase. Please modify the file and upload it again.	ton. Cancel
	ок	Generate Cancel

# **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 196 in Creating a New WLAN.

# FIGURE 344 Monitoring and Configuring Guest Pass Options

🛄 System		Guest Pass Generati	on Guest Pa	ss Printout Customization	Email SMS							
Services	•	Guest Pass Generatio Authenticated users ca		st passes at the URL show	vn below.							
AAA Servers		Guest Pass Generati	on URL https:/	//10.223.54.228/guestpas	s Show QR Code							
Access Control		Authentication	Server Local	I Database 🗸	•							
Application Recognition & Control											Apply	
onjour Gateway		Admin Generated Gue										
ynamic PSK		These tables list the g		passes. You can review the	e guest passes gene	rated for your users. You m	ay also remove them		arch	Q	2 4	ø
Guest Access Service												
otspot Services		Guest Name	Role	Key	Email	Phone Number	Remarks	Create Time	Expires		Re	aı
adio Control		No data available.										
											_	
1PS									0-0 of 0 sho	wn	1 »	Ð
JRL Filtering												

Click Show QR Code and the QR Code pop-up page is displayed. Click Print to print the QR code or scan the QR code using a smartphone camera.

## FIGURE 345 QR Code Page

Do you want to print the QR code for this Wi-Fi network?

#### 1. How to use Wi-Fi QR code?

You can print and share it to your users, and ask them to open the camera app on the smartphone and hold it over the Code. A notification should pop up and connect them to the wireless network automatically. If this did not work, check the smartphone settings and make sure that the QR Code scanning feature is enabled. If it still not working, then you may need to ask your user to download a third-party QR Code scanner from smartphone app store.

#### 2. How can I regenerate the QR code later?

You can to to WiFi Networks page and select your WiFi, click the "More" button and then click "Show QR Code" from the dropdown list, a QR code page should pop up.



Print

An administrator can generate guest passes from the web interface. Under Admin Generated Guest Passes, click Create. For more information, refer Generating a Guest Pass on page 214.

# **Hotspot Services**

A Hotspot Service is required to deploy a Hotspot (WISPr 1.0) WLAN.

You can create a Hotspot service when creating a new WLAN (by clicking **Create New** after you select Hotspot Service as the WLAN type), or you can create multiple Hotspot services from the Administration settings and then deploy them to your Hotspot WLANs afterwards.

Additionally, you can use the Admin & Services pages to edit or reconfigure Hotspot service policy settings after WLAN creation.

# **Creating a Hotspot Service**

The Admin & Services > Services > Hotspot Services page can be used to configure a WISPr Hotspot service to provide public access to users. In addition to the Unleashed APs, you will need the following to deploy a Hotspot:

- **Captive Portal**: A special web page, typically a login page, to which users that have associated with your Hotspot will be redirected for authentication purposes. Users will need to enter a valid user name and password before they are allowed access to the Internet through the Hotspot. Open source captive portal packages, such as Chillispot, are available on the Internet. For a list of open source and commercial captive portal software, visit https://en.wikipedia.org/wiki/Captive\_portal#Software\_Captive\_Portals, and
- **RADIUS Server**: A Remote Authentication Dial-In User Service (RADIUS) server through which users can authenticate.

For installation and configuration instructions for the captive portal and RADIUS server software, refer to the documentation that was provided with them. After completing the steps below, you will need to edit the WLAN(s) for which you want to enable Hotspot service, as described in *Assigning a WLAN to Provide Hotspot Service*.

Unleashed supports up to 32 WISPr Hotspot service entries, each of which can be assigned to multiple WLANs.

To create a Hotspot service:

- 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 reauthenticate. 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 267 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 437.

# FIGURE 346 The Hotspot Services page

System   System   Services   Ad Servers   locate New   application & Control   application & Control   application & Control   application & Control   application & Servers   application & Control   application & Control   application & Control   application & Server   application & Server   application & Control   application & Server   application & Server	Clients	N	o Clients					Total 0 Co	onnected 0	Blocked	
System   System   Services   Services   Name   Legin Page   Start Page   WiSPr Smart Client Support   Actions   Services   Name   Legin Page   Start Page   WiSPr Smart Client Support   Actions   Services   Services   Services   Services   Services   Services   Services   Services   Services											
System   System   Services   Services   Name   Legin Page   Start Page   WiSPr Smart Client Support   Actions   Services   Name   Legin Page   Start Page   WiSPr Smart Client Support   Actions   Services   Services   Services   Services   Services   Services   Services   Services   Services	Delete								unden 3	0	
System   System   Services   Ad Servers   locate New   application & Control   application & Control   application & Control   application & Control   application & Servers   application & Control   application & Control   application & Control   application & Server   application & Server   application & Control   application & Server   application & Server	Access Points							Total Z	Vorking Z	Disconnected	
System   Services   Adservers   Acciss Control   Application Recognition & Control   Benybur Cateway   BHCP Services   Upramic F5K.   Borger Services											
Name       Login Page       Start Page       WISP' Smart Client Support       Action         Add Servers       adsfadd       adsfadd       The user's Intended page       None       Edit Clone         Add Servers       coasts Control       Coaster Neurer       Edit Clone       Edit Clon	Admin & Servio	ces									▼
Name       Login Page       Start Page       WiSP' Smart Client Support       Actions         AAA Servers											
Name       Login Page       Start Page       WISP' Smart Client Support       Action         Add Servers       adsfadd       adsfadd       The user's Intended page       None       Edit Clone         Add Servers       coasts Control       Coaster Neurer       Edit Clone       Edit Clon											
Image: Services       Image: Services       None       Edit Clone         Add Servers       Coaste News       Image: Services       Image	System		Hotspot S	Services							
AA Servers AAA Servers Access Control Application Recognition & Control Benjour Gateway OHCP Server Jymanic PSK Guet Access Service Hotgos Service	9 Sondeos	-									
Access Control     Delete     0-1-1 (1)       Application Recognition & Control     Search terms     Delete     0-1-1 (1)       Bonjour Gateway     Include all terms     Include any of these terms       DHCP Server     Include all terms     Include any of these terms       Upmark PSK     Include all terms     Include any of these terms       Bonjour Gateway     Include all terms     Include any of these terms				asdfasdf	adsfadsf	The user's intended page	None		Edit Clone		
Application Recognition & Control Bonjour Gateway DHCP Server Upmanic PSK Guest Access Service Hotppot Service	WAA Servers		Create 1	New							
Bonjaur Gateway         Benjaur Gateway           DHCP Server         Image and of the decide at centrs of include at centrs of includ	Access Control								Dele	te ⊖1-1 (1)⊖	
DHCP Server DhCP Server Dhamk PSK Guest Access Service Hotspot Service	Application Recognition & Control		Search te	erms	Inc	lude all terms 💿 Include any of these terms					
Dynamik PSK Guest Access Service Hotspot Services	Sonjour Gateway										
Guest Access Service Hotspot Services	HCP Server										
Hotspot Services	Jynamic PSK										
Hotopot Services Radio Control	Guest Access Service										
Radio Control	lotspot Services										
	Radio Control										
WPS	VIPS										
🏚 Administer											

# FIGURE 347 Creating a new Hotspot service

	General	Authentication Wa	alled Garden	Policy			nts Info 🕨	
			Hotspot 1					
0 0 Clients	Redire			Enabled 🔘 Only W	ISPr Smart Client allowed			
		Login Page	Redirect unau	uthenticated user to		for authentication.		
		Start Page	After user is a	authenticated,				
			redirect to	the URL that the us	er intends to visit.			
			redirect to to	the following URL:				
	User S	Session						
		Session Timeout	(Requires white	elist for gateway and	other allowed hosts.)			
			Terminate	user session after	1440 minutes			
		Grace Period	Allow users	s to reconnect witho	out re-authentication for 30	minutes	4:00	
		Intrusion Prevention	<ul> <li>Temporarily</li> </ul>	y block Hotspot clie	nts with repeated authentication	n attempts.		

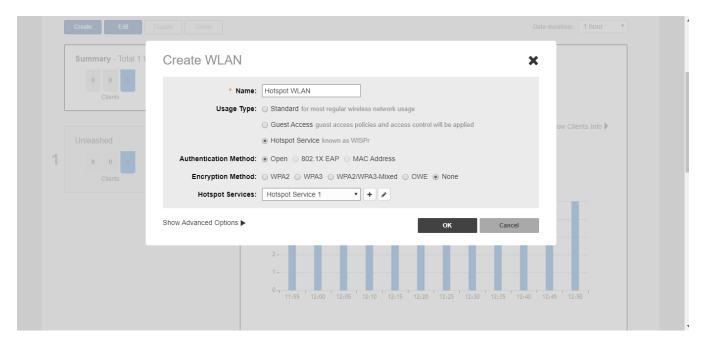
# Assigning a WLAN to Provide Hotspot Service

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 434).
- 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 348 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 439).

## 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 349 Self Healing

											•	
Access Points	5								Total 2	Working 2	Disconnected	
🗘 Admin & Serv	vices											V
System	•											
Services		Self Healing	Background Scanning	Client Load Balancing	Band Balancing	Radar Avoidance Pre-Scanning						
AAA Servers						to maximize wireless network pe	rformance.					
Access Control		Automa	tically adjust AP radio p	ower to optimize covera	e when interferen	ice is present.						
Application Recognition & Contr	ol			atically adjust AP channe nge channels to learn, op		and performance optimization. I and avoid interference.	Background Scanning will	change AP channel who	en interference is pres	ent. Channelfly cor	nstantly monitors	
				hannels using Backgrou		T						
Bonjour Gateway		☑ Auton	natically adjust 5GHz cha	annels using Background	Scanning	•						
Bonjour Gateway DHCP Server											Apply	
DHCP Server												
DHCP Server Dynamic PSK												
DHCP Server Dynamic PSK Guest Access Service												
DHCP Server Dynamic PSK Guest Access Service Hotspot Services												

# **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 350 Background Scanning

Clients	Client: 1 Connected 1 Blocked
Access Points	Total 2 Working 2 Disconnected
Admin & Servio	ies V
🛄 System	Self Healing Background Scanning Client Load Balancing Band Balancing Radar Avoidance Pre-Scanning
Services	Background scans are performed by APs to evaluate radio channel usage. The process is progressive; one frequency is scanned at a time. This scanning enables rogue device detection, AP locationing, and self-healing.
AAA Servers	Run a background scan on 2.4GHz radio every 20 seconds
Access Control	Run a background scan on 5GHz radio every 20 seconds
Application Recognition & Control	
Bonjour Gateway	Apply To view all WLANs with background scanning off, click here
DHCP Server	To view aut visuals witch background scanning off, click nere
Dynamic PSK	
Guest Access Service	
Hotspot Services	
Radio Control	
WIPS	
Administer	

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 351 Viewing the WLANs with Background Scanning Disabled

	Self Healing	Background Scanning	Client Load Balancing	Band Balancing	Radar Avoidance Pr	e-Scanning	
Services	De al anno 1		De teo conclusito en d'a star	The second se			
WAA Servers	-	I scans are performed by A scanning enables rogue de				one frequency is s	canned at a
Access Control				<u>.</u>	_		
Application Recognition & Control	🖉 Run	a background scan on 2.40	SHZ radio every 20		seconds		
Bonjour Gateway	🖉 Run	a background scan on 5GH	Iz radio every 20		seconds		
DHCP Server							Apply
JHCP Server	To view a	ll WLANs with background	scanning off, click here				
Dynamic PSK		·····					
Guest Access Service	Name		Authenticatio	n	Er	cryption	
	Guest-WL	AN-1	open		no	ine	
Hotspot Services							©1-1 (1)©
Radio Control	Search ter		@ Include all	torme @lasludo	any of these terms		
WIPS	Search ter		• Include at	i terms i motude	any or these terms		

# **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 352 Client Load Balancing

Access Points									Total 2	Working 2	Disconnected	
🗘 Admin & Servic	ces											•
⊒ System	►	Colf Hashing	Background Scanning	Client Load Balancing	Read Palancian	Da dan Aurid	ance Pre-Scanning					
Services	•			_	Band Balancing	Kadar Avold	ance Pre-scanning					_
WA Servers		Balances th	he number of clients acn	oss adjacent APs.								
Access Control			Run load balancing on 2	.4GHz radio			Adjacent radio thr	eshold(dB) 50				
Application Recognition & Control			Run load balancing on 5	GHz radio			Adjacent radio thr	eshold(dB) 43				
Bonjour Gateway											Apply	
DHCP Server												
Dynamic PSK												
Guest Access Service												
Hotspot Services												
Radio Control												
WIPS												
Administer	•											

# 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 353 Disable Load Balancing for a WLAN

Ruci		Usage Type: O Standard for most regular wireless network usage © Guest Access guest access policies and access control will be applied O Hotspot Service known as WISPr	s-Unleashed 47m	admin 🖗 Log	
-	0 0 4 Clients	Guest Access Service : guest-service-1 Create New			
1	Guest-	Hide advanced options   Priority Access Control Radio Control Others			
2	Clients Unleash	Wireless Media Fast BSS Transition :  □ Enable 802.11r FT Roaming Management : (Recommended to enable 802.11k Neighbor-list Report for assistant.) Radio Resource Management : □ Enable 802.11k Neighbor-list Report Background Scanning :  ☑ Enable	5:07 15:08		
	0_0_0 Clients	(All radio will preform background scanning) Load Balancing : □ Enable (Applies to this WLAN only.it may not be active on other WLANs) Band Balancing : ② Enable (Applies to this WLAN only. Band Balancing might be enabled on other WLANs) 802.11d : ③ Support			
		OK Cancel		-	

# **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 282 for the WLAN using the WLAN Advanced Options.

# **FIGURE 354 Band Balancing**

Access Points									Total 2	Working 2	Disconnected	►
Admin & Serv	/ices											▼
_												
System		Calf Healing	Realization of Computing	Client Land Palmarian	Band Balancing	Radar Avoidance Pre-Scanning						
🔒 Services	•	Self Healing	Background Scanning	Client Load Balancing	band Balancing	Radar Avoidance Pre-Scanning						
AAA Servers		Balances th	e load on Radios, by dis	tributing the clients on 2	2.4GHz and 5GHz ra	dios.						
Access Control			Percent of clients (	on 2.4GHz radio			25	%				
Application Recognition & Contro	al										Apply	
Bonjour Gateway												
DHCP Server												
Dynamic PSK												
Guest Access Service												
Hotspot Services												
Radio Control												

# **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 388).

## FIGURE 355 Radar Avoidance Pre-Scanning

Clients	Client: 1	Total 1 Connected 1	Blocked
Access Points		Total 2 Working 2	Disconnected
Admin & Services			
System  System  AAA Servers  Access Control  Application Recognition & Control  Bonjour Gateway  DHCP Server  Dynamic PSK  Guest Access Service  Rotapot Services  Rota Control  WIPS	Setf Healing       Background Scanning       Client Load Balancing       Radar Avoidance Pre-Scanning         Image: Client Load Balancing       Enable Radar Avoidance Pre-Scanning       Image: Client Load Balancing       Radar Avoidance Pre-Scanning		Apply

# **WIPS**

Unleashed provides several built-in intrusion prevention features designed to protect the wireless network from security threats such as Denial of Service (DoS) attacks and intrusion attempts. These features, called Wireless Intrusion Prevention Services (WIPS), allow you to customize the actions to take and the notifications you would like to receive when each of the different threat types is detected.

# **Denial of Service (DoS)**

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

To configure the DoS protection options:

- 1. Go to Admin & Services > Services > WIPS > Denial of Service (DoS).
- 2. Configure the following settings:
  - **Protect my wireless network against excessive wireless requests**: If thiscapability is activated, excessive 802.11 probe request frames and management frames launched by malicious attackers will be discarded.
  - **Temporarily block wireless clients with repeated authentication failures for [] seconds:** If this capability is activated, any clients that repeatedly fail in attempting authentication will be temporarily blocked for a period of time (10~1200 seconds, default is 30).

3. Click Apply to save your changes.

## FIGURE 356 Denial of Service (DoS)

										•	
Access Point	ts							Total 2	Working 2	Disconnected	
Admin & Se	rvices										
•											
💻 System	•										
0		Denial of	Service(DoS)	Intrusion Detection and Prevention	Rogue DHCP Server Detection	Rogue Devices					
Services	•	Unleas	hed utilizes buil	t-in mechanisms to protect against com	nmon wireless network intrusions.						
AAA Servers			Protect my v	vireless network against excessive wirel	ass ranuasts						
Access Control				block wireless clients with repeated aut			seconds				
Application Recognition & Con	trol	2	remporanty	block wireless clients with repeated au			seconds				
Bonjour Gateway										Apply	
DHCP Server											
Dynamic PSK											
Guest Access Service											
Hotspot Services											
Radio Control											
WIPS											

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

Denial of Servi	ce(DoS) Intrusion D	etection and Prevention	Rogue DHCP Server Detection	n Rogue	Devices	
Currently A	Active Rogue Devic	es		Sear	ch	Q C
Tree	MAC Address	Device Name	Location	Channel	Radio	Туре
	08:95:2a:54:16:a8			1	802.11g/n	
<b>e 2</b>	c0:c5:22:dd:a0:70			1	802.11g/n	AP
	d4:c1:9e:35:c9:40	R610 - Master				
<b>.</b>	c0:c5:22:e2:d1:b8			6	802.11g/n	AP
• Q	c0:c5:22:e3:9f:38			1	802.11g/n	AP
	Currently A	MAC Address           * 10         08:95:2a:54:16:a8           * 10         08:95:2a:54:16:a8           * 10         00:c5:22:dd:a0:70           * 10         d4:c1:9e:35:c9:40           * 10         c0:c5:22:d2:d1:a0	MAC Address         Device Name           @ 10         08:95:2a:54:16:a8           @ 10         c0:c5:22:dd:a0:70	MAC Address         Device Name         Location           @ 10         08:95:2a:54:16:a8            @ 11         c0:c5:22:dd:a0:70            @ 12         c0:c5:22:dd:a0:70            @ 12         c0:c5:22:dd:a0:70            @ 12         c0:c5:22:dd:a0:70	Currently Active Rogue Devices         Tree       MAC Address       Device Name       Location       Channel         * * 0       08:95:2a:54:16:a8       1       1         * * 0       08:95:2a:54:16:a8       1       1         * * 0       08:95:2a:64:a0:70       1       1         * * 0       c0:c5:22:dd:a0:70       1       1         * * 0       c0:c5:22:e2:dd:a0       R610 - Master       6	Tree         MAC Address         Device Name         Location         Channel         Radio           * 1         08:95:2a:54:16:a8         1         802.11g/n           * 1         c0:c5:22:dd:a0:70         1         802.11g/n           * 1         d4:c1:9e:35:c9:40         R610 - Master         6         802.11g/n

4. To mark a rogue device as a "Known" device (for example, a nearby neighbor's network), click **Mark As Known**. This device will no longer trigger rogue device detection alarm events on the *Administration > Diagnostics* pages.

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

FIGURE 358 Marking rogue devices as known or malicious

Admin & Serv	vices						,
🛄 System		Denial of Service	e(DoS) Intrusion Detection and Preventio	n Rogue DHCP Serve	er Detection	Rogue Devices	
Services	•						
AAA Servers		Currently Ac	tive Rogue Devices				
Access Control		ourrenuy Ac	are nogue beriets			Search	Q 2
Application Recognition & Control		Encryption	SSID	Last Detected	RSSI	Action	
Bonjour Gateway		Encrypted	TC8715DA2	2019/09/19 10:34:33		Mark As Known	Mark As Malicious
Dynamic PSK		Encrypted	Backup-Grande-2G	2019/09/19 10:34:33		Mark As Known	Mark As Malicious
Guest Access Service				2019/09/19 10:34:33	60		
Hotspot Services		Encrypted	ARRIS-D1BA	2019/09/19 10:36:13		Mark As Known	Mark As Malicious
Radio Control		Encrypted	SPJauregui	2019/09/19 10:30:53		Mark As Known	Mark As Malicious
		Encrypted	Ruckus1	2019/09/19 10:34:33		Mark As Known	Mark As Malicious

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

FIGURE 359 Manage known rogue devices

Remove Search			Remove
AC Address Channel Radio Type Encryption SS	Channel Radio Type E	Channel	MAC Address
cc5:22:e2:d1:b8 6 802:11g/n AP Encrypted AR	b8 6 802.11g/n AP E	6 8	c0:c5:22:e2:d1:b8
er Blocked Rogue Devices	Rogue Devices	e Devices	
Remove			Jser Blocked Rogu

#### **Rogue AP Detection**

To enable/disable and configure Rogue Access Point detection:

- 1. Go to Admin & Services > Services > WIPS > Intrusion Detection and Prevention.
- 2. Enable the Enable report rogue devices option to include rogue device detection in logs and email alarm event notifications.
- 3. Select which devices to include in rogue device reports:
  - **Report all rogue devices**: Send alerts for all rogue AP events.
  - Report only malicious rogue devices of type: Select which event types to report.
    - SSID-spoofing: A malicious rogue AP that uses the same SSID as ZoneDirector's AP, also known as an "Evil-twin" AP.
    - Same-Network: A malicious rogue AP that is connected to the same wired network.
    - MAC-spoofing: A malicious rogue AP that has the same BSSID (MAC) as one of the virtual APs managed by ZoneDirector.
    - User-Blocked: A rogue AP that has been marked as malicious by the user.
- 4. Enable the **Protect the network from malicious rogue access points** feature to automatically protect your network from network connected rogue APs, WLAN-spoofing APs and MAC-spoofing APs. When one of these rogue APs is detected (and this check box is enabled), the Ruckus AP automatically begins sending broadcast de-authentication messages spoofing the rogue's BWLAN (MAC) to prevent wireless clients from connecting to the malicious rogue AP. This option is disabled by default.
- 5. Click **Apply** to save your changes.

## FIGURE 360 Intrusion Detection and Prevention

Admin & Servi	Ces	
🛄 System	Denial of Service(DoS) Intrusion Detection and Prevention Rogue DHCP Server Detection Rogue Devices	
0 comises	Intrusion Detection	-
Services	Unleashed uses background scan results to detect rogue 802.11 access points. If the rogue access point is spoofing a managed AP's	
AAA Servers	SSID or MAC address or is found on the wired network, it will be flagged as malicious. Rogue detection requires backgroud scanning to be enabled.	
Access Control	✓ Enable report rogue devices	
Application Recognition & Control	Report all rogue devices	
Application Recognition & Control	Report only malicious rogue devices of type	
Bonjour Gateway	<ul> <li>SSID-Spoofing Same-Network MAC-Spoofing Ver-Blocked</li> <li>Protect the network from malicious rogue access points.</li> </ul>	
Dynamic PSK	Apply	
Guest Access Service		
Hotspot Services		
Radio Control		
WIPS		

# **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

#### **Configuring Admin & Services Settings** Services

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

## FIGURE 361 Rogue DHCP Server Detection

🛄 System		
Services	Denial of Service(DoS) Intrusion Detection and Prevention Rogue DHCP Service	ver Detection
AAA Servers	Unleashed can scan the network periodically for rogue DHCP servers.	
Access Control		Apply
Application Recognition & Control		
Bonjour Gateway		
DHCP Server		
Dynamic PSK		
Guest Access Service		
Hotspot Services		
Radio Control		
WIPS		

# **URL Filtering**

URL filtering allows administrators to manage internet usage by preventing access to inappropriate websites using a customizable combination of blocklists and allowlists.

The Ruckus URL filtering implementation uses a third-party web classification system that groups a wide variety of internet domains into various levels of inappropriate content, and allows flexible control according to the deployment environment.

Each website is categorized into one of the 83 categories. To find out which category a website falls into, see the Webroot BrightCloud Server site lookup tool (https://www.brightcloud.com/tools/url-ip-lookup.php).

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

There are four pre-defined category groups and one custom category group:

- No adult content: No adult content or nudity.
- Clean and safe: No adult content plus no malware, spyware, phishing, botnets or spamware.
- Child and student friendly: Clean and safe plus no alcohol, intimate apparel, dating, or weapons.
- Strict: Child and student friendly plus no streaming media, personal storage and games.
- Custom: Select the categories of traffic to block from the list.

Once enabled, you can view lists of the top URLs blocked by the system, top clients attempting to visit restricted domains, top allowed URLs and content categories by traffic volume, and other useful metrics from the URL Filtering Summary tab.

# FIGURE 362 URL Filtering

Admin & Serv	ices			
🛄 System	Summary Profiles License			
省 Services	URL Filtering Traffic	C Last 1 hour T all APs	▼ all SSIDs	•
AAA Servers	Top 10 Allowed URLs by Traffic	Top 10 Allowed Categories by Traffic	Top 10 Allowed Clients by Traffic	
Access Control				
Application Recognition & Control				
Bonjour Gateway	googlevideo.com(108.2KB)	Computer and Internet Info(192.6KB) Streaming Media(151.8KB)	04:B1:67:47:C4:20(1.0MB)	
Dynamic PSK	pulipstatp.com(102.3kB) tencentgames.helpshift.com(87.2KB)	Parked Domains(127.6KB)		
Guest Access Service	i16-tb.isnssdk.com(62.2KB)	Society(118.0KB)		
	graph.facebook.com(49.6KB)	Games(105.4KB)	•	
Hotspot Services	datasaver.googleapis.com(35.3KB)	Business and Economy(88.8KB)		
Radio Control	oneclient.sfcms(32.9KB)	Social Networking(69.3KB)	•	
WIPS	secure-web.cisco.com(32.0KB)	Internet Portals(46.7KB)		
WIF 5	clients4.google.com(30.3KB)	Web Advertisements(33.8KB) Training and Tools(32.9KB)	· ·	

# **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 363 Creating a URL Filtering Profile

🛄 System		Summary	Profiles	License							
Services	•	+ Create	🔊 Edit	Clone	Delete		Search	1	Q	0	٥
AAA Servers		Name			Description	Filtering Level	Blocked Categories	Blocklist	AI	lowlist	:
Access Control		Profile 1				Strict	45	0	0		
Application Recognition & Control										1	
Bonjour Gateway								1-1 of 1 sh	own		
Dynamic PSK											
Guest Access Service											
Hotspot Services											
Radio Control											

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

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

## FIGURE 364 Selecting Level of Strictness

General			•
* Nar Descripti	e Profile 1		
Categories			-
Click here to check category with URL o O No adult content O Clean and safe	No adult content or nudity No adult content plus, no malware, spyware, phishing, botne Clean and safe plus no alcohol, intimate apparel, dating, or v	weapons	
Child and student friendly Strict Custom (25 Blocked)Blocked Categories	Child and student friendly plus no streaming media, personal Please chose the contents you want to block in below check		
<ul> <li>Strict</li> </ul>			

# FIGURE 365 Blocklisting or Allowlisting a Specific URL

Click here to check category with URI No adult content Clean and safe Child and student friendly Strict Custom V (25 Blocked)Blocked Categorie	No adult conte No adult conte Clean and saf Child and stud Please chose	Jomain or IP No adult content or nudity No adult content plus, no malware, spyware, phishing, botnet or spamware Clean and safe plus no alcohol, intimate apparel, dating, or weapons Child and student friendly plus no streaming media, personal storage and games Please chose the contents you want to block in below checkbox group				
Blocklist & Allowlist				•		
Bloc	klist	Order	Domain Name	Action		
	Create New	Delete				
Allo	wlist	Order	Domain Name	Action		
	Create New	Delete				
Safe Search				•		
Google Safe Se	arch 🔲 Enable God	ogle Safe Search				
	arch 🗌 Enable You					
Bing Safe Se	arch 🔲 Enable Bin	g Safe Search				

- 6. Optionally, in *Blocklist & Allowlist*, you can add custom URLs to either block or allow. Allowlist and blocklist entries override the rules configured above. A maximum of 16 blocklist and 16 allowlist entries can be created per profile.
- 7. Optionally, in Safe Search, enable or disable "Safe Search" functionality from Google, Youtube, or Bing.

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

# Applying a URL Filtering Policy to a WLAN

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

To apply a URL filtering policy to a WLAN:

- 1. Go to WiFi Networks, select the WLAN you would like to configure, and click Edit.
- 2. Scroll down and expand the **Advanced Options** section.
- 3. Click the Access Control tab.
- 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 366 Enabling URL filtering for a WLAN

Hide Advanced Options	,					•
Zero-IT & DPSK WL	AN Priority Access Control	Radio Control	Others			
Call Admission Con	ntrol: 🔲 Enforce CAC when C	CAC is enabled on	the radio		10:05	
Rate L	imit: Per STA rate limiting wil	I not work if SSID	ate limiting	j is enabled.		
	Per Station Uplink	Disab	ed 🔻			
	Per Station Downlink	Disab	ed 🔻	]		
	Enable Per SSID Up	olink 0		mbps (0.1~200.0)		
	Enable Per SSID Do	ownlink 0		mbps (0.1~200.0)		
Access Col	ntrol: Layer2 MAC ACL :	No ACL	+			
	Layer3/4 ACL :	No ACL 🔻	+			
	Device Policy :	No ACL 🔻	+			
Application Visit	ility: 🔲 Enable					
	Apply policy group :	No_Policy	• + /			
URL Filte	ring: 🗹 Enable				10:05	
	URL Filtering Profile :	Profile 1	• +			
				OK Cancel		
						-

# Working with URL Filtering Licenses

URL filtering service requires an active URL filtering license to function. URL filtering licenses can be purchased from RUCKUS partners and distributors, and a temporary license is also available to allow customers to try out the service for a limited time of 90 days before purchasing.

Within 90 days, a valid URL filtering license that is greater or equal to the number of connected APs must be loaded; otherwise, URL filtering will be disabled until a valid license is loaded.

# FIGURE 367 URL Filtering License Warning Message



Complete the following steps to manage URL filtering licenses.

- 1. Go to Admin & Services > Services > URL Filtering.
- 2. Click the License tab and select one of the following options:
  - Update Services By File: Import a new locally saved license file.
  - Renew Services Online: Connect to the RUCKUS license server to download a license file.
  - Show Details: Select the license file from the list and click Show Details to view the license expiration details.

# FIGURE 368 Working with URL Filtering Licenses

🖵 System	•	Summary Profiles Lic	ense					
省 Services	•	1 Update Services By File	C Renew S	Services Online	details	Search	Q	2 0
AAA Servers		Unleashed ID		Number of AP	Start Time	Expires	Status	Sales Or
Access Control		un9418490011251569244	1593778	128	2019/09/24 10:23:48	2019/12/23 09:23:48	Active	URL Filte
Application Recognition & Control								
Bonjour Gateway						1-1	of 1 shown	« <b>1</b> »
Dynamic PSK								
Guest Access Service								
Hotspot Services								
Radio Control								

# Wi-Fi Calling

The RUCKUS Unleashed Wi-Fi Calling feature aims to provide better call quality by reducing latency, jitter, and roaming delays for voice calls over Wi-Fi.

To achieve this, the RUCKUS Unleashed access point must perform identification, classification, and marking of voice calls when Wi-Fi calling is enabled and a call is made from a supported client device. Once a call is identified, voice packets are classified and marked to be delivered over an Internet Protocol Security (IPsec) tunnel from the client through the AP and the controller and on to the mobile operator's data center.

The Wi-Fi calling provides the following benefits:

- Faster inter-AP roaming using RUCKUS SmartRoam along with standards-based .11r/k technologies minimizes IPsec session timeouts or teardowns to avoid call drops.
- Voice-aware SmartCast prioritization helps maintain sustained call quality even when there are other clients generating regular Internet packet data.
- A voice call on one SSID will be prioritized in the voice queue over Internet packet data from other SSIDs.

The process consists of the following steps:

- 1. User turns on Wi-Fi Calling in the phone menu, or turns on Wi-Fi and connects to the wireless network.
- 2. Client initiates a DNS lookup to the domain name of the Evolved Packet Data Gateway (ePDG) (for example, T-Mobile: ss.epdg.epc.mnc260.mcc310.pub.3gppnetwork.org).

## NOTE

The ePDG on an LTE network acts as an interface between the user device and the non-trusted 3rd Generation Partnership Project (3GPP) access network (for example, Wi-Fi hostpot), providing a security mechanism through a secure IPsec tunnel that is established with the user device.

- 3. Client initiates an Internet Key Exchange version 2 (IKEv2) handshake towards the ePDG to authenticate and set up an IPsec tunnel.
- 4. Client initiates an IPsec session towards the ePDG.
- 5. User is notified that Wi-Fi Calling is activated.
- 6. User initiates a voice call. All voice traffic is tunneled to the ePDG within the IPsec tunnel.

# **Creating a Wi-Fi Calling Profile**

A Wi-Fi calling profile must be associated to any WLAN with Wi-Fi calling enabled.

To create a Wi-Fi calling profile:

- 1. Go to Admin & Services > Services > W-Fi Calling and click the Profiles tab.
- 2. Click Create to create a new profile.

- 3. In the *Create New* dialog, enter the following to create a new profile:
  - Name: Enter a name for the profile.
  - **Description**: Optionally, enter a description of the profile.
  - QoS Priority: Select a priority from the list (typically, Voice for highest QoS priority).
  - Evolved Packet Data Gateway (ePDG): Click Create New to create a new ePDG entry. Enter Domain Name and optionally IP address, and click Save to save the entry.

## FIGURE 369 Create a Wi-Fi calling profile

		Per Station Up	link Disabled v		
Creat	te New			:	×
Gene	ral			•	
Evolv	* Qo	Name AT&T     AT&T     AT&T     OS Priority Voice     ta Gateway (ePDG)		•	
	Order	Domain Name	IP Address	Action	
	Order	Domain Name internal.att.com	IP Address 129.192.166.10	Action Save Cancel	
	1 •				
	1 •	internal.att.com		Save Cancel	

# Enabling Wi-Fi Calling for a WLAN

Once a Wi-Fi calling profile has been created, you must configure each WLAN with one or more profiles to enable the feature for the WLAN. To enable Wi-Fi calling for a WLAN:

- 1. Select the WLAN that will support Wi-Fi calling, and click **Edit**.
- 2. Click Show Advanced Options > Access Control.
- 3. In WiFi Calling, click Edit to select Wi-Fi calling profiles.

4. Select a profile from the list of Available Profiles, click the right arrow to move it to the list of Selected Profiles, and click **OK** to save your changes.

FIGURE 370 Add profiles from the available profiles to selected profiles for the WLAN

	Rate Limi	t: Per STA rate limiting will not w	vork if SSID rate limiting is enabled.		<b>^</b>
		Per Station Uplink	Disabled		
	Select Wi-Fi Calling	Profiles		×	(3:30
	Available Profiles	+ / 1	Selected Profiles		
	search here	Q	search here	Q	
	AT&T				
		-			
					3:30
			ок	Cancel	
Clients					Disconnected 0

5. Click **OK** to save the changes to the WLAN advanced options.

FIGURE 371 Enabling Wi-Fi calling for a WLAN

	Enable Per SSID Uplink     0     mbps (0.1~200.0)	
	Enable Per SSID Downlink     0     mbps (0.1~200.0)	
Access Control	: Layer2 MAC ACL : No ACL 🔻 +	
	Layer3/4 ACL : No ACL 🔻 🕈	
	Device Policy : No ACL 🔻 +	
Application Visibility	: Enable	
	Apply Policy Group : No_Policy T +	
URL Filtering	: Enable	
	URL Filtering Profile : Filter 1 +	
WiFi Calling	: 🖉 Enable	
	<i>ø</i> ₱ Edit	13:30
	Name	
	AT&T	
	OK Cancel	
Clients		Disconnected 0
Clients		
		· · · · · · · · · · · · · · · · · · ·

# **Tunnel Configuration**

Only WLANs that are enabled with Tunnel mode are affected.

Refer to Configuring Advanced WLAN Options on page 267 in the WLAN configuration section for information on enabling Tunnel mode.

Complete the following steps to configure data encryption and filtering for tunneled WLANs.

- 1. From the dashboard, select Admin & Services > Services.
- 2. Scroll down to the bottom of the page and locate the Tunnel Configuration section.
- 3. Select the check boxes next to the options you want to enable.
  - Enable tunnel encryption for tunneled traffic: By default, when WLAN traffic is tunneled to Dedicated Master, only the control traffic is encrypted while data traffic is unencrypted. When this option is enabled, the Access Point will decrypt 802.11 packets and use an AES-encrypted tunnel to send them to Dedicated Master.
  - Block multicast traffic from network to tunnel: Prevents [all/non-well-known] multicast traffic from propagating on the tunnel.
  - Block broadcast traffic from network to tunnel except ARP and DHCP: Prevents all broadcast traffic other than Address Resolution Protocol and DHCP packets.
  - Enable Proxy ARP of tunnel WLAN with rate limit threshold: Reduces tunnels. When Dedicated Master receives a broadcast ARP request for a known host, it acts on behalf of the known host to send out unicast ARP replies at the rate limit it will forward it to the tunnel to all APs according to the rate limit threshold set in the Packet Inspection Filter program (like Wireshark).
- 4. Click Apply in the same section to save your changes.

## FIGURE 372 Setting Tunnel Configuration Parameters for all WLANs with Tunnel Mode Enabled

Admin & Services		•
System  AAA Servers  AAA Servers  Access Control  Application Recognition & Control  Bonjour Gateway  Dynamic PSK  Guest Access Service  Hotspol Services  Radio Control  WIPS  URL Filtering  Wi-Fi Calling  Tunnel Configuration	Tunnel Configuration         Block       multicast traffic from network to tunnel.         Block block       multicast traffic from network to tunnel except ARP and DHCP.         Enable Proxy ARP of tunnel WLAN rate limit threshold       10         (Range: 0 - 3000 pitatisec)	Apply

# **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 373 Configuring administrator preferences

Admin & Ser	vices	▼
🛄 System	Language	
省 Services	Select the display language that you want to use on the Web interface. Language: English	
Administration	Administrator Name/Password	
Preferences	Authenticate using the admin name and password     Authenticate with Auth Server Ruckus AD     +	
Backup & Restore	Fallback to admin name/password if failed	
Upgrade	Admin Name* admin	
Registration	Current Password*	
Diagnostics	New Password Remain empty will keep current password 🏾 🛷	
Certificate	Confirm New Password Remain empty will keep current password 🎻	_
Network Connectivity	Apply	
Network Management	Setup Password Recovery  Enable Password Recovery	
Mobile App	Apply	

## FIGURE 374 Enabling password recovery

Preferences	Authenticate with Auth Server Ruckus AD +
Backup & Restore	Fallback to admin name/password if failed
Upgrade	Admin Name* admin
Registration	Current Password*
Diagnostics	New Password Remain empty will keep current password
Certificate	Confirm New Password Remain empty will keep current password 🎻
Network Connectivity	Apply
Network Management	Setup Password Recovery
Mobile App	Security email and security question will be used to verify your identity if you forgot your password or username Security Email* example@example.com
	Security Question*
	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 375 Backup and Restore

Admin & Serv	ices	
🛄 System	Back Up Configuration	
🕘 Services	Click Back Up to save an archive file of your current Unleashed configuration. This archive will simplify system recovery if needed.  Back up	
Administration	Restore Configuration	
Preferences	If you need to restore the system configuration, click Browse, and then select the backup file that contains the settings that you want to restore.	
Backup & Restore	Browse	
Upgrade		
Registration	Restore to Factory Settings	
Diagnostics	If needed, you can restore Unleashed to its factory settings, which will delete all settings that you have configured. You will need to manually set up Unleashed again. For more information, see the online help.	
Certificate	Restore to Factory Settings	
Network Connectivity	restore to 1 dotory Settings	
Network Management		

# FIGURE 376 Choose a Restore type

Admin & Serv	ices	
🛄 System	Back Up Configuration	
Services	Click Back Up to save an archive file of your current Unleashed configuration. This archive will simplify system recovery if needed. Back up	
Administration	Restore Configuration	
Preferences	If you need to restore the system configuration, click Browse, and then select the backup file that contains the settings that you want to restore.	
Backup & Restore	Ruckus-Unleashed db 082719 11 07.bak (579672 bytes). Choose a restore type:	
Upgrade	Restore everything.	
Registration	Restore everything, except system name and IP address settings (for failover deployment at the same site).	
Diagnostics	Restore only WLAN settings, access control list, roles, users, country code and system time (use this as a template for	
Certificate	different sites).	
Network Connectivity	Restore	
Network Management	Restore to Factory Settings	
Mobile App	If needed, you can restore Unleashed to its factory settings, which will delete all settings that you have configured. You will need to manually	

# **Restore to Factory Settings**

In certain extreme conditions, you may want to re-initialize your Master AP and reset it to the factory default state. Once the Master has been reset to factory default state, all AP logs, client logs, application data and other records, wireless networks, user accounts, and any other configuration settings must be reconfigured.

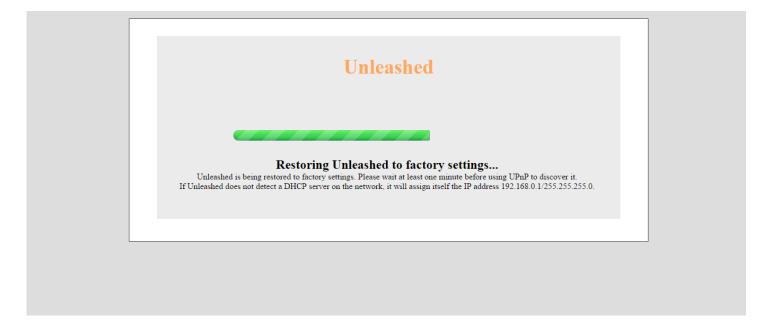
Complete the following steps to reset your Master AP to factory default settings:

- 1. Go to Admin & Services > Administer > Backup & Restore.
- 2. Click Restore to Factory Settings.
- 3. Click **OK** to confirm.

The **Restoring Unleashed to factory settings** progress screen appears. Wait for this progress screen to finish before attempting to login again.

4. Repeat the initial setup and configuration procedures as described in Setting Up an Unleashed Wi-Fi Network on page 129.

# FIGURE 377 Restore Factory Settings Progress Screen



# **Alternate Factory Default Reset Method**

If you are unable to complete the software-based resetting of RUCKUS Unleashed to factory default, you can use the following "hard restore" method.

# NOTE

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

- 1. Locate the **Reset** pin hole on the rear panel of the Master AP.
- 2. Insert a straightened paper clip in the hole and press for at least 6 seconds.

After the reset is complete, the PWR LED will initially be solid red, indicating bootup is in process. The LED then blinks green, indicating that the system is in the factory default state.

After you complete the Setup Wizard, the PWR LED will be steady green.

# **Rediscovering the Unleashed AP on the Network**

If you do not know the IP address, you can rediscover an Unleashed AP on the network using UPnP or Bonjour service discovery.

To discover an Unleashed AP using UPnP (Windows clients only), go to the **Network** section of Windows Explorer (**Start > Network** or **Start > Computer > Network**). Locate the Unleashed device in the *Network Infrastructure* section. Double-click the icon to launch the web UI, or right-click and select **View device webpage**, or type the address displayed into your browser's navigation bar.

# FIGURE 378 Discovering Unleashed using UPnP in Windows

Co ⊂ 🗣 ト Network ト	A CALL REAL PROPERTY AND A	✓ 4y Search Netwo	ork	x P
Organize 👻 Network and Sharing	Center Add a printer Add a wireless device		•= <b>•</b>	0
Year of the second	Computer (1)     Network Infrastructure (2)     Ruckus-Unleashed 10.10.0.70     ZoneDirector1200 10.10.0.175			
3 items				

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 465
- Local Upgrade on page 468

# **Online Upgrade**

Use the online upgrade method to upgrade your RUCKUS Unleashed network with the latest firmware available from the RUCKUS Unleashed firmware server.

Complete the following steps to upgrade the Master AP and all connected member APs using the online upgrade method:

- 1. Go to Admin & Services > Administer > Upgrade.
- 2. Select Online Upgrade.
- 3. Under Select Firmware Version, select one of the available firmware versions.

## NOTE

You can rollback to the previous image version and restore the configuration of the previous version. The roll back syncs automatically to all member APs. If the old Master AP reboot fails and a member AP becomes the Master AP, then the new Master AP can still roll back to the previous version with the corresponding configuration.

# NOTE

Optionally, select **Auto reboot the system** to automatically reboot each AP after the firmware has been deployed to the AP. By default, this option is enabled. You may want to disable this option if you prefer to wait until all APs have the new firmware before rebooting them all at once. That is, if you have multiple Unleashed AP models that require different firmware image files, you can either select the **Auto reboot the system** option and wait until all the APs have finished downloading the firmware and the entire Unleashed network is automatically rebooted, or you could choose to wait until all the APs have finished downloading the firmware and click **Reboot** to reboot the entire Unleashed network.

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

# FIGURE 379 Configuring Online Upgrade

Clients No Clients	Total 0 Connected 0 Blocked
Access Points	Total 2 Working 2 Disconnected
Admin & Services	
System	Firmware Upgrade Current firmware version: 200.2.9.13.156
Administer     Preferences Backup & Restore	Select upgrade method:  Contine Upgrade Contine Upgrade Conventional firmware from Ructus Witeless)  Select firmware version:
Upgrade Registration Diagnostics	Loading   Reload  Upgrade
Certificate	Allo reboot the system  AP Role Name Mac Model Upgrade Progress
Network Connectivity Network Management	Master         RuckusAP         10.bb.52:1b:10.40         R500           Member         RuckusAP         10.bb.52:1c:12:c0         R500

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 380 Successful Online Upgrade

Clients No Clients	Total 0 Connected 0 Blocked	•
Access Points	Total 2 Victing 2 Disconnected	•
Admin & Services		▼
System	Firmware Upgrade Current firmware version: 200.2.9.13.156	
Administer  Preferences Backup & Restore	Select upgrade method: Online Upgrade Ownload finware from Ruckus Wireless) Upload finware from local PC) Select image file(s) & Upgrade	
Upgrade	(Upgrade one model at at ärne. <b>Varning: Leave fils page will reset the local upgrade process.</b> ) Model R500 (2 APs) Filename. rols_/he/Dr (20590940 bytes), Version: 200.2.9.13.146	
Diagnostics	AP Role Name Mac Model Upgrade Progress	
Certificate	Master RuckusAP f0:b0:52:1b:10:40 R500 Success 100%	
	Member RuckusAP 10:b0:52:1c:12:c0 R500 Success 100%	
Network Connectivity		
Network Connectivity Network Management	Reboot Cancel	

5. When all of the APs in the list display "Success 100%" in the **Upgrade Progress** column, click **Reboot**. The **Rebuilding the Unleashed Network** progress screen appears.

FIGURE 381 Rebuilding the Unleashed Network Progress Screen

Rebuilding the Unleashed Network. It may take a few minutes. WARNING - Do not power off or reboot the AP. - Do not refresh your browser or hit the browser's back button.	
WARNING - Do not power off or reboot the AP.	Rebuilding the Unleashed Network. It may take a few minutes.
- Do not power off or reboot the AP.	
	- Do not power off or reboot the AP.
	- Do not refresh your browser or hit the browser's back button.

After the process is completed, you are redirected to the login page.

6. Log in and go to Admin & Services > System > System Info to confirm the new software build number.

# Local Upgrade

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

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

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

## FIGURE 382 The Upgrade Page

Clients No Clients						Total 0	Connected 0	Blocked	►
Access Points						Total 2	Working 2	Disconnected	►
Admin & Services									▼
System	Firmware	Upgrad	e Current firmwar	e version: 2	200.2.9.13.156				
Services									
Administer   Preferences	Select upgrad Online Up (Download			Local U (Upload)	Ipgrade Irmware from local PC)				
Backup & Restore	Select firmwar								
Upgrade	Loading	• Re	eload						
Registration			Upgrad	de					
Diagnostics			<ul> <li>Auto reboot</li> </ul>						
Network Connectivity	AP Role Master	Name RuckusAP	Mac f0:b0:52:1b:f0:40	Model	Upgrade Progress				
Network Management	Member	RuckusAP	10:b0:52:1c:12:c0						

2. Select Local Upgrade as the upgrade method.

3. Click Browse to locate the firmware image file on your local computer.

RUCKUS Unleashed will perform a check to make sure it is the proper image for the AP model before proceeding.

#### NOTE

Each AP model has a different firmware image file that must be loaded onto the Master and then distributed to all member APs of that model. So, for example, if you have a mix of RUCKUS Unleashed R510 and R610 APs, you could upgrade all of the R510s first and then the R610s, or the other way around, but you cannot upgrade both models at once.

#### NOTE

While the upgrade process will check to make sure you do not try to upgrade an RUCKUS Unleashed AP with the incorrect model firmware, there is no check to ensure that you do not upgrade/downgrade an RUCKUS Unleashed AP to a RUCKUS Solo AP (standalone) firmware image. If you do this, the AP will no longer function as an RUCKUS Unleashed AP until RUCKUS Unleashed firmware is re-loaded onto it.

#### FIGURE 383 Local Upgrade

Clients No Cl	Sents				Total 0	Connected 0	Blocked	
Access Points					Total 2	Working 2	Disconnected	►
Admin & Services								V
System	Firm	nware Upgrade	Current firmware version: 2	00.2.9.13.156				
Administer   Preferences	•	elect upgrade method: Online Upgrade (Download firmware from Ruckus V	Local U Vireless)     (Upload 1	pgrade rmware from local PC)				
Backup & Restore Upgrade Registration		elect image file(s) & Upgrade (Upgrade one model at a time. Warning Model R500 (2 APs) Browse	y: Leave this page will reset the local up	grade process.)				
Diagnostics	AP	AP Role Name	Mac Model	Upgrade Progress				
Certificate	Ма	Aaster RuckusAP	f0:b0:52:1b:f0:40 R500					
Network Connectivity	Me	Jember RuckusAP	f0:b0:52:1c:12:c0 R500					

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

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

FIGURE 384 Upgrade successful, click Reboot to reboot the APs and apply the new firmware

Clients		No Clients						Total 0	Connected 0	Blocked	►
Access Points	;							Total 2	Working 2	Disconnected	►
🗘 Admin & Serv	ices										•
🛄 System	Þ		Firmware	Upgrade	Current firmwa	re version: 1	200.2.9.13.156				
Services     Administer Preferences	•		Select upgrade		Wireless)	Local U (Upload)	Ipgrade firmware from local PC)				
Backup & Restore Upgrade Registration			(Upgrade one m Model R500 (	2 APs)	ng: Leave this page will re		ograde process.)				
Diagnostics			AP Role	Name	Мас	Model	Upgrade Progress				
Certificate			Master	RuckusAP	f0:b0:52:1b:f0:40	R500	Success 100%				
Network Connectivity			Member	RuckusAP	f0:b0:52:1c:12:c0	R500	Success 100%				
Network Management							Reboot Cancel				

Repeat steps 3-5 for any additional AP models. 6.

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

Rebuilding the Unleashed Network. It may take a few minutes. WARNING - Do not power off or reboot the AP. - Do not refresh your browser or hit the browser's back button.	WARNING - Do not power off or reboot the AP.
- Do not power off or reboot the AP.	- Do not power off or reboot the AP.

FIGURE 385 "Rebuilding the Network" Progress Screen

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

# **Diagnostics**

The *Diagnostics* pages provide options for troubleshooting and diagnostics, including configuration settings for alarms, viewing system event log messages, configuring which debug information is to be collected in log files, and saving the current logs to your local computer.

## FIGURE 386 Configuring Diagnostics Options

🛄 System	•									
		All Alarms	Events	Debug Info	Logs	SpeedFlex Service	Client Troubleshooting	Packet Capture		
Services		Alarms							l	
		This workspa	ace lists all	uncleared ala	rms. If al	l listed alarms have be	en cleared or are no longe	r valid, click Clear A	AII.	
Administration	•	Clear	All Clea			Se	earch	۹ All -	· 2 •	
Preferences		Date	/Time 🗸	Sev	/erity	User	Activities			
Backup & Restore		2020	/04/20 14	:00:08 Hig	h		A new Same-Ne	etwork Rogue[f0:b0:	:52:1b:f0:4c] with S	
Upgrade		2020	/04/20 14:	:00:07 Hig	h		A new Same-Ne	etwork Rogue[f0:b0:	:52:1b:f0:48] with S	
Registration		2020	/04/20 13:	53:05 Hig	h		A new Same-Ne	etwork Rogue[b4:79	):c8:14:26:4c] with S	
Diagnostics		2020	/04/20 13:	:53:04 Hig	h		A new Same-Ne	etwork Rogue[b4:79	0:c8:14:26:48] with \$	
Certificate		2020	/04/20 13:	47:54 Hig	h		A new Same-Ne	etwork Rogue[44:1e	e:98:1b:f0:dc] with S	
Network Connectivity			/04/20 13:					etwork Rogue[44:1e		

# **Viewing Alarms**

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

To view and clear recent alarm messages:

- 1. Go to Admin & Services > Administration > Diagnostics > All Alarms.
- 2. To delete an alarm event from the list, select it and click **Clear**.

3. Click Clear All to clear all alarm events from the list.

#### FIGURE 387 Viewing a List of Alarm Event Messages

	vices									•
🖵 System	•									
		All Alarms	Events	Debug Info	Logs	SpeedFlex Service	Client Troubleshooting	Packet Capture		
Services	•	Alarms							I	
		This workspa	ace lists all	uncleared al	arms. If al	l listed alarms have be	en cleared or are no longe	r valid, click Clear	All.	
Administration	•	Clea	r All Clear			Se	earch	Q All	- 2 0	
Preferences		Date	e/Time 👻	Se	verity	User	Activities			
Backup & Restore		2020	0/04/20 14:	00:08 Hig	gh		A new Same-Ne	etwork Rogue[f0:b0	):52:1b:f0:4c] with S\$	
Upgrade		2020	0/04/20 14:	00:07 Hig	gh		A new Same-Ne	etwork Rogue[f0:b0	):52:1b:f0:48] with S	
Registration		2020	0/04/20 13:	53:05 Hij	gh		A new Same-Ne	etwork Rogue[b4:79	9:c8:14:26:4c] with S	
Diagnostics		2020	0/04/20 13:	53:04 Hi	gh		A new Same-Ne	etwork Rogue[b4:79	9:c8:14:26:48] with \$	
Certificate		2020	0/04/20 13:	47:54 Hig	gh		A new Same-Ne	etwork Rogue[44:16	e:98:1b:f0:dc] with S	

# Viewing System Event Messages

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

Compared to Alarms, Event messages include less critical messages - such as when an AP changes channel, a configuration sync is performed, a new client joins the network, etc.

You can customize the level of events to display in the Events list using the Event Log Level setting, as follows:

- Any: All event log levels will be displayed.
- Critical & Warning: Only events whose log level is "critical" or "warning" level appear.
- Critical Only: Only events whose log level is "critical" will appear.

#### FIGURE 388 The Events Page

🛄 System	▶		~	~	V			
	All Alarms	Events	Debug Info	Logs	SpeedFlex Service	Client Troubleshooting	Packet Capture	
🞱 Services	Events Se	ettings						
			The second		arning <ul><li>Critical Only</li></ul>			
Preferences Backup & Restore	Events		eniy edi		aming (Chucai Oniy			Apply
	- Events This work	_				rnal log file. (For informati	on on saving this inf	
Backup & Restore	This work server, se	space displa e the Online	ys the most re-		rds in Unleashed's inte	rnal log file. (For informati	-	formation to a syslog
Backup & Restore Upgrade	This work server, se	space displa	ys the most re-		rds in Unleashed's inte	rnal log file. (For informati	on on saving this Inf	formation to a syslog

# **Configuring Debug Logs**

You can use the **Diagnostics > Debug Info** page to configure which debug components to include in log files and on the **Events** page.

#### NOTE

Check the box Debug log per APs or clients MAC address and enter AP/Client info to filter debug output for a specific AP or client.

You can also save the log files using the **Save Debug Info** button. If you request assistance from Ruckus technical support, you may be asked to supply detailed debug information from RUCKUS Unleashed.

Click the **Save Debug Info** button, and then save the file to your computer. You can then email this file to Ruckus Support to assist with troubleshooting.

## NOTE

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

You can also allow the Master AP to automatically save log files to a specified FTP or TFTP server in the event of a controller process failure. By default, this feature is disabled. When enabled, the Master will send the core, dump, and debug files to an FTP/TFTP server before restart. This information can be very useful in debugging controller reboot issues. To enable this feature, select the check box next to **Enable upload debug logs** to remote server, select **FTP** or **TFTP**, and enter the server address only (for TFTP) or **Host**, **Port**, **Username** and **Password** (for FTP).

## FIGURE 389 The Debug Info Page

Admin & Ser	vices		7
🛄 System		All Alarms Events Debug Info Logs SpeedFlex Service Client Troubleshooting Packet Capture Network Connectivity	
Services	•	, Debug Logs	
		Debug Components	
Administration	-	System Management Web Authentication	
Preferences		🛛 RADIUS 🖉 Access Points	
		RF Management Dispot Services	
Backup & Restore		🖾 Web Server 🖉 Auto Election	
Upgrade		Client Association	
Diagnostics		🛛 802.1x 🕑 802.11	
Certificate		Smart Redundancy	
Centificate		Debug log per AP's or client's mac address	
Network Management		(e.g. aatbb:cc:dd:ee.ff)	
Mobile App			Apply
Technical Support			

# 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 390 The Logs Page

🛄 System 🕨 🕨	
	All Alarms Events Debug Info Logs SpeedFlex Service Client Troubleshooting Packet Capture
🔐 Services 🕨 🕨	System Logs
Administration	To show current system logs, click here. Save System Log
Preferences	AP Logs
Backup & Restore	To show current APs' logs, click here .
Upgrade	
Registration	
Diagnostics	
Certificate	
Network Connectivity	

# **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 391 Displaying Current AP Logs

	•
□ System ►	
L System	All Alarms Events Debug Info Logs SpeedFlex Service Client Troubleshooting Packet Capture
😂 Services 🕨 🕨	System Logs
Administration     Vreferences	To show current system logs, click here. Save System Log AP Logs
Backup & Restore	To show current APs' logs, click here .
Upgrade	
Registration	Apr 27 17:13:24 Ruckus-Unleashed last message repeated 4 times Apr 27 17:14:24 Ruckus-Unleashed last message repeated 4 times
Diagnostics	Apr 27 17:15:09 Ruckus-Unleashed last message repeated 3 times Apr 27 17:16:24 Ruckus-Unleashed last message repeated 5 times
	Apr 27 17:17:24 Ruckus-Unleashed last message repeated 4 times Apr 27 17:18:24 Ruckus-Unleashed last message repeated 4 times
Certificate	

# **SpeedFlex Service**

SpeedFlex service (enabled by default) can be disabled to prevent mobile or web clients from performing a SpeedFlex performance test. For more information on the SpeedFlex performance testing tool, see Running a SpeedFlex Performance Test on a Wireless Client on page 355. To disable SpeedFlex, clear the **Enable SpeedFlex Service** option and click **Apply**.

## FIGURE 392 Enabling or Disabling SpeedFlex Service

🛄 System							v			
		All Alarms	Events	Debug Info	Logs	SpeedFlex Service	Client Troubleshooting	Packet Capture		
Services		SpeedFlex S	Service							_
Administration	•	Enable Spee	edFlex too	I on the system	n, user ca	an test SpeedFlex from	webUI or Mobile App.			
		🗷 Enable S	SpeedFlex	Service						
Preferences									Apply	
Backup & Restore										
Upgrade										
Upgrade Registration										
Registration										

# **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 393 Click Troubleshooting to perform client connectivity trace

	Ітапіс: 0.15 МВ		
Clients	Clients	Total 2 Conn	ected 2 Disconnected 0
2 clients connected, 0 clients disco	nnected.		
Wired Clients	0 wired clients connected		•
Wireless Clients	2 wireless clients connected		▼
Show details Rename 🛉 Mar	k Favorite 🗶 Unmark Favorite Troubleshooting More 🗸	Search	Q 2 0
★ Mac Address	IP Address OS Name	User AP Name	wlan s
f0:03:8c:fb:73:38	192.168.0.2 N/A	Unleashed	Unleashed E
04:b1:67:47:c4:20	192.168.0.11	RuckusAP	Unleashed E
		1-2	of 2 shown < 1 >
Access Points		Total 3 Wor	king 3 Disconnected 0

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 394 Click Start to begin connectivity trace

		-							ced 0	
3 Client(:	Troubleshooting								×	
Block	*Client MAC Address	3c:a9:f4:48:af:90 Please connect your clie	nt manually aft	er start troubles	hooting, if the cli	ent is connected,	it will be disconr	ected firstly and th	en connect automa	tically.
os		·	,		<u>,</u>					
	Connectivity Trace	► Start Stop	📋 Clear	1 Import	Ł Export					
						Nucitus-on	cashed onice	oncu	LAGOIOIR	
	10.00.00.10.10.00	10.10.0.07	Roomb							
	10.00.00.10.10.00	10.10.0.07	Koomo	a-r opo				1-3 of 3 sh	own « 1 »	

#### FIGURE 395 Connectivity trace in progress

Access Points hearing	client's probe requests	:				
Name	Radio	Client SNR (dBm)	Latency (ms)	Connection Failure (%)	Airtime Utilization (%)	
Ruckus-Unleashed	5GHz (36)	58	0	0.00	0	-0
RuckusAP	5GHz (36)	39	0	0.00	0	
RuckusAP	2.4GHz (1)	37	0	0.00	12	
Ruckus-Unleashed	2.4GHz (11)	92	0	0.00	3	•
✓ 802.11 Disassoci	ation 9:56:46	Info 🕥			1-4 of 4 shown ≤ 1 ≥	
<ul> <li>✓ 802.11 Disassoci</li> <li>AP: RuckusAP(f0:b0:52:1</li> </ul>					Time:9:56:46	
AP: RuckusAP(f0:b0:52:1	1c:12:c0) <b>SSID:</b> Unleast ation Request 9:56:46	Radio: 5GHz	Unleas	S XXX	Time:9:56:46	
AP: RuckusAP(f0:b0:52:1	1c:12:c0) <b>SSID:</b> Unleast ation Request 9:56:46	Radio: 5GHz	Unleashed	AVA Server		
<ul> <li>AP: RuckusAP(f0:b0:52:1</li> <li>✓ 802.11 Authentica</li> <li>✓ 802.11 Authentica</li> </ul>	1c:12:c0) <b>SSID:</b> Unleast ation Request 9:56:46	Radio: 5GHz		AAA Server	Time:9:56:46	

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

# **Saving Client Connection Logs**

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

RUCKUS Unleashed provides two options for saving client connection logs - download the current log file immediately from the web interface, or configure RUCKUS Unleashed to send the logs to a syslog server automatically. For information on delivering logs to syslog, see *Customizing the Current Log Settings*.

To download and save current client connection logs:

- 1. Go to Admin & Services > Administration > Diagnostics > Client Troubleshooting, and locate the Client Connection Logs section.
- 2. In "To save client connection logs. click here," click the click here link.
- 3. Save the file to your local computer.

FIGURE 396 Saving Client Connection Logs to a Local Computer

<u>□</u> System	•								
	-	All Alarms	Events	Debug Info	Logs	SpeedFlex Service	Client Troubleshooting	Packet Capture	
Services		Client Troub	leshooting	)			1		
Administration	•			hooting, click h	iere				
Preferences		Client Conn							
Backup & Restore		to save clie	nt connect	tion logs. click l	nere				
Upgrade									
Registration									
Diagnostics									
Certificate									
Network Connectivity									

# **Capturing Remote Packets**

Remote packet capture puts one or more APs into packet sniffer mode, allowing them to capture the wireless packets. The packets are either saved to local files or streamed to packet inspection program such as Wireshark for later analysis.

- 1. Go to Admin & Services > Administration > Diagnostics > Packet Capture.
- 2. For Radio, select 2.4 GHz or 5 GHz.

3. Under Currently Managed APs, select APs from the list and click Add to Capture APs.

## FIGURE 397 Adding Currently Managed APs to Capture APs

Admin & Services		•
System S	All Alarms       Events       Debug Info       Logs       SpeedFlex Service       Client Troubleshooting       Packet Capture         Packet Capture       Use this feature to capture wireless packets during normal operation and save them in local files or stream them to Wireshark.       Radio 2.4 GHz • 5GHz         Radio 2.4 GHz • 5GHz       Capture APs       Capture APs         Add to Capture APs       Capture APs       Capture APs         MAC Address • IP Address       Device Name       • • • • • • • • • • • • • • • • • • •	-
Network Management Mobile App		

The selected currently managed APs are moved to the Capture APs table.

- 4. Select Local Mode or Streaming Mode as the capture mode.
  - To capture a limited snapshot on each AP, select Local Mode.
    - a. Click **Start** to begin capturing packets.
    - b. Click **Stop** to end the capture.
    - c. Click Save to save the packet capture to a local file.
  - To stream the captured packets to Wireshark, select **Streaming Mode**.
    - a. Click **Start** to launch Wireshark.
    - b. Select Capture Options. Under Capture: Interface, select Remote. A Remote Interface dialog box is displayed.
    - c. Under Host, enter the IP address of the AP you want to view. Leave the Port field empty and click OK.

The remote host interface list on the right side is updated.

d. Select wifi0 or wifi1 from the list, depending on whether you are streaming on the 2.4-GHz or 5-GHz radio.

#### FIGURE 398 Selecting the Capture Mode

Admin & Services		
System		
	All Alarms Events Debug Info Logs SpeedFlex Service Client Troubleshooting Packet Capture	
Services	Packet Capture Use this feature to capture wireless packets during normal operation and save them in local files or stream them to Wireshark.	
Administration	Radio 🔿 2.4GHz 💿 5GHz	
Preferences	Current Managed APs Capture APs Search Q 2 Remove All Remove A	
Backup & Restore	MAC Address V IP Address Device Name Device Name Device Name	
Upgrade	No data available.	
Diagnostics		
Certificate	0-0 of 0 shown < 1 >	
Network Connectivity	Local Mode (Capture a limited snapshot on each AP, then Stop and Save to file)	
Network Management	Filter (Packets to/from one IP or MAC address)	
Mobile App	<ul> <li>Streaming Mode(Use Wireshark\'s Remote Capture Option to connect to wifi0 or wifi1)</li> </ul>	
	Start Save	

# 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 399 SSL certificate screens

System  Generate a request Import Signed Certificate Advanced Options  Generate a request Import Signed Certificate Advanced Options  Generate a request Create a new certificate request. For more Information, click here.  Common Name' MyCompany  Subject Alternative Name IP   Organization Int  Organization Int  Organization Int  Country' Sunnyvale  State/ Province' California  Country' United States	•	No Traffic					Total 2	Working 2	Disabled	
Admin & Services   System   Services   Administer   Cenerate a request   Common Name   MyCompany   Subject Atternative Name   Deprate   Common Name   MyCompany   Subject Atternative Name   Deprate   Common Name   MyCompany   Subject Atternative Name   Deprate   Common Name   MyCompany   Subject Atternative Name   Deprotes	Clients	No Clients					Total 0	Connected 0	Blocked	
System  System  Cenerate a request Import Signed Certificate Advanced Options  Cenerate a request Create a new certificate request. For more information, click here. Common Name McCompany Subject Atternative Name IP  Organization  Subject Atternative Name IP  Country United States  Country United States	Access Points						Total 2	Working 2	0 Disconnected	
Generate a request Import Signed Certificate Advanced Options     Generate a request Generate a request     Create a new certificate request. For more information, click here.     Common Name* MyCompany     Subject Alternative Name IP •      Organization II     Organization III     Locality/City Sunnyvale     Diagnostics Common V     Organization III	Admin & Services									
Organization Unit     Organization Unit       Jpgrade     Locality/ City       Legistation     State/ Province       State/ Province     California       Jagnostics     Country	⊇ System	Generate a request Import S	aned Certificate Advanced Ontions							
Diagnostics Country <sup>*</sup> United States	Administer 💌	Generate a request Create a new certificate reque Common Name' Subject Alternative Name	st. For more information, click here. MyCompany		 	 				
		Generate a request Create a new certificate reque Common Name <sup>*</sup> Subject Alternative Name Organization* Organization Unit	st. For more information, click here. MyCompany IP  TDepartment		 	 				
	Administer  Preferences Backup & Restore Upgrade Registration	Generate a request Create a new certificate reque Common Name* Subject Alternative Name Organization* Organization Unit Locality/ City* State/ Province*	st. For more information, click here. MyCompany IP v [ IT Department Sunnyvale California						Apply	

# **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 400	Generating a	CSR file
------------	--------------	----------

Clients Access Admin 8	Points & Services			Total 0 Connected 0 Blocked Total 2 Working 2 Disconnected	• •
🎗 Admin 8	& Services			Total 2 Working 2 Disconnected	•
•					▼
🛄 System					
Services	•	Generate a request Impo Generate a request Create a new certificate re	rt Signed Certificate Advanced Optio		
Administer Preferences	r 🔻	Common Name* Subject Alternative Name		The fully qualified domain name for your web server. This must be an exact match. e.g. www.nckuswietess.com The subject alternative name extension allows various literal values to be included in the configuration file. These include DNS (type your domain The subject alternative name extension allows various literal values to be included in the configuration file. These include DNS (type your domain The subject alternative name extension allows various literal values to be included in the configuration file.	
Backup & Restore		Organization*	IT Department	name), IP (type your IP address). The exact legal name of your organization. Do not abbreviate your organization name. e.g.Ruckus Wireless, Inc.	
Upgrade		Organization Unit		Division or department of the organization. e.g. Network Management	
Registration		Locality/ City*	Sunnyvale	The city where your organization is legally located. e.g. Sunnyvale	
Diagnostics		State/ Province*		The state or province where your organization is legally located. Can not be abbreviated. e.g. CA	
Certificate		Country*	United States •		-
Network Connectivity				Арріу	
Network Management					

- 5. Go to a certificate authority's web site and follow the instructions for purchasing an SSL certificate.
- 6. When you are prompted for the certificate signing request, copy and paste the content of the text file that you saved to your local computer, and then complete the certificate purchase.

After the certificate authority approves your CSR, you will receive the SSL certificate via email. The following is an example of a signed certificate that you will receive from a certificate authority:

BEGIN CERTIFICATE
MIIFVjCCBD6gAwIBAgIQLfaGuqKukMumWhbVf5v4vDANBgkqhkiG9w0B
AQUFADCBsDELMAkGA1UEBhMCVVMxFzAVBgNVBAoTDlZlcmlTaWduLCBJ
bmMuMR8wHQYDVQQLBgEFBQcBAQRtMGswJAYIKwYBBQUHMAGGGGh0dHA6
Ly9vY3NwLnZlcmlzaWduLmNvbTBDBggrBgEFBQcwAoY3aHR0cDovL1NW
UlNlY3VyZS1haWEudmVyaXNpZ24uY29tL1NWUlNlY3VyZTIwMDUtYWlh
LmNlcjBuBggrBgEFBQcBDARiMGChXqBcMFowWDBWFglpbWFnZS9naWYw
ITAfMAcGBSsOAwIaBBRLa7kolgYMu9BSOJsprEsHiyEFGDAmFiRodHRw
Oi8vbG9nby52ZXJpc2lnbi5jb20vdnNsb2dvMS5naWYwDQYJKoZIhvcN
AQEFBQADggEBAI/S2dmm/kgPeVAlsIHmx-
751o4oq8+fwehRDBmQDaKiBvVXGZ5ZMnoc3DMyDjx0SrI91kPsn223CV
3UVBZo385g1T4iKwXgcQ7WF6QcUYOE6HK+4ZGcHermFf3fv3C1-
FoCjq+zEu8ZboUf3fWbGprGRA+MR/dDI1dTPtSUG7/zWjXO5jC//
0pykSldW/q8hg08kq30S8JzCwkqrXJfQ050N4TJtgb/
YC4gwH3BuB9wqpRjUahTiK1V1-
ju9bHB+bFkMWIIMIXc1Js62JClWzwFgaGUS2DLE8xICQ3wU1ez8RUPGn
wSxAYtZ2N7zDxYDP2tEiO5j2cXY708mR3ni0C30=
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 486 for instructions.

# Importing an SSL Certificate

After you receive the signed certificate from the certificate authority, you must import it into RUCKUS Unleashed.

Complete the following steps to import a signed certificate.

1. Click the **Browse** button and select the file that contains the certificate (in PEM, CRT, or CER format) to upload it.

## FIGURE 401 Import Signed Certificate Tab

Admin & Ser	rices	
🛄 System	Generate a request Import Signed Certificate Advanced Options	_
실 Services	Import Signed Certificate To show current certificate information, click here.	
Administration	Import a signed certificate file to replace the current certificate, or import the backup certificate file from another Unleashed     Browse	
Preferences		
Backup & Restore		
Upgrade		
Diagnostics		
Certificate		
Network Management		
Mobile App		
Technical Support		

2. If there are no intermediate CA certificates, click the Import button to install the uploaded certificate.

#### NOTE

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

#### NOTE

Beginning with Unleashed 200.13, the Elliptic Curve Cryptography (ECC) certificate is supported. The recommended encryption algorithm is Prime256v1.

#### NOTE

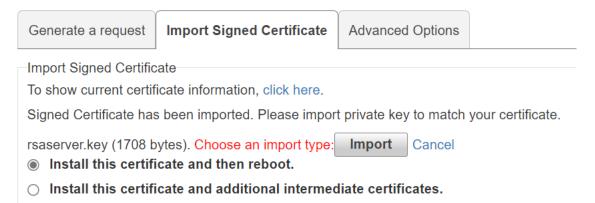
Currently, the dual-certificate mode is not supported on an Unleashed AP. If an Elliptic Curve Cryptography certificate is used, the browser of the earlier version may fail to log in to the Unleashed web interface.

#### FIGURE 402 Installing a Private Key

Generate a request	Import Signed Certificate	Advanced Options	
Import Signed Certific	cate		
To show current certif	icate information, click here.		
Import a signed certif	icate file to replace the current	certificate, or import th	he backup certificate file from another Unleashed
	2 bytes). The uploaded certific ificate and then re-install a c		h Unleashed's private key. Import Cancel ich matches Unleashed's private key.
Accept this certi	ficate and then install a priva	ate key to match you	r certificate.

- 3. If the certificate was issued by an intermediate CA, you must also import the intermediate CA certificate (as well as all other intermediate CA certificates in the path to the root CA). In this event, you would receive intermediate CA certificate download instructions from the certificate vendor. Complete the following steps to import an intermediate CA certificate.
  - a) After selecting the end certificate, click the intermediate certificate import option.
  - b) Click the Import button to display the Import Intermediate Certificates form.
  - c) Click the Browse button and select the file containing the intermediate certificate (PEM, CRT, or CER format) to upload it.
  - d) If there are no additional intermediate certificates, click the **Import** button to install the uploaded certificate.

# FIGURE 403 Installing the Certificate



Alternatively, you can simplify this process by appending the intermediate CA certificates to the RUCKUS Unleashed certificate file. Then, you only need to import a single file. The intermediate certificates will be imported automatically. In this case, you will see multiple ----BEGIN CERTIFICATE--- and ---END CERTIFICATE--- pairs in the file.

# **SSL Certificate Advanced Options**

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

These include the following:

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

#### NOTE

Restoring Unleashed to factory default state does not remove imported SSL certificates. Use this option to remove any imported certificates and revert to the factory default state.

- Back Up Private Key: Back up the current private key by downloading it for disaster recovery or for use on another Unleashed AP. If your Unleashed AP is replaced due to an RMA, you will need to restore the private key if you have installed a public certificate. Ensure that the private key is kept secure because the security of your SSL communications depends on it.
- Back up certificates for Smart Redundancy: If you have more than one Unleashed AP, you can install the same SSL certificate/private key pair on both devices. In this way, you can access the shared virtual management interface advertised in DNS for the same FQDN without seeing the security warning.
- Back Up Trusted CA Information: Use this option to apply the same trusted CA from this Unleashed AP to peer Unleashed APs. The file is output as a .tar.gz file containing all trusted Certificate Authoritiy information currently installed on this Unleashed AP. This compressed file must be decompressed and the files imported into the peer Unleashed AP using the Add a Trusted CA feature described below.

- **Re-Generate Private Key of a Specific Key Length**: Use this option if your previous private key has been compromised or you need to use a stronger key (either 1024 or 2048 bits). Note that a new certificate must be generated and installed afterwards.
- Add a Trusted CA: Use this option to import CA information. Click the Click Here link to display all of the current trusted CA information, with each trusted CA separated by a string of number symbols ("#######"). Options include:
- Add a new trusted CA: Import a single CA file.
- Cover all trusted CA: Use the new trusted CA file to cover all existing trusted CA files

#### FIGURE 404 SSL Certificate Advanced Options

🛄 System	►	Generate a request Import Signed Certificate Advanced Options	
Services	►	Restore to Default Certificate/Private Key	
🌣 Administer	•	If needed, you can discard the imported certificate and private key. Unleashed will use factory default certificate/key after restore and reboot.           Restore	
Preferences		Back Up Private Key	
Backup & Restore		If you want to apply the same certificate from this Unleashed to other Unleasheds, please back up the private key from this Unleashed and then apply it to other Unleasheds for certificate key pairing. Back Up Private Key	
Upgrade		Back Up Certificates for Smart Redundancy	
Registration		If you want to apply the same certificate and private key from this Unleashed to peer Unleasheds, please back up the certificate from this Unleashed and then apply it to peer Unleasheds.	
Diagnostics		Back Up Certificate	
Certificate		Back Up trusted CA information If you want to apply the same trusted CA from this Unleashed to peer Unleasheds, please back up the trusted CA from this Unleashed and then apply it to peer Unleasheds.	
Network Connectivity		Back Up trusted CA	
Network Management		Re-generate private key of a specific key length Re-generate a new private key of a specific key length. This function is only needed when your certificate vendor only accepts 2048 key length instead of 1024 key length. Warning: The Unleashed will be rebooted after re- generating a new private key. Private key length  1024 2048 Create New	
		Add a trusted CA	
		To show all trusted CA click here. Import a trusted CA to Unleashed. When Unleashed received a server's certificate, Unleashed will match the server's CA against the Unleashed's list of trusted CA. If there is not match, Unleashed will send a error. Add a new trusted CA	
		Cover all trusted CA     Choose File     No file chosen	

# **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 405 Using Ping and Traceroute to test network connectivity

Clients	Client: 1				Tota	Connected 1	Blocked	
Access Points					Tota	2 Working 2	Disconnected	Þ
Admin & Services								V
모 System   용 Services	Toublesheet	your network connectivity.	Ping Trace Route					
Administer  Preferences Backup & Restore								
Restart Upgrade								
Registration Diagnostics								
Certificate Network Connectivity			Clear					

# **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 406 SNMPv2 Agent

🔶 WiFi Networks	No Traffic		Total 3 Working 3	Disabled	►
Clients	No Clients		Total 0 Connected 0	Blocked	►
Access Points			Total 2 Working 2	Disconnected	►
Admin & Services					▼
System	SNMPv2 Agent SNMPv3 Agent SNMP Trap	Enable SNMP Agent			
Administer       Preferences       Backup & Restore	System Contact* System Location* SNNP RO community* SNNP RW community*	support@ruckuswireless.com 880 West Maude Avenue, Suite 101, ' public private			
Upgrade Registration				Apply	у
Diagnostics Certificate					
Network Connectivity Network Management					

## SNMPv3

If your network uses SNMPv3:

- 1. Go to Admin & Services > Administer > Network Management.
- 2. On the SNMPv3 Agent tab, select the Enable SNMPv3 Agent check box.

- 3. Enter the following information for both the **Read Only** and **Read-Write** privileges:
  - User: Enter a user name between 1 and 31 characters.
  - Authentication: Choose MD5 or SHA authentication method (default is MD5).
  - MD5: Message-Digest algorithm 5, message hash function with 128-bit output.
  - SHA: Secure Hash Algorithm, message hash function with 160-bit output.
  - Auth Pass Phrase: Enter a passphrase between 8 and 32 characters in length.
  - Privacy: Choose DES, AES or None.
  - **DES**: Data Encryption Standard, data block cipher.
  - **AES**: Advanced Encryption Standard, data block cipher.
  - None: No Privacy passphrase is required.
  - Privacy Phrase: If either DES or AES is selected, enter a Privacy phrase between 8 and 32 characters in length.
- 4. Click Apply to save your changes.

#### FIGURE 407 SNMPv3 Agent

🔶 WiFi Networks	No Traffic			Total 3 Working	3 Disabled	∕ ▶
Clients	No Clients			Total 0 Connecte	ed 0 Blocked	•
Access Points				Total 2 Working	g 2 Disconnected	•
Admin & Services						▼
🖵 System 🕨						
🕘 Services 🕨	SNMPv2 Agent SNMPv3 Agent S Enable SNMPv3 Agent					
			Privacy Privacy Phrase			
Administer V	☑ Enable SNMPv3 Ager	nt	Privacy Privacy Phrase DES  Person passphrase			
Administer   Preferences	Enable SNMPv3 Agen Privilege User	Authentication Auth Pass Phrase				
Administer  Preferences Backup & Restore	Enable SNMPv3 Age  Privilege User  Read Only public	Authentication Auth Pass Phrase	DES		Арр	sly
Administer	Enable SNMPv3 Age  Privilege User  Read Only public	Authentication Auth Pass Phrase	DES		Арр	ly ⊧
Administer  Preferences Backup & Restore Upgrade	Enable SNMPv3 Agen      Privilege     User      Read Only     public      Read/Write     private	Authentication Auth Pass Phrase	DES		Арр	ly ⊧
Administer     Preferences Backup & Restore Upgrade Registration	Enable SNMPv3 Agen      Privilege     User      Read Only     public      Read/Write     private	Authentication Auth Pass Phrase	DES		Арр	ly ⊧
Administer      Preferences Backup & Restore Upgrade Registration Degrostics	Enable SNMPv3 Agen      Privilege     User      Read Only     public      Read/Write     private	Authentication Auth Pass Phrase	DES		Арр	ly ≻

# **Enabling SNMP Trap Notifications**

If you have an SNMP trap receiver on the network, you can configure Unleashed to send SNMP trap notifications to the server.

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

To enable SNMP trap notifications:

- 1. Go to Admin & Services > Administer > Network Management.
- 2. On the SNMP Trap tab, select the Enable SNMP Trap check box.

- 3. In **SNMP Trap format**, select either **SNMPv2** or **SNMPv3**. You can select only one type of trap receiver. If you select SNMPv2, you only need to enter the IP addresses of up to four SNMP trap receivers on your network. If you select SNMPv3, enter up to four trap receiver IP addresses along with authentication method passphrase and privacy (encryption) settings.
- 4. Click **Apply** to save your changes.

#### FIGURE 408 SNMP Trap

	Traffic: 0.19 MB		
Clients	Client: 1	Total 1 Connected 1	Blocked
Access Points		Total 2 Working 2	Disconnected
Admin & Services			•
System Services Administer	SNMP V2 Agent SNMP 3 Agent SNMP Trap Enable SNMP Trap		
Administer      Preferences Backup B. Restore Restart	SNAP Community" public Trap Server IP Trap Server 2 IP		
Upgrade Registration Diagnostics	Trap Server3 IP		Apply
Certificate Network Connectivity Network Management			

# **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 409 Enabling Unleashed Multi-Site Manager management

⊒ System	•					· · · · ·		
		SNMPv2 Agent	SNMPv3 Agent	SNMP Trap	Unleashed Multi-Site Manager	Alarm Notification		
Services	•	Unleashed Multi	-Site Manager					
Administer	•	Multi-Site Manag	jer.	-	RL and set the time interval at whic		status updates to Unleashed	
Preferences		omeastieu mu	-			e/server		
Backup & Restore			URL*	https:// 192.1		e/server		
Upgrade		Last successful	Interval*		nutes)			
Registration							Analy	
Diagnostics							Apply	
Certificate								
Network Connectivity								

# **Configuring Alarm Event Notification Settings**

The web interface allows you to customize the content and delivery for a wide range of alarm events. When a matching event occurs, admins can be notified either through email or the mobile app.

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

- 1. Go to Admin & Services > Administer > Network Management > Alarm Notification.
- 2. In Alarm Event, select/deselect the event categories for which notifications will be delivered.
- 3. Click Apply to save your changes.
- 4. In *Email Address*, enable the check box and enter the destination address for alarm notifications. An email server must first have been configured from the *System > System Info* screen.

5. Click **Test** to test email delivery. Click **Apply** to save your changes.

SNMPv2 Agent	SNMPv3 Age	nt SNMP Trap	Unleashed Multi-Site Mar	nag	er Alarm Notification
Alarm Notification					
Alarm Notific	ation 🔽	AP Has Hardwar	re Problem		RADIUS Authentication Server Unavailable
		AP Has Joined		<b>√</b>	Rogue DHCP Server Detected
	~	AP Lost Contact	t	<b>~</b>	SSID-spoofing AP Detected
		AP Radio Off		<b>√</b>	Same-Network Rogue AP Detected
		AP Radio On			Survivability entries reach maximum
		Config Invalid			URL Filtering is diabled
		Config Mismatc	h		URL Filtering license expired
		External Gatewa	ay status change		URL Filtering license file download fail
		ICX Urgent Mess	sage		URL Filtering license will expire
		MAC-spoofing A	P Detected		SIM Card Remove
		Master AP Chan	ge		Favorite Client Disconnect
		RADIUS Account	nting Server Unavailable		Favorite Client Connect
					Apply

## FIGURE 410 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 411 Enabling mobile app remote management

Admin & Ser	Ces	
🛄 System		
•	Remote Management & Mobile App Notification Remote User Control	
Services	Remote Management	
Administration	♥ When Remote Management is enabled, the Unleashed network can be managed resttings. If you don't have mobile app installed, please follow these links	
Preferences	Remote Management requires valid Unleashed Support contract. If you have not pr	urchased it, please contact Ruckus Supoort.
Backup & Restore	Status: Pending	
Upgrade	Enable Mobile app remote management	Apply
Registration		Арріу
Diagnostics	Mobile App Notification	
Certificate	This feature is to send notification to your mobile device when an alarm is triggered installed, please follow these links 🖨 🗳 to download or search for "Ruckus Unleast for iOS.	
Network Connectivity	<ul> <li>It is triggered.</li> </ul>	
Network Management	Serio an app nouncation when all alarm is triggered.	

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

FIGURE 412 Remote Management

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

#### FIGURE 413 Remote user control

🛟 Admir	n & Services				▼
Admin     System     Services     Administrat     Preferences     Backup & Restore     Upgrade     Diagnostics     Certificate	•	Remote Management &	& Mobile App Notification Remote User Cont Potete State	trol Create On	Search Q Last Login
Network Management					

# **Technical Support**

You can request technical support to troubleshoot your Unleashed technical issues.

Complete the following steps to request technical support.

1. Select Admin & Services > Administration > Technical Support.

## FIGURE 414 Requesting Technical Support

⊒ System	►	Technical Support		
Services	•	Ticket Timeout on 2021/11/16 15:04:43		
	-		2/1/1/16 15:00:43, took too long to connect to the remote server. Please check your internet connectivity. Click "Submit" button to try again.	
Administration	•	* Email Address	example@example.com	
eferences		Phone Number	+861861111111	
ickup & Restore		Company Name	example	
ograde		* Problem Category	Client Connectivity *	
agnostics		* Please describe the problem	example	
rtificate				
etwork Management				
bile App				
chnical Support		ſ	✓ I have read, understood and accepted the terms & conditions	
			Submit	

- 2. Enter your email address.
- 3. (Optional) Enter your phone number and company name.
- 4. From the **Problem Category** list, select a problem type.
- 5. Enter a description about your technical problem.
- 6. Select the I have read, understood and accepted the terms & conditions check box and click Submit.

#### NOTE

When you enable technical support, Unleashed disconnects from its registered UMM and connects to the RUCKUS remote UMM. After the requested technical support is completed, Unleashed registers back to UMM.

# Unleashed Access Point Power Supply Considerations

•	AP Power Warnings	499
•	Power Limitations by PoE Mode and AP Model	501

# **AP Power Warnings**

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

## FIGURE 415 Warning icons indicate an AP is operating in reduced-power mode

Clients Clients	Total 3 Connected 3 Disconnected 0	
Access Points	Total 1 Disconnected 0	•
Edt Restart Remove 🗮 🗗	Data duration: 1 hours •	
Summary - Total 1 Access Points	Summary	
Clients Traffic	Maximun 50 APs support 1 Access Points connected, 0 Access Points disconnected.	
R610 - M[35:c9:40]	3 Clients Show Clients Info	
Glients Traffic	Events Show Events	
	Client Status for last 1 hours	

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

## FIGURE 416 Showing AP Power Consumption Mode

			2 WLANs	Show WLANs Info
	Ruckus-U[35:c9:40	Master D]	Sy	Stem Overview
1	0 0 3	2.4G	Mac Address	d4:c1:9e:35:c9:40
	Clients	Traffic	IP Address	192.168.0.3
			External IP:Port	192.168.0.3:12225
			Model	R610
			S/N	941849001125
			Group Name	System Default
			GPS Coordinates	
			Mesh Type	Disabled
			Current Channel(802.11a/n/ac)	149
			Current Channel(802.11b/g/n)	6
			Power Consumption Mode	802.3at PoE
			Max Clients	100
			Version	200.8.10.3.173
			Role Fixed	no
			Download Logs	Logs 🚣

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 417 Override PoE Operating Mode

 Restart		Q [				Data duration: 1 hour •
	1 Access Points			Ruckus-Unleash	ed [d4:c1:9e:35:c9:40]	
Edit AF	<sup>-</sup> (d4:c1:96	e:35:c9:40	))			×
 General	Radio 2.4 GHz	Radio 5.0 GHz	Network Of	her		
	St	atus LEDs	verride Group Co	nfig Disable Status LEDs	С	Cancel
				Mesh Type	Disabled	

# **Power Limitations by PoE Mode and AP Model**

The following tables list the Power over Ethernet (PoE) operating modes for each AP model, along with the performance and feature limitations when the AP is in any of the supported reduced power modes.

Indoor AP	Outdoor AP
R850	T610
R750	M510
R720	Т750
R710	T750SE
R650	T350c
R610	T350d
R550	T350SE
H550	

# **R850**

## TABLE 36 R850 PoE Modes

	LLDP Power Ask	2.4G Tx/Rx	5G Tx/Rx	5Gbps Eth	1Gbps Eth	USB	loT	Comments
DC		4/4	8/8	Enabled	Enabled	Enabled	N/A	
802.3af		1/4	1/8	Enabled	Disabled	Disabled	N/A	Not supported in operation mode
802.3at	25W	4/4	4/8	Enabled	Enabled	Enabled (0.5W)	N/A	
802.3bt/class5	35W	4/4	8/8	Enabled	Enabled	Enabled	N/A	
PoE injector (Model 480125A) 60W		4/4	4/8	Enabled	Enabled	Enabled	N/A	Force to 802.3bt/class5 from SZ GUI

# **R750**

## TABLE 37 R750 PoE Modes

	LLDP Power Ask	2.4G Tx/Rx	5G Tx/Rx	2.5Gbps Eth	1Gbps Eth	USB	ют
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 38 R720 PoE Modes

LLDP Power Ask 2.4G Tx/Rx	5G Tx/Rx	2.5Gbps Eth	1Gbps Eth	USB	Comments
---------------------------	----------	-------------	-----------	-----	----------

# Unleashed Access Point Power Supply Considerations

Power Limitations by PoE Mode and AP Model

## TABLE 38 R720 PoE Modes (continued)

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 39 R710 PoE Modes

	LLDP Power Ask	2.4G Tx/Rx	5G Tx/Rx	1Gbps Eth(PoE)	1Gbps Eth	USB
DC		4/4 (22dBm)	4/4 (20dBm)	Enabled	Enabled	Enabled
802.3af		2/4 (20dBm)	4/4 (19dBm)	Enabled	Disabled	Disabled
802.3at/Injector (Model 480125A)	25W	4/4 (22dBm)	4/4 (20dBm)	Enabled	Enabled	Enabled

# **R650**

## TABLE 40 R650 PoE Modes

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

# **R610**

# TABLE 41 R610 PoE Modes

	LLDP Power Ask	2.4G Tx/Rx	5G Tx/Rx	1Gbps Eth(PoE)	1Gbps Eth	USB
DC		4/4	4/4	Enabled	Enabled	Enabled
802.3af		2/4	4/4	Enabled	Disabled	Disabled
802.3at/Injector (Model 480125A)	24W	4/4	4/4	Enabled	Enabled	Enabled

# **R550**

## TABLE 42 R550 PoE Modes

	LLDP Power Ask	2.4G Tx/Rx	5G Tx/Rx	1bps Eth(PoE)	1Gbps Eth	USB	ют
DC		2/2 (22 dBm)	2/2 (22 dBm)	Enabled	Enabled	Enabled	Enabled
802.3af		2/2 (10 dBm)	2/2 (18 dBm)	Enabled	Disabled	Disabled	Disabled
802.3at	25W	2/2 (22 dBm)	2/2 (22 dBm)	Enabled	Enabled	Enabled	Enabled

Power Limitations by PoE Mode and AP Model

#### TABLE 42 R550 PoE Modes (continued)

PoE Injector	2/2 (22 dBm)	2/2 (22 dBm)	Enabled	Enabled	Enabled	Enabled
(Model 480125A)						

# H550

## TABLE 43 H550 PoE Modes

	LLDP Power	2.4G Tx/	5G Tx/	1Gbps Eth	USB	loT		PSE	
	Ask	<b>Rx</b> (16dBm)	<b>Rx</b> (19dBm)				POE_Out	Power @ PD	Maximum Cable Length
DC		2/2	2/2	Enabled	Enabled	Enabled	Enabled		
802.3af	12.95W	2/2	2/2	Enabled	Disabled	Enabled	Disabled	NA	NA
802.3at/	25W	2/2	2/2	Enabled	Enabled	Enabled	Disabled	NA	NA
injector					Enabled		Enabled	8.4W	20m
					Disabled		Enabled	12.4W	20m
802.3bt, uPoE, PoH	40W	2/2	2/2	Enabled	Enabled	Enabled	Enabled	12.95W	100m

# **T610**

### TABLE 44 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 45 M510 PoE Modes

	LLDP Power Ask	2.4G Tx/Rx	5G Tx/Rx	1Gbps Eth(PoE)	1Gbps Eth	USB
DC	Full	2/2 (23dBm)	2/2 (20dBm)	Enabled	Enabled	Enabled
802.3af	12.95W	1/2 (19dBm)	2/2 (19dBm)	Enabled	Disabled	Disabled
802.3at/Injector (Model 480125A)	25W	2/2 (23dBm)	2/2 (20dBm)	Enabled	Enabled	Enabled

# **T750**

# TABLE 46 T750 PoE Modes

	LLDP Power Ask	2.4G Tx/Rx	5G Tx/Rx	2.5Gbps Eth	1Gbps Eth	USB	юТ	PSE	Comment
DC		4/4	4/4	Enabled	Enabled	Enabled	Enabled	Enabled	

# Power Limitations by PoE Mode and AP Model

## TABLE 46 T750 PoE Modes (continued)

802.3af		1/4	1/4	Enabled	Disabled	Disabled	Disabled	Disabled	Not supported operation mode
802.3at w/o USB	25W	4/4	4/4	Enabled	Enabled	Disabled	Enabled	Disabled	
802.3at w/ USB	25W	2/4	4/4	Enabled	Disabled	Enabled	Enabled	Disabled	Alt AT mode config by AP CLI
802.3bt/Class 5	35W	4/4	4/4	Enabled	Enabled	Enabled	Enabled	Disabled	
803.3bt/Class 6		4/4	4/4	Enabled	Enabled	Enabled	Enabled	Disabled	51W by H/W negotiation
802.3bt/Class 7		4/4	4/4	Enabled	Enabled	Enabled	Enabled	Enabled	62W by H/W negotiation
PoE injector (Model 480125A)		4/4	4/4	Enabled (1Gbps speed)	Enabled	Enabled	Enabled	Disabled	Force to 802.3bt/Class 5
PoE injector		4/4	4/4	Enabled	Enabled	Enabled	Enabled	Enabled	Force to 802.3bt/Class 7

# **T750SE**

# TABLE 47 T750SE PoE Modes

	LLDP Power Ask	2.4G Tx/Rx	5G Tx/Rx	2.5Gbps Eth	1Gbps Eth	USB	loT	PSE	Comment
DC		4/4	4/4	Enabled	Enabled	Enabled	Enabled	Enabled	
802.3af		1/4	1/4	Enabled	Disabled	Disabled	Disabled	Disabled	Not supported operation mode
802.3at w/o USB	25W	4/4	4/4	Enabled	Enabled	Disabled	Enabled	Disabled	
802.3at w/ USB	25W	2/4	4/4	Enabled	Disabled	Enabled	Enabled	Disabled	Alt AT mode config by AP CLI
802.3bt/Class 5	35W	4/4	4/4	Enabled	Enabled	Enabled	Enabled	Disabled	
803.3bt/Class 6		4/4	4/4	Enabled	Enabled	Enabled	Enabled	Disabled	51W by H/W negotiation
802.3bt/Class 7		4/4	4/4	Enabled	Enabled	Enabled	Enabled	Enabled	62W by H/W negotiation
PoE injector (Model 480125A)		4/4	4/4	Enabled (1Gbps speed)	Enabled	Enabled	Enabled	Disabled	Force to 802.3bt/Class 5
PoE injector		4/4	4/4	Enabled	Enabled	Enabled	Enabled	Enabled	Force to 802.3bt/Class 7

# T350c

## TABLE 48 T350c PoE Modes

	LLDP Power Ask	2.4G Tx/Rx	5G Tx/Rx	1Gbps Eth	loT
802.3af		2/2 (19dBm)	2/2 (18dBm)	Enabled	Disabled
802.3at/PoE injector	25W	2/2	2/2	Enabled	Enabled

# T350d

## TABLE 49 T350d PoE Modes

	LLDP Power Ask	2.4G Tx/Rx	5G Tx/Rx	1Gbps Eth	USB	ют
DC		2/2	2/2	Enabled	Enabled	Enabled
802.3af		2/2 (19dBm)	2/2 (18dBm)	Enabled	Disabled	Disabled
802.3at/PoE injector	25W	2/2	2/2	Enabled	Enabled	Enabled

# **T350SE**

## TABLE 50 T350SE PoE Modes

	LLDP Power Ask	2.4G Tx/Rx	5G Tx/Rx	1Gbps Eth	USB
DC/PoE injector		2/2	2/2	Enabled	Enabled
802.3at	25W	2/2	2/2	Enabled	Enabled
802.3af		2/2 (16dBm)	2/2 (16dBm)	Enabled	Disabled



© 2022 CommScope, Inc. All rights reserved. 350 West Java Dr., Sunnyvale, CA 94089 USA https://www.commscope.com