ADMINISTRATION GUIDE

RUCKUS ZoneDirector 10.4.1 User Guide

Supporting Release 10.4.1

Part Number: 800-72629-001 Rev D
Publication Date: June 2023

© 2023 CommScope, Inc. All rights reserved.

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

Export Restrictions

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

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

Disclaimer

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

Limitation of Liability

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

Trademarks

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

Patent Marking Notice

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

Contents

Contact Information, Resources, and Conventions **11**
Contacting RUCKUS Customer Services and Support 11
What Support Do I Need? 11
Open a Case 11
Self-Service Resources 12
Document Feedback 12
RUCKUS Product Documentation Resources 12
Online Training Resources 12
Document Conventions 13
Notes, Cautions, and Safety Warnings 13
Command Syntax Conventions 13

About This Guide **15**
Overview 15
Related Documentation 15
New in This Document 16

Introducing ZoneDirector **17**
Overview of ZoneDirector 17
ZoneDirector Physical Features 17
ZoneDirector 1200 17
Introduction to the Ruckus Network 19
Installing ZoneDirector 20
Ensuring That APs Can Communicate with ZoneDirector 22
How APs Discover ZoneDirector on the Network 22
How to Ensure that APs Can Discover ZoneDirector on the Network 22
Firewall Ports that Must be Open for ZoneDirector Communications 28
Accessing ZoneDirector's Command Line Interface 29
Using the ZoneDirector Web Interface 30
Navigating the Dashboard 32
Registering Your Product 33

Managing Access Points **35**
Managing Access Points Overview 35
Adding New Access Points to the Network 35
Connecting the APs to the Network 36
Verifying or Approving New APs 36
Working with Access Point Groups 37
Modifying the System Default AP Group 38
Creating a New Access Point Group 40
Modifying Access Point Group Membership 41
Modifying Model Specific Controls 42
Configuring Global Access Point Policies 53
Using Limited ZD Discovery for N+1 Redundancy 55
Importing a USB Software Package 56
To provision a SmartPoint Access Point with USB software: 57
Managing Access Points Individually 57
Configuring Hotspot 2.0 Venue Settings for an AP 60

Optimizing Access Point Performance 61
Assessing Current Performance Using the Access Point Table 61
Adjusting AP Settings 61
Prioritizing WLAN Traffic 62

Managing a Wireless Local Area Network 63
Overview of Wireless Networks 63
About RUCKUS WLAN Security 64
Creating a Wireless LAN 65
General Options 66
WLAN Usage Types 66
Authentication Method 67
Encryption Options 69
Advanced WLAN Options 72
Creating a Copy of an Existing WLAN for Workgroup Use 79
Customizing WLAN Security 80
Reviewing the Initial Security Configuration 80
Fine Tuning the Current Security Mode 81
Switching to a Different Security Mode 81
Using the Built in EAP Server 82
Authenticating with an External RADIUS Server 82
If You Change the Internal WLAN to WEP or 802.1X 83
Working with WLAN Groups 83
Creating a WLAN Group 84
Viewing a List of APs That Belong to a WLAN Group 86
Deploying ZoneDirector WLANs in a VLAN Environment 86
Tagging Management Traffic to a VLAN 88
Using VLAN Override 90
How Dynamic VLAN Works 91
Working with VLAN Pools 93

Managing User Access 97
Enabling Automatic User Activation with Zero-IT 97
Clients that Support Zero-IT 98
Self-Provisioning Clients with Zero-IT 98
Self-Provisioning Clients without Ethernet Ports 100
Provisioning Clients that Do Not Support Zero-IT 101
Working with Dynamic Pre-Shared Keys 101
Enabling Dynamic Pre-Shared Keys on a WLAN 102
Setting Dynamic Pre-Shared Key Expiration 107
Generating Multiple Dynamic PSKs 108
Downloading Generated DPSKs 113
Adding New User Accounts to ZoneDirector 113
Internal User Database 113
Managing Current User Accounts 114
Changing an Existing User Account 115
Deleting a User Record 115
Creating New User Roles 116
Role Based Access Control Policy 117
Managing Generated Dynamic PSKs 119
Managing Generated Guest Passes 120

Using an External Server for User Authentication....120
Enabling Web Authentication....122
Captive Portal Redirect on Initial Browser HTTPS Request....123
Managing Guest Access....125
Configuring Guest Access....125
Creating a Guest Access Service....125
Using Guest Pass Self-Service....127
Configuring Guest Subnet Restrictions....141
Guest Access Walled Garden....142
Creating a Guest WLAN....143
Using the BYOD Onboarding Portal....144
Working with Guest Passes....149
Generating a Guest Pass from the Clients Page....149
Configuring Guest Pass Generation....152
Generating and Delivering a Single Guest Pass....155
Generating and Printing Multiple Guest Passes at Once....159
Monitoring Generated Guest Passes....161
Creating a Custom Guest Pass Printout....162
Delivering Guest Passes via Email....163
Delivering Guest Passes via SMS....164
Social Auth WLANs....165
About the Ruckus Facebook Wi-Fi Implementation....165
OAuth Social Media Types....167
Create an OAuth2.0 WLAN on ZoneDirector....179
User Login to Social Media WLAN....180
WeChat WLANs....183
Working with Hotspot Services....185
Creating a Hotspot Service....185
Assigning a WLAN to Provide Hotspot Service....189
Common WISPr Attribute Abbreviations....190
Creating a Hotspot 2.0 Service....191
Create a Service Provider Profile....191
Create an Operator Profile....192
Create a Hotspot 2.0 WLAN....193
Customizing the Captive Portal....194
Replacing the Captive Portal Logo....195
Troubleshooting....199
Troubleshooting Failed User Logins....199
Performing Client Connectivity Diagnostics....200
Fixing User Connections....201
Troubleshooting Client Connections....201
Using the Ping and Traceroute Tools....202
If WLAN Connection Problems Persist....204
Measuring Wireless Network Throughput with SpeedFlex....205
Using SpeedFlex in a Multi-Hop Smart Mesh Network....209
Allowing Users to Measure Their Own Wireless Throughput....210
Starting a Radio Frequency Scan....211
Generating a Debug File....212
Viewing and Saving Current System Logs....213

Saving Client Connection Logs ... 213
Viewing Current AP Logs ... 214
Packet Capture and Analysis ... 215
Local Capture ... 216
Streaming Mode ... 216
AP Diagnostic Information ... 219
Importing a Script ... 220
Enabling Remote Troubleshooting ... 220
Disabling SpeedFlex ... 220
Restarting an Access Point ... 221
Restarting ZoneDirector ... 221

Configuring Services and Profiles ... 223
Application Recognition and Control ... 223
Configure Application Policies ... 223
Configure IP Based User Defined Applications ... 226
Configure Port Based User Defined Applications ... 227
Well-Known Service and Destination Port Mappings Defined in Application Visibility ... 228
Configuring Network Access Controls ... 228
Creating Layer 2/MAC Address Access Control Lists ... 229
Creating Layer 3/Layer 4/IP Address Access Control Lists ... 230
Configuring Device Access Policies ... 231
Configuring Precedence Policies ... 232
Blocking Client Devices ... 233
Configuring Client Isolation White Lists ... 236
URL Filtering ... 238
Creating a URL Filtering Profile ... 239
Applying a URL Filtering Policy to a WLAN ... 242
Applying a URL Filtering Policy to a Role ... 243
Working with URL Filtering Licenses ... 244
Configuring Maps ... 245
Configuring Floorplan Maps ... 245
Guest Access ... 247
Hotspot Services ... 247
Mesh Configuration ... 247
Using an External AAA Server ... 248
Active Directory ... 248
LDAP ... 251
RADIUS /RADIUS Accounting ... 254
TACACS+ ... 263
Testing Authentication Settings ... 264
Services ... 264
Self Healing ... 264
Load Balancing ... 269
Band Balancing ... 271
Radar Avoidance Pre-Scanning ... 272
AeroScout RFID Tag Detection ... 273
Ekahau Tag Detection ... 273
Active Client Detection ... 273
Tunnel Configuration ... 274
Packet Inspection Filter ... 275

Configuring Wireless Intrusion Prevention ... 275
DoS Protection ... 275
Intrusion Detection and Prevention ... 276
Rogue DHCP Server Detection ... 278
DHCP Relay ... 279
To enable DHCP Relay for a WLAN: ... 280
Bonjour Gateway ... 281
Bridge Service Rules ... 282
Bridge Service Records ... 282
Creating a Bonjour Gateway Rule - ZD Site ... 282
Creating a Bonjour Gateway Rule AP Site ... 283
Applying a Bonjour Policy to an AP ... 285
Example Network Setup ... 285
Bonjour Fencing ... 286
Configuring Bonjour Fencing Policies ... 286
Applying a Bonjour Fencing Policy to an AP or AP Group ... 287
SPoT Location Services ... 288

Configuring System Settings ... 291
System Configuration Overview ... 291
Changing the System Name ... 291
Changing the Network Addressing ... 291
IPv6 Configuration ... 292
Enabling an Additional Management Interface ... 293
Creating Static Route Entries ... 294
Static Route Example ... 296
Enabling Smart Redundancy ... 296
Configuring ZoneDirector for Smart Redundancy ... 297
Managing Smart Redundancy AP License Pools ... 299
Configuring the Built-in DHCP Server ... 300
Enabling the Built-in DHCP server ... 301
Viewing DHCP Clients ... 302
Controlling ZoneDirector Management Access ... 302
Setting the System Time ... 303
Configuring a User-Defined Time Zone ... 304
Setting the Country Code ... 305
Channel Optimization ... 306
Configuring System Log Settings ... 307
Reviewing the Current Log Contents ... 307
Customizing the Current Log Settings ... 308
Setting Up Email Alarm Notifications ... 312
Customizing Email Alarms ... 314
Configuring SMS Settings for SMS Guest Pass Delivery ... 315
Enabling Login Warning Messages ... 316
Configuring Dashboard Map Settings ... 317
Enabling Network Management Systems ... 318
Enabling SmartCell Insight Communication ... 318
Enabling Management via UMM ... 320
Enabling Northbound Portal Interface Support ... 321
Configuring SNMP Support ... 322
Enabling Telnet ... 328

Setting Administrator Preferences **329**
Changing the Web Interface Display Language 329
Changing the ZoneDirector Administrator User Name and Password 331
Using an External Server for Administrator Authentication 332
Setting Administrator Login Session Timeout 333
Working with Backup Files 334
Backing Up a Network Configuration 334
Restoring Archived Settings to ZoneDirector 335
Restoring ZoneDirector to Default Factory Settings 337
Alternate Factory Default Reset Method 338
Upgrading ZoneDirector and Connected APs 339
Importing an AP Firmware Bundle 341
Enabling Secured AP Image Upgrade 342
Performing an Upgrade with Smart Redundancy 342
Working with Licenses and Support 343
Upgrading the AP License 343
Support Entitlement 345
Working with URL Filtering Licenses 345
Working with SSL Certificates 346
Basic Certificate Installation 346
Generating a Certificate Signing Request 347
Importing an SSL Certificate 348
SSL Certificate Advanced Options 350

Monitoring Your Wireless Network **357**
Reviewing the ZoneDirector Monitoring Options 357
Monitoring Access Points 357
Using the AP Status Overview Page 357
Monitoring Individual APs 362
Monitoring WLAN Status 366
Reviewing Current User Activity 367
Active Client Action Icons 368
Viewing Application Usage Statistics 368
Monitoring Individual Clients 370
Monitoring Wired Clients 373
Monitoring AAA Server Statistics 373
Reviewing Recent System Events 374
Reviewing Current Alarms 374
Monitoring Location Services 375
Monitoring Mesh Status 376
Real Time Monitoring 377
Detecting Rogue Access Points 379
Monitoring System Information 381
Monitoring System Ethernet Port Status 381

Deploying a Smart Mesh Network **383**
Overview of Smart Mesh Networking 383
Smart Mesh Networking Terms 384
Supported Mesh Topologies 384
Standard Topology 384
Wireless Bridge Topology 385

Hybrid Mesh Topology ... 386
Viewing the Mesh Topology ... 387
Deploying a Wireless Mesh via ZoneDirector ... 388
Step 1: Prepare for Wireless Mesh Deployment ... 388
Step 2: Enable Mesh Capability on ZoneDirector ... 389
Step 3: Provision and Deploy Mesh Nodes ... 390
Step 4: Verify That the Wireless Mesh Network Is Up ... 396
Optional Mesh Configuration Features ... 397
Understanding Mesh-related AP Statuses ... 397
Using the AP LEDs to Determine the Mesh Status ... 397
On Dual-band Ruckus APs ... 398
Using Action Icons to Configure and Troubleshoot APs in a Mesh ... 399
Setting Mesh Uplinks Manually ... 400
Troubleshooting Isolated Mesh APs ... 401
Understanding Isolated Mesh AP Statuses ... 401
Recovering an Isolated Mesh AP ... 402
Best Practices and Recommendations ... 403

Mesh Networking Best Practices ... 405
Calculating the Number of APs Required ... 405
Placement and Layout Considerations ... 405
Signal Quality Verification ... 406
Mounting and Orientation of APs ... 407
Indoor APs - Typical Orientation ... 407
Outdoor APs - Typical Horizontal Orientation ... 408
Elevation of RAPs and MAPs ... 408
Mesh Best Practice Checklist ... 408

Access Point Power Supply Considerations ... 411
AP Power Warnings ... 411
Power Limitations by PoE Mode and AP Model ... 413
R850 ... 414
R750 ... 414
R730 ... 414
R720 ... 414
R710 ... 415
R650 ... 415
R610 ... 415
R550 ... 415
T610 ... 416
M510 ... 416
T750 ... 416

Contact Information, Resources, and Conventions

- Contacting RUCKUS Customer Services and Support 11
- Document Feedback 12
- RUCKUS Product Documentation Resources 12
- Online Training Resources 12
- Document Conventions 13
- Command Syntax Conventions 13

Contacting RUCKUS Customer Services and Support

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

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

What Support Do I Need?

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

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

Open a Case

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

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

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

Self-Service Resources

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

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

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

Document Feedback

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

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

When contacting us, include the following information:

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

For example:

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

RUCKUS Product Documentation Resources

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

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

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

Online Training Resources

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

Document Conventions

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

TABLE 1 Text Conventions

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

Notes, Cautions, and Safety Warnings

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

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

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



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



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

Command Syntax Conventions

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

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

About This Guide

- Overview 15
- Related Documentation 15
- New in This Document 16

Overview

This *User Guide* describes how to install, configure and manage the Ruckus ZoneDirector version 10.4.

This guide is intended for use by those responsible for managing Ruckus network equipment. Consequently, it assumes a basic working knowledge of local area networking, wireless networking and wireless devices.

> **NOTE**
> If release notes are shipped with your product and the information there differs from the information in this guide, follow the instructions in the release notes.

Most user guides and release notes are available in Adobe Acrobat Portable Document Format (PDF) or HTML on the Ruckus Support website at https://support.ruckuswireless.com/documents.

> **NOTE**
> By downloading this software and subsequently upgrading the ZoneDirector to version 10.4, please be advised that the ZoneDirector will periodically connect to Ruckus and Ruckus will collect the ZoneDirector serial number, software version and build number. Ruckus will transmit a file back to the ZoneDirector and this will be used to display the current status of the ZoneDirector Support Contract. Please also be advised that this information may be transferred and stored outside of your country of residence where data protection standards may be different.

Related Documentation

In addition to this User Guide, each ZoneDirector documentation set includes the following:

- *Release Notes*: Provide information about the current software release, including new features, enhancements, and known issues.
- *Online Help*: Provides a web-based version of the content contained in the User Guide. The online help is accessible from the web interface and is searchable.
- *Command Line Reference Guide*: Provides a list of CLI commands, their usage syntax and examples.
- *SNMP Reference Guide*: Provides a list of supported Simple Network Management Protocol (SNMP) Management Information Base (MIB) objects.
- *Syslog Alarms and Events Reference Guide*: Provides a list of Syslog alarms and events.
- *Upgrade Guide*: Provides instructions for upgrading your ZoneDirector and connected RUCKUS Access Points (APs).
- For information on common ZoneDirector support issues (including video tutorials), visit https://support.ruckuswireless.com/how-to-hub.

New in This Document

TABLE 2 Summary of Changes in ZoneDirector 10.4.1 (Rev D), June 2023

Feature	Description	Location
Addressing reported defects	**Updated**: Updating the procedure for approving new access points.	Verifying or Approving New APs on page 36

TABLE 3 Summary of Changes in ZoneDirector 10.4.1 (Rev C), December 2022

Feature	Description	Location
Addressing reported defects	**Updated**: Adding more information about the authentication methods.	Authentication Method on page 67
	Updated: Adding detailed instructions to configure 802.1x & MAC.	Using 802.1X EAP + MAC Address Authentication on page 257
	Updated: Adding instructions to configure SAE passphrase.	SAE Passphrase (Only for WPA3 and WPA2/WPA3-Mixed WLANs) on page 70

TABLE 4 Summary of Changes in ZoneDirector 10.4.1 (Rev B), September 2021

Feature	Description	Location
Addressing reported defects	**Updated**: Updating setup procedures for LinkedIn and Microsoft social media logins.	• OAuth Setup Procedure for LinkedIn Social Media Login on page 173 • OAuth Setup Procedure for Microsoft Live Social Media Login on page 176

Introducing ZoneDirector

- Overview of ZoneDirector 17
- ZoneDirector Physical Features 17
- Introduction to the Ruckus Network 19
- Installing ZoneDirector 20
- Ensuring That APs Can Communicate with ZoneDirector 22
- Accessing ZoneDirector's Command Line Interface 29
- Using the ZoneDirector Web Interface 30
- Registering Your Product 33

Overview of ZoneDirector

Ruckus Networks ZoneDirector serves as a central control system for Ruckus Wi-Fi Access Points (APs). ZoneDirector provides unified AP configuration and updates, wireless LAN security control, RF management, and automatic coordination of Ethernet-connected and mesh-connected APs.

Using ZoneDirector in combination with Ruckus APs allows deployment of a Smart Mesh network, to extend wireless coverage throughout a location without having to connect each AP to Ethernet.

In a Smart Mesh network, the APs form a wireless mesh topology to route client traffic between any member of the mesh and the wired network. Meshing significantly reduces the cost and time requirements of deploying an enterprise-class wireless LAN (WLAN), in addition to providing much greater flexibility in AP placement.

ZoneDirector also integrates network monitoring, sophisticated user access controls, Wi-Fi performance diagnostic tools, highly configurable guest access features and advanced security features within a single system.

User authentication can be accomplished using an internal user database, or forwarded to an external Authentication, Authorization and Accounting (AAA) server such as RADIUS or Active Directory. Once users are authenticated, client traffic is not required to pass through ZoneDirector, thereby eliminating bottlenecks when higher speed Wi-Fi technologies - such as 802.11ax - are used.

This user guide provides complete instructions for using the ZoneDirector web-based user interface. With the web interface, you can customize and manage all aspects of ZoneDirector and your Ruckus Wi-Fi deployment.

ZoneDirector Physical Features

This section describes the physical features of the ZoneDirector models currently available.

As of release 10.3, ZoneDirector 1200 is the only model currently available.

NOTE
ZoneDirector 3000 is discontinued as of this release and cannot be upgraded to 10.3 or any later release.

- ZoneDirector 1200 on page 17

ZoneDirector 1200

This section describes the following physical features of ZoneDirector 1200:

- Buttons, Ports, and Connectors on page 18

- Front Panel LEDs on page 19

FIGURE 1 ZoneDirector 1200



ZoneDirector 1200 is designed specifically for small-to-medium enterprises (SMEs), and features a fanless desktop form factor, two GbE ports, and support for up to 150 APs per controller.

PHYSICAL CHARACTERISTICS	
Power	• External power adapter • Input: 110 - 240V AC • Output: 12V DC, 2A
Physical Size	Desktop: 25cm (L), 15.93cm (W), 3.164cm (H)
Weight	2.2 lbs (1 kilogram)
Ports	• 2 Ethernet ports, auto MDX, auto-sensing 10/100/1000 Mbps • 1 Console RJ-45 port
Environmental Conditions	• Operating Temperature: 32°F (0°C) - 104°F (40°C) • Operating humidity: 20% - 90% non-condensing

Buttons, Ports, and Connectors

The following table describes the buttons, ports and connectors on ZoneDirector 1200.

TABLE 5 ZoneDirector 1200 front panel elements

Label	Description
Reset	Use the Reset button to restart ZoneDirector.
10/100/1000 Ethernet	Two auto negotiating 10/100/1000Mbps Ethernet ports.
Console	RJ-45 Console port for accessing the ZoneDirector command line interface.
F/D	Factory Default button. To reset ZoneDirector to factory default settings, press and hold the F/D button for at least five (5) seconds. For more information, refer to Alternate Factory Default Reset Method on page 338. **NOTE** Resetting ZoneDirector to factory default settings will erase all configuration changes that you made, except for AP licenses and SSL certificates.

Front Panel LEDs

The following table describes the LEDs on the front panel of ZoneDirector 1200.

TABLE 6 ZoneDirector 1200 LED descriptions

LED Label	State	Meaning
Power	Solid Green	ZoneDirector is receiving power.
	Off	ZoneDirector is NOT receiving power. If the power cable or adapter is connected to a power source, verify that the power cable is connected properly to the power jack on the rear panel of ZoneDirector.
Status	Solid Green	Normal state.
	Flashing Green	ZoneDirector has not yet been configured. Log into the web interface, and then configure ZoneDirector using the setup wizard.
	Red	ZoneDirector has shut down (but is still connected to a power source).
	Flashing Red	ZoneDirector is starting up or shutting down.
Ethernet Link	Solid Green or Amber	The port is connected to a device.
	Flashing Green or Amber	The port is transmitting or receiving traffic
	Off	The port has no network cable connected or is not receiving a link signal.
Ethernet Rate	Green	The port is connected to a 1000Mbps device.
	Amber	The port is connected to a 100Mbps device.
	Off	The port is connected to a 10Mbps device.

Introduction to the Ruckus Network

Your new Ruckus network starts when you disperse a number of Ruckus access points (APs) to efficiently cover your site. After completing the ZoneDirector Setup Wizard and connecting the APs to ZoneDirector, you have a secure wireless LAN (WLAN) for both internal users and guest users.

After using the web interface to set up user accounts for staff and other authorized users, your internal WLAN can be put to full use, enabling authorized users to access the local network, surf the internet, share files, print, check email, and more.

Internal users can easily configure their corporate-issued and BYOD client devices to connect to your corporate WLANs using "Zero-IT Activation", which allows users to self-register their devices and automatically configure them with the proper connection settings with minimal involvement from the IT department.

And as a bonus, guest workers, contractors and visitors can be granted limited controlled access to a separate Guest WLAN with minimal setup required.

Using the ZoneDirector web interface, you can fine-tune and monitor your Wi-Fi networks, customize additional WLANs for specific use cases, manage authorized and guest users, monitor the network's security and performance, and expand your radio coverage, if needed.

Installing ZoneDirector

Basic installation instructions are included in the *Quick Start Guide* that shipped with your ZoneDirector. The steps are summarized below:

1. Connect and discover ZoneDirector using UPnP (Universal Plug and Play). On Windows clients, you may need to turn on network discovery in the **Network and Sharing Center** > **Advanced Sharing Settings**.

   NOTE
   Beginning in ZoneDirector 10.2, you can also perform the same Setup Wizard steps using a CLI Wizard. Refer to the *ZoneDirector 10.2 Command Line Interface Reference Guide* for more information.

2. Double-click the ZoneDirector icon when UPnP displays it, or
3. Point your web browser to ZoneDirector's IP address (default: **192.168.0.2**).
4. Run the Setup Wizard to create an internal and (optionally) a guest WLAN.
5. Distribute APs around your venue, and connect them to power and to your LAN.

6. Begin using your Ruckus network.

FIGURE 2 Discover ZoneDirector using UPnP

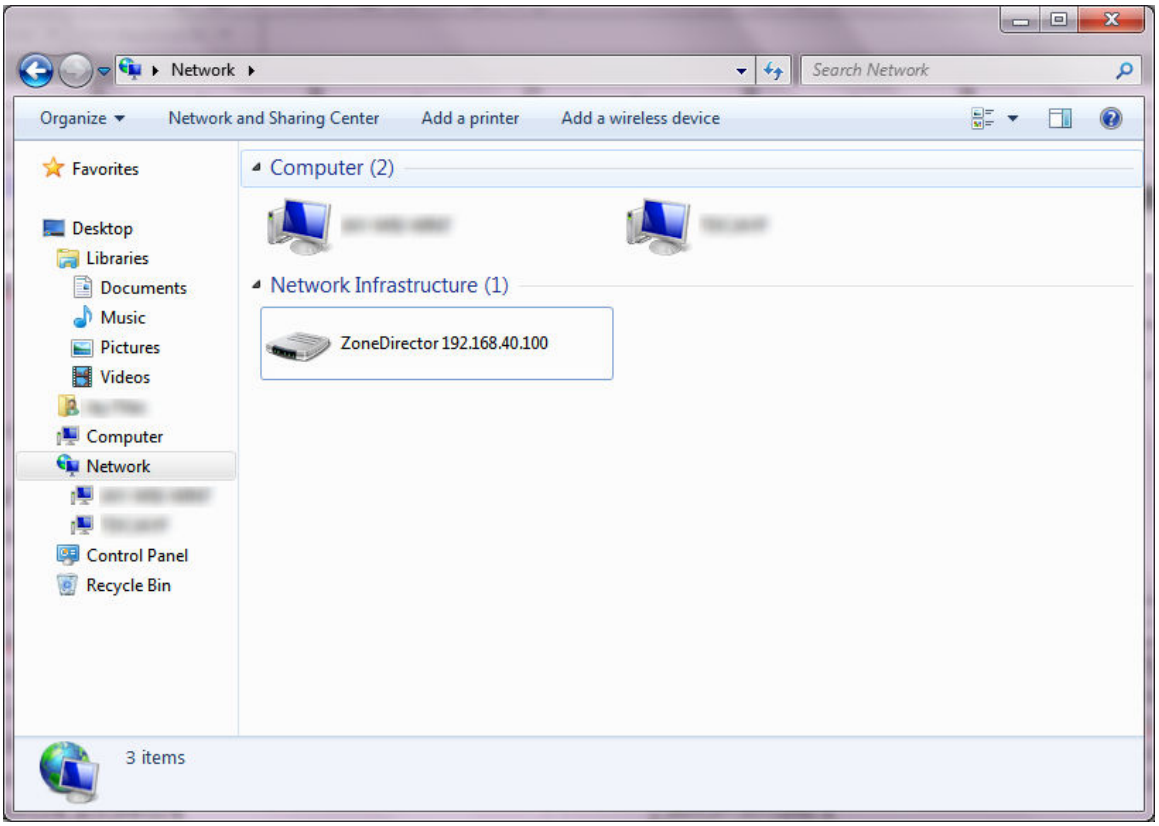
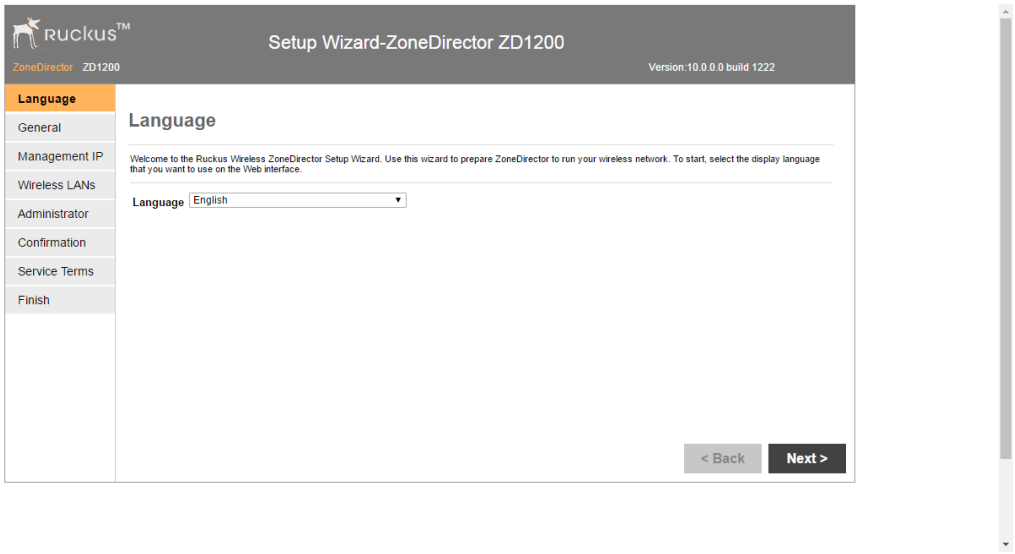


FIGURE 3 ZoneDirector Setup Wizard



Ensuring That APs Can Communicate with ZoneDirector

Before ZoneDirector can start managing an AP, the AP must first be able to discover ZoneDirector on the network when it boots up. This requires that ZoneDirector's IP address be reachable by the AP (via UDP/IP port numbers 12222 and 12223), even when they are on different subnets.

This section describes procedures you can perform to ensure that APs can discover and register with ZoneDirector.

> **NOTE**
> This guide assumes that APs on the network are configured to obtain IP addresses from a DHCP server. If APs are assigned static IP addresses, they must be using a local DNS server that you can configure to resolve the ZoneDirector IP address using **zonedirector.{DNS domain name}** or **zonedirector** if no domain name is defined on the DNS server.

How APs Discover ZoneDirector on the Network

1. When an AP starts up, it sends out a DHCP discovery packet to obtain an IP address.
2. The DHCP server responds to the AP with the allocated IP address. If you configured DHCP Option 43 (or DHCPv6 Option 17) (see Option 2: Customize Your DHCP Server on page 23), the DHCP offer response will also include (among others) the IP addresses of ZoneDirector devices on the network along with the address of the DNS server that can help resolve the ZoneDirector IP addresses.
3. After the AP obtains an IP address, it first attempts to contact a ZoneDirector whose IP address has been pre-configured on the AP. If an AP has a pre-configured ZoneDirector IP address, it will always use an L3 LWAPP (lightweight access point protocol) discovery message to attempt to discover the pre-configured primary/secondary ZoneDirector.
   - An AP with a pre-configured ZoneDirector IP address will only attempt to discover the pre-configured ZoneDirector(s) and will skip the DHCP/DNS/last joined ZoneDirector steps. If it is unable to contact its pre-configured ZoneDirector, it will enter “sulk” state, and will remain in an idle/discover/sulk loop until it receives a response from a pre-configured primary or secondary ZoneDirector.
4. If a primary/secondary ZoneDirector IP address has not been configured on the AP, the AP next attempts to build a list of candidate ZoneDirectors by sending an L3 discovery request (IPv4 subnet broadcast/IPv6 multicast packet) to each candidate address received from DHCP and DNS at the same time, and waits for a response from any ZoneDirector that can respond.
   - The AP may receive multiple responses from DHCP and DNS if multiple ZoneDirector IP addresses have been configured on the DHCP server or DNS server.
5. If the AP receives a response from a single ZoneDirector device, it will attempt to register with that ZoneDirector device.
6. If the AP receives responses from multiple ZoneDirector devices, it will attempt to register with the ZoneDirector that it previously registered with (if any).
   - This ZoneDirector can be on the same local IP subnet or a different subnet. The AP will have a preference for a ZoneDirector device that it previously registered with.
7. If this is the first time that the AP is registering with ZoneDirector, it will attempt to register with the ZoneDirector device that has the lowest AP load. The AP computes the load by subtracting the current number of APs registered with ZoneDirector from the maximum number of APs that ZoneDirector is licensed to support.

If the AP does not receive a response from any ZoneDirector device on the network, it goes into idle mode. After a short period of time, the AP will repeat this discovery cycle until it successfully registers with a ZoneDirector.

How to Ensure that APs Can Discover ZoneDirector on the Network

If you are deploying the APs and ZoneDirector on different subnets, you have three options for ensuring successful communication between these two devices:

- Option 1: Perform Auto Discovery on Same Subnet then Transfer the AP to Intended Subnet on page 23

- Option 2: Customize Your DHCP Server on page 23
- Option 3: Register ZoneDirector with a DNS Server on page 26

NOTE
If the AP and ZoneDirector Are on the Same Subnet: If you are deploying the AP and ZoneDirector on the same subnet, you do not need to perform additional configuration. Simply connect the AP to the same network as ZoneDirector. When the AP starts up, it will discover and attempt to register with ZoneDirector. Approve the registration request (if auto approval is disabled).

Option 1: Perform Auto Discovery on Same Subnet then Transfer the AP to Intended Subnet

If you are deploying the AP and ZoneDirector on different subnets, let the AP perform auto discovery on the same subnet as ZoneDirector before moving the AP to another subnet.

To do this, connect the AP to the same network as ZoneDirector. When the AP starts up, it will discover and attempt to register with ZoneDirector. Approve the registration request if auto approval is disabled. After the AP registers with ZoneDirector successfully, transfer it to its intended subnet. It will be able to find and communicate with ZoneDirector once you reconnect it to the other subnet.

NOTE
If you use this method, make sure that you do not change the IP address of ZoneDirector after the AP discovers and registers with it. If you change the ZoneDirector IP address, the AP will no longer be able to communicate with it and will be unable to rediscover it.

Option 2: Customize Your DHCP Server

NOTE
The following procedure describes how to customize a DHCP server running on Microsoft Windows. If your DHCP server is running on a different operating system, the procedure may be different.

NOTE
For ZoneDirector discovery using IPv6, see *IPv6 Configuration for ZoneDirector Discovery using DHCPv6*.

Configuring the DHCP Server for ZoneDirector-AP Communication

To customize your DHCP server, you need to configure DHCP Option 43 (043 Vendor Specific Info) with the IP address of the ZoneDirector device on the network.

When an AP requests an IP address, the DHCP server will send a list of ZoneDirector IP addresses to the AP. If there are multiple ZoneDirector devices on the network, the AP will automatically select a ZoneDirector to register with from this list of IP addresses.

RFC 2132 describes DHCP Option 60 and Option 43. DHCP Option 60 is the Vendor Class Identifier (VCI). The VCI is a text string that identifies a vendor/type of a DHCP client. All Ruckus Access Points are configured to send “Ruckus CPE” as the Vendor Class Identifier in option 60, and expect ZoneDirector IP information to be provided in DHCP option 43 (Vendor Specific Info), encapsulated with sub-option code 03 (the sub-option code for ZoneDirector).

The RFC describes how vendors can encapsulate vendor-specific sub-option codes (ranging from 0 to 255). Sub-options are embedded in option 43 as TLV (type, length, value) blocks.

Ruckus Access Points support non-TLV format option 43 values with comma separated IP address strings for discovering ZoneDirectors, and also TLV based option 43 encapsulation as specified in RFC 2132.

For ZoneDirector information (sub-option code 03)

- **Type**: 0x03

- **Length**: Count of the characters in the ASCII string. (Length must include the commas if there is more than one ZoneDirector specified.)
- **Value**: A non-null terminated ASCII string that is a comma-separated list of ZoneDirector IP addresses

Example: If the there are two ZoneDirectors with IP addresses 192.168.0.10 and 192,168.0.20, then the value will be "**192.168.0.10,192.168.0.20**" and the length is **25** (hex value 0x19).

For UMM information (sub-option code 01)

To configure your DHCP server for Unleashed Multi-site Manager (UMM, formerly known as FlexMaster) discovery, use the following settings.

- **Type**: 0x01
- **Length**: Count the number of characters in the ASCII string. (Length must include "http", plus all colons, slashes and decimals in the complete URL.)
- **Value**: A non-null terminated ASCII string that is a URL.

Example: If the UMM (FlexMaster) URL is http://192.168.10.1/intune/server, the length is 33 (hex value 0x21).

You will need this information when you configure DHCP Option 43 for both UMM and ZoneDirector. To calculate the length field conversion from decimal to hexadecimal, you can use an online conversion website, such as http://www.easycalculation.com/decimal-converter.php, to perform the conversion.

The table below lists the sub-option code, UMM URL and ZoneDirector IP address that are used as examples in this procedure, along with their lengths in decimal and hexadecimal values.

	URL / IP Address	Decimal Length	Hexadecimal Length	Sub-option Code
UMM	http://192.168.10.1/intune/server (URL)	33	21	01
ZoneDirector	192.168.10.2 (IP Address)	12	0C	03

Most commonly used DHCP servers such as Microsoft DHCP and ISC DHCP support vendor class DHCP option spaces and mapping of those option spaces to option 60. While you can achieve encapsulating TLVs in option 43 by hard coding the DHCP option 43 value, Ruckus recommends using vendor class option spaces - especially when you have more than one vendor type on the network and need option 43 to be supported for different vendor type DHCP clients.

The following example describes how you can encapsulate option 43 using DHCP vendor class option spaces to provide two ZoneDirector IP addresses: 192.168.0.10 and 192.168.0.20.

Configure Vendor Class Identifier and Vendor Specific Info sub-options on Microsoft DHCP server

Configure vendor class for Ruckus Access Points:

1. In the **Server Manager** window, right-click the IPv4 icon, and choose **Define Vendor Classes** from the menu.
2. In the **DHCP Vendor Classes** dialogue, click **Add** to create a new vendor class.
3. Enter the value to describe the option class/space, (e.g., **RuckusWirelessAP**). Optionally, you can also enter a description.
4. Add the VCI string in the **ASCII** field and click **OK**. The new vendor class is created **Close** to close the dialogue.
5. Right-click the newly created vendor class and select **Set Predefined Options...**
6. Predefine the ZoneDirector sub-option type for the newly created vendor class. This section defines the code and format of the sub-option (code for ZoneDirector and comma separated IP addresses in ASCII text string).
7. Configure the option with a value either at the server level, scope level or at **Configure Options** > **Advanced**

NOTE
You can also optionally configure DHCP Option 12 (Host Name) to specify host names for APs. Then, when an AP joins ZoneDirector and ZoneDirector does not already have a device name for this AP, it will take the host name from DHCP and display this name in events, logs and other web interface elements. See your DHCP server documentation for instructions on Option 12 configuration.

IPv6 Configuration for ZoneDirector Discovery Using DHCPv6

Beginning with release 9.13, ZoneDirector also supports AP discovery using IPv6 DHCP Option 17 (in addition to IPv4 DHCP Option 43).

NOTE
The following instructions assume isc-dhcp-server as the Linux DHCP server. For other DHCP servers, refer to the relevant documentation for instructions on customizing the DHCPv6 Option 17 sub-options.

To configure a DHCPv6 server for AP controller discovery, use the following procedure:

1. Install radvd

```
yum radvd
```

2. Install isc-dhcp-server:

```
yum isc-dhcp-server
```

3. Edit the “/etc/radvd.conf” file as follows:

```
interface eth1
{
        AdvSendAdvert on;
        AdvOtherConfigFlag on;
        prefix 2001:db8:0:2::/64
        {
        };
};
```

4. Edit the “dhcp6.conf file” as follows:

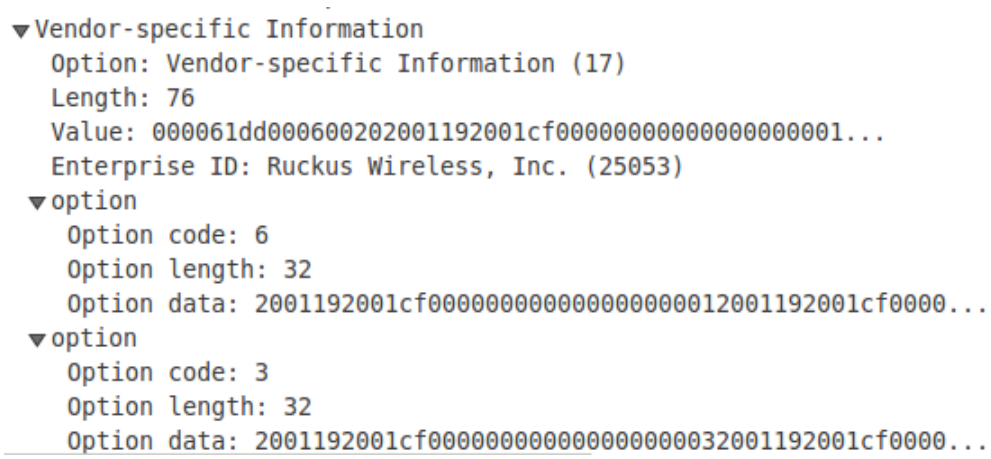
```
default-lease-time 600;
max-lease-time 7200;
log-facility local7;
subnet6 2001:db8:0:2::/64 {
        # Range for clients
            range6 2001:db8:0:2::129 2001:db8:0:2::254;
            # Additional options
            option dhcp6.name-servers fec0:0:0:1::1;
            option dhcp6.domain-search "domain.example";
            option dhcp6.vendor-opts 00:00:61:dd:
            00:06:<-- suboption code 6 for SmartZone List
            00:20:<-- suboption length, 2 IP addresses in the list, so value is 0x20
            20:01:19:20:01:cf:00:00:00:00:00:00:00:00:00:01:<-- IP address
            20:01:19:20:01:cf:00:00:00:00:00:00:00:00:00:02:<-- IP address
            00:03:<-- suboption code 3 for ZD List
            00:20:<-- suboption length, 2 IP addresses in the list, so value is 0x20
            20:01:19:20:01:cf:00:00:00:00:00:00:00:00:00:03:<-- IP address
            20:01:19:20:01:cf:00:00:00:00:00:00:00:00:00:04;<-- IP address
        # Prefix range for delegation to sub-routers
        prefix6 2001:db8:0:200:: 2001:db8:0:f00:: /56;
        # Example for a fixed host address
        host specialclient {
            host-identifier option dhcp6.client-id
            00:01:00:01:4a:1f:ba:e3:60:b9:1f:01:23:45;
            fixed-address6   2001:db8:0:2::127;
```

5. To confirm that the AP has received the correct IP info through DHCPv6 option 17, you can check the /tmp/dhcp6_vendor_opts file. Use the following command on the AP CLI:

```
# cat /tmp/dhcp6_vendor_opts
code3
2001:1920:1cf::3
2001:1920:1cf::4
end
code6
2001:1920:1cf::1
2001:1920:1cf::2
end
```

6. You have completed configuring the isc-dhcp-server for controller discovery using DHCPv6 Option 17. To confirm that the DHCPv6 options are configured properly (whether using isc-dhcp-server or another DHCPv6 server), you should ensure that the Option 17 configuration looks like the following figure:

   FIGURE 4 Ensuring that DHCPv6 Option 17 is configured correctly



Option 3: Register ZoneDirector with a DNS Server

If you register ZoneDirector with your DNS server, supported APs that request IP addresses from your DHCP server will also obtain DNS related information that will enable them to discover ZoneDirector devices on the network. Using the DNS information they obtained during the DHCP request, APs will attempt to resolve the ZoneDirector IP address (or IP addresses) using **zonedirector.{DNS domain name}**.

To register ZoneDirector devices with DNS server:

- Step 1: Set the DNS Domain Name on the DHCP Server
- Step 2: Set the DNS Server IP Address on the DHCP Server
- Step 3: Register the ZoneDirector IP Addresses with a DNS Server

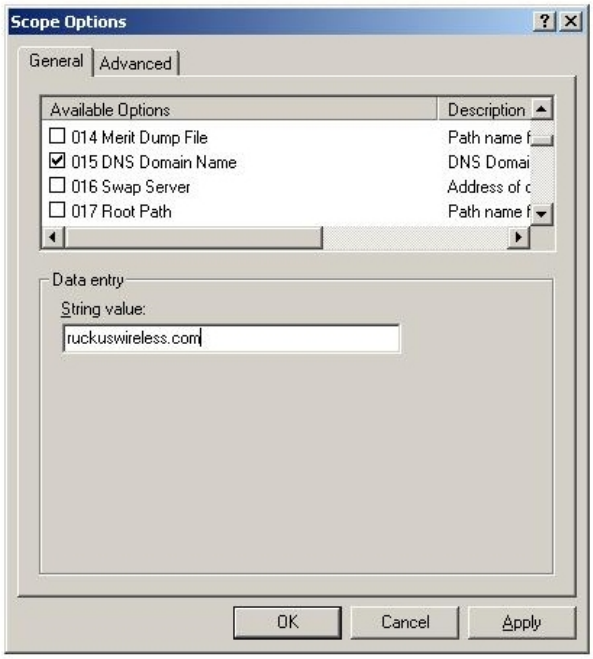
NOTE
The following procedures describe how to customize a DHCP server running on Microsoft Windows Server. If your DHCP server is running on a different operating system, the procedure may be different.

Step 1: Set the DNS Domain Name on the DHCP Server

1. From **Windows Administrative Tools**, open DHCP, and then select the **DHCP** server that you want to configure.

2. If the **Scope** folder is collapsed, click the plus (+) sign to expand it.
3. Right-click **Scope Options**, and then click **Configure Options**. The General tab of the **Scope Options** dialog box appears.
4. Under **Available Options**, look for the **15 DNS Domain Name** check box, and then select it.
5. In the **String value** text box under **Data Entry**, type your company's domain name
6. Click **Apply** to save your changes.
7. Click **OK** to close the Scope Options dialog box.

FIGURE 5 Select the 015 DNS Domain Name check box, and then type your company domain name in String value

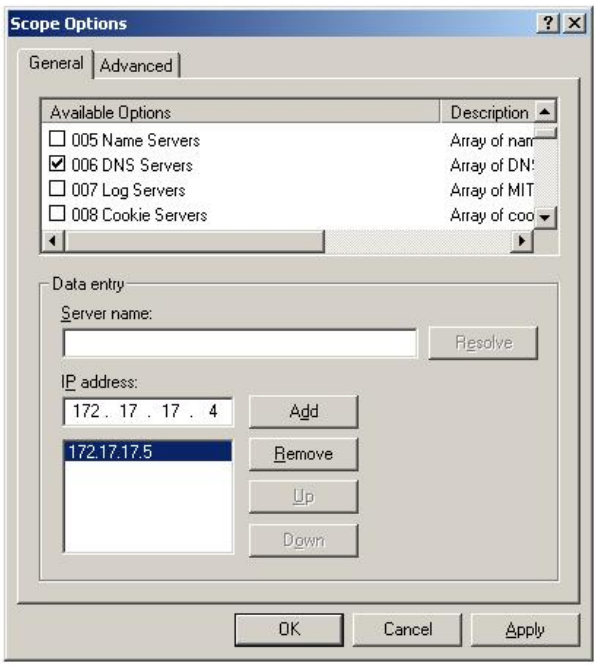


Step 2: Set the DNS Server IP Address on the DHCP Server

1. From **Windows Administrative Tools,** open **DHCP**, and then select the DHCP server you want to configure.
2. If the **Scope** folder is collapsed, click the plus (+) sign to expand it.
3. Right-click **Scope Options**, and then click **Configure Options**. The tab of the **Scope Options** dialog box appears.
4. Under **Available Options**, look for the **6 DNS Servers** check box, and then select it
5. In the IP address box under **Data Entry**, type your **DNS server's IP address**, and then click **Add**. If you have multiple DNS servers on the network, repeat the same procedure to add the other DNS servers.
6. Click **Apply** to save your changes.

7. Click **OK** to close the **Scope Options** dialog box.

FIGURE 6 Select the 006 DNS Servers check box, and then type your DNS server's IP address in the Data entry section



Step 3: Register the ZoneDirector IP Addresses with a DNS Server

After you complete configuring the DHCP server with DNS related information, you need to register the IP addresses of ZoneDirector devices on the network with your DNS server. The procedure for this task depends on the DNS server software that you are using.

Information on configuring the built-in DNS server on Windows is available at http://support.microsoft.com/kb/814591

NOTE
If your DNS server prompts you for the corresponding host name for each ZoneDirector IP address, you MUST enter zonedirector. This is critical to ensuring that the APs can resolve the ZoneDirector IP address.

After you register the ZoneDirector IP addresses with your DNS server, you have completed this procedure. APs on the network should now be able to discover ZoneDirector on another subnet.

Firewall Ports that Must be Open for ZoneDirector Communications

Depending on how your network is designed, you may need to open ports on any routers or firewalls located between ZoneDirector, the access points, and other network components.

The following table lists the ports that need to be open for different types of communications.

TABLE 7 Firewall ports that must be open for ZoneDirector communications

Communication	Ports
ZoneDirector Web UI access	TCP ports 80 and 443 (HTTP and HTTPS)
AP < > ZoneDirector LWAPP	UDP ports 12222 and 12223

TABLE 7 Firewall ports that must be open for ZoneDirector communications (continued)

Communication	Ports
AP < > ZoneDirector AP provisioning	TCP port 21 for FTP (the firewall must be stateful for PASV FTP transfers using a port higher than 1024)
AP < > ZoneDirector SpeedFlex	UDP port 18301
AP < > ZoneDirector (AP) firmware upgrade	TCP port 21 for FTP (the firewall must be stateful for PASV FTP transfers using a port higher than 1024)
AP < > ZoneDirector application statistics reporting	TCP port 21 for FTP (the firewall must be stateful for PASV FTP transfers using a port higher than 1024)
ZoneDirector < > ZoneDirector Smart Redundancy	TCP port 443 and port 33003
ZoneDirector > UMM registration/inform/firmware upgrade	TCP port 443
UMM > ZoneDirector management interface	TCP port as specified in UMM Inventory 'Device Web Port Number Mapping'
ZoneDirector CLI access	TCP port 22 (SSH)
TACACS+ server < > ZoneDirector	TCP port 49 (TACACS+) (default)
ZoneDirector portal page access (for Guest and Web-based-authentication WLANs)	TCP port 9999 (HTTP access) and port 8099 (HTTPS access)
ZoneDirector < > RADIUS server	UDP ports 1812, 1813, 1815, and 3799 **NOTE** Note: 1812 is for RADIUS authentication, 1813 is for RADIUS accounting, 1815 is for Radsec, 3799 is for RADIUS DM (Disconnect Messages) and COA (Change of Authorization).
ZoneDirector/AP > external syslog server	UDP port 514
AP < > ZoneDirector location service	TCP port 8883
AP > ZoneDirector secure AP image upgrade over HTTPS (if enabled, disabled by default)	TCP port 11443
ZoneDirector CLI access (Telnet, disabled by default)	TCP port 23
ZonerDirector SNMP Access	UDP port 161

Accessing ZoneDirector's Command Line Interface

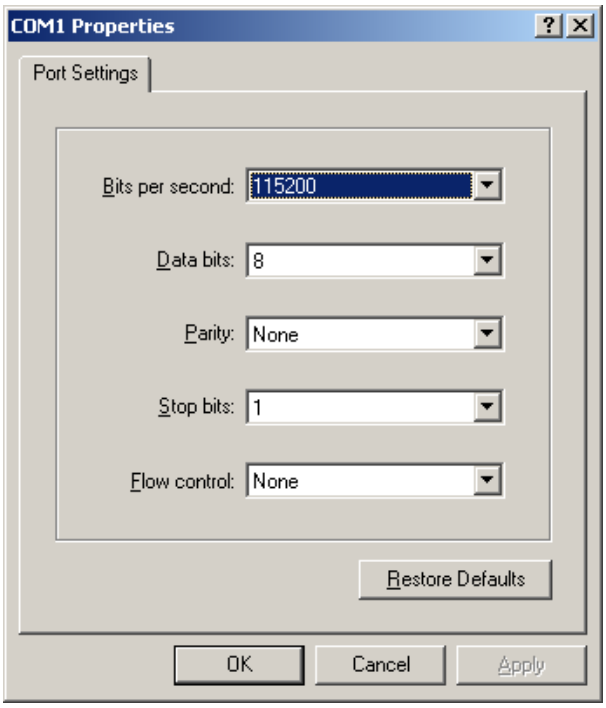
In general, this User Guide provides instructions for managing ZoneDirector and your ZoneFlex network using the ZoneDirector web interface. You can also perform many management and configuration tasks using the ZoneDirector Command Line Interface (CLI) by connecting directly to the Console port or an Ethernet port.

To access the ZoneDirector CLI:

1. Connect an admin PC to the ZoneDirector Console port or any of the LAN ports (using either a DB-9 serial cable for the console port, or an Ethernet cable for LAN ports).
2. Launch a terminal program, such as Hyperterminal, PuTTy, etc.

3. Enter the following connection settings:
   - Bits per second: 115200
   - Data bits: 8
   - Parity: None
   - Stop bits: 1
   - Flow control: None

   FIGURE 7 Configure a terminal client



4. Click **OK** or **Open** to connect (depending on your terminal client).
5. At the **Please Login** prompt, enter the admin login name (default: **admin**) and password (default: **admin**).

You are now logged into ZoneDirector with limited privileges. As a user with limited privileges, you can view a history of previously executed commands and ping a device. If you want to run more commands, you can switch to privileged mode by entering **enable** at the root prompt.

To view a list of commands that are available at the root level, enter **help** or **?**.

For more information on using the CLI, see the *Ruckus Wireless ZoneDirector Command Line Interface Reference Guide*, available from http://support.ruckuswireless.com/.

Using the ZoneDirector Web Interface

The ZoneDirector web interface consists of several interactive components that you can use to manage your Ruckus Wi-Fi deployment including ZoneDirector and all connected APs.

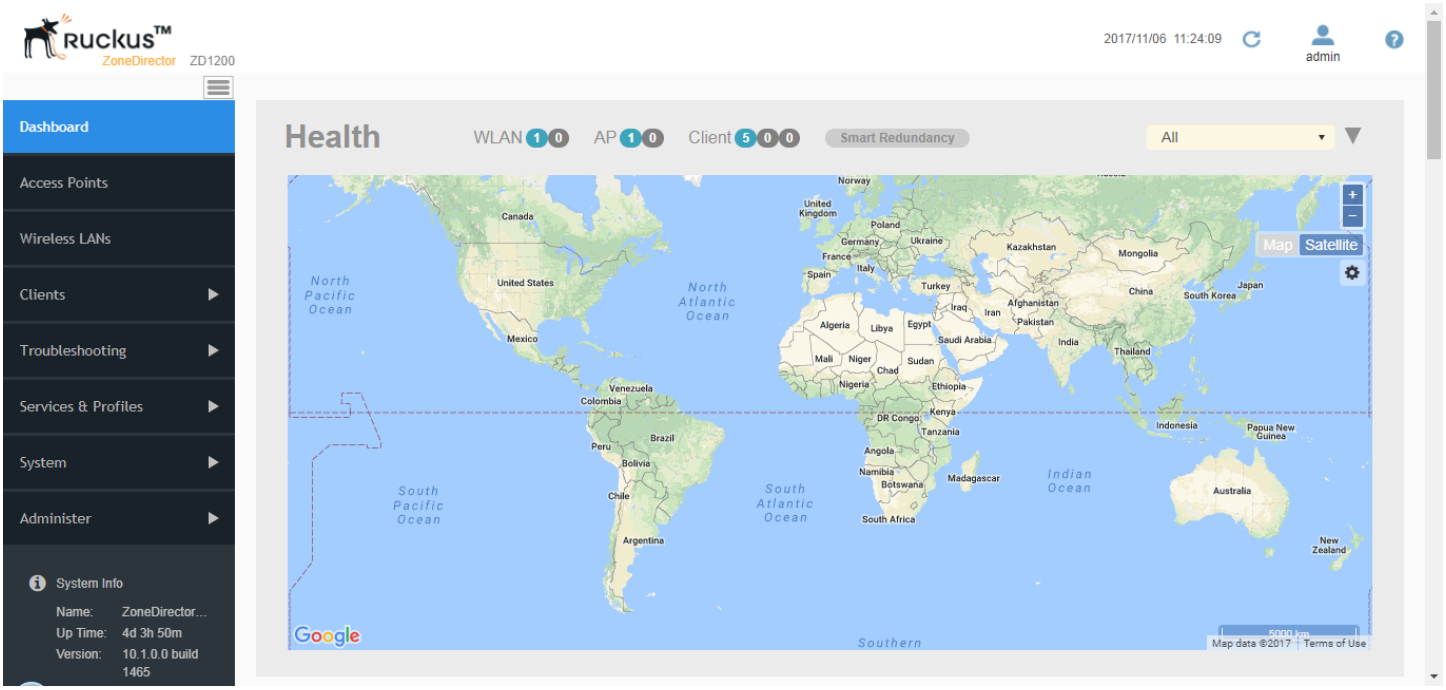
When you first log into your ZoneDirector using the web interface, the **Dashboard** appears, displaying a map view of your APs (if coordinates are configured) in the top section, and a **Traffic Analysis** view of total network traffic and client statistics in the bottom section.

In addition to the Dashboard, the ZoneDirector web interface contains several expandable menu items on the left side. Click the menu option to view more details and configuration options for access points, clients, WLANs, system and administration settings, and ZoneDirector services.

TABLE 8 ZoneDirector web interface elements

Dashboard	The Dashboard provides an overview of the system and is divided into two sections; Health and Traffic Analysis.
Access Points	Click this tab to view and configure access points, AP groups, AP policies, and other AP-related settings.
Wireless LANs	Click this tab to view and configure WLANs, WLAN groups, Zero-IT and DPSK settings.
Clients	Expand this tab to monitor and configure wireless clients, wired clients, generated PSKs and guest passes, and view application usage and performance statistics.
Troubleshooting	Expand this tab to access troubleshooting tools such as ping, traceroute, and client connectivity issue diagnosis, and to perform other troubleshooting procedures such as downloading debug logs or executing a packet capture.
Services & Profiles	Expand this tab to configure ZoneDirector services such as Application Control, Access Control, Guest Access and Hotspot profiles, as well as internal and external system settings such as Mesh and AAA server configuration.
System	Expand this tab to configure ZoneDirector system settings such as IP address settings, Smart Redundancy, email and SMS settings, and to view general system information such as a system overview and a list of all events/activities maintained by ZoneDirector's event log.
Administer	Expand this tab to configure admin settings such as admin login name and password, and to perform admin functions such as system backup, restore and upgrade.

FIGURE 8 Dashboard - top



Navigating the Dashboard

The Dashboard provides a basic overview of the general health and traffic status of the network.

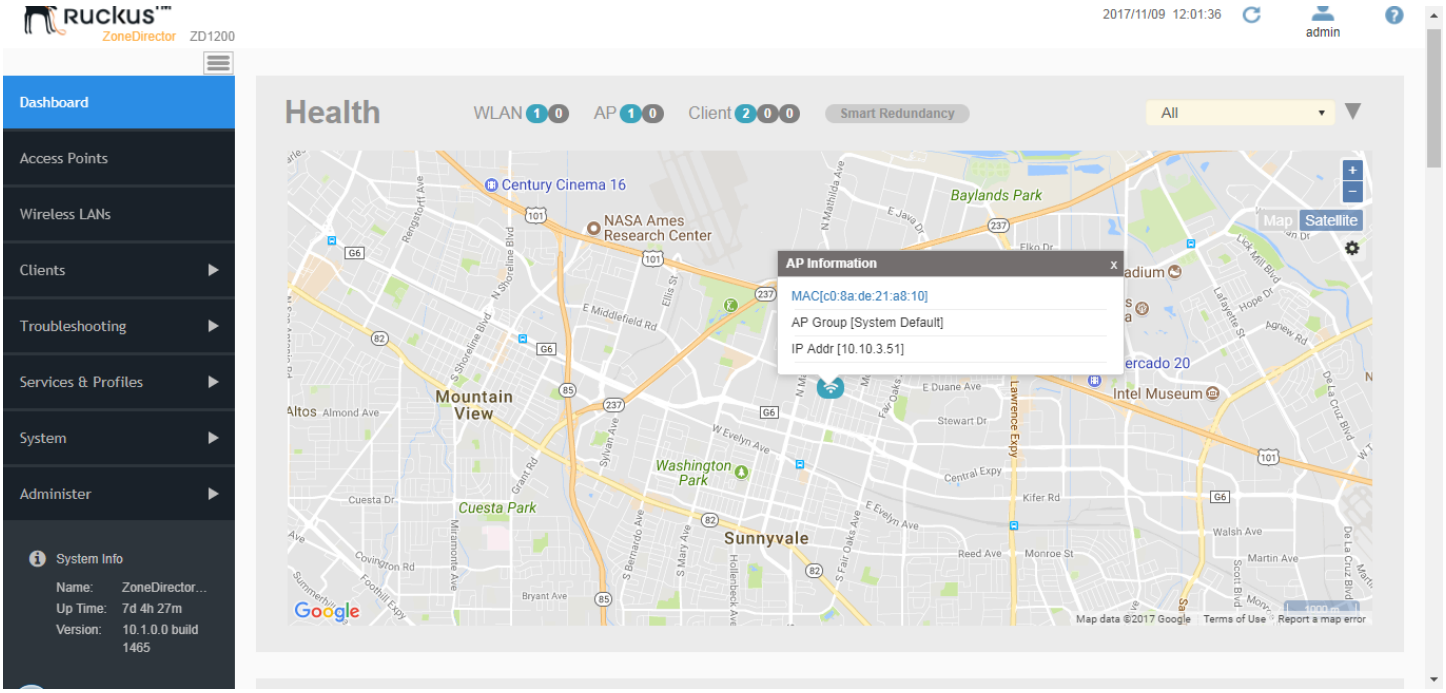
Health

The **Health** section includes a summary of the total number of WLANs, APs and clients currently connected above the map view. The map view itself provides a geographical view of the placement of APs (if map coordinates are configured), and can be filtered by AP group or replaced with a custom interior map using the drop-down menu above the map.

Hover over an AP on the map to view its MAC address, AP group and IP address.

NOTE
If an AP is incorrectly located or does not appear on the map, go to **Access Points** and configure the AP's **GPS Coordinates**.

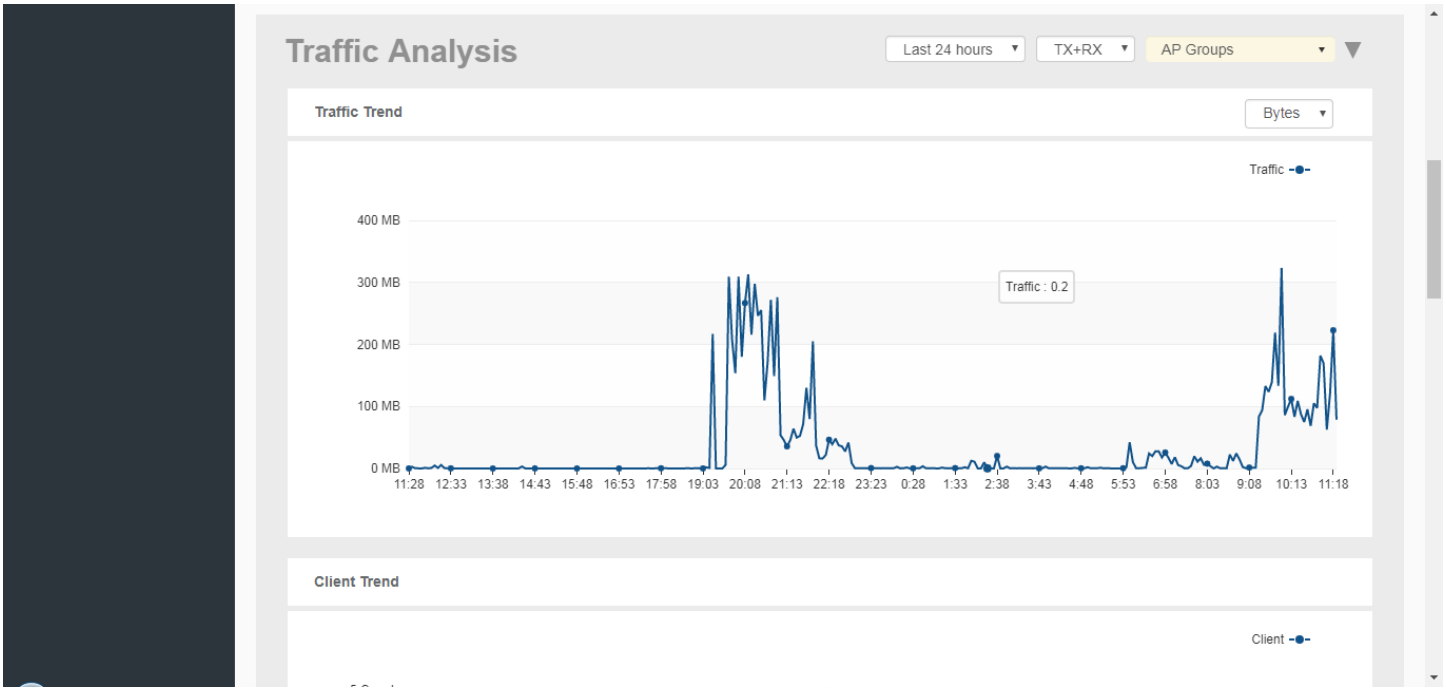
FIGURE 9 Hover over an AP to view its details (if map coordinates are configured)



Traffic Analysis

The **Traffic Analysis** section contains graphs of traffic and client count statistics, top clients by traffic volume, and a pie chart displaying the breakdown of clients by device type. Each of these views can be customized to display data for the last hour or last 24 hours, and can be filtered by AP, AP group and WLAN. You can also click the gear icon to customize the information displayed in the tables.

FIGURE 10 The Traffic Analysis section of the ZoneDirector Dashboard



Registering Your Product

Ruckus Networks encourages you to register your ZoneDirector product to receive updates and important notifications, and to make it easier to receive support in case you need to contact Ruckus for customer assistance. You can register your ZoneDirector along with all of your APs in one step using ZoneDirector's Registration form.

> **NOTE**
> To ensure that all registration information for all of your APs is included, be sure to register *after* all APs have been installed. If you register ZoneDirector before installing the APs, the registration will not include AP information.

To register your ZoneDirector:

1. Go to **Administer** > **Support**.
2. Click the **Product Registration** link.
3. Enter all information in the required fields, and click **Apply**.
4. The information is sent to a CSV file that opens in a spreadsheet program (if you have one installed). This file includes the serial numbers and MAC addresses of your ZoneDirector and all known APs, and your contact information.
5. Save the CSV file to a convenient location on your local computer.
6. Click the link on the **Registration** page to upload the CSV file (https://support.ruckuswireless.com/register). If you do not already have a Support account login, first click the https://support.ruckuswireless.com/get_access_now link to create a support account, and then click the register link to upload the CSV file to Ruckus Support.

Your ZoneDirector is now registered with Ruckus.

Managing Access Points

- Managing Access Points Overview..... 35
- Adding New Access Points to the Network..... 35
- Working with Access Point Groups..... 37
- Configuring Global Access Point Policies..... 53
- Importing a USB Software Package..... 56
- Managing Access Points Individually..... 57
- Optimizing Access Point Performance..... 61

Managing Access Points Overview

ZoneDirector provides extensive options for managing APs individually or in AP groups.

Using the *Access Points* options, admins can configure specific radio controls such as channel and channel width for a specific AP, or general controls such as which WLANs will be broadcast on which AP radios.

The *Access Points* page also provides monitoring and troubleshooting tools that allow the admin to monitor application performance, test connectivity using Ping/Traceroute, reboot an AP, run a SpeedFlex throughput performance test, perform RF spectrum analysis, download RF info debug logs, or track AP-specific events/activities.

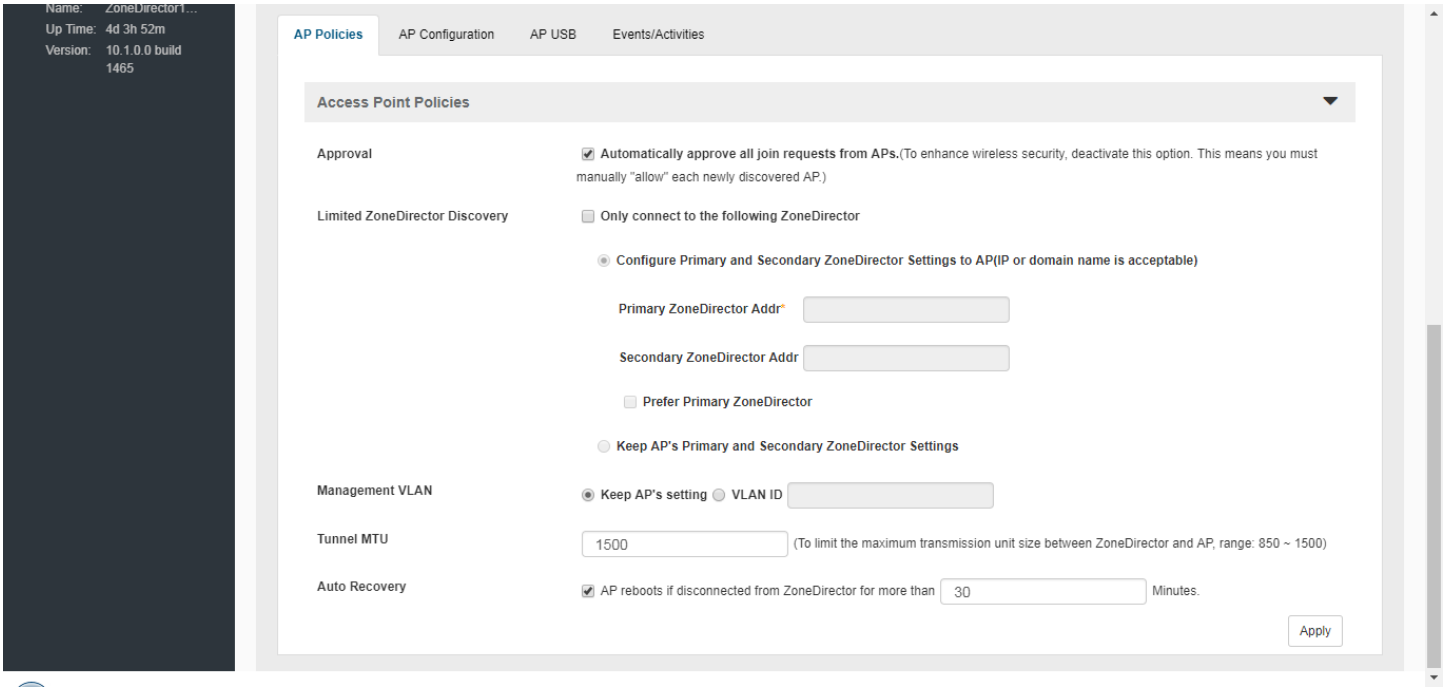
Adding New Access Points to the Network

If your staffing or wireless coverage needs increase, you can add APs to your network easily and efficiently.

Depending on your network security preferences, new APs can be automatically detected and activated, or new APs may require per-device manual approval before becoming active.

The Automatic AP Approval process is enabled by default, automatically approving AP join requests. If you prefer, you can disable Automatic Approval. If this is your preference, ZoneDirector will detect new APs, alert you to their presence, and then wait for you to manually “approve” their activation.

FIGURE 11 Automatic AP approval is enabled by default. Deselect this option to manually approve each AP join request.



Connecting the APs to the Network

1. Place the new APs in the appropriate locations.
2. Write down the MAC address (on the bottom of each device) and note the specific location of each AP as you distribute them.
3. Connect the APs to the LAN with Ethernet cables.

   NOTE
   If using PoE, ensure that you use Cat5e or better Ethernet cables.

   NOTE
   By default, Ruckus APs will attempt to obtain an IP address via DHCP as soon as they are connected to the network. If you do not want the AP to automatically request an IP address, you must first configure a static IP address using the AP web interface or CLI before connecting them to your network.

4. Connect each AP to a power source.

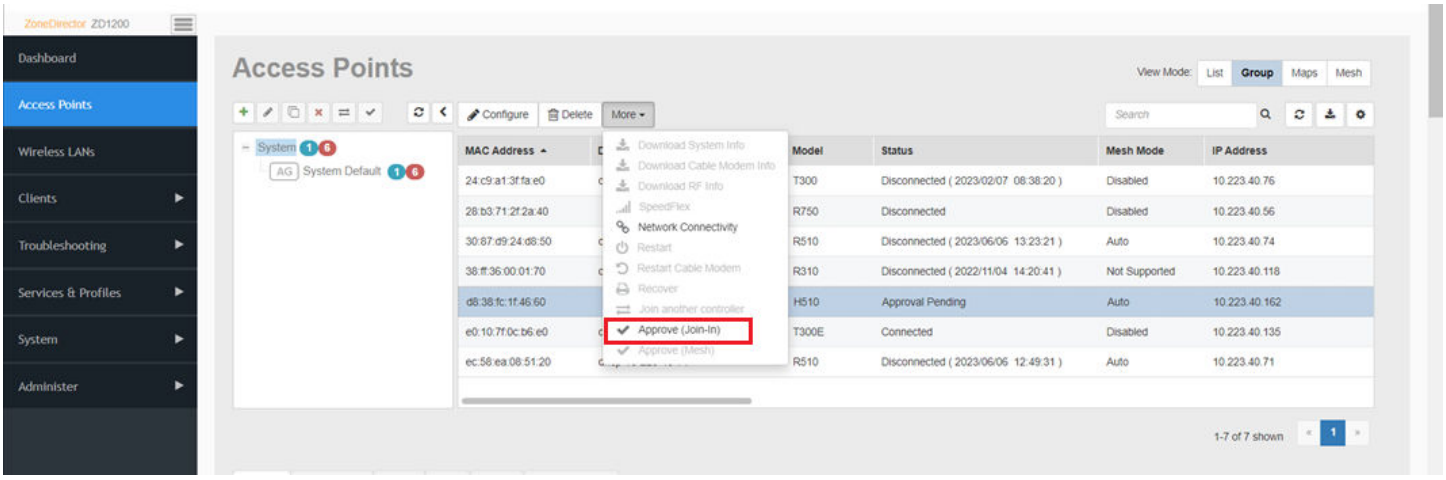
   NOTE
   Alternatively, if the APs that you are using are PoE-capable, they will draw power through the Ethernet cable if connected to a PoE switch.

Verifying or Approving New APs

1. Go to **Access Points**. The **Access Points** page displays the access points that have been approved or are awaiting approval.

2. Review the **Access Points** table:
   - If the **Approval** check box is checked, the new APs listed in the table display the status as **Connected**.
   - If the **Automatic AP Approval** option is disabled, the new APs listed display the status as **Approval Pending**.
3. Select an AP that is displaying the **Approval Pending** status and click **More** > **Approve (Join-In)**.

FIGURE 12 Approving a New AP



The new AP is activated and ready for use.

Working with Access Point 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. Access Point groups are similar to WLAN groups (see Working with WLAN Groups on page 83). While WLAN groups can be used to specify which WLAN services are served by which APs, AP groups are used for more specific fine-tuning of how the APs themselves behave.

The following sections describe the three main steps involved in working with AP groups:

- Modifying the System Default AP Group on page 38: The first step in working with AP groups is defining the default behavior of all APs controlled by ZoneDirector.
- Creating a New Access Point Group on page 40: After you have defined how you want your default APs to behave, you can create a subset of access points with different settings from the default settings.
- Modifying Access Point Group Membership on page 41: Lastly, you can easily move access points between groups as described in this section.

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 (**Access Points > Edit [AP MAC address]**) and set the Tx Power setting to a lower setting.

TABLE 9 Maximum number of AP groups by ZoneDirector model

ZoneDirector Model	Max AP Groups
ZoneDirector 1200	128

Modifying the System Default AP Group

If you want to apply global settings to all access points that are controlled by ZoneDirector, you can modify the settings of the System Default AP group and apply them to all ZoneDirector-controlled APs at once.

To modify the System Default Access Point group and apply global configuration:

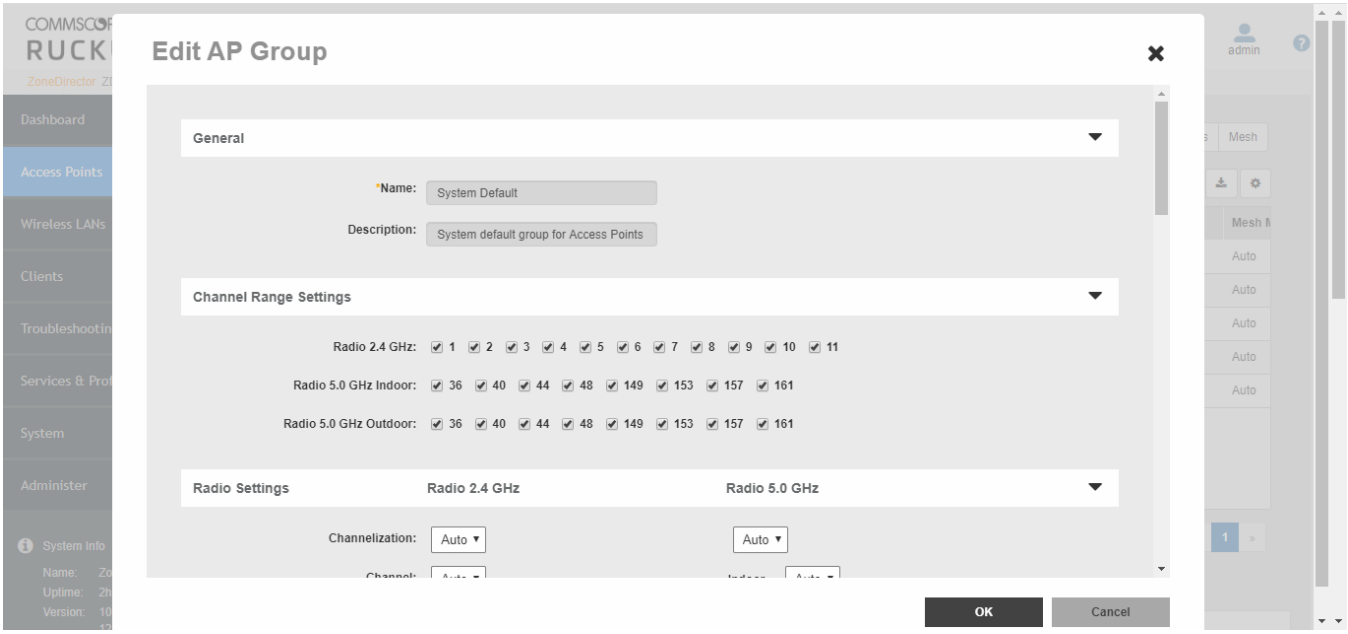
1. Go to **Access Points**.
2. In the **Access Point Groups** section on the left side of the screen, select the *System Default* access point group, and click the **Configure** button. The **Edit AP Group** form appears.

3. Modify any of the settings in the following table that you want to apply to the System Default AP group, and click **OK** to save your changes.

Setting	Description
Name	The System Default group name cannot be changed (you can edit this field when creating/editing any other AP group).
Description	The System Default description cannot be changed (you can edit this field when creating/editing any other AP group).
Channel Range Settings	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, 20 MHz or 40 MHz 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
WLAN Group	Specify which WLAN group this AP group belongs to.
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 on the 2.4 GHz radio. 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.
IP Mode	Set IPv4, IPv6 or dual-stack IPv4/IPv6 IP addressing mode.
Location Service	Enable this option to enable ZoneDirector's share in the Ruckus SmartPositioning Technology (SPoT) location based service solution. Select the Venue Name that you created on the *Services & Profiles > Location Services* page. See SPoT Location Services on page 288. For information on configuration and administration of Ruckus SmartPositioning Technology (SPoT) service, refer to the *SPoT User Guide*, available from the Ruckus support site: *https://support.ruckuswireless.com*.
Model Specific Control	Use this section to configure max clients, LEDs and port settings for all APs of each specific model that are members of the group. See Modifying Model Specific Controls on page 42.

Setting	Description
Group Settings	The Group Settings section is used to move access points between groups. See Modifying Access Point Group Membership on page 41.

FIGURE 13 Editing the System Default access point group settings



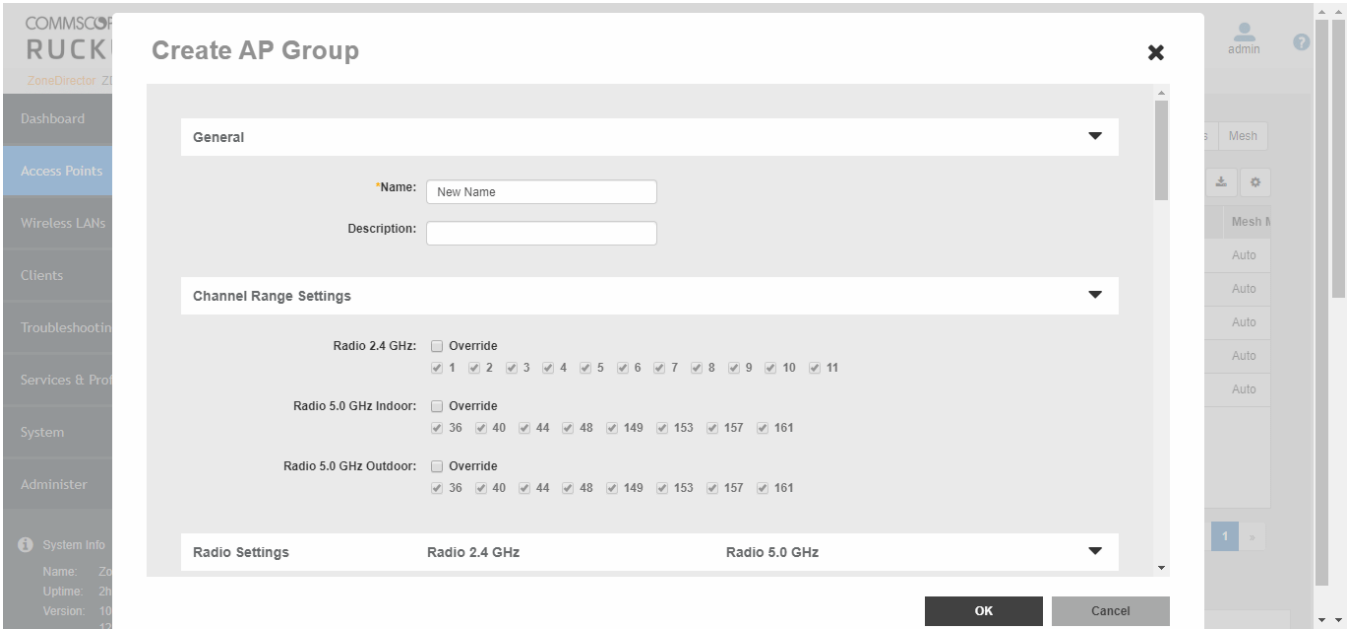
Creating a New Access Point Group

To create a new AP group with custom settings:

1. Go to **Access Points**.
2. In the **Access Point Groups** section, click the **Create AP Group** button.
3. Enter a **Name** and optionally a **Description** for the new AP group.

4. Modify any of the settings that you want to apply to the new AP group, and click **OK** to save your changes.

FIGURE 14 Creating a new AP Group



Modifying Access Point Group Membership

When more than one AP group exists, you can move APs between groups using the Group Settings section of the *Edit AP Group* form.

The *Group Settings* section is divided into two subsections:

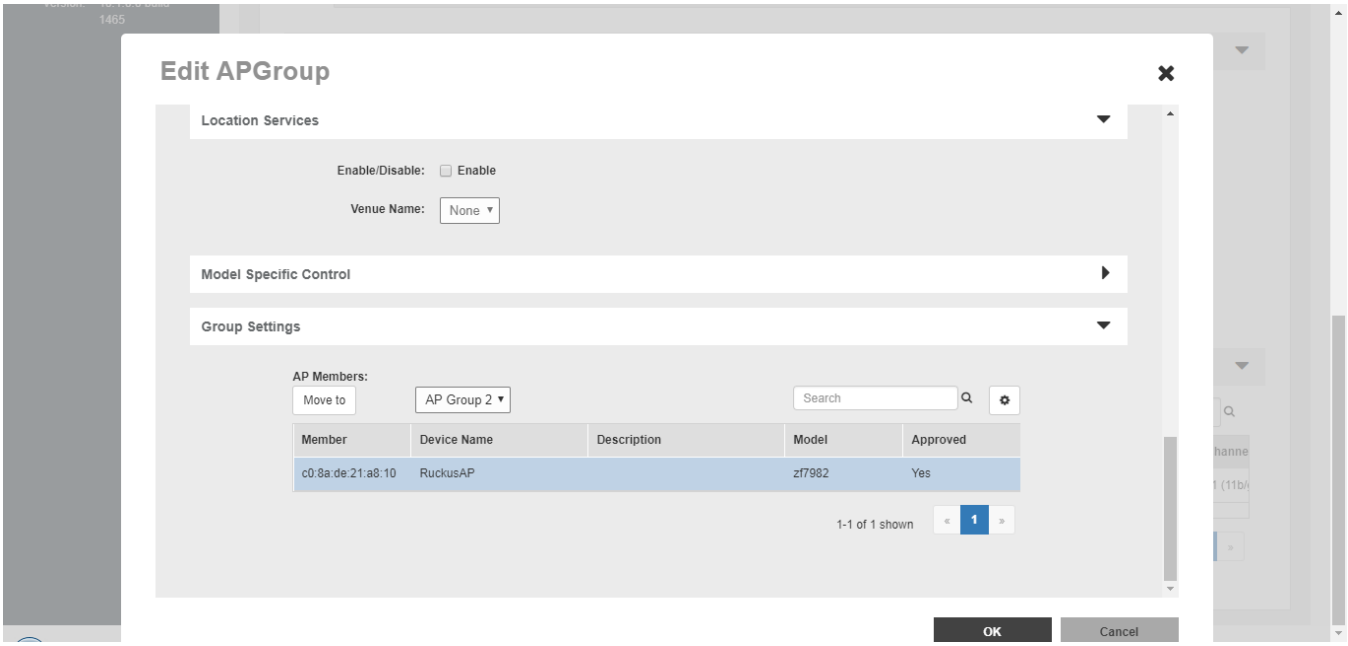
- **AP Members**: Lists the current member APs of this AP group.
- **Available Access Points**: Lists the APs that are members of other AP groups.

To move an AP from the current AP group to another group:

1. In **Members**, select the AP (or APs) that you want to move to another AP group, select the target AP group from the menu, and click the **Move To** to button.
2. Click **OK** to save your changes.

3. **To move an AP from another AP group into the AP group you are currently editing:**
   a) In **Access Points**, click the check box next to any AP you want to move, and click **Add** to this group. The AP disappears from the Access Points list and appears immediately in the Members list.
   b) Click **OK** to save your changes.

FIGURE 15 Modify AP group membership



Modifying Model Specific Controls

The following settings can be applied to all APs of a particular model that are members of the AP group:

- **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).

  NOTE
  If your ZoneDirector country code is set to United Kingdom, an additional “Enable 5.8 GHz Channels” option will be available, and an additional "5.8 GHz Channels License" option will be available for outdoor APs. Enabling the 5.8 GHz Channels option allows the use of restricted C-band channels. These channels are disabled by default and should only be enabled by customers with a valid license to operate on these restricted channels. Enabling the **5.8 GHz Channels License** option for outdoor APs will allow outdoor APs to use full power in 5.8 GHz channels.

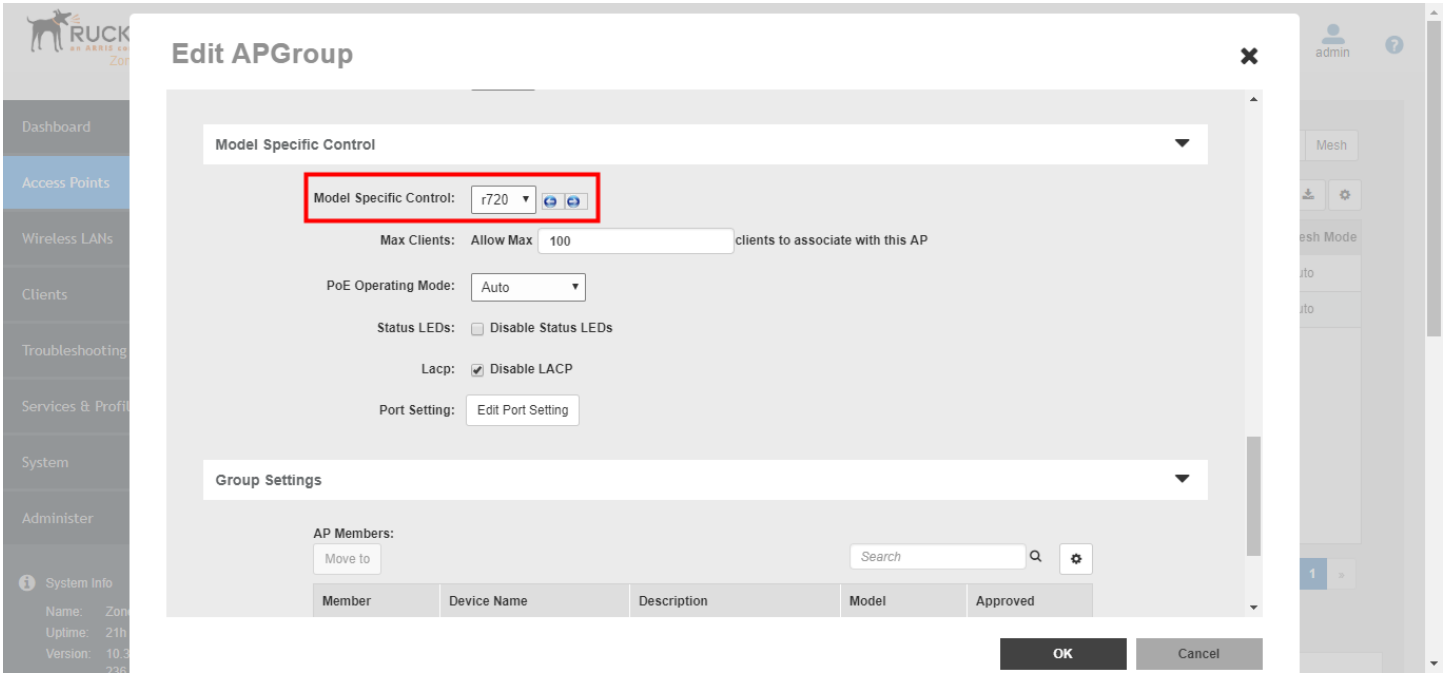
- **PoE Operating Mode**: Select PoE operating mode, Auto, 802.3at, 803.3at+, and 802.3af PoE (specific AP models only). Default is Auto. If 802.3af PoE is selected, the AP will operate in 802.3af mode (not 802.3at mode), and will consume less power than in 802.3at mode. However, when this option is selected, some AP features are disabled to reduce power consumption, such as the USB port and one of the Ethernet ports. See the *Ruckus Access Point User Guide* for model-specific information.
- **USB Port**: On APs with USB ports, you can disable the USB port for all APs of a specific model in an AP group using this setting (USB ports are enabled by default). For more information, see Configuring AP USB Ports on page 52.

- **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.
- **LACP/LAG**: Enable Link Aggregation Control Protocol (LACP) to bond two Ethernet ports together into one logical port for increased maximum Ethernet throughput (this option is only available on the following AP models: R610, R710, R720).
- **External Antenna**: On APs with external antenna options, select *Override System Default*, and *Enable* for the external antenna to be enabled. When enabled, enter a gain value in the range of 0 to 90 dBi.
- **LACP**: Link Aggregation Control Protocol (LACP) is a software feature designed to aggregate multiple physical Ethernet links together into one logical link to increase collective bandwidth. This feature allows an AP whose maximum throughput exceeds that of one of its Ethernet ports to virtually bind two ports together, allowing speeds of up to 2 Gbps over the two combined 1 Gbps ports. Beginning with 802.11ac (Wave 2), the theoretical maximum throughput of an AP has increased beyond 1 Gpbs (the speed of most AP Ethernet ports). This feature is designed to circumvent the 1 Gbps speed limit imposed by the Ethernet ports.

  NOTE
  LACP is currently supported on the following APs only: R610, R710 and R720.

- **Port Settings**: Refer to Configuring AP Ethernet Ports on page 44 for more information on configuring AP-specific Ethernet port settings.

FIGURE 16 Model Specific Controls



NOTE
The ZoneDirector web interface does not provide an option for LLDP (Link Layer Discovery Protocol). This option is currently configurable only via CLI. Please refer to the *ZoneDirector Command Line Interface Reference Guide* for more information.

Configuring AP Ethernet Ports

You can use AP groups to control Ethernet ports on all APs of a certain model. Then, if you want to override the port settings for a specific AP, you can do so as explained in the *Managing Access Points Individually* section below.

To configure Ethernet ports for all APs of the same model:

1. Go to **Access Points**
2. In **Access Point Groups**, click **Edit** for the group you want to configure.
3. Locate the **Model Specific Control** section, and select the AP model that you want to configure from the list.
4. In **Port Setting**, click **Edit Port Setting**. The screen changes 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 the check box next to **Tunnel** to tunnel all Ethernet traffic on this access port to ZoneDirector.

   By default, Ethernet traffic is bridged to the network at the AP, rather than tunneled to ZoneDirector. In some specific scenarios (such as Point of Sales and hotel room applications), tunneling Ethernet traffic to ZoneDirector may be preferable.

   NOTE
   Note that enabling port tunneling may impact wireless performance. Additionally, some features are not available for tunneled Ethernet traffic, including client fingerprinting, application visibility, SpeedFlex performance testing, etc. Therefore, Ruckus recommends against enabling port tunneling except in specific cases where it is needed.

7. Select **DHCP_Opt82** if you want to enable this option for this port (see DHCP Option 82 on page 46).
8. 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 single port APs (e.g., R310), the single LAN port must be a Trunk Port and is therefore not configurable.
   - 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 on page 47 for more information.)
9. (If Smart Mesh is not enabled), choose whether this port will serve as an 802.1X Authenticator or Supplicant, or leave 802.1X settings disabled (default). (See Using Port Based 802.1X on page 48 for more information.)

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

FIGURE 17 The Ruckus R510 has two Ethernet ports, LAN1 and LAN2

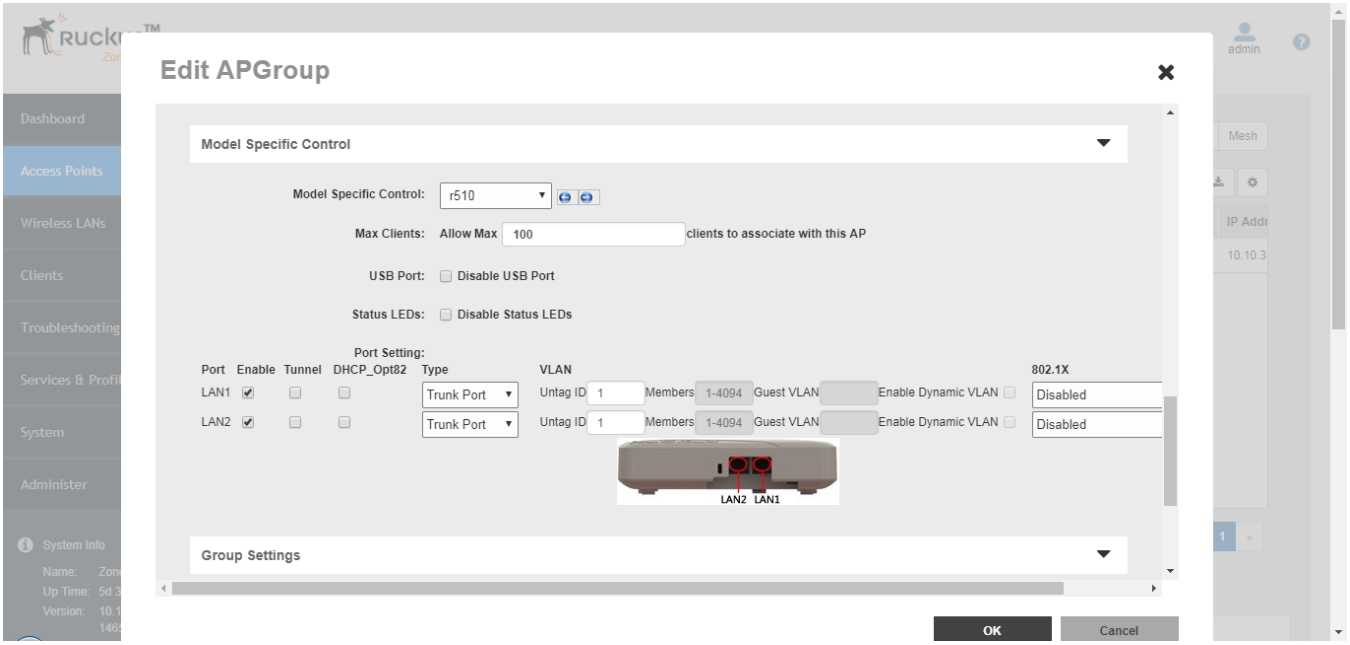
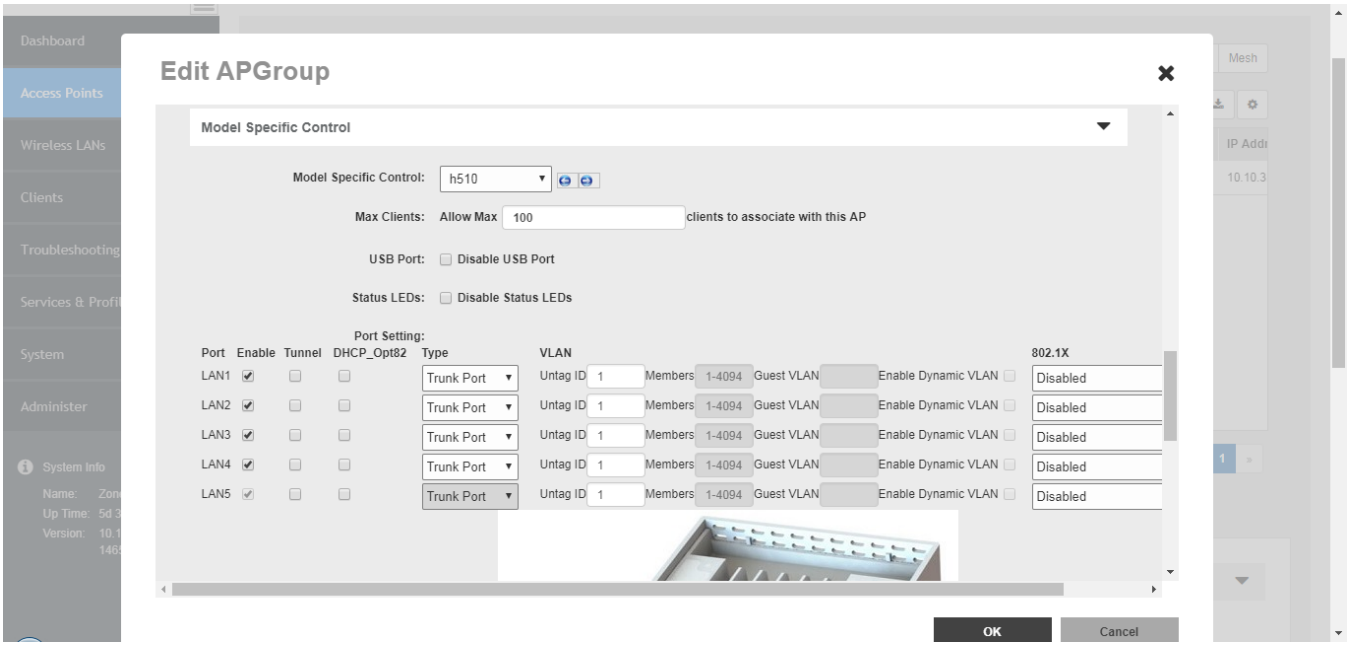


FIGURE 18 The Ruckus H510 has four front-facing Ethernet ports and one rear port



DHCP Option 82

The "DHCP Relay Agent Information Option" (Option 82) allows a DHCP Relay Agent to insert specific identification information into a request that is being forwarded to a DHCP server.

When this option is enabled for an Ethernet port or a WLAN SSID, additional information will be encapsulated in DHCP option 82 and inserted into DHCP request packets. This option supports the ability for a service provider to allocate IP addresses intelligently by considering information on the origin of the IP allocation request.

DHCP Option 82 Sub Options

Option 82 sub-options can be used to further customize the format and content of information provided in DHCP requests. ZoneDirector supports the following Option 82 sub-options:

- Sub-option 1: Agent Circuit ID
- Sub-option 2: Agent Remote ID
- Sub-option 150: DHCPv4 Virtual Subnet Selection
- Sub-option 151: DHCPv4 Virtual Subnet Selection Control
- Sub-option 1 (Circuit ID) can be customized to send only the AP's MAC address in hexadecimal format or the MAC address and ESSID. The default format is: IF-Name:VLAN-ID:ESSID:AP-Model:AP-Name:AP-MAC. Sub-option 2 (Remote ID) sends the client's MAC address by default. It can be configured to send the AP's MAC address, or the client MAC plus ESSID or AP MAC plus ESSID. Sub-option 150 can be enabled to encapsulate the VLAN ID. Sub-option 151 can be enabled to encapsulate either the ESSID or a configurable Area Name.

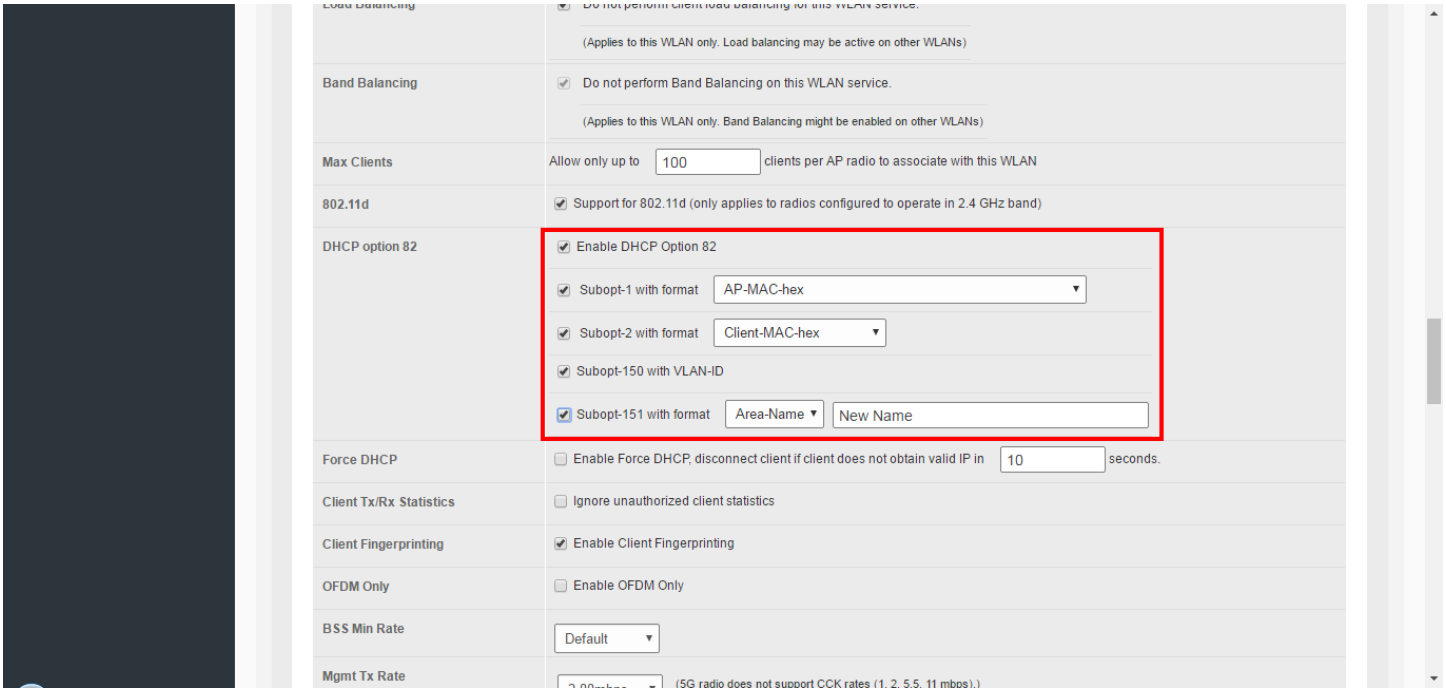
Sub-option 1 (Circuit ID) can be customized to send only the AP's MAC address in hexadecimal format or the MAC address and ESSID. The default format is: IF-Name:VLAN-ID:ESSID:AP-Model:AP-Name:AP-MAC.

Sub-option 2 (Remote ID) sends the client's MAC address by default. It can be configured to send the AP's MAC address, or the client MAC plus ESSID or AP MAC plus ESSID.

Sub-option 150 can be enabled to encapsulate the VLAN ID.

Sub-option 151 can be enabled to encapsulate either the ESSID or a configurable Area Name.

FIGURE 19 Enabling DHCP Option 82 sub-options for a WLAN



Designating Ethernet Port Type

Ethernet ports are defined as one of the following port types:

- Trunk Ports on page 48
- Access Ports on page 48
- General Ports on page 48

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 ZoneDirector web interface, as long as at least one port on each AP is designated as a Trunk Port.

> **NOTE**
> By default, all ports are enabled as Trunk Ports with Untag VLAN set as 1 (except for Wall Plate APs, such as H510, whose four front-bottom ports are enabled as Access Ports by default, and whose rear port is a Trunk Port and is non-configurable).

If configured as an Access Port, all untagged ingress traffic is sent to the configured Untag VLAN, and all egress traffic is sent untagged. If configured as a Trunk Port, all untagged ingress traffic is the configured Untag VLAN (by default, 1), and all VLAN-tagged traffic on VLANs 1-4094 will be seen when present on the network.

The default Untag VLAN for each port is VLAN 1. Change the Untag VLAN to:

- Segment all ingress traffic on this Access Port to a specific VLAN
- Redefine the Native VLAN on this Trunk Port to match your network configuration

Trunk Ports

Trunk links are required to pass VLAN information between switches. Trunking is a function that must be enabled on both sides of a link. If two switches are connected together, for example, both switch ports must be configured as trunk ports. The Trunk port is a member of all the VLANs that exist on the AP/switch and carries traffic for all VLANs between switches.

For a Trunk port, the VLAN Untag ID field is used to define the native VLAN - the VLAN into which untagged ingress packets are placed upon arrival. If your network uses a different VLAN as the native VLAN, configure the AP Trunk port's VLAN Untag ID with the native VLAN used throughout your network.

Access Ports

Access ports provide access to the network and can be configured as members of a specific VLAN, thereby separating the traffic on these ports from traffic on other VLANs.

All Access Ports are set to Untag (native) VLAN 1 by default. This means that all Access Ports belong to the native VLAN and are all part of a single broadcast domain. When untagged frames from a client arrive at an AP's Access Port, they are given an 802.1Q VLAN header with "1" as their VLAN ID before being passed onto the wired network.

When VLAN 1 traffic arrives destined for the client, the VLAN tag is removed and it is sent as plain (untagged) 802.11 traffic. When any tagged traffic other than VLAN 1 traffic arrives at the same Access Port, it is dropped rather than forwarded to the client.

To remove ports from the native VLAN and assign them to specific VLANs, select **Access Port** and enter any valid VLAN ID in the **VLAN ID** field (valid VLAN IDs are 2-4094).

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

TABLE 10 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 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.

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.

NOTE
If mesh mode is enabled on ZoneDirector, the 802.1X port settings will be unavailable for any APs that support mesh.

AP Ethernet Port as Authenticator

The Access Point is similar in many ways to a wireless switch. On APs with two or more wired ports, the AP acts as a network edge switch and can be configured to authenticate downstream wired stations (which could include multiple clients connected to another edge switch).

When the AP Ethernet port is configured as an 802.1X authenticator, it can be further defined as either Port-based or MAC-based. MAC-based authenticator mode is only supported if the port is an Access Port.

TABLE 11 Authenticator support vs. Port Type

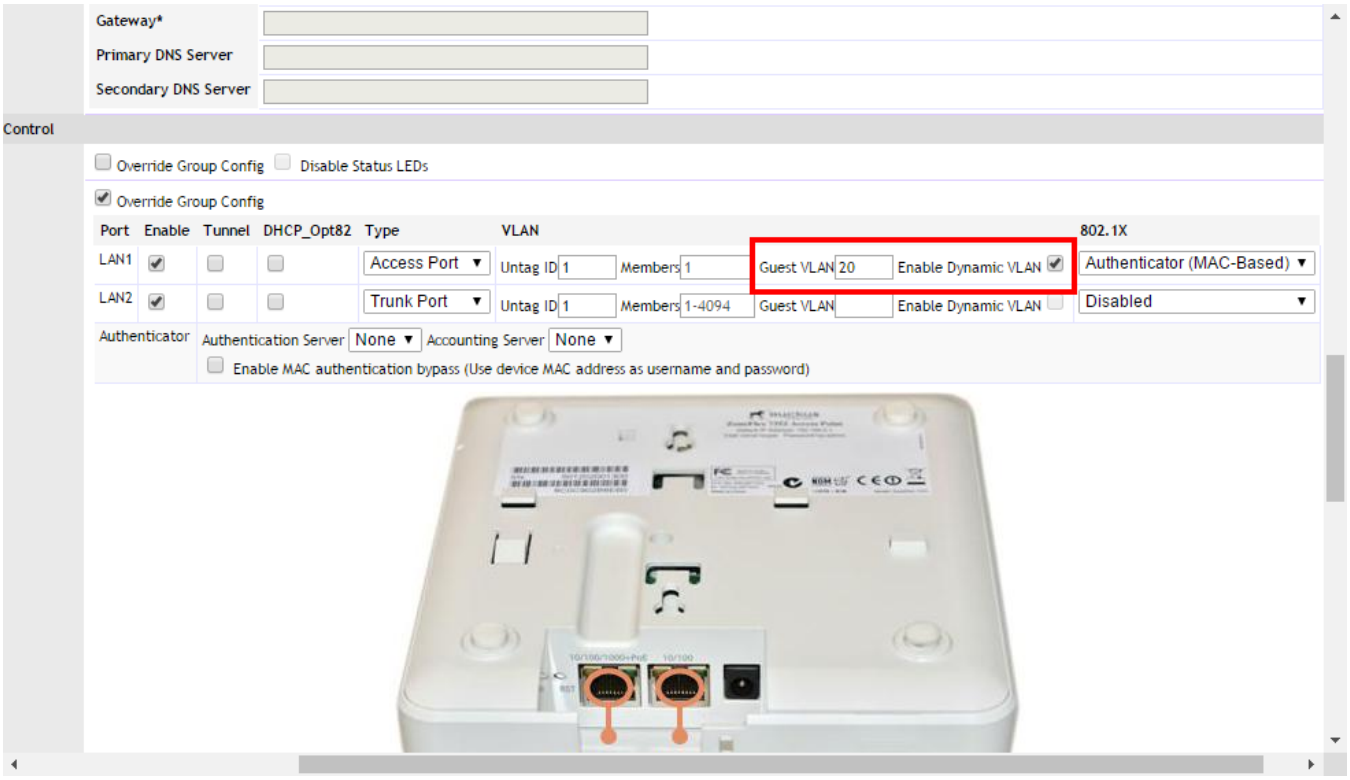
	Trunk Port	Access Port	General Port
Port-based mode	X	X	X
MAC-based mode		X	

To configure an AP Ethernet port as an 802.1X authenticator:

1. Go to **Access Points** and click the **Configure** icon for the AP whose ports you want to configure.
2. Locate the **Port Setting** section and select **Override Group Config**. The screen changes to display the AP's Ethernet ports.
3. For **Type**, select **Access Port**.
4. For **802.1X**, select **Authenticator (MAC-based)** or **Authenticator (Port-based)**.
   - In Port-based mode, only a single MAC host must be authenticated for all hosts to be granted access to the network.
   - In MAC-based mode, each MAC host is individually authenticated. Each newly-learned MAC address triggers an EAPOL request-identify frame.
     - Guest VLAN: (Default disabled). When a station fails to authenticate to this port, it will be assigned to this “guest” VLAN, with access to Internet but not to internal resources.
     - Dynamic VLAN: (Default disabled). Dynamically assign VLANs based on the policies set on the RADIUS server.
     - Authenticator: Select the RADIUS server from the list. A RADIUS server must be selected to set this port as a MAC-based authenticator.

5. Enable MAC authentication bypass: Enable this option to allow AAA server queries using the MAC address as both the user name and password. If MAC authentication is unsuccessful, the normal 802.1X authentication exchange is attempted.

FIGURE 20 Enabling Guest VLAN and Dynamic VLAN on a MAC-based 802.1X Authenticator port



AP Ethernet Port as Supplicant

You can also configure a port to act as a supplicant and force it to authenticate itself to an upstream authenticator port. Until the AP has successfully done so, the state of the authenticator port is closed and packets from the AP or stations behind it will be dropped at the authenticator port.

In this configuration, it is expected that the connected authenticator port is configured with the following characteristics:

- As a Trunk Port to pass all VLAN packets, and
- In port-based authentication mode

Each AP is allowed to configure a maximum of one Ethernet port as an 802.1X supplicant, and the supplicant port must be a Trunk Port.

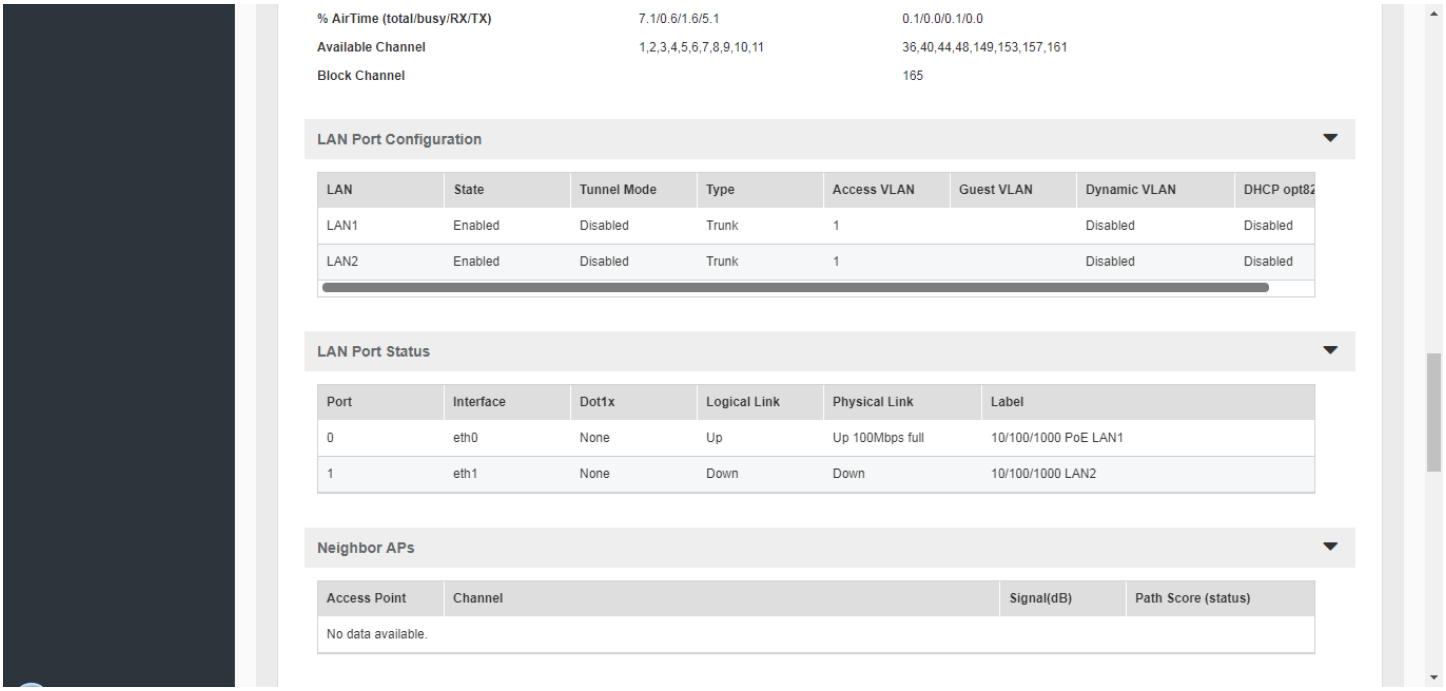
FIGURE 21 Configuring an AP Ethernet port as an 802.1X Supplicant



Viewing AP Ethernet Port Status

You can view the status of an AP's port configuration by going to *Access Points*, selecting the AP you want to monitor, and scrolling down to the *LAN Port Configuration* and *LAN Port Status* sections.

FIGURE 22 Viewing an AP's Ethernet port configuration



Configuring AP USB Ports

Some Ruckus APs support customer-supplied, low power (1W or less), USB devices for Internet of Things (IoT) applications such as Bluetooth Low Energy (BLE) beacons, Zigbee, Z-Wave, etc.

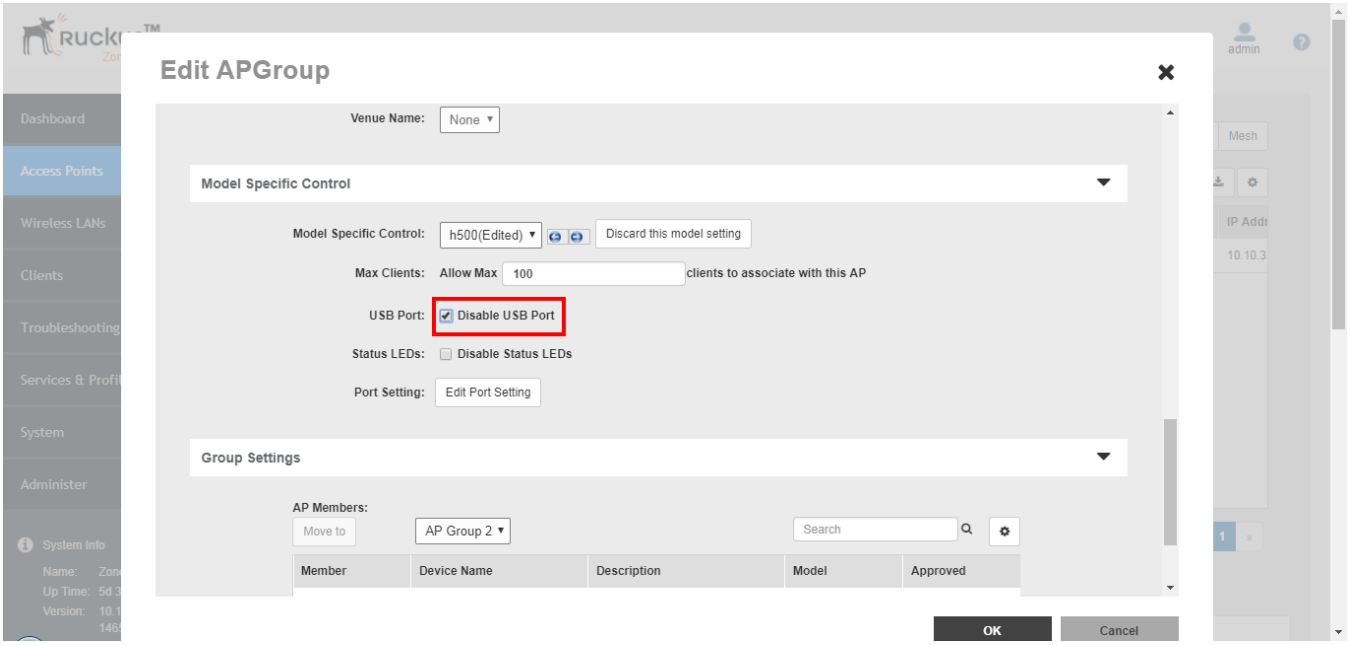
The IoT devices plug into a USB port on the AP, and the AP can be configured to turn power to the USB port either on or off. These USB devices then perform whatever tasks they are designed to do without interference from or control (other than supplying USB power) by the Ruckus equipment.

USB ports are enabled by default. To disable the USB ports for all APs of a specific model in an AP group:

1. Go to **Access Points**.
2. In **Access Point Groups**, click **Edit** for the group you want to configure.
3. Locate the **Model Specific Control** section, and select the AP model that you want to configure from the list.
4. In **USB Port**, select **Disable USB Port**.

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

FIGURE 23 Disabling AP USB ports



Configuring Global Access Point Policies

The Access Point Policies options allow you to define how new APs are detected and approved for use in WLAN coverage, as well as policies on ZoneDirector discovery and communicating with ZoneDirector.

These policies are enforced on all APs managed by ZoneDirector unless a specific WLAN setting overrides them. For example, if you want to enable Load Balancing for most APs but disable it on specific WLANs, you would enable it in the **Access Point Policies** section, then disable it for the particular WLAN from the **Wireless LANs** page.

To review and revise the general AP policies, follow these steps:

1. Go to **System** > **AP General Settings**.

2. Review the current settings in **Access Point Policies**. You can change the following settings:
   - **Approval**: This 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 this check box.
   - **Limited ZoneDirector Discovery**: If you have multiple ZoneDirectors on the network and want specific APs to join specific ZoneDirectors, you can limit ZoneDirector discovery. To do this, select the **Limited ZD Discovery** check box, and then enter the IP addresses (or FQDN) of the primary and secondary ZoneDirector units to which you want APs to join. When **Limited ZD Discovery** is enabled, APs will first attempt to join the primary ZoneDirector. If they cannot find or are unable to join the primary ZoneDirector, they will attempt to join the secondary ZoneDirector. 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 ZoneDirector.

     NOTE
     If you have two ZoneDirectors of the same model, Ruckus recommends using the Smart Redundancy feature. If you have two ZoneDirectors of different models, you can use Limited ZD Discovery to provide limited redundancy; however, this method does not provide synchronization of the user database. For information on Smart Redundancy configuration, see Enabling Smart Redundancy on page 296. For information on N+1 redundancy using Limited ZD Discovery, see Using Limited ZD Discovery for N+1 Redundancy on page 55.

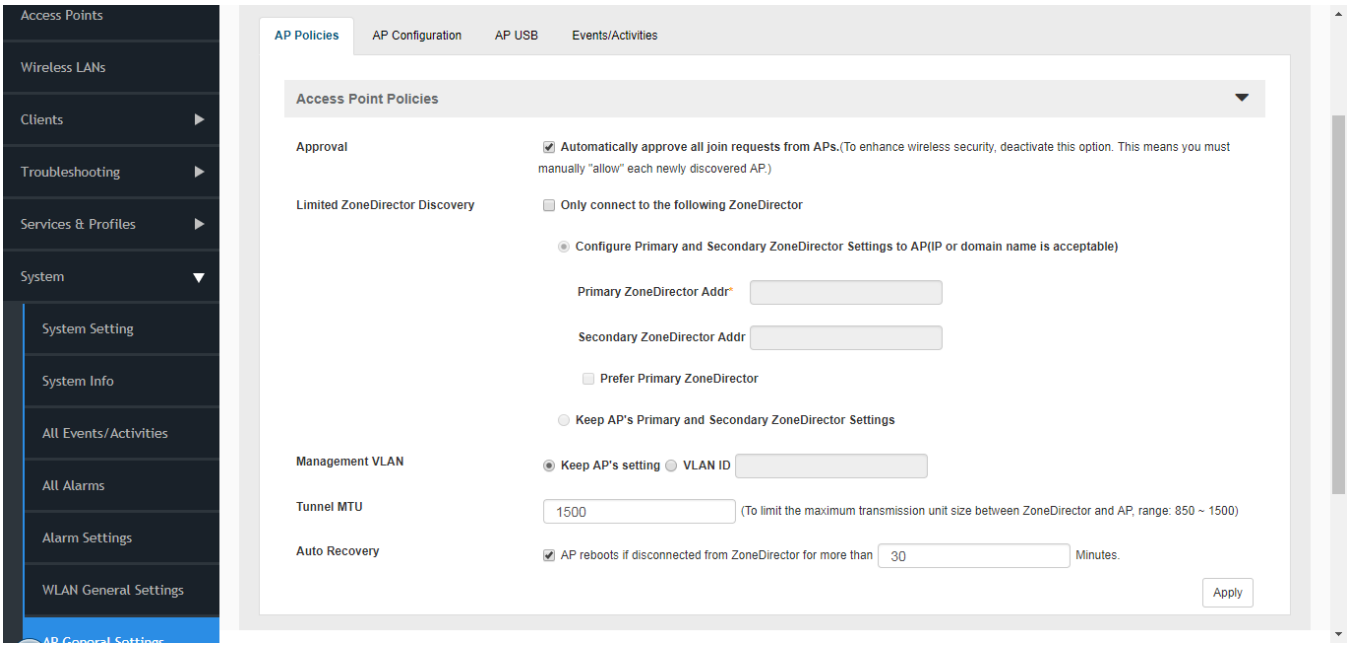
   - – **Prefer Primary ZD**: Enable this option if you want APs to revert to the primary ZoneDirector's control after connection to the primary controller is restored.
     – **Keep AP's Primary and Secondary ZD Settings**: Enable this option if you want the AP's existing settings to take precedence (not be overwritten by secondary controller's settings after failover to secondary ZD).
   - **Management VLAN**: You can enable the ZoneDirector management VLAN if you want to separate management traffic from regular network traffic. The following options are available:
     – **Keep AP's setting**: Click this option if you want to preserve the Management VLAN settings as configured on the AP. Note that Management VLAN on the AP is disabled by default.
     – **VLAN ID**: Enter a valid VLAN ID to segment management traffic into the VLAN specified. Valid VLAN IDs are 1-4094.

       NOTE
       If you change the Management VLAN ID here, you also need to set the Management VLAN ID that ZoneDirector needs to use on the *System > System Settings* page. Otherwise, ZoneDirector and the APs will be unable to communicate via the Management VLAN.

   - **Load Balancing**: Balances the number of clients across adjacent APs (see Load Balancing on page 269).
   - **Tunnel MTU**: Use this field to set the Maximum Transmission Unit for tunnel packets between ZoneDirector and APs. The MTU is the size of the largest protocol data unit (in bytes) that can be passed. Supported MTU values range from 850 to 1500 (default is 1500). Note that changing this setting to a value less than 1280 will affect IPv6 connectivity.
   - **Auto Recovery**: Set an AP auto recovery time in minutes, after which APs will reboot in attempt to reconnect to ZoneDirector. Default is 30 minutes.

3. Click **Apply** to save and apply your settings.

FIGURE 24 Setting global AP policies



Using Limited ZD Discovery for N+1 Redundancy

ZoneDirector's Smart Redundancy feature can only be used with two ZoneDirectors of the same model. If you want to deploy one ZoneDirector as a backup controller for multiple primary controllers, you can use Limited ZD Discovery to achieve limited N+1 redundancy.

NOTE
Using Limited ZD Discovery for redundancy purposes does not synchronize the user database, guest database or DPSKs.

To deploy multiple ZoneDirectors in a limited redundancy configuration:

1. On each primary ZoneDirector, go to **Access Points** > **Access Point Policies** and locate the *Limited ZD Discovery* section.
2. Activate the check box next to **Only connect to the following ZoneDirector**.
3. Enter the IP address of the primary ZoneDirector (the one you are currently configuring) in **Primary ZoneDirector Addr**.
4. Enter the IP address of the backup ZoneDirector in **Secondary ZoneDirector Addr**.
5. (Optional) Enable the check box next to **Prefer Primary ZD**. This ensures that the AP will revert to its primary controller after connection to the primary has been restored.
6. Click **Apply** to save your changes.
7. Once all the APs, WLANs, WLAN groups and AP groups have been deployed on the primary ZoneDirector(s), back up the AP configurations for each primary controller, by going to Administer > Backup and clicking the Backup button under Back Up Configuration.

8. **NOTE**
   You should also configure the same exact settings for WLANs, WLAN groups, AP Groups, Mesh settings and AAA servers on the backup controller prior to importing AP lists. If you do, the APs will be automatically mapped to their respective settings on the backup controller. If you do not configure these settings first before importing AP lists, you will need to configure them for each AP after importing. For example, you will need to manually move APs into their respective AP groups from the System Default group if you did not create the AP groups prior to importing

   Log into the secondary/backup ZoneDirector, and go to **Configure** > **Access Points**
9. Import the AP lists that you backed up from the primary ZoneDirectors by selecting Import this backup file and additional backup file(s) and clicking Import.
10. Repeat until all backup files have been imported.
11. Go to **Access Points** > **Access Point Policies**, and enable the check box next to **Keep AP's Primary and Secondary ZD Settings**. This ensures that the APs' primary/secondary ZD settings will not be overwritten by the secondary ZoneDirector's configuration after failover to the secondary controller.
12. Click **Apply** to save your changes.
13. Reboot the backup/secondary ZoneDirector for all changes to take effect (**Administer** > **Restart** > **Restart**.)

The imported APs will be placed into AP Groups according to the settings that were backed up from the primary controller. If the original AP Group or WLAN Group name does not exist on the destination controller, the AP will be placed in the System Default AP Group/WLAN Group. Additionally, you must make sure that the maximum number of APs is not exceeded.

TABLE 12 Max APs per Controller

Model	Max APs per controller
ZoneDirector 1200	150

Importing a USB Software Package

Ruckus Access Points with USB ports ("SmartPoint" APs) can be configured to support a range of 3G, 4G/LTE, and WiMAX wireless USB devices for non-Wi-Fi wireless connection to a service provider's network.

The ZoneDirector web interface allows administrators to provision SmartPoint APs with the USB device configuration files directly through ZoneDirector, providing a simple and straightforward provisioning process with minimal human intervention required.

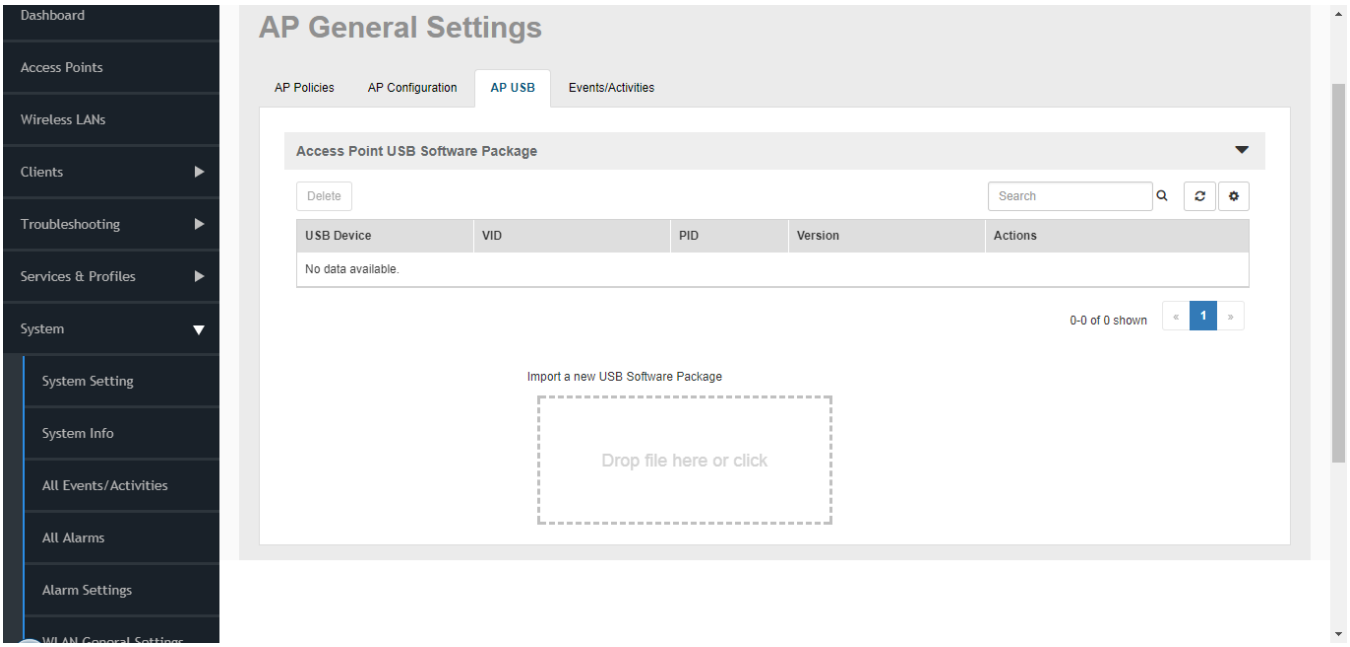
Provisioning requires that the SmartPoint Access Points must be connected to the ZoneDirector acting as the provisioning server over the wired network. After an AP is provisioned, an automatic 3G/4G/LTE/WiMAX network connection is made to connect the AP to the Internet, then to ZoneDirector, enabling the creation of an LWAPP tunnel and providing 802.11 wireless services.

To upload a USB provisioning file to ZoneDirector:

1. Go to **System > AP General Settings > AP USB**.
2. Drag a USB software package file into the import box.

3. Click **OK** to upload the file to ZoneDirector

FIGURE 25 Importing a USB software package



To provision a SmartPoint Access Point with USB software:

1. Plug the 3G/4G/LTE/WiMAX USB modem into the SmartPoint AP's USB port.
2. Connect the SmartPoint AP to ZoneDirector via wired L2 or L3 network.
3. Once an LWAPP tunnel between the AP and ZoneDirector has been established, ZoneDirector automatically pushes the corresponding USB drivers, network connection scripts and configuration files to the AP.
4. The AP saves the files to its persistent storage.
5. Disconnect the wired network connection, then reboot the AP.
6. After reboot, the AP detects the appropriate drivers on its persistent storage, goes through the 3G/4G/LTE network connection process and establishes an LWAPP tunnel with ZoneDirector.
7. ZoneDirector pushes the 802.11 wireless configuration to the AP.
8. The AP implements the 802.11 wireless configuration and is ready to provide 802.11 wireless services.
9. A wireless client connects to the AP's 802.11 wireless service, and the data traffic is tunneled to ZoneDirector through the LWAPP tunnel.

Managing Access Points Individually

You can add a description, or change the channel selection, transmit power and Ethernet port settings of a managed access point by editing the AP's parameters. Additionally, you can manually assign an IP address or disable WLAN service entirely for a specific radio.

Configuring any of these settings for an individual AP overrides the settings configured in AP Groups.

To edit the parameters of an access point:

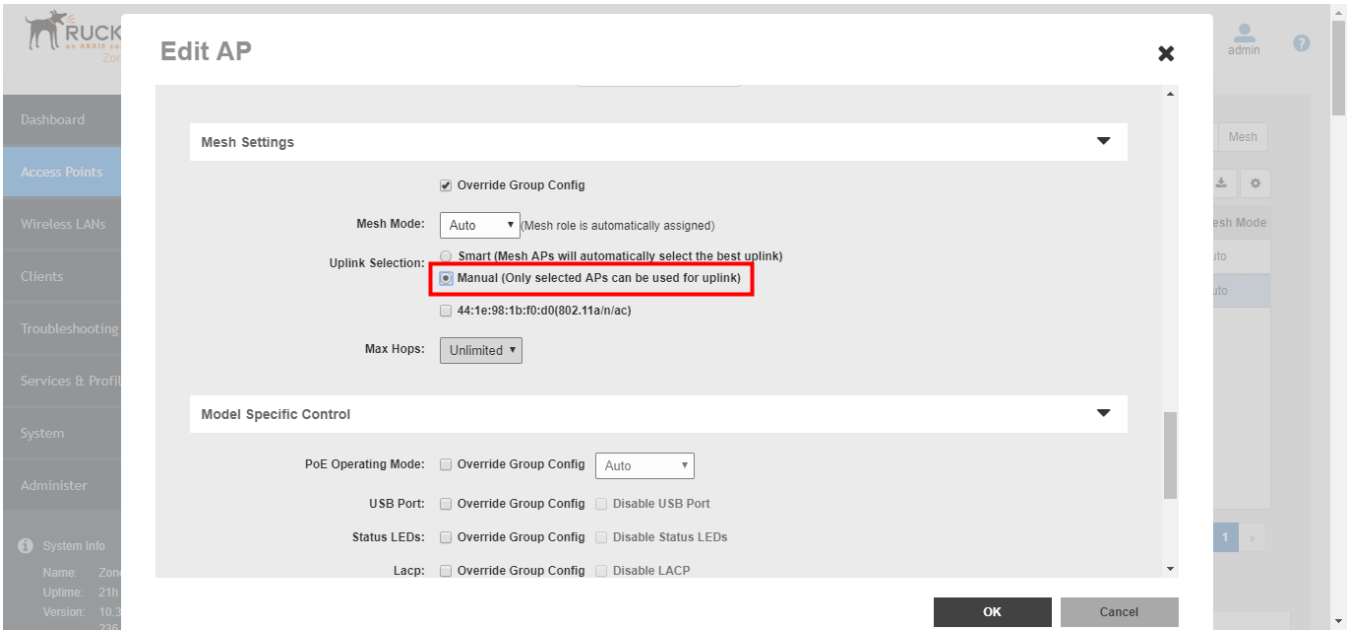
1. Go to **Access Points**.
2. Select the AP you want to edit from the **Access Points** table, and then click the **Configure** button.
3. In the **Edit AP** form, edit any of the following *General* settings:
   - **Device Name**: Enter a descriptive name for the AP for easy identification in ZoneDirector tables and Dashboard widgets. Names can consist of up to 64 letters, numbers, hyphens and underscores. Note however that only the first 17 characters of the device name will be displayed in the Events/Activities tables.
   - **Description**: Enter a description for the AP. This description is used to identify the AP in the Map View.
   - **Location**: Enter a recognizable location for the AP.
   - **GPS Coordinates**: Enter GPS coordinates for AP location on the Google/Bing Maps on the Dashboard.
   - **Group**: Select an AP group from the list if you want to place this AP into a group other than the system default group.
   - **Bonjour Gateway**: Designate this AP as a AP-side Bonjour Gateway. See Creating a Bonjour Gateway Rule AP Site on page 283.
   - **Bonjour Fencing**: Implement on Bonjour Fencing Policy on this AP. See Bonjour Fencing on page 286.
4. In *Channel Range Settings*, you can manually configure available channels. Click **Override Group Config** and change the default values, the following parameters can be configured independently for each AP radio:
   - **Channel Range Settings**: Deselect any channels that you do not want the AP to use in channel selection.
5. In **Radio B/G/N/AX (2.4 GHz)**, and **Radio A/N/AC/AX (5 GHz)**, override the AP group configuration and configure the following settings:
   - **Channelization**: Sets the channel width of each channel in the spectrum used during transmission.
   - **Channel**: Manually set the channel used by the AP radio.
   - **Tx Power**: Manually set the maximum transmit power level relative to the calibrated power.

     Max = max allowable Tx power according to country regulations

     Min = 0dBm per chain for 11n APs, 2dBm per chain for 11ac APs
   - **WLAN Group**: Specify a WLAN group for this radio.
   - **Call Admission Control**: (Disabled by default). Enable Wi-Fi Multimedia Admission Control (WMM-AC) to support Polycom/ Spectralink VIEW certification. See Advanced WLAN Options on page 72 under *Creating a WLAN* for more information.
   - **WLAN Service**: Uncheck this check box to disable WLAN service entirely for this radio. (This option can be useful if you want dual-band 802.11n/ac APs to provide service only on the 5 GHz radio, in order to reduce interference on the 2.4 GHz band, for example.) You can also disable service for a particular WLAN at specific times of day or days of the week, by setting the Service Schedule. For more information, see Advanced WLAN Options on page 72 for creating a WLAN.
   - **External Antenna**: On APs with external antenna options, select **Override System Default**, and Enable for the external antenna to be enabled. Once enabled, enter a gain value in the range of 0 to 90dBi.
   - **Protection Mode**: (2.4 GHz radio only) Configure advanced RF settings as follows:
     - **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.

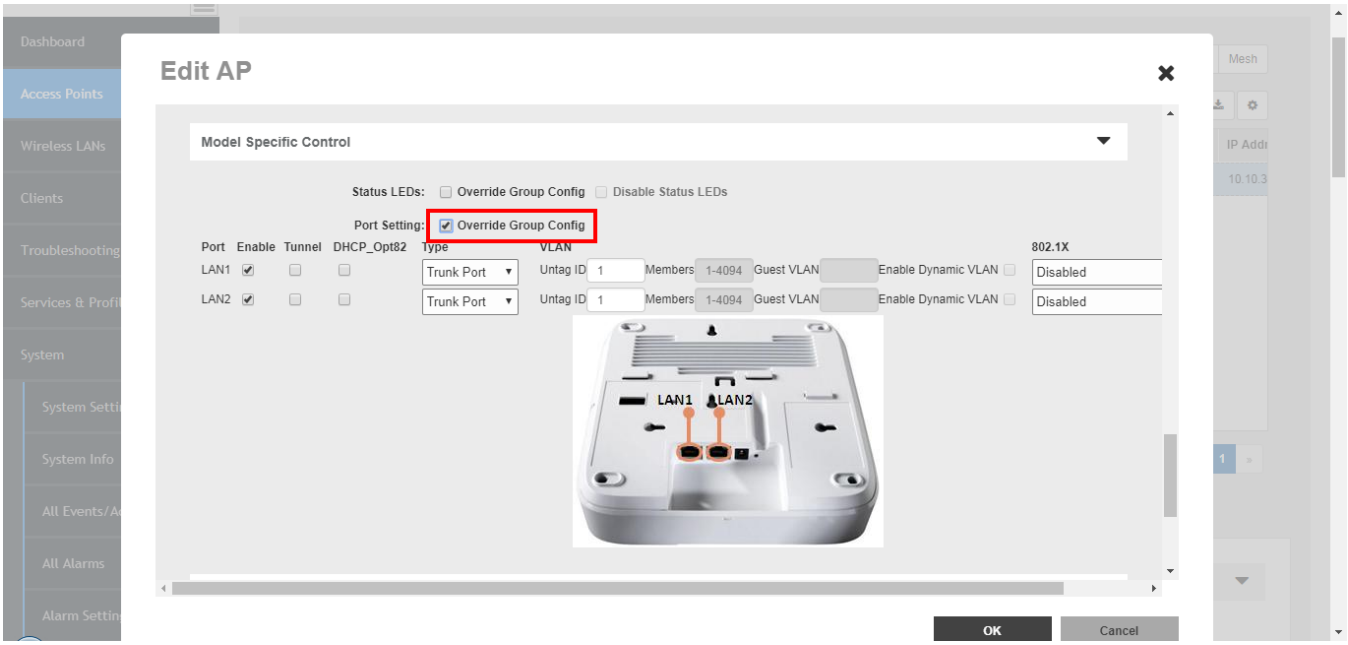
6. The **Network Setting** options allow you to configure the IP address settings of the AP:
   - **IP Mode**: Select IPv4 only, IPv6 only or dual IPv4/IPv6 addressing mode. If you want the AP to keep its current IP address, click **Keep AP's Setting**. If the AP's IP address has not been set, it will automatically attempt to obtain an IP address via DHCP.
   - If you want the AP to automatically obtain its IP address settings from a DHCP server on the network, click the **DHCP** option in Management IP. You do not need to configure the other settings (netmask, gateway, and DNS servers).
   - If you want to assign a static IP address to the AP, click the **Manual** option next to *Device IP Settings*, and then set the values for the following options:
     - IP Address
     - Netmask
     - Gateway
     - Primary DNS Server
     - Secondary DNS Server
7. If Smart Mesh is enabled (see Deploying a Smart Mesh Network on page 383), the **Mesh Settings** section lets you define the role this AP should play in the mesh network--Auto, Root AP, Mesh AP, or Disable (default is Auto). In most cases, Ruckus recommends leaving this setting on **Auto** to reduce the risk of isolating a Mesh AP. Select **Disable** if you do not want this AP to be part of your mesh network.
8. If this AP is a Mesh AP and you want to manually set which APs can serve as its uplinks, select the **Manual** radio button under **Advanced Options > Uplink Selection** (default is Smart). The other APs in the mesh appear below the selection.
9. Select the check box next to each AP that you want to allow the current AP to use as an uplink. If you set Uplink Selection for an AP to Manual and the uplink AP that you selected is off or unavailable, the AP status on the **Access Points** page will appear as *Isolated Mesh AP*. See Troubleshooting Isolated Mesh APs on page 401 for more information.

FIGURE 26 Manual uplink selection for APs in a mesh



10. In **Model Specific Control**, override the AP group configuration and configure the following options for this AP (for information on these settings, see *Working with Access Point Groups*:
    - **PoE Operating Mode**: Choose Auto (default), 802.3af, 802.3at, or 802.3at+ PoE operating mode.
    - **USB Port**: Disable the USB port on this AP.
    - **Status LEDs**: Disable the status LEDs on this AP.
    - **LACP/LAG**: Enable Link Aggregation Control Protocol (LACP) on this AP.
    - **Port Setting**: Configure AP Ethernet port settings. See the following step.
11. If you select **Override Group Config** in the **Port Setting** section, a new section opens where you can customize the Ethernet port behavior for this AP. Enabling this will override the AP Group settings made on Configuring AP Ethernet Ports on page 44.

    FIGURE 27 Ethernet port configuration - Override Group Config



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

Configuring Hotspot 2.0 Venue Settings for an AP

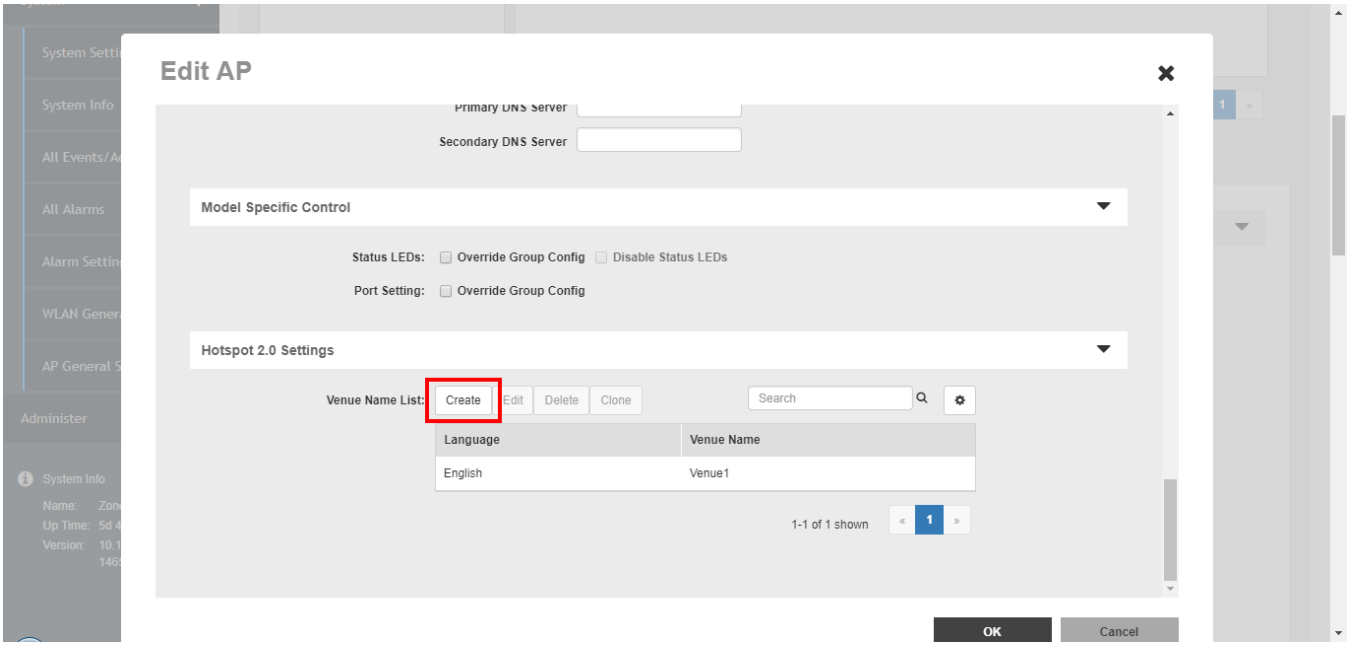
If this Access Point will be serving a Hotspot 2.0 hotspot, you can set the Venue Name for the venue at which the AP will be operating. You can create up to two Venue Names (two languages for the venue name).

To set the Hotspot 2.0 Venue Name for an AP:

1. Go to **Access Points**.
2. Select the AP you want to configure, and click the **Configure** button.
3. Scroll down to the bottom and locate the**Hotspot 2.0 Settings** section.
4. In **Venue Name List**, click **Create**to create a new venue name for this AP. Select the language and enter the venue name in that language.

5. Click **Save** to save the entry, and click **OK** to save the Venue Name settings for the AP.

FIGURE 28 Setting the Venue Name for a Hotspot 2.0 service AP



Optimizing Access Point Performance

The ZoneDirector web interface allows you to remotely monitor and adjust key hardware settings on each of your network APs.

After assessing AP performance in the context of your specific network's performance, you can reset channels and adjust transmission power, or adjust the priority of certain WLANs over others, as needed.

Assessing Current Performance Using the Access Point Table

1. Go to **Access Points**.
2. When the **Access Points** page appears, review the table for specific AP settings, especially the **Channel** and **Clients** columns.
3. Click on the MAC address of any AP to view detailed information about the AP such as associated clients, channel, signal strength, neighbor APs and warnings/events associated with the AP.
4. If you want to make changes to individual AP settings, proceed to the next task, Adjusting AP Settings on page 61.

Adjusting AP Settings

1. Go to **Access Points**.
2. Review the **Access Points** table and identify an AP that you want to adjust.
3. Click the **Edit** button in that AP row.

4. Review and adjust any of the following Editing (AP) options.

   NOTE
   Some options are read-only depending on the approval status.

   - **Channelization**: Choose 20/40/80MHz or Auto channel width.
   - **Tx Power**: Choose the amount of power allocated to this channel. The default setting is "Auto" and your options range from "Full" to "Min."
   - **Mesh Mode**: Use this setting to manually configure this AP's Mesh role (Root AP, Mesh AP, or Disable). Default is Auto.
   - **Uplink Selection**: Use this setting to manually define which APs can serve as an uplink for this Mesh AP.

5. Click **OK**. The adjusted AP will be automatically restarted, and when it is active, will be ready for network connections.

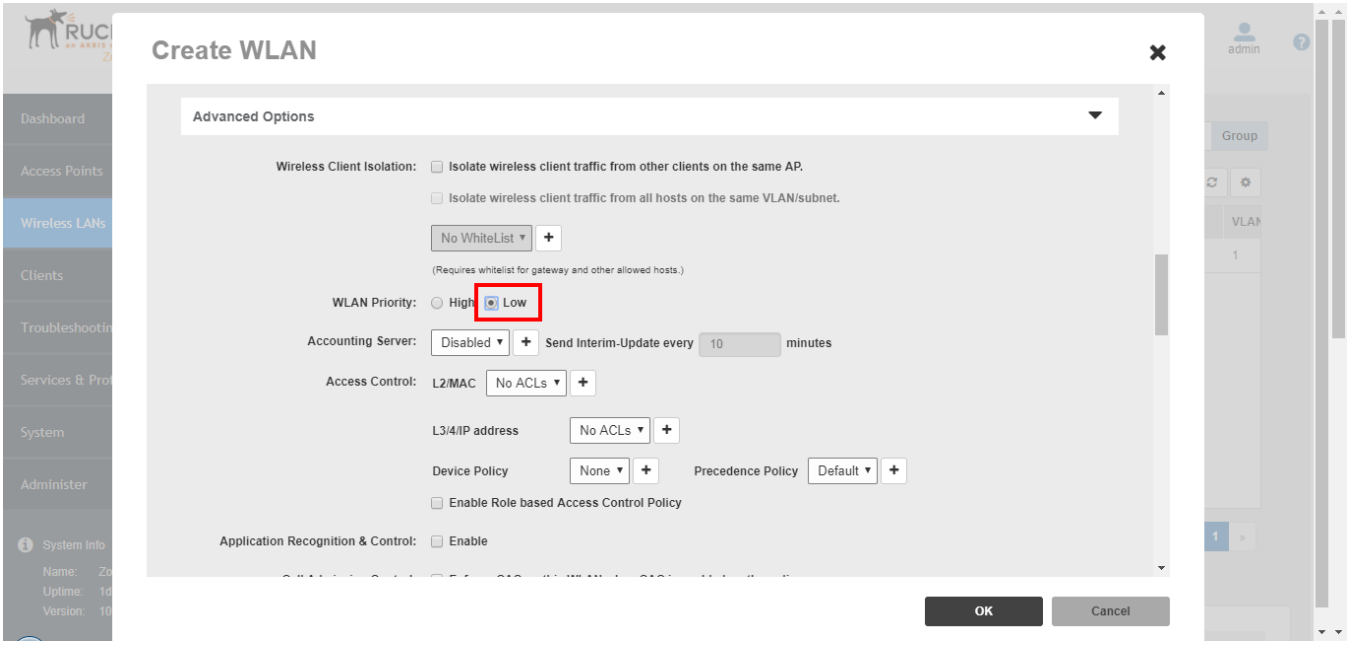
Prioritizing WLAN Traffic

If you want to prioritize internal traffic over guest WLAN traffic, for example, you can set the WLAN priority in the WLAN configuration settings to "high" or "low." By default all WLANs are set to high priority.

To set a specific WLAN to lower priority:

1. Go to **Wireless LANs**.
2. Select the WLAN you want to configure with a lower priority, and click the **Edit** button.
3. Expand the **Advanced Options** section.
4. Click **OK** to save your changes.

FIGURE 29 Set WLAN priority Low



Managing a Wireless Local Area Network

- Overview of Wireless Networks..... 63
- About RUCKUS WLAN Security..... 64
- Creating a Wireless LAN..... 65
- Creating a Copy of an Existing WLAN for Workgroup Use..... 79
- Customizing WLAN Security..... 80
- Working with WLAN Groups..... 83
- Deploying ZoneDirector WLANs in a VLAN Environment..... 86

Overview of Wireless Networks

Once you have completed the ZoneDirector Setup Wizard, you have a fully functional wireless network based on one or two secure WLANs (if you enabled the optional guest WLAN), providing wireless access for authorized internal users and guests.

By default, the internal WLAN provides Zero-IT activation to allow users to automatically self-provision their client devices with WLAN settings the first time they connect. Once authenticated, they are able to access any available wired or wireless resources on the network that the admin allows.

The guest WLAN provides visitors to your organization with a connection to the Internet, but not to your internal corporate network (by default).

The following are just a few examples of situations in which you may want to create additional WLANs to supplement the internal and guest WLANs that you created during the Setup Wizard:

- To limit certain WLANs to groups of qualified users, to enhance security and efficiency (for example, an "Engineering" WLAN with a closed roster of users).
- To configure a specific WLAN with different security settings. For example, you may need a WLAN that utilizes WEP encryption to support legacy wireless devices are only capable of WEP-key encryption.
- To create special WLANs with different advanced settings for specific purposes. For example, a "VoIP WLAN" for voice traffic, with Tunnel Mode enabled and Background Scanning and Load Balancing disabled, or a "Student WLAN" that is only available during school hours.

In the first scenario, you can clone the existing internal WLAN to create additional WLANs for specific groups of users, and then configure authentication settings to allow only users belonging to specified user groups.

In the second scenario, you can create a new WLAN with different security settings for those specific devices.

In the third scenario, you can customize the WLAN advanced settings to disable WLAN service during certain time periods, fine-tune advanced RF features and enable Tunnel Mode to tunnel all traffic to ZoneDirector for VoIP WLANs.

As a result, you will have the default internal WLAN for authorized internal users, a guest WLAN for visitors, and any needed WLANs that fulfill different wireless security or user segmentation requirements.

The maximum number of WLANs configurable per ZoneDirector controller is as follows:

TABLE 13 Max WLANs by ZoneDirector model

Model	Max WLANs
ZoneDirector 1200	512

NOTE
RUCKUS 802.11n APs support a maximum of 27 service WLANs per AP radio. Each AP radio actually supports up to 32 SSIDs, but five are reserved (two are reserved for mesh SSIDs, and one each for monitor, recovery and scan).

NOTE
RUCKUS 802.11ac APs (both Wave 1 and Wave 2) support up to 27 service WLANs on the 2.4 GHz radio, and 13 service WLANs on the 5 GHz radio.

NOTE
Deploying a large number of WLANs on a single AP will have a significant performance impact. RUCKUS recommends deploying no more than eight WLANs per AP radio.

About RUCKUS WLAN Security

One of the first things you should decide for each WLAN you create is which methods of authentication and encryption to use, for both internal users and guests.

Authentication options include:

- Open
- 802.1X EAP
- MAC Address
- 802.1X EAP + MAC Address

Encryption options depend on which type of authentication is chosen. "Open" authentication allows the use of WPA2, WPA3, WEP, OWE or no encryption.

Open authentication + WPA2 encryption (also known as WPA2-Personal, or WPA2-PSK, for "Pre-Shared Key") 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.

The new WPA3 encryption method provides several security enhancements over WPA2.

The 802.1X EAP authentication method (also known as WPA2-Enterprise, or WPA3-Enterprise) provides effective authentication regardless of the encryption method, and requires a back-end (RADIUS) authentication server. 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, provide visibility and control over devices on the network.

You can also choose to authenticate clients by MAC address. MAC authentication requires a RADIUS server and uses the MAC address as the user login name and password.

The 802.1X EAP + MAC Address authentication option allows clients to authenticate to the same WLAN using either MAC address or 802.1X authentication. (However, this requires that the supplicant support this feature, which no public domain supplicants currently do.)

All client authentication options (Open, 802.1X, MAC, and 802.1X+MAC) are detailed in Creating a Wireless LAN on page 65, and you can learn how to apply them to your WLANs in the same section.

Encryption options include:

- WPA2
- WPA3
- WPA2/WPA3-Mixed
- OWE
- WPA-Mixed
- WEP-64
- WEP-128
- None

See Encryption Options on page 69 for information on WLAN encryption options.

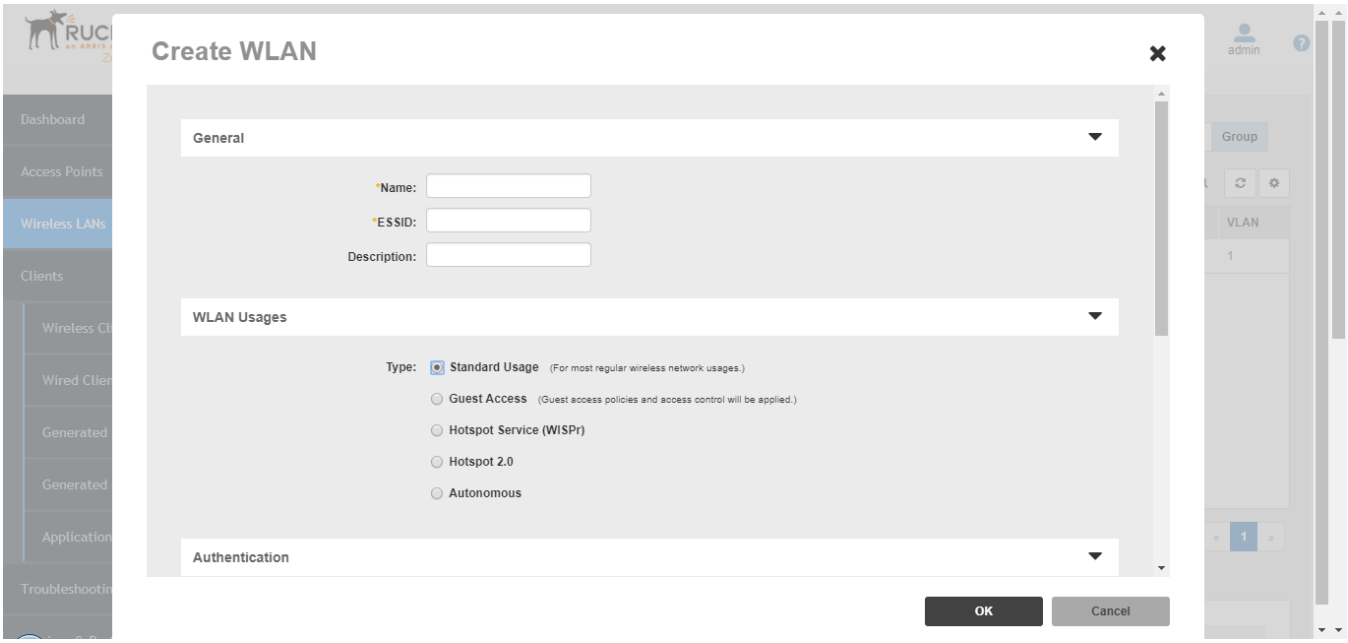
Creating a Wireless LAN

You can create new WLANs to provide additional wireless services, in addition to those created during the Setup Wizard.

To create a new WLAN:

1. Go to **Wireless LANs**. The first table displays all WLANs that have already been created in ZoneDirector.
2. In the top section (WLANs), click **Create**. The **Create WLAN** workspace appears.

FIGURE 30 Creating a new WLAN



3. Configure any of the general or advanced WLAN settings listed below.

The **Create WLAN** workspace includes the following configuration options used to customize your new WLAN.

The individual options are explained in detail in the following sections, beginning with General Options on page 66.

TABLE 14 Create new WLAN options

Option	Description
General Options	Enter WLAN name and description.
WLAN Usages	Select usage type (Standard Usage, Guest Access, Hotspot (WISPr), Hotspot 2.0, Autonomous).
Authentication Options	Select an authentication method for this WLAN (Open, 802.1X EAP, MAC address, 802.1X EAP + MAC Address).
Encryption Options	Select encryption method (WPA2, WPA3, WPA2/WPA3-Mixed, OWE, WPA-Mixed, WEP, or None), encryption algorithm (AES, Auto AES+TKIP, AES-GCMP-256).
Password	Enter a WPA passphrase (WPA2 or WPA-Mixed), SAE passphrase (WPA3), both PSK and SAE passphrase (WPA2/WPA3-Mixed), or WEP key (WEP-64 or WEP-128). If the encryption method is **OWE** or **None**, no password is required.

TABLE 14 Create new WLAN options (continued)

Option	Description
Options	Select whether web-based authentication (captive portal) will be used, and which type of authentication server will be used to host credentials (local database, Active Directory, RADIUS, LDAP). Also, enable or disable Wireless Client Isolation, Zero-IT Activation, Dynamic PSK and Priority for this WLAN.
Advanced Options	Select accounting server, ACLs, rate limiting, VLAN/dynamic VLAN settings, tunneling, Background Scanning, maximum client threshold and service schedule.

4. When you finish, click **OK** to save the entries. This WLAN is ready for use.
5. You can now select from these WLANs when assigning roles to users, as detailed in Creating New User Roles on page 116.

General Options

- **Name/ESSID**: Type a short name for this WLAN. The SSID must contain between 1 and 32 characters. Allowable characters include printable ASCII characters from space (char 32) to ~ (char 126). A space can be used in the name, but the name cannot begin or end with a space character. If a space is included at the beginning or end of the ESSID, it will be automatically removed. If a disallowed ASCII character (not within the range 32-126) is included, an error message will appear.
  - In general, the WLAN name is the same as the advertised SSID (the name of the wireless network as displayed in the client's wireless configuration program). However, you can also separate the ESSID from the WLAN name by entering a name for the WLAN in the first field, and a broadcast SSID in the second field. In this way, you can advertise the same SSID in multiple locations (controlled by the same ZoneDirector) while still being able to manage the different WLANs independently. Each WLAN "name" must be unique within ZoneDirector, while the broadcast SSID can be the same for multiple WLANs.
- **Description**: Enter a brief description of the qualifications/purpose for this WLAN, e.g., "Engineering" or "Voice."

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**: Select a default "Guest Access" WLAN with open authentication and customizable encryption (see Configuring Guest Access on page 125). Guest WLANs are subject to guest access policies, such as redirection, client isolation and subnet access restrictions. Guest Access WLANs can also be configured to allow guests to log in using social media or WeChat accounts.
- **Hotspot Service (WISPr)**: Create a Hotspot WLAN. A Hotspot service must first have been created (**Sevices & Profiles > Hotspot Services**) before it will be available for selection. See Working with Hotspot Services on page 185.
- **Hotspot 2.0**: Create a Hotspot 2.0 WLAN. A Hotspot 2.0 Operator must first have been created (**Sevices & Profiles > Hotspot 2.0 Services**) before it will be available for selection. See Creating a Hotspot 2.0 Service on page 191.
- **Autonomous**: Autonomous WLANs are special WLANs designed to continue providing service to clients when APs are disconnected from ZoneDirector. See Autonomous WLANs on page 66.

Autonomous WLANs

The Autonomous WLAN usage type supports Open authentication and WPA2 (WPA2/WPA-Mixed), WEP, or no encryption only.

In this configuration, client authentication/association requests are processed at the access point and are not forwarded to ZoneDirector. The AP maintains connections to authorized clients and continues providing wireless service after disconnection from ZoneDirector.

NOTE
If AP Auto Recovery is enabled (**Access Points > Access Point Policies**), the APs will reboot after the specified time. Therefore Auto Recovery should be disabled if at least one Autonomous WLAN is configured.

There are several limitations of autonomous WLANs, including:

- ZoneDirector displayed client statistics may be incorrect.
- Stations may be disconnected when an unreachable ZoneDirector becomes reachable again, as ZoneDirector will re-deploy all WLAN services to AP radios.
- Client capacity limits defined on ZoneDirector will not be applied on Autonomous WLAN APs, and clients may be disconnected upon reconnecting to ZoneDirector if those limits are reached.
- The following features are not supported with Autonomous WLANs:
  - Zero-IT, Dynamic PSK, Dynamic VLAN, Web Auth, Role-Based Access Control, Accounting server, Tunnel Mode, Grace Period, Force DHCP, Client Fingerprinting, Auto Proxy, Service Schedules.
  - ZoneDirector's Blocked Clients list will not be enforced on Autonomous WLANs when a Layer 2 ACL is assigned. To force blocking of these clients, copy individual clients to the assigned L2 ACL.

Authentication Method

Authentication Method defines the method by which users are authenticated prior to gaining access to the WLAN.

The authentication method is only configurable for "Standard Usage" type WLANs. For other WLAN types, the authentication method is "Open" and encryption methods vary by WLAN type.

ZoneDirector provides the following authentication method options:

- **Open** [Default]: No authentication mechanism is applied to connections. Any encryption method can be used. Open authentication allows the use of WPA2, WPA3, WPA2/WPA3-Mixed, OWE, or no encryption. Open authentication + WPA2 encryption (also known as WPA-PSK) is the most common type of WLAN encryption method and should be the default configuration if there are no special requirements for authentication or encryption.
- **802.1X/EAP**: Uses 802.1X authentication against a user database. The 802.1X EAP authentication method (also known as "WPA2-Enterprise") provides effective authentication regardless of the encryption method, and requires a back-end (RADIUS) authentication server. WPA2-Enterprise provides secure connectivity by ensuring that every device must authenticate to an authentication server before it is allowed access to network resources. Authentication can be based on digital certificates, and granular policies can be designed to govern the level of access and to provide visibility and control over devices on the network.
- **MAC Address**: Uses the device's MAC address for both the user name and password against an external RADIUS server or internal database.
- **802.1X EAP + MAC Address**: Allows the use of both authentication methods on the same WLAN. See Using 802.1X EAP + MAC Address Authentication on page 257.

Fast BSS Transition

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.

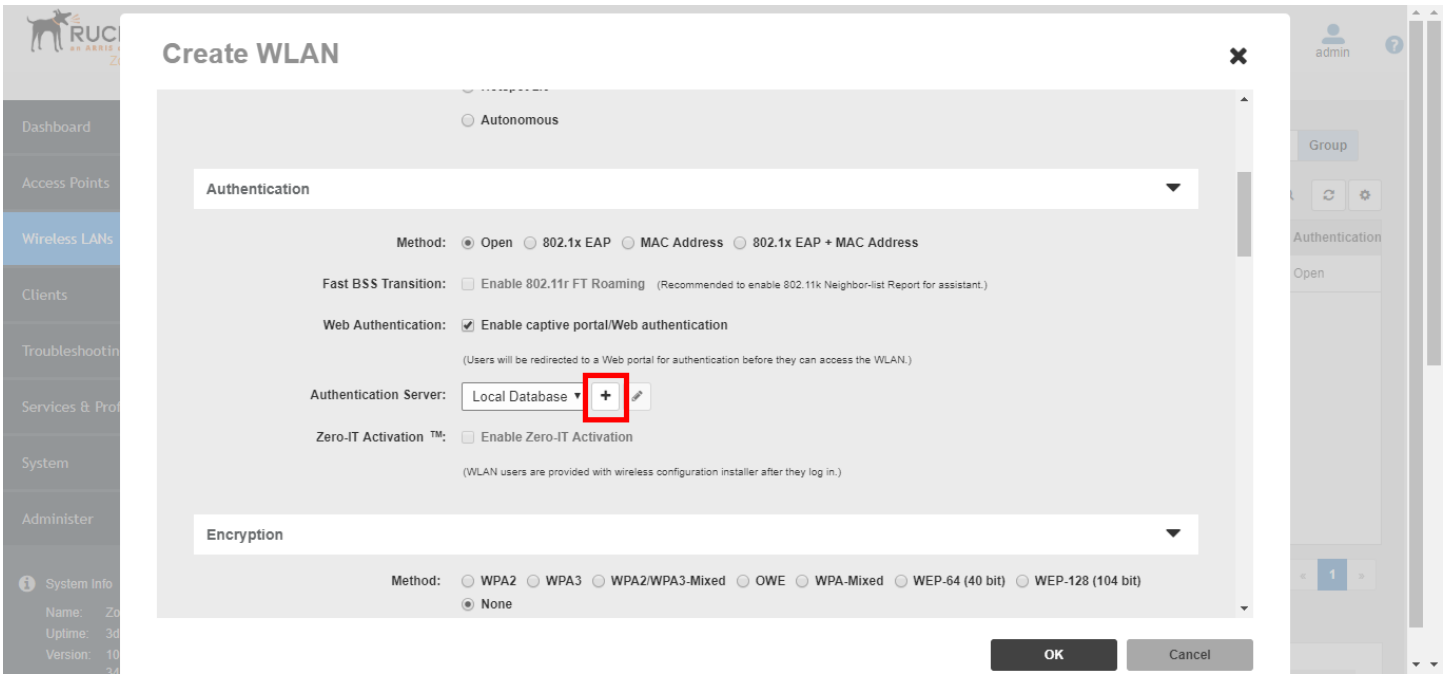
A fast BSS transition is a BSS transition in the same mobility domain that establishes the state necessary for data connectivity before the re-association rather than after the re-association. In this way, clients that support the 11r standard (including iOS devices) can achieve significantly faster roaming between APs.

Authentication Options

The Authentication section allows you configure authentication settings for the WLAN.

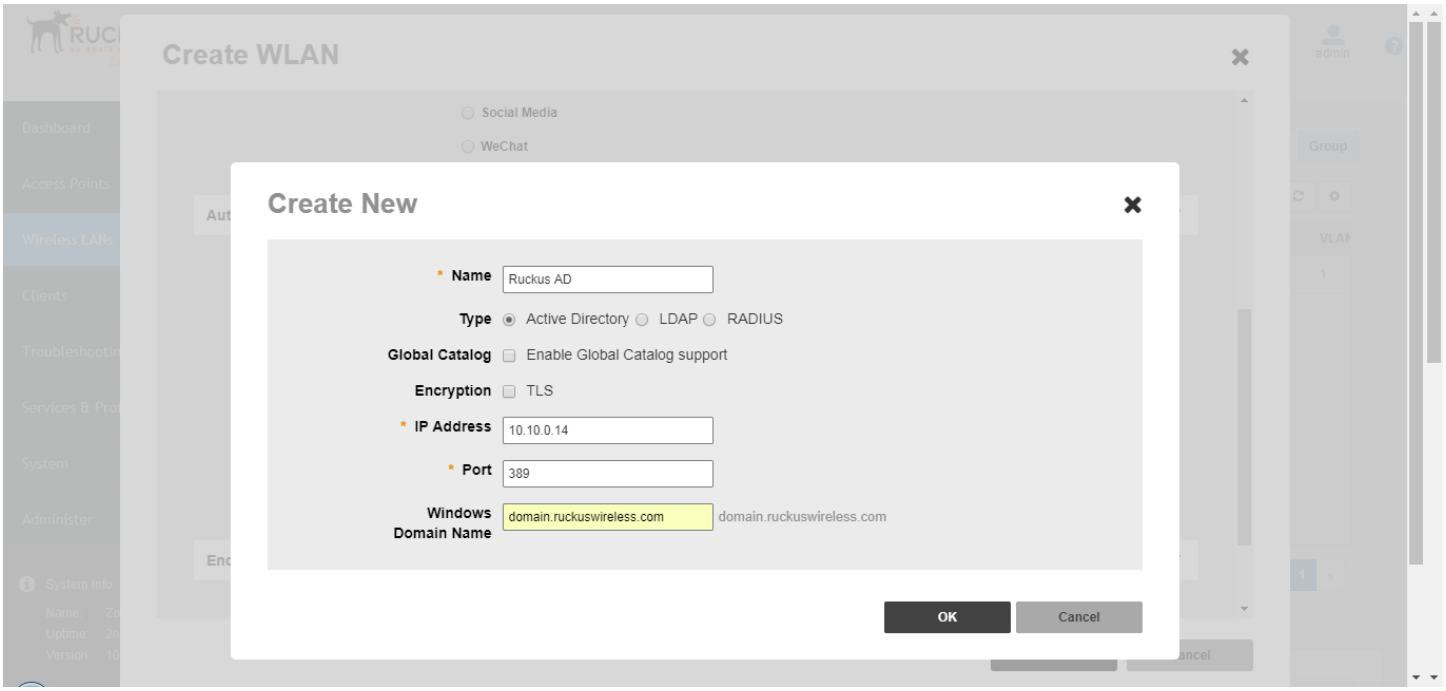
- **Web Authentication**: [Available only with *Standard Usage* WLAN type and *Open* authentication.] Enable this option to require all WLAN users to complete a web-based login to this network each time they attempt to connect (see Enabling Web Authentication on page 122).
- **Authentication Server**: When Web Auth is active, use this option to designate the server used to authenticate captive portal user logins. When "802.1X" or "MAC Address" authentication is active, use this option to designate the server used to authenticate users (without web authentication). Options include Local Database, or a user-configured authentication server. When one of these authentication server types is selected (other than "Local Database"), you will need to point ZoneDirector to the proper authentication server configured on the **Services & Profiles > AAA Servers** page. Alternatively, click the **Create New** (+) button to create a new AAA server object from within the WLAN configuration screen.

FIGURE 31 Click Create New to create a new AAA server



A popup window appears in which you can configure an Active Directory, LDAP or RADIUS AAA server.

FIGURE 32 Create new AAA server



- **Zero-IT Activation**: [Only available with *Standard Usage* WLAN type and *Open* authentication.] Enable this option to activate ZoneDirector's share in the automatic device activation process, in which users can self-register a new wireless device to a WLAN easily and quickly, with minimal IT involvement required. For more information, see Enabling Automatic User Activation with Zero-IT on page 97.
- **Dynamic PSK**: Dynamic PSK is available when you have enabled *Zero-IT Activation* and *WPA2* as the encryption method. When a client is activated, ZoneDirector provisions the user with a unique per-device pre-shared key. For more information, see Working with Dynamic Pre-Shared Keys on page 101.

Encryption Options

Encryption choices include WPA2, WPA3, WPA2/WPA3-Mixed, OWE, WPA/WPA2-Mixed, WEP-64, WEP-128 and None.

WPA2 and WPA3 are the only encryption methods certified by the Wi-Fi Alliance. WEP has been proven to be easily circumvented, and RUCKUS recommends against using WEP whenever possible.

WPA-Mixed allows WPA and WPA2 encryption methods to both be used on the same WLAN.

OWE (Opportunistic Wireless Encryption) provides encrypted communications for open networks. OWE complies with the RFC 8110 specification.

The WPA3 encryption method provides several security enhancements over WPA2. The WPA2/WPA3-Mixed option allows for backward compatibility with clients that do not yet support the newer WPA3 standard.

Method

- *WPA2*: The WPA2 encryption method complies with the 802.11i security standard. Announced in 2004, WPA2 encryption remains mandatory for all new products that bear the Wi-Fi trademark.
- *WPA3*: Announced in January 2018, the WPA3 standard replaces WPA2 with several security enhancements.

- *WPA2/WPA3-Mixed*: Allows mixed networks of WPA2 and WPA3 compliant devices.
- *WPA-Mixed*: Allows mixed networks of WPA and WPA2 compliant devices.
- *OWE*: (Opportunistic Wireless Encryption) provides encrypted communications for open networks.
- *WEP-64*: Provides a lower level of encryption, and is less secure, using shared key 40-bit WEP encryption.
- *WEP-128*: Provides a higher level of encryption than WEP-64, using a shared 104-bit key for WEP encryption. However, WEP is inherently less secure than WPA2.
- *None*: No encryption; communications are sent in clear text.

NOTE
If you set the encryption method to WEP-64 (40 bit) or WEP-128 (104 bit), the WLAN will operate in 802.11g mode.

Algorithm

- *AES*: (AES-CCMP) This algorithm provides enhanced security over TKIP, and is the only encryption algorithm supported by the 802.11i standard (the standard that introduced WPA2).
- *AES-GCMP-256*: Galois Counter Mode Protocol (GCMP) is supported by 802.11ac, is more efficient than AES-CCMP and provides better performance for wireless clients. AES-GCMP-256 uses 256 bit AES encryption keys.
- *Auto (TKIP+AES)*: Automatically selects TKIP or AES encryption based on the client's capabilities. Note that since it is possible to have clients using both TKIP and AES on the same WLAN, only unicast traffic is affected (broadcast traffic must fall back to TKIP; therefore, transmit rates of broadcast packets from 11n/11ac APs will be at lower 11g rates).



CAUTION
If you set the encryption algorithm to TKIP, the WLAN will operate in 802.11g mode.



CAUTION
If you set the encryption algorithm to TKIP, the AP will only be able to support up to 26 clients. When this limit is reached, additional clients will be unable to associate with the AP.

SAE Passphrase (Only for WPA3 and WPA2/WPA3-Mixed WLANs)

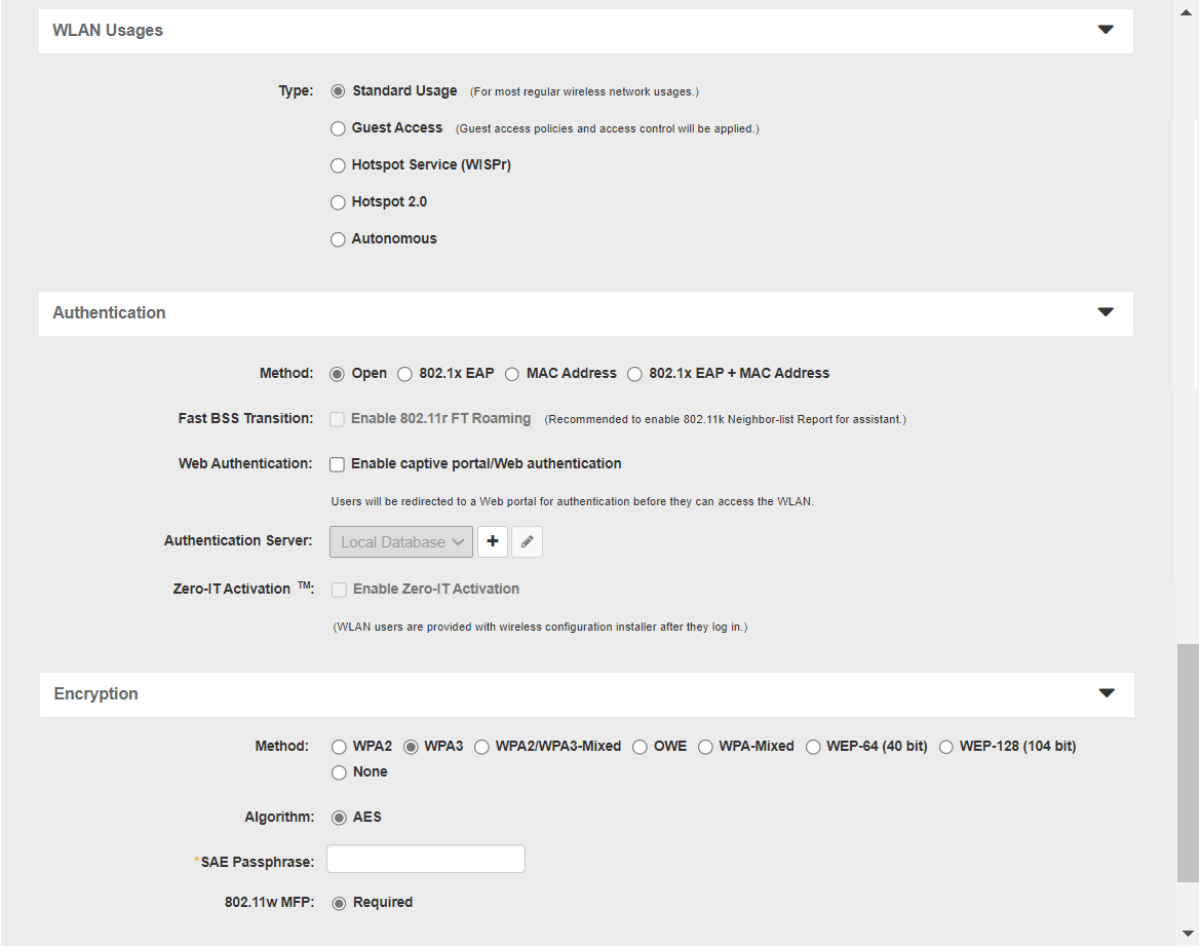
The SAE Passphrase (Simultaneous Authentication of Equals) is a new authentication algorithm for WPA3 that replaces the Pre-Shared Key used in WPA2. SAE Passphrases are designed to simplify login for devices with no keyboards, and to mitigate the risk of weak passwords that can be easily defeating using dictionary attacks.

Complete the following procedure to configure a WLAN using the SAE passphrase encryption method.

1. From the ZoneDirector dashboard, go to **Wireless LANs**.
2. Select a WLAN group from the left pane and select the WLAN that you want to configure and click **Edit** (or click **Create** to create a new WLAN, refer to Creating a Wireless LAN on page 65).
3. Under **WLAN Usages**, for **Type**, select **Standard Usage**.
4. Under **Authentication**, for **Method**, select **Open**.
5. Under **Encryption**, for **Method**, select **WPA3** or **WPA2/WPA3-Mixed** and enter the password for PSK and SAE passphrases.
6. Click **OK** to save your changes.

NOTE
- PSK passphrase must contain 8 through 63 characters or 64 hexadecimal characters, and cannot start or end with a space ( ).
- SAE passphrase must contain 8 through 63 characters and cannot start or end with a space ( ).

FIGURE 33 Configuring a WLAN Using the SAE Passphrase Encryption Method



WEP Key/Passphrase

- *WEP Key*: WEP methods only. Click in the Hex field and type the required key text. If the key is for WEP-64 encryption, the key text must consist of 10 hexadecimal characters. If it is for WEP-128 encryption, enter a key 26 characters in length. Alternatively, click Generate to have ZoneDirector automatically generate a WEP key.
- *Passphrase*: WPA-PSK methods only. Click in this field and type the text of the passphrase used for authentication.

802.11w Management Frame Protection

The Protected Management Frame (PMF) feature, also known as Management Frame Protection (MFP), is defined in 802.11w to protect 802.11 Robust Management frames, including Disassociation, Deauthentication, and Robust Action frames.

To enable, set **802.11w MFP** to *Optional* or *Required* on the **Wireless LANs > Edit WLAN** page. *Optional* allows legacy devices that do not support the 802.11w standard to associate with the SSID while also allowing devices that support 802.11w to use the 802.11w features. *Required* will prevent clients that do not support 802.11w from associating.

Advanced WLAN Options

The advanced options can be used to configure special WLANs.

For example, you might want to create a special WLAN for VoIP phone use only, or create a student WLAN that should be time-controlled to provide access only during school hours.

- **Wireless Client Isolation**: Enable Wireless Client Isolation to prevent communication between WLAN clients and other local network resources.

  NOTE
  If Client Isolation and L3/L4/IP address ACLs are both in place and have conflicting rules, the L3/L4/IP address ACL will take precedence, as the ACLs are applied upon ingress, while the Client Isolation rules are applied after bridging.

  - **Isolate wireless client traffic from other clients on the same AP**: Prevents clients connected to the same AP from communicating with each other, but does not prevent clients from communicating with other hosts connected to different APs on the same subnet.
  - **Isolate wireless client traffic from all hosts on the same VLAN/subnet**: Enable this option to prevent clients from communicating with any other host on the network, unless they are specifically allowed in a white list. A Client Isolation White List must first be created on the **Services & Profiles > Access Control** page before appearing here (see Configuring Client Isolation White Lists on page 236).
- **Bypass Apple CNA Feature**: Enable this option to prevent clients (Mac and iOS) from accessing the Apple Captive Network Assistant mini-browser to skip the login page for web auth and guest WLANs. For more information, see Bypass Apple CNA on page 78.
- **WLAN 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.
- **Accounting Server**: Select or configure a RADIUS Accounting server. If you added a RADIUS Accounting server on the AAA servers page, select the RADIUS Accounting server from the drop-down list, and then set the accounting update interval in Send Interim-Update every x minutes. Valid values are 0-1440. Setting the value to 0 disables periodic interim updates to the accounting server, but client IP changes are still sent to the RADIUS Accounting server. For more information, see RADIUS /RADIUS Accounting on page 254.
- **Access Controls**: Toggle this drop-down list to select Access Control Lists (L2 or L3/L4), Device Policy and Precedence Policy to apply to this WLAN. An access control entry must be created before being available here. For more information, see Configuring Network Access Controls on page 228.
- **Enable Role based Access Control Policy**: This feature allows different user groups to have different access policies based on their user roles using the same WLAN. See Role Based Access Control Policy on page 117.
- **Application Recognition and Control**: Enable this option to allow APs to collect client application data, which can then be consolidated for use by the **Applications** and **Top 10 Applications by Usage** graphs.

  NOTE
  This feature is not supported on all Ruckus access points.

  NOTE
  When Application Recognition and Control is enabled, the **Apply Policy group** option becomes available. Use this option to apply an Application Policy to this WLAN (see Configure Application Policies on page 223).

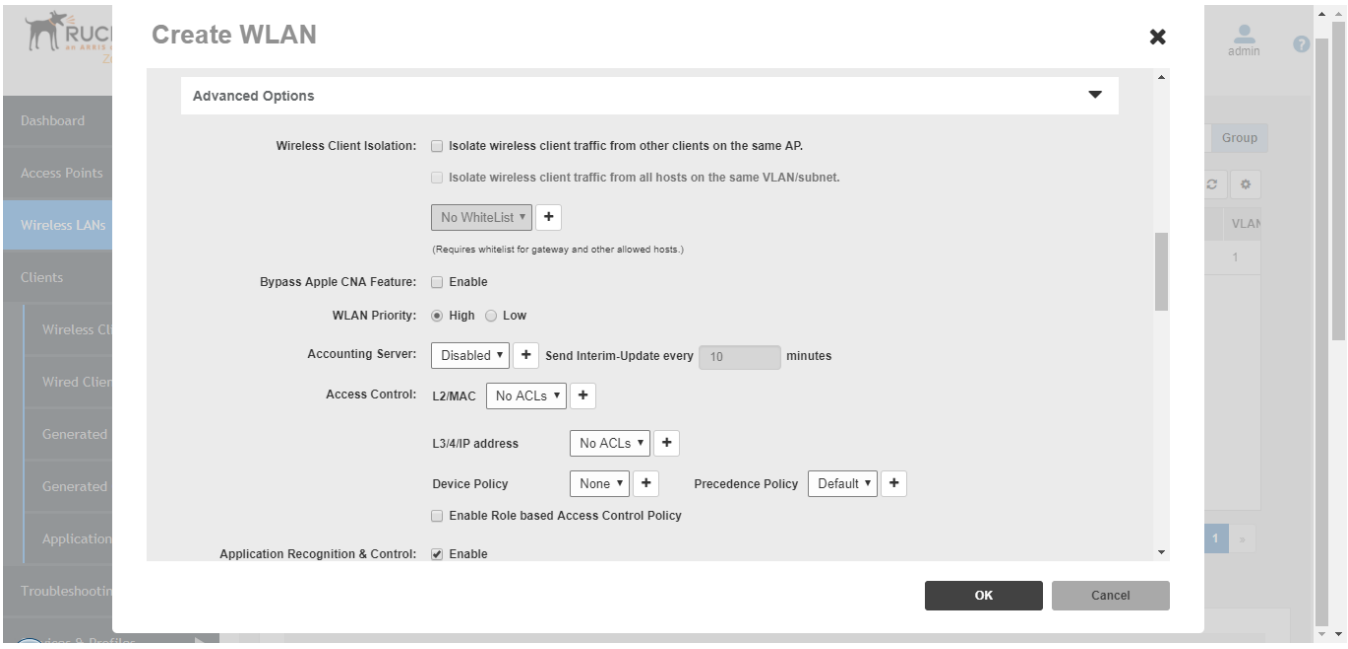
- **Call Admission Control** (Disabled by default): Enable WiFi Multimedia Admission Control (WMM-AC) to support Polycom/Spectralink VIEW certification. When enabled, the AP announces in beacons if admission control is mandatory or not for various access categories and admits only the traffic streams 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. (You will also need to enable Call Admission Control on any APs supporting this WLAN from the **Access Points** page.)

- **Rate Limiting**: 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.
- **SSID Rate Limiting**: In addition to per-station rate limiting, admins can also limit the total bandwidth of all clients connected to the same SSID of an AP, across both 2.4 GHz and 5 GHz radios. The bandwidth limits are applied to each radio according to the number of clients connected, so for example, if there are 7 clients connected to the 2.4 GHz radio and 3 clients connected to the 5 GHz radio, and the total bandwidth configured in SSID rate limiting is 10 Mbps, then the 7 clients in the 2.4 GHz band would share 7 Mbps, while the other 3 clients in the 5 GHz band would share the remaining 3 Mbps.

NOTE
Per-station rate limiting is disabled if per-SSID rate limiting is enabled.

FIGURE 34 Advanced options for creating a new WLAN



- **Multicast Filter**: When enabled for a WLAN, all client multicast traffic will be dropped at the AP. Broadcast and unicast frames remain unchanged.
- **VLAN Pooling**: Assign a pool of VLANs to this WLAN. For more information, see Working with VLAN Pools on page 93
- **Access VLAN**: By default, all wireless clients associated with APs that ZoneDirector is managing are segmented 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. For more information, see Deploying ZoneDirector WLANs in a VLAN Environment on page 86.
  - Select the **Enable Dynamic VLAN** check box to allow ZoneDirector to assign VLAN IDs on a per-user basis. Before enabling dynamic VLAN, you need to define on the RADIUS server the VLAN IDs that you want to assign to users. See How Dynamic VLAN Works on page 91.

- **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.
- **Tunnel Mode**: Select this check box if you want to tunnel the WLAN traffic back to ZoneDirector. 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. Multicast voice packets, however, are allowed.

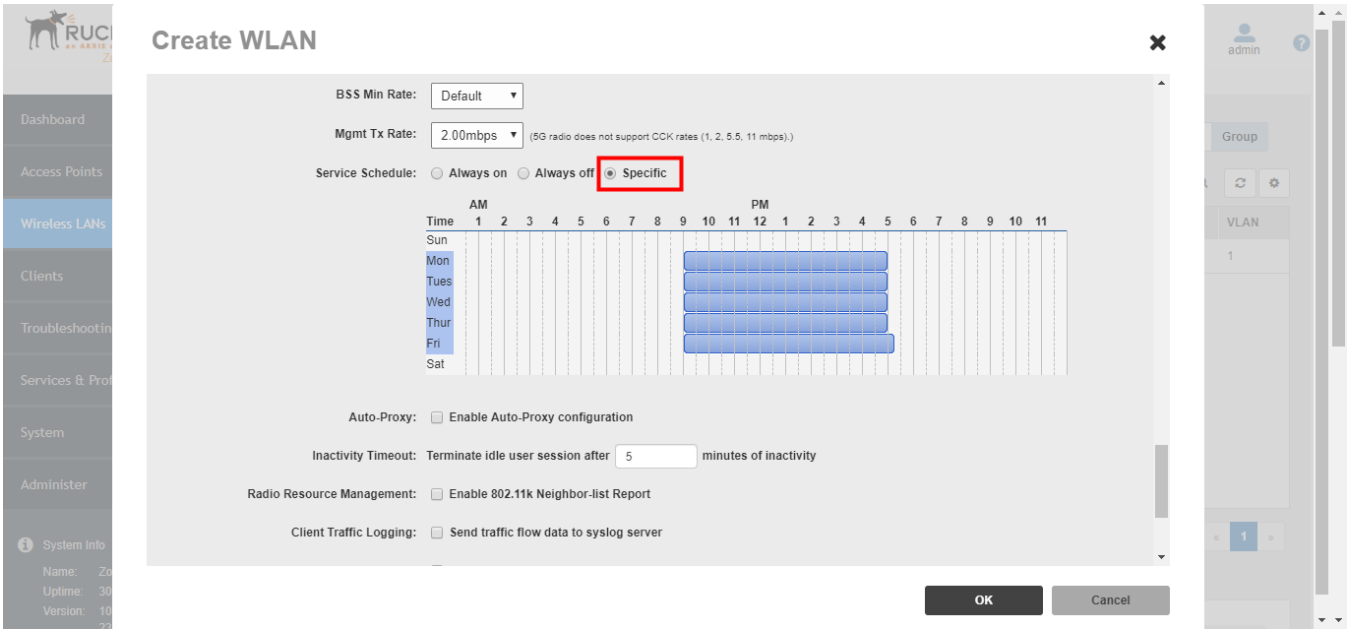
- **Proxy ARP**: When enabled on a WLAN, the AP provides proxy service for stations when receiving neighbor discovery packets (e.g., IPv4 ARP requests and ICMPv6 Neighbor Solicit messages), and acts on behalf of the station in delivering ARP replies. When the AP receives a broadcast ARP/Neighbor Solicit request for a known host, the AP replies on behalf of the host. If the AP receives a request for an unknown host, it forwards the request at the rate limit specified in the Packet Inspection Filter.
- **DHCP Relay**: Enable DHCP Relay agent to convert broadcast DHCP messages to unicast in Tunnel Mode WLANs. For more information, see DHCP Relay on page 279.
- **Background Scanning**: Background scanning enables the Ruckus access points to continually scan for the best (least interference) channels and adjust to compensate. However, disabling Background Scanning may provide better quality (lower latency) for time-sensitive applications like voice conversations. If this WLAN will be used primarily as a voice network, select this check box to disable Background Scanning for this WLAN. You can also disable Background Scanning per radio (see Background Scanning on page 265).
- **Load Balancing**: Client load balancing between APs is disabled by default on all WLANs. To disable load balancing for this WLAN only (when enabled globally), check this box. Ruckus recommends disabling load balancing on VoIP WLANs. For more information, see Load Balancing on page 269.
- **Band Balancing**: Client band balancing between the 2.4 GHz and 5 GHz radio bands is disabled by default on all WLANs. To disable band balancing for this WLAN only (when enabled globally), check this box. For more information, see Band Balancing on page 271.
- **Max Clients**: Limit the number of clients that can associate with this WLAN per AP radio (default is 100). You can also limit the total number of clients per AP using the AP Groups settings. See Modifying Model Specific Controls on page 42 for more information.
- **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. Enable this option if you are operating in one of these additional regulatory domains. For optimal performance of Apple iOS devices, it is recommended that you enable this option. Please be aware that some legacy embedded devices such as wireless barcode scanners may not operate properly if this option is enabled. This option is enabled by default for any WLANs created on ZoneDirector version 9.6 or later, and disabled by default for any WLANs created running earlier versions. If upgrading from a previous version to 9.6 or later, existing WLANs will retain their original settings.
- **DHCP Option 82**: When this option is enabled and an AP receives a DHCP request ID, AP name, SSID and MAC address) into the DHCP request packets before forwarding them to the DHCP server. The DHCP server can then use this information to allocate an IP address to the client from a particular DHCP pool based on these parameters. See also DHCP Option 82 on page 46 for information on enabling this option for Ethernet ports.
- **Force DHCP**: 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. Additionally, if a client performs Layer 3 roaming between different subnets, in some cases the client sticks to the former IP address. This mechanism optimizes the roaming experience by forcing clients to request a new IP address.
- **DTIM Interval**: Configure the Delivery Traffic Indication Message interval to control how often DTIM messages are transmitted. This setting affects the frequency of data transmissions per broadcast beacon. Setting the DTIM interval to a lower value results in more frequent DTIM messages, which can prevent mobile devices from going into power save mode, thereby increasing battery consumption.

- **Directed MC/BC Threshold**: Directed Multicast/Broadcast is a feature that allows Ruckus APs to convert incoming broadcast and multicast traffic to unicast, reducing airtime utilization and improving data throughput performance. Enter a value to set the client count at which an AP will stop converting group addressed data traffic to unicast traffic.
- **Client Tx/Rx Statistics**: Enable this option to ignore unauthorized client statistics and report only statistics from authorized clients in device view and other reports. This can be useful for service providers who are more interested in accounting statistics (after authorization) than in all wireless client statistics. For example, a Hotspot WLAN can be configured to allow unauthorized clients to connect and traverse any walled garden web pages without adding to transmission statistics (until after authorization).
- **Client Fingerprinting**: When this option is enabled ZoneDirector will attempt to identify client devices by their Operating System, device type and Host Name, if available. This makes identifying client devices easier in the Dashboard, Client Monitor and Client Details screens.
- **OFDM Only**: Enabling this option disables CCK rates of 1, 2, 5.5, and 11 Mbps, so no 802.11b-only clients can connect. Beacons and probe responses will be transmitted at 6 Mbps, and data frames at 6, 9, 18, 24, 36, 48, and 54 Mbps. Enforcing higher minimum data rates increases overall network throughput capacity, but reduces the distance at which clients are able to remain connected.
- **BSS Min Rate**: Use this option to configure the minimum transmission rate supported by the WLAN. If OFDM Only is enabled, the only valid options are 12 Mbps and 24 Mbps, with Mgmt Tx frames fixed at 6 Mbps. This option can also be used to prevent 11b clients from connecting, and to allow greater client density with higher data rates.
- **Mgmt Tx Rate**: This option is only available if both OFDM Only and BSS Min Rate are disabled. (Otherwise, the Mgmt Tx Rate is defined by those settings.) Use this setting to configure the rate at which management frames are sent. The default is 2 Mbps.
- **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 ZoneDirector does not have the correct time. To ensure ZoneDirector always maintains the correct time, configure an NTP server and point ZoneDirector to the NTP server's IP address, as described in *Setting the System Time*.

  NOTE
  WLAN service schedule times should be configured based on your browser's current time zone. If your browser and the target AP/WLAN are in different time zones, configure the on/off times according to the desired schedule according to your local browser. For example, if you wanted a WLAN in Los Angeles to turn on at 9:00 am and your browser was set to New York time, you would configure the WLAN service schedule to enable the WLAN at 12:00 noon. When configuring the service schedule, all times are based on your browser's current time zone.

FIGURE 35 Configuring WLAN service schedule



- **Auto-Proxy**: The Auto-Proxy feature automatically configures client browsers with web proxy settings when the user joins the wireless network. Clients locate the proxy script according to the Web Proxy Autodiscovery Protocol (WPAD). WPAD uses discovery methods such as DNS and DHCP Option 252 to locate the configuration file. To use this feature, you must designate where the wpad.dat file is to be stored. Click Choose File to upload a wpad.dat file conforming to the WPAD protocol to ZoneDirector, or select External Server and enter the IP address of the external DHCP/DNS server where the file is stored.
  - Internet Explorer supports DNS and DHCP Option 252, while Firefox, Chrome and Safari support the DNS method only.
  - If the wpad.dat file is stored on ZoneDirector, only one file can be uploaded and this file applies to all WLANs that use the ZD-stored file.
  - Up to 8 wpad.dat files can be saved on external servers in addition to the single wpad.dat file that can be stored on ZoneDirector.

    NOTE
    If Wireless Client Isolation, ACLs or Web/Guest Captive Portal are enabled on the WLAN, an additional ACL may be required to allow wireless clients to access the web proxy server and ZD Captive Portal redirection page. For more information, refer to the Auto-Proxy Application Note available from https://support.ruckuswireless.com.

- **Inactivity Timeout**: Enter a value in minutes after which idle stations will be disconnected (1 to 10 minutes).
- **Radio Resource Management**: Radio Resource Management utilizes 802.11k Neighbor Reports, which are sent by the AP to inform clients of the preferred roaming target AP. The client sends a neighbor report request to an AP, and the AP returns a neighbor report containing information about known neighbor APs that are candidates for a service set transition.

  NOTE
  Background Scanning (**Services & Profiles > Services**) and Report Rogue Devices (**Services & Profiles > WIPS**) must be enabled for 802.11k radio resource management to work properly. If these options are not enabled, the AP will send neighbor reports consisting of only APs found on the same channel as the operating channel of the AP.

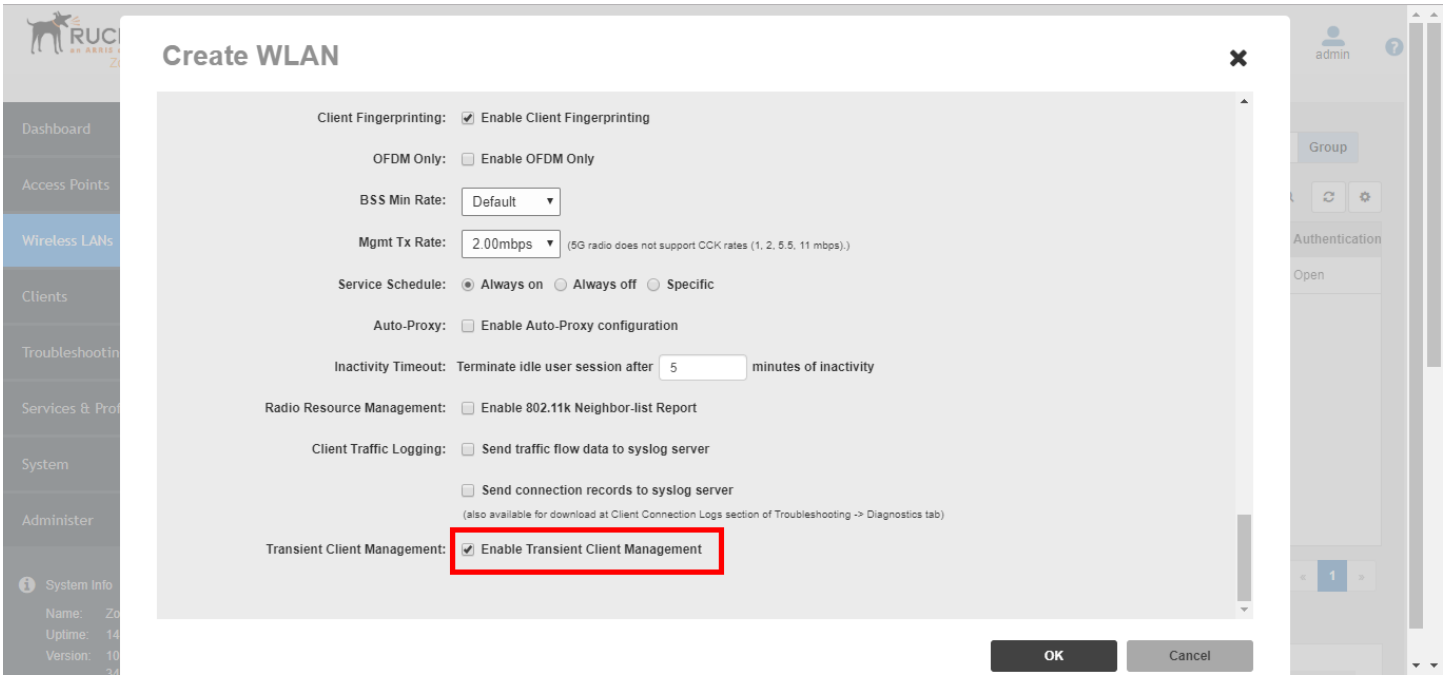
NOTE
If 802.11k is disabled, fast roaming between APs is achieved using Opportunistic Key Caching (OKC) and Pairwise Master Key caching (PMK caching). These methods also require Background Scanning to be enabled. Both methods allow clients to roam without having to repeat the entire 802.1X authentication process. For more information, see PMK Caching and Opportunistic Key Caching on page 79.

- **Client Traffic Logging**: Enable these options to collect and transmit client traffic flow data and/or connection logs to a syslog server.
  - **Send traffic flow data to syslog server**: Enable this option to allow ZoneDirector to transmit client session data to a syslog server. When this option is enabled and a syslog server is configured (*System > System Settings > Log Settings*), ZoneDirector collects and records data for each packet session, including source/destination IP address, port, and source MAC address. This information is then delivered to a syslog server for use in meeting legal obligations for Hotspot service providers in certain countries, and/or for emerging Wi-Fi monetization projects, where the possibility of exporting this data could be useful for marketing or use by a third-party platform.

    NOTE
    If you wish to capture client session data using client traffic flow data logging, you must also set the Priority Level for Managed APs to "All" or "Info" on the *System > System Settings > Log Settings* page.

  - **Send connection records to syslog server**: These logs are generated for each client connect and disconnect event, and contain client information including host name, IP address, MAC address, AP MAC address, and social media login name, if applicable. This feature is designed to help service providers comply with regulatory requirements for client data collection in some countries.
- **Transient Client Management**: In some high-traffic environments, such as a train station or a retail Wi-Fi hotspot, where smart phone users frequently pass by quickly and do not intend to use the Wi-Fi network, admins can enable this option to allow the AP to delay client association to wireless LANs for a brief time to prevent passers-by from unintentionally joining the network. A common problem in public spaces is that a user passing by a hotspot might get AP cell coverage momentarily and unknowingly switch to the Wi-Fi network, and then within a short duration switch back to the cellular network once out of range. This leads to a poor user experience as the user's cell phone switches from cellular to Wi-Fi and back within short duration, and can have an impact on the performance of the Wi-Fi network, as these transient clients consume air time resources unnecessarily. Enable the Transient Client Management option if your APs are located in a high-traffic area and you want to reduce the impact of transient clients attempting to connect.

FIGURE 36 WLAN Advanced options continued



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:

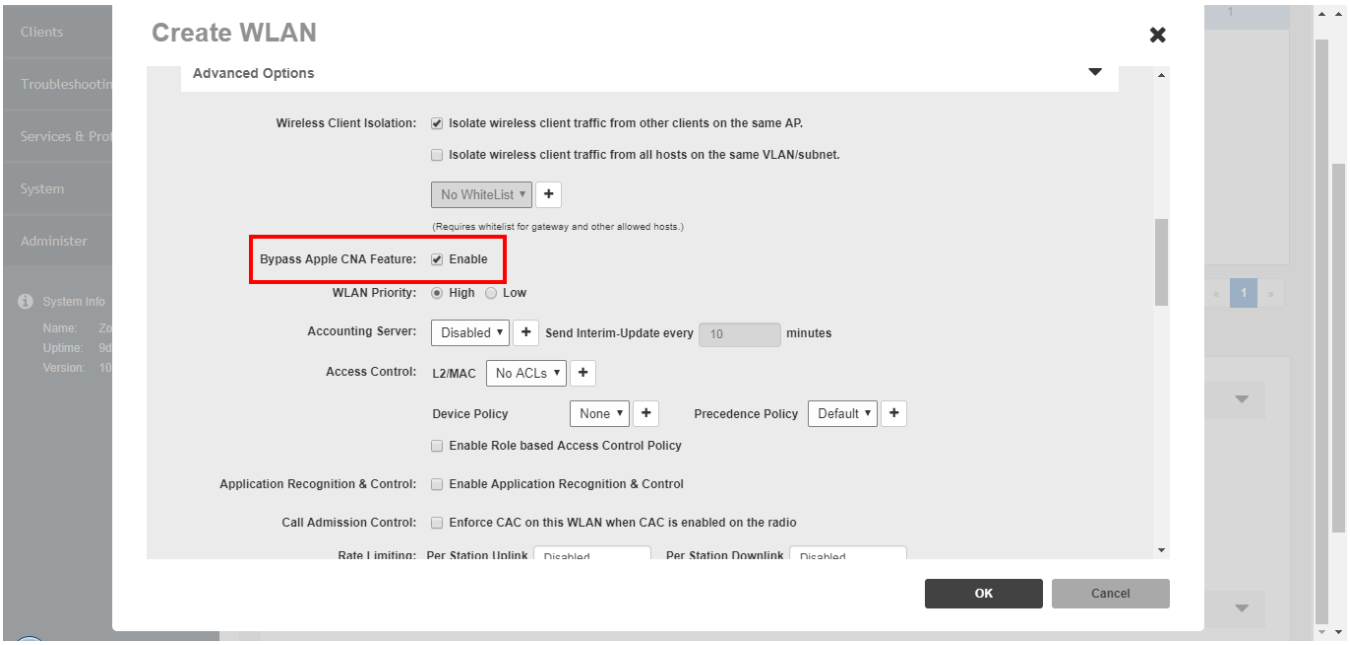
1. Go to **Wireless LANs**.
2. Select the WLAN you want to configure and click **Edit**, or click **Create** to create a new WLAN.

   Select one of the following WLAN usage types:

   - Standard Usage with Web Auth enabled
   - Guest Access (including Social Media)
   - Hotspot (WISPr)
3. Scroll down and expand the **Advanced Options** section.
4. Locate the **Bypass Apple CNA Feature**, and select **Enable**.

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

FIGURE 37 Enabling the Bypass Apple CNA Feature



PMK Caching and Opportunistic Key Caching

Pairwise Master Key (PMK) caching and Opportunistic Key Caching (OKC) allow clients to roam without having to repeat the entire 802.1X authentication process.

PMK Caching

PMK caching allows the client to skip 802.1X authentication to any AP to which it has previously authenticated (only the 4-way handshake is required). PMK Caching is the method defined in the 802.11i specification, which also defined WPA2.

OKC Caching

With this method, a client can skip the 802.1X authentication to an AP as long as the client has authenticated successfully to at least one of the APs in the same zone as the an AP that handled the previous successful authentication. In this case, the PMK is cached at a central location (ZoneDirector).

Creating a Copy of an Existing WLAN for Workgroup Use

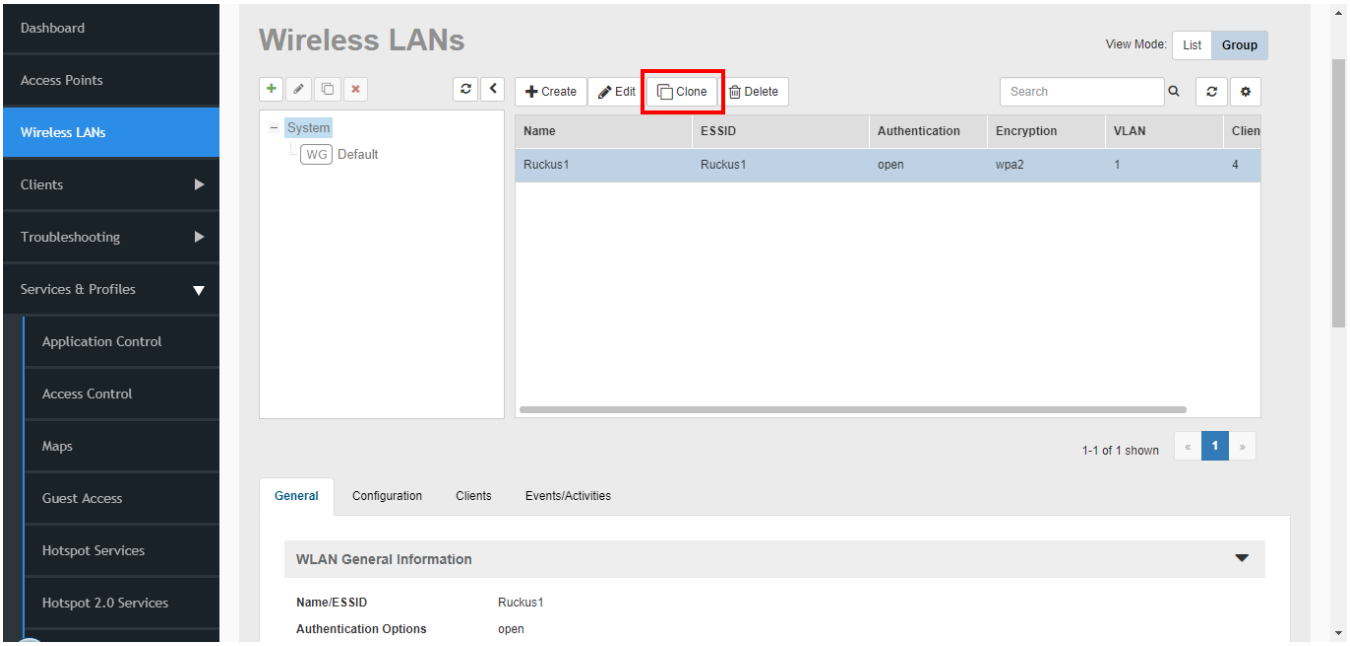
If you want to create an additional WLAN based on your existing default WLAN and limit its use to a select group of users (e.g, Marketing, Engineering), you can do so by following these steps:

1. Make a list of the group of users.
2. Go to**Wireless LANs**.

3. Select the WLAN that you would like to copy, and click **Clone**.

   The **Create WLAN** screen appears, displaying the default settings of a new WLAN, using the same configuration settings as the cloned WLAN.
4. Type a descriptive **Name** for this WLAN, and then click **OK**. This new WLAN is ready for use by selected users.
5. You can now assign access to this new WLAN to a limited set of internal users, as detailed in Creating New User Roles on page 116.

FIGURE 38 Cloning a wireless LAN



Customizing WLAN Security

When you worked through the installation wizard, you were instructed to create your first WLAN. Most users will likely have created an “Open/WPA2” (open authentication, WPA2 encryption, aka “WPA-Personal”) WLAN as their first wireless network.

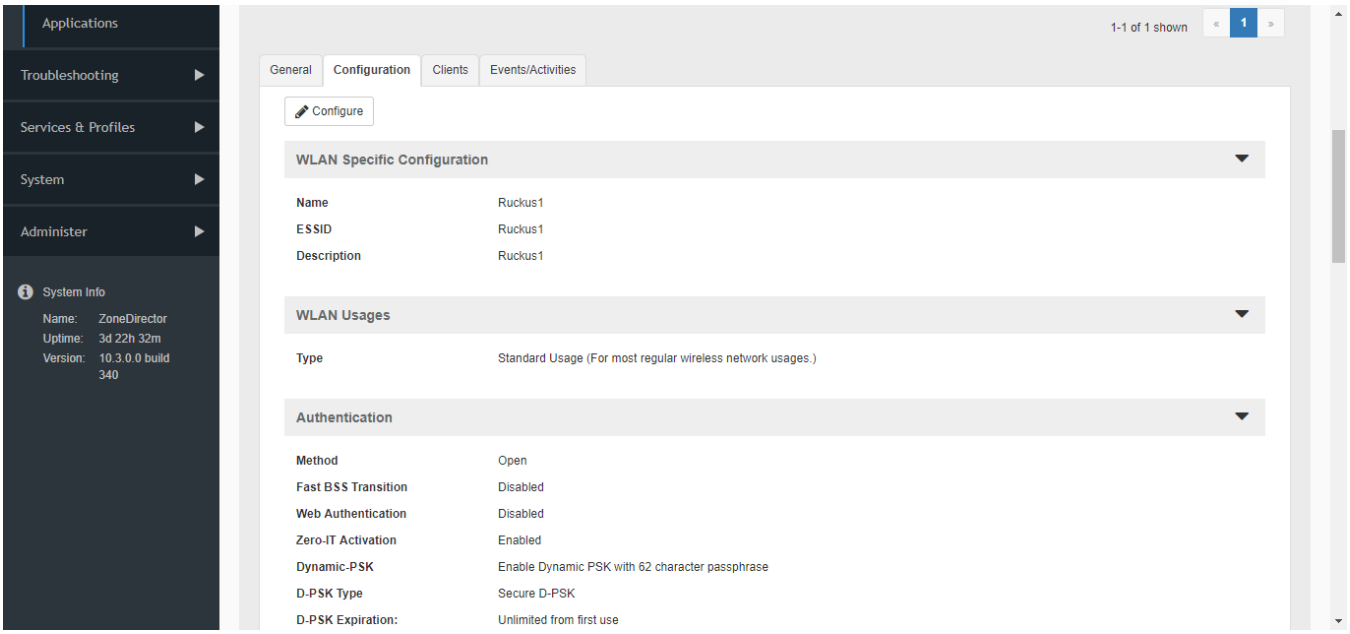
To review the security configuration and the available options (customize the existing WLAN setup or replace it with a totally different configuration), review the following procedures.

Reviewing the Initial Security Configuration

1. Go to **Wireless LANs**
2. The **Wireless WLANs** table lists the WLANs created during the setup process. You can review the details of a WLAN’s configuration by clicking on the WLAN name, and then selecting the **Configuration** tab below.

3. You have three options for the internal WLAN: [1] continue using the current configuration, [2] fine-tune the existing security mode, or [3] replace this mode entirely with a different authentication and encryption method. The two WLAN-editing processes are described separately, below.

FIGURE 39 Viewing wireless LANs



Fine Tuning the Current Security Mode

To keep the original security mode and fine-tune its settings:

1. Go to**Wireless LANs**
2. In the internal/corporate WLAN row, click **Edit**.
3. Choose from the following options to keep the default WPA encryption with no authentication (Open Auth).
   - **WPA-Mixed**: Allows both WPA and WPA2 compliant devices to access the network.
   - **Passphrase**: Replace the current passphrase with a new one, to help lower the risk of unauthorized access.
4. Click **OK** to apply any changes.

Switching to a Different Security Mode

You also have the option of replacing the default internal WLAN's Open authentication/WPA2 encryption mode with one of several other modes:

- Open Auth/WEP encryption: Least security, only use if necessary to support older WEP-only client devices.
- Open Auth/WPA2 encryption: The recommended configuration for modern wireless clients.
- Open Auth/WPA3 encryption: The next-generation wireless encryption standard, which offers several security enhancements over WPA2.
- Open Auth/WPA2-WPA3 Mixed encryption: Enables WPA3 encryption for client devices that support WPA3, but also allows clients that only support WPA2 to connect to the WLAN using a WPA2 passphrase.

- OWE: OWE (Opportunistic Wireless Encryption) provides encrypted communications for open networks. OWE complies with the RFC 8110 specification.
- Open Auth/WPA-Mixed encryption: Allows both WPA and WPA2 devices on the same WLAN. Use this option only if older WPA devices cannot be upgraded to WPA2.
- 802.1X EAP Auth/Any encryption: Authentication to an AAA server (RADIUS or Local Database) using IEEE 802.1X authentication protocol. OWE and WPA2/WPA3-Mixed are not supported with 802.1X EAP authentication. WPA3 encryption is supported with 802.1X EAP authentication, but clients can only be authenticated against a RADIUS server (Local Database is not supported).
- MAC Auth/Any encryption: Authentication by MAC address. Provides limited security due to ease of MAC address spoofing.
- 802.1X EAP + MAC Auth/Any encryption: Allows clients to connect using either MAC address or 802.1X authentication.

To change the security mode for an existing WLAN:

1. Go to **Wireless LANs**.
2. When the WLANs workspace appears, you will want to review and then change the **Edit** in the Internal WLAN row.
3. When the Editing (Internal) options appear, look at the two main categories -- Authentication Options and Encryption Options.
4. If you click an Authentication Option Method such as Open, or 802.1X, different sets of encryption options are displayed:
   - *Open* allows you to configure a WPA, WPA2, WPA3, OWE or WEP-based encryption, or "None" if you're so inclined. After selecting a WPA or WEP level, you can then enter a passphrase or key text of your choosing.
   - *802.1X EAP* allows you to choose from all available encryption methods, but you do not need to create a key or passphrase. Instead, users will be authenticated against ZoneDirector's internal database or an external RADIUS server.
   - *MAC Address* allows you to use an external RADIUS server to authenticate wireless clients based on their MAC addresses. Before you can use this option, you need to add your external RADIUS server to ZoneDirector's *Services & Profiles > AAA Servers* page. You also need to define the MAC addresses that you want to allow on the RADIUS server.
   - *802.1X EAP + MAC Address* allows the use of both authentication methods on the same WLAN.
5. Depending on your *Authentication Option Method* selection, review and reconfigure the related Encryption Options.
6. Review the *Advanced Options* to change any settings as needed.
7. When you are finished, click **OK** to apply your changes. Replacing your WPA2 configuration with 802.1X requires the users to make changes to their wireless connection configurations, which may include the importation of new SSL certificates.

Using the Built in EAP Server

(Requires the selection of "Local Database" as the authentication server.) If you are re-configuring your internal WLAN to use 802.1X/EAP authentication, you normally have to generate and install certificates for your wireless users.

With the built-in EAP server and Zero-IT Wireless Activation, certificates are automatically generated and installed on the end user's computer. Users simply follow the instructions provided during the Zero-IT Wireless Activation process to complete this task (see Self-Provisioning Clients with Zero-IT on page 98). Once this is done, users can connect to the internal WLAN using 802.1X/EAP authentication.

Authenticating with an External RADIUS Server

You can also use an external RADIUS server for your wireless client 802.1X EAP authentication.

An EAP-aware RADIUS server is required for this application. Also, you might need to deploy your own certificates for wireless client devices and for the RADIUS server you are using. In this case, ZoneDirector works as a bridge between your wireless clients and the RADIUS server during the wireless authentication process.

ZoneDirector allows wireless clients to access the networks only after successful authentication of the wireless clients by the RADIUS server. For information on configuring a RADIUS server for client authentication, see RADIUS /RADIUS Accounting on page 254.

If You Change the Internal WLAN to WEP or 802.1X

If you replace the default configuration of the internal WLAN, your users must reconfigure the wireless LAN connection settings on their devices.

This process is described in detail below and can be performed when logging into the WLAN as a new user.

If Switching to WEP-based Security

1. Each user should be able to repeat the Zero-IT Wireless Activation process and install the WEP key by executing the activation script.
2. Alternatively, they can manually enter the WEP key text into their wireless device connection settings.

If Switching to 802.1X-based Security

1. (Applies only to the use of the built-in EAP server.) Each user should be able to repeat the Zero-IT Wireless Activation process and download the certificates and an activation script generated by ZoneDirector
2. Each user must first install certificates to his/her computer.
3. Each user must then execute the activation script, in order to configure the correct wireless setting on his/her computer.
4. To manually configure 802.1X/EAP settings for non-EAP capable client use, use the wireless settings generated by ZoneDirector.

Working with WLAN Groups

WLAN groups are used to specify which APs provide which WLAN services. If your wireless network covers a large physical environment (for example, multi-floor or multi-building office) and you want to provide different WLAN services to different areas of your environment, you can use WLAN groups to do this.

For example, if your wireless network covers three building floors (1st Floor to 3rd Floor) and you need to provide wireless access to visitors on the 1st Floor, you can do the following:

1. Create a WLAN service (for example, “Guest Only Service”) that provides guest-level access only.
2. Create a WLAN group (for example, “Guest Only Group”), and then assign “Guest Only Service” (WLAN service) to “Guest Only Group” (WLAN group).
3. Assign APs on the 1st Floor (where visitors need wireless access) to your “Guest Only Group”.

Any wireless client that associates with APs assigned to the “Guest Only Group” will get the guest-level access privileges defined in your “Guest Only Service.” APs on the 2nd and 3rd Floors can remain assigned to the Default WLAN Group and provide normal-level access.

NOTE
Creating WLAN groups is optional. If you do not need to provide different WLAN services to different areas in your environment, you do not need to create a WLAN group.

NOTE
A default WLAN group called Default exists. The first 27 WLANs that you create are automatically assigned to this Default WLAN group.

NOTE
A WLAN Group can include a maximum of 27 member WLANs. For dual radio APs, each radio can be assigned to only one WLAN Group (single radio APs can be assigned to only one WLAN Group).

The maximum number of WLAN groups that you can create depends on the ZoneDirector model.

TABLE 15 Maximum number of WLAN groups by ZoneDirector model

ZoneDirector Model	Max WLAN Groups
ZoneDirector 1200	512

Creating a WLAN Group

1. Go to **Wireless LANs**.
2. In the **WLAN Groups** section, click **Create**. The **Create WLAN Group** form appears.
3. In **Name**, type a descriptive name that you want to assign to this WLAN group. For example, if this WLAN will contain WLANs that are designated for guest users, you can name this as "Guest WLAN Group."
4. In **Description** (optional), type some notes or comments about this group.
5. Under **Group Settings**, select the check boxes for the WLANs that you want to be part of this WLAN group.
6. In the **VLAN override** settings, choose whether to override the VLAN configured for each member WLAN. Available options include:
   - **No Change**: Click this option if you want the WLAN to keep the same VLAN tag (default: 1).
   - **Tag**: Click this option to override the VLAN configured for the WLAN service.

7. Click **OK**. The **Create WLAN Group** form disappears and the WLAN group that you created appears in the table under WLAN Groups. You may now assign this WLAN group to an AP.

FIGURE 40 Click Create WLAN Group icon

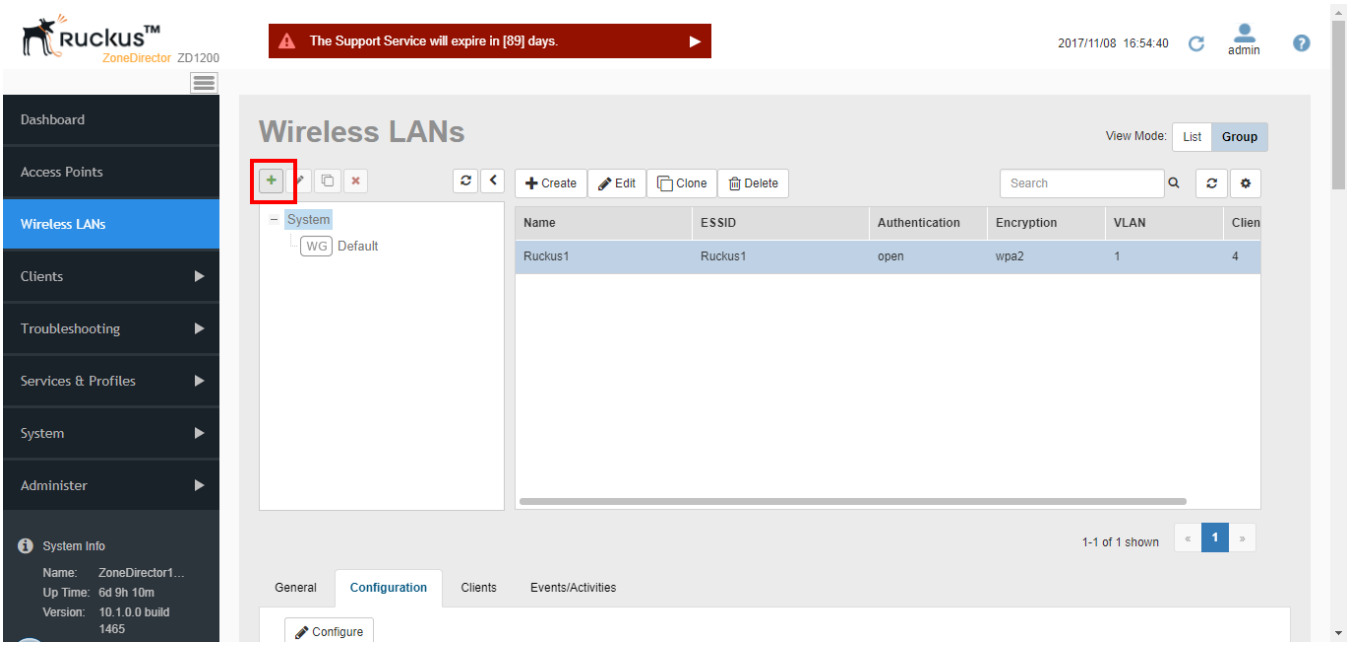
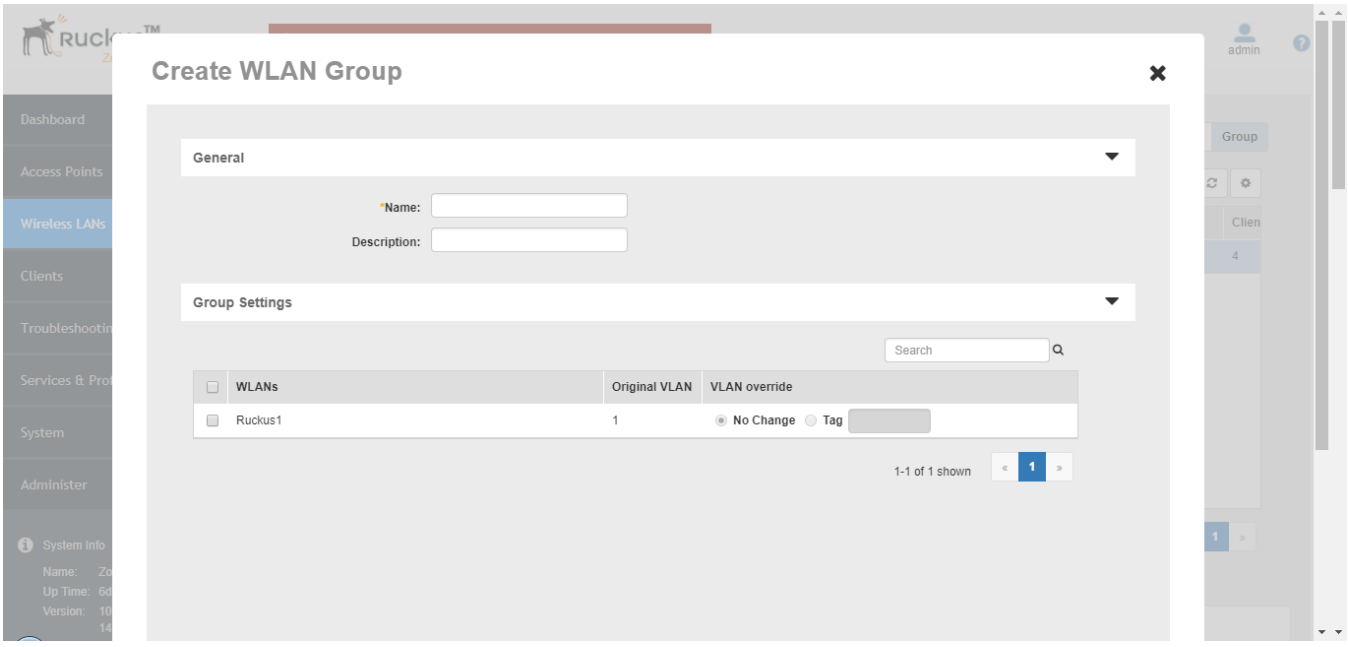


FIGURE 41 Creating a WLAN Group

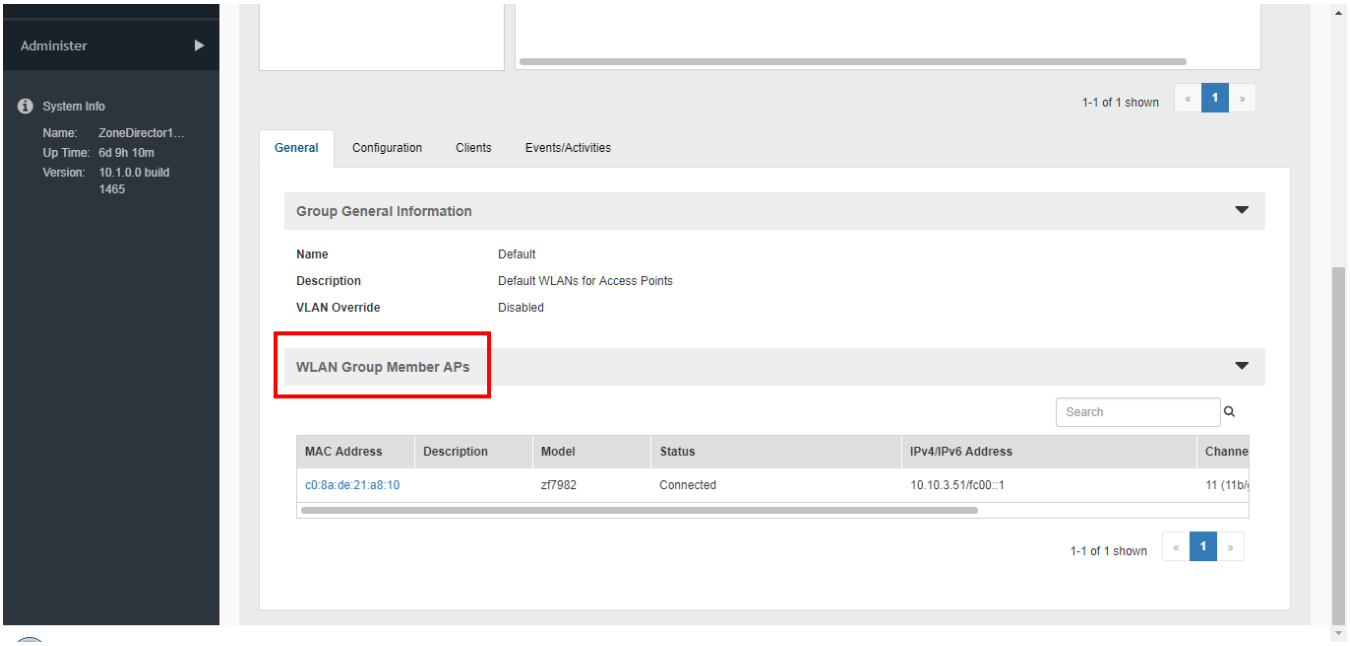


Viewing a List of APs That Belong to a WLAN Group

1. Go to **Wireless LANs**.
2. In the WLAN group box, click the WLAN group name for which you want to view the member AP list.
3. Scroll down to *WLAN Group Member APs*.

   All APs that belong to this WLAN group are listed.

FIGURE 42 Viewing WLAN Group membership



Deploying ZoneDirector WLANs in a VLAN Environment

Configuring VLANs for ZoneDirector, Access Points and wireless clients is not required for normal operation, and should not be undertaken without a thorough understanding of your network's VLAN environment and switch port configuration.

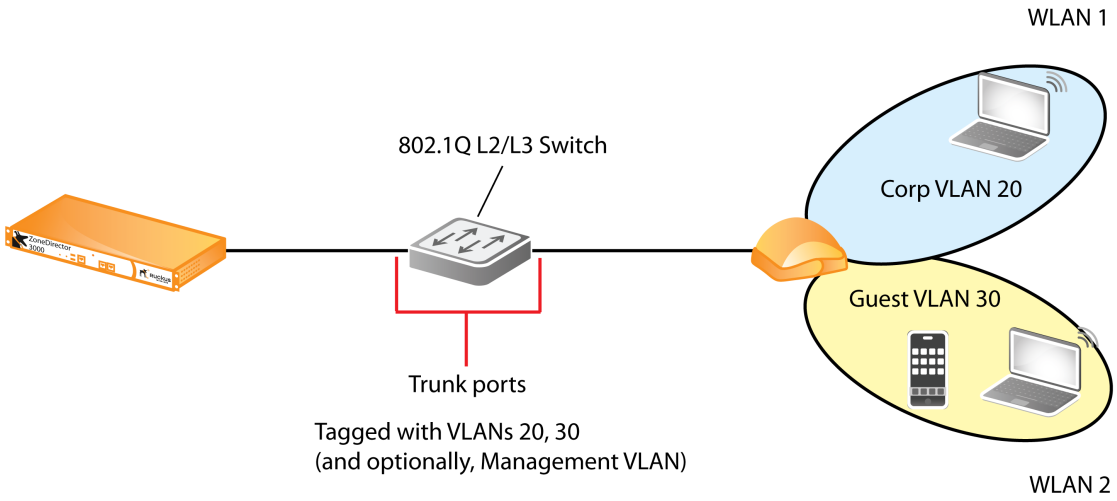
You can set up a ZoneDirector wireless LAN as an extension of a VLAN network environment by tagging wireless client traffic to specific VLANs. Then, when wireless traffic enters the wired network through an access point, it is automatically segmented into the proper VLAN before being forwarded toward its destination.

Qualifications include the following:

- Verifying that the VLAN switch supports native VLANs. A native VLAN is a VLAN that allows the user to designate untagged frames going in/out of a port to a specific VLAN.
- For example, if an 802.1Q port has VLANs 1, 20, and 30 enabled with VLAN 1 being the native VLAN, frames on VLAN 1 that egress (exit) the port are not given an 802.1Q header (i.e., they are plain Ethernet frames). Frames which ingress (enter) this port and have no 802.1Q header are assigned to VLAN 1. Traffic from WLANs configured with access VLANs 20 and 30 is tagged with an 802.1Q header containing the respective VLAN assignment before being forwarded to its destination on the Ethernet network.
- Connecting ZoneDirector and any Access Points (APs) to trunk ports on the switch.
- Verifying that those trunk ports are on the same native VLAN.

Example configuration (see Figure below): VLAN 20 is used for internal clients, VLAN 30 is used for guest clients, and Management VLAN configuration is optional.

FIGURE 43 Sample VLAN configuration



You must ensure that switch ports are configured properly to pass the VLAN traffic necessary for ZoneDirector, AP and client communications. In the sample VLAN scenario above, the switch ports would need to be configured as follows:

- Corp VLAN: 20
- Guest VLAN: 30
- Management VLAN: (optional)

Some common VLAN scenarios include:

- WLANs assigned to specific VLANs; ZD and APs with no management VLAN
- WLANs assigned to specific VLANs; ZD and APs within their own single management VLAN
- WLANs assigned to specific VLANs; ZD and APs are configured for management VLAN, but are different VLANs and there is an L3 connection between (typical branch/remote office deployments)
- WLANs assigned to specific VLANs; ZD or APs only (not both) configured with management VLAN (again typically with an L3 connection between ZD and APs)

The following factors need to be taken into consideration:

- Default/Native VLAN configuration
- Where the DHCP/DNS servers sit in the architecture
- If tunneling is used for WLANs
- Trunking between switch ports

NOTE
All DNS, DHCP, ARP, and HTTP traffic from an unauthenticated wireless client will be forwarded by the AP onto the ZoneDirector via the management LWAPP tunnel. If the client belongs to a particular VLAN, the ZoneDirector will add the respective VLAN tag before forwarding the traffic to the wired network. After client authentication is complete, the AP adds the respective VLAN tag and forwards the client traffic directly to the wired network. This explains why it is necessary to configure the tagged VLANs on all switch ports connected to the ZoneDirector and APs.

Tagging Management Traffic to a VLAN

Assigning management traffic to a specific management VLAN can provide benefits to the overall performance and security of a network.

If your network is designed to segment management traffic to a specific VLAN and you want to include ZoneDirector's AP management traffic in this VLAN, you can set the parameters in the ZoneDirector system configuration. Assigning management traffic to a VLAN makes automatic AP provisioning more complicated, and should not be undertaken without a thorough understanding of your wired network configuration as well as the wireless deployment.

Configuring a management VLAN is not required. Access ports in a native VLAN can be used as the management VLAN rather than actually configuring a management VLAN.

To assign ZD - AP management traffic to a management VLAN:

1. Go to **Access Points**.
2. In **AP Policies**, click **VLAN ID** next to *Management VLAN*, and enter the VLAN ID in the field provided.
3. Click **Apply** to save your settings.
4. Go to **System** > **System Settings**.
5. In **Device IP Settings**, enter the VLAN ID in the Access VLAN field.
6. If you are using an additional management interface for ZoneDirector, enter the same ID in the Access VLAN field for the additional management interface.
7. Click **Apply** to save your settings.

NOTE
ZoneDirector will need to be rebooted after changing management VLAN settings.

8. Go to **Administer** > **Restart**, and click **Restart** to reboot ZoneDirector.

CAUTION

When configuring or updating the management VLAN settings, make sure that the same VLAN settings are applied on the Access Points > Access Point Policies > Management VLAN page, if APs exist on the same VLAN as ZoneDirector.

FIGURE 44 Configuring management VLAN for APs

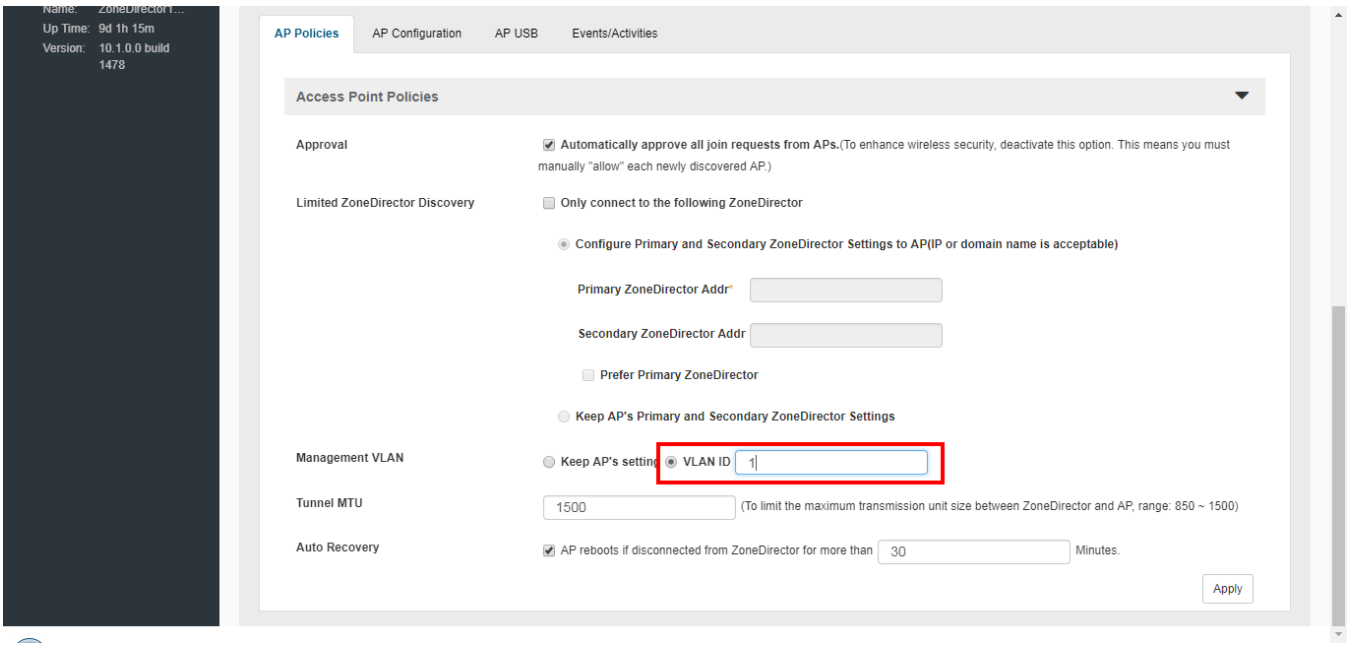
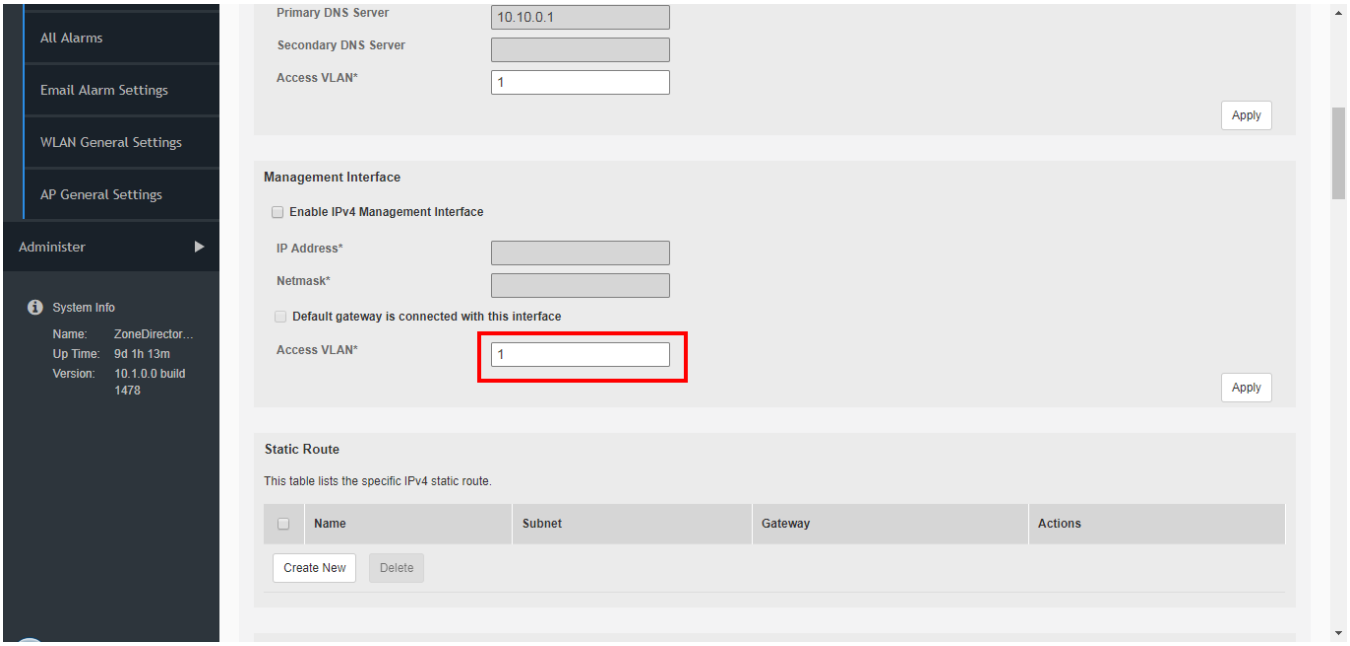


FIGURE 45 Configuring management VLAN for ZoneDirector



Using VLAN Override

There are many instances where Zonedirector manages multiple Access Points at different locations, and the deployment requires that the same SSID be broadcast by two or more APs at different locations with different VLAN tags.

In this case, you can use the VLAN Override settings in WLAN Groups to configure separate access VLANs for clients connecting to the same WLAN on different APs.

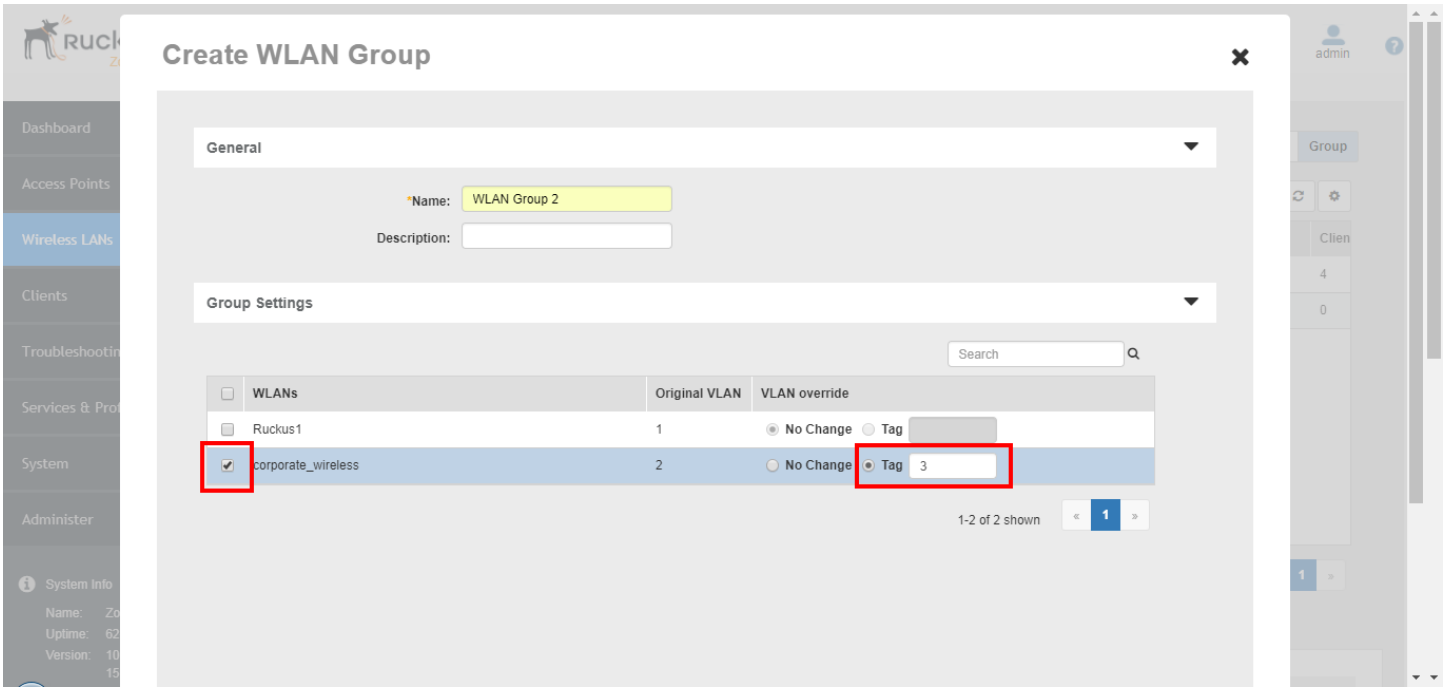
Assume ZoneDirector manages two Access Points, AP1 and AP2, and the network admin wants all wireless clients to be segmented into two subnets, VLAN 2 and VLAN 3, both with access to the same SSID, *corporate_wireless*. Clients connected to AP1 should be in VLAN 2, and those connected to AP2 should be in VLAN 3.

1. Initially, configure a WLAN named *corporate_wireless* with Access VLAN tag "2". Go to **Wireless LANs > Create WLAN > Advanced Options > Access VLAN**, enter **2** in the **VLAN ID** field, and click **OK** to save your changes.

   At this point, all clients connected to the *corporate_wireless* SSID will be assigned to VLAN 2.
2. Next, go to **Wireless LANs > WLAN Groups**, and create a new WLAN group. Choose the *corporate_wireless* WLAN and select the **Tag** option under the **VLAN override** column. Enter **3** in the VLAN ID field, and click **OK** to save your changes.
3. Go to **Access Points**, and click the **Configure** button for AP2.
4. Change the **WLAN Group** from System Default to the new WLAN group you created above.
5. After this change, AP1 and AP2 will both broadcast the *corporate_wireless* SSID, but users will be segmented into different subnets.
6. Repeat this procedure to segment more APs into additional VLANs.

   If you have many APs and do not want to override settings for each one individually, you can also configure separate AP Groups, and override the WLAN group configuration for all APs in that AP group.

FIGURE 46 Configure WLAN group VLAN Override



NOTE
In the above example, ensure that VLAN 2 is tagged at the switch port connected to AP1 and VLAN 3 is tagged at the switch port connected to AP2.

NOTE
Ensure that the APs are located far enough away from one another so that clients do not conflict with different subnets.

How Dynamic VLAN Works

Dynamic VLAN can be used to automatically and dynamically assign wireless clients to different VLANs based on RADIUS attributes.

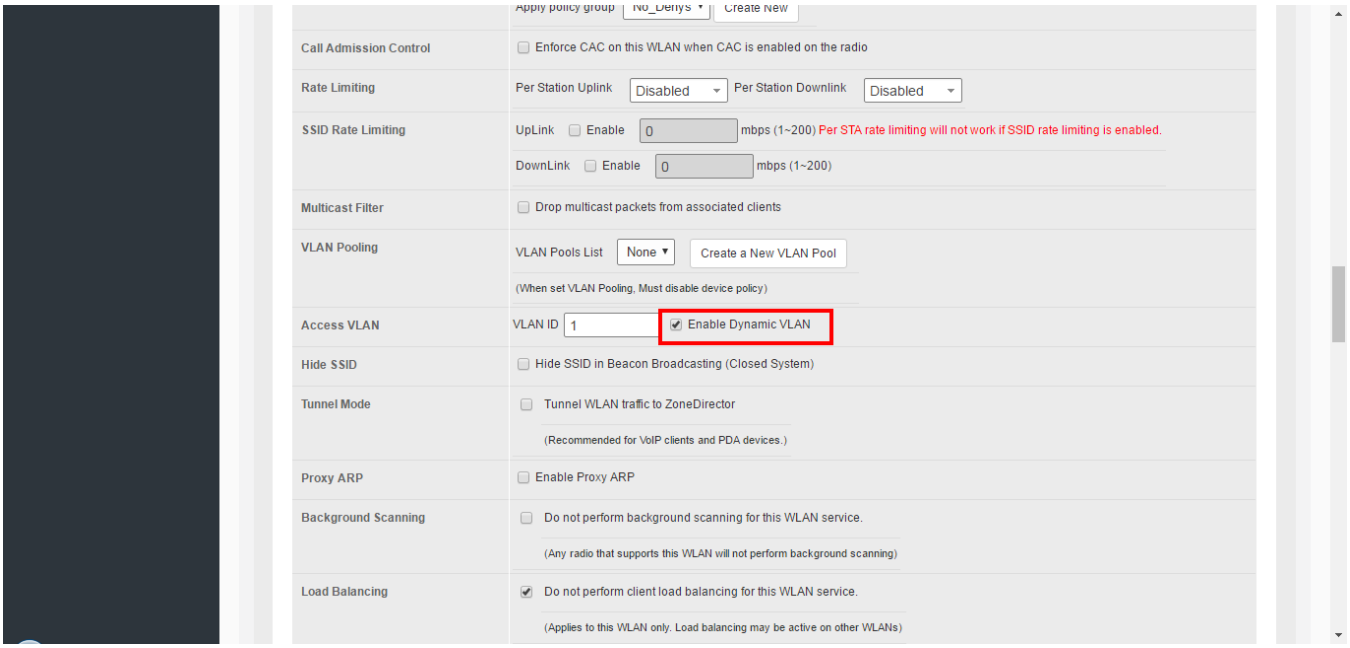
Dynamic VLAN Requirements:

- A RADIUS server must have already been added to the controller
- WLAN authentication method must be set to 802.1X, MAC address or 802.1X + MAC address

To enable Dynamic VLAN for a WLAN:

1. Go to**Wireless LANs**.
2. Click **Configure** for to the WLAN you want to configure.
3. In **Authentication Server**, select the RADIUS server that you configured on the AAA Servers page.
4. Expand the **Advanced Settings** section and click the**Enable Dynamic VLAN box** next to Access VLAN.
5. Click **OK** to save your changes.

FIGURE 47 Enabling Dynamic VLAN



Priority of VLAN Dynamic VLAN and Tunnel Mode

If the VLAN, Dynamic VLAN and Tunnel Mode features are all enabled and they have conflicting rules, ZoneDirector prioritizes and applies these three features in the following order:

- Dynamic VLAN (top priority)
- VLAN
- Tunnel Mode

How It Works

- User associates with a WLAN on which Dynamic VLAN has been enabled.
- The AP requires the user to authenticate with the RADIUS server via ZoneDirector.
- When the user completes the authentication process, ZoneDirector sends the join approval for the user to the AP, along with the VLAN ID that has been assigned to the user on the RADIUS server.
- User joins the AP and is segmented to the VLAN ID that has been assigned to him.

Required RADIUS Attributes

For dynamic VLAN to work, you must configure the following RADIUS attributes for each user:

- **Tunnel-Type**: Set this attribute to VLAN.
- **Tunnel-Medium-Type**: Set this attribute to IEEE-802.
- **Tunnel-Private-Group-ID**: Set this attribute to the VLAN ID to which you want to segment this user.

Depending on your RADIUS setup, you may also need to include the user name or the MAC address of the wireless device that the user will be using to associate with the AP. The following table lists the RADIUS user attributes related to dynamic VLAN.

TABLE 16 RADIUS user attributes related to dynamic VLAN

Attribute	Type ID	Expected Value (Numerical)
Tunnel-Type	64	VLAN (13)
Tunnel-Medium-Type	65	802 (6)
Tunnel-Private-Group-Id	81	VLAN ID

Here is an example of the required attributes for three users as defined on Free RADIUS:

```
0018ded90ef3
   User-Name = user1,
   Tunnel-Type = VLAN,
   Tunnel-Medium-Type = IEEE-802,
   Tunnel-Private-Group-ID = 0014
00242b752ec4
   User-Name = user2,
   Tunnel-Type = VLAN,
   Tunnel-Medium-Type = IEEE-802,
   Tunnel-Private-Group-ID = 0012
013469acee5
   User-Name = user3,
   Tunnel-Type = VLAN,
   Tunnel-Medium-Type = IEEE-802,
   Tunnel-Private-Group-ID = 0012
```

NOTE
The values in bold are the users' MAC addresses.

Working with VLAN Pools

When Wi-Fi is deployed in a high density environment such as a stadium or a university campus, the number of IP addresses required for client devices can easily run into the thousands. Placing thousands of clients into a single large subnet or VLAN can result in degraded performance due to factors like broadcast and multicast traffic.

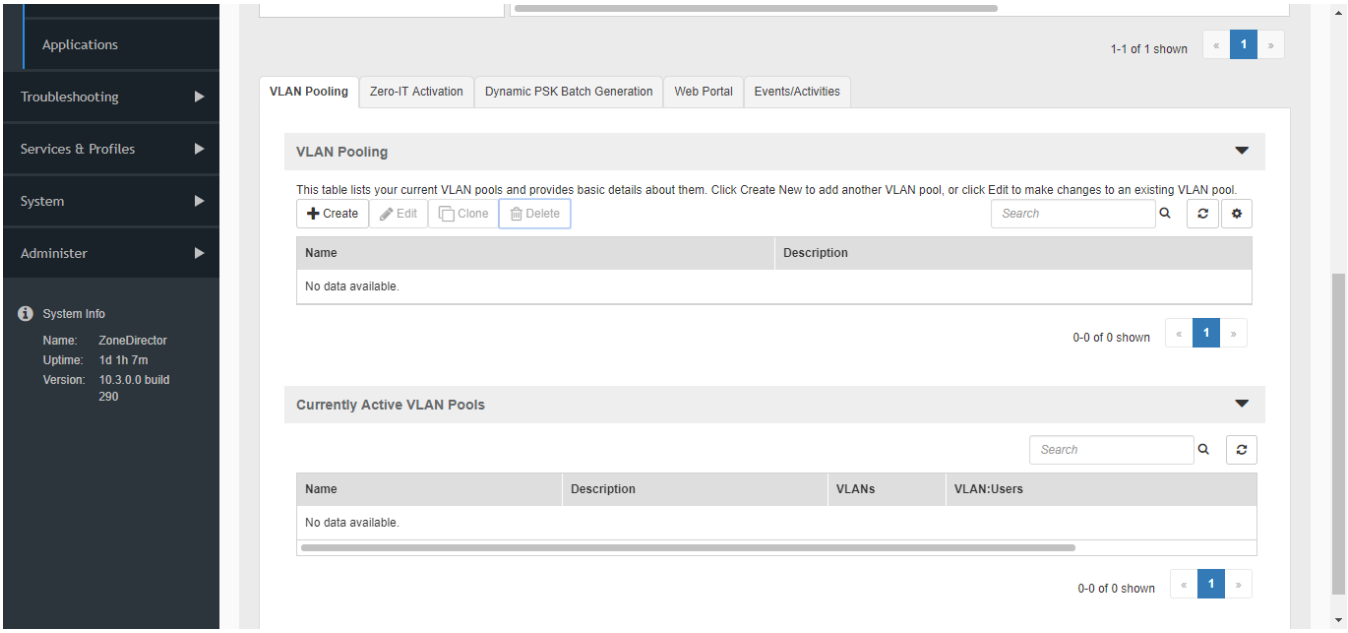
To address this problem, VLAN pooling allows administrators to deploy a pool of multiple VLANs to which clients are assigned, thereby automatically segmenting large groups of clients into multiple smaller subgroups, even when connected to the same SSID.

As the client device joins the WLAN, the VLAN is assigned to one of the VLANs in the pool based on a hash of the client's MAC address. While you can also achieve the same results using Dynamic VLAN with VLANs assigned by a RADIUS server (see How Dynamic VLAN Works on page 91), the VLAN pooling feature allows distribution of clients into multiple VLANs without the need for a RADIUS server.

To create a VLAN pool:

1. Go to **Wireless LANs**, and locate the **VLAN Pooling** section.
2. Click **Create** to create a new VLAN pool.

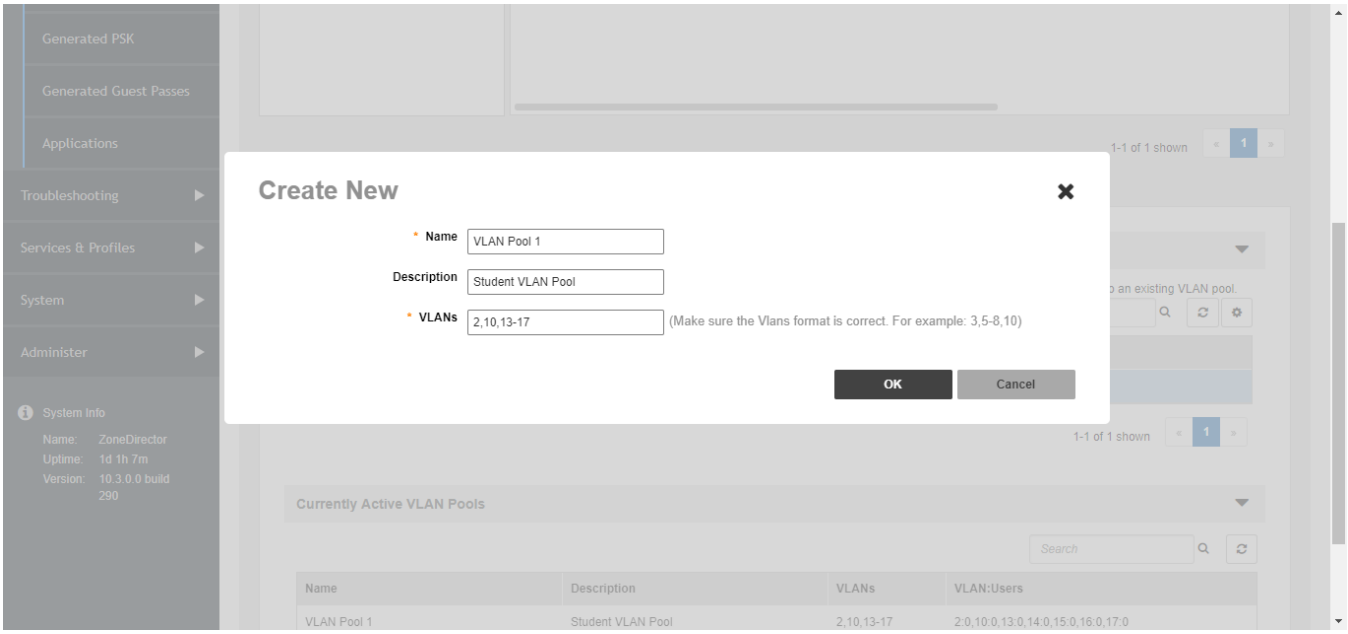
FIGURE 48 VLAN pooling



3. Enter a **Name**, and optionally a **Description** for this VLAN pool.
4. In VLANs, enter the VLAN IDs to be assigned to this pool. VLAN IDs can be separated by hyphens, commas, or a combination (e.g., 7-10, 13, 17, 20-28).

5. Click **OK** to save the VLAN pool. Each VLAN pool can contain up to 16 VLANs, and a maximum of 64 VLAN pools can be created. Each WLAN can be configured with a single VLAN pool.

FIGURE 49 Creating a VLAN pool

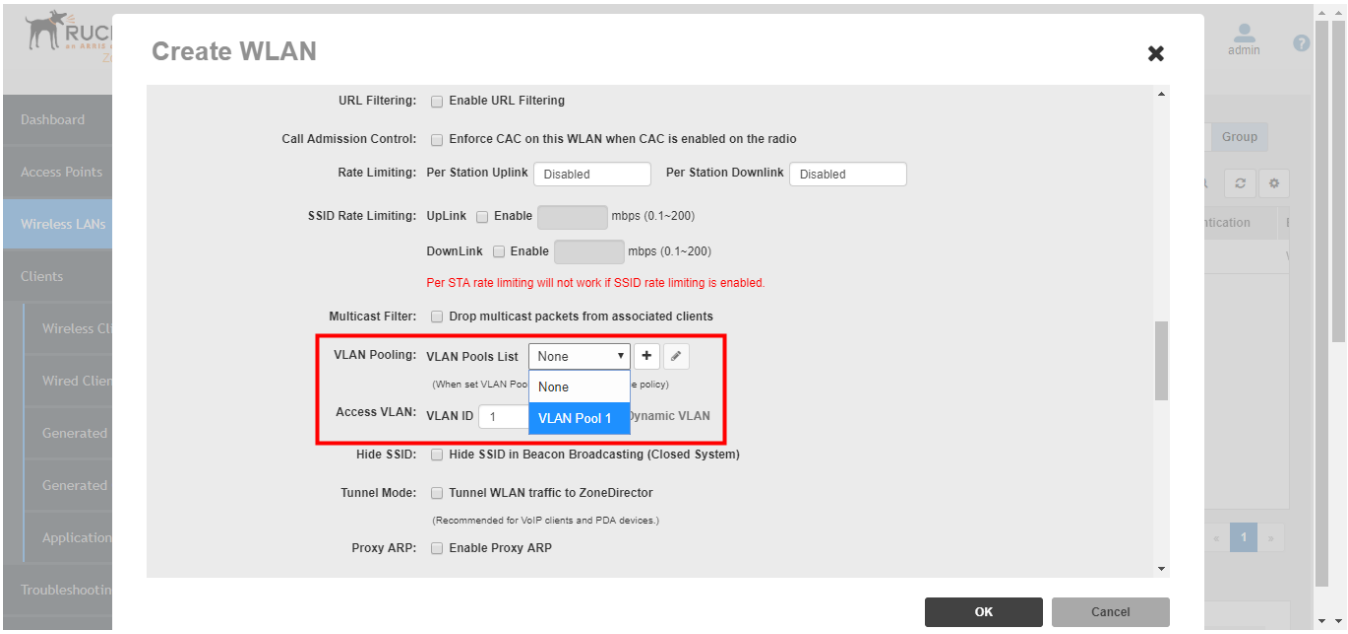


To assign a pool of VLANs to an SSID

1. Go to **Wireless LANs**.
2. Click **Create New** or **Edit** to create or edit a WLAN.
3. Expand the **Advanced Options** section, and locate the **VLAN Pooling** entry.
4. Select the VLAN Pool you created from the **VLAN Pools List**. Alternatively, you can create a new VLAN pool by clicking **Create New VLAN Pool**.

5. Click **OK** to save your changes. Clients connecting to this WLAN will now be automatically assigned to a VLAN from the specified VLAN pool.

FIGURE 50 Assign a VLAN Pool to a WLAN



NOTE
A VLAN pool cannot be applied to a WLAN with a Device Policy enabled, and vice-versa. If a Device Policy is selected, the VLAN Pooling option will automatically be disabled. If a VLAN pool is selected, the Access VLAN option will be disabled.

NOTE
VLAN Pooling has the lowest priority when used in conjunction with other VLAN assignment features. In case of conflict, the priority is as follows: 1) Role-Based Access Control (RBAC), 2) AAA Server, 3) Device Policy 4) VLAN Pooling.

For additional information on configuring VLANs for Access Point Ethernet ports, refer to Configuring AP Ethernet Ports on page 44.

Managing User Access

- Enabling Automatic User Activation with Zero-IT 97
- Working with Dynamic Pre-Shared Keys 101
- Adding New User Accounts to ZoneDirector 113
- Managing Current User Accounts 114
- Creating New User Roles 116
- Managing Generated Dynamic PSKs 119
- Managing Generated Guest Passes 120
- Using an External Server for User Authentication 120
- Enabling Web Authentication 122

Enabling Automatic User Activation with Zero-IT

Ruckus 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 Ruckus network is set up, you need only direct users to the Activation URL, and they will be able to automatically authenticate themselves to securely access your wireless LAN.

Before enabling Zero-IT, make sure you have at least one of each of the following configured:

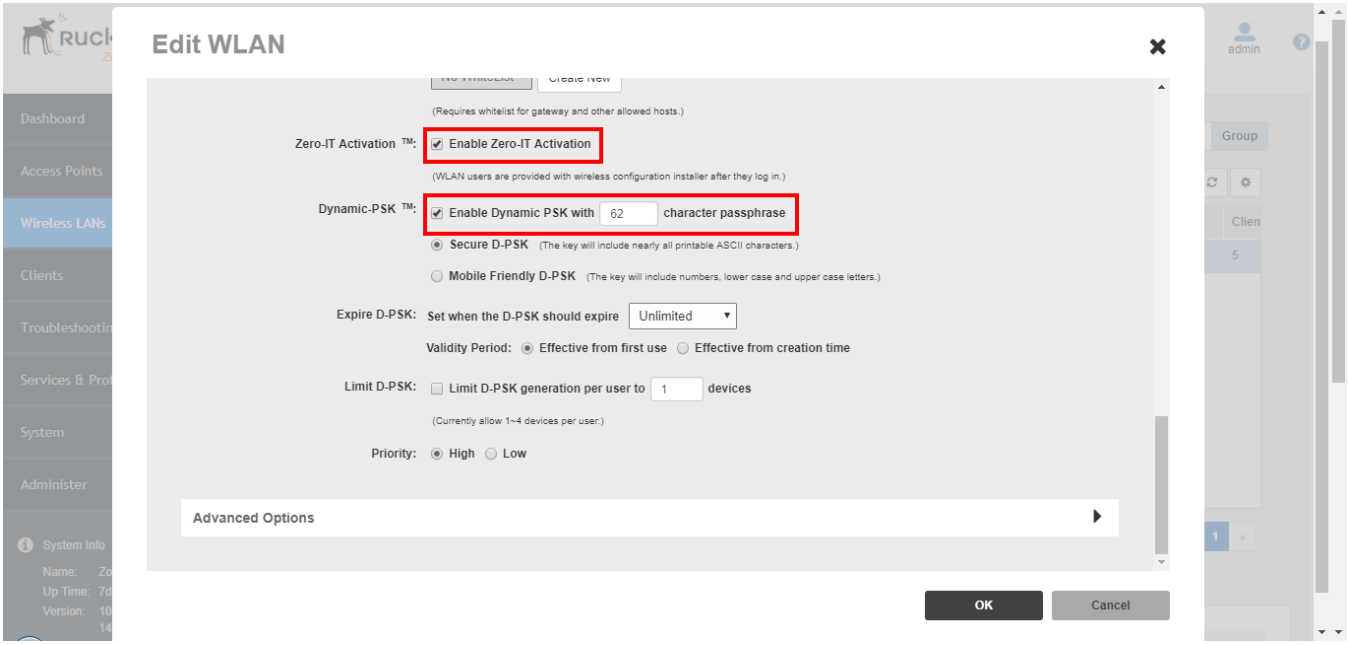
- A WLAN configured (*Wireless LANs*)
- A user Role with access to this WLAN (*Services & Profiles > Roles*)
- A User with this role assigned that exists in either the internal database or an external RADIUS, Active Directory or LDAP server (*Services & Profiles > Users*)

To enable Zero-IT activation, do the following:

1. Go to **Wireless LANs**.
2. Click **Edit** on the WLAN where you want to enable Zero-IT Activation.
3. Enable **WPA2** (not WPA3, WPA-Mixed, WPA2/WPA3-Mixed or OWE; selecting any of these encryption options will disable the Zero-IT option).
4. Enter a passphrase. (This passphrase will only be used for administrator testing - you will not need to provide this passphrase to end users.)
5. Enable **Zero-IT Activation**.
6. Optionally, enable **Dynamic PSK** if your WLAN's authentication and encryption methods support it (Open authentication and WPA2 encryption only; see Working with Dynamic Pre-Shared Keys on page 101 for more information.)
7. If the Authentication Method is 802.1X or MAC Address, select which **Authentication Server** to authenticate users against. If you are not using an external server for authentication, you can use ZoneDirector's internal database.
8. Note the **Activation URL** in the Zero-IT Activation section further down the page.

9. Click **OK** to save your settings.

FIGURE 51 Enabling Zero-IT for a WLAN



You have completed enabling Zero-IT for this WLAN. At this point, any user with the proper credentials (username and password) and running a supported operating system can self-provision his/her wireless client to securely access your wireless LANs.

Clients that Support Zero-IT

For a detailed list of the operating systems that the Zero-IT configuration supports, refer to the *ZoneDirector Release Notes*.

Zero-IT Activation can be used with many modern operating systems including Microsoft Windows (7/8/10), Apple OS X, Apple iOS, Windows Phone and Android OS.

For Windows 7/8/10 or Mac notebook clients with Ethernet ports, the user simply connects to the ZoneDirector activation URL and runs the self-activation script. For clients running Mac OS X, the user must be logged in as an administrator for Zero-IT activation to work.

Linux clients do not support automatic wireless configuration using the Zero-IT provisioning file.

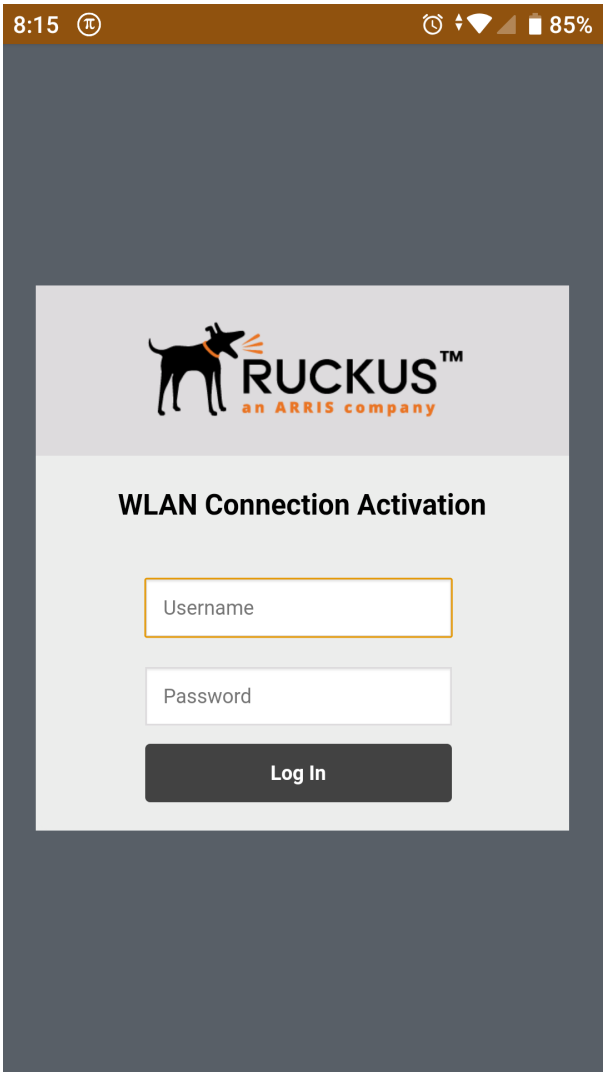
Self-Provisioning Clients with Zero-IT

To self-provision a computer to the wireless LAN, use the following procedure:

1. Connect the computer to the wired LAN using an Ethernet cable.
2. Open a browser and enter the Activation URL in the navigation bar (**http://<zonedirector's_IP_address>/activate**). A *WLAN Connection Activation* web page appears.

3. Enter **User Name** and **Password**, and click **OK**. If the user name and password are confirmed and the computer is running a supported operating system, an automated script will launch.

   FIGURE 52 Zero-IT automatic activation



4. Run the prov.exe script to automatically configure this computer's wireless settings for access to the secure internal WLAN.

5. If you are not running a supported operating system, you can manually configure wireless settings by clicking the link at the bottom of the page (see Provisioning Clients that Do Not Support Zero-IT on page 101).

FIGURE 53 Corporate WLAN configuration



You have completed Zero-IT configuration for this user. Repeat this procedure to automatically configure all additional users of your internal WLAN.

Self-Provisioning Clients without Ethernet Ports

Many mobile devices without Ethernet ports - such as smart phones and tablets - can also use Zero-IT Activation.

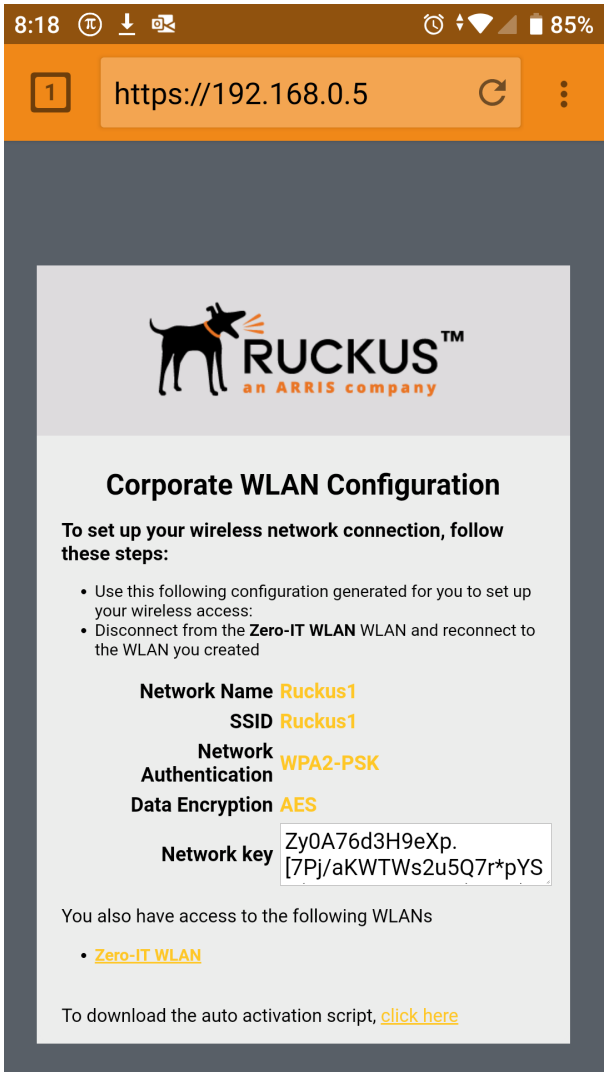
This is done using the "BYOD Onboarding Portal," which is described in Using the BYOD Onboarding Portal on page 144.

Provisioning Clients that Do Not Support Zero-IT

If your users are connecting with clients running earlier versions of Windows, Linux, or other operating systems that do not support Zero-IT provisioning, users must manually configure wireless settings.

A manual configuration page displays the settings needed for manual configuration.

FIGURE 54 Manual configuration information



Working with Dynamic Pre-Shared Keys

Dynamic PSK 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 Dynamic PSK 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.

Dynamic PSK offers the following benefits over standard PSK security:

- Every device on the WLAN has its own unique Dynamic PSK (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 also 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 the other devices which are encrypting their traffic with their own unique DPSKs.

DPSKs can be created in bulk and manually distributed to users and devices, or ZoneDirector can auto-configure each device with a unique DPSK when it connects to the network for the first time using Zero-IT Activation (see Enabling Automatic User Activation with Zero-IT on page 97).

Enabling Dynamic Pre-Shared Keys on a WLAN

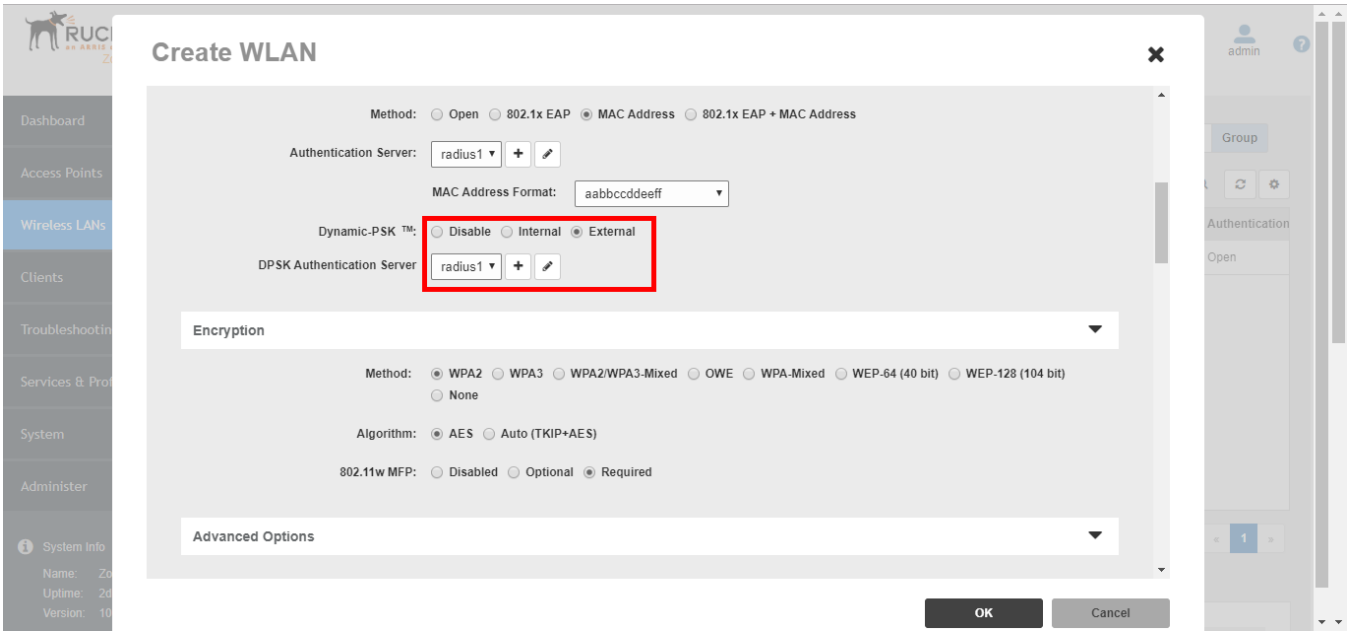
To use DPSK for client authentication, you must enable it for a particular WLAN (if you did not enable it during the initial ZoneDirector Setup Wizard process).

To enable DPSK for a WLAN:

1. Go to **Wireless LANs**.
2. Either **Edit** an existing WLAN or **Create New** to open the WLAN configuration form.
3. Under **Type**, select **Standard Usage**.
4. Under **Authentication Options: Method**, select **MAC Address** or **Open**.
5. Under **Encryption Options: Method**, select **WPA2** (not WPA-Mixed, WPA3, or WPA2/WPA3-Mixed, OWE, WEP-64, or WEP-128, as selecting any of these encryption methods will disable the DPSK option).
6. Under **Encryption Options: Algorithm**, select AES (not Auto, as selecting Auto will disable the DPSK option).
7. If using MAC Address authentication, choose an **Authentication Server** to authenticate clients against--either Local Database or RADIUS Server.
8. Next to **Dynamic-PSK**, select one of the following:
   - **Internal**: Use the internal database for client authentication.
   - **External**: Use an external AAA (RADIUS) server for client authentication.

9. If using an external RADIUS server for authentication, select the **DPSK Authentication Server** from the list, and click **OK** to save.

FIGURE 55 External DPSK



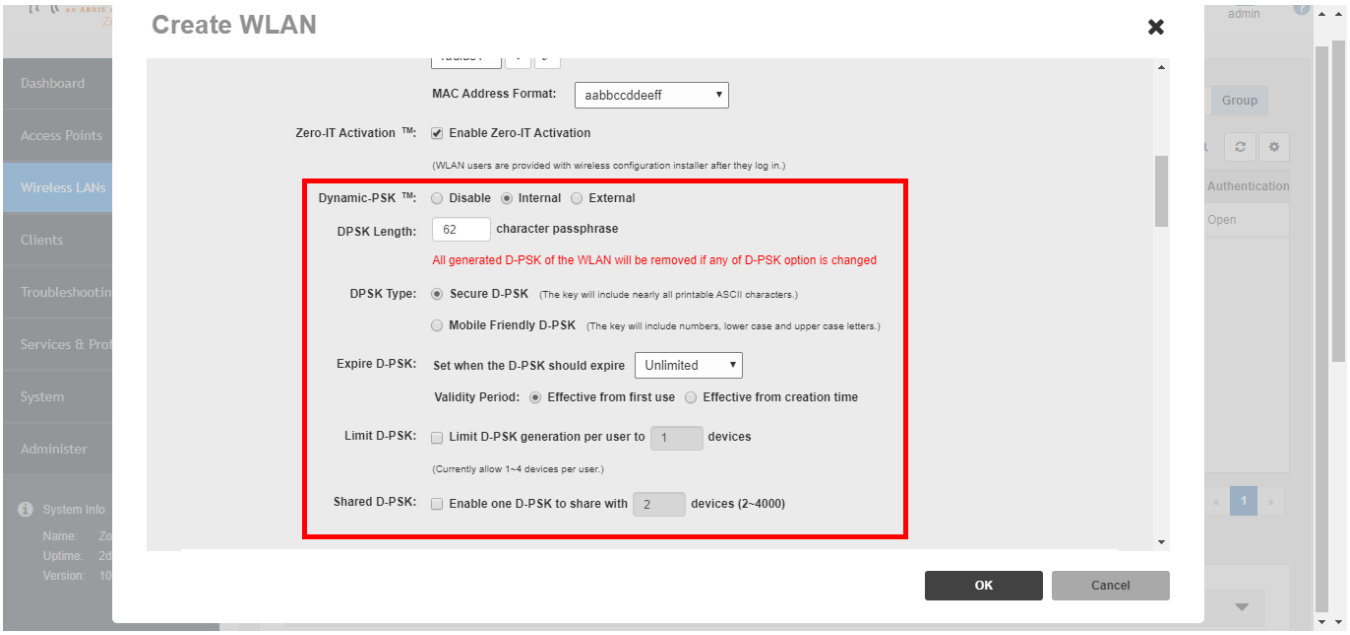
10. If using the internal database, continue with the following steps.
11. In **DPSK Length**, enter a DPSK passphrase length (between 8 and 62 characters).
12. In **DPSK Type**, choose whether to use **Secure DPSK** or **Mobile Friendly DPSK**:
    - **Secure DPSK**: Includes almost all printable ASCII characters, including periods, hyphens, dashes, etc. This option is more secure, however it is difficult to input for mobile clients whose keyboards may not contain the entire set of printable ASCII characters.
    - **Mobile Friendly DPSK**: Choose this option if this WLAN will be used primarily for mobile clients. This option limits the range of characters to lower case and upper case letters and numbers, which makes it easier for users to input the DPSK when activating a mobile client to a Zero-IT WLAN. (You may also want to limit the DPSK length to 8 characters for the convenience of your mobile client users.)
13. In **Expire DPSK**, set when the DPSK should expire. In **Validity period**, choose whether the DPSK expiration period will start from first use or creation time.

    NOTE
    The DPSK expiration date is calculated in number of hours. Therefore, one day = 24 hours; one week = 7 days; two weeks = 14 days; one month = 30 days; two months = 60 days; three months = 90 days; half a year = 182.5 days; one year = 365 days.

14. In **Limit DPSK**, enable the check box and enter a number to limit the number of DPSKs that can be generated per user. By default, each authenticated user can generate multiple DPSKs. Select this option to limit the number of DPSKs each user can generate (1-4).
15. In **Shared DPSK**, 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. This option allows admins to override this rule and allow a user to share a single DPSK across multiple devices.

16. Click **OK** to save your settings.

FIGURE 56 Enabling Dynamic PSK for a WLAN



This WLAN is now ready to authenticate users using Dynamic Pre-Shared Keys once their credentials are verified against either the internal database or an external AAA server.

Using External DPSK with RADIUS Authentication

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

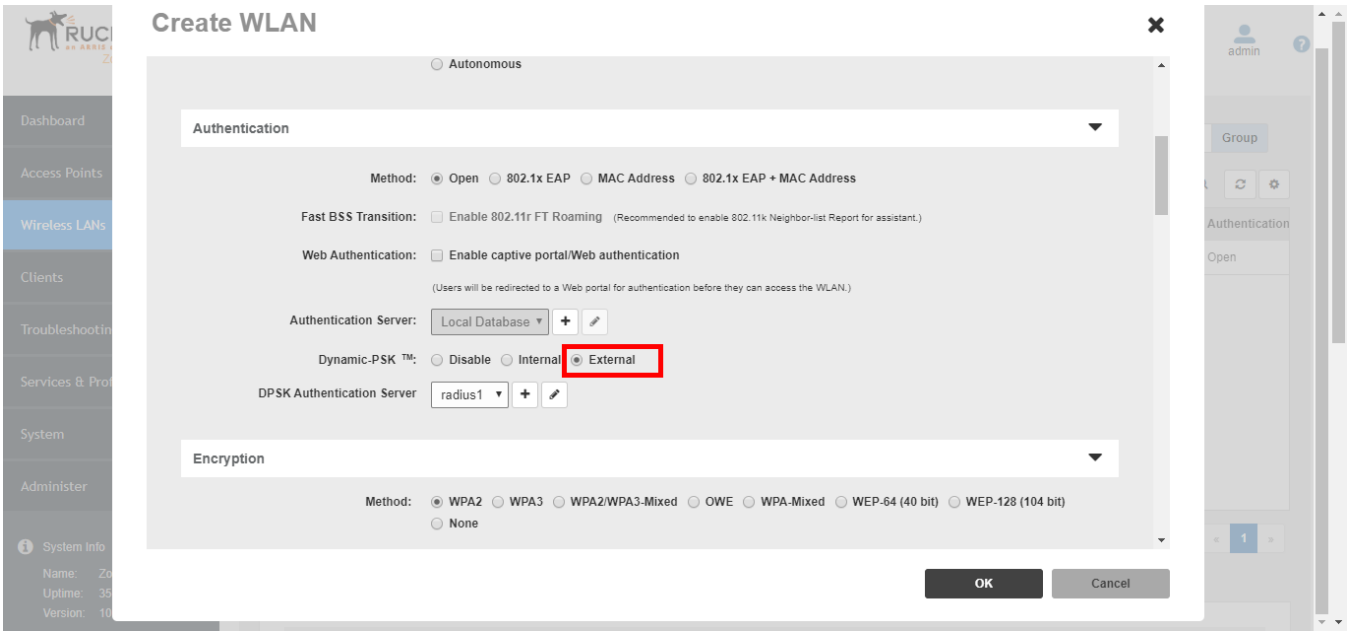
The external DPSK feature allows customers to exceed the maximum number of DPSKs that can be stored on the controller, and provides the option to store and manage DPSKs on the AAA server for distribution to multiple controllers.

To enable external DPSK using an external authentication server:

1. Go to **Wireless LANs > Create/Edit WLAN**.
2. Select **Standard Usage** for *Type*, and select **WPA2** for *Method*.
3. In **Dynamic PSK**, select **External**.
4. In **Authentication Server**, select or create an AAA server entry.

5. Click **OK**.

FIGURE 57 External DPSK



6. The controller will send `Access-Request` messages to the RADIUS server with following attributes: `Ruckus-SSID, Ruckus-BSSID, User-Name, Ruckus-Dpsk-Params`.
7. 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.
8. The AAA server generates a DPSK key (PMK) for each wireless station. This key is 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.

9. 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.
10. 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 17 Access-Request message parameters

	Parameter	AVP / VSA name	Comment
1	SSID	Ruckus-SSID	Since DPSK passphrases are bound to SSIDs, it's expected that AAA server will have the PMK lists indexed by SSID value.
2	UE's MAC address	User-Name	This AVP chosen for backward compatibility with MAC Authentication use case. The AAA server can override this value with a real (human or account) user-name when User-Name AVP is included in an Access-Accept or Access-Reject message.
3	AP's BSSID	Ruckus-BSSID	Note: the AAA Interface Document needs to be updated. Currently it states, "BSSID for each WLAN in each radio"; however, only a single BSSID (the one the client has associated with) is included in the VSA.
4	Anonce	Ruckus-DPSK-params	This is a new Ruckus VSA, defined below.
5	Snonce	Ruckus-DPSK-params	The Snonce is parsed from the EAPOL Key Frame field of Ruckus-dpsk-params.
6	MIC	Ruckus-DPSK-params	The MIC is parsed from the EAPOL Key Frame field of Ruckus-dpsk-params.
7	4WHS-M2 EAPOL Key frame	Ruckus-DPSK-params	The EAPOL-Key-Frame is used for the MIC calculation.
8	Cipher	Ruckus-DPSK-params	If the UE has negotiated TKIP-based encryption (this would be a really old device), then the key integrity algorithm is different than AES (Advance Encryption Standard, the encryption algorithm currently in use). In this case, AAA server also has to use the same algorithm as the UE in order to properly identify the PMK. TKIP is indicated according to the Cipher octet (see below). Note that two different integrity algorithms are used: HMAC-SHA1 ands HMAC-MD5.
9	AKM Suite	Ruckus-DPSK-params	The use of the AES key integrity and key hierarchy is indicated by the AKM Suite value. If the UE has negotiated FT encryption (FT - fast transition, aka 802.11r), generating the PTK from the PMK uses a different algorithm than AES. In this case, AAA server also has to use the same algorithm as the UE in order to properly identify the PMK. The AKM Suite value indicates whether FT is used.

The following parameters are used in access-accept/access-reject messages.

TABLE 18 Access-accept/Access-reject message parameters

	Parameter	RADIUS AVP or VSA name	Mandatory / Optional	Comment
1	MS-MPPE-Recv-Key	MS-MPPE-Recv-Key	Mandatory	Included whenever the AAA server has found a matching PMK (for either bound or unbound case).
2	PMK-time	Session-Timeout	Mandatory	Included whenever the AAA server has found a matching PMK, this is PMK expired time for the controller. Its range could be 0-14400 minutes.
3	User-name	User-name	Optional	Included if admin desires the username to be included in syslog events generated by the controller.

TABLE 18 Access-accept/Access-reject message parameters (continued)

4	VLAN assignment	The following triplet of AVPs: 1. Tunnel-Type 2. Tunnel-Medium-Type 3. Tunnel-Private-Group-Id	Optional	Included if admin requires dynamic VLAN assignment. Note: the Tag field in all three AVPs is set to the same value (see RFC-2868). 1. Tunnel-Type is set to the value "VLAN". Note: the AVP encodes this enumeration as an integer set to the value of 13 (see RFC-3580). 2. Tunnel-Medium-Type is set to the string value of "802" 3. Tunnel-Private-Group-Id is set to the value "<VLAN ID>". VLAN ID has a value between 1 and 4094 and is encoded as a string (see RFC-3580).
5	Ruckus-User-Groups	Ruckus-User-Groups	Optional	Ruckus-User-Groups is used as Role of UE, It is the same as "Group Attributes " in ZD WebUI Configuration "Roles and Policies ".
6	Authorization reason	Reply-message	Optional	Included if AAA server sends an Access-Accept in the workflow for DPSK passphrase renewal. When included, the ZD shall copy the contents of this AVP to the relevant syslog message (event ID 206 clientAuthorization).

Setting Dynamic Pre-Shared Key Expiration

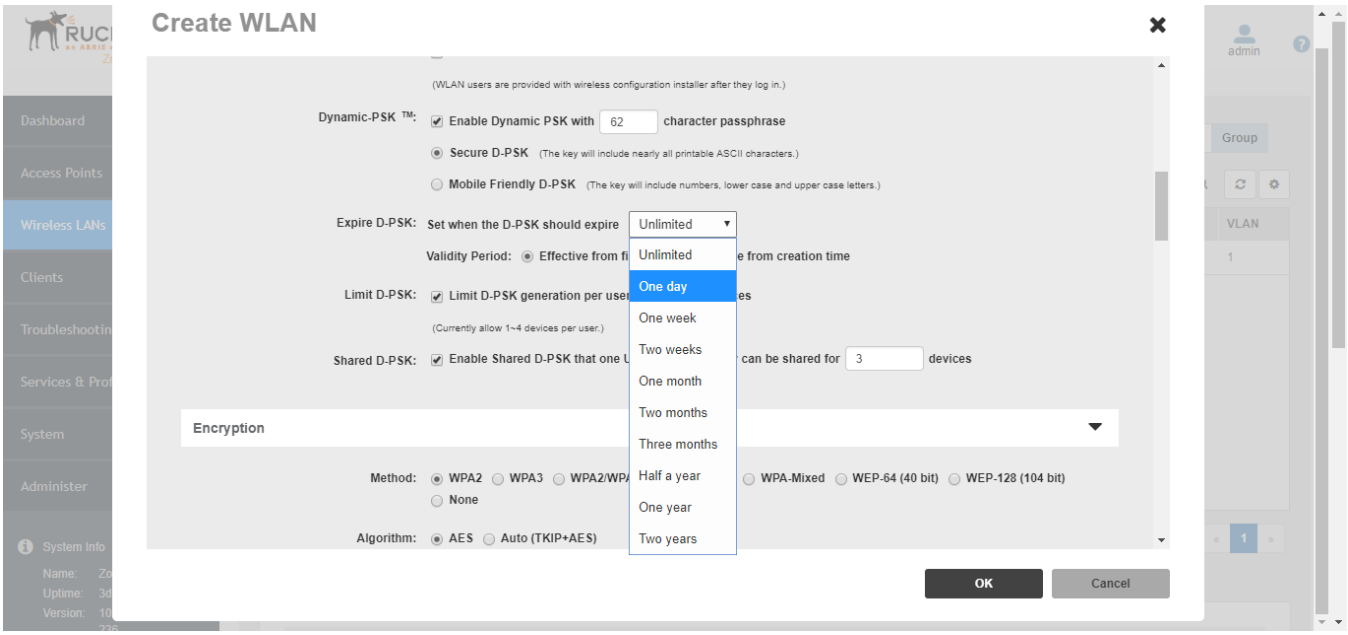
By default, dynamic pre-shared keys do not expire and are effective from first use. You can control when the PSK expires, at which time the users will be prompted to reactivate their wireless access.

To set the dynamic PSK expiration:

1. Go to **Wireless LANs**, and click **Edit** to modify your DPSK WLAN.
2. Expand the **Advanced Options** and locate the **Dynamic PSK** section.
3. In the **Expire DPSK** section, select the PSK expiration time. Range includes one day to unlimited (never expires).
4. In **Validity Period**, select **Effective from first use** or **Effective from creation time**.

5. Click **OK** to save your changes. The new setting goes into effect immediately.

FIGURE 58 Dynamic PSK expiration options



NOTE
If you change the dynamic PSK expiration period, the new expiration period will only be applied to new DPSKs. Existing DPSKs will retain the expiration period that was in effect when the DPSKs were generated. To force expiration, go to *Clients* > *Generated PSK/Certs*.

Generating Multiple Dynamic PSKs

If you will be generating DPSKs frequently (for example, to configure school-owned laptops in batch), you may want to generate multiple DPSKs at once and distribute them to your users in one batch.

Before performing this procedure, check your WLAN settings and make sure that the Dynamic PSK check box is selected.

To generate multiple dynamic PSKs:

1. Go to **Wireless LANs**.
2. Scroll down and click the **Dynamic PSK Batch Generation** tab.
3. In **Target WLAN**, select one of the existing WLANs with which the users will be allowed to associate. (Only WLANs with DPSK enabled will be listed.)
4. In **Number to Create**, select the number of dynamic PSKs that you want to generate. ZoneDirector will automatically populate the names of each user (BatchDPSK_User_1, BatchDPSK_User_2, and so on) to generate the dynamic PSKs.
5. In **Role**, select the Role you want to apply to this batch of DPSK users.
6. In **Dynamic VLAN ID**, enter Dynamic VLAN ID (if Dynamic VLAN is enabled for this WLAN).
7. If you want to be able to identify the dynamic PSK users by their names, click **Choose File**, and upload a batch dynamic PSK profile instead. See Creating a Batch Dynamic PSK Profile on page 110 for more information.

8. Click **Generate**. ZoneDirector generates the dynamic PSKs, and then the following message appears:

   To download the latest DPSK record generated from this page, "click here."

9. Click the**click here** link in the message to download a CSV file that contains the generated dynamic PSKs.

You have completed generating the dynamic PSKs for your users. Using a spreadsheet application (for example, Microsoft Excel), open the CSV file and view the generated dynamic PSKs.

The CSV file contains the following columns:

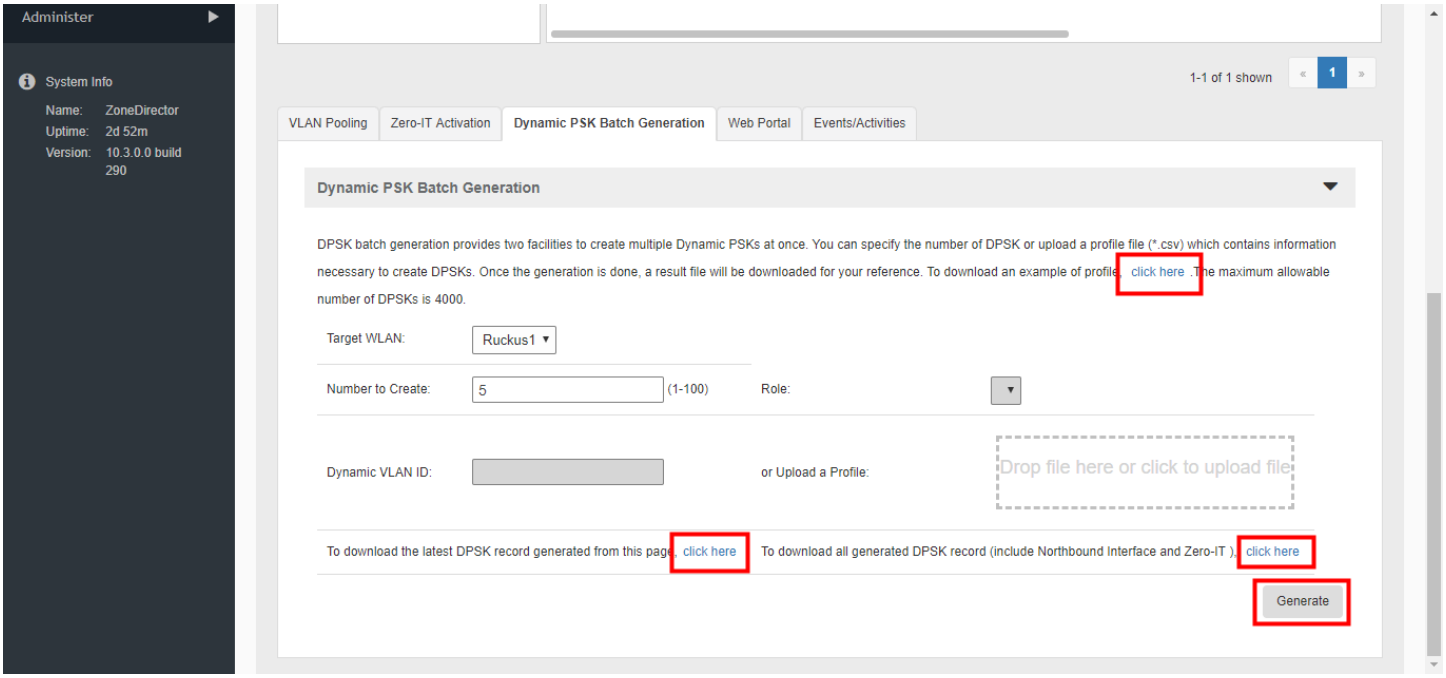
- User Name
- Passphrase
- Role
- WLAN Name
- MAC Address
- VLAN ID
- Expiration

  NOTE
  The MAC address column shows 00:00:00:00:00:00 for all users. When a user accesses the WLAN using the dynamic PSK that has been assigned to him, the MAC address of the device that he used will be permanently associated with the dynamic PSK that he used.

To enable wireless users to access the wireless network, you need to send them the following information:

- **User Name**: The user name generated via batch DPSK generation (by default, “Batch_DPSK_User_[#]”.
- **WLAN Name**: This is the WLAN with which they are authorized to access and use the dynamic PSK passphrase that you generated.
- **Passphrase**: This is the network key that the user needs to enter on his WLAN configuration client to access the WLAN.
- **Expiration**: (Optional) This is the date when the DPSK passphrase will expire. After this date, the user will no longer be able to access the WLAN using the same DPSK

FIGURE 59 DPSK batch generation



NOTE
Alternatively, you can allow users to automatically self-provision their clients using Zero-IT, as described in Enabling Automatic User Activation with Zero-IT on page 97.

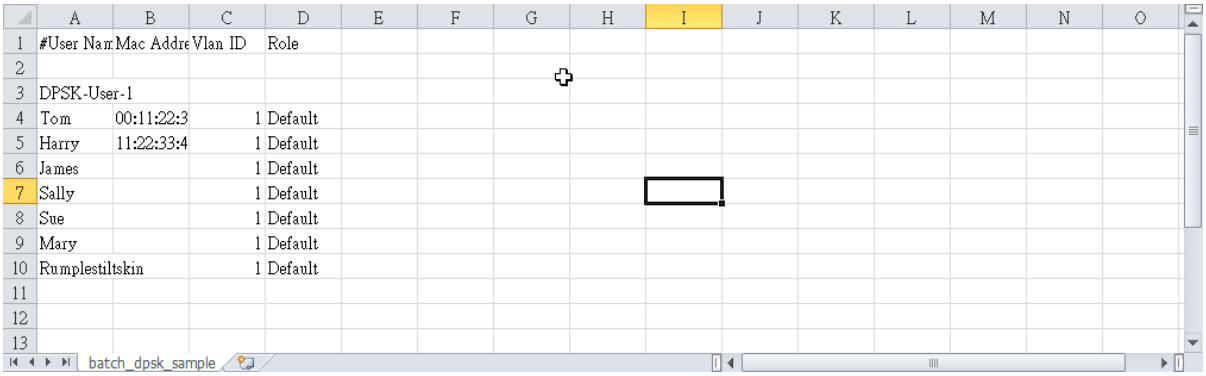
Creating a Batch Dynamic PSK Profile

Creating a DPSK batch generation profile is useful if you want to customize the user names that will be used for accessing the DPSK WLAN, as opposed to user names such as "BatchDPSK_User_1," etc.

1. Go to **Wireless LANs**.
2. Click the **Dynamic PSK Batch Generation** tab, look for the following message: **To download an example of profile, click here.**
3. Click the **click here** link to download a sample profile.
4. Save the sample batch DPSK profile (in CSV format) to your computer.

5. Using a spreadsheet application, open the CSV file and edit the batch dynamic PSK profile by filling out the following columns:
   - **User Name**: (Required) Type the name of the user (one name per row).
   - **MAC Address**: (Optional) If you know the MAC address of the device that the user will be using, type it here.

   FIGURE 60 Editing the batch_dpsk_sample.csv file to create a custom batch DPSK profile



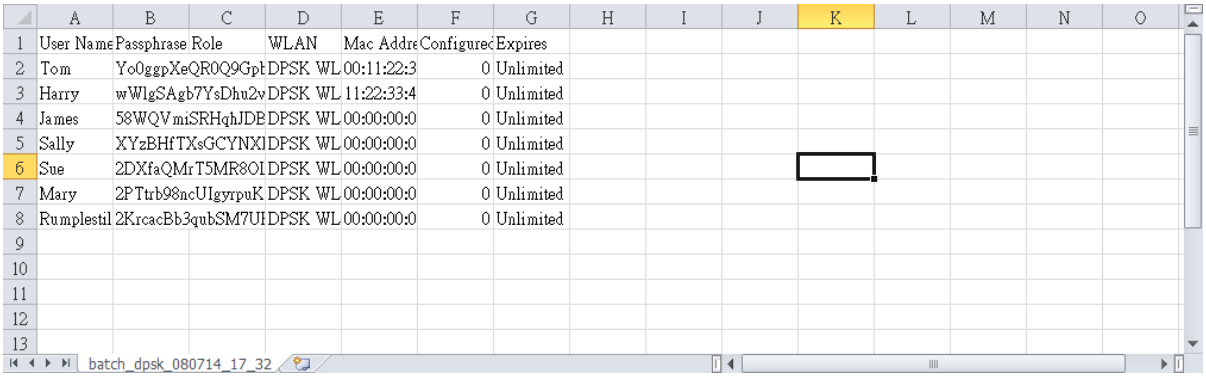
	A	B	C	D
1	#User Nam	Mac Addre	Vlan ID	Role
2				
3	DPSK-User-1			
4	Tom	00:11:22:3	1	Default
5	Harry	11:22:33:4	1	Default
6	James		1	Default
7	Sally		1	Default
8	Sue		1	Default
9	Mary		1	Default
10	Rumplestiltskin		1	Default
11				
12				
13				

batch_dpsk_sample

6. Go back to the **Dynamic PSK Batch Generation** page and drop the file you edited into the field provided to upload.
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) by clicking the **Click Here** link at the end of the "To download the generated DPSK record, click here" sentence.

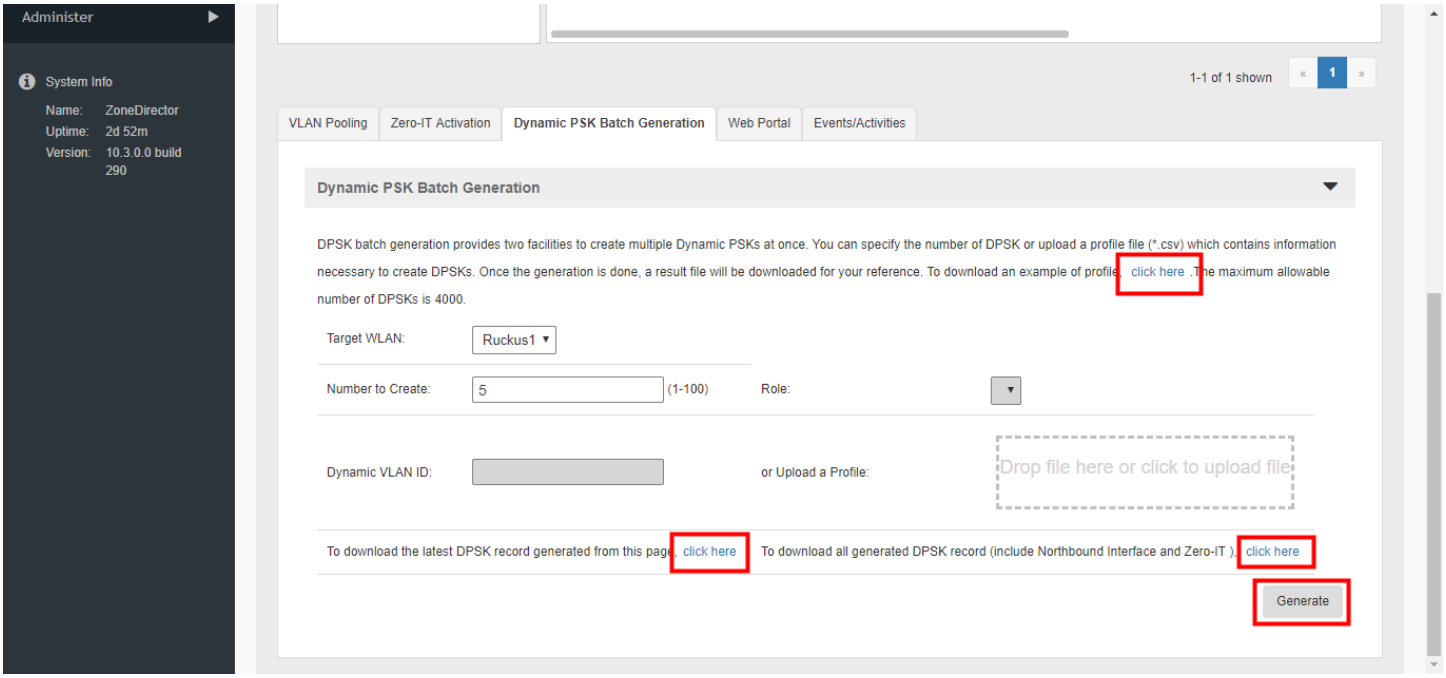
FIGURE 61 Downloading a generated batch DPSK profile



	A	B	C	D	E	F	G
1	User Name	Passphrase	Role	WLAN	Mac Addre	Configurec	Expires
2	Tom	Yo0ggpXeQR0Q9Gpt		DPSK WL	00:11:22:3	0	Unlimited
3	Harry	wWlgSAgb7YsDhu2v		DPSK WL	11:22:33:4	0	Unlimited
4	James	58WQVmiSRHqhJDE		DPSK WL	00:00:00:0	0	Unlimited
5	Sally	XYzBHfTXsGCYNXI		DPSK WL	00:00:00:0	0	Unlimited
6	Sue	2DXfaQMrT5MR8OI		DPSK WL	00:00:00:0	0	Unlimited
7	Mary	2PTtrb98ncUIgyrpuK		DPSK WL	00:00:00:0	0	Unlimited
8	Rumplestil	2KrcacBb3qubSM7UI		DPSK WL	00:00:00:0	0	Unlimited
9							
10							
11							
12							
13							

batch_dpsk_080714_17_32

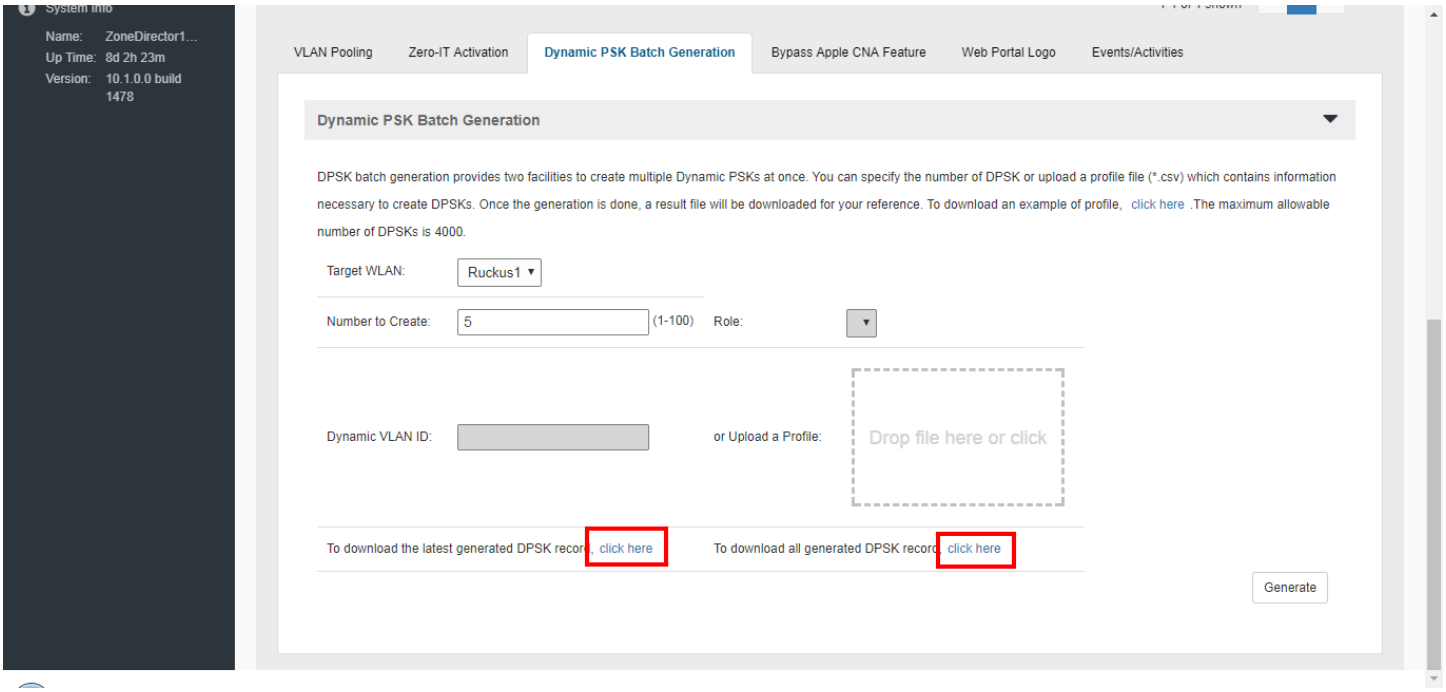
FIGURE 62 DPSK batch generation



Downloading Generated DPSKs

Once Dynamic PSKs have been generated, you can download either the latest batch generated or the entire list of generated DPSKs that currently exists on ZoneDirector.

FIGURE 63 Click either link to download latest/all generated DPSKs



Adding New User Accounts to ZoneDirector

Once your wireless network is set up, you can instruct ZoneDirector to authenticate wireless users using an existing Active Directory, LDAP or RADIUS server, or to authenticate users by referring to accounts that are stored in ZoneDirector's internal user database.

This section describes the procedures for managing users using ZoneDirector's internal user database. For authentication using an external AAA server, see Using an External AAA Server on page 248.

Internal User Database

To use the internal user database as the default authentication source and to create new user accounts in the database:

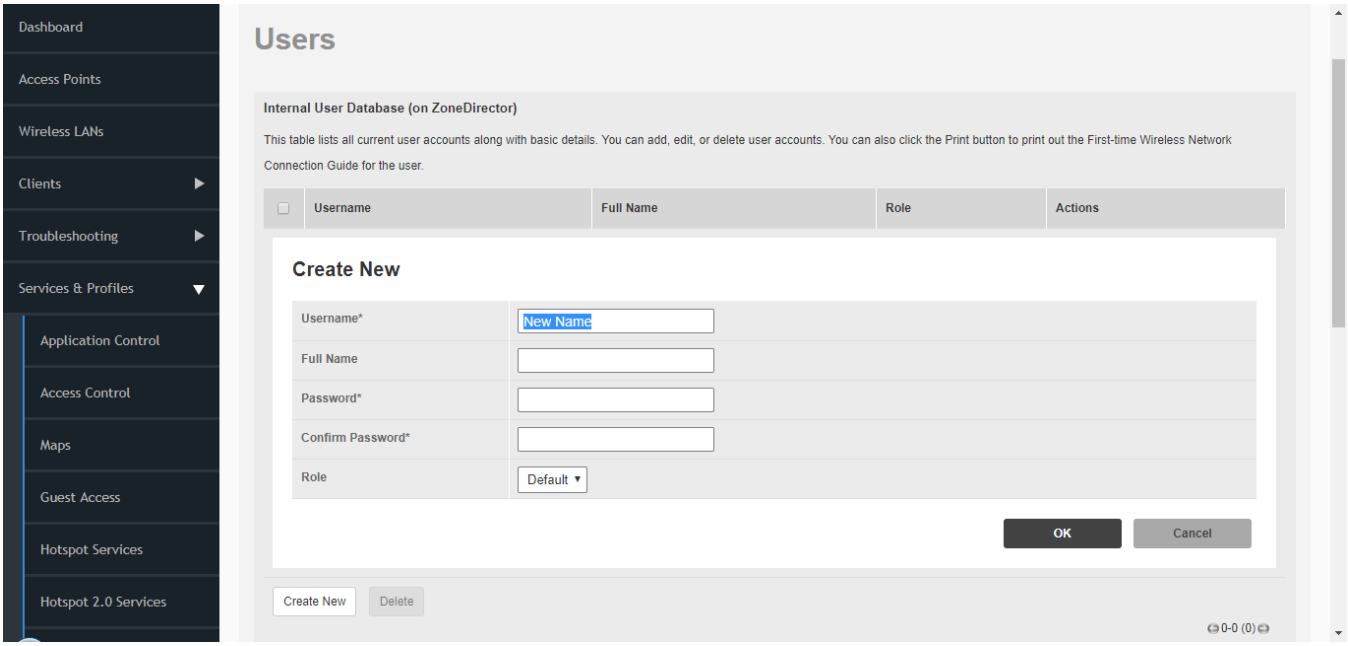
1. Go to **Services & Profiles** > **Users**.
2. In the **Internal User Database** table, click **Create New**.

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.

     NOTE
     ZoneDirector 1200 can support up to 4,000 DPSK users and guest passes, and up to 4,000 concurrently connected clients. When the maximum number of users that ZoneDirector supports has been reached, additional clients attempting to connect will be refused.

4. If you have created roles that enable non-standard client logins or that gather staff members into workgroups, open the **Role** menu, and then choose the appropriate role for this user. For more information on roles and their application, see Creating New User Roles on page 116.
5. Click **OK** to save your settings. Be sure to communicate the user name and password to the appropriate end user.

FIGURE 64 The Create New form for adding users to the internal database



Managing Current User Accounts

ZoneDirector allows you to review your current user roster on the internal user database and to make changes to existing user accounts as needed.

Refer to the following for more information:

- *Changing an Existing User Account*

- *Deleting a User Record*

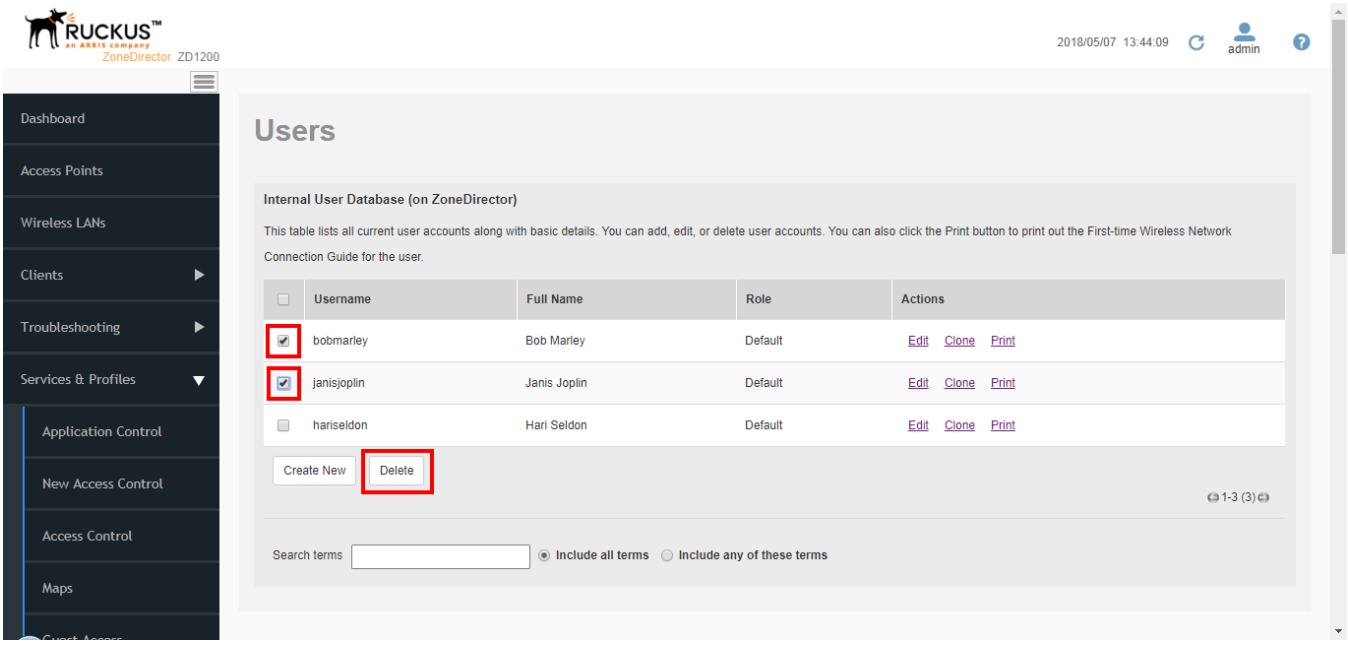
Changing an Existing User Account

1. Go to **Services & Profiles** > **Users**
2. On the *Users* page, select the specific user account in the **Internal User Database** panel, and then click **Edit**.
3. When the **Editing [user name]** form appears, make the needed changes.
4. If a role must be replaced, open that menu and choose a new role for this user. (For more information, see Creating New User Roles on page 116.)
5. Click **OK** to save your settings. Be sure to communicate the relevant changes to the appropriate end user.

Deleting a User Record

1. Go to **Services & Profiles** > **Users**.
2. When the *Users* screen appears, review the *Internal User Database* table.
3. To delete one or more records, select those account records.
4. Click the now-active **Delete** button.
5. When the **Deletion Confirmation** dialog box appears, click **OK** to save your settings. The records are removed from the internal user database.

FIGURE 65 Deleting a user record from the internal user database



Creating New User Roles

ZoneDirector 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 **Services & Profiles** > **Roles**. The **Roles and Policies** page appears, displaying a Default role in the Roles table.
2. Click **Create New** (below the Roles table).
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 or LDAP server (see Group Extraction on page 253). Enter the User Group name here. Active Directory/LDAP users with the same group attributes are automatically mapped to this user role.

     NOTE
     For information on how to authenticate administrators using an external authentication server, refer to Using an External Server for Administrator Authentication on page 332.

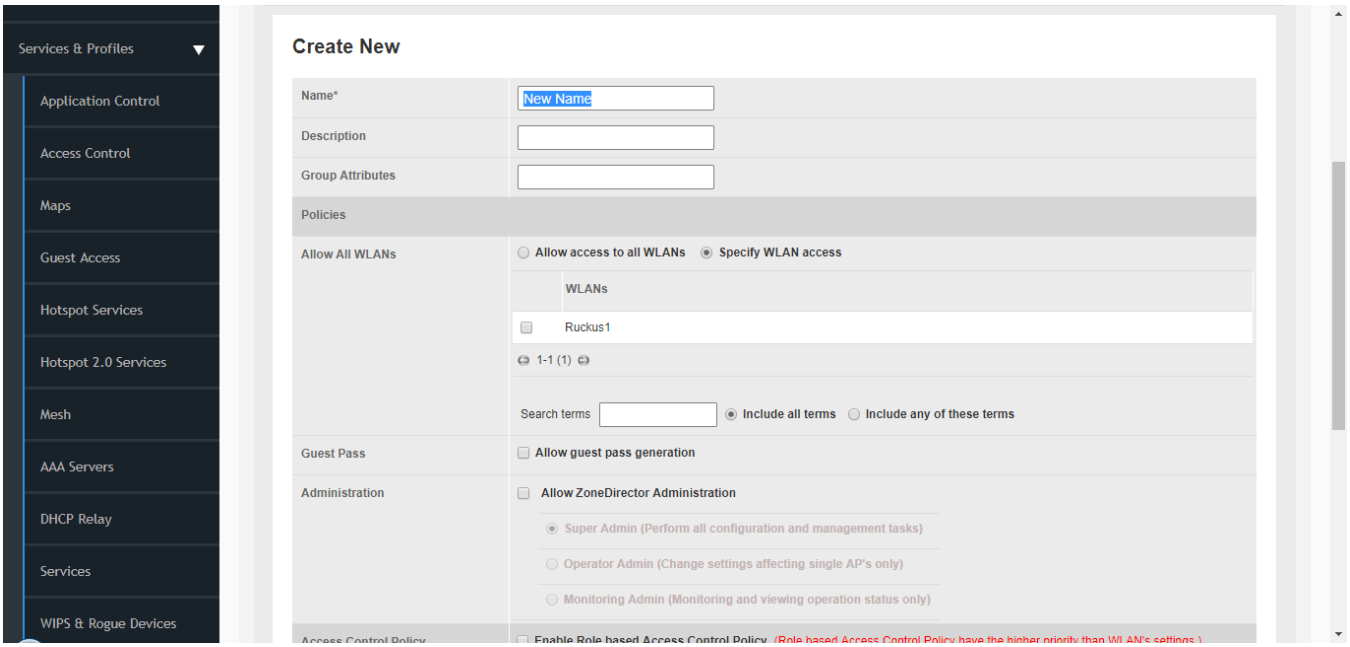
   - **Allow All WLANs**: You have two options: (1) Allow Access to all WLANs, or (2) Specify WLAN Access. If you select the second option, you must specify the WLANs by clicking the check box next to each one. This option requires that you create WLANs prior to setting this policy. See Creating a Wireless LAN on page 65.
   - **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. If you create a Role and allow guest pass generation, but do not allow the Role access the relevant WLAN, members of the "Guest Pass Generator" Role will still be unable to generate guest passes for the Guest WLAN.

   - **Administration**: This option allows you to create a user role with ZoneDirector administration privileges - either full access or limited access.
   - **Access Control Policy**: Enforce an access control policy on members of this role. See Role Based Access Control Policy on page 117.
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 66 The Create New form for adding a role



Role Based Access Control Policy

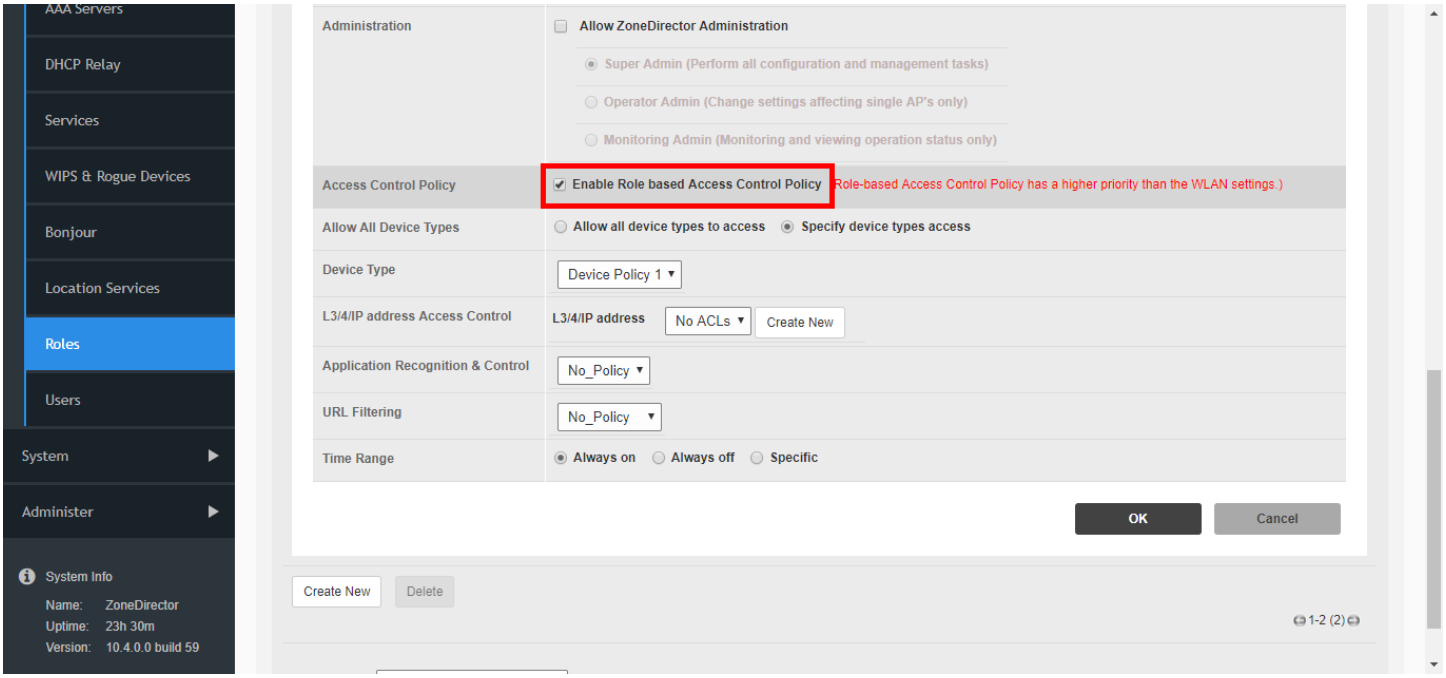
Using the Role Based Access Control Policy (RBAC) feature, organizations can deploy a single SSID for multiple roles, and provide different access privileges based on the user's role in the organization.

For example, a school could create a single secure WLAN for both students and staff members. Then, when either type of user connects to the network, they will be granted the proper access privileges based on their role at the school.

Users created on an AAA server can be mapped to roles on ZoneDirector using group attributes. When a client completes authentication successfully, ZoneDirector gets the group attributes assigned to this user from the AAA server and uses the group attributes to determine the user's role, and applies the access control restrictions defined in that role to the client's access privileges.

NOTE
When RBAC is enabled on a WLAN, Client Fingerprinting must be enabled, and Dynamic VLAN should also be enabled if VLANs will be assigned based on user roles.

FIGURE 67 Enabling RBAC policy for a role



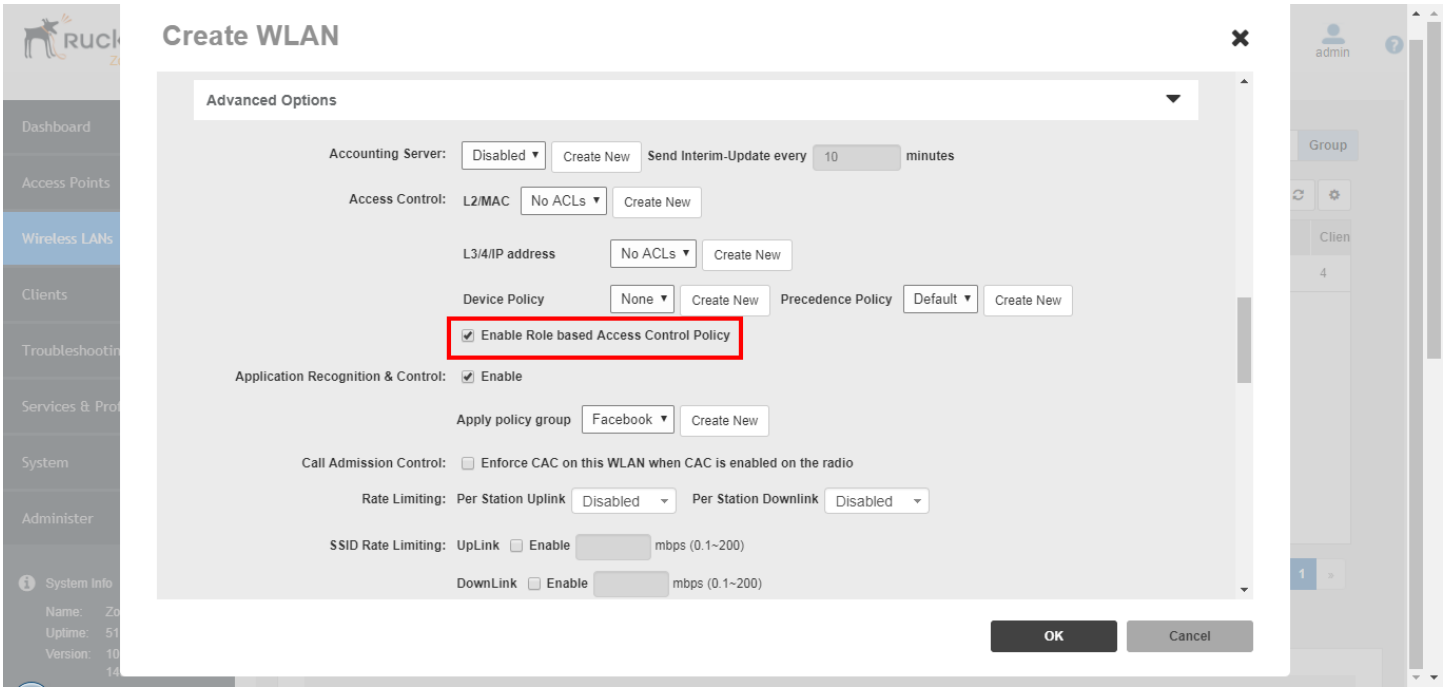
RBAC Policy Options

The following control policies can be applied to a role:

- **Device type**: Limit access based on operating system/device type.
- **VLAN**: Assign a VLAN ID to this role.
- **Rate Limiting**: Limit per-station uplink and downlink speeds.
- **L3/L4/IP address ACL**: Apply a Layer 3/Layer 4/IP address ACL to this role.
- **Application Recognition & Control**: Apply an application policy to this role.
- **Time Range**: Limit the time range during which this role will be allowed to access the WLAN.

Once you have created access control policies for your user roles, you will need to apply them to any WLANs for which you want to enforce these policies. To do this, edit the WLAN, expand the **Advanced Options**, and enable the check box next to **Enable Role Based Access Control Policy** in the **Access Control** section.

FIGURE 68 Enable RBAC policy enforcement for a WLAN



NOTE
When role-based application recognition and control (ARC) policies and WLAN-based ARC policies both exist, role-based ARC takes priority. If an application policy is available based on RADIUS attributes, then RADIUS group attributes take priority. In other words, the priority is: *RADIUS attribute* > *Role* > *WLAN*.

Managing Generated Dynamic PSKs

With Ruckus Dynamic PSK, a unique key is automatically generated for each wireless user. If a user leaves the organization, you can manually delete the DPSK using the *Clients* > *Generated PSK* page.

To delete generated DPSKs:

1. Go to **Clients** > **Generated PSK**.
2. Select the check boxes for the DPSKs that you want to delete.
3. Click **Delete** to delete the selected items.

The selected PSKs are deleted from the system. A user with a deleted PSK will not be able to connect to the wireless network without obtaining a new key.

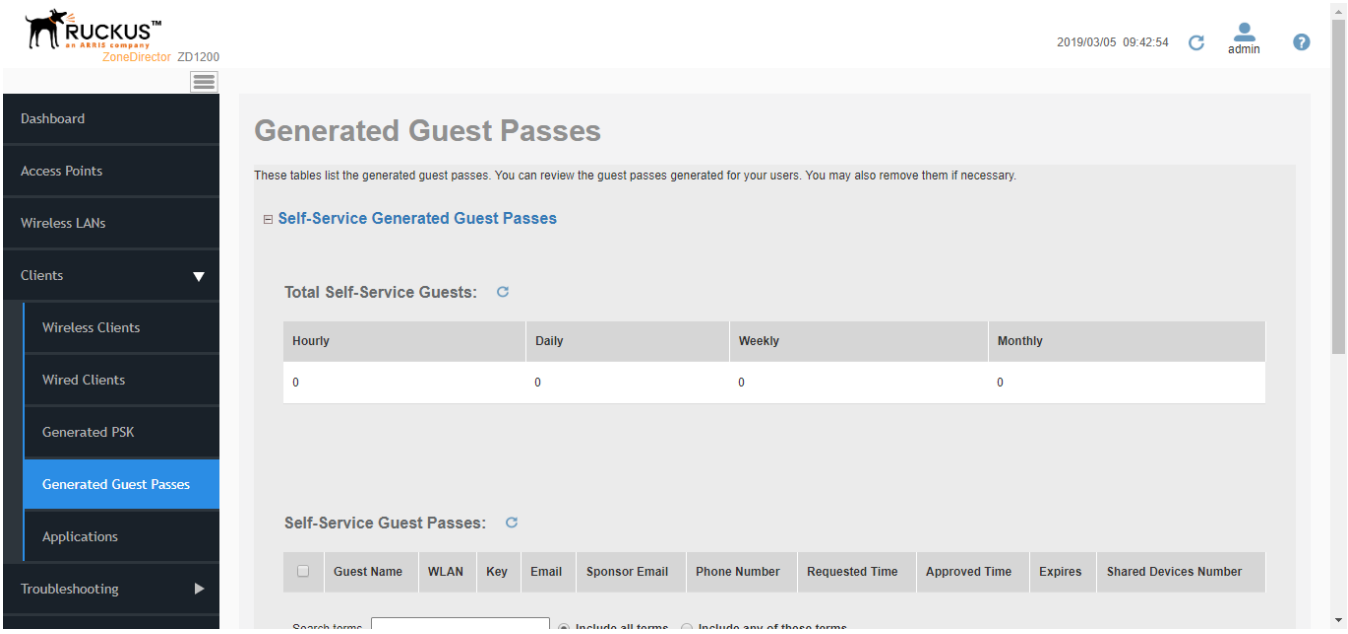
Managing Generated Guest Passes

Generated Guest Passes can be deleted using the *Clients > Generated Guest Passes* page. This page also provides the option to download a list of generated guest passes to CSV file.

To manage admin-generated or self-service guest passes, use the following procedure:

1. Go to **Clients > Generated Guest Passes**.
2. Select the check boxes next to any guest passes that you want to delete in either the *Self-Service Guest Passes* or the *Admin Generated Guest Passes* table, and click the respective **Delete** button to delete.
3. To delete all records at once (either self-generated or admin-generated), click **Delete All**.
4. To download a list of generated guest passes, click **Export to CSV**. ZoneDirector will generate a list of guest passes in a CSV file that can be opened in a spreadsheet program.

FIGURE 69 Managing generated guest passes



Using an External Server for User Authentication

Once your wireless network is set up, you can instruct ZoneDirector to authenticate wireless users using your existing Authentication, Authorization and Accounting (AAA) server. The following types of AAA servers are supported:

- Active Directory
- LDAP
- RADIUS / RADIUS Accounting

The ZoneDirector web interface provides a sample template for each of the AAA server types. These templates can be customized to match your specific network setup, or you can create new AAA server objects and add them to the list.

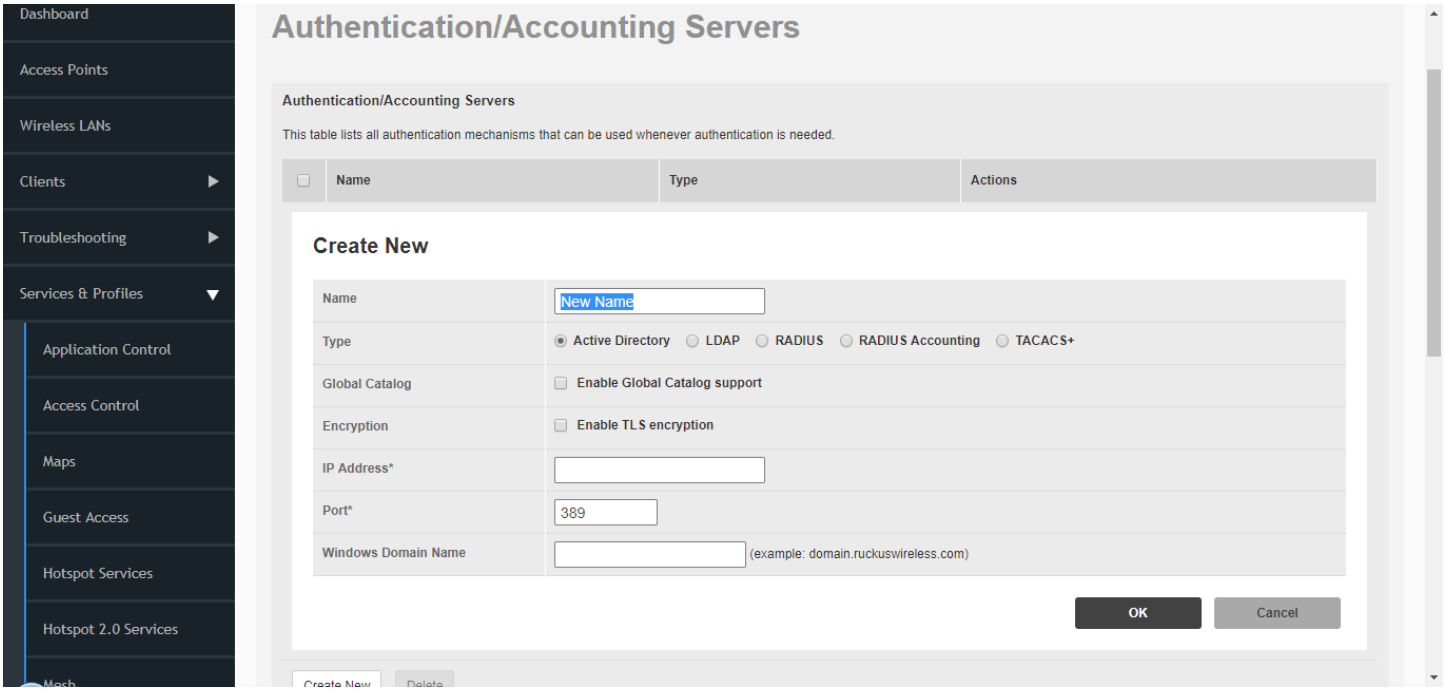
To use an external authentication server:

1. Go to **Services & Profiles** > **AAA Servers**. The Authentication/Accounting Servers page appears.
2. Click the **Create New** link in the Authentication/Accounting Servers table, or click **Edit** next to the relevant server type in the list.
3. When the **Create New** form (or "Editing" form) appears, make the following entries:
   - In Name, type a descriptive name for this authentication server (for example, "Active Directory").
   - In Type, verify that one of the following options is selected:
     - **Active Directory**: If you select this option, you also need to enter the IP address of the AD server, its port number (default is 389), and its Windows Domain Name.
     - **LDAP**: If you select this option, you also need to enter the IP address of the LDAP server, its port number (default is 389), and its LDAP Base DN.
     - **RADIUS**: If you select this option, you also need to enter the IP address of the RADIUS server, its port number (default is 1812), and its shared secret.
     - **RADIUS Accounting**: If you select this option, you also need to enter the IP address of the RADIUS Accounting server, its port number (default is 1813), and its shared secret.
4. Additional options appear depending on which AAA server Type you have selected. See the respective server type for more information.
5. Click **OK** to save this server entry. The page refreshes and the AAA server that you added appears in the list of authentication and accounting servers.

Note that input fields differ for different types of AAA server. ZoneDirector only displays the option to enable Global Catalog support if Active Directory is chosen, for example, and only offers backup RADIUS server options if RADIUS or RADIUS Accounting server is chosen. Also note that attribute formats vary between AAA servers.

NOTE
If you want to test your connection to the authentication server, enter an existing user name and password in the Test Authentication Settings panel, and then click Test. If testing against a RADIUS server, this feature uses PAP or CHAP depending on the RADIUS server configuration and the choice you made in RADIUS/RADIUS Accounting. Make sure that either PAP or CHAP is enabled on the Remote Access Policy (assuming Microsoft IAS as the RADIUS server) before continuing with testing authentication settings.

FIGURE 70 The Create New form for adding an authentication server



Enabling Web Authentication

Web authentication (also known as a "Captive Portal") redirects users to a login web page the first time they connect to the WLAN, and requires them to log in before granting access to use the WLAN.

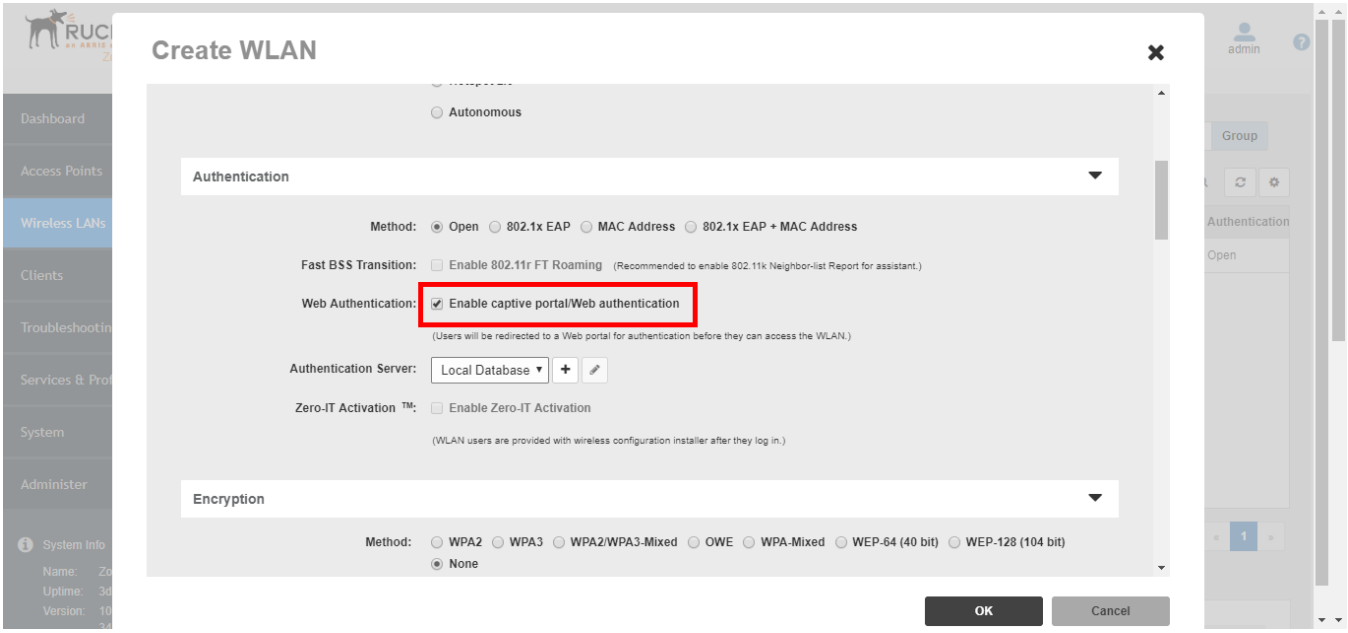
After you activate web authentication on your WLAN, you must then provide all users with a URL to your login page. After they discover the WLAN on their wireless device or laptop, they open their browser, connect to the Login page and enter the required login information.

To activate web authentication:

1. Go to **Wireless LANs**. The WLAN page appears.
2. Select the WLAN that you want to edit, and then click the **Edit** button.
3. When the **Editing [WLAN Name]** form appears, locate the **Web Authentication** option.
4. Click the check box to **Enable captive portal/Web authentication**.
5. Select the preferred authentication server from the **Authentication Server** drop-down menu.

6. Click **OK** to save this entry.

FIGURE 71 Activating captive portal/web authentication



NOTE
For information on customizing the web portal logo, see Customizing the Captive Portal on page 194.

Captive Portal Redirect on Initial Browser HTTPS Request

When logging in to a Web Auth/Hotspot/Guest WLAN by initially requesting an HTTPS page in the browser, the client may encounter one or two SSL/HTTPS security warnings as follows:

- The first is generated because the SSL certificate of the HTTPS site the user is trying to reach does not match the certificate installed on the ZoneDirector. Depending on the browser/OS, this maybe flagged as a potential Man in the Middle attack (MiM).
- The second is generated if the ZoneDirector or Hotspot server does not have an SSL certificate signed by a recognized Certificate Authority installed when the client is redirected to the login page.

These browser security warnings are there to encourage users to take care when browsing secure sites and ensure their authenticity. However, there are two options to help mitigate these warnings:

1. Completely disable the "redirect on initial browser HTTPS request" feature (refer to the *ZoneDirector CLI Reference Guide*, "no https-redirection" command). Users will no longer be redirected to the captive portal when their browser initially requests an HTTPS page and the browser will display a message similar to "Page not found" or "SSL connection error". In this case, the user will then need to request an HTTP page (not HTTPS) to be redirected to the login page. This approach prevents users from being "conditioned" to click-through browser security warnings.
2. Install an SSL certificate signed by a recognized Certificate Authority on the ZoneDirector or captive portal server. This will only prevent the second security warning - the first will still occur because the certificate will not match that of the requested secure site. See Working with SSL Certificates on page 346 for more information.

Managing Guest Access

- Configuring Guest Access 125
- Creating a Guest Access Service 125
- Creating a Guest WLAN 143
- Using the BYOD Onboarding Portal 144
- Working with Guest Passes 149
- Social Auth WLANs 165
- Working with Hotspot Services 185
- Creating a Hotspot 2.0 Service 191
- Customizing the Captive Portal 194

Configuring Guest Access

Using ZoneDirector's Guest Access features, visitors to your organization can be allowed limited access to a guest WLAN with configurable guest policies, or given the option to self-activate their devices to an internal WLAN using Zero-IT activation via the BYOD Onboarding Portal, or both.

ZoneDirector's Guest Pass system allows admins to generate one-time passwords that are only valid for a certain amount of time, along with any other access restrictions, but which also provide all of the security benefits of a standard PSK passphrase.

Guest WLANs can be configured to allow visitors to self-authenticate using a social media account, such as Facebook, LinkedIn, Microsoft, Google or WeChat.

The following sections describe how to configure guest WLANs and guest access policies to control visitors' use of your wireless networks.

Creating a Guest Access Service

Each guest WLAN must be associated with a Guest Access Service, which defines the behavior of the guest WLAN interface.

To create a Guest Access Service:

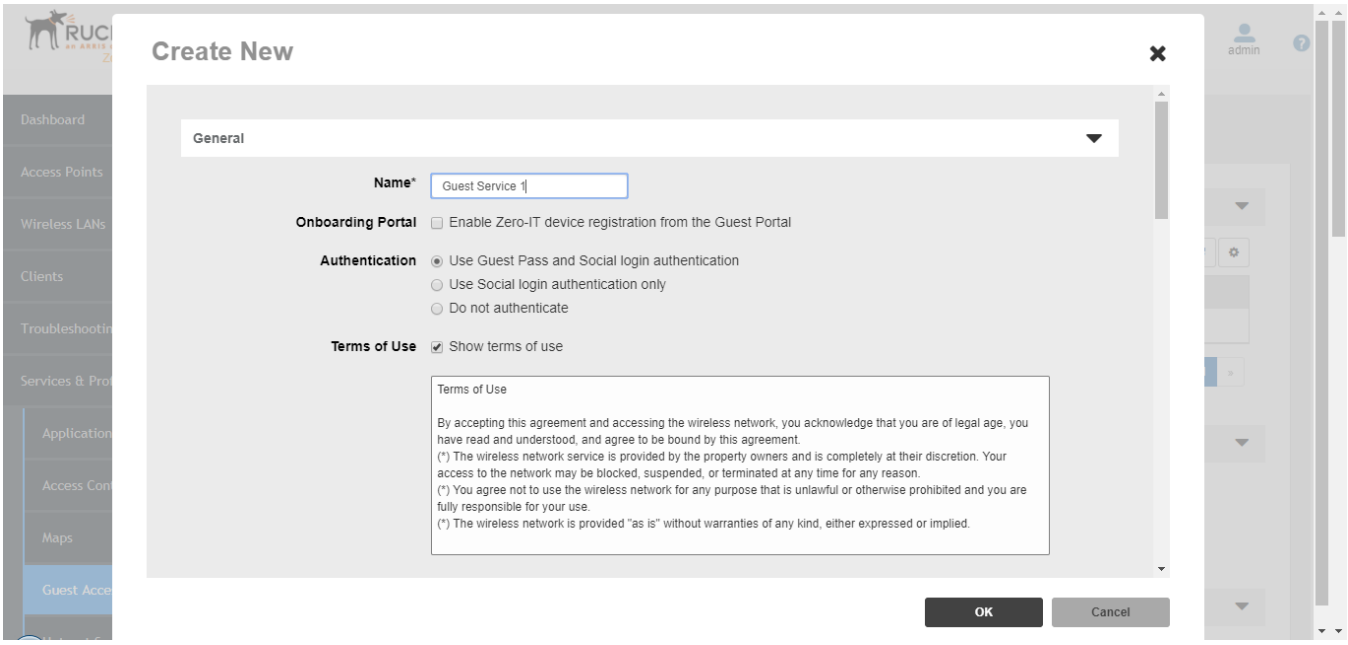
1. Go to **Services & Profiles** > **Guest Access**.
2. Click **Create** to configure a guest access service.

   NOTE
   Alternatively, you can create a Guest Access Service from the WLAN creation page while creating a new WLAN or modifying an existing WLAN (**Wireless LANs > Edit > Type > Guest Access > Guest Access Service > + Create**.)

3. Enter a **Name** for the guest service.
4. In **Onboarding Portal**, choose which options to display in the BYOD Onboarding Portal. See Using the BYOD Onboarding Portal on page 144.
5. In **Authentication**, choose whether to use Guest Pass login, Social Media login, or no authentication:
   - **Use Guest Pass and Social Login authentication**: Redirect the user to a page requiring the user to enter a valid guest pass before allowing access to the guest WLAN. See Working with Guest Passes on page 149, or allow login using a social media account.
   - **Use Social login authentication only**: Allow login using a social media account and no guest pass login.
   - **Do not authenticate**: Do not require authentication.

6. In **Terms of Use**, enable the **Show terms of use** check box to require the guest user to read and accept your terms of use prior to use. Type (or cut and paste) your terms of use into the large text box.

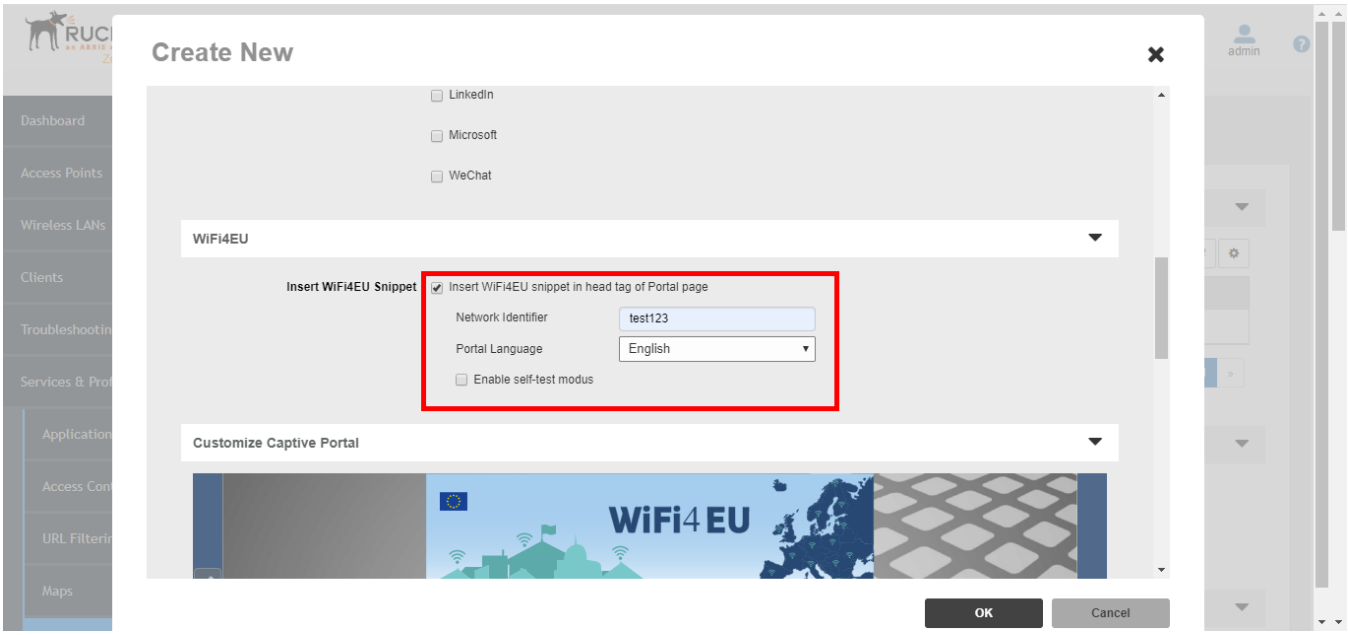
FIGURE 72 Configuring Guest Access



7. In **Redirection**, select one of the following radio buttons to use/not use redirection:
   - **Redirect to the URL that the user intends to visit**: Allows the guest user to continue to their destination without redirection.
   - **Redirect to the following URL**: Redirect the user to a specified web page (entered into the text box).
8. In **Guest Pass Option** (if the guest pass feature is enabled), configure guest pass options as follows:
   - **Validity Period**: Choose whether guest passes will be effective from creation time or effective from first use, and enter an expiration period after which guest passes will become invalid.
   - **Guest Pass Self-Service**: Enable this option to allow users to self-activate guest passes. See Using Guest Pass Self-Service on page 127.
9. In **Social Auth Options**, configure social media login settings as required. For more information on social media login, see Social Auth WLANs on page 165.

10. In **WiFi4EU**, enable the **Insert WiFi4EU Snippet** option to insert a WiFi4EU snippet in the head tag of the web auth portal page. This allows the WLAN to be used by members of the WiFi4EU "digital single market" for EU member states.

FIGURE 73 Insert WiFi4EU Snippet



11. In **Customize Captive Portal**, you can customize the look and feel of the login page that guests will see when connecting to your guest WLAN. For more information, see Customizing the Captive Portal on page 194.
12. In **Restricted Subnet Access**, configure any subnet restrictions that you want to apply to your visitors. See Configuring Guest Subnet Restrictions on page 141.
13. Click **OK** to save your settings.

Using Guest Pass Self-Service

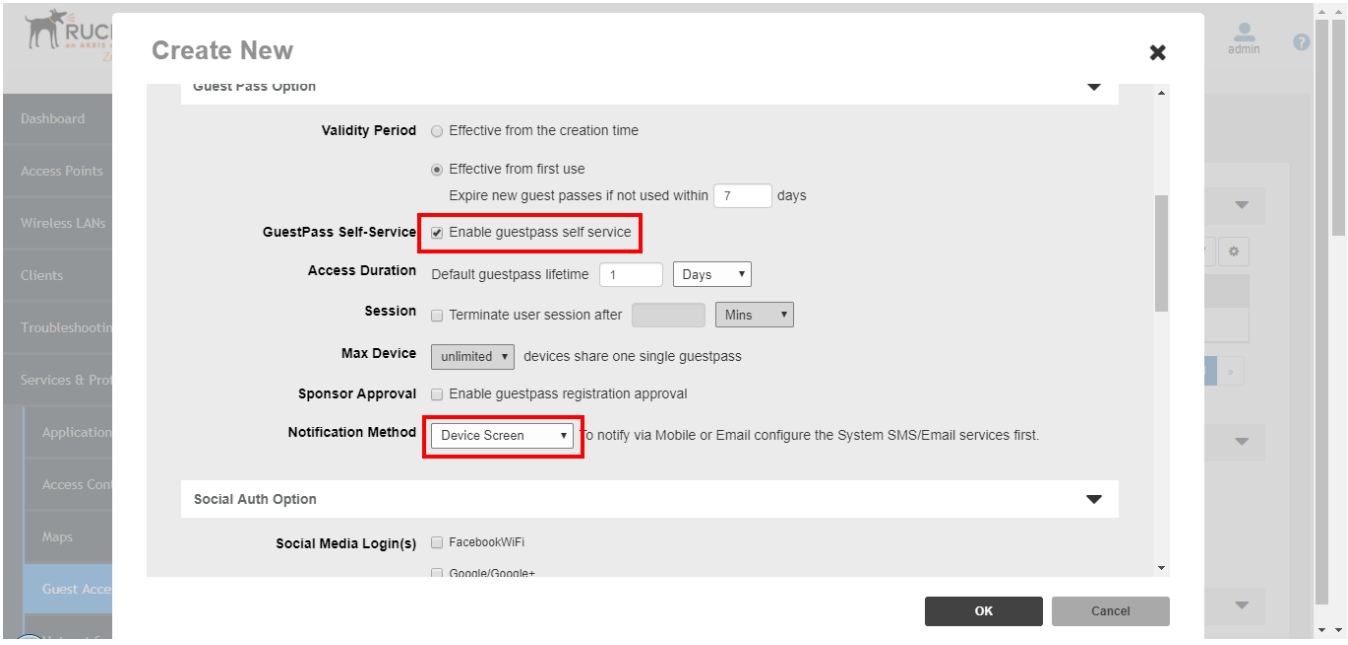
The Guest Pass Self-Service feature allows guests to connect to a guest SSID and submit basic information (name, email address and mobile phone number) to receive a guest pass code. The guest then enters this code to gain access to the internet, with no IT involvement required.

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.
To enable Guest Pass Self-Service:

1. On the **Services & Profiles** > **Guest Access** page, create a new Guest Access service or edit an existing one.
2. Enter a **Name** for the guest access service.
3. In **Authentication**, select **Use Guest Pass and Social login authentication**.
4. Enable **Terms of Use** and customize the content in the text box, if you want to require guests to read and accept a Terms of Use prior to accessing the network.
5. In **Redirection**, select **Redirect to the following URL** and enter a destination URL, or select **Redirect to the URL that the user intends to visit**.

6. Set the guest pass **Validity Period** by selecting one of the following options:
   - **Effective from the creation time**: This type of guest pass is valid from the time it is first created to the specified expiration time, even if it is not being used by any end user.
   - **Effective from first use**: This type of guest pass is valid from the time the user uses it to authenticate with ZoneDirector until the specified expiration time. An additional parameter (A Guest Pass will expire in X days) can be configured to specify when a guest pass will expire when unused. The default is 7 days.
7. Select **Enable Guest Pass Self-Service**. The following new options appear:
   - **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 133.)
   - **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.
8. Click **OK** to save your changes.
9. Go to **Wireless LANs**, and apply this Guest Access Policy to a Guest Access WLAN, as described in Creating a Guest WLAN on page 143.

FIGURE 74 Creating a Self-Service Guest Access service



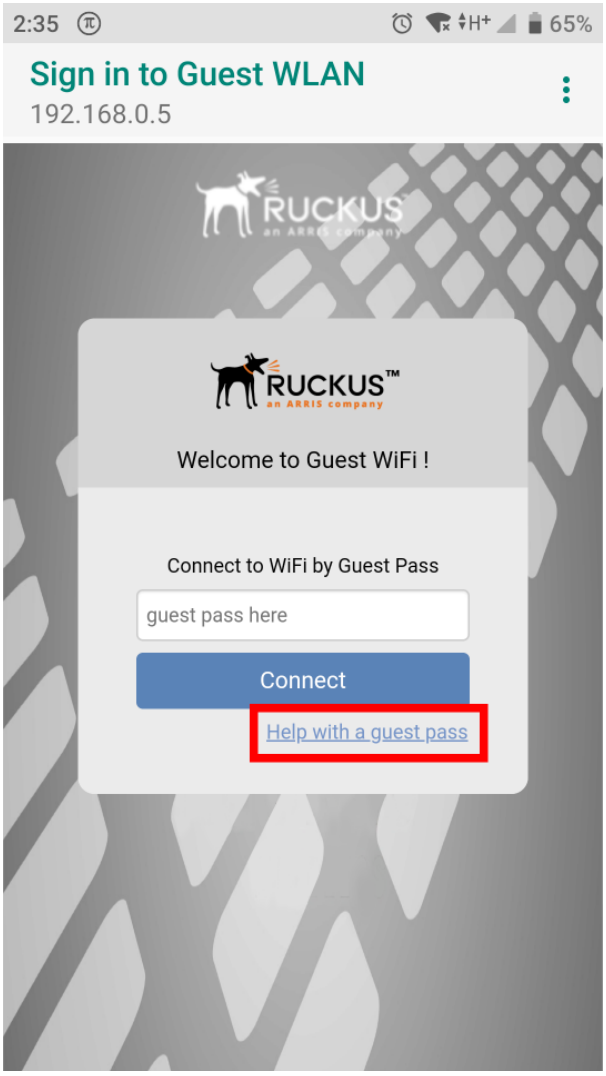
Accessing a Self-Service Guest WLAN

The simplest way to deploy a self-service guest WLAN is to enable the self-service option and do not change any of the default settings. When a self-service guest WLAN is deployed in this way, the user follows these steps to self-activate and begin using a guest pass:

1. Connect to the guest WLAN, launch a web browser and attempt to browse to any site.
2. The browser redirects to the **Welcome to Guest WiFi!** page.

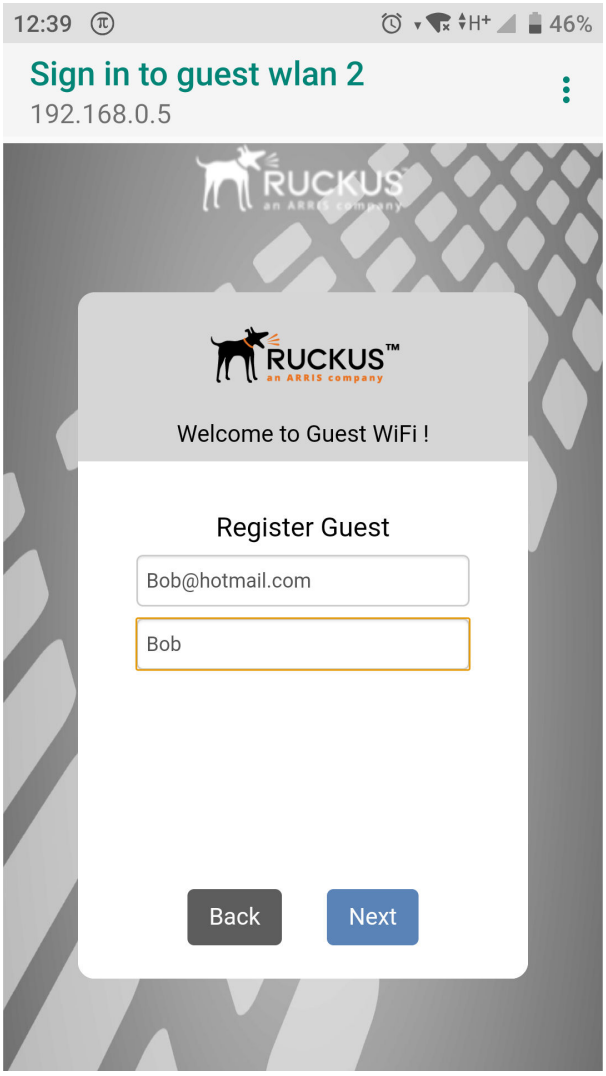
3. Click **Help with a guest pass**.

FIGURE 75 Guest Pass login page



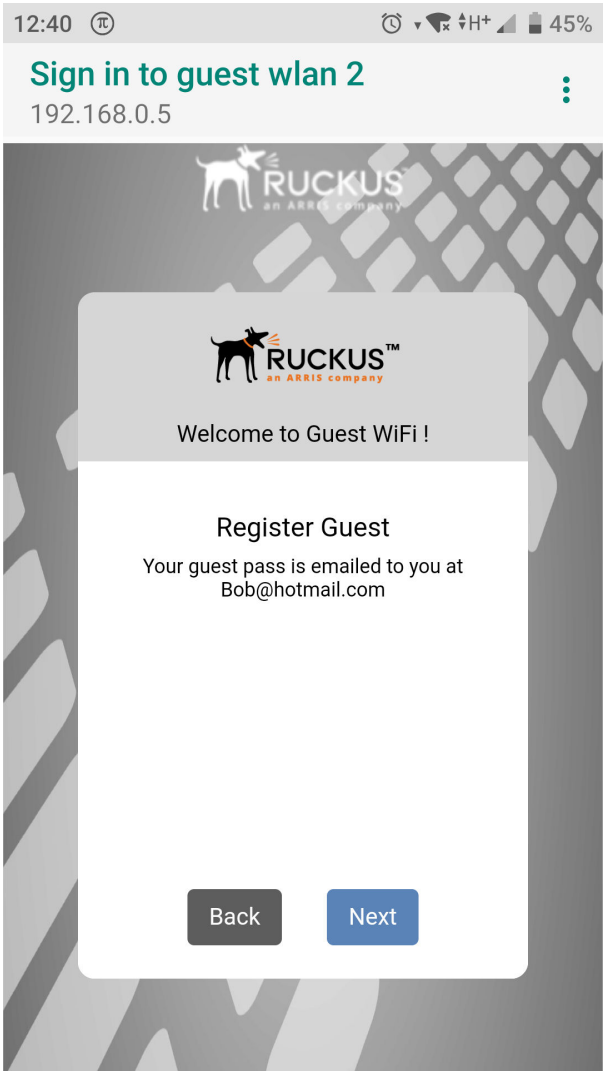
4. The *Register Guest* screen appears.

FIGURE 76 New Guest Registration page



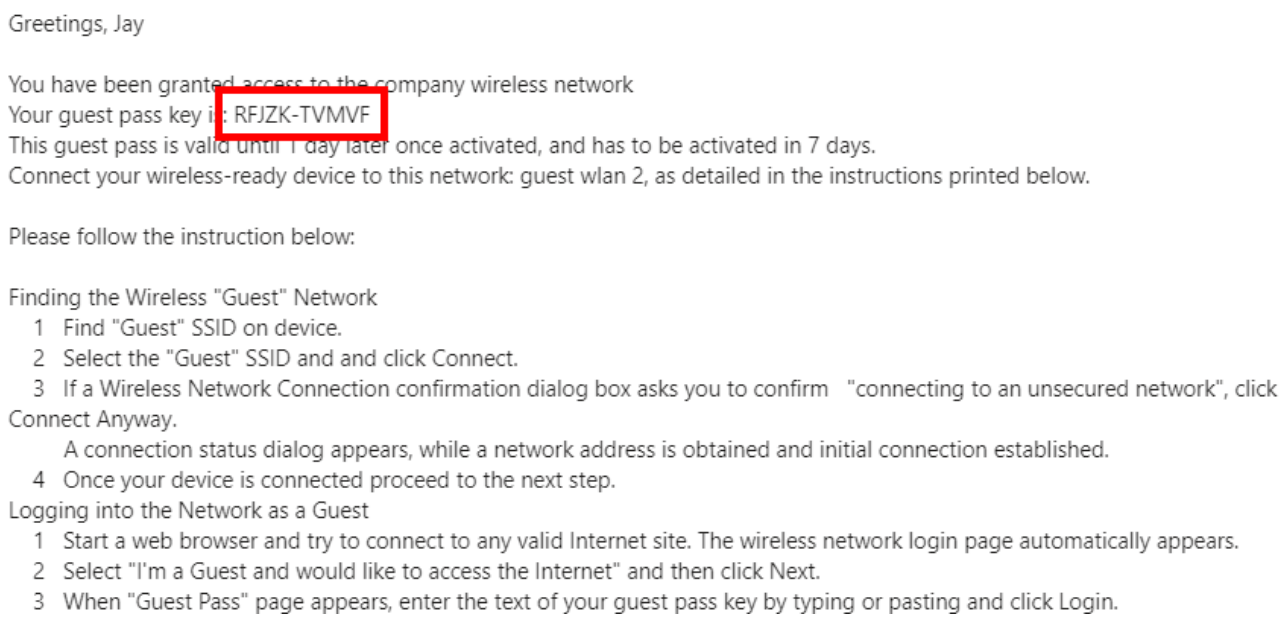
5. Enter your email address and name, and click **Next**. An email delivery message appears.

FIGURE 77 New Guest Registration page



6. Open the email account you entered and check for the email containing the guest pass.

FIGURE 78 Guest pass email



Greetings, Jay

You have been granted access to the company wireless network
Your guest pass key is: RFJZK-TVMVF
This guest pass is valid until 1 day later once activated, and has to be activated in 7 days.
Connect your wireless-ready device to this network: guest wlan 2, as detailed in the instructions printed below.

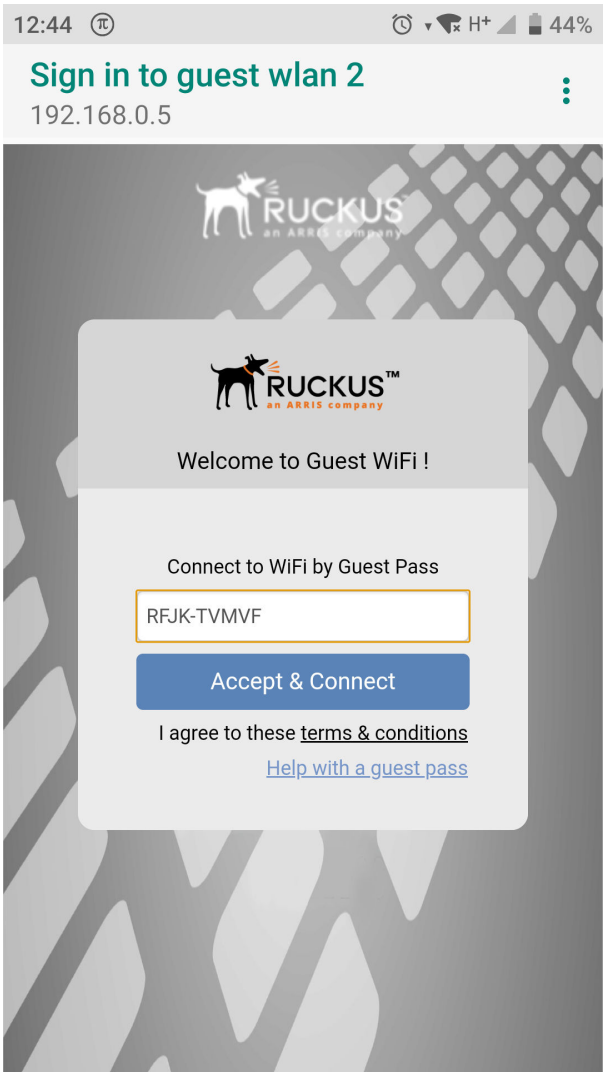
Please follow the instruction below:

Finding the Wireless "Guest" Network
1 Find "Guest" SSID on device.
2 Select the "Guest" SSID and and click Connect.
3 If a Wireless Network Connection confirmation dialog box asks you to confirm "connecting to an unsecured network", click Connect Anyway.
A connection status dialog appears, while a network address is obtained and initial connection established.
4 Once your device is connected proceed to the next step.
Logging into the Network as a Guest
1 Start a web browser and try to connect to any valid Internet site. The wireless network login page automatically appears.
2 Select "I'm a Guest and would like to access the Internet" and then click Next.
3 When "Guest Pass" page appears, enter the text of your guest pass key by typing or pasting and click Login.

7. Copy this guest pass and go back to the WLAN login screen.

8. On the **Sign In to Guest WLAN** page, enter the guest pass you received in your email and click **Accept & Connect**. Your guest pass is now activated and you can begin using the wireless network.

FIGURE 79 Sign In with Guest Pass



Requiring Sponsor Approval for Self-Service Guest Pass Authentication

If the "Sponsor Approval" option is enabled, when the user connects to the WLAN, he or she submits registration information along with a Sponsor's email address and waits for sponsor approval. The Sponsor receives an email request and clicks a link to allow this user access to the guest WLAN. Once the registration is approved, ZoneDirector then generates a guest pass and sends it to the user via email and/or SMS using the contact information the user provided.

NOTE
If using Sponsor Approval, ZoneDirector must be configured with your SMTP settings for email delivery, or with a valid Twilio, Clickatell or custom SMS provider account to deliver guest passes via SMS. See Delivering Guest Passes via Email on page 163 and Delivering Guest Passes via SMS on page 164 for more information.

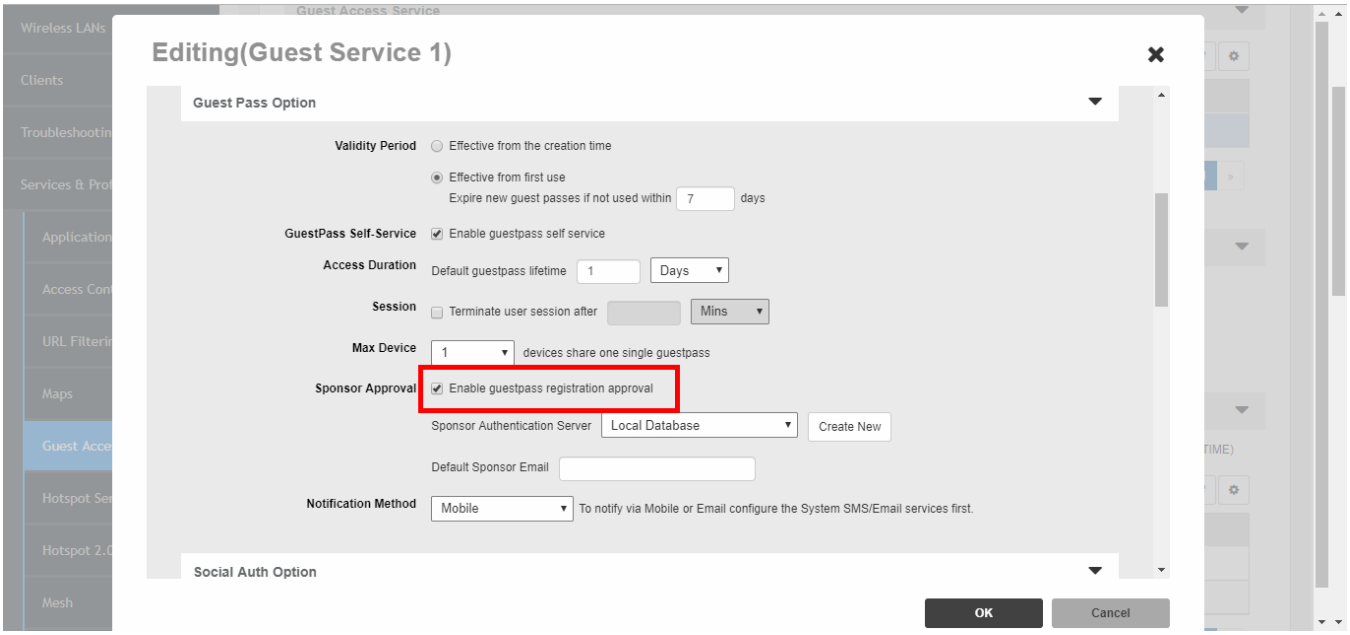
Configure the following options if Sponsor Approval is enabled:

- **Sponsor Authentication Server**: Select the authentication server to be used for sponsor authentication. When a guest pass approval request is sent to the sponsor's email, the sponsor must click the link in the email, log in to this authentication server, and approve or reject the request. Options include Local Database, Active Directory, LDAP and RADIUS.

  NOTE
  When sponsor approval is enabled, all guest service profiles share the same sponsor authentication server. If you select a different authentication server when creating a new guest service, the new server will be used for all guest services.

- **Default Sponsor Email**: Enter the default email address to which sponsor approval messages will be delivered.
- **Notification Method**: Select whether the guest pass will be delivered via email, SMS, or displayed directly on the device screen. When Sponsor Approval is enabled, the Device Screen option is not allowed.

FIGURE 80 Configuring Sponsor Approval for Self Service Guest Passes

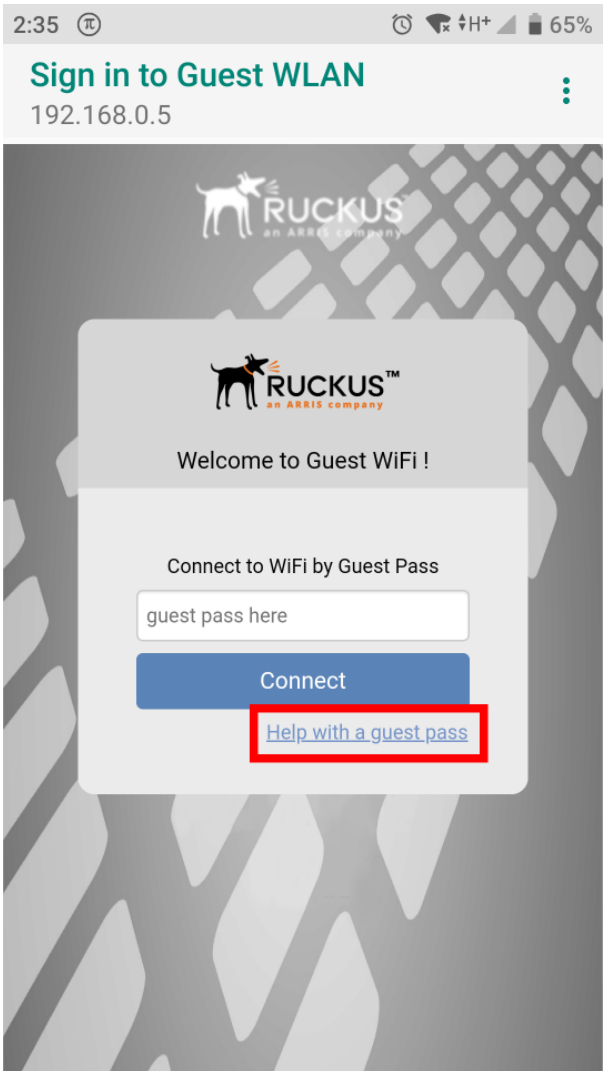


When a user connects to a guest WLAN with Sponsor Approval enabled, the option to request a new guest pass appears.

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

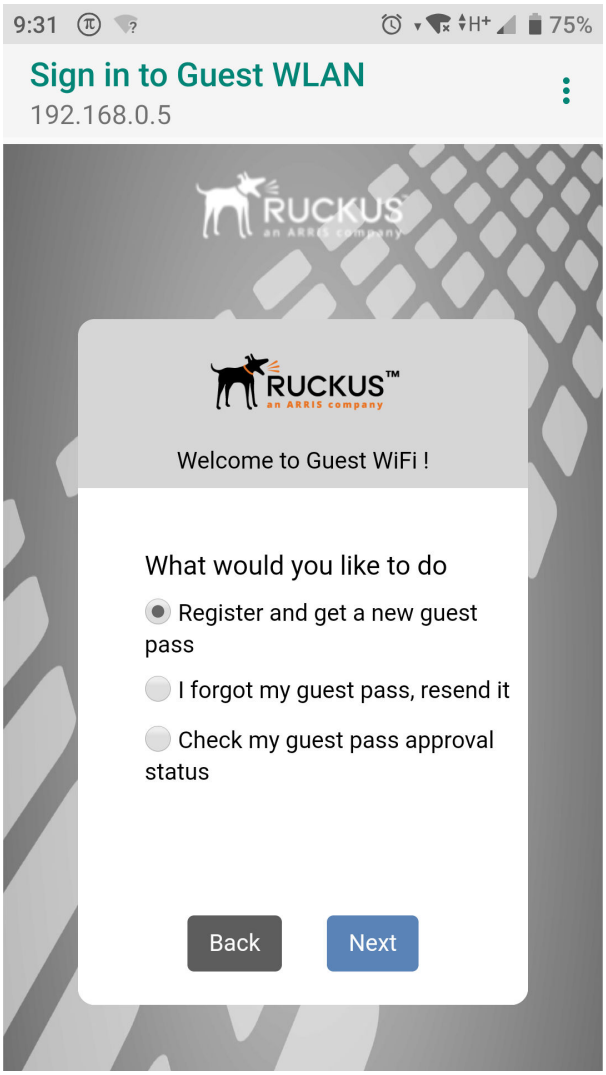
1. On the **Welcome to Guest WiFi** screen, click **Help with a guest pass**.

FIGURE 81 Click "Help with a guest pass" to request a new guest pass



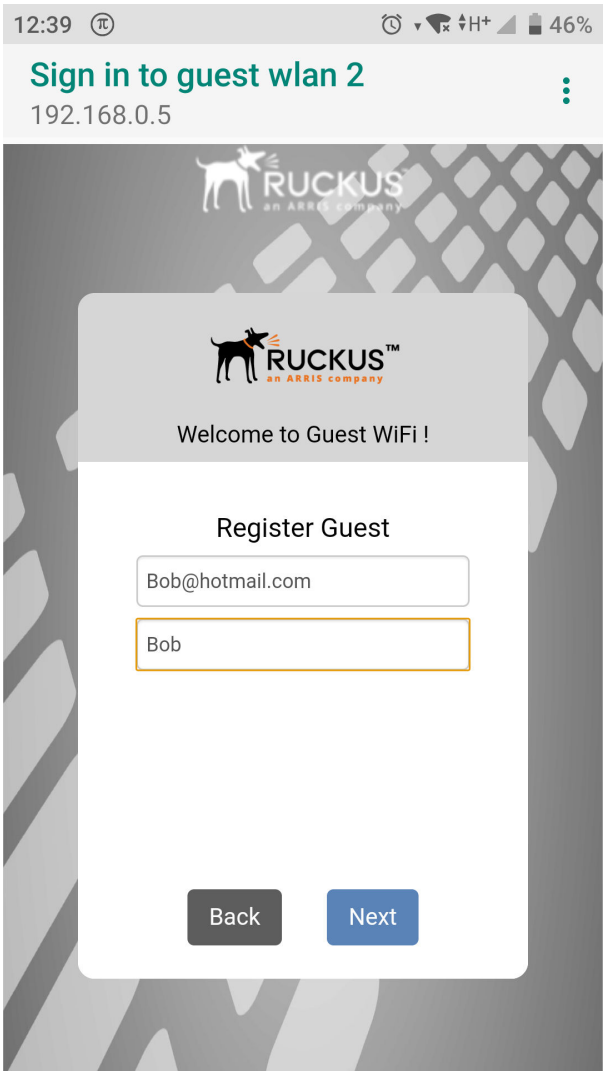
2. On the *What would you like to do* screen, select **Register and get a new guest pass**, and click **Next**.

FIGURE 82 Request a guest pass from a sponsor



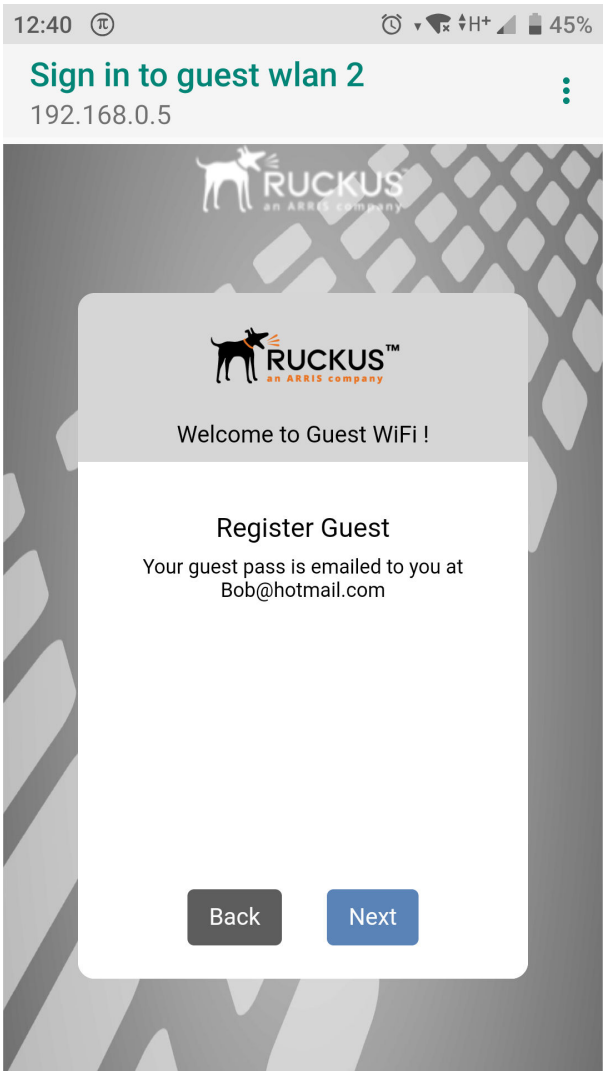
3. Enter your name and email address and click **Next**. A guest pass request email is sent to the sponsor's address.

FIGURE 83 Request a guest pass from a sponsor



4. The screen displays a confirmation message confirming that your guest pass will be emailed to the email address provided.

FIGURE 84 Request a guest pass from a sponsor



5. The sponsor will then receive an email requesting approval for guest pass activation.
6. (As the sponsor), open the email and click the link to open the Sponsor/Approver Authentication page.

FIGURE 85 Sponsor approval email

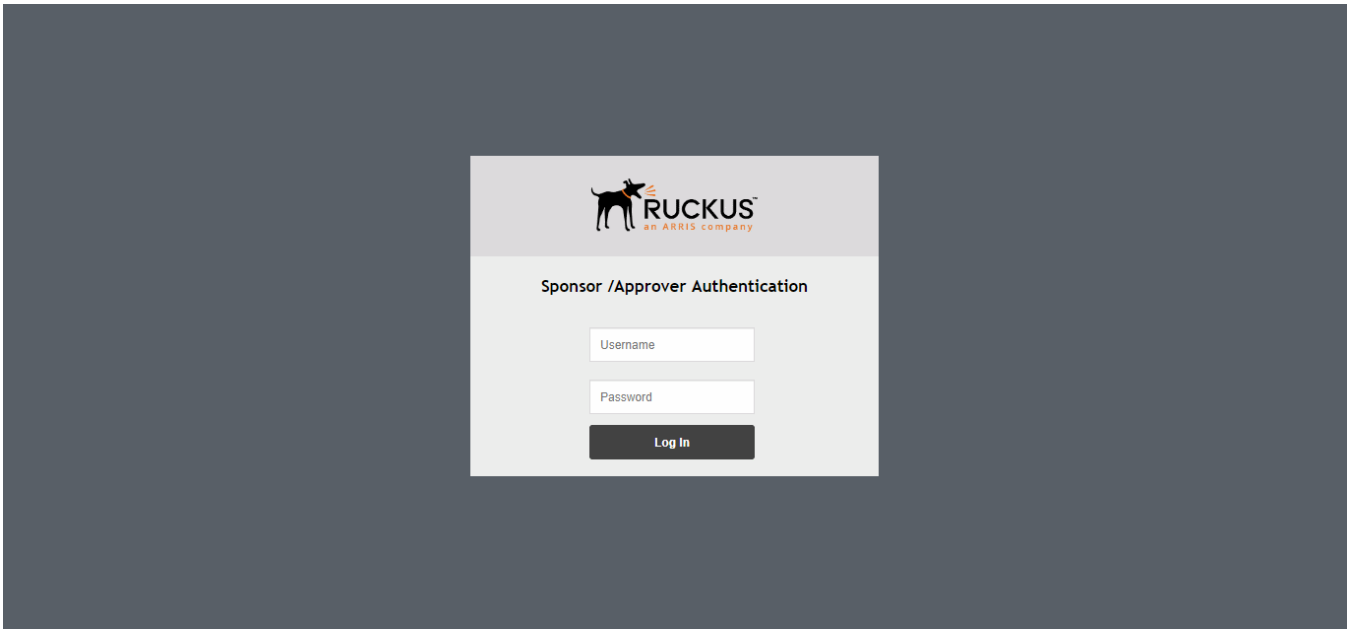
Dear Sponsor/Admin,

You are a designated approver for Bob's WiFi access. Click link below to approve or reject the request.
https://192.168.0.5/user/sponsor_login.jsp?email=HDGMGJGOGHHDGBGOGEGBHCHCGPHHHDDBDAEAGIGPHEGNGBGJGMCOGDGPGN&user=&ssid=EHHFGFHDHECAFHEMEBEO
Name: Bob
Mobile No: 6692249368
Email:
SSID: Guest WLAN

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

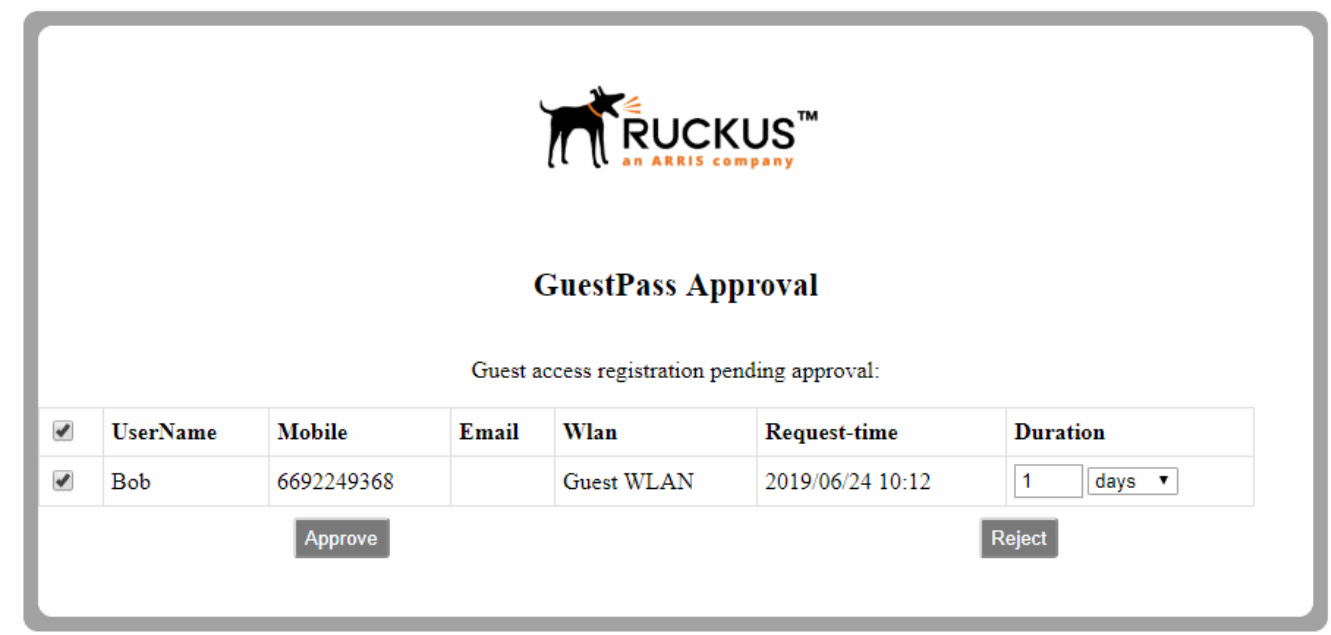
   NOTE
   This user name and password must exist on the Authentication Server (Local Database, AD, LDAP or RADIUS) configured with guest pass generation privileges for this guest access service.

FIGURE 86 Sponsor Login



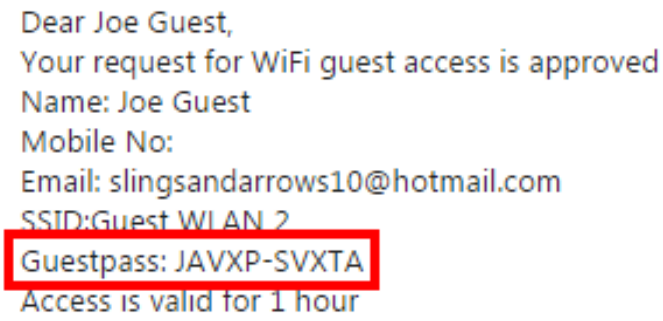
8. Upon successful login, the **Guest Pass Approval** page appears, displaying the name, phone and email addresses of all pending guest pass requests. Select the check boxes next to each guest pass you wish to approve, set the **Duration** for each, and click **Approve** to approve them.

FIGURE 87 Guest Pass Approval



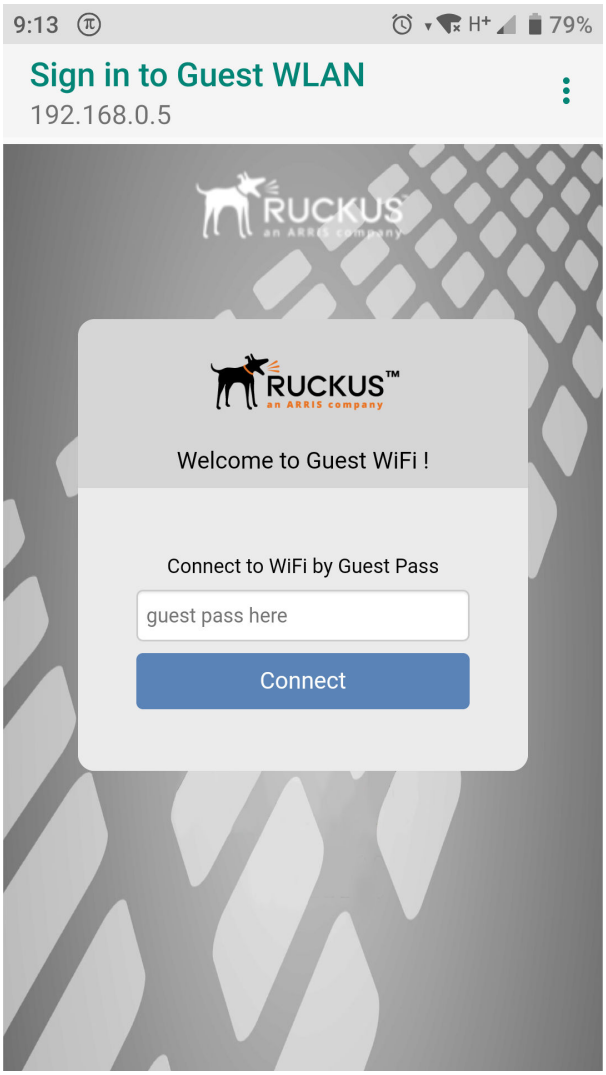
9. Approving a guest pass triggers delivery of an email (and/or SMS message) containing the guest pass code to the guest.
10. As a guest user, open this email and copy the **Guest Pass** code to the clipboard.

FIGURE 88 Guest pass activation email



11. Launch a web browser and browse to any URL. You will be redirected to the **Welcome** login page.
12. Enter the **Guest Pass** code received in the activation email and click **Connect**.

FIGURE 89 Enter Guest Pass code and click Go Online



13. You have successfully authenticated to this guest network using the guest pass provided. Click **Continue** to complete activation and continue to your original destination URL.

Configuring Guest Subnet Restrictions

By default, guest pass users are automatically blocked from the ZoneDirector 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 22 subnet access rules, which will be enforced both on the ZoneDirector side (for tunneled/redirect traffic) and the AP side (for local-bridging traffic).

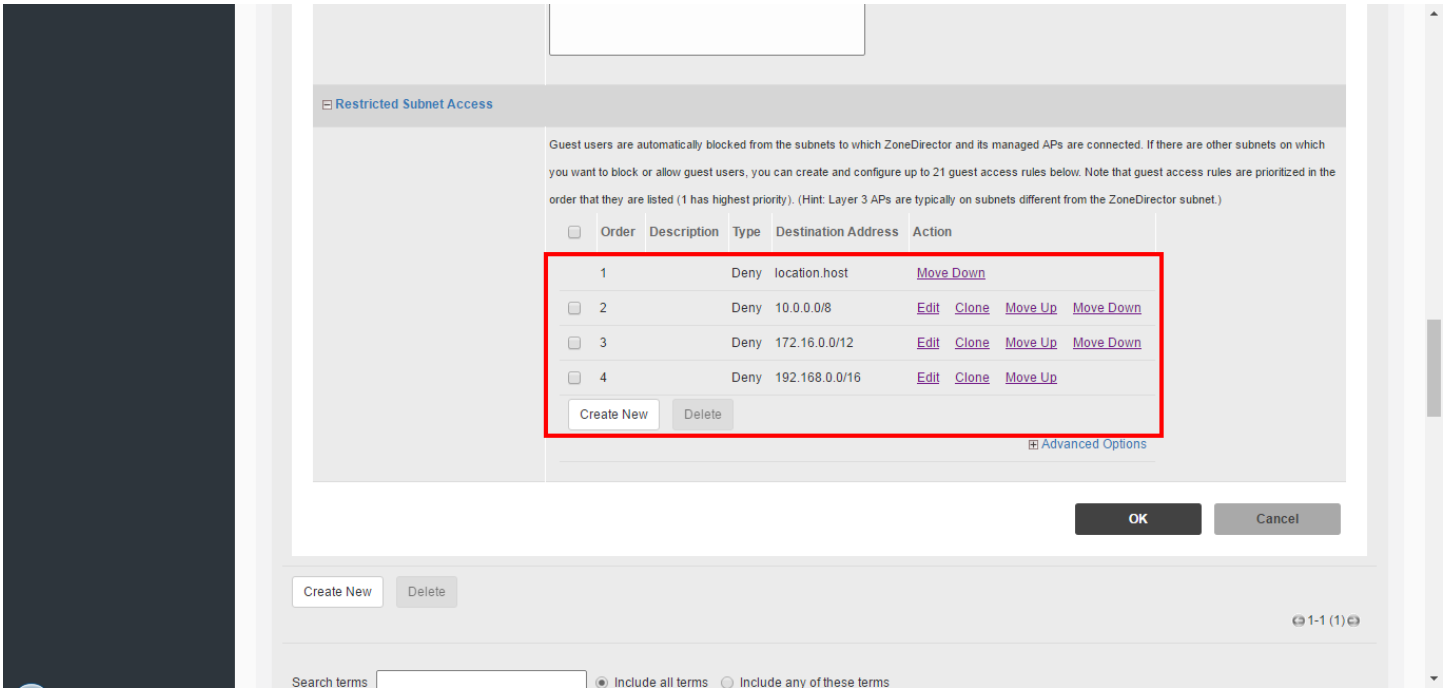
To create a guest access rule for a subnet:

1. Go to **Services & Profiles** > **Guest Access**.

2. Edit or create a new Guest Access Service.
3. Scroll down to the bottom and expand the **Restricted Subnet Access** section.
4. 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.
5. Under **Description**, type a name or description for the access rule that you are creating.
6. 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.
7. Under **Destination Address**, type the IP address and subnet mask (format: A.B.C.D/M) on which you want to allow or deny users access.
8. If you want to allow or restrict subnet access based on the application, protocol, or destination port used, click the **Advanced Options** link, and then configure the settings.
9. Click **OK** to save the subnet access rule.

Repeat Steps 4 to 9 to create up to 22 subnet access rules.

FIGURE 90 The Restricted Subnet Access options



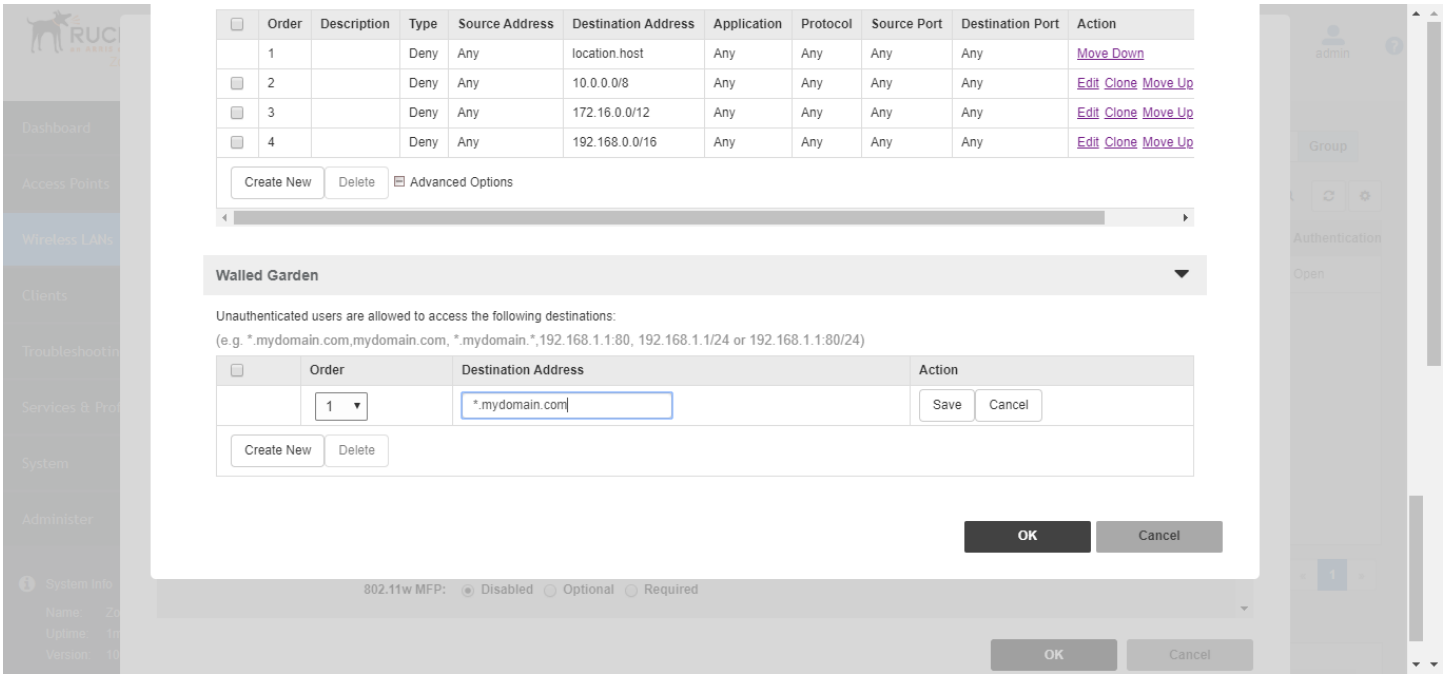
Guest Access Walled Garden

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 **Services & Profiles > Guest Access > Create/Edit (Guest Service) > Walled Garden**. Click **Create New** to create a new rule, and enter the destination IP address or domain name in the field.

FIGURE 91 Enter domain name or IP addresses to allow access to unauthenticated users



Creating a Guest WLAN

Once you have created a guest access service, create a WLAN of the type "Guest Access."

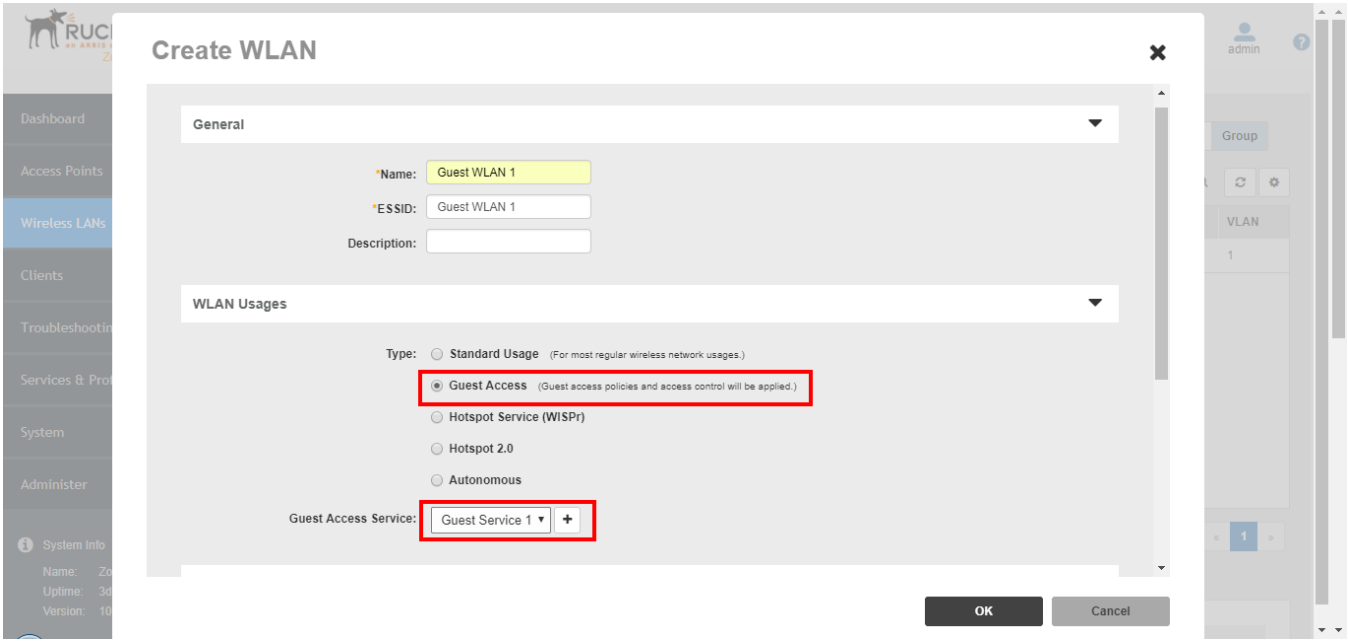
This WLAN can be configured to allow access only to a specific set of resources - such as ZoneDirector's Zero-IT activation address - from which users can then activate their devices to gain access to other WLANs (such as the corporate/internal WLAN).

To create a Guest WLAN:

1. Go to **Wireless LANs**.
2. Under WLANs, click **Create New**. The **Create New WLAN** form appears.
3. Enter a **Name (SSID)** for this WLAN that will be easy for your guests to remember (e.g., "Guest WLAN"). The **Description** field is optional.
4. Under **Type**, select **Guest Access**.
5. Select a **Guest Access Service** from the list of services created on the **Services & Profiles > Guest Access** page. If you have not yet created a Guest Access Service, click **Create New** to create one. See Creating a Guest Access Service on page 125.
6. Choose an **Encryption Method** that provides the best compromise between security and compatibility, based on the kinds of client devices that you expect your guests will use.
7. Under **Advanced Options**, select the options to enable for this WLAN. For more information on WLAN advanced options, see Advanced WLAN Options on page 72.
    - If you want your internal wireless traffic to have priority over guest traffic, set the **Priority** to **Low**.
    - Optionally, enable a **Grace Period** (disabled by default) and enter a value in minutes to allow disconnected users a grace period after disconnection, during which users will not need to re-authenticate.

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

FIGURE 92 Create a Guest Access WLAN



Using the BYOD Onboarding Portal

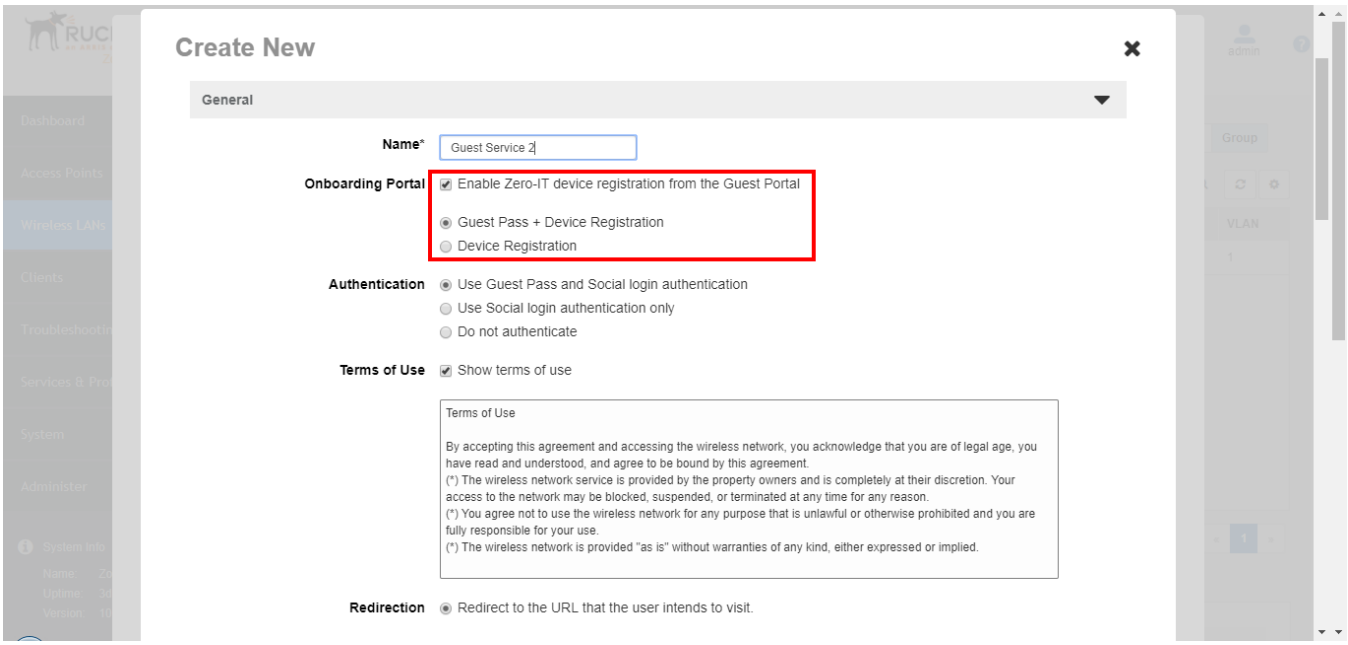
The Onboarding Portal feature provides a series of intuitive option screens that allow mobile users to choose whether to connect to a Guest WLAN or to self-configure their mobile devices to authenticate to an internal WLAN using Zero-IT activation.

To enable the Onboarding Portal for mobile devices:

1. Go to **Services & Profiles** > **Guest Access**.
2. Click **Edit** or **Create New** to configure a guest access service.
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*.

6. Click **Apply**.

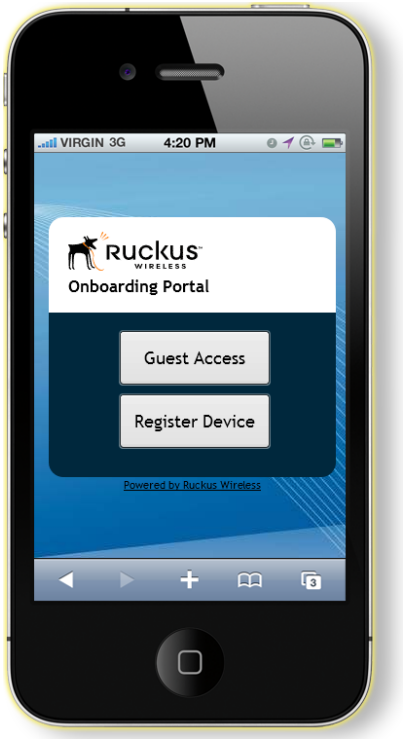
FIGURE 93 Enable Onboarding Portal



When a client connects to the Open Guest WLAN for the first time, the Ruckus Onboarding Portal page is displayed. The screen displays the following three options:

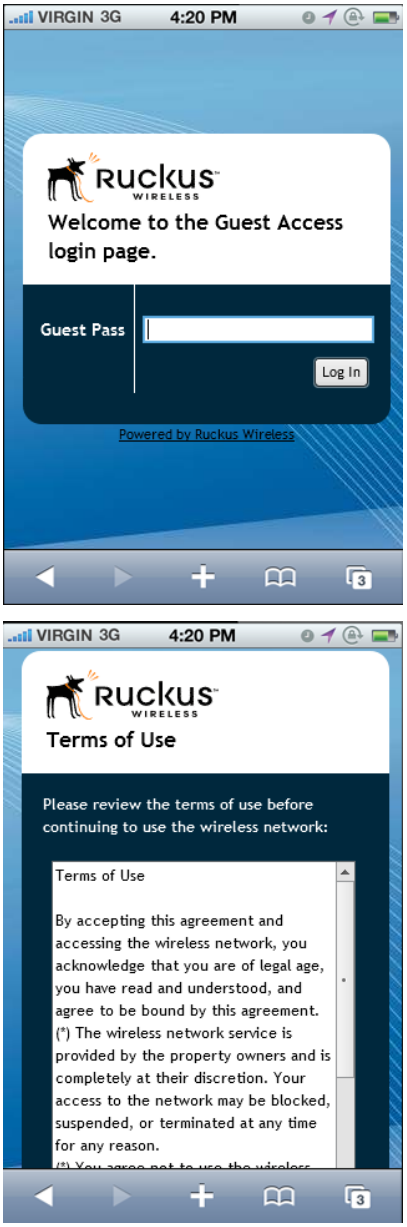
- Guest Access
- Register Device (download Zero-IT activation file)
- Both

FIGURE 94 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 95 Guest Access welcome and terms of use screens



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

FIGURE 96 Activate device using the WLAN Connection Activation screen, and download activation file



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

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

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

Working with Guest Passes

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

ZoneDirector 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:

- Print out wireless connection instructions containing guest pass key
- Send SMS to guest user containing guest pass key
- Send email to guest user containing guest pass key

NOTE
To enable guest pass delivery via email or SMS, you must first configure an email server or an SMS delivery account from the **System > System Settings** page.

NOTE
ZoneDirector 1200 can support up to 4,000 DPSK users and guest passes, and up to 4,000 concurrently connected clients. When the maximum number of users that ZoneDirector supports has been reached, additional clients attempting to connect will be refused.

Generating a Guest Pass from the Clients Page

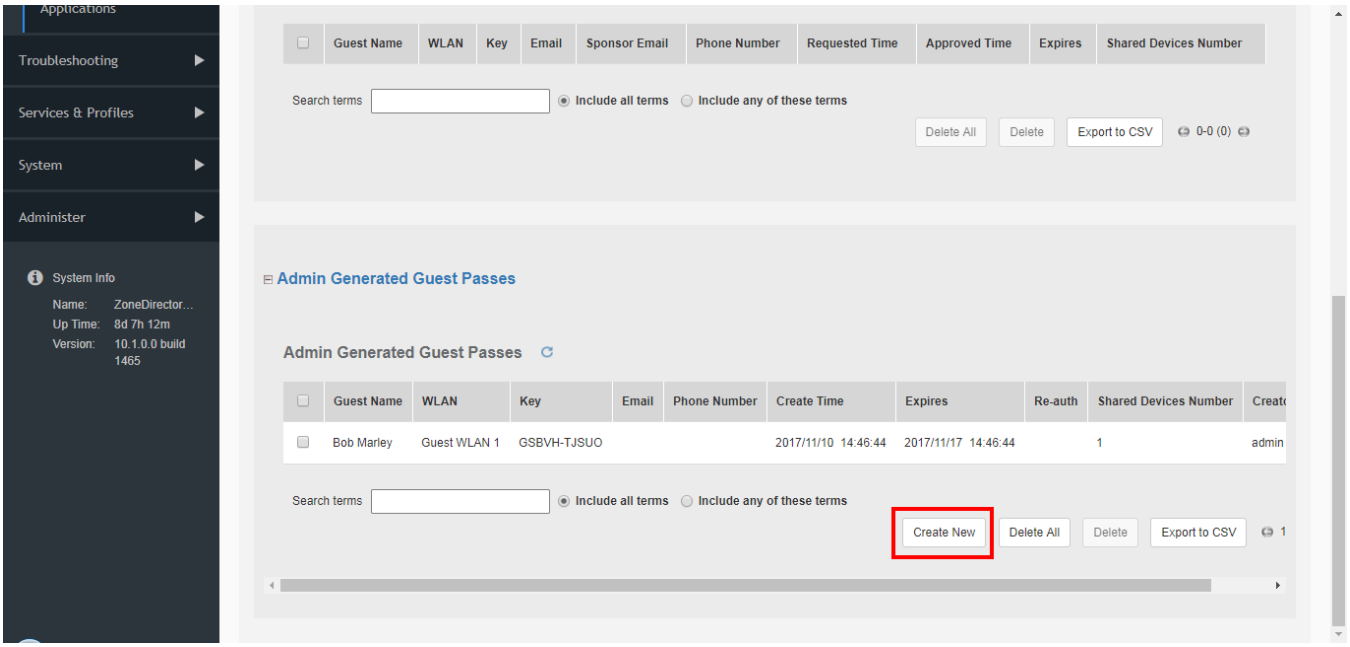
ZoneDirector administrators can create guest passes from within the UI, using the **Clients > Generated Guest Passes** page.

To generate a guest pass:

1. Go to **Clients > Generated Guest Passes**.
2. Expand the **Admin Generated Guest Passes** section.

3. Click **Create New** to generate a new guest pass.

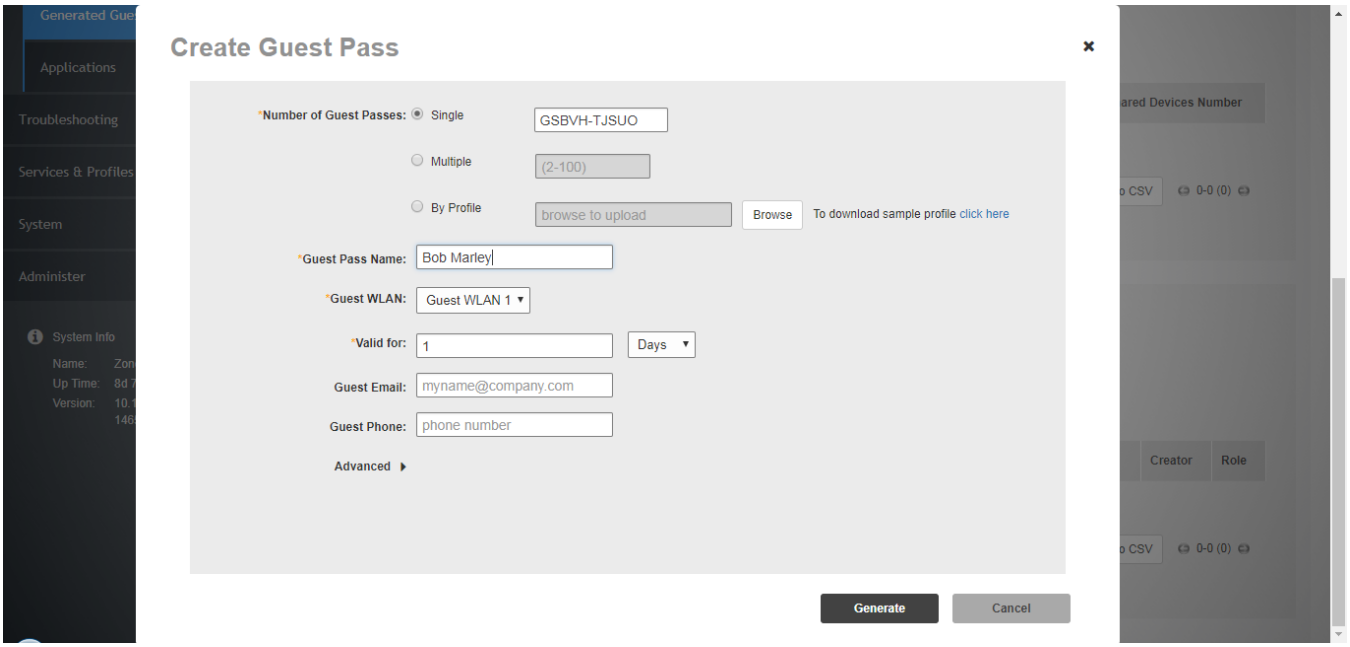
FIGURE 97 Create a new Guest Pass



4. In **Number of Guest Passes**, select one of the following:
   - **Single**: Create a single guest pass. For more information, see Generating and Delivering a Single Guest Pass on page 155.
   - **Multiple**: Generate multiple guest passes (2~100). For more information, see Generating and Printing Multiple Guest Passes at Once on page 159.
   - **By Profile**: Import a guest pass profile. For more information, see Creating a Guest Pass Profile on page 161.
5. In **Guest Pass Name**, enter the guest's name.
6. In **Guest WLAN**, select the WLAN for which the guest pass will be issued.
7. In **Valid For**, enter a number and select an increment (Hours, Days, or Weeks) for which the guest pass will remain valid.
8. Optionally, enter **Guest Email** and **Guest Phone** number. If these options are entered, and the email server and/or SMS delivery method have been configured (from the **System > System Settings** page), you can deliver the guest pass to the visitor using email or SMS.
9. Optionally, expand the **Advanced Options**, and configure the following:
   - **Session Timeout**: Enable this check box and select a time increment after which guests will be required to log in again. If this feature is disabled, connected users will not be required to re-log in until the guest pass expires.
   - **Shared Pass**: Use this option to allow multiple users to share a single guest pass.

10. Once you are satisfied with your choices, click **Generate** to create the guest pass(es).

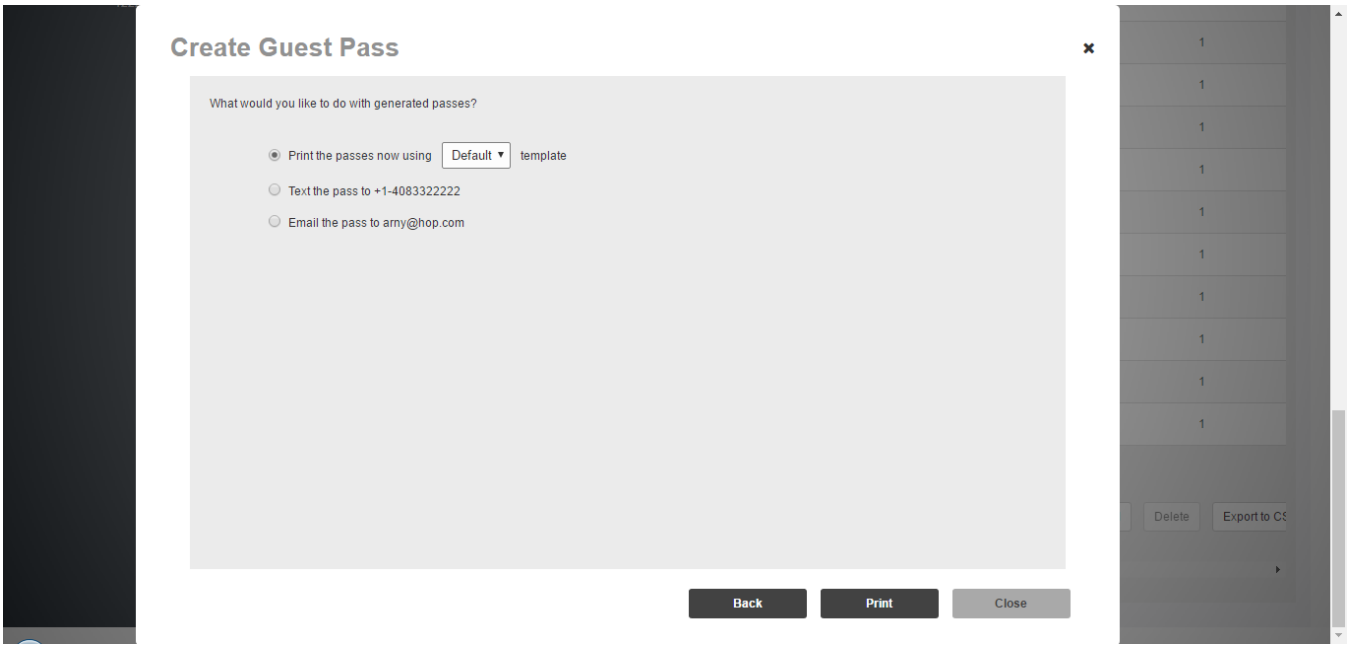
FIGURE 98 Generating a single guest pass from the Clients > Generated Guest Passes page



11. On the **Create Guest Pass** screen, select a delivery method:
    - **Print passes now using Default template**: Print the guest pass to a printer.
    - **Text the pass to [phone]**: Deliver the guest pass code via SMS text message to the phone number entered.
    - **Email the pass to [email]**: Deliver the guest pass code via email to the email address entered.
12. If you have created multiple guest passes, the options will be:
    - **Print the passes now**
    - **Download all passes now**
    - **Show me all passes and let me decide to print/SMS/email passes**

13. Click **Close** to close the delivery method selection screen. The guest pass(es) are added to the list of **Admin Generated Guest Passes**.

FIGURE 99 Select a guest pass delivery method



Configuring Guest Pass Generation

By default, all authenticated users with the Default role are allowed to generated guest passes. However, Default role users do not have ZoneDirector admin privileges, so they are unable to create guest passes from within the UI.

If you want to allow certain users to create guest passes (but not to have ZoneDirector admin privileges), you can create a new user Role for the task (and, optionally, you can also edit the Default role to disable guest pass generation privileges). Users with the new role will then be able to access an external URL (*https://[ZoneDirector-IP-Address]/guestpass/*) to generate guest passes.

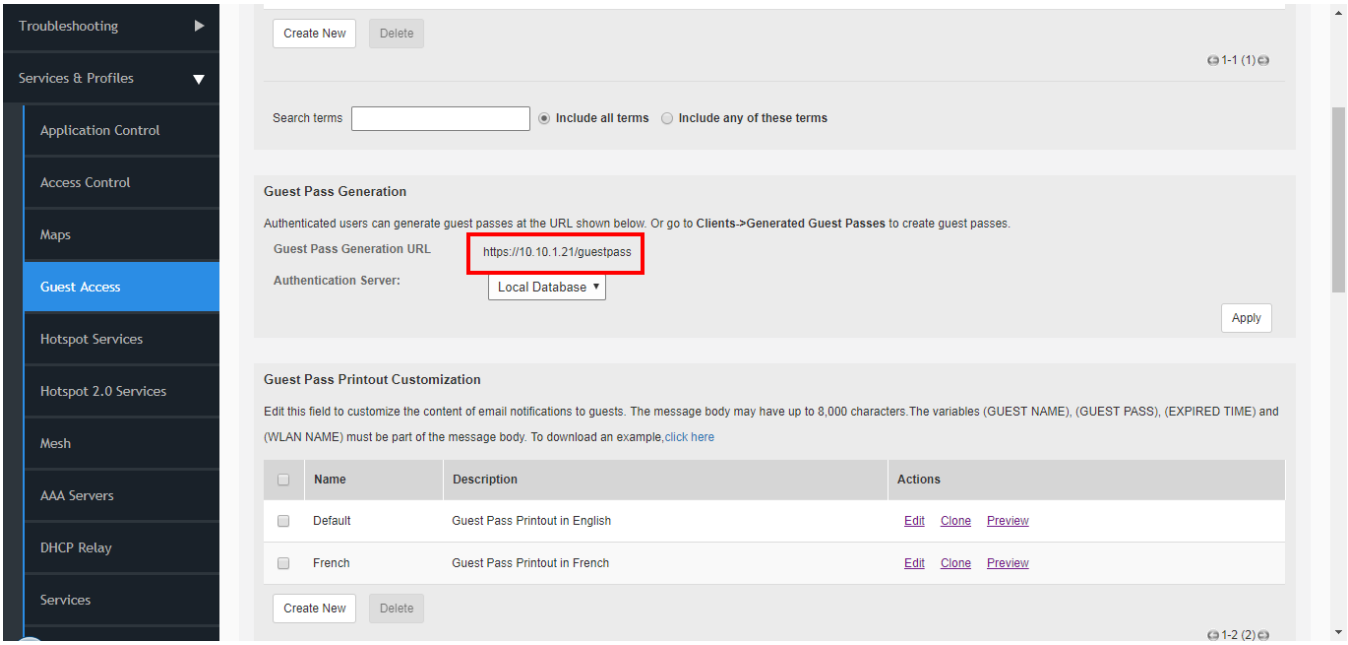
First, you will need to define how your guest pass generator users will be authenticated.

1. Go to **Services & Profiles** > **Guest Access**. The **Guest Access Service** page appears.
2. Scroll down to the **Guest Pass Generation** section.
3. In **Authentication Server**, select the authentication server that you want to use to authenticate users who want to generate guest passes.
   - If you configured an AAA server (RADIUS, Active Directory or LDAP) on the **Services & Profiles > AAA Servers** page and you want to use that server to authenticate users, select the server name from the drop-down menu. (See Using an External AAA Server on page 248.)
   - If you want to use ZoneDirector's internal database, select **Local Database**.

4. When you finish, click **Apply** to save your settings and make this new policy active.

> **NOTE**
> Remember to inform users that they can access the **Guest Pass Generation** page at https://[ZoneDirector-hostname-or-ipaddress]/guestpass. In the example, the Guest Pass Generation URL is **https://10.10.1.21/guestpass**.

FIGURE 100 The Guest Pass Generation URL



5. Next, you will need to edit the Default role to disable guest pass generation, as described in Controlling Guest Pass Generation Privileges on page 153, and create a new role with guest pass generation enabled, as described in Creating a Guest Pass Generation User Role on page 153.

Controlling Guest Pass Generation Privileges

To disable the guest pass generation privilege granted to all basic "Default" role users, follow these steps:

1. Go to **Services & Profiles** > **Roles**. When the **Roles and Policies** page appears, a table lists all existing roles, including "Default."
2. Click **Edit** (in the "Default" role row).
3. In the **Guest Pass** section, clear the **Allow Guest Pass Generation** check box.
4. Click **OK** to save your settings. Members of the "Default" role no longer have guest pass generation privileges.
5. Continue to Creating a Guest Pass Generation User Role on page 153.

Creating a Guest Pass Generation User Role

To create a guest pass generator role that can be assigned to authorized users, follow these steps:

1. Go to **Services & Profiles** > **Roles**.
2. In the **Roles** table, click **Create New**.

3. When the **Create New** form appears, configure the following options:
   - **Name**: Enter a name for this role (e.g., "Guest Pass Generator," or "Front Desk," etc.).
   - **Description**: Enter a short description of this role's application.
   - **Group Attributes**: This field is only available if you choose Active Directory as your authentication server. Enter the Active Directory User Group names here. Active Directory users with the same group attributes are automatically mapped to this user role.
   - **Allow All WLANs**: You have two options: (1) allow all users with this role to connect to all WLANs, or (2) limit this role's users to specific WLANs, and then pick the WLANs they can connect to.

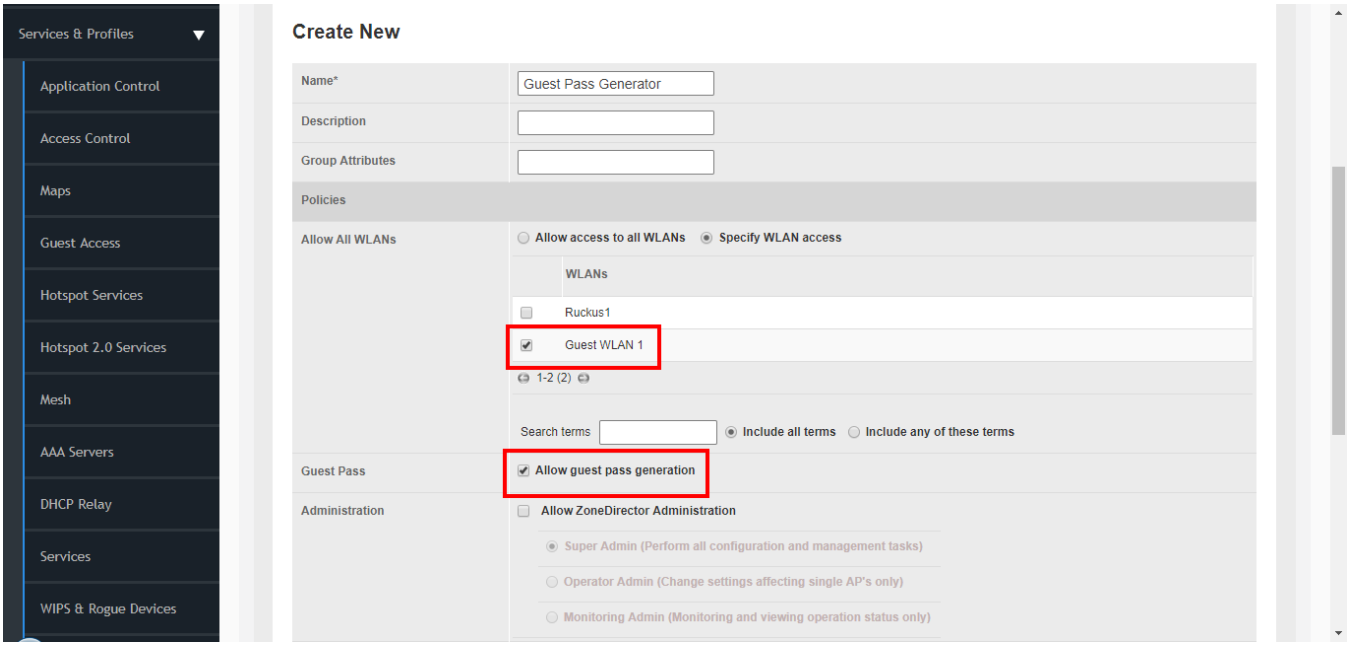
     NOTE
     When creating a guest pass generator Role, you must ensure that this Role is given access to the Guest WLAN(s). If you create a Role and allow guest pass generation, but do not allow the Role access the relevant WLAN, members of the Role will be unable to generate guest passes for the Guest WLAN.

   - **Guest Pass**: Enable this option to allow users with this role to generate guest passes.
   - **Administration**: Typically, you would want to leave this option disabled, so that your guest pass generators do not have ZoneDirector administration privileges.

     NOTE
     For more information on configuring user roles, see Creating New User Roles on page 116.

4. Click **OK** to save your settings. This new role is ready for application to authorized users.

FIGURE 101 Create a guest pass generator Role



Assigning a Pass Generator Role to a User Account

Use the following procedure to assign a guest pass generator role to a user account on the internal database.

1. Go to **Services & Profiles** > **Users**.

2. At the bottom of the **Internal User Database**, click **Create New**.
3. When the **Create New** form appears, fill in the text fields with the appropriate entries.
4. Select the desired guest pass generator role for this user from the **Role** menu.
5. Click **OK** to save your settings. Be sure to communicate the role, user name and password to the appropriate end user.

Generating and Delivering a Single Guest Pass

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

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

NOTE
The following procedure will guide you through generating and delivering a guest pass. For instructions on how to generate multiple guest passes, see Generating and Printing Multiple Guest Passes at Once on page 159.

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

To generate a single guest pass:

1. On your computer, start your web browser.
2. In the address or location bar, type the URL of the ZoneDirector Guest Pass Generation page: *https://[ZoneDirector's IP address]/guestpass*.

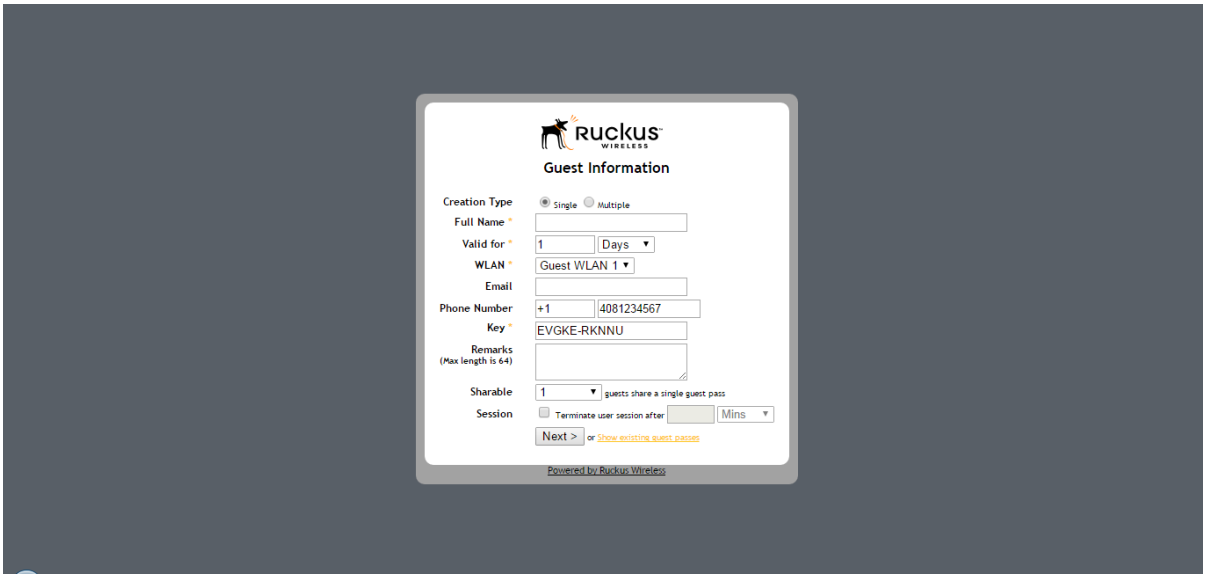
FIGURE 102 Request a Guest Pass



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

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

FIGURE 103 Creating a Guest Pass



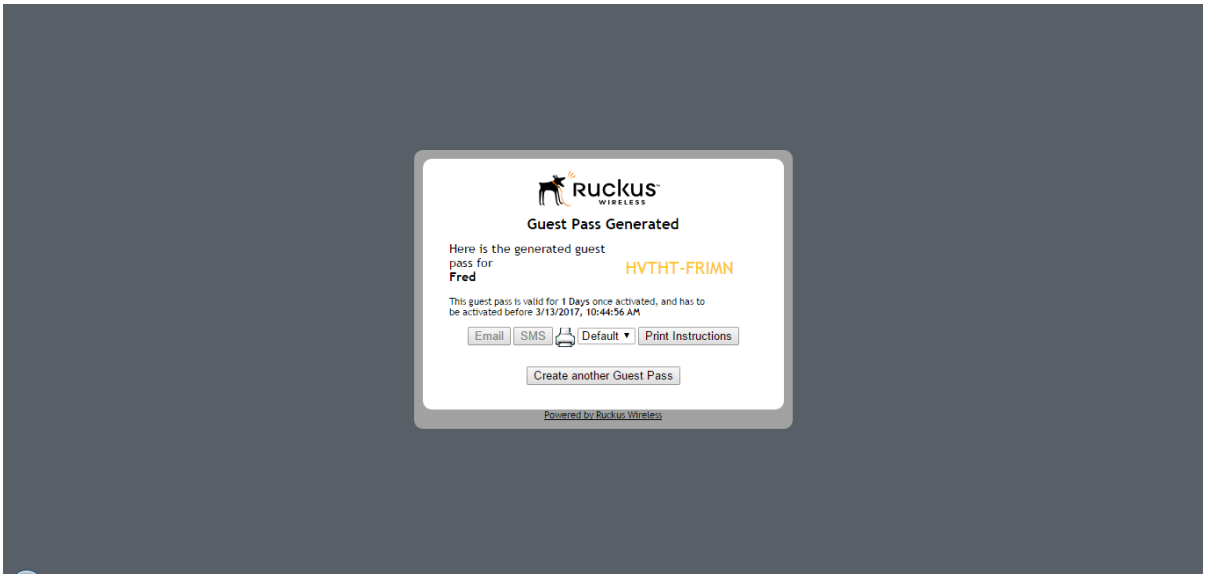
6. On the **Guest Information** page, fill in the following options:
   - **Creation Type**: Choose **Single** to generate a single guest pass. To generate multiple guest passes in batch, see Generating and Printing Multiple Guest Passes at Once on page 159.
   - **Full Name**: Type the name of the guest user for whom you are generating the guest pass.
   - **Valid for**: Specify the time period when the guest pass will be valid. Do this by typing a number in the blank box, and then selecting a time unit (Hours, Days or Weeks).
   - **WLAN**: Select the WLAN for this guest (typically, a "guest" WLAN).
   - **Email** (optional): Enter the email address for this user.
   - **Phone Number** (optional): Enter a phone number for this user.
   - **Key**: Leave as is if you want to use the random key that ZoneDirector generated. If you want to use a key that is easy to remember, delete the random key, and then type a custom key. For example, if ZoneDirector generated the random key OVEGS-RZKKF, you could change it to "joe-guest-key". Customized keys must be between one and 16 ASCII characters.

     NOTE
     Each guest pass key must be unique and is distributed on all guest WLANs.

   - **Remarks** (optional): Type any notes or comments. For example, if the guest user is a visitor from a partner organization, you could type the name of the organization.
   - **Sharable**: Use this option to allow multiple users to share a single guest pass.
   - **Session**: Enable this check box and select a time increment after which guests will be required to log in again. If this feature is disabled, connected users will not be required to re-log in until the guest pass expires.
7. Click **Next**. The **Wireless Access Portal** page appears.
8. Choose whether to activate this guest pass for either yourself or a guest, and click **Next**.

9. The **Request a Guest Pass** page appears.
10. Enter the guest **User Name** and **Password**, and click **Log In**.
11. The **Guest Pass Generated** page appears. This page presents the guest pass code and a list of options for delivering this code to your guest(s). Options include **Email** (if you configured an email address for the guest), **SMS** (if you configured a phone number for the guest) and **Print Instructions**.

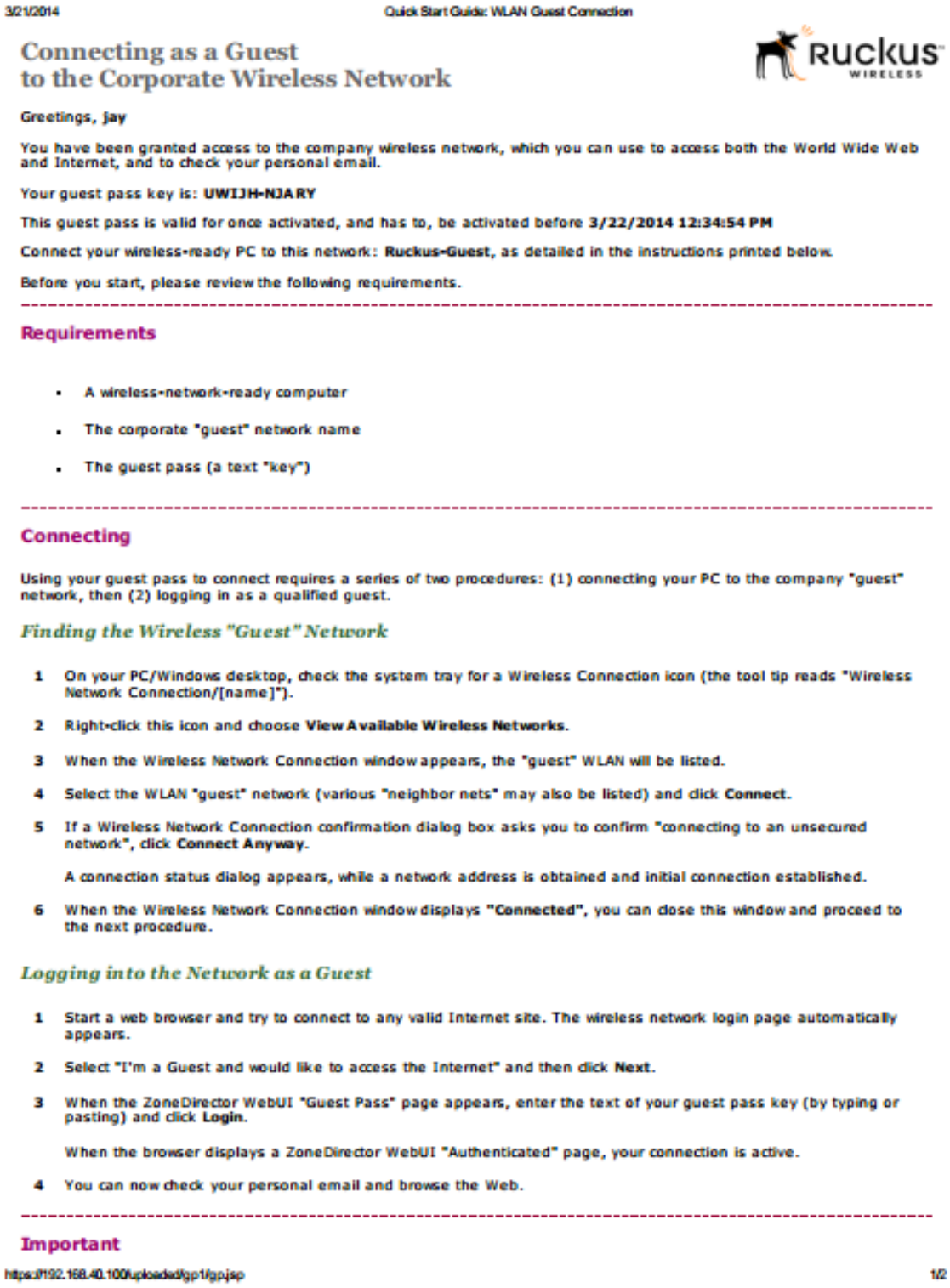
FIGURE 104 The Guest Pass Generated page



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

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

FIGURE 105 Sample guest pass printout



3/21/2014 Quick Start Guide: WLAN Guest Connection

Connecting as a Guest to the Corporate Wireless Network

Ruckus WIRELESS

Greetings, Jay

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

Your guest pass key is: **UWIJH-NJARY**

This guest pass is valid for once activated, and has to, be activated before **3/22/2014 12:34:54 PM**

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

Before you start, please review the following requirements.

Requirements

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

Connecting

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

Finding the Wireless "Guest" Network

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

   A connection status dialog appears, while a network address is obtained and initial connection established.
6. When the Wireless Network Connection window displays **"Connected"**, you can close this window and proceed to the next procedure.

Logging into the Network as a Guest

1. Start a web browser and try to connect to any valid Internet site. The wireless network login page automatically appears.
2. Select "I'm a Guest and would like to access the Internet" and then click **Next**.
3. When the ZoneDirector 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 ZoneDirector WebUI "Authenticated" page, your connection is active.
4. You can now check your personal email and browse the Web.

Important

https://192.168.40.100/uploaded/gp1/gp.jsp 1/2

Generating and Printing Multiple Guest Passes at Once

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

> **NOTE**
> The following procedure will guide you through generating and printing multiple guest passes. For instructions on how to generate a single guest pass, see Generating and Delivering a Single Guest Pass on page 155.

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

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

1. On your computer, start your web browser.
2. In the address or location bar, type the URL of the ZoneDirector Guest Pass Generation page: https://%7Bzonedirector-hostname-or-ipaddress%7D/guestpass
3. In **User Name**, type your user name.
4. In **Password**, type your password.
5. Click **Log In**. The Guest Information page appears. On this page, you need to provide information about the guest users to enable ZoneDirector to generate the guest passes.

6. On the **Guest Information** page, fill in the following options:
   - **Creation Type**: Select **Multiple**.
   - **Valid for**: Specify the time period during which the guest passes will be valid. Do this by typing a number in the blank box, and then selecting a time unit (Days, Hours, or Weeks).
   - **WLAN**: Select one of the existing WLANs with which the guest users will be allowed to associate.Using the BYOD Onboarding Portal.
   - **Number**: Select the number of guest passes that you want to generate. ZoneDirector will automatically populate the names of each user (Batch-Guest-1, Batch-Guest-2, and so on) to generate the guest passes.

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

   - **Profile (*.csv)**: If you have created a Guest Pass Profile (see Creating a Guest Pass Profile on page 161), use this option to import the file.
   - **Sharable**: Configure this option if you want to allow multiple users to share a single guest pass (default: 1; not shared).
   - **Session**: Enable this check box and select a time increment after which guests will be required to log in again. If this feature is disabled, connected users will not be required to re-log in until the guest pass expires.

   FIGURE 106 Generating multiple guest passes at once



   NOTE
   If you want to be able to identify the guest pass users by their names (for monitoring or auditing purposes in a hotel setting, for example), click **Choose File**, and upload a guest pass profile instead. See Creating a Guest Pass Profile on page 161 for more information.

7. Click **Next**. The **Guest Pass Generated** page appears, displaying the guest pass user names and expiration dates.
8. In **Select a template for Guest Pass instructions**, select the guest pass instructions that you want to print out. If you did not create custom guest pass printouts, select **Default**.

9. Print the instructions for a single guest pass or print all of them.
   - To print instructions for all new guest passes at once, click the **Print All Instructions Below** link.
   - To print instructions for a single guest pass, click the **Print** icon that is in the same row as the guest pass for which you want to print instructions. A new browser page appears and displays the guest pass instructions. At the same time, the **Print** dialog box appears.
10. Select the printer that you want to use, and then click **OK** to print the guest pass instructions.

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

Creating a Guest Pass Profile

1. Log in to the guest pass generation page, as described in Generating and Printing Multiple Guest Passes at Once on page 159.
2. In **Creation Type**, click **Multiple**.
3. Click the **click here** link in *To download a profile sample*, ***click here***.
4. Save the sample guest pass profile (in CSV format) to your computer.
5. Using a spreadsheet application, open the CSV file and edit the guest pass profile by filling out the following columns:
   - #Guest Name: Type the name of the guest user (one name per row)
   - Remarks: (Optional) Type any note or remarks about the guest pass.
   - Key: Type a guest pass key consisting of 1-16 alphanumeric characters. If you want ZoneDirector to generate the guest pass key automatically, leave this column blank.
6. Go back to the Guest Access page, and then complete steps 6 to 10 in Generating and Printing Multiple Guest Passes at Once on page 159 to upload the guest pass profile and generate multiple guest passes.

Monitoring Generated Guest Passes

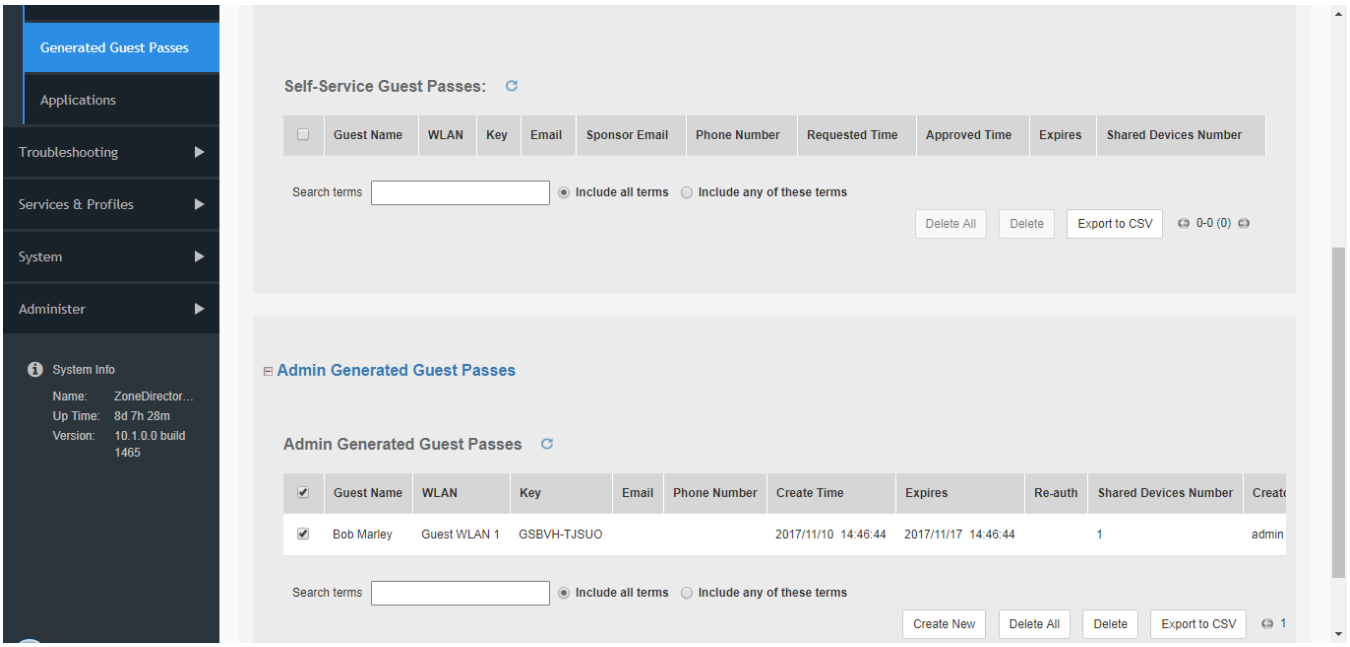
The *Generated Guest Passes* page provides options for managing guest passes.

Generated guest passes includes self-service guest passes and admin-generated guest passes. Both types can be viewed, deleted individually or deleted all at once, or exported to a CSV file. Admin-generated guest passes can also be created from this page.

1. Go to **Clients** > **Generated Guest Passes**.
2. View generated guest passes.
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.
4. Click **Export to CSV** to export the list to a CSV file that can be opened in a spreadsheet program.

5. To create new guest passes, click **Create New**. See Generating a Guest Pass from the Clients Page on page 149.

FIGURE 107 Viewing generated Guest Passes



Creating a Custom Guest Pass Printout

The guest pass printout is a printable HTML page that contains instructions for the guest pass user on how to connect to the wireless network successfully. 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 is 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 **Services & Profiles** > **Guest Access**.
2. Scroll down to the **Guest Pass Printout Customization** section.
3. Click the **click here** link under the *Guest Pass Printout Customization* section title to download the sample guest pass printout (in HTML format). Save the HTML file to your computer.

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

     NOTE
     The guest pass printout contains several tokens or variables that are substituted with actual data when the guest pass is generated. When you customize the guest pass printout, make sure that these tokens are not deleted. For more information on these tokens, see Guest Pass Printout Tokens on page 163.

   - Go back to the **Guest Pass Printout Customization** section, and then click **Create New**. The **Create New** form appears.
5. 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.
6. In **Description** (optional), add a brief description of the guest pass printout.
7. Click **Browse**, select the HTML file that you customized earlier, and then click Open. ZoneDirector copies the HTML file to its database.
8. Click **Import** to save the HTML file to the ZoneDirector database.

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

TABLE 19 Tokens that you can use in the guest pass printout

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

Delivering Guest Passes via Email

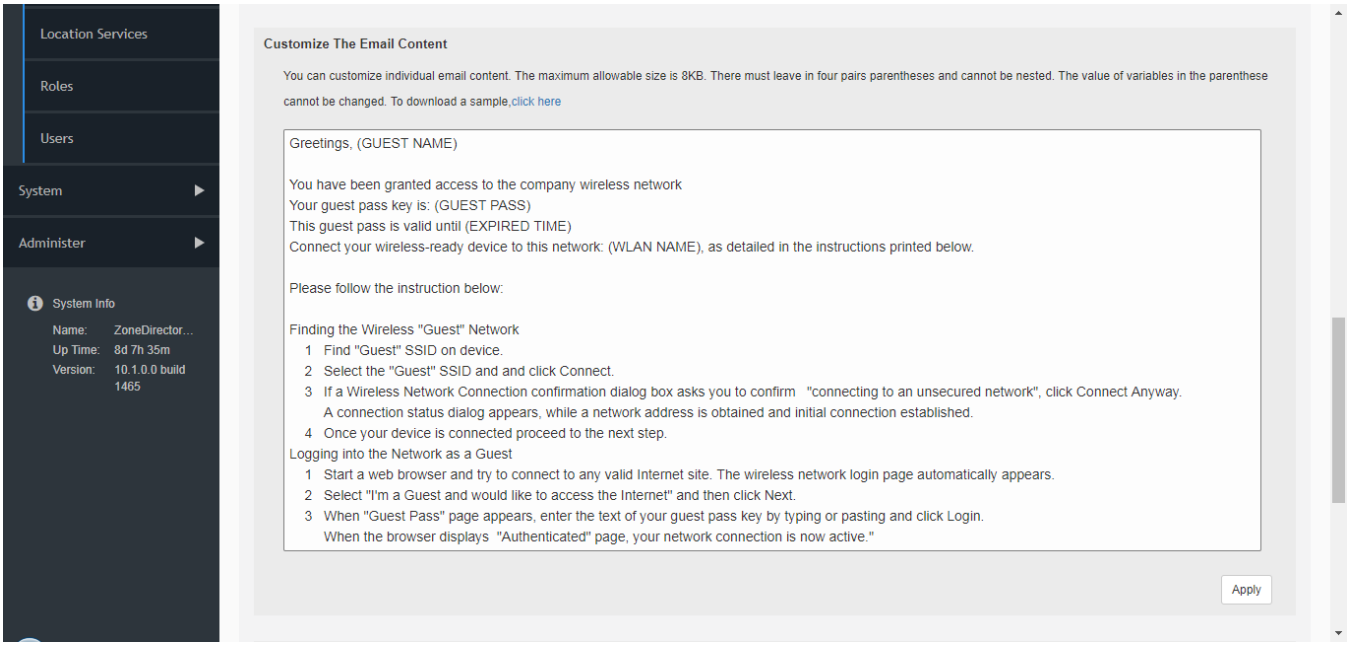
Email delivery requires that the SMTP settings on the *System Settings* page are first configured to allow ZoneDirector to use the configured email server to deliver guest passes.

For information on configuring ZoneDirector's SMTP settings for email delivery, see Setting Up Email Alarm Notifications on page 312.

To customize the content of the email message used to deliver the guest pass code, use the following procedure:

1. On the **Services & Profiles** > **Guest Access** page, locate the **Customize the Email Content** section.
2. Customize the message in the text box and click **Apply** to save your changes.

FIGURE 108 Customize the email content



Delivering Guest Passes via SMS

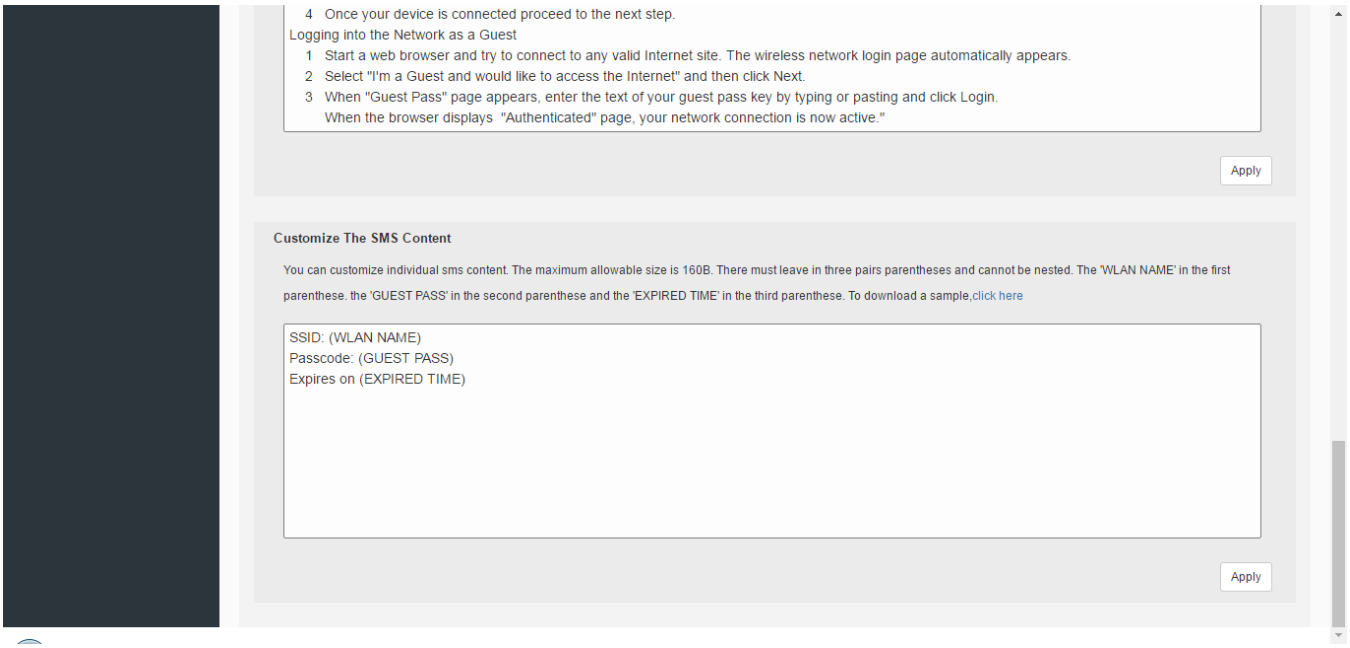
SMS delivery requires that the SMS settings on the *System Settings* page are first configured to allow ZoneDirector to use the external SMS service provider account to deliver guest passes.

For information on configuring ZoneDirector's SMS delivery settings, see Configuring SMS Settings for SMS Guest Pass Delivery on page 315.
To customize the content of the SMS message used to deliver the guest pass code, use the following procedure:

1. On the **Services & Profiles** > **Guest Access** page, locate the **Customize the SMS Content** section.

2. Customize the message in the text box and click **Apply** to save your changes.

FIGURE 109 Customize the SMS content



NOTE
For more information on Captive Portal redirection for Hotspot, Web Auth and Guest Access WLANs, see Captive Portal Redirect on Initial Browser HTTPS Request on page 123.

Social Auth WLANs

Social Auth WLANs allow guest users to access the wireless network 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
- Google/Google+
- LinkedIn
- Microsoft
- WeChat

About the Ruckus Facebook Wi-Fi Implementation

Business owners can use this WLAN type to require users to visit the business owner's Facebook page and log 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*.

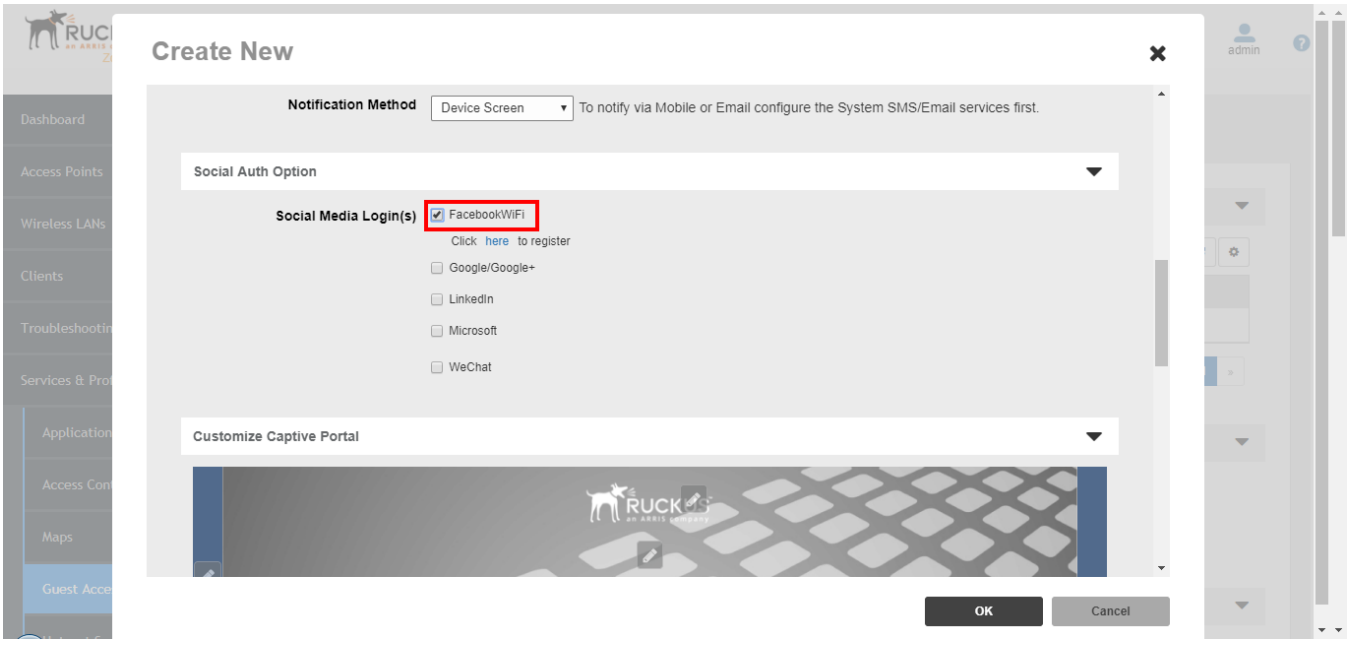
The following caveats and limitations should be considered before deploying a Facebook Wi-Fi WLAN:

- The maximum number of Facebook Wi-Fi profiles that can be created on ZoneDirector is four (4).
- Users must launch a browser to trigger the Facebook authentication.
- Invalid users are determined by Facebook. ZoneDirector 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 ZoneDirector fails to receive a response, it will re-send the request four times. If there is no response after five requests, ZoneDirector will delete the related stations.

To enable a Facebook Wi-Fi social media WLAN:

1. Go to **Services & Profiles > Guest Access**.
2. Click **Create** to create a new guest access service.
3. In **Authentication**, select **Use Guest Pass and Social login authentication or Use Social login authentication only**.
4. Under **Social Auth Options**, select **Facebook Wi-Fi**, and click the **Click here to register** button.
5. A new browser window opens to allow you to log into your Facebook account.
6. Configure the Facebook Wi-Fi settings according to your preferences:
   - **Facebook Page**: If you have multiple Facebook Pages, select the one that is associated with your business's location.
   - **Bypass Mode**: Choose whether customers can use a Wi-Fi code that you give them or click on a link to skip checking in.
   - **Session Length**: Configure the length of time to allow guests to access the network without having to check in again.
   - **Terms of Service**: Select whether to display and require users to accept a Terms of Service agreement.
   - Click **Save Settings**.
7. Click **OK** to save the profile.

FIGURE 110 Configure a Facebook Wi-Fi profile



OAuth Social Media Types

For Google+, LinkedIn and Windows Live Social Media login methods, you must enter an Application ID and Application Secret.

These social media login methods (LinkedIn, Google+, Windows Live) comply with the OAuth 2.0 specification. For more information on OAuth 2.0, refer to the OAuth website, *http://oauth.net*.

Refer to the documentation for the social media website for which you want to provide social media login to obtain this information for your social media account.

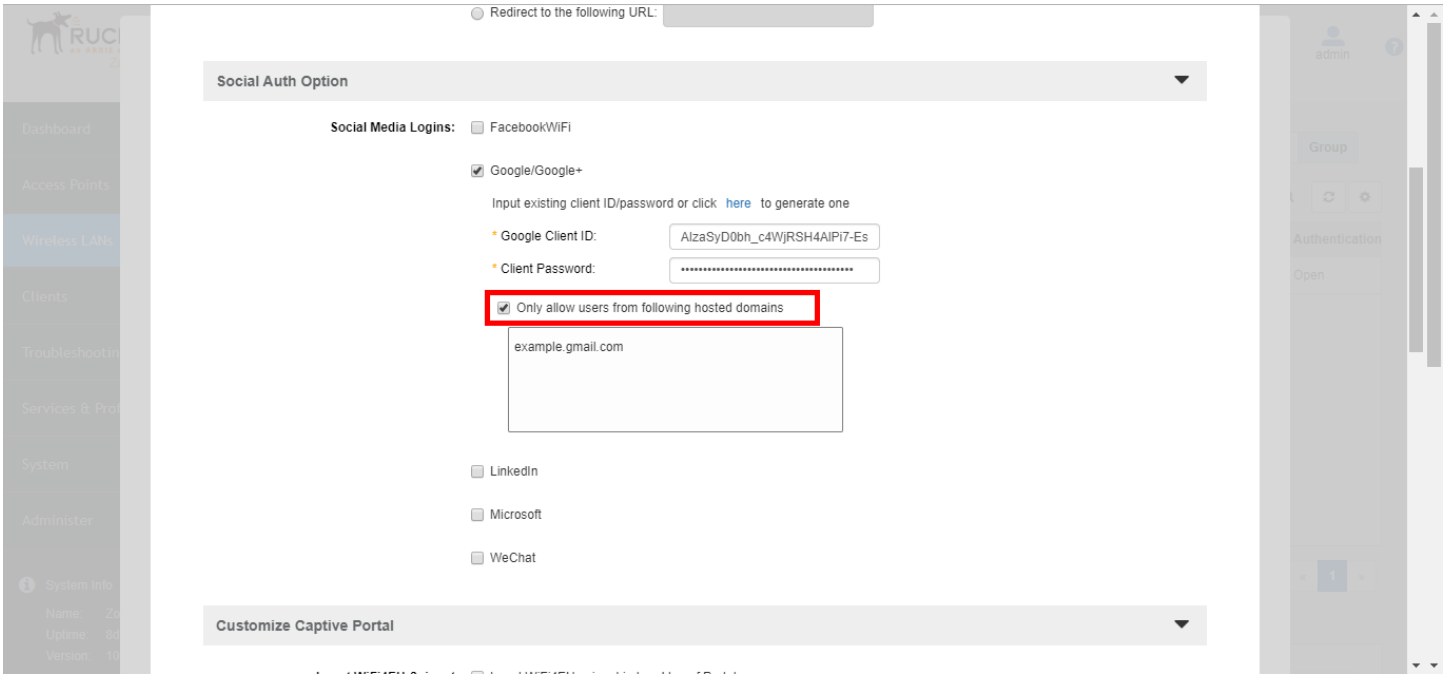
OAuth Setup Procedure for Google+ Social Media Login

The following instructions provide an example of the setup procedure for deploying a Google+ Social Media WLAN.

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 or new lines, in the text box below.

For example, if a company that uses Gmail accounts wants to limit access to the WLAN to Google accounts that match the company's domain name, enable this feature and enter the company's Google domain (company_name.gmail.com). This will prevent any other @gmail.com accounts from being used to access this WLAN.

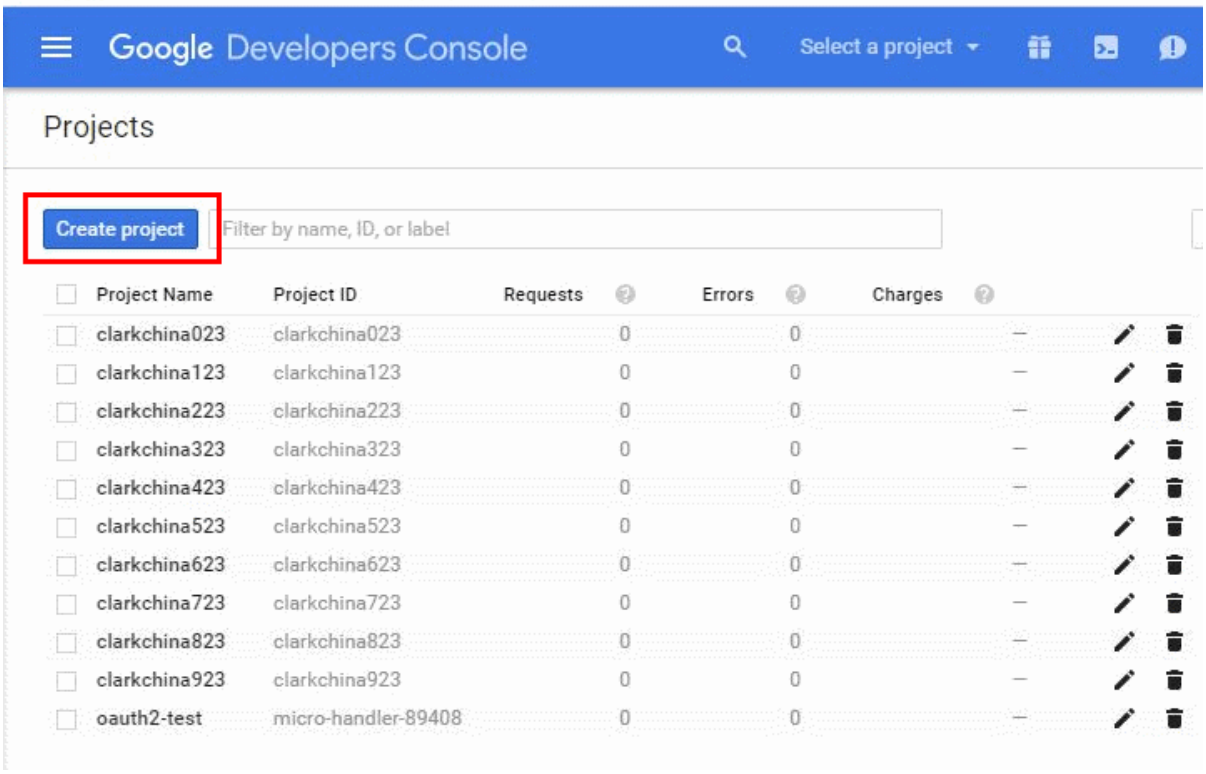
FIGURE 111 Only allow users from specified domains



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

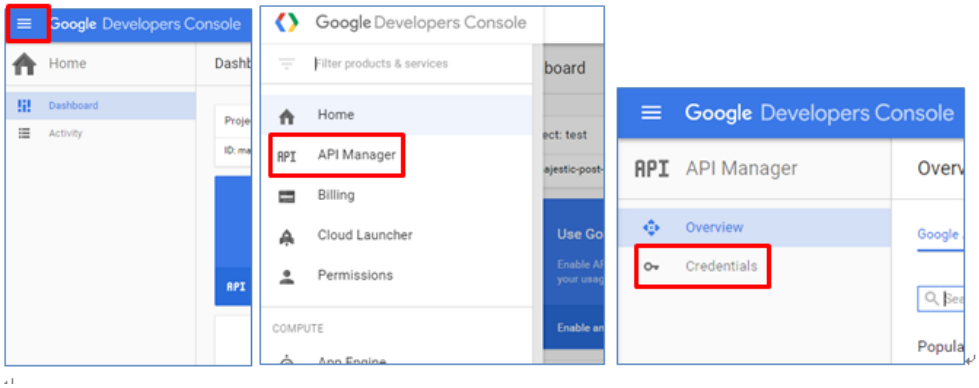
   NOTE
   Alternatively, click the **Click here** link to create a new application/project link from within the ZoneDirector guest access settings.

FIGURE 112 Create new project on Google OAuth Console



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

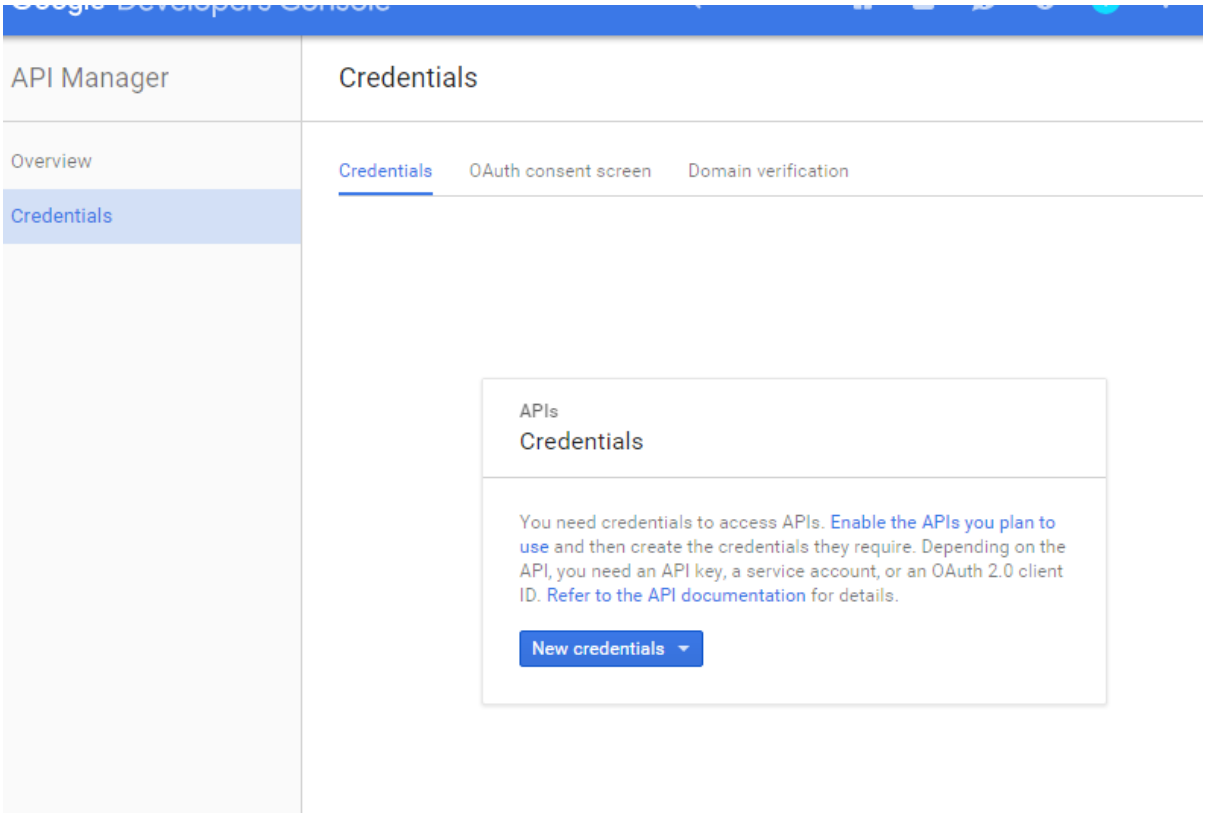
FIGURE 113 How to get to the Credentials page



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

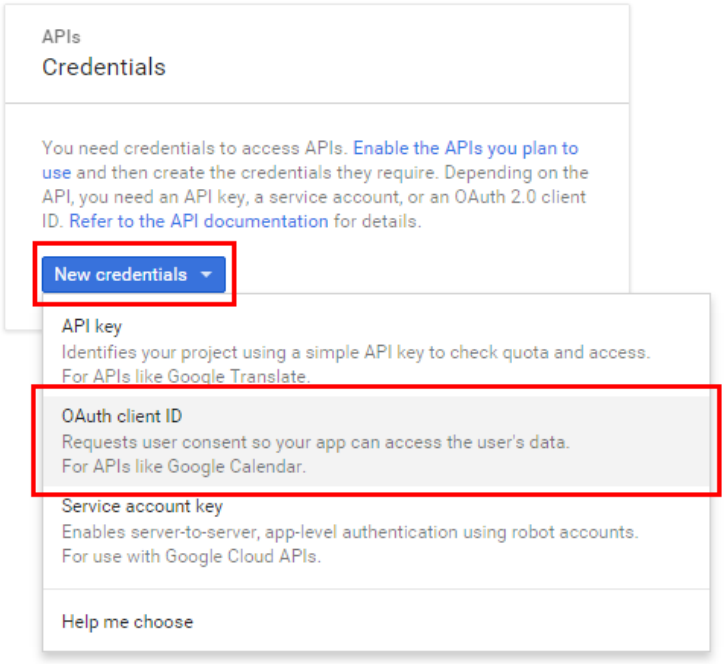
3. The **Credentials** page appears, as shown below.

FIGURE 114 Credentials page



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

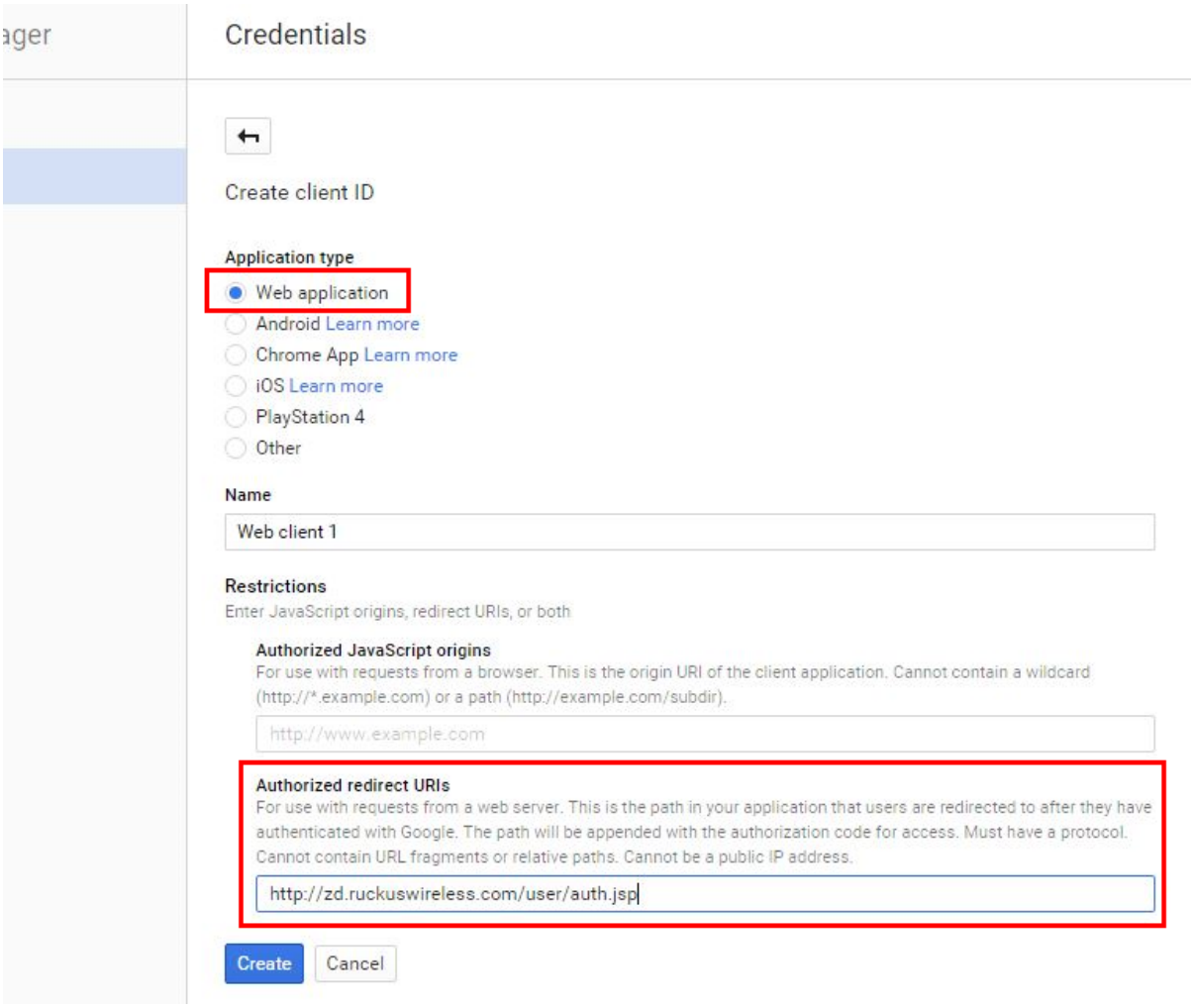
FIGURE 115 New credentials - OAuth client ID



5. For Application type, select Web application, and for Authorized redirect URIs, enter http://zd.ruckuswireless.com/user/auth.jsp as shown below.

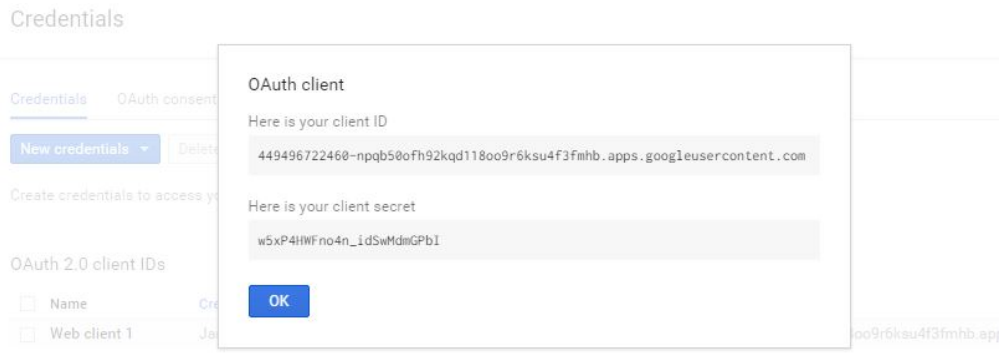
NOTE
If you have imported a certificate with FQDN to ZoneDirector, you should use the real FQDN instead of "zd.ruckuswireless.com". For example, if the FQDN is "mydomain.com", the Authorized redirect URIs should be "http://mydomain.com/user/auth.jsp".

FIGURE 116 Select Web application and enter Authorized redirect URI



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

FIGURE 117 OAuth Client ID and Client Secret

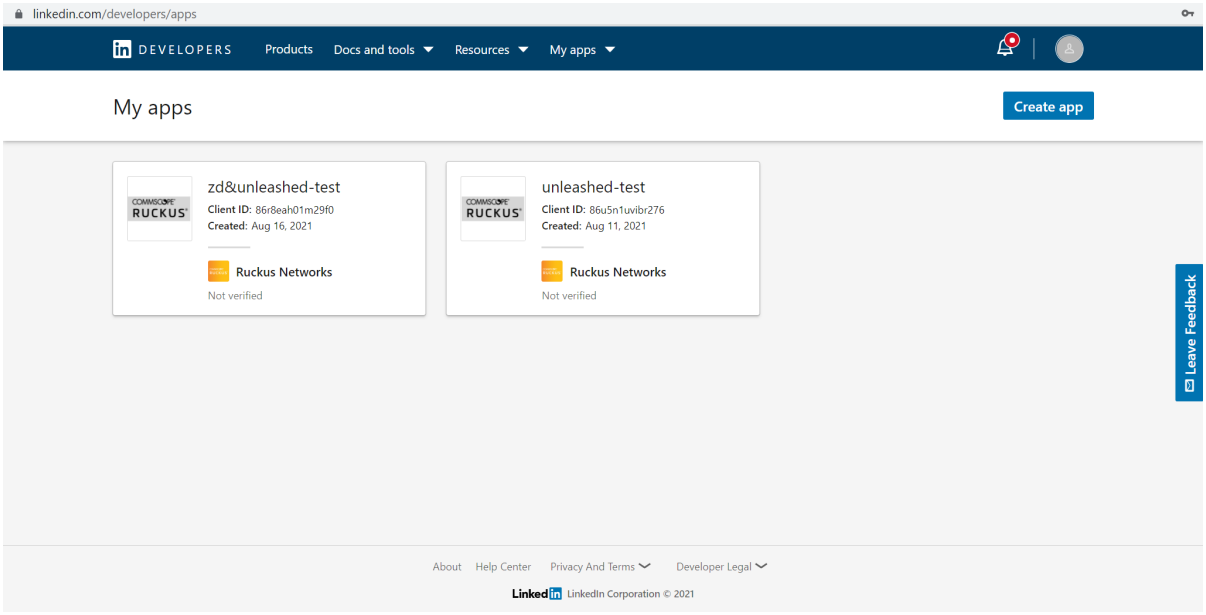


7. Take note of the **Client ID** and **Client Secret**. You will need to enter these values into the ZoneDirector web interface.
8. Continue to Create an OAuth2.0 WLAN on ZoneDirector on page 179.

OAuth Setup Procedure for LinkedIn Social Media Login

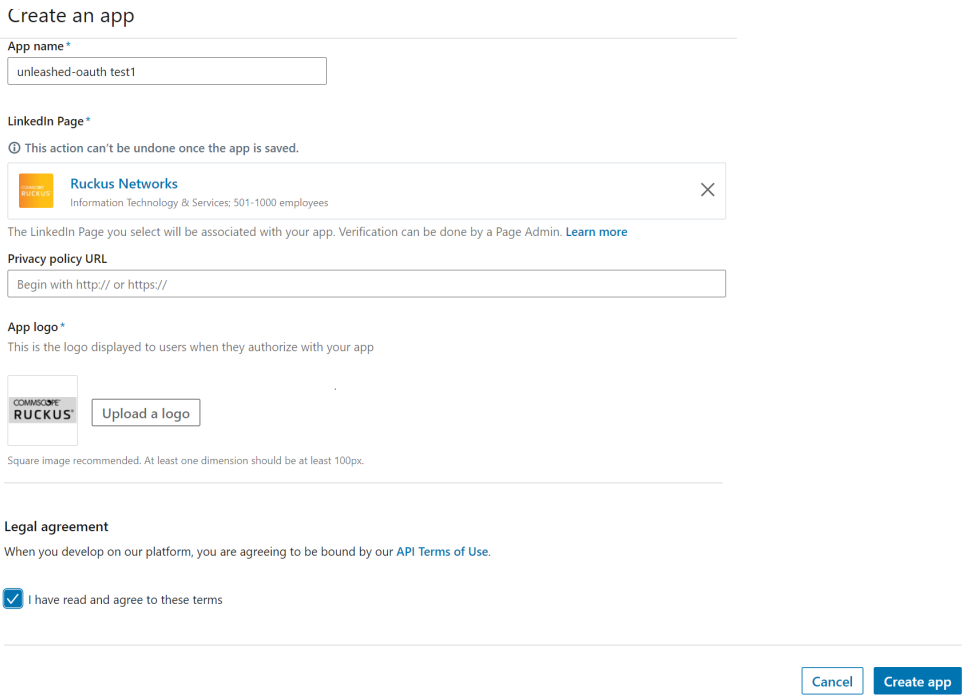
1. Go to the following URL to access the LinkedIn developer network: https://www.linkedin.com/developer/apps and click **Create App**.

FIGURE 118 LinkedIn My Applications



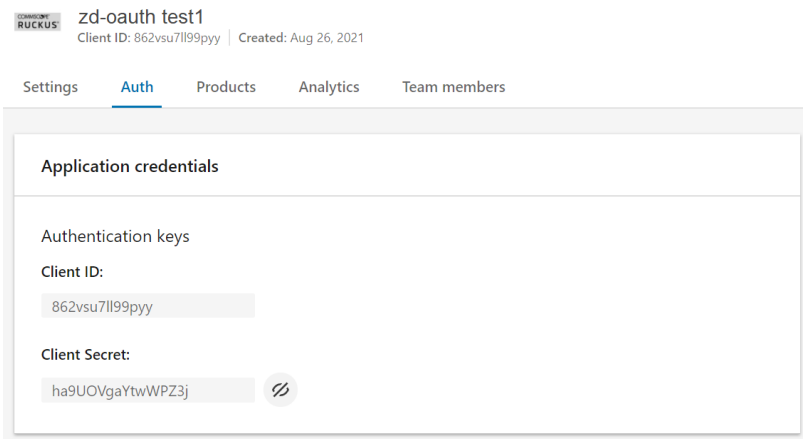
2. Enter the required application information and click **Create app**.

FIGURE 119 Create a New LinkedIn Application



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

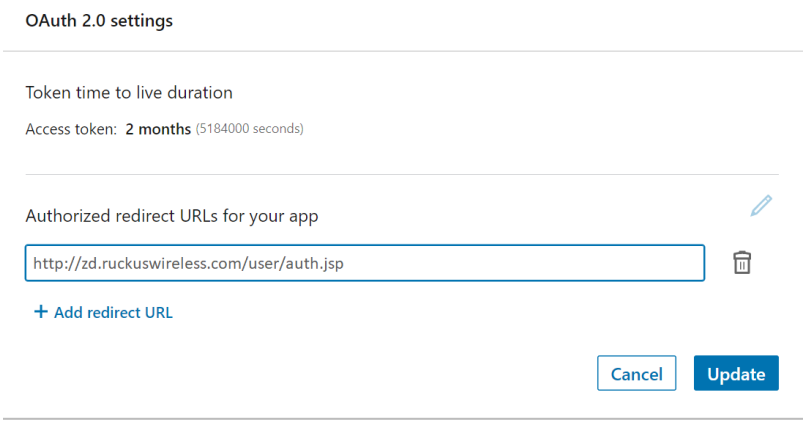
FIGURE 120 LinkedIn Authentication Keys



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

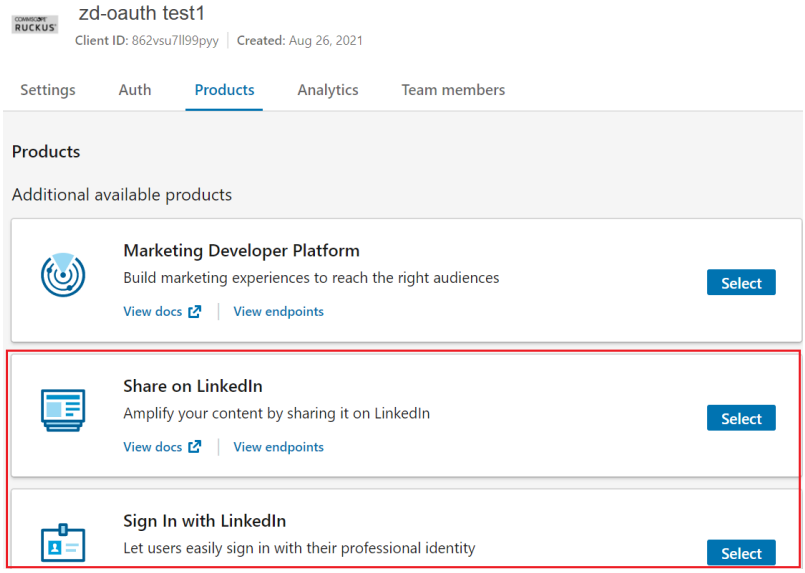
   NOTE
   If you have imported a certificate with FQDN to ZoneDirector, you must use the real FQDN instead of "zd.ruckuswireless.com". For example, if the FQDN is "mydomain.com", the authorized redirect URI must be "http://mydomain.com/user/auth.jsp".

FIGURE 121 Entering the Authorized Redirect URI



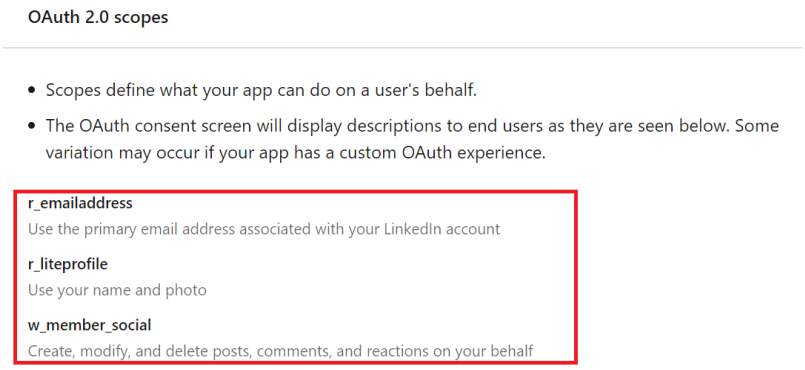
5. Under the **Product** tab, select the options **Share on LinkedIn** and **Sign In with LinkedIn**.

FIGURE 122 Sharing and Signing with LinkedIn



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

FIGURE 123 Checking the Permissions Added for Linkedin Login

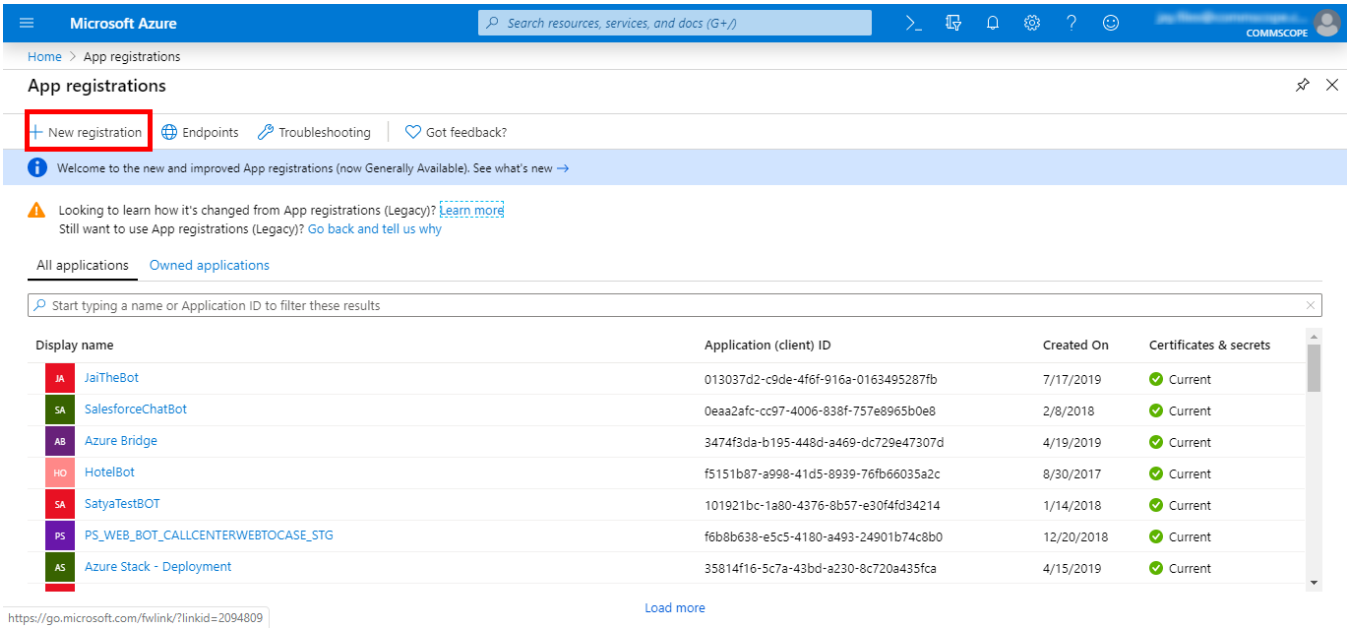


OAuth Setup Procedure for Microsoft Live Social Media Login

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 124 Creating a New App Registration

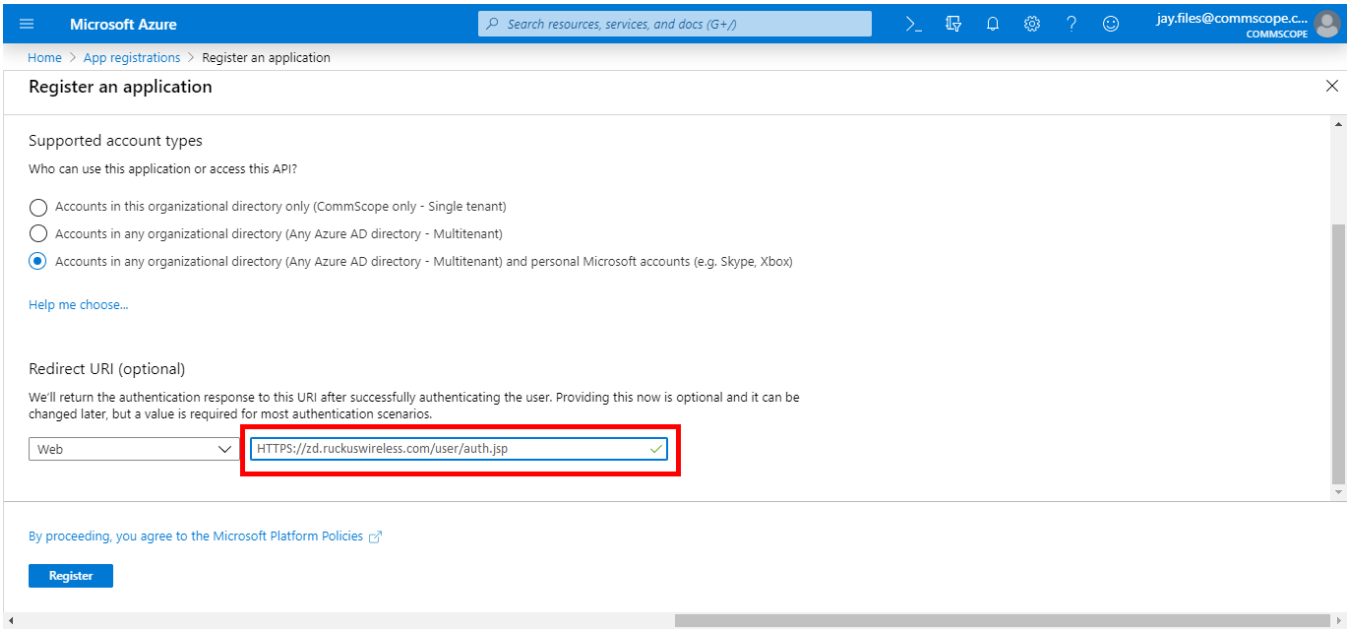


3. Enter a **Name** for the application.

4. For **Support Account Types**, select the **Accounts in any organizational directory and personal Microsoft accounts** button (refer Figure 125).
5. In, **Redirect URI:**, provide a valid redirect callback URL, for example:
   - HTTPS://zd.ruckuswireless.com/user/auth.jsp

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

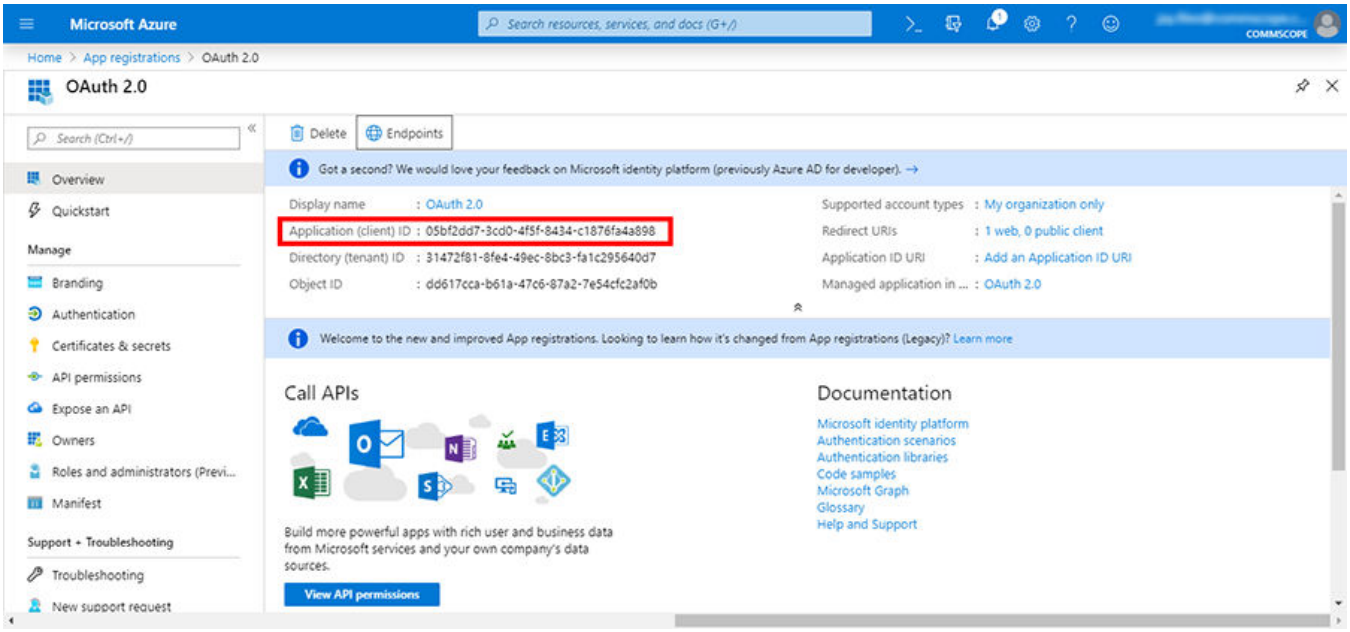
FIGURE 125 Registering an Application



6. Click **Register**.

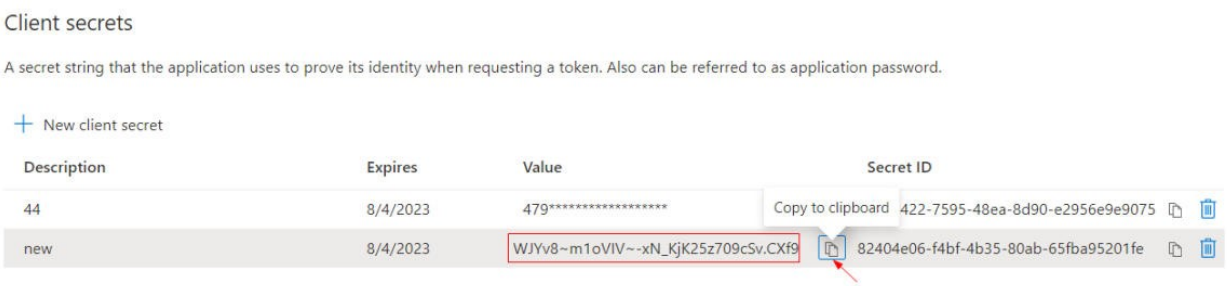
7. Microsoft will provide you with the **Application (client) ID**. Take note of these values, as you will need to enter them into the ZoneDirector web interface later.

   FIGURE 126 Taking Note of Application (Client) ID



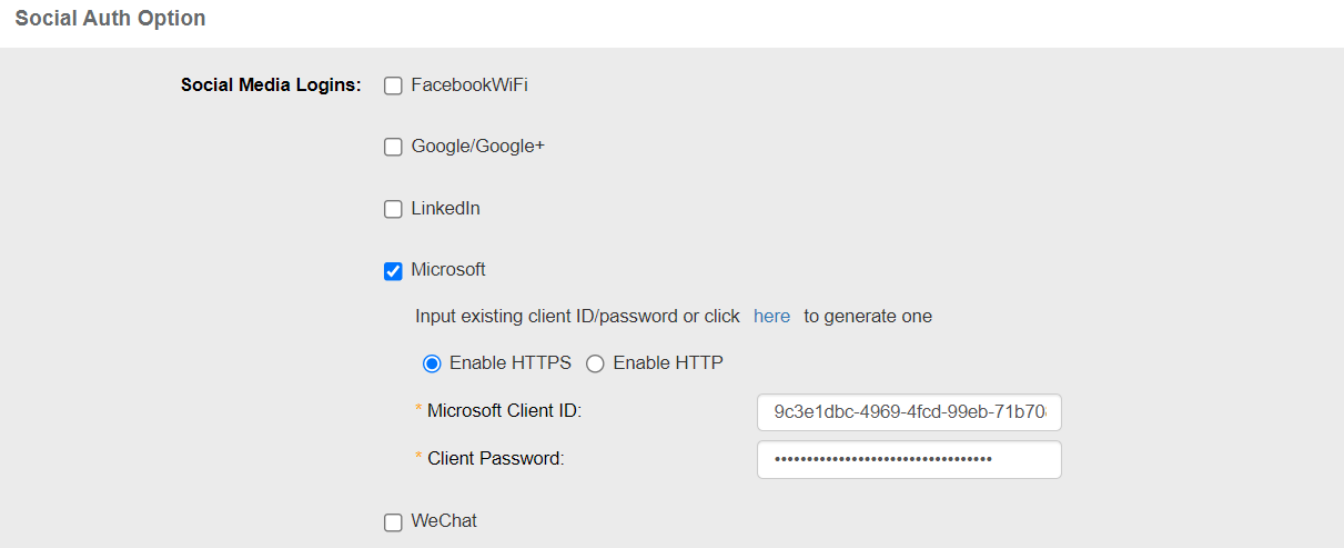
8. Create a client secret by completing the following steps:
   a) Under **Manage**, select **Certificates & secrets**.
   b) Select the **New client secret** button.
   c) Enter a value in **Description**, select any option for **Expires**, then click **Add**.
   d) Copy and save the client secret value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

   FIGURE 127 Taking Note of Client Secret



9. In the ZoneDirector UI, use the following settings on the **Create WLAN configuration** screen as shown.
   - Social Media Logins: Select **Microsoft**.
   - Microsoft Client ID: This is the Application (Client) ID shown in Figure 126.
   - Client Password: The client secret described in Figure 127.

   FIGURE 128 Creating WLAN Configuration - Microsoft Social Media Login



   Alternatively, you can create a Guest Access Service from the **Services & Profiles** > **Guest Access** > **Guest Access Service** > **Create**. (Refer to Creating a Guest Access Service on page 125.)

Create an OAuth2.0 WLAN on ZoneDirector

Once you have generated an application Client ID and Client Password for your OAuth 2.0 application, perform the following procedure to create an OAuth 2.0 Social Media WLAN on the ZoneDirector web interface.

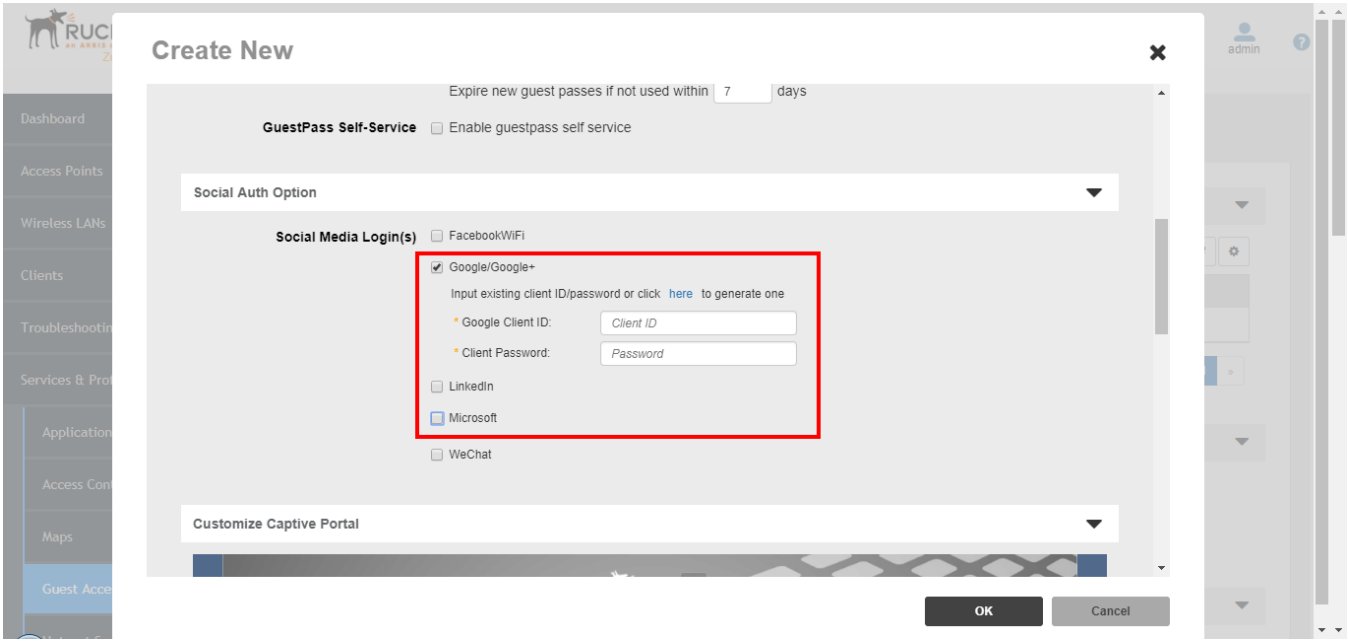
1. Go to **Wireless LANs** and create a WLAN.
2. In the **Type** option, select **Guest Access**.
3. In *Guest Access Service*, click **+ Create**.

   The *Create New* guest access service window appears.
4. In *Social Auth Options*, select one or more OAuth 2.0 social media login options:
   - Google/Google+
   - LlinkedIn
   - Microsoft

     NOTE
     WeChat requires a separate setup procedure and is not OAuth 2.0 compatible. For WeChat social media login, see *WeChat WLANs*.
5. Input the **Client ID** and **Client Password**.

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

FIGURE 129 Creating an OAuth 2.0 guest access profile



User Login to Social Media WLAN

Once your OAuth 2.0 Social Media WLAN is deployed, users can login and begin using your network. Use the following procedure:

1. Connect to an OAuth 2.0 wlan.
2. Launch your web browser and attempt to visit any HTTP or HTTPS web page.

3. ZoneDirector will redirect the user to the social media site's *Login* page.

FIGURE 130 Google Login page

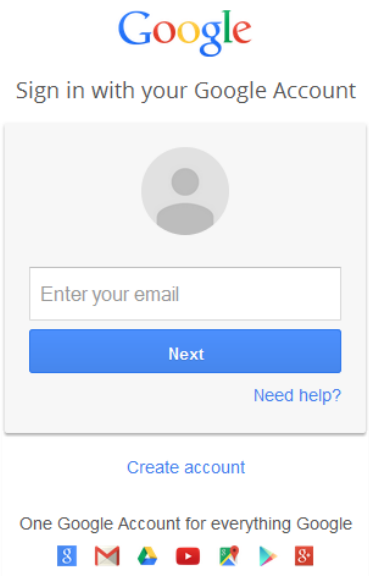


FIGURE 131 LinkedIn Login page

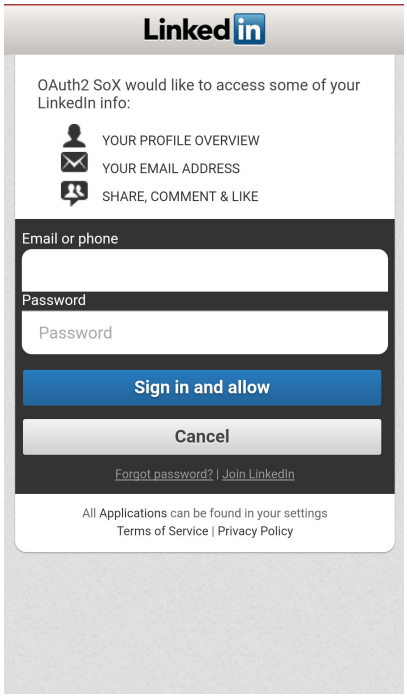
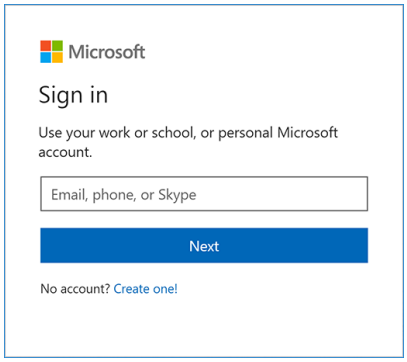
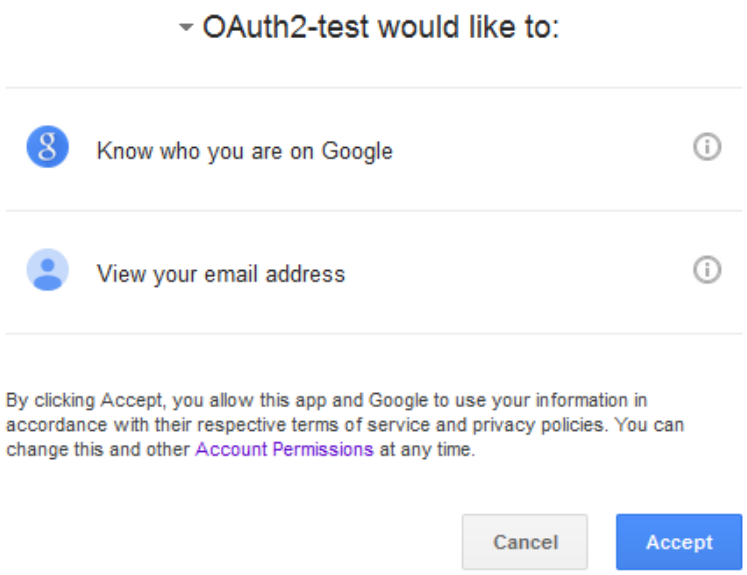


FIGURE 132 Microsoft Login page



4. Enter login details and authenticate. After authentication to a Google OAuth 2.0 WLAN, the end user will see the following screen ("Accept" screens for other social media sites are similar):

FIGURE 133 Click Accept to continue



NOTE
This confirmation screen will only be displayed once, the first time the user logs in, unless the user revokes the relationship from the Google account management center.

5. Click **Accept**. ZoneDirector immediately sets the user to authenticated state, and the user can now access the wireless network and the Internet.

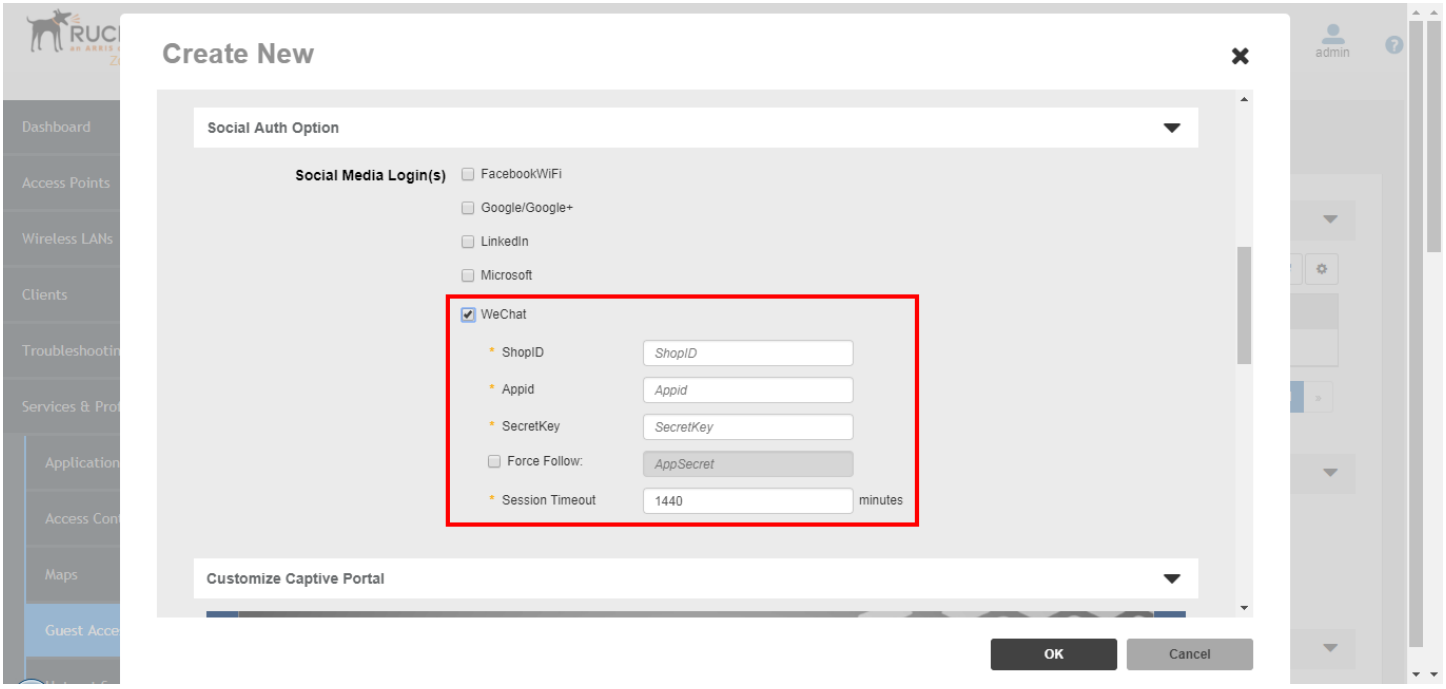
WeChat WLANs

"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.

> **NOTE**
> The ZoneDirector WeChat WLAN implementation supports the WeChat mobile app only; the desktop version is not supported, nor are smart phones without the WeChat app (via web browser).

FIGURE 134 Creating a WeChat login WLAN



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.

   FIGURE 135 WeChat login welcome screen

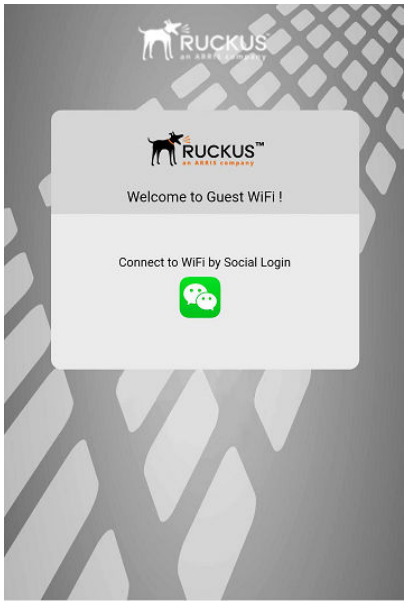
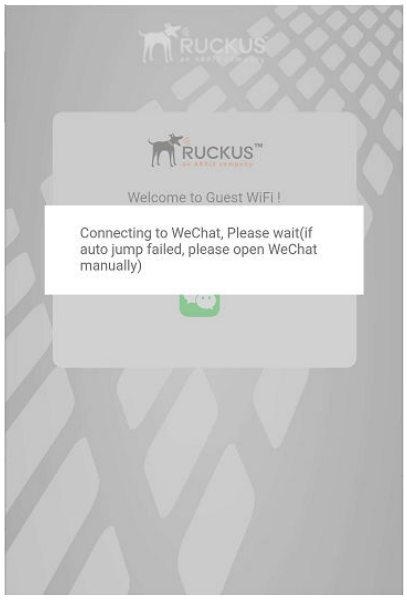


   FIGURE 136 Connecting via WeChat app



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.

Working with Hotspot Services

A hotspot is a venue or area that provides Internet access to devices with wireless networking capability such as notebooks and smart phones.

Hotspots are commonly available in public venues such as hotels, airports, coffee shops and shopping malls. ZoneDirector provides two types of Hotspot services based on the WISPr (Wireless Internet Service Provider roaming) 1.0 and 2.0 specifications, as described in the following sections.

Creating a Hotspot Service

ZoneDirector's *Hotspot Services* page can be used to configure a traditional (WISPr 1.0) hotspot service to provide public access to users via its WLANs.

> **NOTE**
> For information on Hotspot 2.0 WLANs, see Creating a Hotspot 2.0 Service on page 191.

In addition to ZoneDirector and its managed 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 http://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.

ZoneDirector supports up to 32 WISPr Hotspot service entries, each of which can be assigned to multiple WLANs.

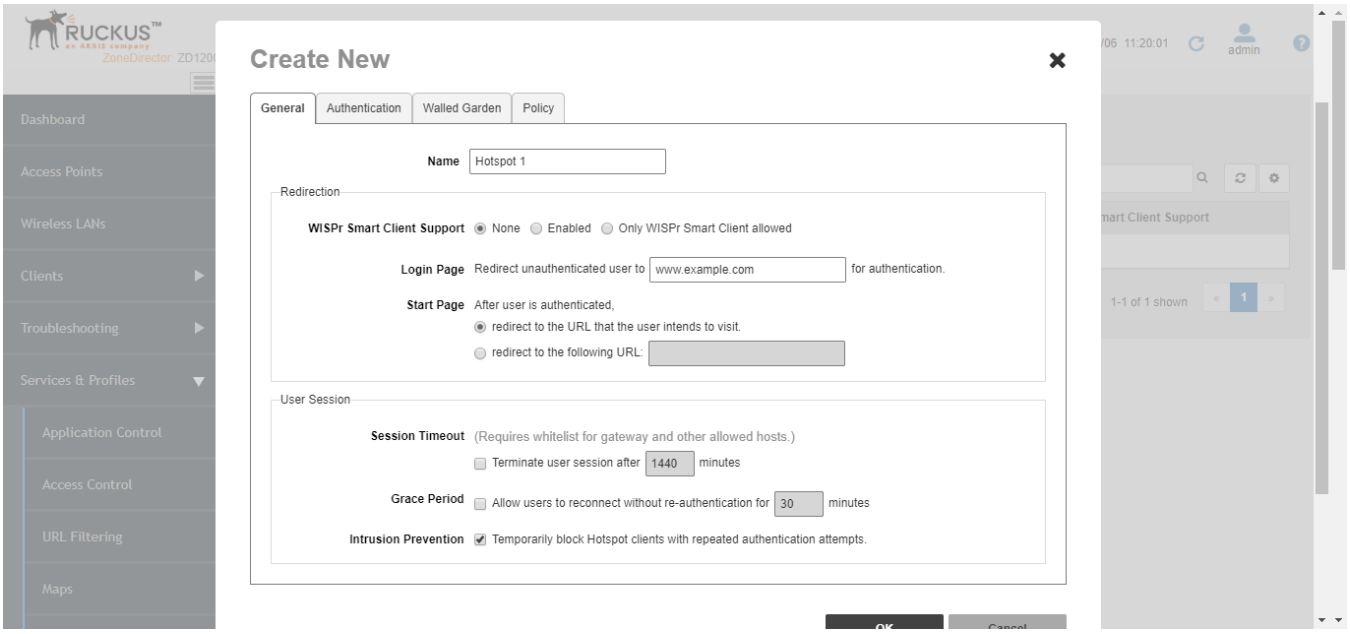
To create a Hotspot service:

1. Go to **Services & Profiles** > **Hotspot Services**.

2. Click **Create New**. The *Create New* form appears.

> **NOTE**
> Alternatively, you can create a Hotspot service from the WLAN creation page while creating a new WLAN or modifying an existing WLAN (**Wireless LANs > Edit > Type > Hotspot Service (WISPr) > Hotspot Services > Create New**.)

FIGURE 137 Creating a Hotspot service



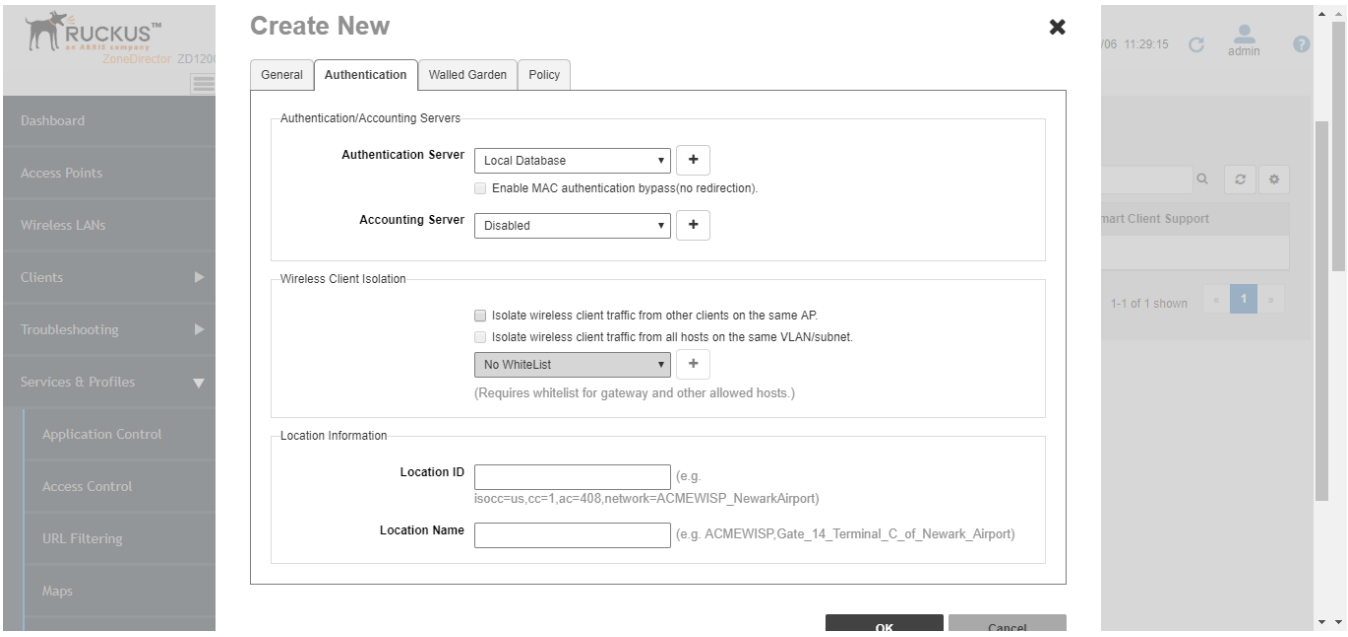
3. In **Name**, enter a name for this hotspot service. (You will need to choose this name from a list when creating a WLAN to serve this hotspot service.)
4. In **WISPr Smart Client Support**, select whether to allow WISPr Smart Client support:
   - **None**: (default).
   - **Enabled**: Enable Smart 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 (under Redirection), type the URL of the captive portal (the page where hotspot users can log in to access the service).
6. 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).

7. In **User Session**, configure session timeout and grace period, both disabled by default, and enable or disable intrusion prevention to block hotspot clients that attempt to authenticate unsuccessfully too many times.
   - **Session Timeout**: Specify a time limit after which users will be disconnected and required to log in again.
   - **Grace Period**: Allow disconnected users a grace period after disconnection, during which clients will not need to re-authenticate. Enter a number in minutes, between 1 and 144,000.
   - **Intrusion Prevention**: Temporarily block Hotspot clients with repeated authentication attempts (enabled by default). When this option is enabled, if the same station attempts to authenticate 10 times unsuccessfully within 300 seconds, the station will be blocked for 300 seconds. If the same user unsuccessfully attempts to authenticate 30 times within the same time period, the user will be blocked for 300 seconds.
8. Configure authentication settings by clicking the **Authentication** tab.

FIGURE 138 Hotspot Authentication settings



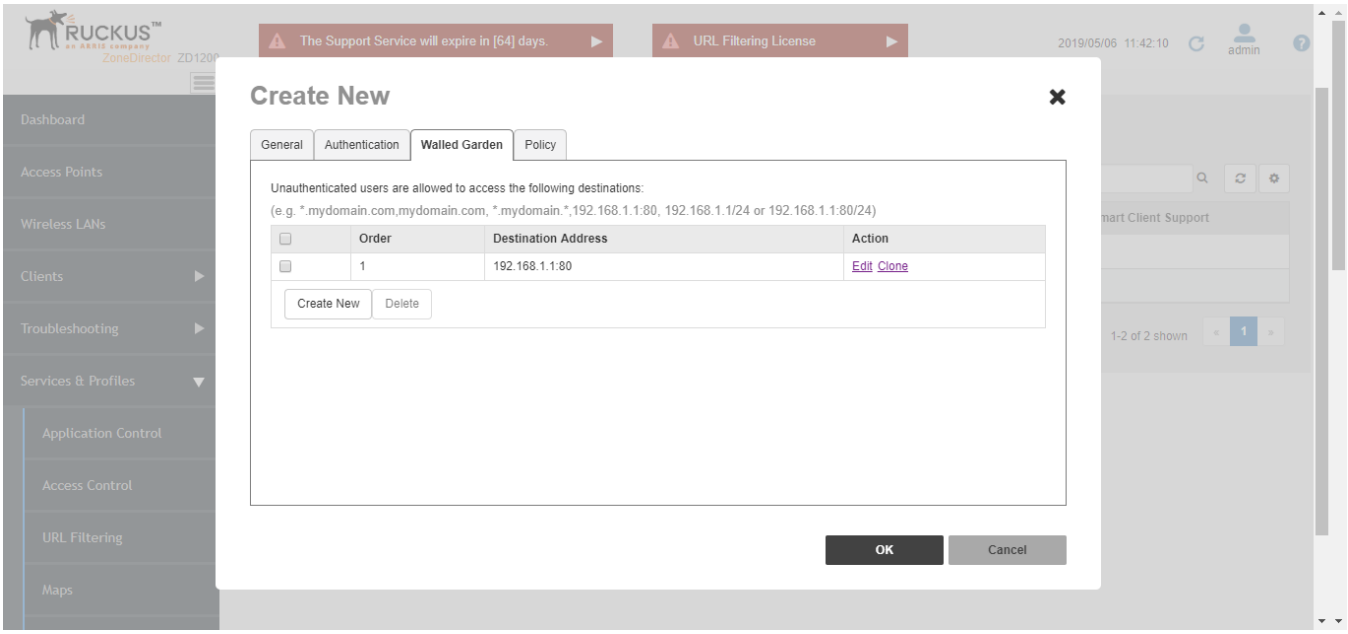
9. In **Authentication Server**, select the AAA server that you want to use to authenticate users.

   NOTE
   Alternatively, you can create an AAA server from the Hotspot configuration page while creating a new WLAN or modifying an existing WLAN.

   - Options include *Local Database* and any AAA servers that you configured on the *Services & Profiles > AAA Servers* page. If a RADIUS server is selected, an additional option appears: Enable MAC authentication bypass (no redirection).
   - **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*.
10. In **Accounting Server**, (if you have an accounting server configured), select the server from the list and configure the frequency (in minutes) at which accounting data will be retrieved.

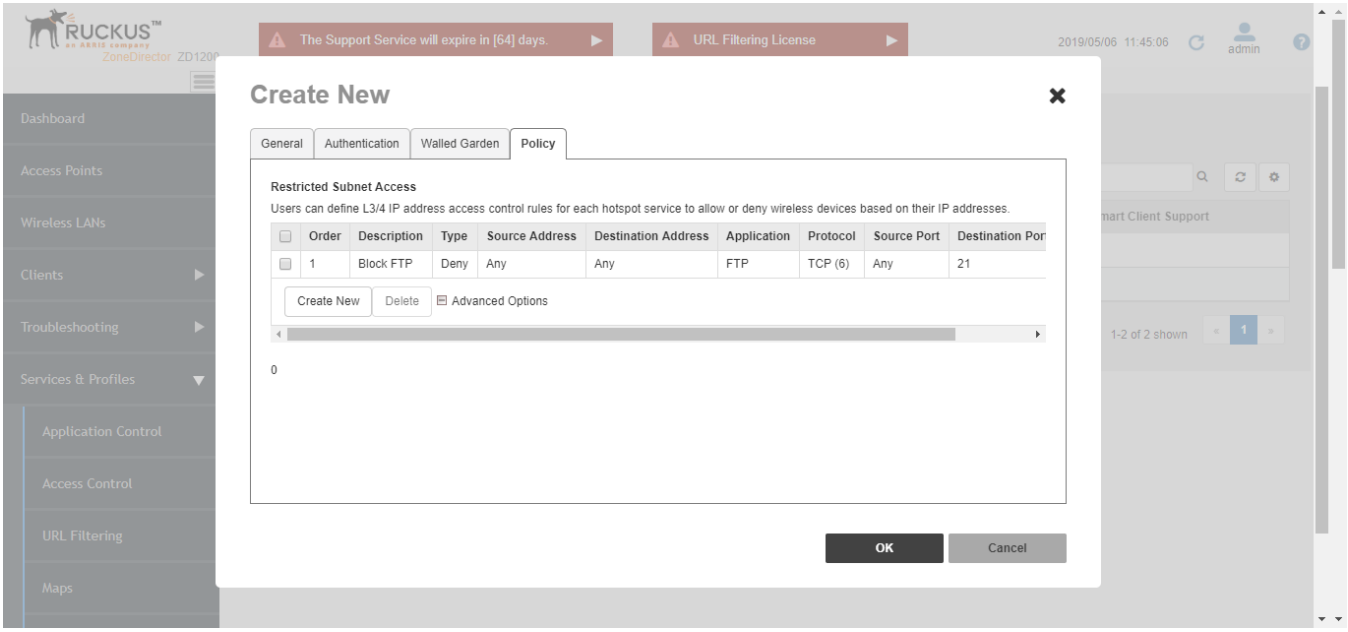
11. In **Wireless Client Isolation**, choose whether clients connected to this Hotspot WLAN should be allowed to communicate with one another locally. See Advanced WLAN Options on page 72 in *Creating a WLAN* for a description of the same feature for regular (non-Hotspot) WLANs.
12. Configure optional **Location Information** settings as preferred. Enter **Location ID** and **Location Name** WISPr attributes, as specified by the WiFi Alliance.
13. 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.

FIGURE 139 Walled Garden settings



14. In the **Policy** tab, configure **Restricted Subnet** settings by defining L3/4 IP address access control rules (ACLs) for the hotspot service to allow or deny wireless devices to access services or resources based on source/destination IP address, application, protocol or port number.

FIGURE 140 Configure hotspot access control policies



15. Click **OK** to save the hotspot service.
16. 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 189.

NOTE
If ZoneDirector is located behind a NAT device and signed certificates are used with hotspot portal authentication, a static entry must be added to the DNS server to resolve ZoneDirector's private IP address to its FQDN. Otherwise, client browsers may enter an infinite redirect loop and be unable to reach the login page. Before the signed certificate gets added the client gets redirected to the IP address of the ZD instead of the FQDN.

Assigning a WLAN to Provide Hotspot Service

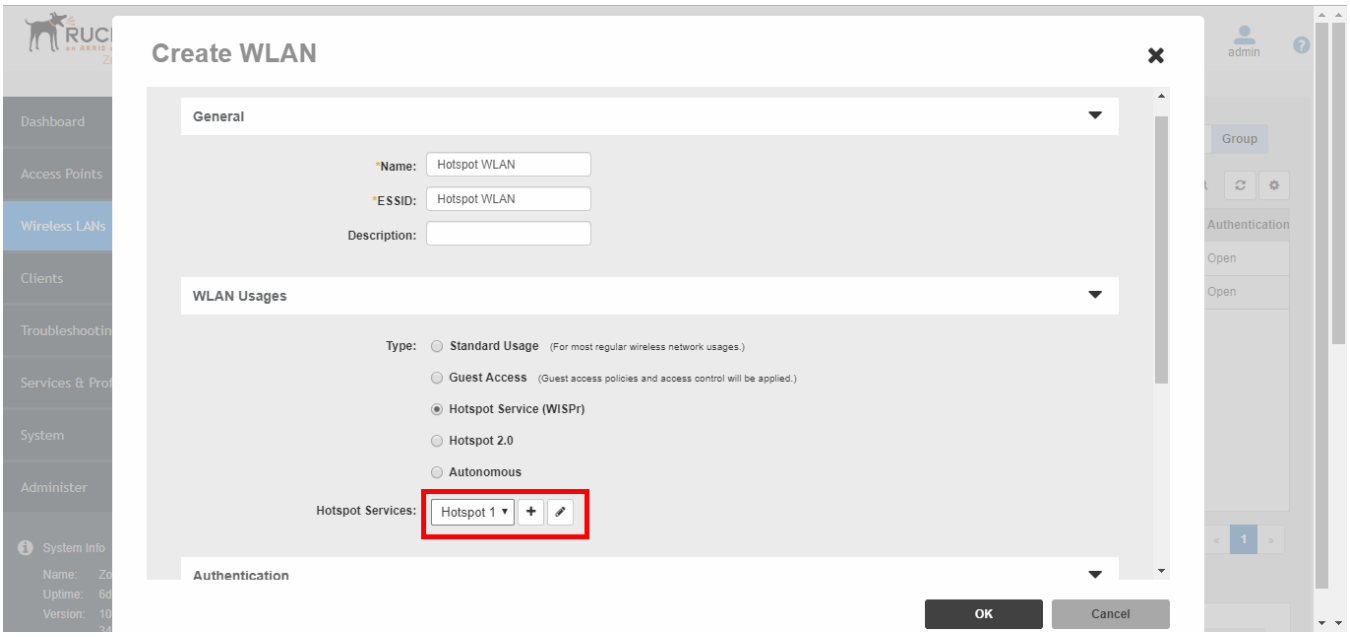
After you create a hotspot service, you need to specify the WLANs to which you want to deploy the hotspot configuration.

To configure an existing WLAN to provide hotspot service, do the following:

1. Go to **Wireless LANs**
2. In the WLANs section, look for the WLAN that you want to assign as a hotspot WLAN, and then click the Edit link that is on the same row. The Editing (WLAN name) form appears
3. In **Type**, click **Hotspot Service (WISPr)**
4. In **Hotspot Services**, select the name of the hotspot service that you created previously.

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

FIGURE 141 Assigning a Hotspot service to a Hotspot WLAN



Common WISPr Attribute Abbreviations

The table below lists common WISPr attributes and their definitions. These attributes are added automatically to the redirect URL sent to the captive portal server.

See the following URL for an example:

```
http://portal.free.com/?sip=192.168.120.15&mac=74911a20
dac0&client_mac=00216a95b0de&uip=192.168.120.13&lid=101
&dn=free.com&url=&ssid=Free-WiFi&loc=London&vlan=101
```

For a more complete guide on enabling WISPr Hotspot services with ZoneDirector, refer to the Ruckus *Enabling WISPr Application Note*.

TABLE 20 Common WISPr Attributes

Abbreviation	Description
sip	The IP address of ZoneDirector.
mac	The MAC address of the Access Point (Ethernet).
lid	The Location ID of the Hotspot service.
uip	The client's real IP address. In a Layer 3 NAT environment, the client's IP address will be translated to the gateway's IP address when logging to the Hotspot service. In this case, the login request has to include the client's real IP address to be handled properly.
dn	The domain name of the ZoneDirector. The domain name is obtained from the SSL certificate when importing a certificate to ZoneDirector.
uid	The user's login ID (passed in the UAM login form's user name parameter).
client_mac	The client's MAC address.
SSID	The SSID to which the client is associated.

TABLE 20 Common WISPr Attributes (continued)

Abbreviation	Description
Loc	The location name defined in the AP settings.
vlan	The client's VLAN ID.
reason	The reason for redirection; can be empty for first redirect, failed for auth failure, or logout when client logs off.

NOTE
For more information on Captive Portal redirection for Hotspot, Web Auth and Guest Access WLANs, see Captive Portal Redirect on Initial Browser HTTPS Request on page 123.

Creating a Hotspot 2.0 Service

"Hotspot 2.0" is a newer Wi-Fi Alliance specification that allows for automated roaming between service provider access points when both the client and access gateway support the newer protocol.

Hotspot 2.0 (also known as "Passpoint", the trademark name of the Wi-Fi Alliance certification) aims to improve the experience of mobile users when selecting and joining a Wi-Fi hotspot by providing information to the station prior to association. This information can then be used by the client to automatically select an appropriate network based on the services provided and the conditions under which the user can access them. In this way, rather than being presented with a list of largely meaningless SSIDs to choose from, the Hotspot 2.0 client can automatically select and authenticate to an SSID based on the client's configuration and services offered, or allow the user to manually select an SSID for which the user has login credentials.

ZoneDirector's Hotspot 2.0 implementation complies with the IEEE 802.11u standard and the Wi-Fi Alliance Hotspot 2.0 Technical Specification.

Enabling Hotspot 2.0 service on ZoneDirector requires the following steps:

1. Create a Service Provider Profile on page 191
2. Create an Operator Profile on page 192
3. Create a Hotspot 2.0 WLAN on page 193

Create a Service Provider Profile

To create a Service Provider Profile:

1. Go to **Services & Profiles** > **Hotspot 2.0 Services**
2. Click **Create New** under **Service Provider Profiles**. Alternatively, you can create a Hotspot 2.0 Service Provider Profile from the WLAN creation page while creating a new WLAN or modifying an existing WLAN (**Wireless LANs** > **Edit** > **Type** > **Hotspot 2.0** > **Hotspot 2.0 Operator** > **Create New** > **Service Provider Profiles** > **Create New**.)

3. Configure the settings in to create a **Service Provider** profile. See the Hotspot 2.0 Service Provider profile configuration table below.

Option	Description
Name	Enter a name for this Service Provider profile.
Description	(Optional) Enter a description.
NAI Realm List	List of network access identifier (NAI) realms corresponding to SSPs or other entities whose networks or services are accessible via this AP. Up to five NAI realm entries can be created. Each NAI realm entry can contain up to four EAP methods. Each EAP method can contain up to four authentication types.
Domain Name List	List of domain names of the entity operating the access network. Up to five entries can be created.
Roaming Consortium List	List of Organization Identifiers included in the Roaming Consortium list, as defined in IEEE802.11u, dot11RoamingConsortiumTable. Up to two Roaming Consortium entries can be created.
3GPP Cellular Network Information	Contains cellular information such as network advertisement information to assist a 3GPP station in selecting an AP for 3GPP network access, as defined in Annex A of 3GPP TS 24.234 v8.1.0. Up to eight entries can be created.

4. Click **OK** to save your changes.
5. Continue to Create an Operator Profile on page 192.

Create an Operator Profile

To create an Operator Profile:

1. Go to **Services & Profiles** > **Hotspot 2.0 Services**.
2. Click **Create New** under. Alternatively, you can create a Hotspot 2.0 Operator Profile from the WLAN creation page while creating a new WLAN or modifying an existing WLAN (*Wireless LANs > Edit > Type > Hotspot 2.0 > Hotspot 2.0 Operator > Create New*.)

3. Configure the settings in Table **Hotspot 2.0 Operator profile configuration options** to create a Hotspot 2.0 Operator profile.

Option	Description
Name	Enter a name for this Operator profile. This name identifies the service operator when assigning an HS2.0 service to a HS2.0 WLAN.
Description	(Optional) Enter a description for the service.
Venue Information	Select venue group and venue type as defined in IEEE802.11u, Table 7.25m/n.
ASRA Option	Additional steps required for access. Select to indicate that the network requires a further step for access.
Internet Option	Specify if this HS2.0 network provides connectivity to the Internet.
Access Network Type	Access network type (private, free public, chargeable public, etc.), as defined in IEEE802.11u, Table 7-43b.
IP Address Type	Select IP address type availability information, as defined in IEEE802.11u, 7.3.4.8.
Operator Friendly Name	Network operator names in multiple languages.
Service Provider Profiles	Information for each service provider, including NAI realm, domain name, roaming consortium, 3GPP cellular network info. (A Service Provider profile must first be created before it appears here.) Up to six Service Provider Profiles can be indicated for each Operator Profile.
HESSID	Homogenous extended service set identifier. The HESSID is a 6-octet MAC address that identifies the homogeneous ESS. The HESSID value must be identical to one of the BSSIDs in the homogeneous ESS.
WAN Metrics	Provides information about the WAN link connecting an IEEE 802.11 access network and the Internet; includes link status and backhaul uplink/downlink speed estimates.
Connection Capability	Provides information on the connection status within the hotspot of the most commonly used communications protocols and ports. 11 static rules are available, as defined in WFA Hotspot 2.0 Technical Specification, section 4.5.
Additional Connection Capability	Allows addition of custom connection capability rules. Up to 21 custom rules can be created.

4. Click **OK** to save this Operator Profile.
5. Continue to Create a Hotspot 2.0 WLAN on page 193.

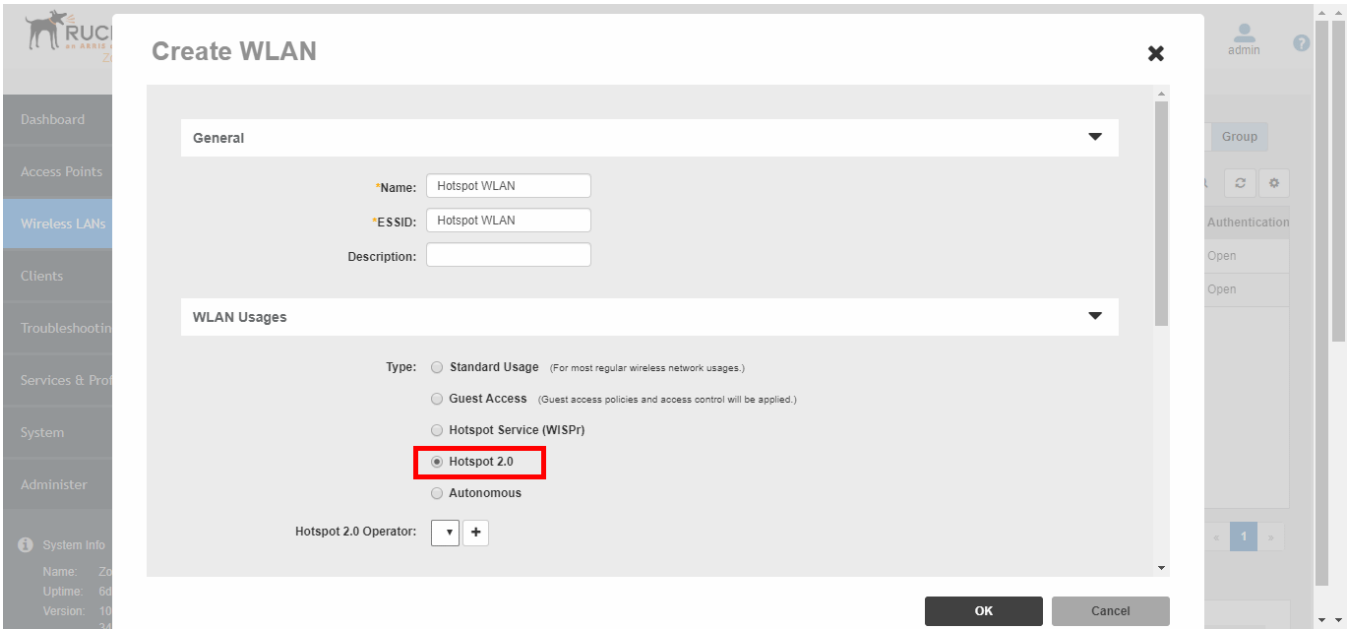
Create a Hotspot 2.0 WLAN

After you create a HS2.0 service, you need to specify the WLANs to which you want to deploy the hotspot configuration. To configure an existing WLAN to provide hotspot service, do the following:

1. Go to **Wireless LANs**.

2. In the **WLANs** section, look for the WLAN that you want to assign as a HS2.0 WLAN, and then click the **Edit** link that is on the same row. The **Editing (WLAN name)** form appears.
3. In **Type**, click **Hotspot 2.0**. 802.1X EAP is the only authentication method and WPA2/WPA3/AES are the only encryption methods available when you select Hotspot 2.0 WLAN type.
4. In **Hotspot 2.0 Operator**, select the name of the Operator profile that you created previously, or click **Create New** to create a new HS2.0 Operator profile.
5. In **Authentication Server**, select the RADIUS server used to authenticate users.
6. Optionally, enable **Proxy ARP** for this Hotspot 2.0 WLAN (see Advanced WLAN Options on page 72 under Creating a WLAN.)
   - If Proxy ARP is enabled, you also have the option to disable downstream group-addressed frame forwarding by selecting the DGAF option. This option prevents stations from forwarding group-addressed (multicast/broadcast) frames and converts group-addressed DHCP and ICMPv6 router advertisement packets from layer 2 multicast to unicast.
7. Click **OK** to save your changes.

FIGURE 142 Creating a Hotspot 2.0 WLAN



Customizing the Captive Portal

You can customize the guest user login page to display your own corporate logo, customize the landing page colors, and include any other login messages such as a custom "Welcome" message visitors connecting to your guest WLAN.

If you want to include a logo, you will need to prepare a web-ready graphic file, in one of three acceptable formats: .JPG, .GIF or .PNG. The recommended image size is 415 x 100 pixels, and the maximum file size is 200KB.

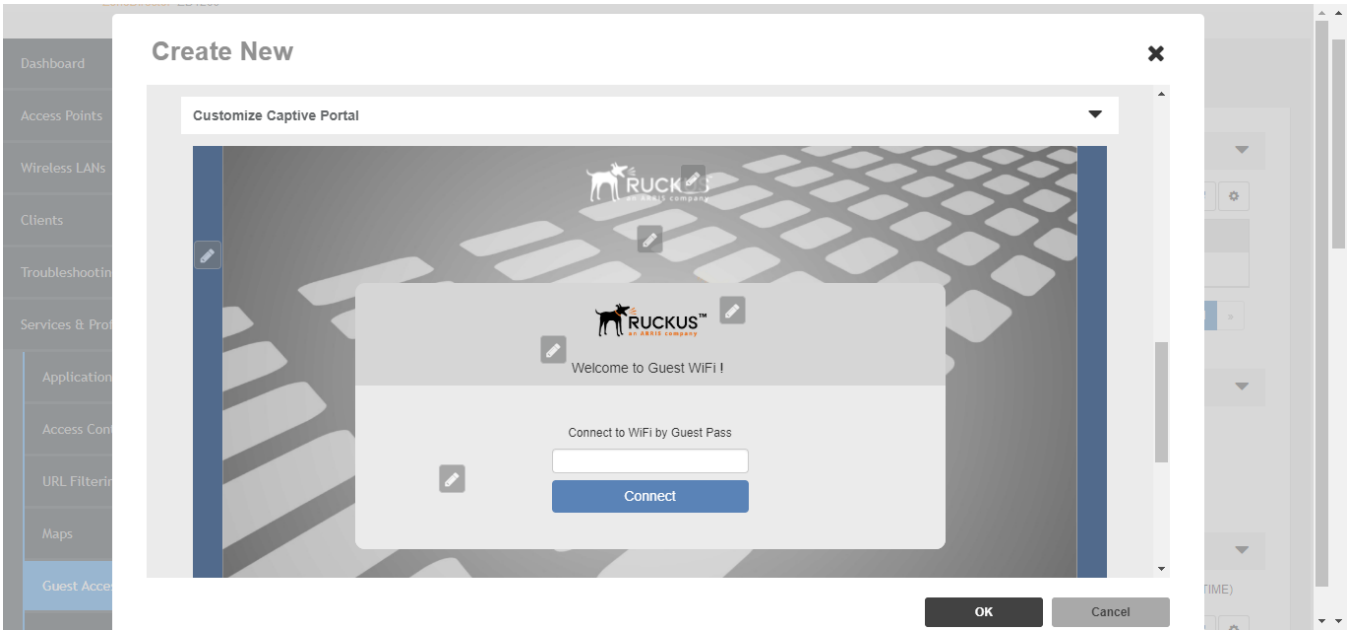
To customize the guest login page:

1. Go to **Services & Profiles > Guest Access > Guest Access Service** and click **Create** to create a new guest access profile or **Edit** to edit an existing one.

   NOTE
   Alternatively, create or modify a guest access service from the WLAN configuration page.

2. In the *Customize Captive Portal* section, configure any of the following:
   - Edit the background color, welcome message and image opacity.
   - Remove or replace the background image, banner and logo. Import an image file to replace the Ruckus logos and default background image. See Replacing the Captive Portal Logo on page 195.
3. Click **Preview** to view your changes and click **OK** to save.

FIGURE 143 Customizing the captive portal



Replacing the Captive Portal Logo

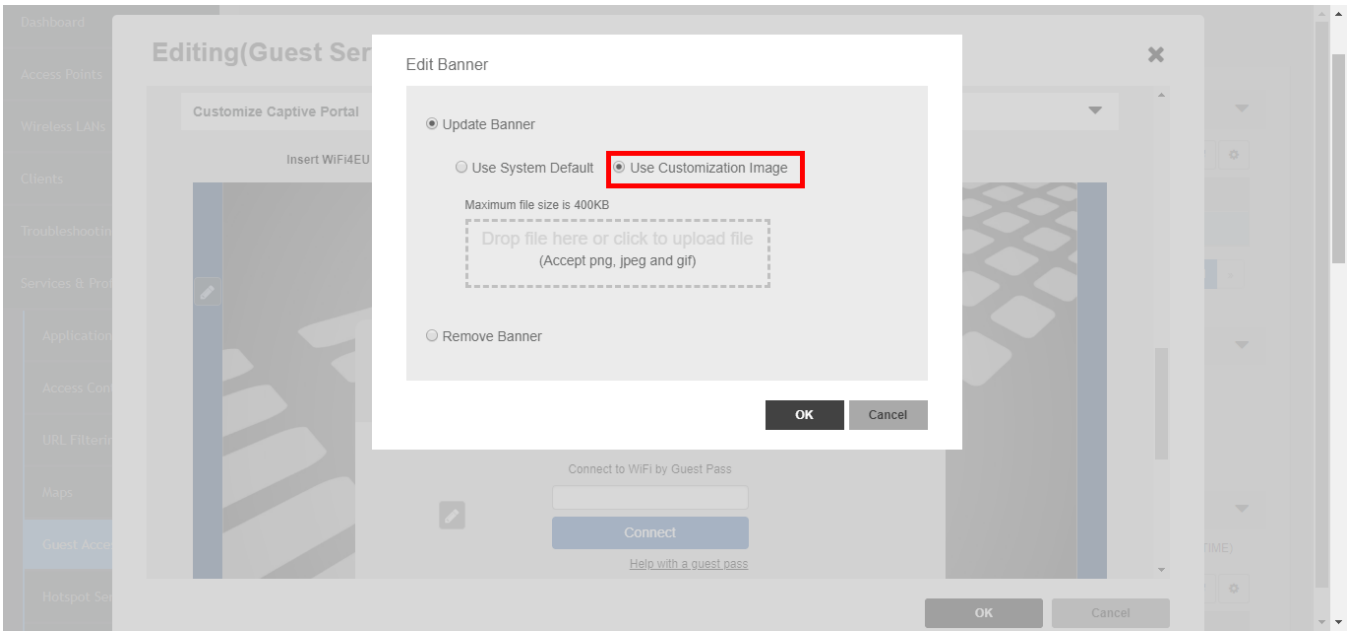
The logo that is displayed when a guest user connects to a WLAN with captive portal enabled can be changed from the default Ruckus logo to another logo by uploading an image file to ZoneDirector to replace the default logo.

To replace the default web portal logo with a custom logo:

1. Go to **Services & Profiles > Guest Access > Guest Access Service > Create/Edit**.
2. Scroll down to *Customize Captive Portal*.
3. Click **Edit Banner** or **Edit Logo** to replace the Ruckus logo. Click **Edit Background Image** to replace the background image.
4. Select **Use Customization Image**.

5. Drag a file (max 400kb, JPG, PNG, GIF) into the drop box and click **OK**.

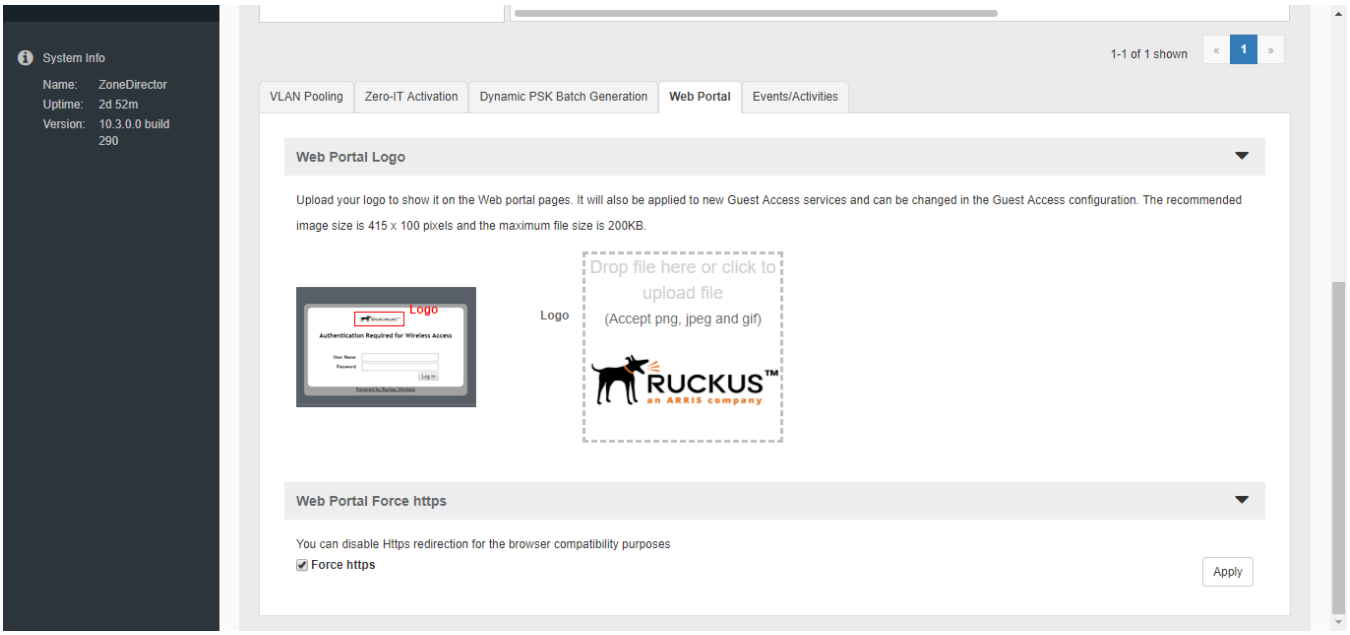
FIGURE 144 Use custom image to replace Ruckus logo in captive portal login page



6. Alternatively, go to **Wireless LANs**, and click the **Web Portal** tab.
7. Drop your image file into the **Logo** field provided.
   The recommended image size is 415 x 100 pixels and the maximum file size is 200KB.
8. Click **Preview** to preview the custom login page.

9. Click **Apply** to save your settings.

FIGURE 145 Customizing the Web Auth Captive Web Portal logo



Troubleshooting

- Troubleshooting Failed User Logins....199
- Performing Client Connectivity Diagnostics....200
- Fixing User Connections....201
- Measuring Wireless Network Throughput with SpeedFlex....205
- Starting a Radio Frequency Scan....211
- Generating a Debug File....212
- Viewing and Saving Current System Logs....213
- Saving Client Connection Logs....213
- Viewing Current AP Logs....214
- Packet Capture and Analysis....215
- AP Diagnostic Information....219
- Importing a Script....220
- Enabling Remote Troubleshooting....220
- Disabling SpeedFlex....220
- Restarting an Access Point....221
- Restarting ZoneDirector....221

Troubleshooting Failed User Logins

This troubleshooting topic addresses the problems that network users might have with configuring their client devices and logging into your Ruckus WLANs.

Upon the completion of the Setup Wizard, ZoneDirector automatically activates a default internal WLAN for authorized users.

A key benefit of the internal WLAN is the Zero-IT feature, which allows new users to self-activate their wireless client devices with little or no assistance from the IT department. Zero-IT client device configuration requires that the client be running a compatible operating system and using a wireless network adapter that implements WPA2 encryption.

If you and your WLAN users run into initial connection failures when using the Zero-IT configuration and login, many of the problems have two key causes:

- Your users' client devices are running another OS, such as Linux, ChromeOS, etc.
- Your users' client devices are using wireless network adapters without a WPA implementation.

The following list of options may be applicable based on your client system's qualifications:

- Option 1: If the client is running a supported operating system, check the wireless network adapter to verify the implementation of WPA.
- Option 2: Upgrade to Windows 7 or later, and if needed, acquire a wireless network adapter with WPA2 support. Once these changes are made, your users can attempt Zero-IT activation again.
- Option 3: If an older version of Windows is in use, or if another OS is being used, the user must manually enter the WPA2 passphrase in their network configuration.
- Option 4: If the client's OS cannot be upgraded and the wireless adapter is limited to WEP, you will need to do the following:
  - Create an additional WEP WLAN for non-standard client connections, then create a Role that refers to this WLAN, and assign that role to the relevant user accounts.
  - Enter the WEP key in the network configuration on the client device.

Performing Client Connectivity Diagnostics

This 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. Go to **Clients > Wireless Clients**.
2. Select the client you want to troubleshoot.

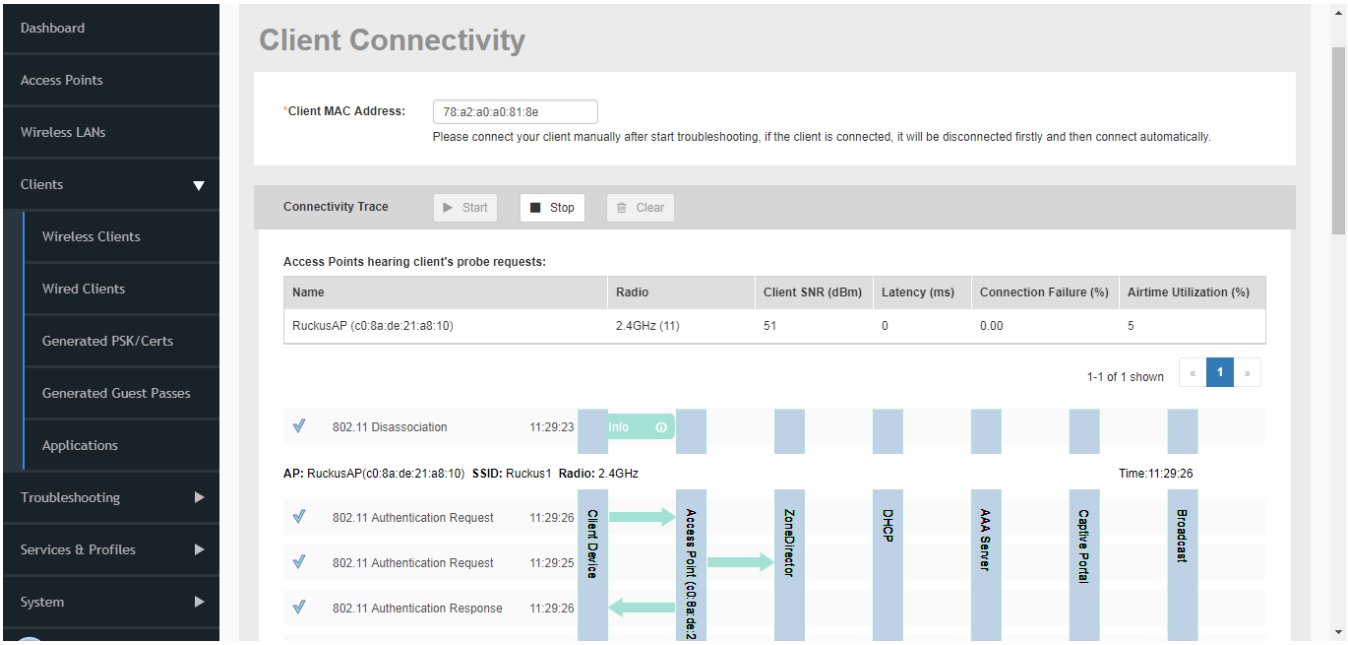
   NOTE
   Alternatively, go to **Troubleshooting > Client Connectivity**, and enter the client's MAC address to begin.

3. Select **More > Troubleshooting** from the menu.

   The *Client Connectivity* page appears.
4. Click **Start**.

   The association trace begins. The page refreshes to display detailed results.
5. Examine the results to isolate the problematic step in the process.

   FIGURE 146 Running a client connectivity trace



6. 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 ZoneDirector.

Fixing User Connections

If any of your users report problematic connections to the WLAN, the following debugging technique may prove helpful.

Basically, you will be deleting that client from the Active Clients table on the ZoneDirector, and when the client connection automatically renews itself, any previous problems will hopefully be resolved.

To disconnect an active client:

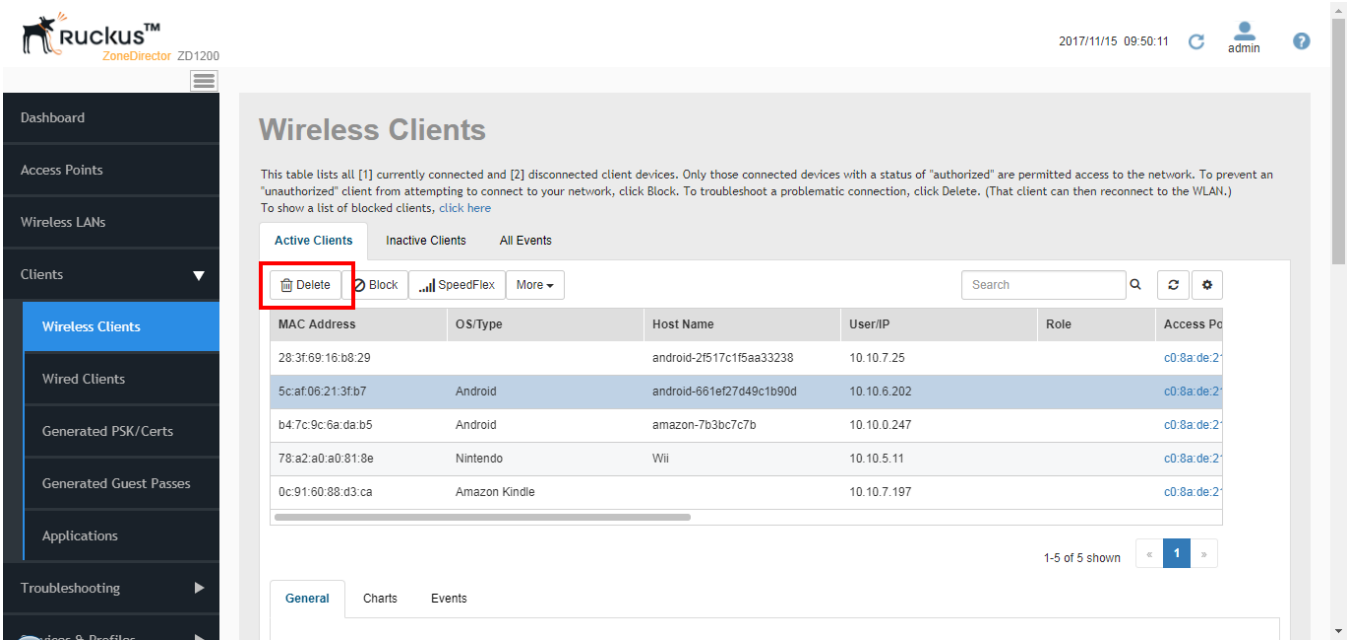
1. Go to **Clients** > **Wireless Clients**.
2. In the **Clients** table, locate the problematic client, and click the **Delete** button to disconnect the client.
3. When the confirmation message *"Are you sure you want to delete the selected entries?"* appears, click **Yes**.

   The client will be immediately disconnected from the WLAN.

   NOTE
   Be sure not to block the client. If you do accidentally block a client, go to **Services & Profiles > Access Control > Blocked Clients** to unblock.

4. From the client computer, refresh the list of wireless networks and attempt to log in again.
5. After several seconds, the **Clients** table will refresh and display the client again.

FIGURE 147 Click Delete to temporarily disconnect a wireless client



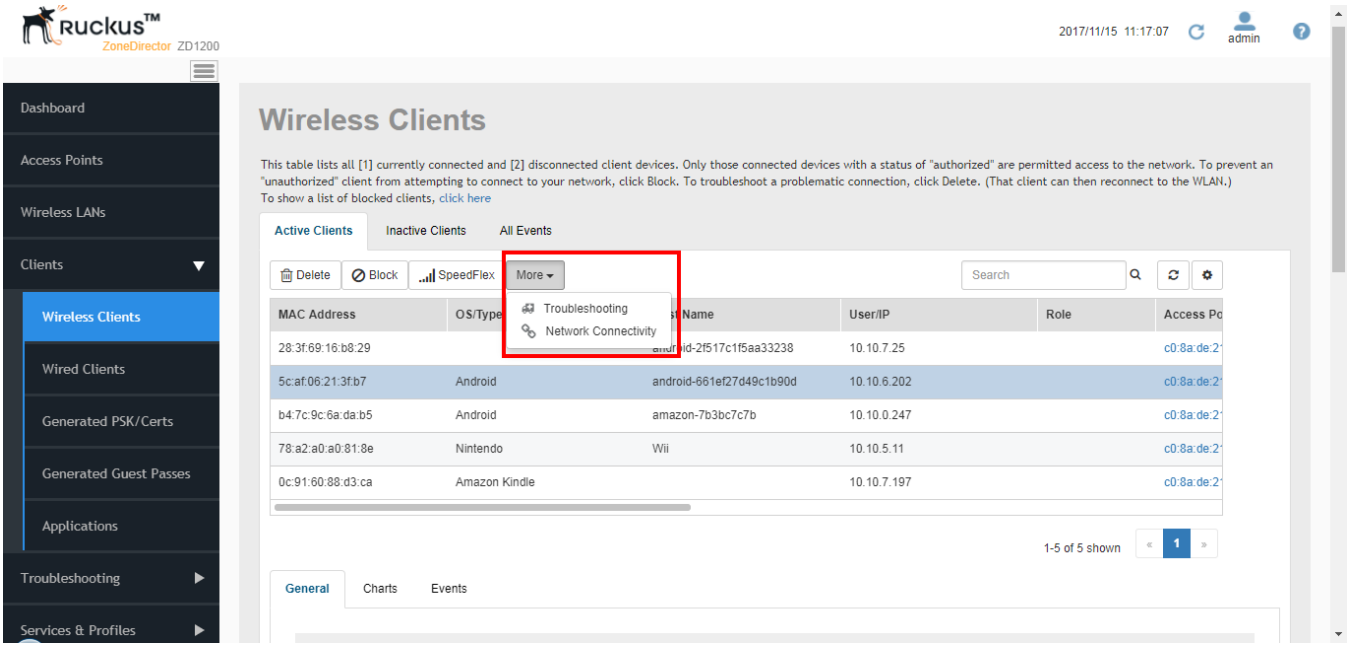
Troubleshooting Client Connections

The Wireless Clients page provides several options for troubleshooting problematic clients.

1. Go to *Clients > Wireless Clients*.
2. Select the client from the list, click the **More** drop-down menu, and then select either **Troubleshooting** or **Network Connectivity**.

3. Continue to Performing Client Connectivity Diagnostics on page 200 or Using the Ping and Traceroute Tools on page 202.

FIGURE 148 Testing and troubleshooting client connectivity

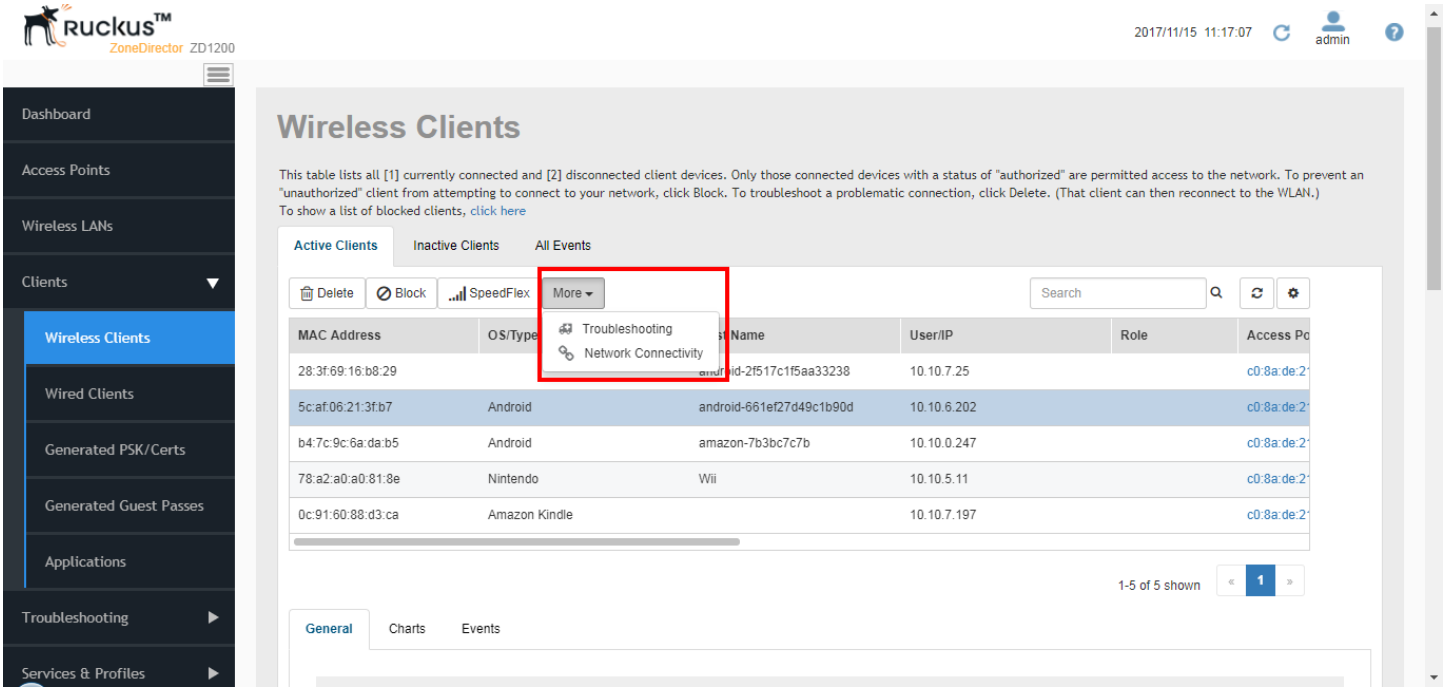


Using the Ping and Traceroute Tools

The ZoneDirector web interface provides two commonly used tools that allow you to diagnose connectivity issues while managing ZoneDirector without having to exit the UI.

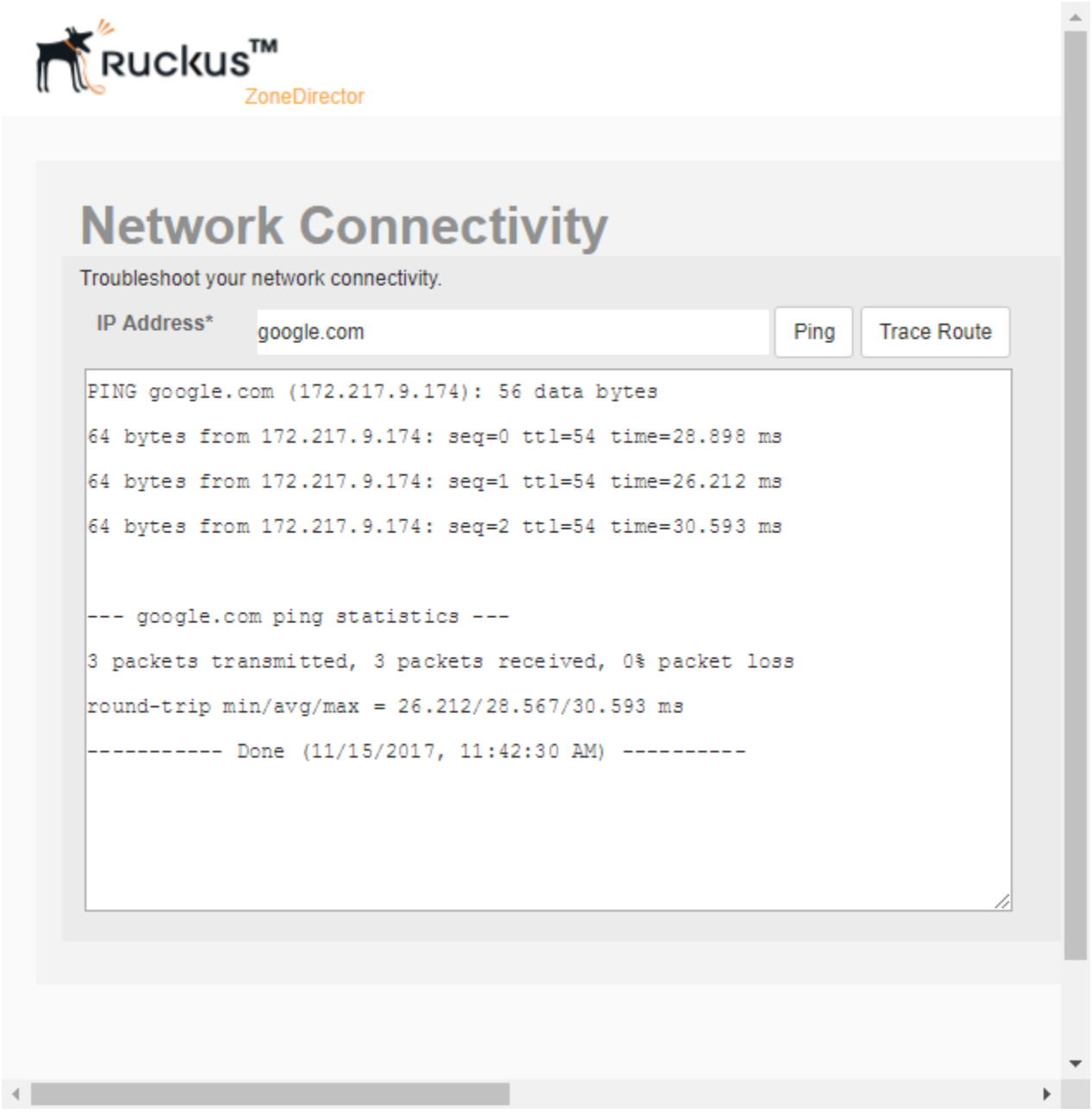
The Ping and Traceroute tools can be accessed from the *Clients > Wireless Clients > Active Clients* page. Select the client from the **Active Clients** list, click **More**, and then click **Network Connectivity** to launch the troubleshooting screen.

FIGURE 149 Launching the Ping and Traceroute tools from the Active Clients list



The *Network Connectivity* window opens. Click **Ping** to ping the IP address or **Trace Route** to diagnose the number of hops to the IP address.

FIGURE 150 Network Connectivity dialog



If WLAN Connection Problems Persist

If the previous technique fails to resolve the connection issues, you may need to guide the user through a reset of their WLAN configuration.

This requires deleting the user record, then creating a new user record, after which the user must repeat the Zero-IT activation process to reconfigure their device with the wireless connection settings.

1. Have the user log out of the WLAN.
2. Go to **Services & Profiles** > **Users**. The Internal User Database table appears, displaying a list of current user accounts.

3. Locate the problematic user account in the table, and click the check box to the left of the user's name.
4. Click **Delete**.
5. Click the **Create New** button to create a new user account for this user. Enter a user name and password, and choose a role from the drop-down menu.
6. Send a notification to the user with instructions on how to re-configure their client and log into the WLAN again.

At the end of this process, the user should be reconnected. If problems persist, they may originate in the client's operating system or in the wireless network adapter.

Measuring Wireless Network Throughput with SpeedFlex

SpeedFlex is a wireless performance tool included in ZoneDirector that you can use to measure actual real-world throughput performance between ZoneDirector and a wireless client, ZoneDirector and an AP, or a wireless client and an AP.

When performing a site survey, you can use SpeedFlex to help find the optimum location for APs on the network with respect to user locations.

NOTE
Before running SpeedFlex, verify that the *Guest Usage* and *Wireless Client Isolation* options (on the *Wireless LANs > Edit WLAN* page) are disabled. The SpeedFlex Wireless Performance tool may not function properly when either or both of these options are enabled. For example, SpeedFlex may be inaccessible to users at http://{zonedirector-ip-address}/perf or SpeedFlex may prompt you to install the SpeedFlex application on the target client, even when it is already installed.

NOTE
The following procedure describes how to run SpeedFlex from the ZoneDirector web interface to measure a wireless client's throughput. For instructions on how to run SpeedFlex from a wireless client (for users), refer to *Allowing Users to Measure Their Own Wireless Throughput*.

NOTE
SpeedFlex is unable to measure the throughput between two devices if those two devices are not on the same VLAN or the same subnet.

To measure the throughput of an AP or a client from the web interface:

1. Find out the MAC address of the AP or wireless client that you want to use for this test procedure.
2. If you are testing client throughput, verify that the wireless client is associated with the AP that you want to test.
3. Log in to the ZoneDirector web interface. You can use the wireless client that you are testing or another computer to log in to the web interface.
4. If you want to test AP throughput, click **Access Points**. If you want to test client throughput, click **Clients > Wireless Clients**.
5. In the list of APs or clients, look for the MAC address of the AP or wireless client that you want to test, and then click **More > SpeedFlex**. The **SpeedFlex Wireless Performance Test** interface loads, showing a speedometer and the IP address of the AP or client that you want to test.

   NOTE
   If ZoneDirector is unable to determine the IP address of the wireless client that you want to test (for example, if the wireless client is using a static IP address), the SpeedFlex link for that client does not appear on the Clients page.

6. Choose **UDP** or **TCP** from the **Protocol** drop-down list. Only one type of traffic can be tested at a time.
7. If you are testing AP throughput, you have the option to test both **Downlink** and **Uplink** throughput. Both options are selected by default. If you only want to test one of them, clear the check box for the option that you do not want to test.

8. Click the **Start** button.
   - If the target client does not have SpeedFlex installed, a message appears in the ZoneDirector administrator's browser, informing you that the SpeedFlex tool has to be installed and running on the client before the wireless performance test can continue. Click the **OK** button on the message, download the appropriate SpeedFlex version (Windows, Mac or Android) from http://<ZoneDirector-IP-Address>/perf, and email it to the user, or instruct the user to go to http://<ZoneDirector-IP-Address>/perf to download and install it. (See Allowing Users to Measure Their Own Wireless Throughput on page 210.) After SpeedFlex is installed and running on the client, click **Start** again to continue with the wireless performance test.

A progress bar appears below the speedometer as SpeedFlex generates traffic to measure the downlink or uplink throughput. One throughput test typically runs for 10-30 seconds. If you are testing both Downlink and Uplink options, the two tests take about one minute to complete.

When the tests are complete, the results appear below the Start button. Downlink and uplink throughput results are displayed along with packet loss percentages.

FIGURE 151 Running SpeedFlex on a client

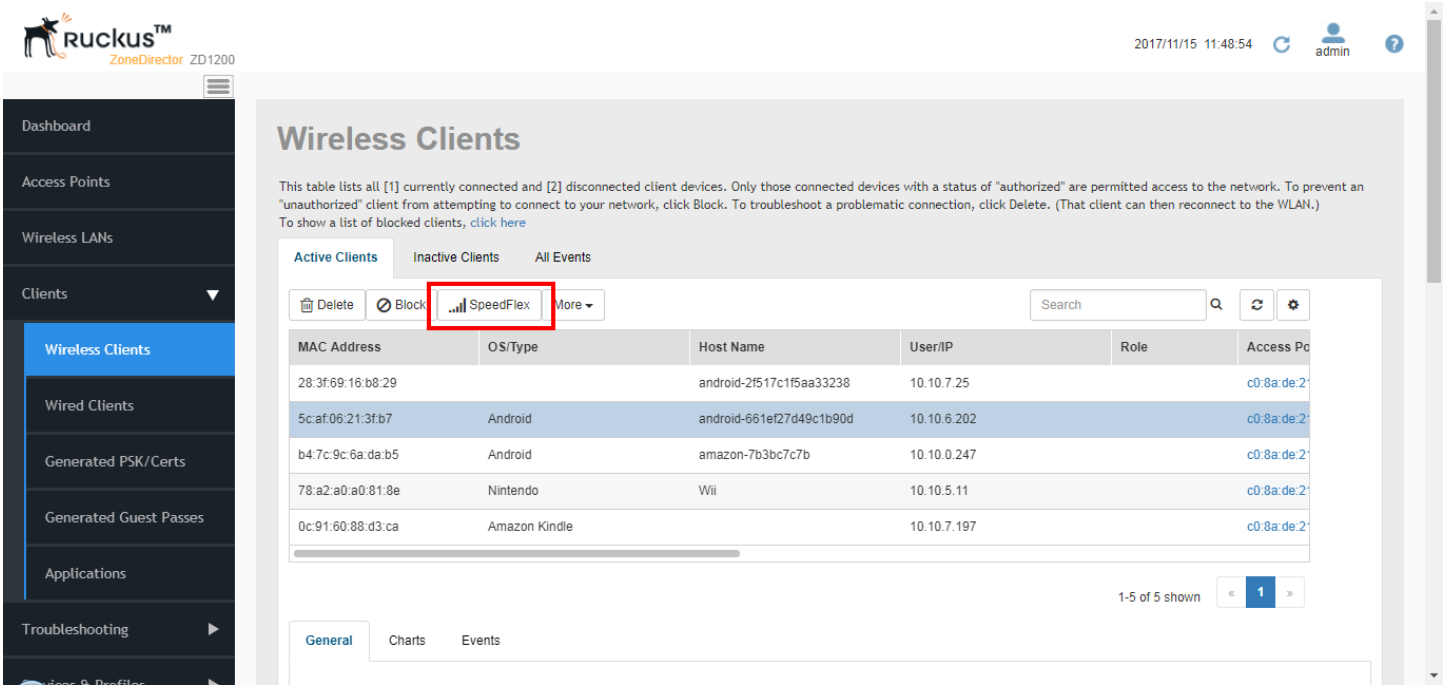


FIGURE 152 The SpeedFlex interface

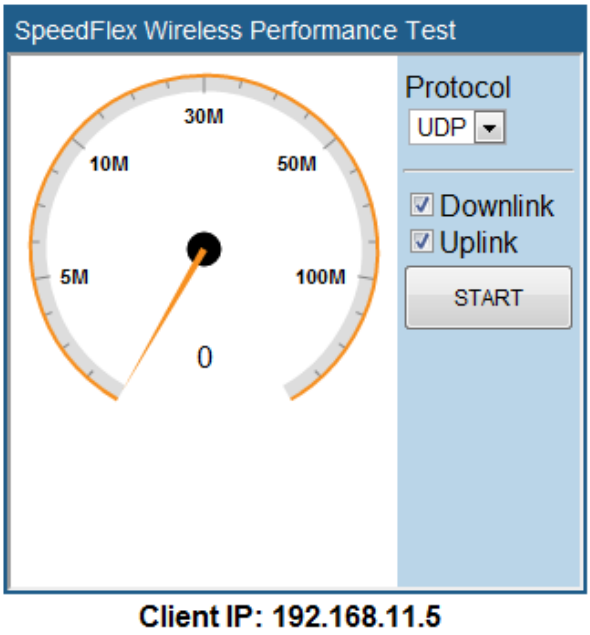


FIGURE 153 Click the download link for the target client's operating system

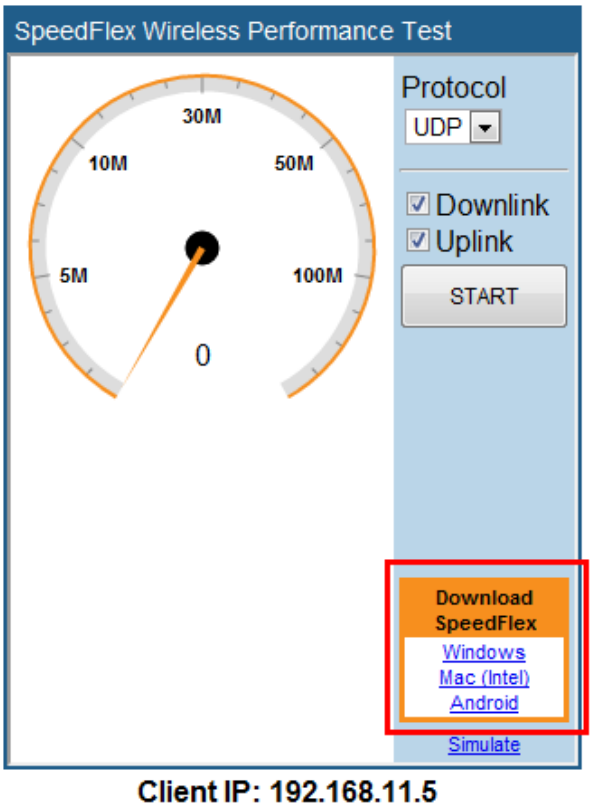


FIGURE 154 A progress bar appears as SpeedFlex measures the wireless throughput

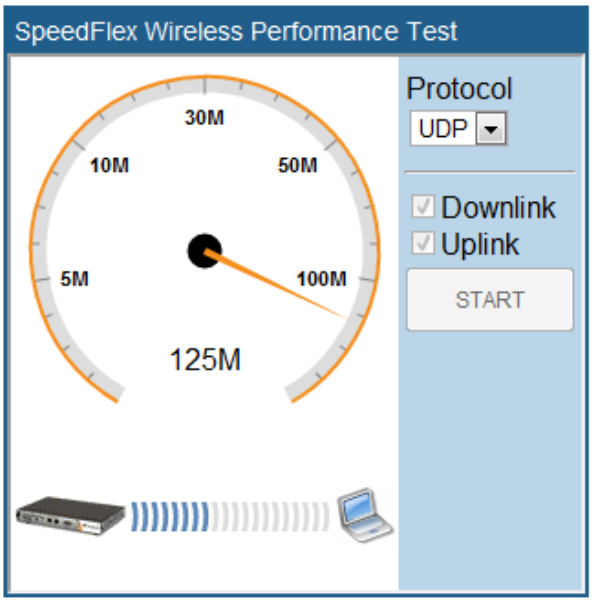
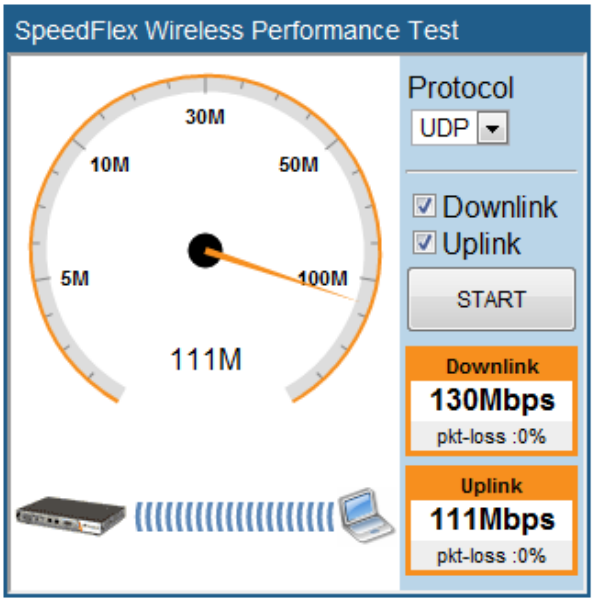


FIGURE 155 When the test is complete, the tool shows the uplink and downlink throughput and packet loss percentage



Using SpeedFlex in a Multi-Hop Smart Mesh Network

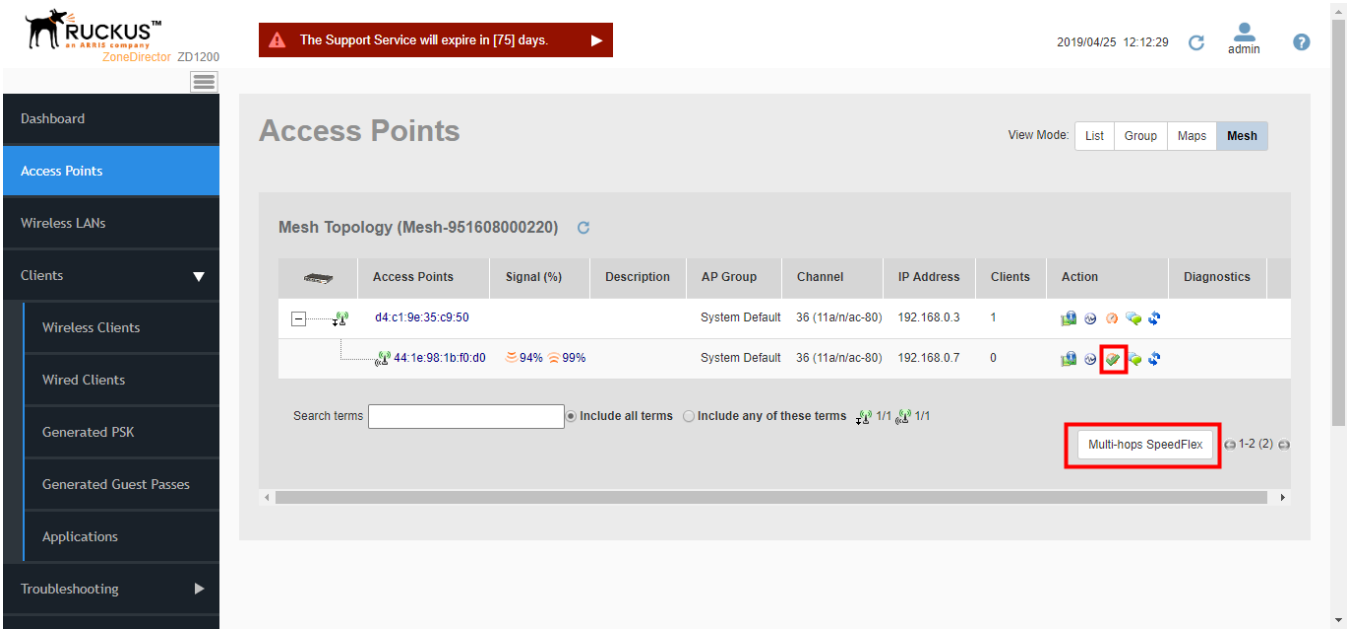
SpeedFlex can also be used to measure multi-hop throughput between APs and ZoneDirector in a mesh tree.

For example, if you have a mesh tree that is three hops deep (i.e., ZoneDirector… Root AP… Mesh AP 1… Mesh AP 2), SpeedFlex can measure the total throughput between ZoneDirector and Mesh AP 2. Running the Multi-Hop SpeedFlex tool returns throughput results for each hop as well as the aggregate throughput from ZoneDirector to the final AP in the tree.

To measure throughput across multiple hops in a Smart Mesh tree:

1. Go to **Access Points** > **View Mode > Mesh**.
2. Locate the AP whose throughput you want to measure, and click the **SpeedFlex** icon on the same row as that AP. The SpeedFlex icon changes to an icon with a green check mark, and the **Multi-Hops SpeedFlex** button appears.

   FIGURE 156 Multi-hops SpeedFlex

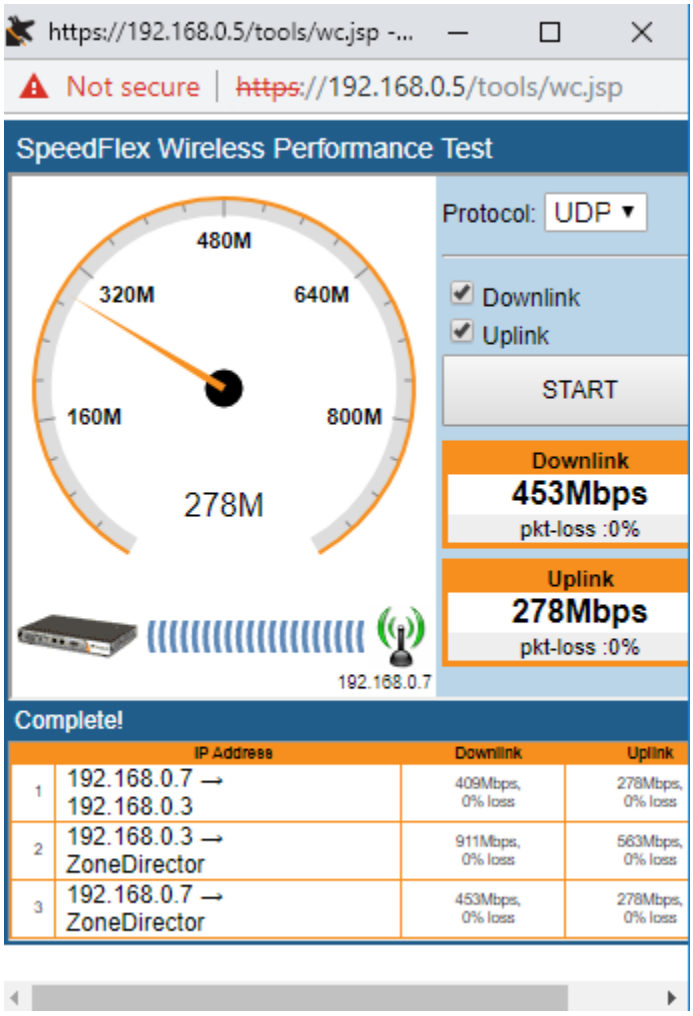


3. Click **Multi-Hops SpeedFlex**. The **SpeedFlex** utility launches in a new browser window.

4. Select **Uplink**, **Downlink** or both (default is both), and click **Start** to begin.

NOTE
Note that multi-hop SpeedFlex takes considerably longer to complete than a single hop. If you want to complete the test faster, deselect either **Uplink** or **Downlink** and test one direction at a time.

FIGURE 157 Multi-Hop SpeedFlex test results



Allowing Users to Measure Their Own Wireless Throughput

ZoneDirector provides another version of the SpeedFlex Wireless Performance Test application that does not require authentication.

This version can be accessed at: `http://{zonedirector-ip-address}/perf`. If you want wireless users to be able to measure their own wireless throughput, you can provide this link to them, along with the instructions below.

Before sending out these instructions, replace the {zonedirector-ip-address} variable with the actual ZoneDirector IP address.

The following instructions describe how you can use SpeedFlex, a wireless performance test tool from Ruckus, to measure the speed of your wireless connection to your access point.

1. Make sure that your wireless device is connected only to the wireless network. If your wireless device is also connected to the wired network, unplug the network cable.
2. Start your web browser, and then enter the following in the address or location bar: `https://{ZD-IP-Address}/perf`. The SpeedFlex Wireless Performance Tool interface loads in your browser.
3. Click the **Start** button. The following message appears:

   ```
   Your computer does not have SpeedFlex running. Click the OK button, download the SpeedFlex
   application for your operating system, and then double-click SpeedFlex.exe to start the application.
   When SpeedFlex is running on your computer, click Start again to continue with the wireless
   performance test.
   ```

4. Click **OK**. Windows, Mac (Intel), and Android download links for SpeedFlex appear on the SpeedFlex Wireless Performance Test interface.
5. Click the SpeedFlex version that is appropriate for your operating system, download the SpeedFlex file, and then save it to your computer's hard drive.
6. After downloading the SpeedFlex file, locate the file, and then double-click the file to start the application. A command prompt window appears and shows the following message: `Entering infinite loop. Enjoy the ride.` This indicates that SpeedFlex was successfully started. Keep the command prompt window open.
7. On the SpeedFlex Wireless Performance Test interface, click the **Start** button again. A progress bar appears below the speedometer as the tool generates traffic to measure the downlink throughput from the AP to the client. The test typically runs from 10 to 30 seconds.

When the test is complete, the results appear below the Start button. Information that is shown includes the downlink throughput (in Mbps) between your wireless device and the AP, as well as the packet loss percentage during the test. If the packet loss percentage is high (which indicates poor wireless connection), try moving your wireless device to another location, and then run the tool again.

Starting a Radio Frequency Scan

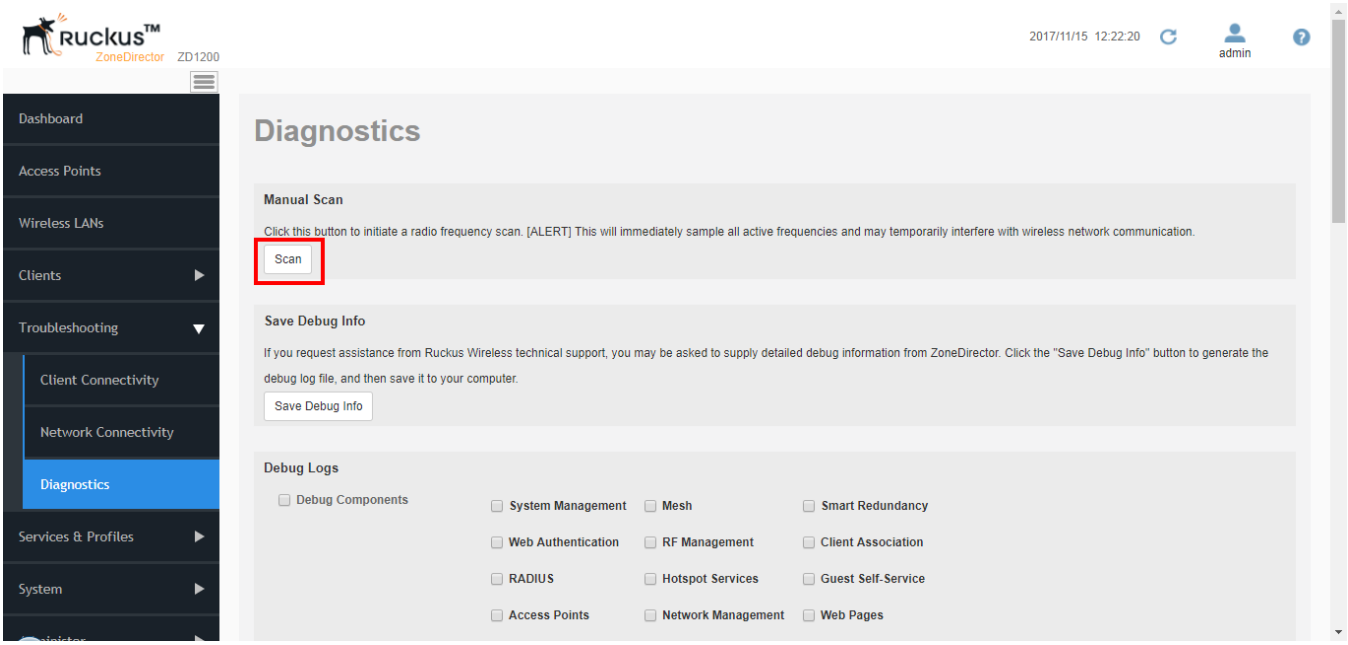
This task complements the automatic RF scanning feature that is built into the Ruckus ZoneDirector. That automatic scan assesses one radio frequency at a time, every 20 seconds (by default).

To manually start a complete radio frequency scan that assesses all possible frequencies in all devices at one time, follow these steps:

1. Go to **Troubleshooting** > **Diagnostics**.
2. When the **Diagnostics** page appears, look for the Manual Scan options, and then click **Scan**. This operation will interrupt active network connections for all current users.

3. Go to **Access Points > Events / Activities** to view updated rogue AP detection.

FIGURE 158 The Diagnostics page



Generating a Debug File

Do not start this procedure unless asked to do so by technical support staff.

If requested to generate and save a debug file, follow these steps:

1. Go to **Troubleshooting** > **Diagnostics**
2. Select the items under **Debug Components** as directed by Ruckus technical support, or check the box next to **Debug Components** to select all. (If they are already selected, skip this step.)
3. If you are instructed to save only log information for a specific AP or client, you can select the check box next to Debug log per AP's or client's mac address, then enter the MAC address in the adjacent field.
4. Click **Apply** to save your settings.
5. In the **Save Debug Info** section, click **Save Debug Info**.
6. Save the file to a convenient location on your local computer.

After the file is saved, you can email it to the technical support representative.

NOTE
The debug (or diagnostics) file is encrypted and only Ruckus support representatives have the proper tools to decrypt this file.

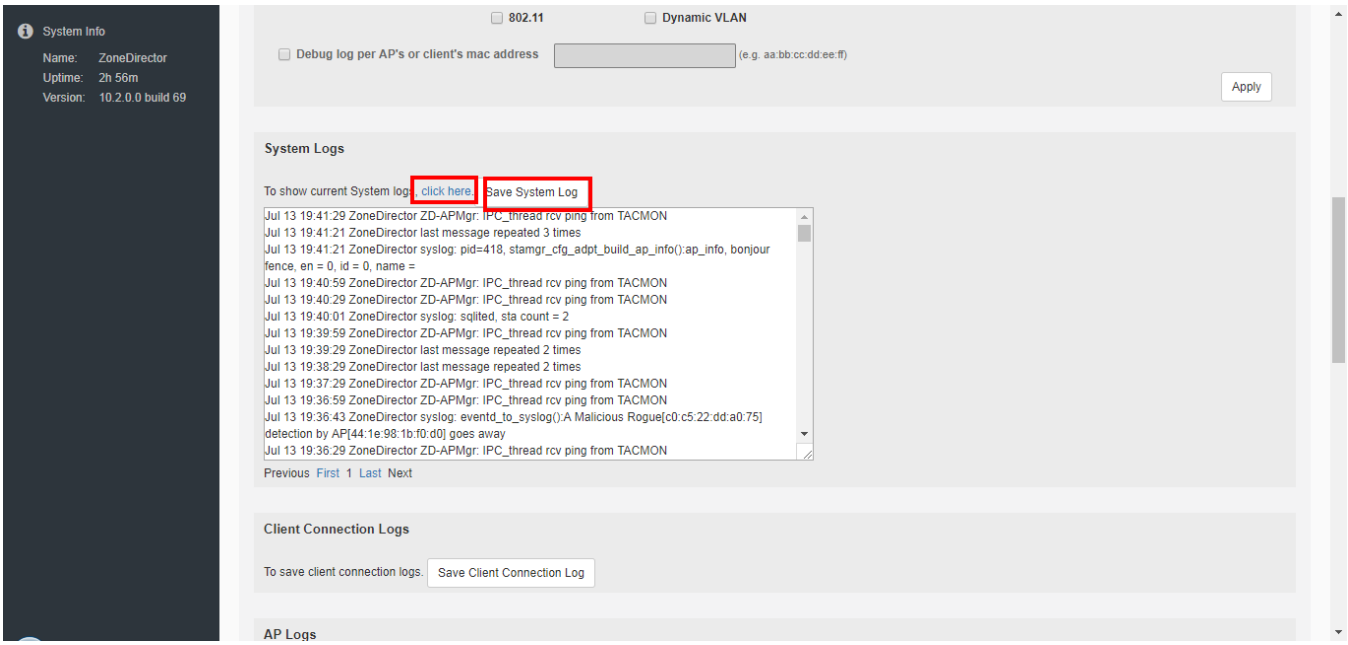
Viewing and Saving Current System Logs

You can display a list of recent ZoneDirector system activity logs from the ZoneDirector web interface and save the log file for troubleshooting analysis.

To view and save ZoneDirector system logs:

1. Go to **Troubleshooting** > **Diagnostics**, and locate the *System Logs* section.
2. Click the "**Click Here**" link next to "To show current System logs..." to view the logs on screen.
3. Click the **Save System Log** button to download and save the log as a compressed .tar file.

FIGURE 159 Viewing and saving current system logs



Saving Client Connection Logs

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

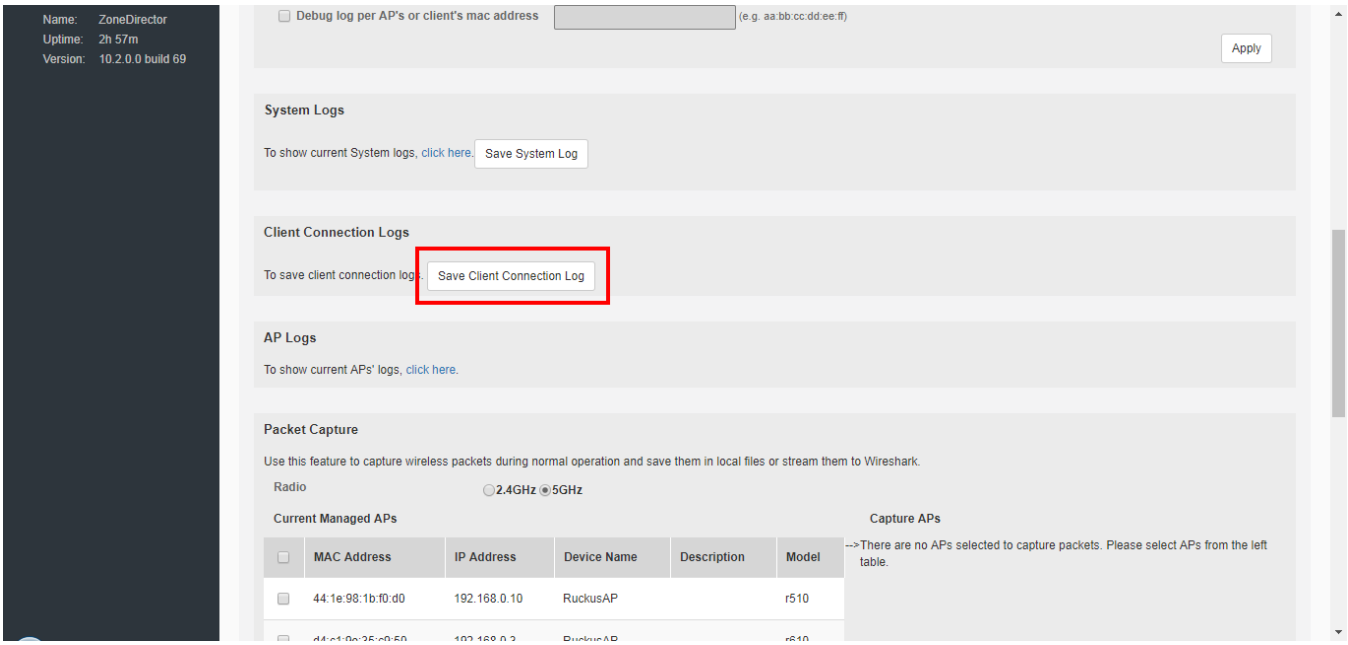
ZoneDirector provides two options for saving client connection logs - download the current log file immediately from the web interface, or set ZoneDirector to send the logs to a syslog server automatically. For information on delivering logs to syslog, see *Customizing the Current Log Settings*.

To download and save current client connection logs:

1. Go to **Troubleshooting > Diagnostics.**.
2. In the *Client Connection Logs* section, click **Save Client Connection Log**.

3. Save the file to your local computer.

FIGURE 160 Saving client connection logs to a local computer



Viewing Current AP Logs

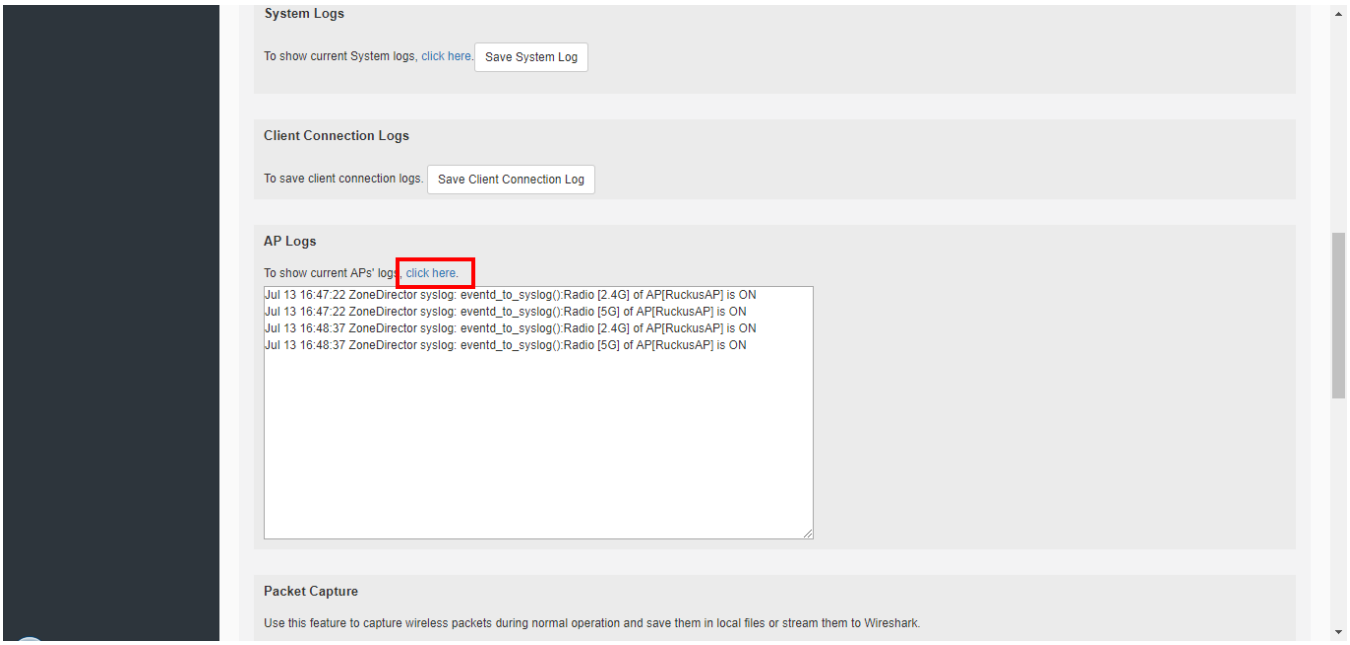
You can display a list of recent ZoneDirector AP activity logs from the ZoneDirector web interface and save the log file for troubleshooting analysis.

To view and save ZoneDirector AP logs:

1. Go to **Troubleshooting** > **Diagnostics**, 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 161 Viewing AP logs



Packet Capture and Analysis

The Packet Capture feature puts one or more APs into packet sniffer mode, allowing them to capture packets and either save them to a local file or stream them to a packet inspection program such as Wireshark for later analysis.

- Local Capture
- Streaming Mode

NOTE
Performing packet capture on the 5 GHz radio of a Mesh AP (MAP) can result in connectivity issues due to the AP's use of the 5 GHz radio for Mesh communications. Therefore, Ruckus recommends performing packet capture only on the 2.4 GHz radio of a Mesh AP. Root APs (and eMAPs) do not have this limitation and packet capture can be performed on either radio.

The local capture mode stores packet data from a single capture session in two files using a "ping-pong" method. Due to memory limitations, the capture files are cleared after they are retrieved by the Save command and before each new capture session, and they are not retained on the AP between reboots.

In streaming capture mode, packet data from the 2.4 GHz and 5 GHz radios are available simultaneously on AP interfaces wifi0 and wifi1, respectively. The streams can be accessed using Wireshark's remote interface capture option. The Windows version of Wireshark (e.g., v1.2.10) supports this option. Linux versions may not.

Both output modes support packet filtering. In local capture mode, the AP accepts a packet filter expression and applies it before storing the file. In streaming mode, Wireshark accepts a capture filter expression and sends it to a daemon running on the AP, which applies it before streaming. Both modes allow compound filter expressions conforming to the pcap-filter syntax, which is described at filter/.

Local Capture

To capture packets to a local file for external analysis:

1. Choose 2.4 GHz radio (you can only capture packets on one radio at a time).
2. Select one or more APs from the list and click **Add to Capture APs**. The APs you selected are moved from the Currently Managed APs table on the left side to the new Capture APs table on the right.
3. Select **Local Mode** to save the packet capture to a local file.
4. Click **Start** to begin capturing packets. Click **Stop** to end the capture, and click **Save** to save the packet capture to a local file.
5. Extract the pcap file(s) from the pcap.zip file and open in Wireshark or other packet analyzer.

Streaming Mode

To view streaming packets in real time using Wireshark's remote capture:

1. Choose 2.4 GHz or 5 GHz radio.
2. Select the AP you want to view and click **Add to Capture APs**.
3. Select Streaming Mode and click **Start**.
4. Launch Wireshark.
5. Go to **Capture Options**.
6. Under **Capture: Interface**, select **Remote**. A **Remote Interface** dialog appears.
7. In Host, enter the IP address of the AP you want to view. Leave the **Port** field empty **OK**.
8. The remote host interface list on the right updates. Select wifi0 from the list if you are streaming on the 2.4 GHz radio, or select wifi1 if streaming on the 5 GHz radio.

9. Click **Start**. Wireshark displays the packet stream in a new window.

FIGURE 162 Add APs from Currently Managed APs list to Capture APs list

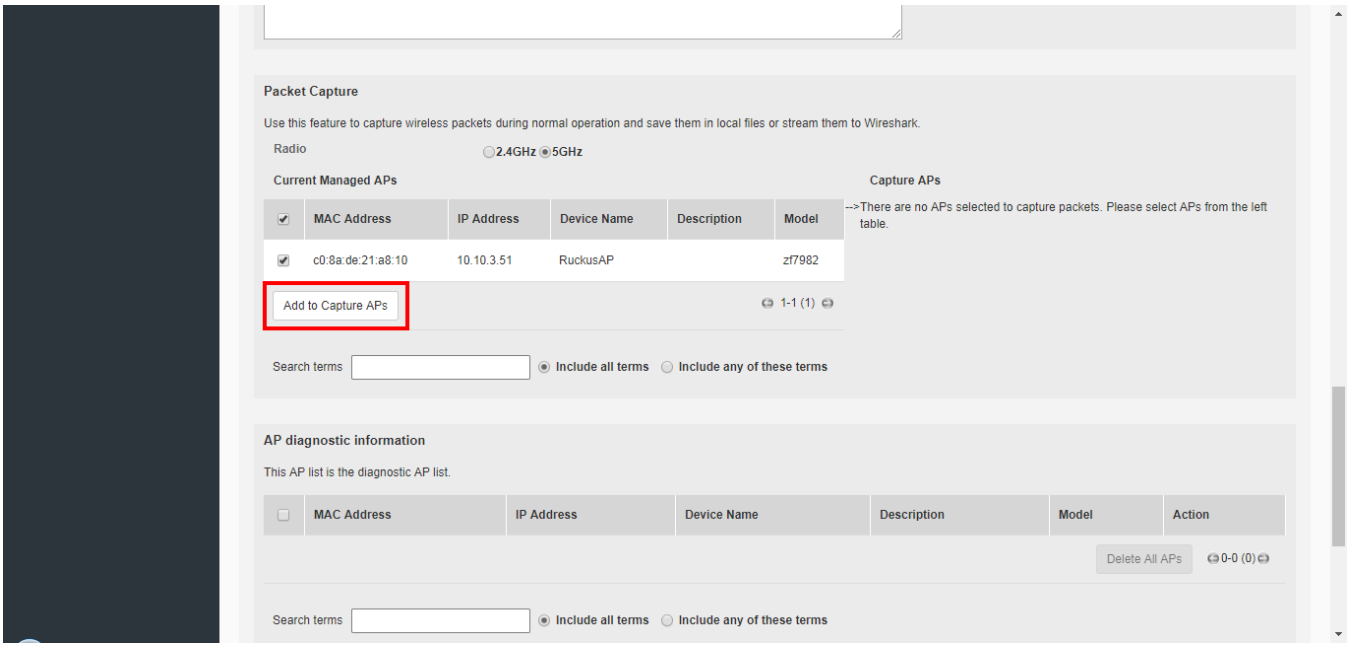
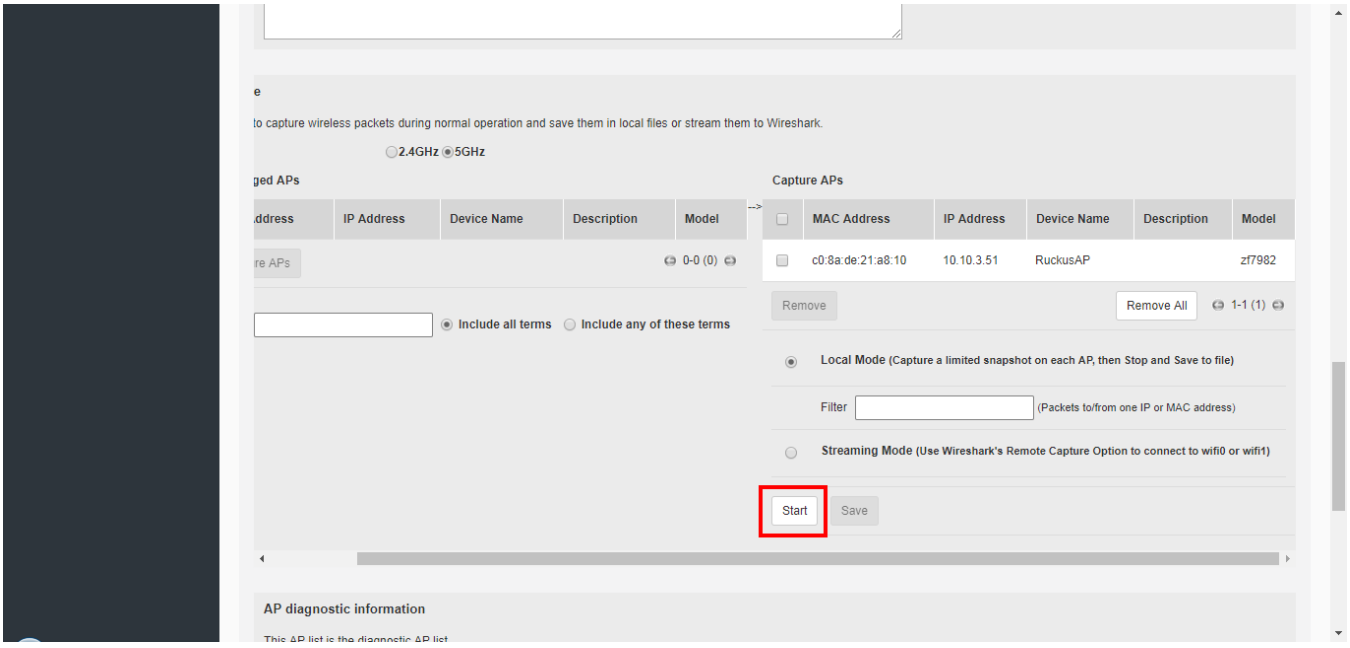


FIGURE 163 Click Start to begin packet capture; click Remove to remove APs from the list



Using Ruckus Custom Indicators

Packets captured on Ruckus APs include some information that is not available when capturing from other Wi-Fi devices. This additional information is stored in the Per-Packet Information (PPI) header that precedes the over-the-air content.

1. The PPI:802.11-Common Header antenna signal and antenna noise fields of packets transmitted by the AP contain the next-to-lowest byte and the lowest byte, respectively, of the antenna pattern used to transmit the packet. On some APs, the pattern value may contain more significant bits, which are not stored in this header. If the packet is 802.11n, it will also contain the full antenna pattern value in the header described below.
2. The PPI:802.11n-MAC+PHY Header EVM-3 field of packets transmitted by the AP contains the full antenna pattern used to transmit the packet (similar to above, except this 32-bit field can accommodate the complete value).
3. The PPI:802.11n-MAC+PHY Header MAC Flags field's upper bits convey additional TX and RX descriptor indicators described in the table below.

TABLE 21 Ruckus-defined indicators conveyed in MAC Flags

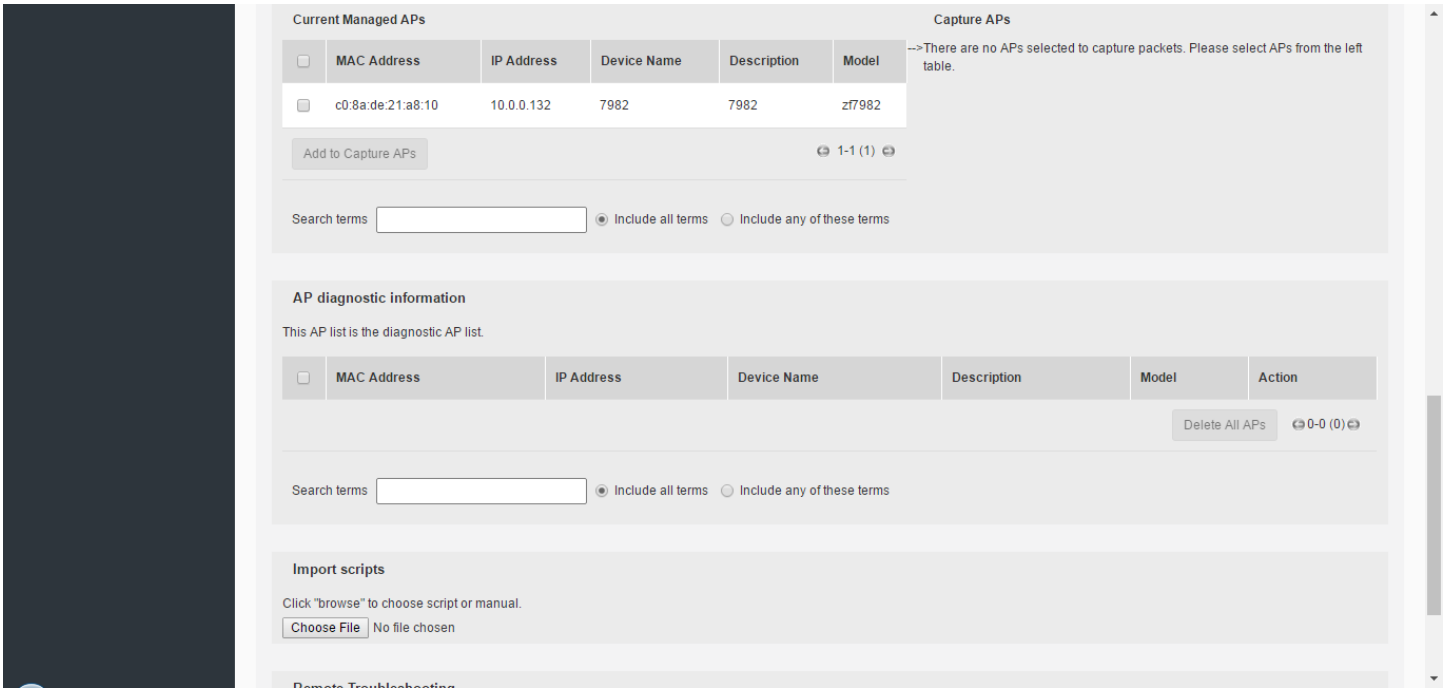
TX Indicator	Bit	RX Indicator
Sounding (0=not; 1=yes)	31	Sounding (0=not; 1=yes)
TxBF (0=not applied; 1=yes)	30	unassigned
Ness (#ext spatial streams)	28-29	Ness (#ext spatial streams)
STBC (0=not applied; 1=yes)	27	STBC (0=not applied; 1=yes)
LDPC (0=not applied; 1=yes)	26	LDPC (0=not applied; 1=yes)
LDPC indicator valid	25	LDPC indicator valid
unassigned	24	unassigned
RTS HTC TRQ	23	HW Upload Data
RTS HTC MRQ	22	HW Upload Data Valid
RTS HTC MSI	20-21	HW Upload Data Type
RTS enabled	19	unassigned
Calibrating	18	unassigned

Limitation: The AP can report RX EVM values or the RX LDPC indicator, but not both. When packet capture is invoked from the ZD UI, the software selects RX EVM values. Therefore, the RX LDPC indicator is not reported, and the LDPC indicator valid bit will be zero. The RX LDPC indicator is available when invoking packet capture from the AP command line interface.

AP Diagnostic Information

The AP Diagnostic Information feature can be used to collect AP processor core dump files from the AP via ZoneDirector. This section will be empty unless there is an AP that has experienced a core dump.

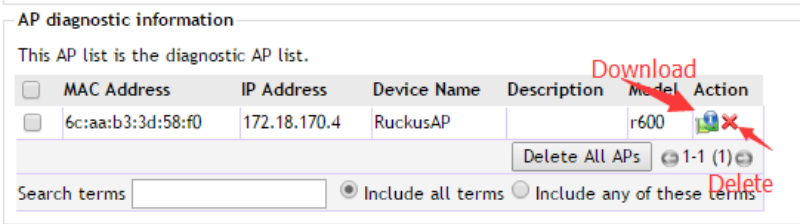
FIGURE 164 AP diagnostic information



When an AP processor core dump occurs, a log file will be created and stored on ZoneDirector, and the AP Diagnostic Information section will list the AP's MAC address, IP address, Device Name, Description and AP Model. Additionally, two buttons will appear: a **Download** and a **Delete** button.

Click the **Download** button to download the core dump log file for delivery to Ruckus Support to assist with troubleshooting, if requested to do so. Click the **Delete** button to delete this core dump log file.

FIGURE 165 AP Diagnostic Information buttons



Importing a Script

The Import Scripts feature can be used to help Ruckus Support in diagnosing customer network issues remotely by allowing the administrator to upload a Ruckus-created script to ZoneDirector themselves.

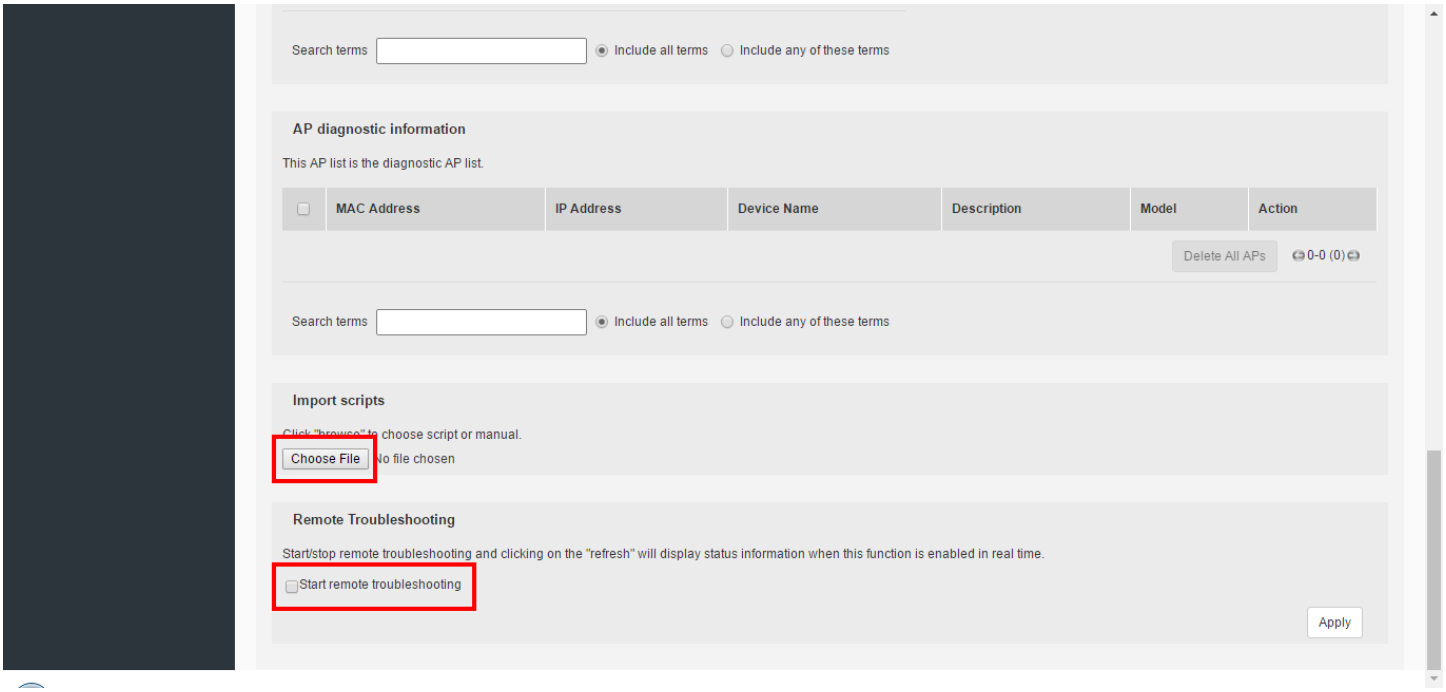
If instructed to do so by Ruckus Support, go to **Troubleshooting** > **Diagnostics** > **Import Scripts** and click **Choose File** to upload a script to ZoneDirector.

Enabling Remote Troubleshooting

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

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

FIGURE 166 The Upload Scripts and Remote Troubleshooting features are used by Ruckus Support in diagnosing customer network issues remotely



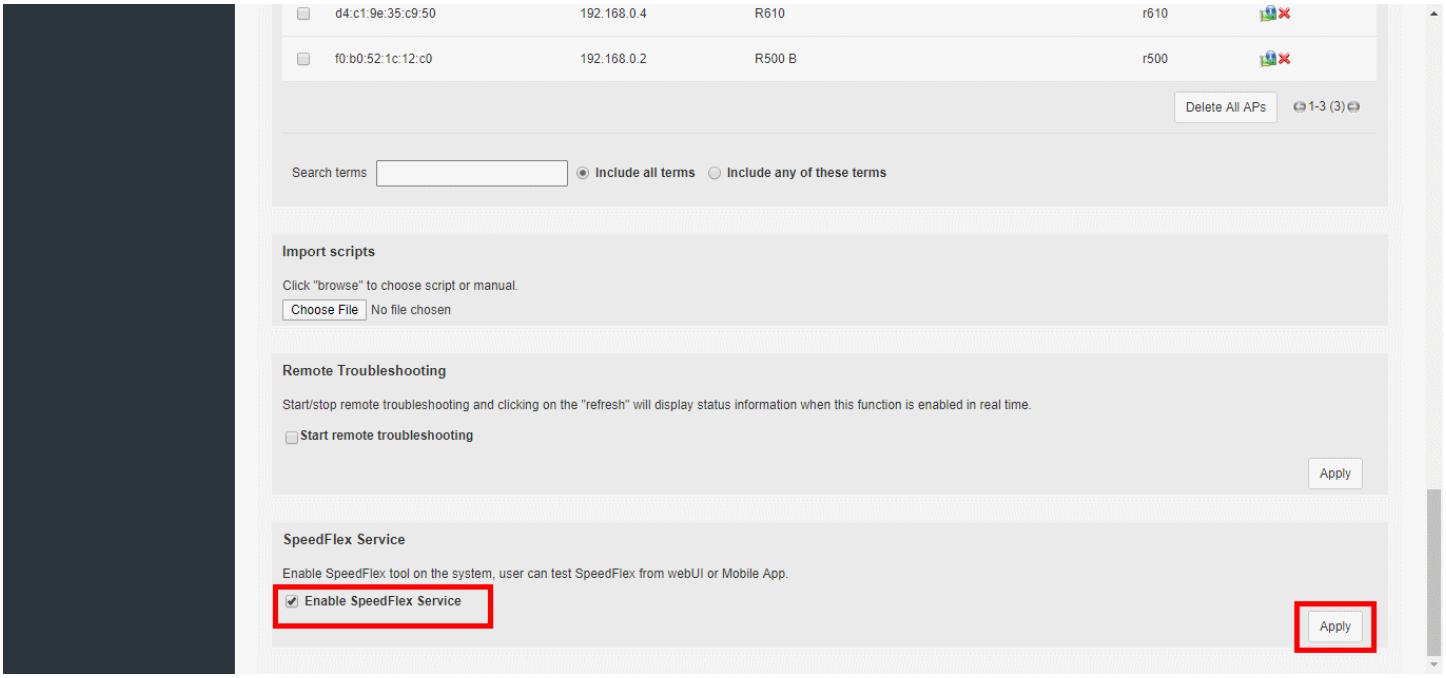
Disabling SpeedFlex

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 Measuring Wireless Network Throughput with SpeedFlex on page 205.

To disable SpeedFlex, deselect the **Enable SpeedFlex Service** option and click **Apply**.

FIGURE 167 Enable or disable SpeedFlex service



Restarting an Access Point

One helpful fix for network coverage issues is to restart individual APs. To do so, follow these steps:

1. Go to **Access Points**.
2. Locate the particular Access Point record from the AP list. The *Status* column should display “Connected.”
3. Scroll down to the *General* > *Info* section, and locate the *Action* icons. Click the **Restart** icon. The **Status** column now displays “Disconnected” along with the date and time when ZoneDirector last communicated with the AP.

After restart is complete and the Ruckus ZoneDirector detects the active AP, the status will be returned to “Connected.”

Restarting ZoneDirector

There are three "restart" options: [1] to disconnect and then reconnect the ZoneDirector from the power source, [2] to follow this procedure which simultaneously shuts down ZoneDirector and all APs, then restarts all devices, and [3] a restart of individual APs (detailed in “Restarting an Access Point”.)

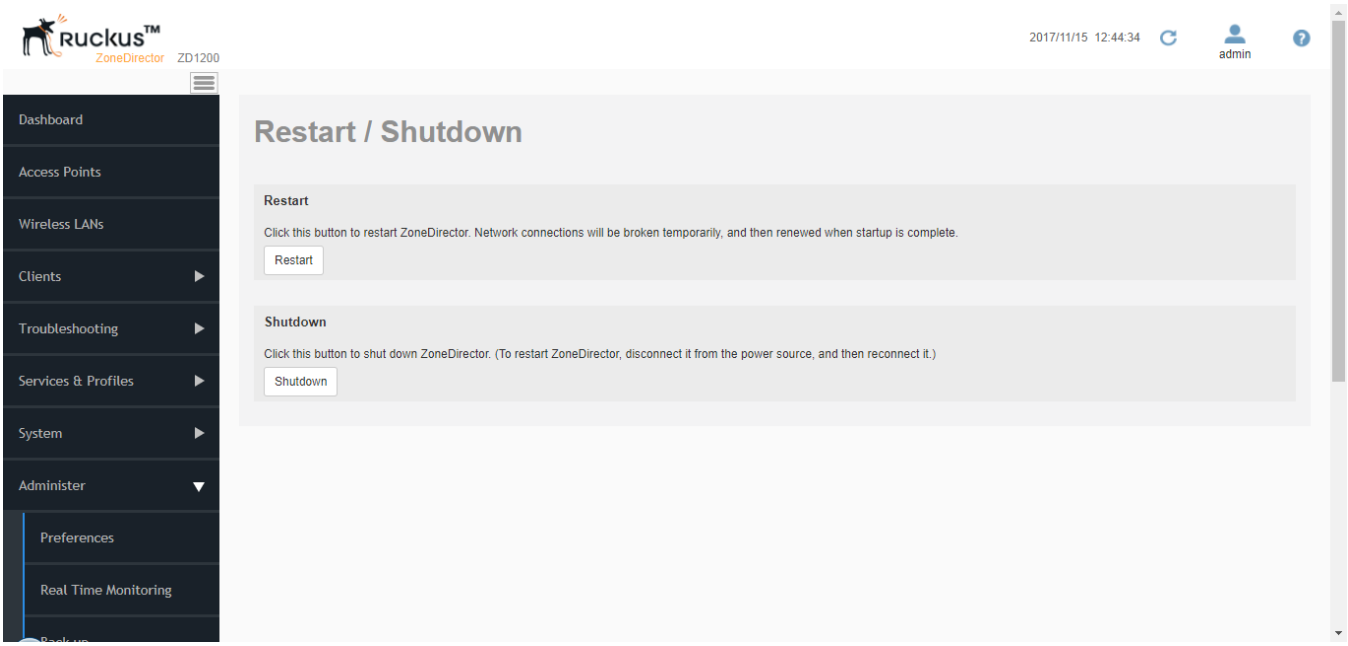
To restart ZoneDirector (and all currently active APs):

> **NOTE**
> If you have made any configuration changes, Ruckus recommends shutting down ZoneDirector to ensure that all configuration changes are saved and persist after reboot. Performing a restart may cause ZoneDirector to lose configuration changes if you forget to click **Apply** after making changes and navigate away from a configuration page, for example.

1. Go to **Administer** > **Restart**.

2. When the **Restart / Shutdown** features appear, click **Restart**. You will be automatically logged out of ZoneDirector. After a minute, when the Status LED is steadily lit, you can log back into ZoneDirector.

FIGURE 168 The Restart/Shutdown page



Configuring Services and Profiles

- Application Recognition and Control....223
- Configuring Network Access Controls....228
- URL Filtering....238
- Configuring Maps....245
- Guest Access....247
- Hotspot Services....247
- Mesh Configuration....247
- Using an External AAA Server....248
- Services....264
- Configuring Wireless Intrusion Prevention....275
- DHCP Relay....279
- Bonjour Gateway....281
- Bonjour Fencing....286
- SPoT Location Services....288

Services & Profiles settings contain a number of options for features such as application recognition, access controls, maps, guest access, hotspot service and mesh configuration.

Application Recognition and Control

ZoneDirector's Application Recognition & Control (ARC) features allow administrators to customize and enhance ZoneDirector's built-in application identification capabilities, apply filtering policies to prevent users from accessing certain applications, or limit the bandwidth consumed by certain applications.

ZoneDirector's built-in application recognition can be enhanced using either an application signature package import feature, or by using the user-defined application sections.

Application Policies include application blocking/denial, QoS traffic shaping and rate limiting. Each Application Policy can contain multiple rules, and admins can define application policies to filter or rate limit traffic by application, and then apply the policy to WLANs using the WLAN Advanced Options.

The Application Control features allow administrators to perform the following tasks:

- Configure Application Policies on page 223
- Configure IP Based User Defined Applications on page 226
- Configure Port Based User Defined Applications on page 227
- Configure Application Policies on page 223

Configure Application Policies

This option allows the administrator to create policies to deny application access, to set QoS traffic shaping priorities for certain traffic types, or to enforce rate limiting policies for applications.

Application Denial Policies

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 Denial 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 micro-site "/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.

QoS Rules

Implement application Quality of Service (QoS) rules to mark traffic with 802.1p or DSCP headers and prioritize according to the uplink and downlink priority selected. QoS rules can be created and applied to any of the system-defined applications or to user-defined applications.

Rate Limiting

Rate limiting rules can be applied to any of the system defined or user defined applications. Set the maximum uplink and downlink rates (0.25 ~ 20 Mbps) that the application can consume.

Configuring an Application Policy

Application Policies can be configured to control access to applications or to control traffic generated by applications.

To create an Application Denial Policy:

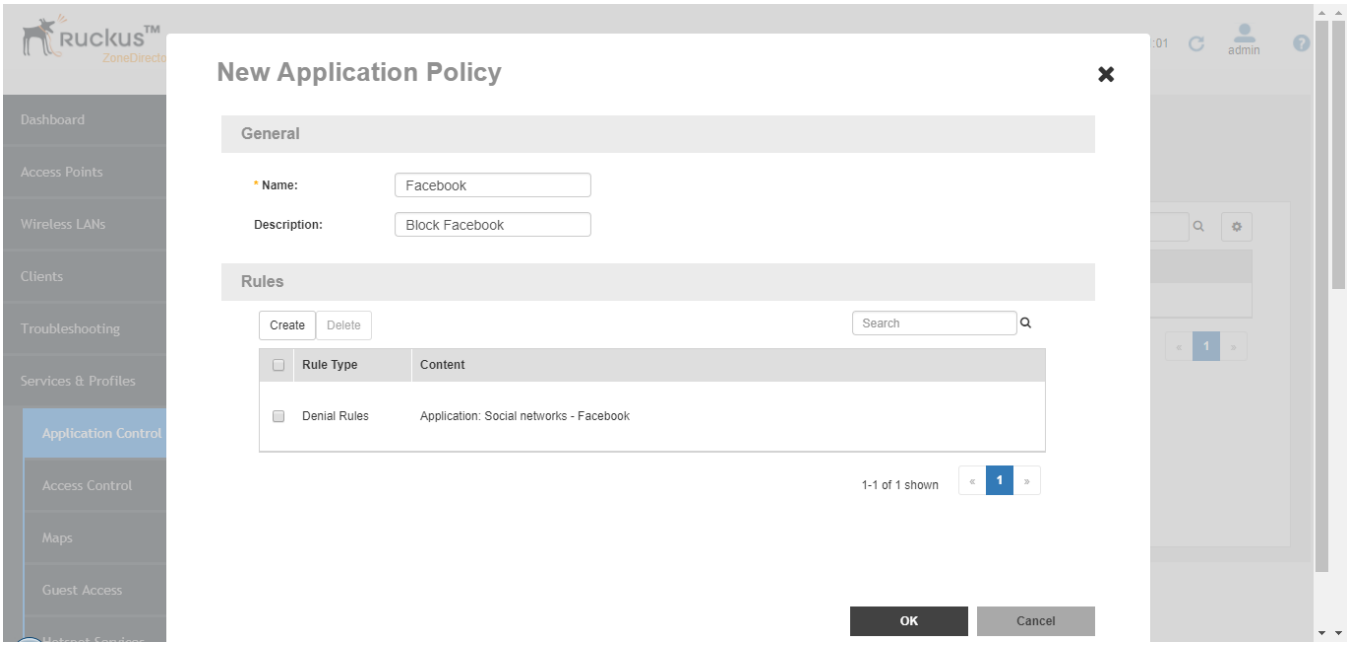
1. Go to **Services & Policies** > **Access Control**.
2. In *Application Policy*, click **Create**.

   NOTE
   Alternatively, you can create an Application Denial Policy from the WLAN creation page while creating a new WLAN or modifying an existing WLAN (**Wireless LANs** > **Edit** > **Advanced Options** > **Application Visibility** > **Enable** > **Apply Policy Group** > **Create New**.)

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 one of the following policy rule types:
   - **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 one of the following application categorization methods:
   - **System Defined**: Choose from a number of built-in categories.
   - **IP Based User Defined Application**: Choose from user-defined applications.
   - **Port Based User Defined Application**: Choose from user-defined applications.
7. In **Application**, select either one of the system-defined or user-defined applications from the list.
8. Click **OK** to save the rule, and click **OK** to save the policy.

FIGURE 169 Blocking an application by Application Type



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 that will apply to both IP protocols and may inadvertently block another application using the other protocol.

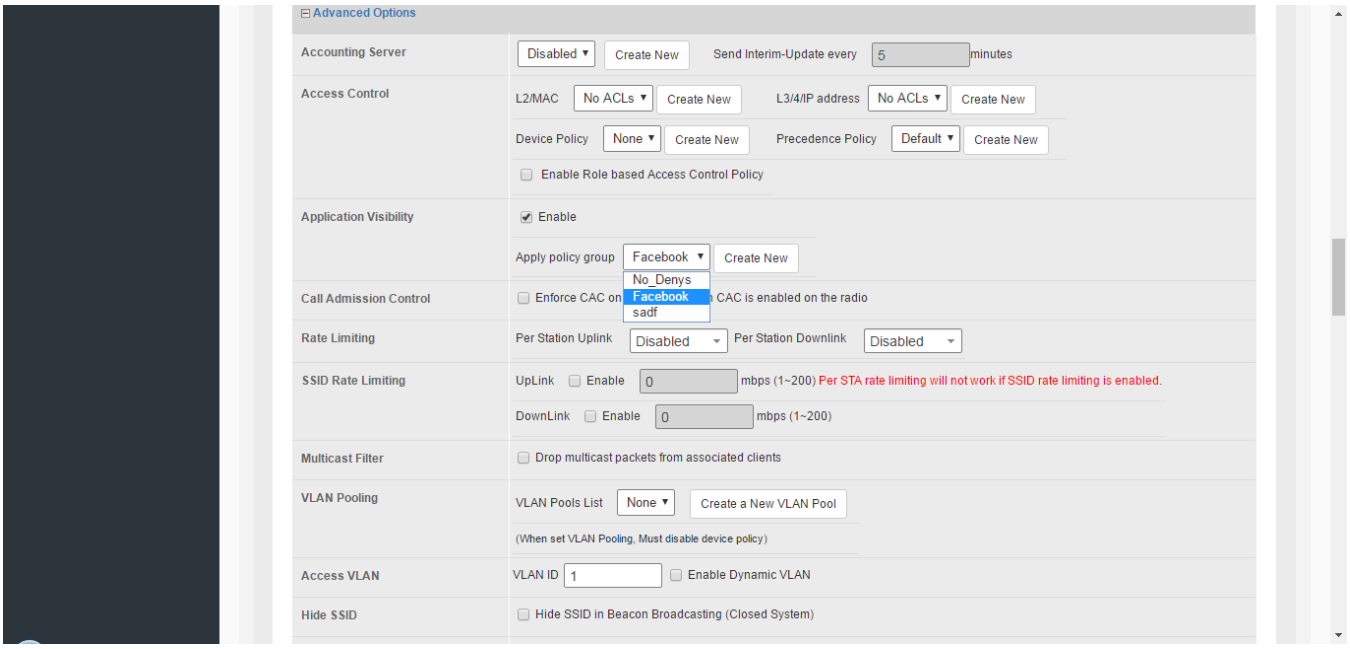
Applying an Application Policy to a WLAN

Once an Application Policy is created, use the following procedure to apply it to one or more WLANs.

1. Go to **Wireless LANs**, and click **Edit** next to the WLAN you want to configure.
2. Expand the **Advanced Options** section.
3. Locate the **Application Visibility** section, and ensure that the **Enable** check box is enabled.
4. Select the policy you created from the **Apply Policy Group** list.

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

FIGURE 170 Apply an Application Policy to a WLAN



Configure IP Based User Defined Applications

When an application is unrecognized and generically categorized, you can configure an explicit application identification policy by destination IP Address, Port and Protocol.

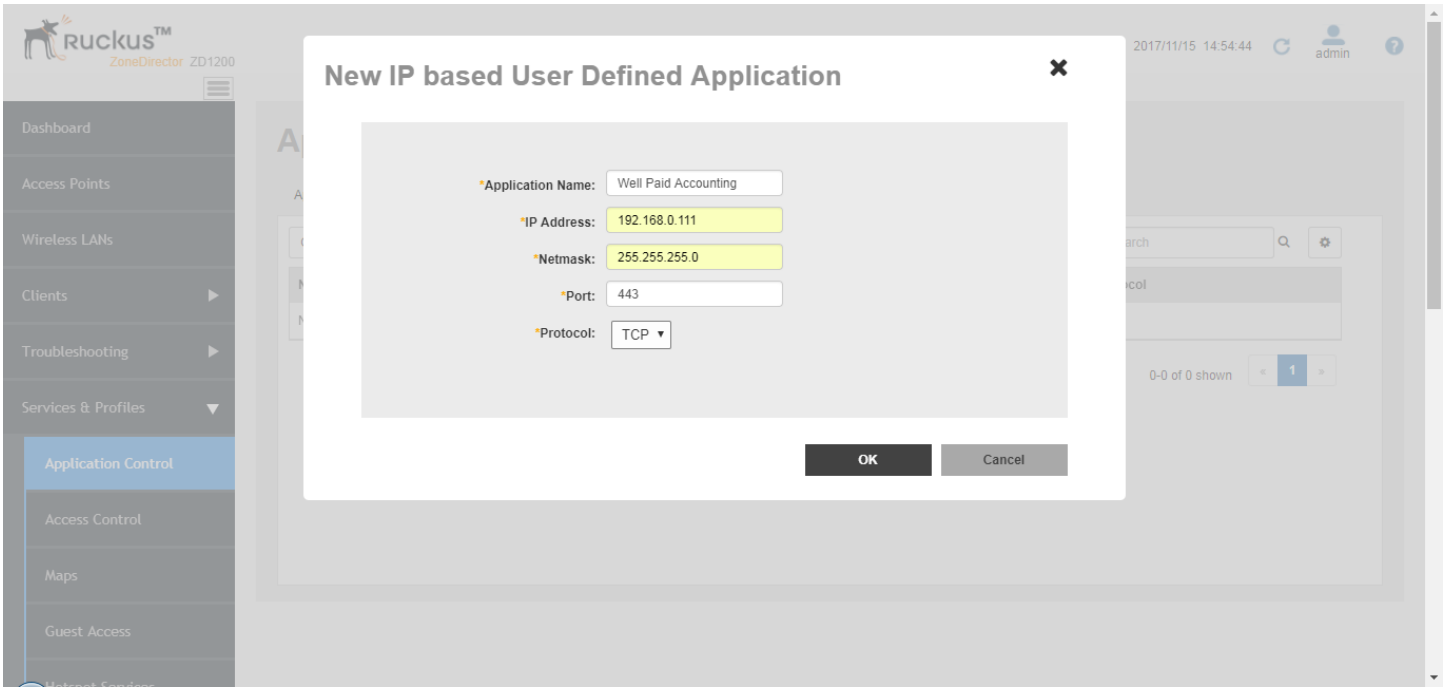
Wireless traffic that matches a configured policy will be displayed using the policy's name on the **Applications** pie charts/tables on the **Wireless Clients** monitoring page.

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

The following figure shows how to configure an IP-based user defined application policy to identify a corporate accounting application. ZoneDirector identifies wireless traffic matching this policy as "Well Paid Accounting" and displays this name in the application recognition pie charts and tables.

FIGURE 171 Defining custom applications for ZoneDirector identification



Configure Port Based User Defined Applications

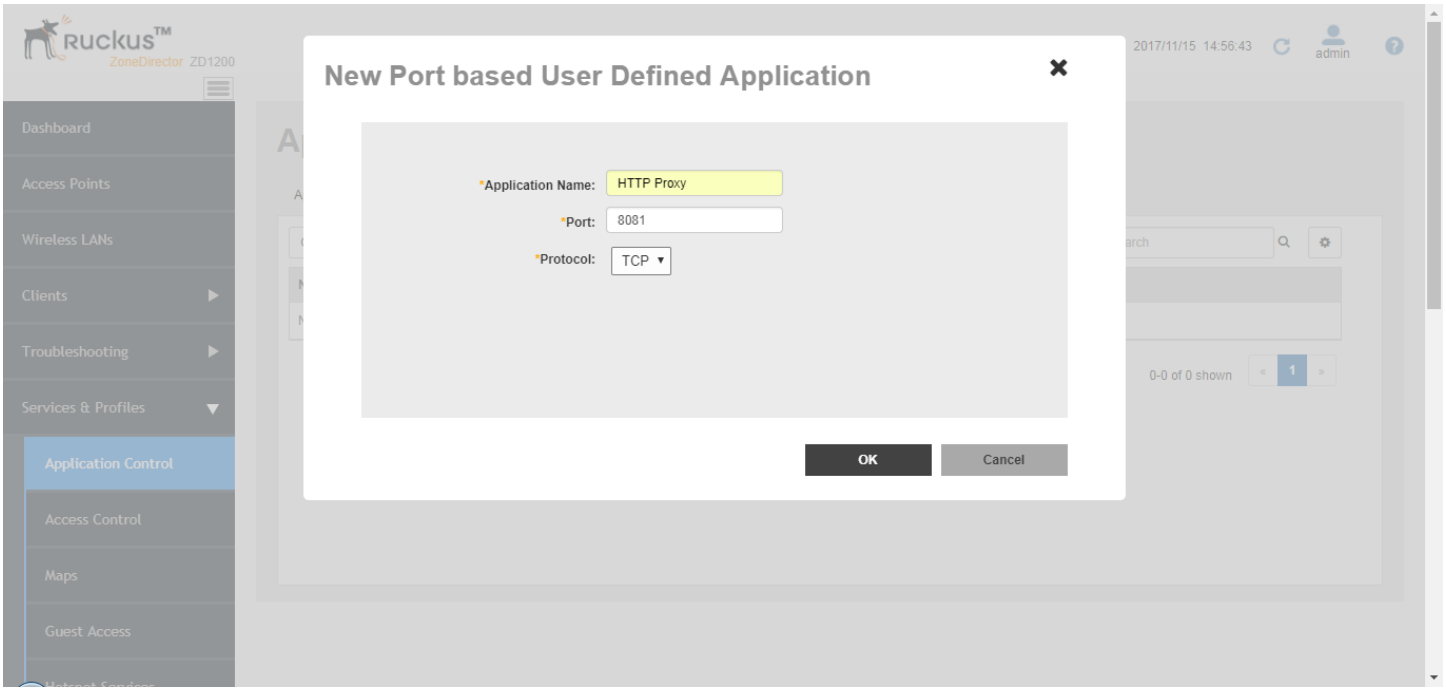
When an application is unrecognized and generically (or incorrectly) categorized you can configure an application identification policy by IP Port and Protocol.

Wireless traffic that matches a configured policy will be displayed using the policy's Description text in the Applications pie charts/tables on the Wireless Clients monitoring page.

This type of policy is the least granular in configuration, and therefore 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 user defined application policy or ZoneDirector's embedded policies will be identified as belonging to this policy.

The following figure shows how a port-based application policy could be used to categorize all otherwise uncategorized wireless traffic on Port 8081 as "HTTP Proxy" traffic and display this name in application recognition pie charts and tables.

FIGURE 172 Creating a new port based user defined application



Well-Known Service and Destination Port Mappings Defined in Application Visibility

ZoneDirector automatically identifies many of the most common applications for use in application recognition and filtering policies.

The following links provide lists of some common applications and ports that are included:

- IANA list of Service Names and Port Numbers
- SpeedGuide.net
- Well known TCP and UDP ports used by Apple software products
- Bitcoin
- Google Cloud Messaging
- PlayStation
- TiVo
- Wii
- Xbox

Configuring Network Access Controls

ZoneDirector provides several options for controlling access to your wireless networks and to other wired/wireless network resources.

This section is divided into the following subsections according to the features on the **Services & Profiles** > **Access Control** page.

Creating Layer 2/MAC Address Access Control Lists

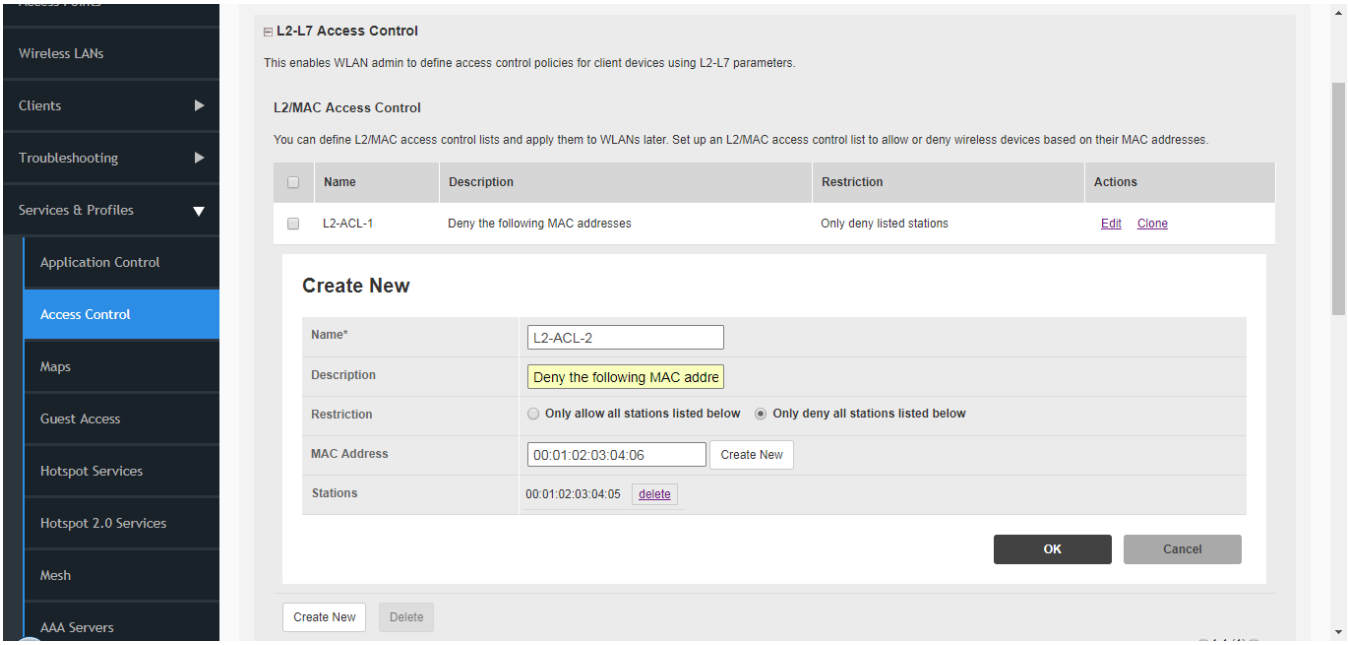
Using the Access Controls configuration options, you can define Layer 2/MAC address ACLs, which can then be applied to one or more WLANs (upon WLAN creation or edit).

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 at ZoneDirector.

To configure an L2/MAC ACL:

1. Go to **Services & Profiles** > **Access Control**
2. Expand the **L2-L7 Access Control** section.
3. In L2/MAC Access Control, click **Create New**Alternatively, you can create a Layer 2/MAC ACL from the WLAN creation page while creating a new WLAN or modifying an existing WLAN (**Wireless LANs** > **Edit** > **Advanced Options** > **Access Control** > **L2/MAC** > **Create New**.)
4. Type a **Name** for the ACL.
5. Type a **Description** of the ACL.
6. Select the **Restriction** mode as either **allow** or **deny**.
7. 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.
8. 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 173 Configuring an L2/MAC access control list



Creating Layer 3/Layer 4/IP Address Access Control Lists

In addition to L2/MAC based ACLs, ZoneDirector also allows you to create access controls at Layer 3 and Layer 4.

These controls can be applied based on a set of criteria including:

- Source Address
- Destination Address
- Application
- Protocol
- Source Port
- Destination Port

To create an L3/L4/IP address based ACL:

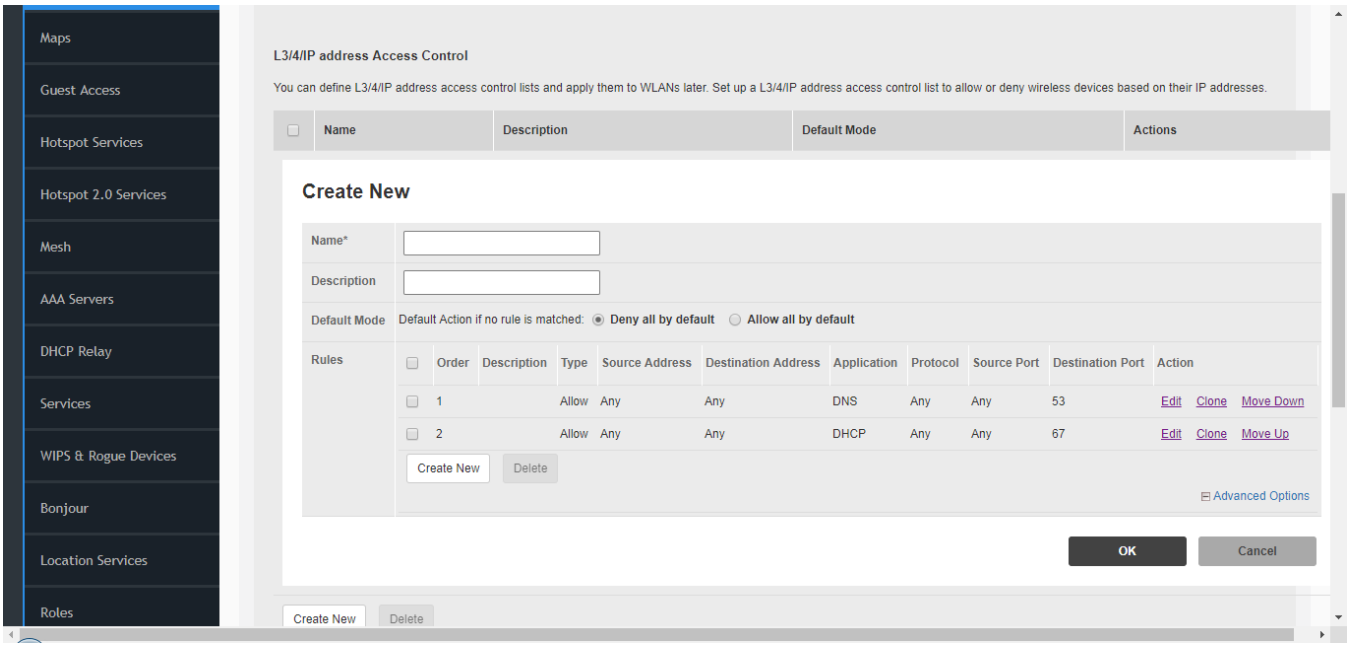
1. Go to **Services & Profiles** > **Access Control**.
2. Expand the **L2-L7 Access Control** section.
3. In **L3/4/IP address Access Control**, click **Create New**.

   NOTE
   Alternatively, you can create a Layer 3/Layer 4/IP Address ACL from the WLAN creation page while creating a new WLAN or modifying an existing WLAN (**Wireless LANs** > **Edit** > **Advanced Options** > **Access Control** > **L3/4/IP Address** > **Create**.)

4. Type a **Name** for the ACL.
5. Type a **Description** for the ACL.
6. In **Default Mode**, set the default action to perform if no rule is matched.
7. In **Rules**, click **Create New** or click **Edit** to edit an existing rule.
8. Define each access rule by configuring a combination of the following:
   - **Type**: The access privilege (allow or deny) that this rule grants.
   - **Source Address**: Enter a source IP address from which to allow or block traffic. IP address must be in the format A:B:C:D/M, where M is the netmask. To allow/deny a single host, use /32 as the netmask.
   - **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 netmask. 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/protocol-numbers.xhtml) to allow or deny. Otherwise, select Any.
   - **Source Port**: Enter a valid port number (1-65534) or port range (e.g., 80-443).
   - **Destination Port**: Enter a valid port number (1-65534) or port range (e.g., 80-443).
9. Click **OK** to save the ACL.

10. Repeat these steps to create up to 32 L3/L4/IP address-based access control rules.

FIGURE 174 Configuring an L3/L4 access control list



Configuring Device Access Policies

Device access policies can be configured to control which device types will be allowed access to your wireless networks.

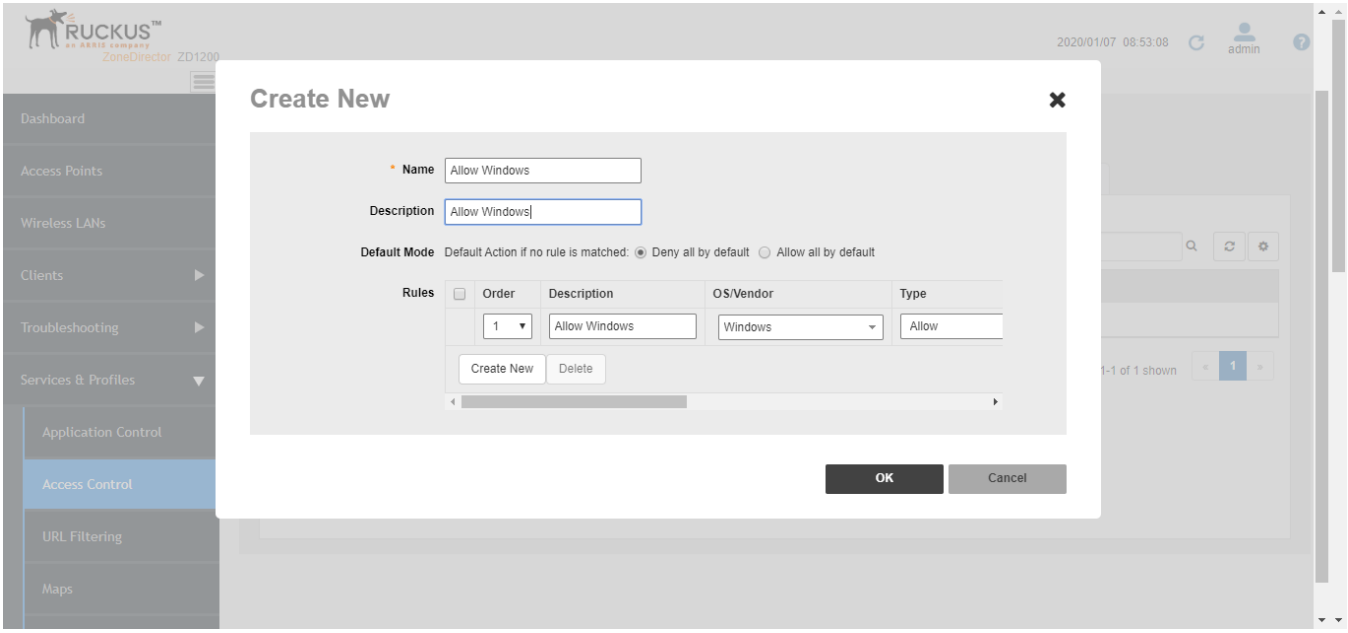
To configure a device access policy:

1. Go to **Services & Profiles > Access Control > Device Access Policy**.
2. Click **Create** to create a new policy or **Edit** to edit an existing policy.
3. Enter a **Name** and optionally a **Description** for the policy.
4. In **Default Mode**, select **Deny all by default** or **Allow all by default**.

   For example, if you want to create a rule that will allow only Windows devices and deny all others, you could select **Deny all by default**, and then create a rule to allow Windows devices.
5. In **Rules**, click **Create New** to create a new rule.
6. For each rule, select an **OS/Vendor** from the list, select **Type** (allow or deny), and optionally, configure per-station rate limiting and VLAN assignment for this device type.

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

FIGURE 175 Creating a device policy rule to allow only Windows devices



Configuring Precedence Policies

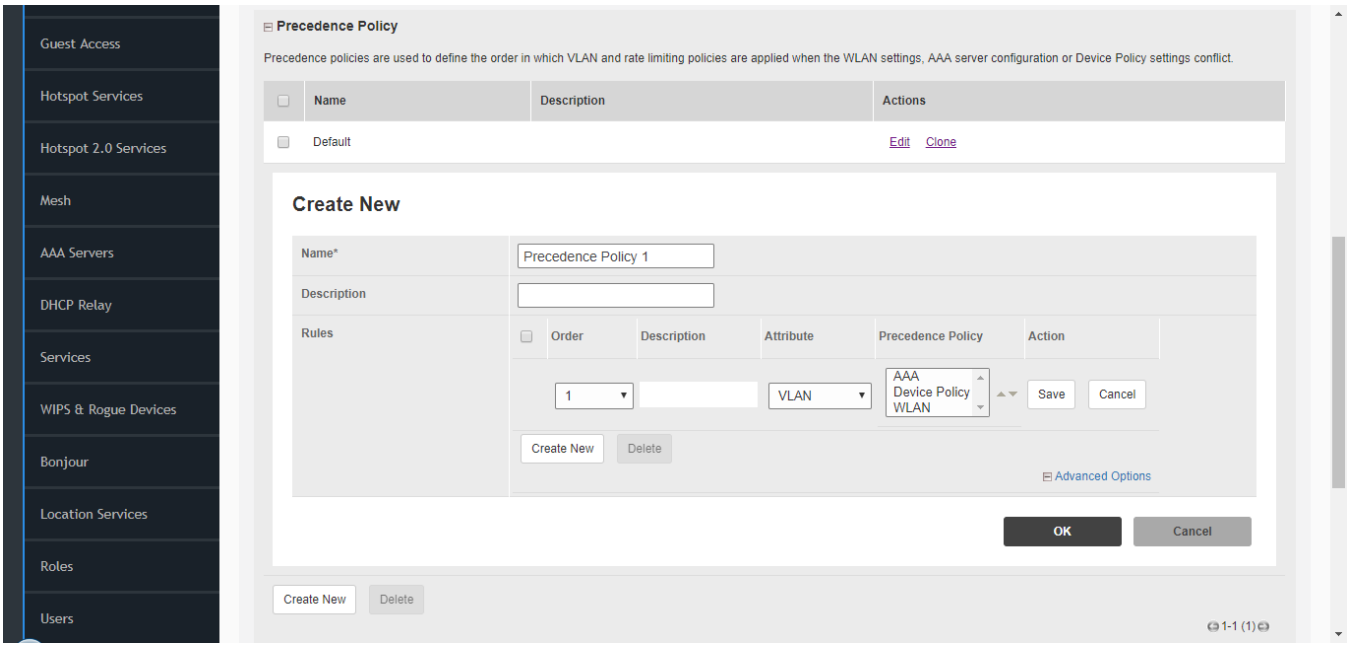
Use the Precedence Policy settings to define the priority order in which rate limiting and VLAN policies are applied to a WLAN.

To configure Precedence Policies:

1. Go to **Services & Profiles** > **Access Control**.
2. In the **Precedence Policy** section, click **Edit** to modify the default policy or click **Create New** to create a new policy to be selectable from the WLAN configuration dialog. Alternatively, you can create a Precedence Policy from the WLAN creation page while creating a new WLAN or modifying an existing WLAN (**Wireless LANs** > **Edit** > **Advanced Options** > **Access Control** > **Precedence Policy** > **Create New**.)
3. Under **Rules**, click **Create New** to create a new rule for this policy.
4. Select an **Attribute** (VLAN or Rate Limiting) to apply a precedence policy.
5. Select a **Precedence Policy** (AAA Server, Device Policy or WLAN Configuration) and click up and down arrows to set the order in which policies will take precedence.
6. Click **Save** to save the rule. You can create up to two rules per policy. The rules will be applied in the order shown in the Order column.

7. Click **OK** to save the precedence policy. This policy is now available for selection in WLAN configuration.

FIGURE 176 Precedence Policy settings



Blocking Client Devices

When users log into a ZoneDirector network, their client devices are recorded and tracked. If, for any reason, you need to block a client device from network use, you can do so from the web interface. The following subtopics describe various tasks that you can perform.

Note the following considerations when managing the Blocked Clients list:

- The block list is system-wide and is applied to all WLANs in addition to any per-WLAN ACLs. If a MAC address is listed in the system-wide block list, it will be blocked even if it is an allowed entry in an ACL. Thus, the block list takes precedence over an ACL
- MAC addresses that are in the deny list are blocked at the AP, not at ZoneDirector.

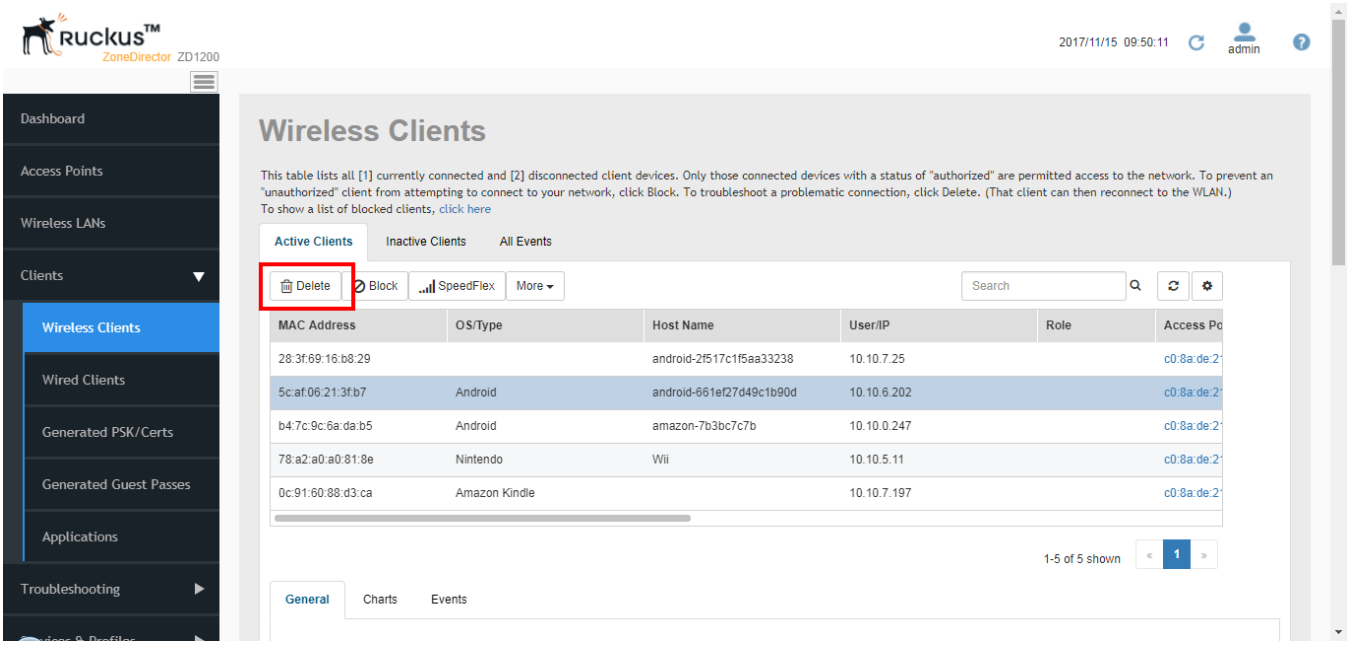
Temporarily Disconnecting Specific Client Devices

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. Go to **Clients > Wireless Clients**.
2. Look at the **Status** column to identify any "Unauthorized" users

3. Click the **Delete** button. The entry is deleted from the **Active Clients** list, and the listed device is disconnected from your Ruckus WLAN.

FIGURE 177 Click the Delete button to temporarily delete a client. The client will be able to reconnect.



The user can reconnect at any time, which, if this proves to be a problem, may prompt you to consider Permanently Blocking Specific Client Devices on page 234.

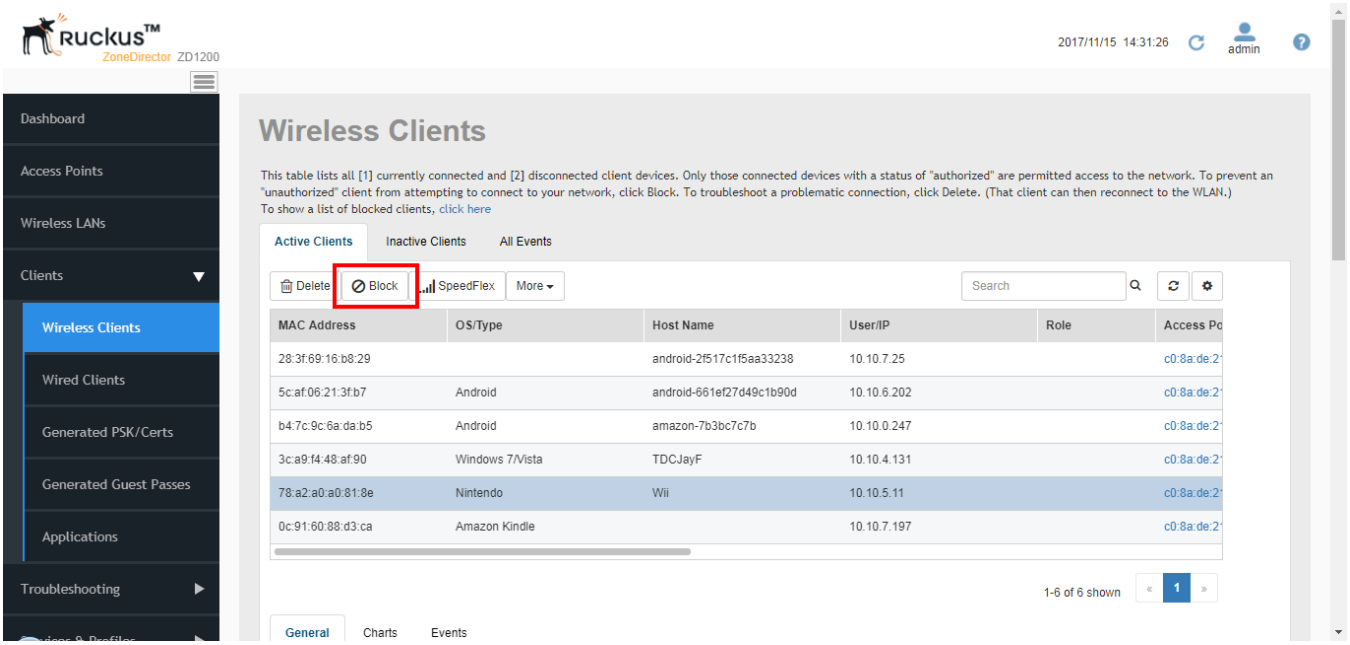
Permanently Blocking Specific Client Devices

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

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

2. Click the **Block** button to move this client to the blocked clients list.

FIGURE 178 Click the Block button to permanently block a client



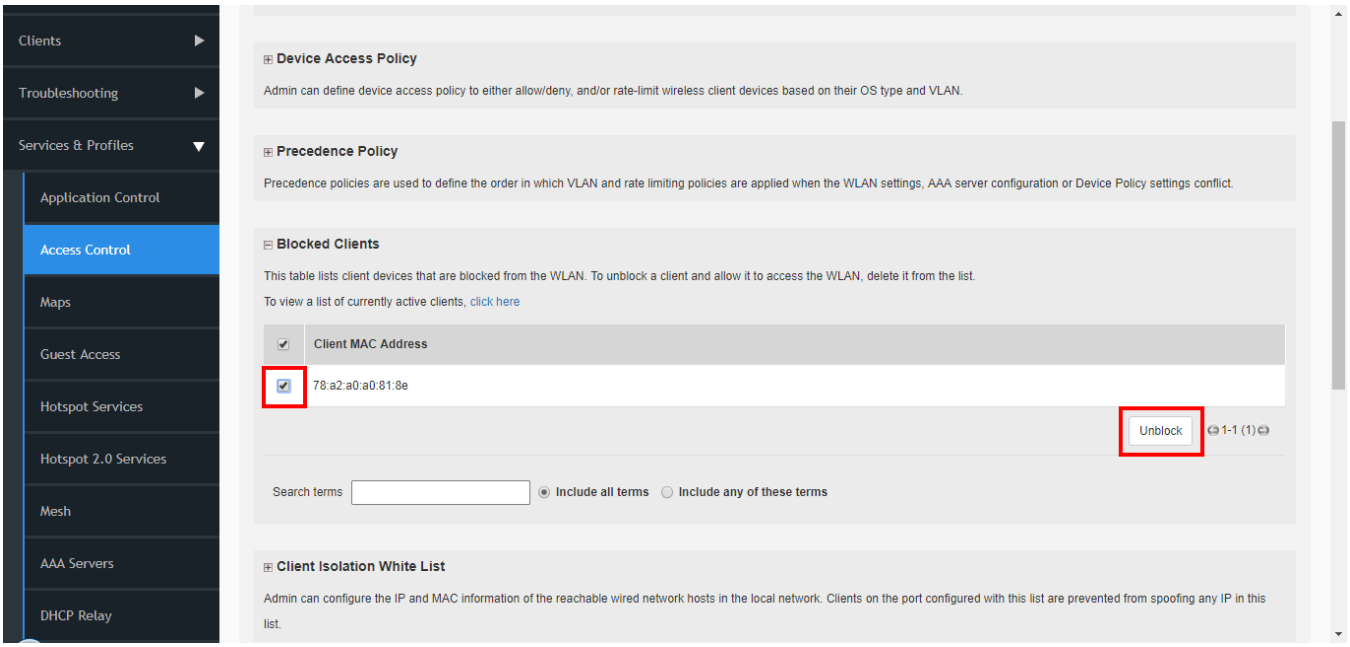
The status is changed to **Blocked**. This will prevent the listed device from using your Ruckus WLANs.

Reviewing a List of Previously Blocked Clients

1. Go to **Services & Profiles** > **Access Control**> **Blocked Clients List**.
2. Review the **Blocked Clients** table.

3. You can unblock any listed MAC address by clicking the **Unblock** button for that address.

FIGURE 179 Unblocking a previously blocked client



Configuring Client Isolation White Lists

When Wireless Client Isolation is enabled on a WLAN, all communication between clients and other local devices is blocked at the Access Point. To prevent clients from communicating with other nodes, the Access Point drops all ARP packets from stations on the WLAN where client isolation is enabled and which are destined to IP addresses that are not part of a per-WLAN white list.

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

To create a Client Isolation White List:

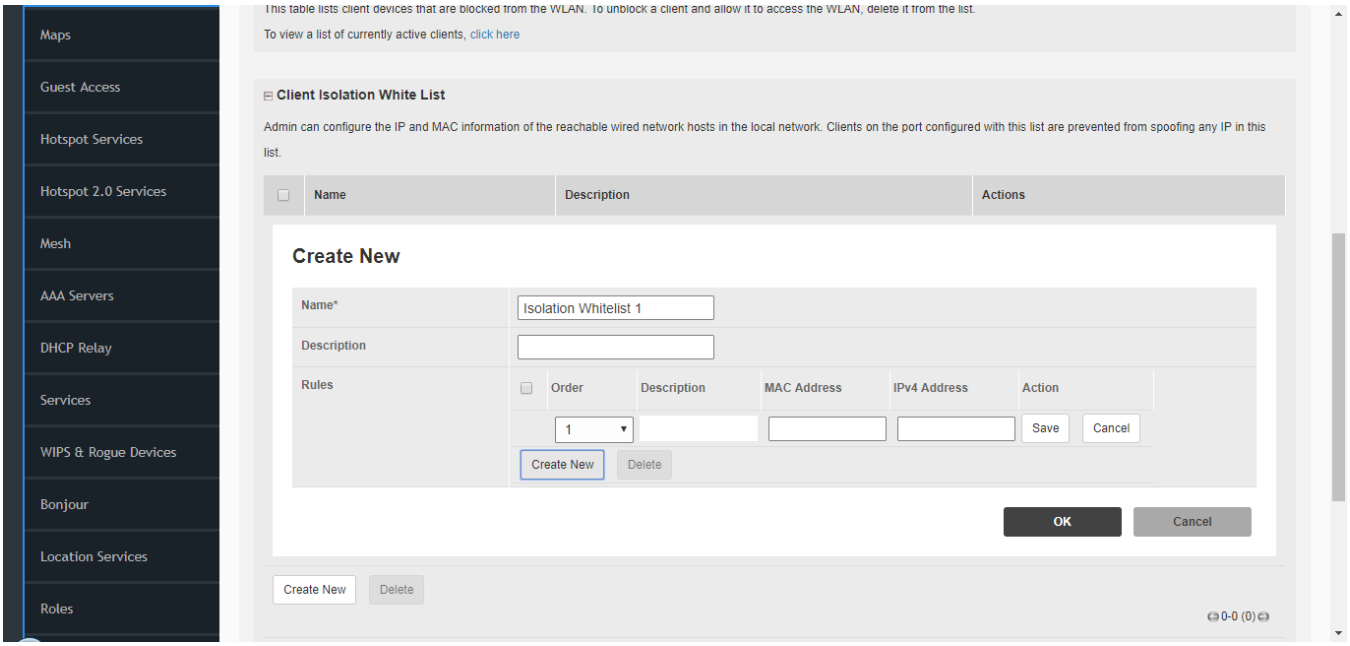
1. Go to **Services & Profiles** > **Access Control** > **Client Isolation Whitelist**.
2. Expand the **Client Isolation White List** section, and click **Create New**.

> **NOTE**
> You can also create a Client Isolation White List while creating a WLAN from within the WLAN configuration screen (**Wireless LANs** > **Create New** > **Wireless Client Isolation** > **Create New**).

3. Enter a **Name** and optionally a **Description** for the access policy.
4. In **Rules**, you can create multiple device-specific rules for each device to be white listed.
   - **Description**: Description of the device.
   - **MAC Address**: Enter the MAC address of the device.
   - **IPv4 Address**: Enter the IP address of the device.
5. Click **Save** to save the rule you created.

6. To change the order in which rules are implemented, select the order from the drop-Order column. You can also **Edit** or **Clone** rules from the **Action** column. To delete a rule, select the box next to the rule and click **Delete**.
7. Click **OK** to save the white list.

FIGURE 180 Creating a Client Isolation White List

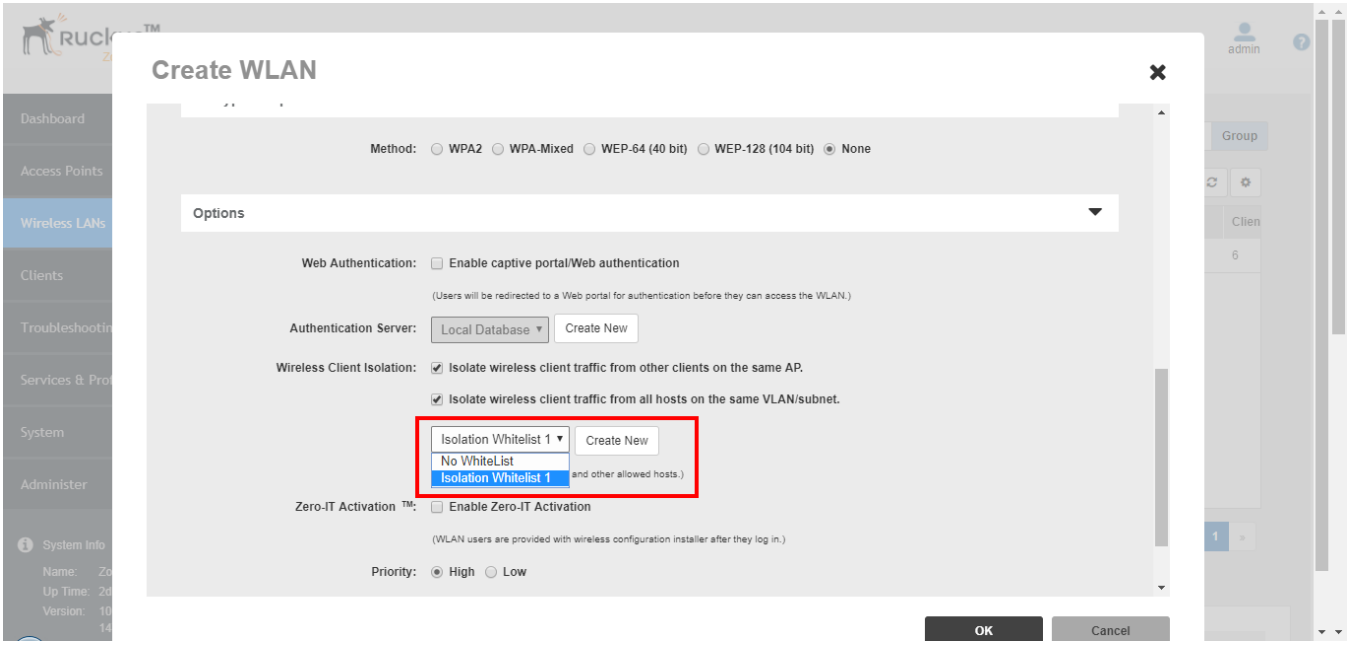


To apply a Client Isolation White List to a WLAN:

1. Go to **Wireless LANs**.
2. Click **Edit** next to the WLAN you want to edit.
3. In **Wireless Client Isolation** (under Options), select the level of client isolation you want to enforce:
   - **Isolate wireless client traffic from other clients on the same AP**: Enable client isolation on the same Access Point (clients on the same subnet but connected to other APs will still be able to communicate).
   - **Isolate wireless client traffic from all hosts on the same VLAN/subnet**: Prevent clients from communicating with any other hosts on the same subnet or VLAN other than those listed on the Client Isolation Whitelist. If this option is chosen, you must select a Whitelist from the drop-down list of those you created on the **Services & Profiles** > **Access Control** page.

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

FIGURE 181 Selecting a Client Isolation White List



URL Filtering

URL filtering allows administrators to manage internet usage by preventing access to inappropriate websites using a customizable combination of blacklists and whitelists.

The ZoneDirector 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*).

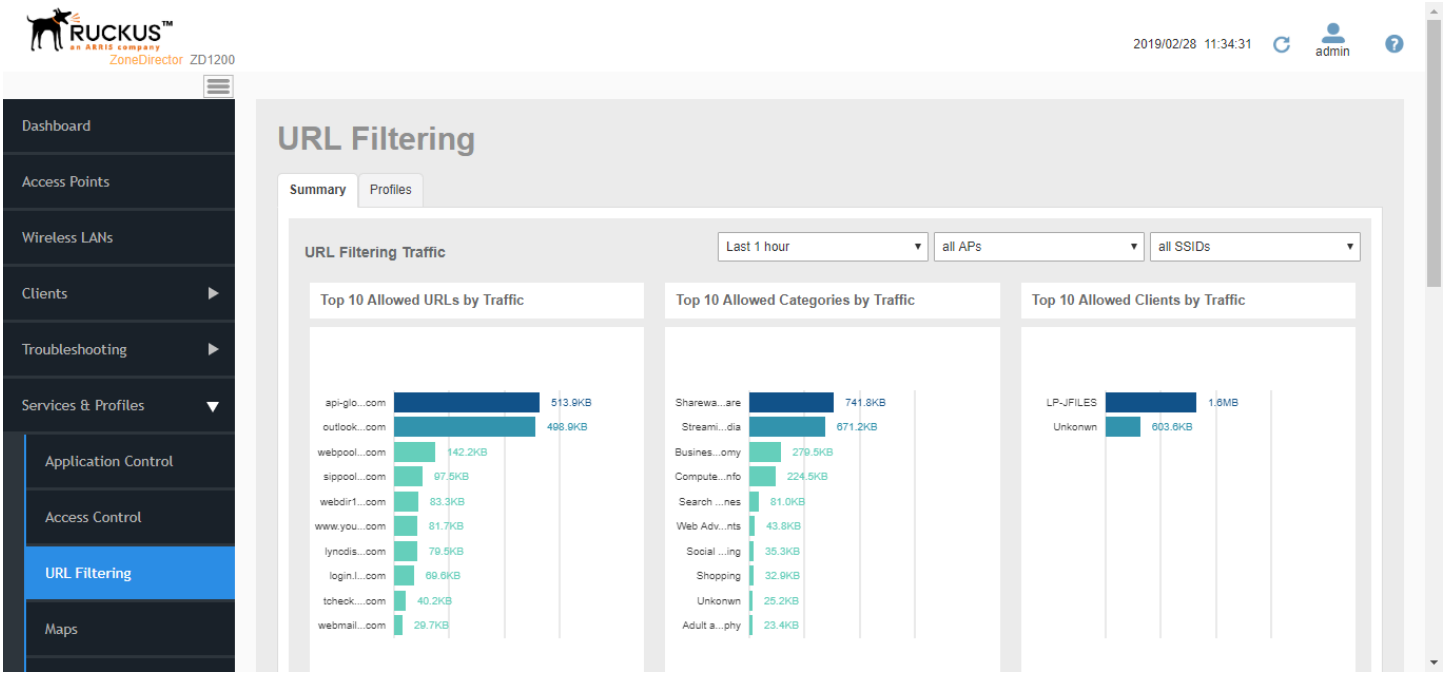
To deploy URL filtering, you must create a URL filtering profile using either one of the preset category groups or a customized selection of categories. Once a profile is created, you can apply it to either one or more WLANs or to a user role for role-based access control.

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 182 Viewing URL filtering reports



Creating a URL Filtering Profile

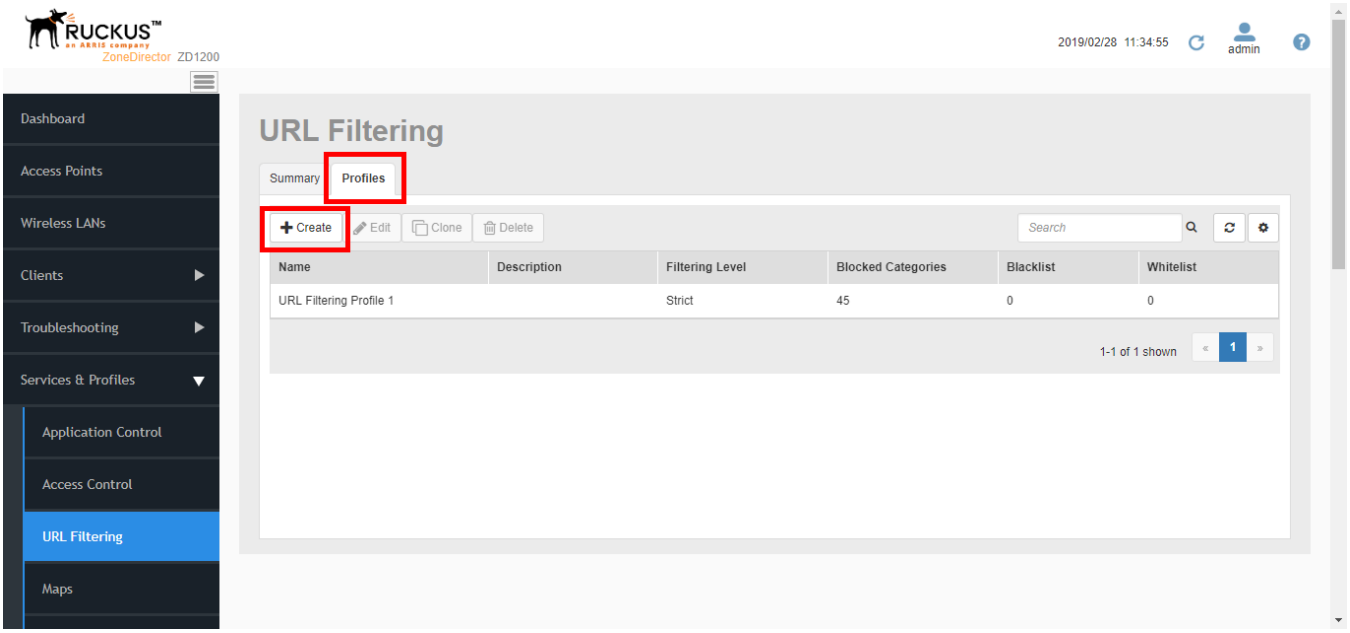
You must create a URL filtering profile before you can apply the profile to a WLAN or to a user role.

To create a URL filtering profile:

1. Go to **Services & Profiles > URL Filtering**.
2. Click the **Profiles** tab.

3. Click **Create**. The *Create New* form appears.

FIGURE 183 Creating a URL filtering profile



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

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

FIGURE 184 Select level of strictness

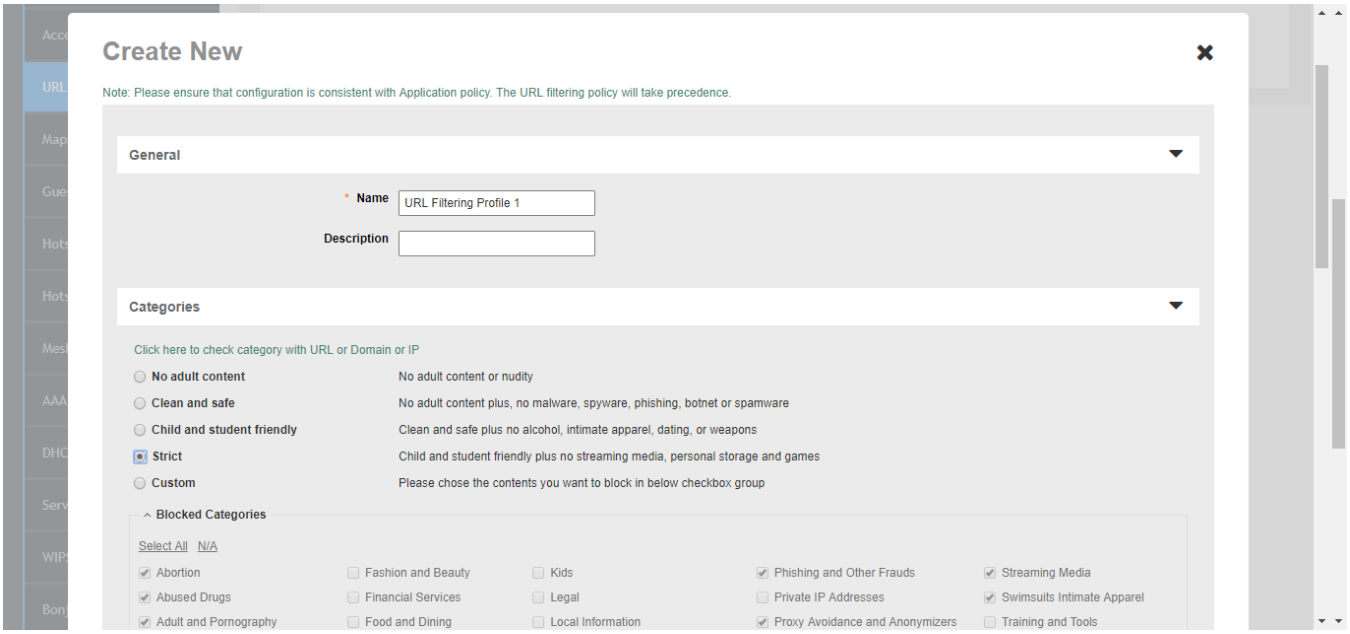
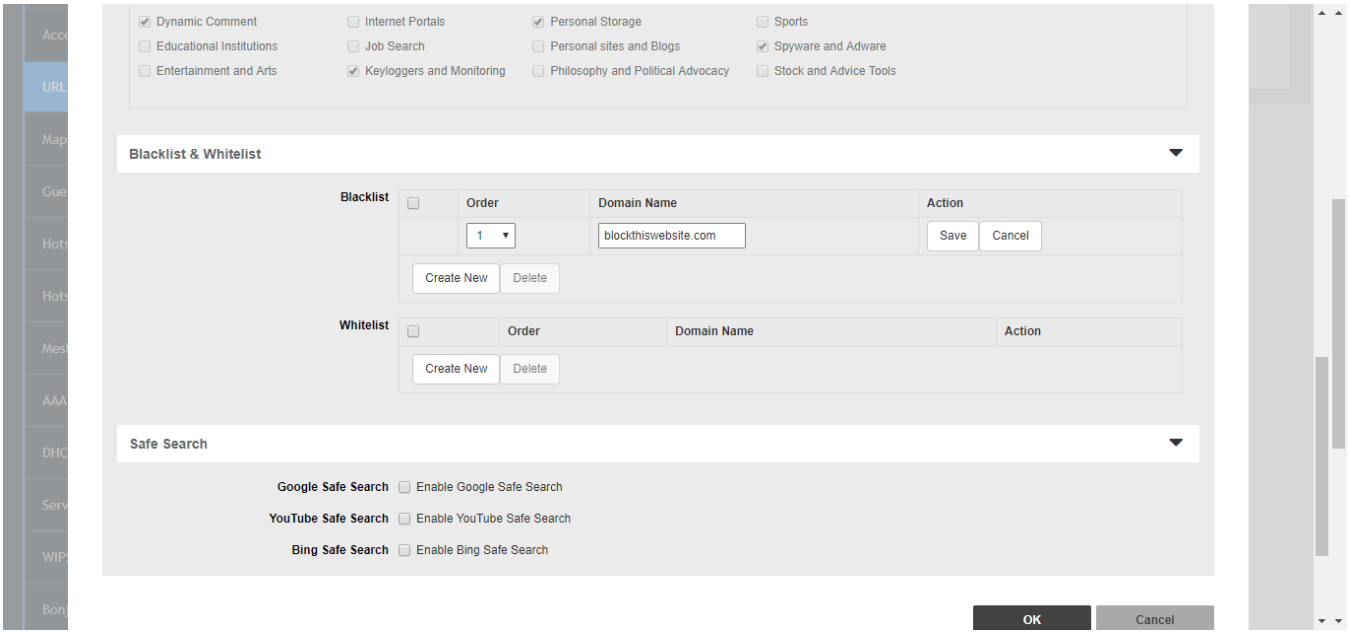


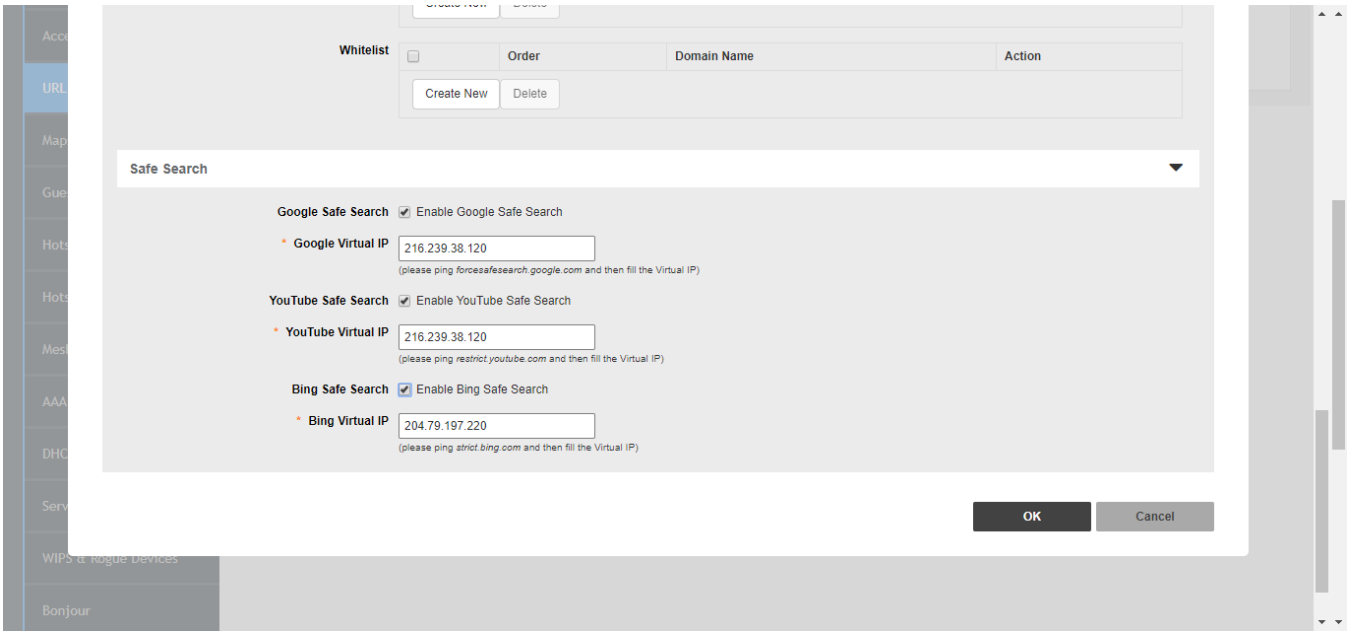
FIGURE 185 Blacklisting or whitelisting a specific URL



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

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

   FIGURE 186 Enable Google, Youtube and Bing Safe Search options



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

Applying a URL Filtering Policy to a WLAN

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

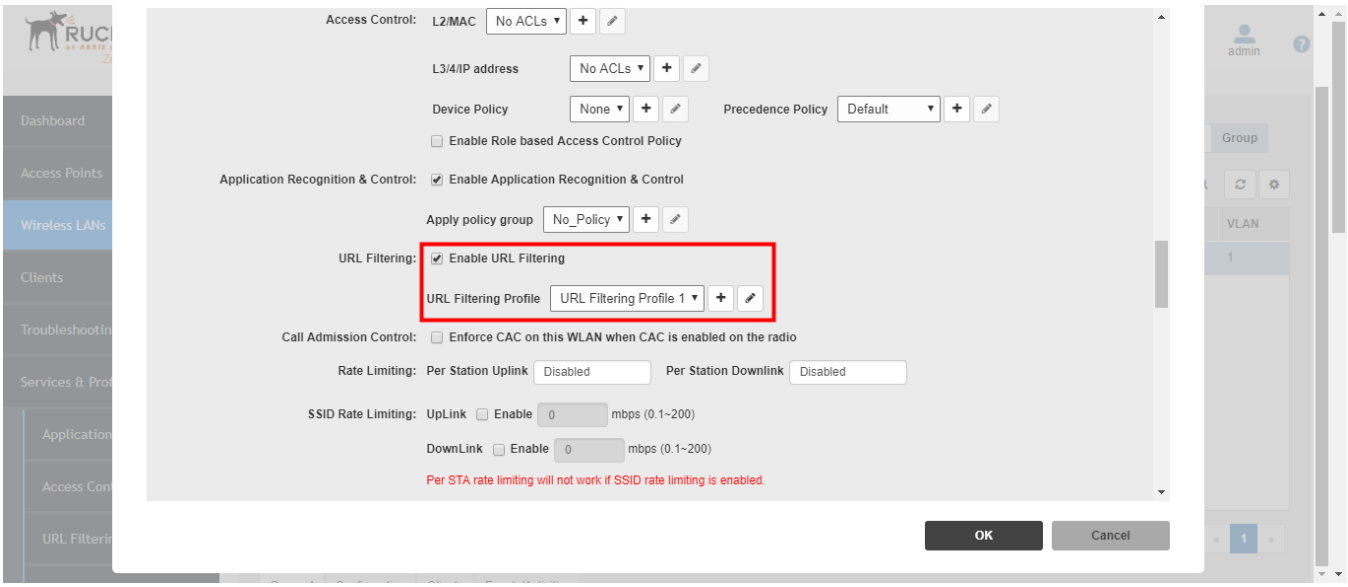
To apply a URL filtering policy to a WLAN:

1. Go to **Wireless LANs**, select the WLAN you would like to configure, and click **Edit**.
2. Scroll down and expand the **Advanced Options** section.
3. In *URL Filtering*, select **Enable URL Filtering** and select a **URL Filtering Profile** that you created from the drop-down list.

   Alternatively, click the **+** (Create New) icon to create a new policy and apply it to this WLAN.

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

FIGURE 187 Enabling URL filtering for a WLAN



Applying a URL Filtering Policy to a Role

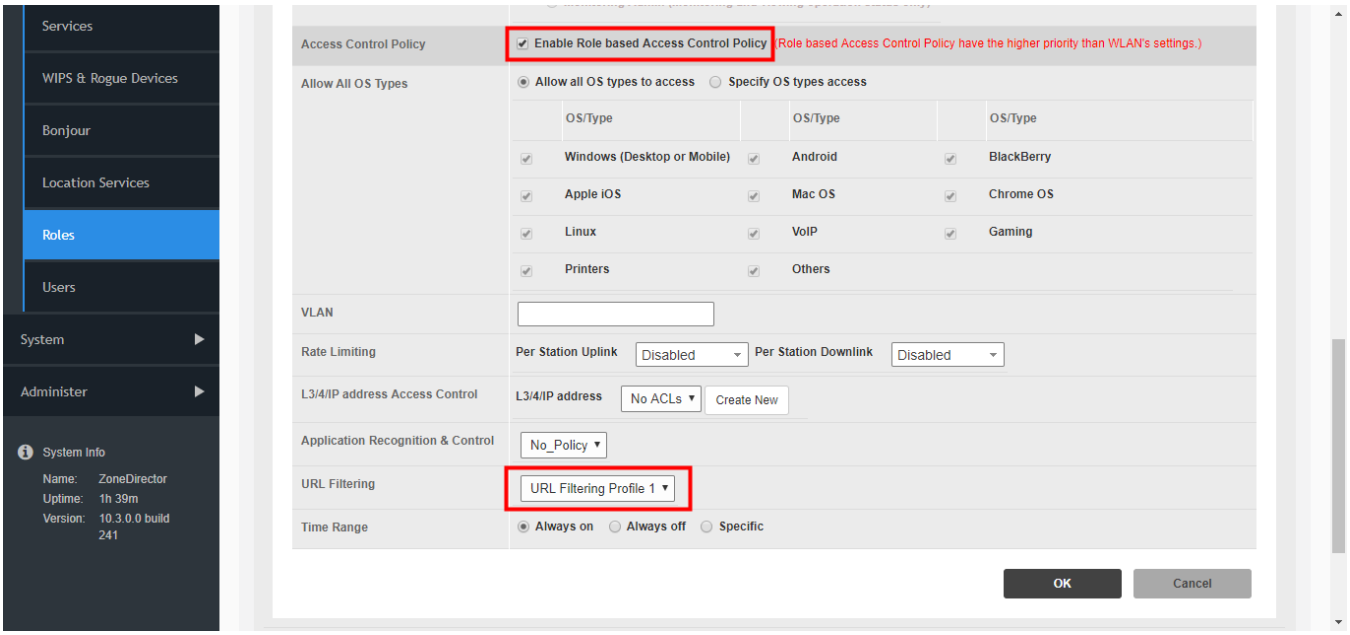
To apply a URL filtering policy to a user role, use the following procedure:

1. Go to **Services & Profiles > Roles**.
2. Select a role from the list and click **Edit**, or click **Create New** to create a new user role.
3. In *Access Control Policy*, enable **Enable Role Based Access Control Policy**.

   For more information on Role Based Access Controls (RBAC), see *Role Based Access Controls*.
4. In *URL Filtering*, select a URL filtering profile you created from the drop-down list.

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

FIGURE 188 Applying a URL Filtering policy to a role



Working with URL Filtering Licenses

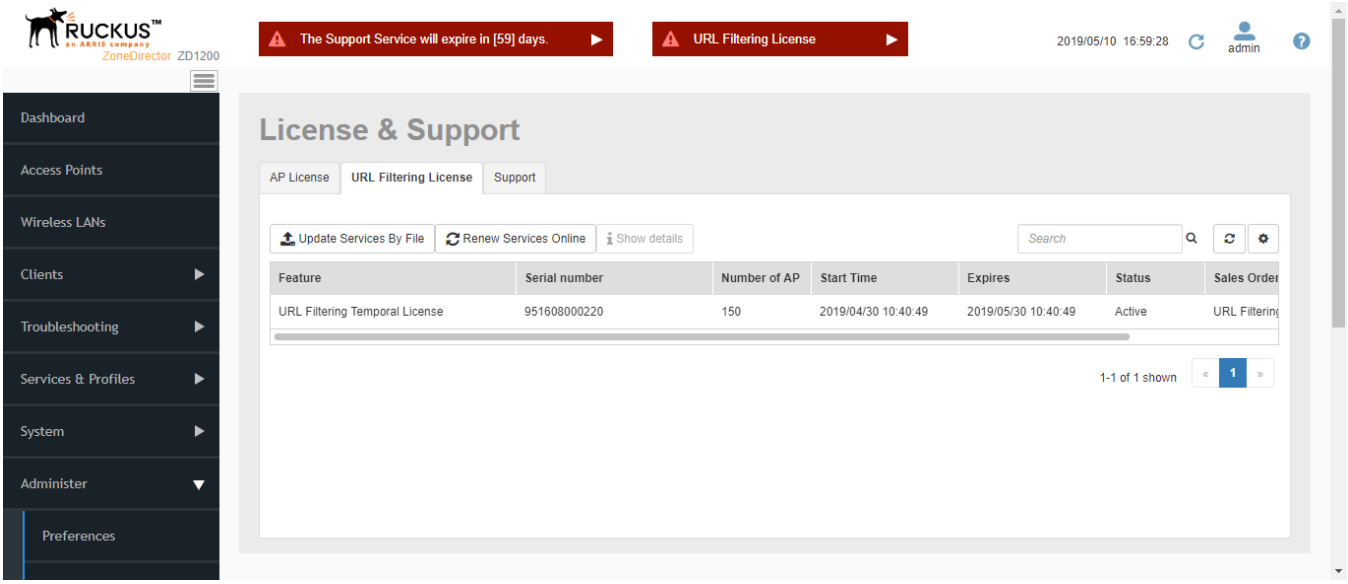
URL Filtering service requires an active URL filtering license on the ZoneDirector to function. URL filtering licenses can be purchased from Ruckus partners and distributors, and a temporary license is also available to allow customers to try out the service for a limited time before purchasing.

To manage URL filtering licenses:

1. Go to **Administer > License & Support**.

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

FIGURE 189 Working with URL filtering licenses



Configuring Maps

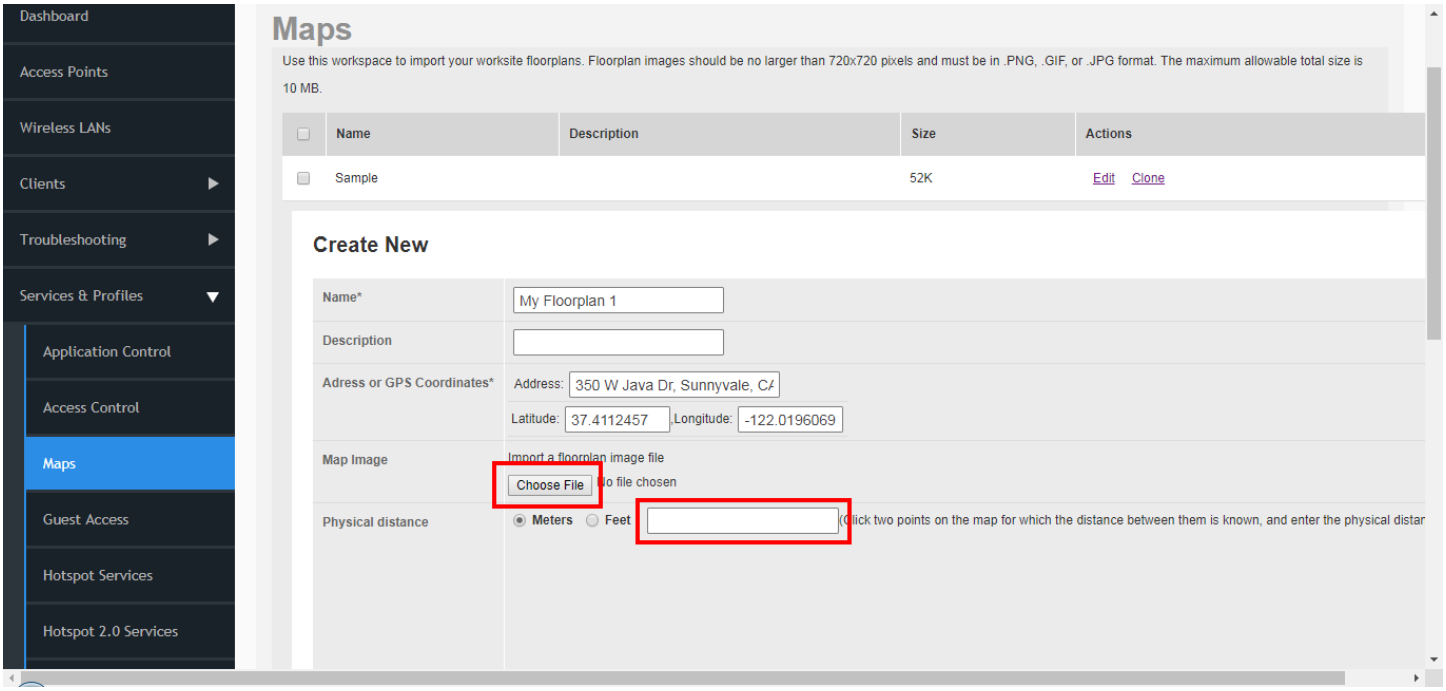
Configuring Floorplan Maps

If you import a floorplan map and enter its GPS coordinates or street address, it will be displayed at the relevant location on the world map on the Dashboard.

To import a floorplan map, go to **Services & Profiles > Maps** and click **Create New**. Enter a **Name** for the map, and either enter the street **Address** or GPS coordinates in **Latitude** and **Longitude**.

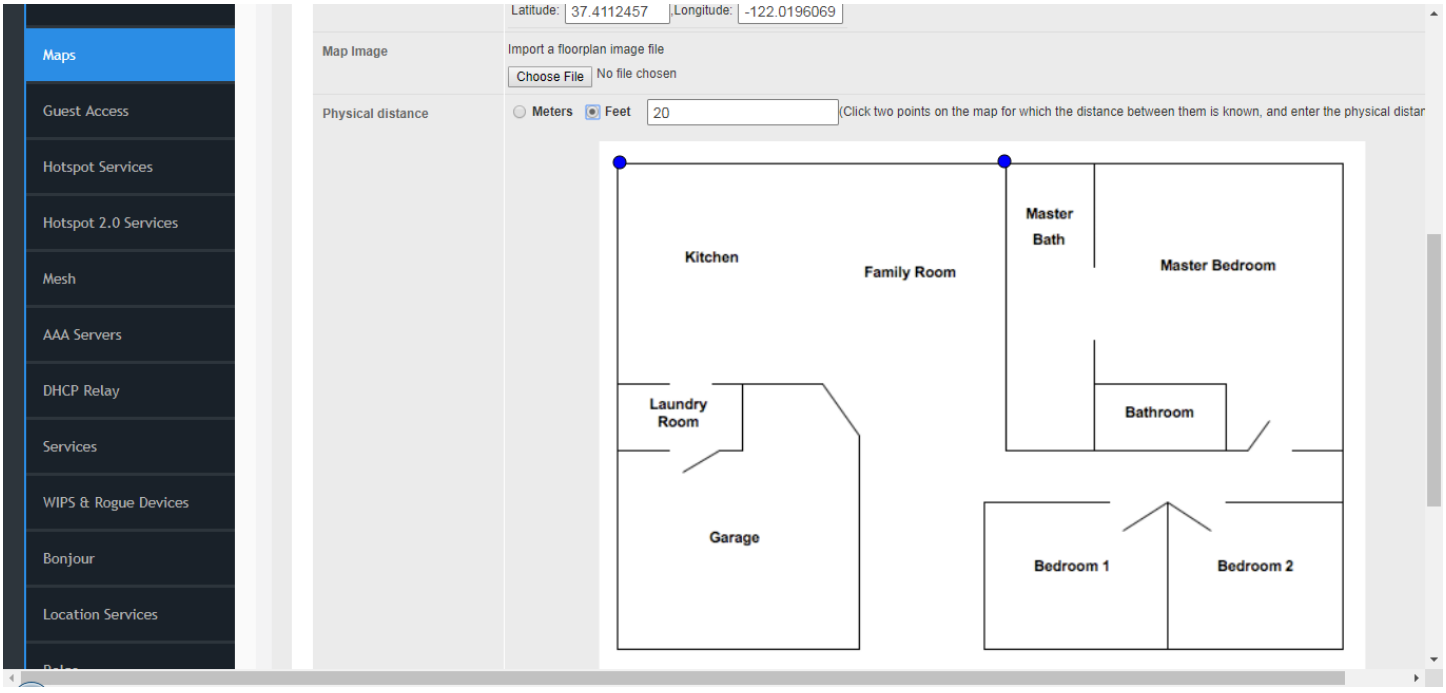
Next, click **Choose File** and select an image in JPG, PNG or BMP image format. Click **Import** to import the image.

FIGURE 190 Creating a new floorplan map



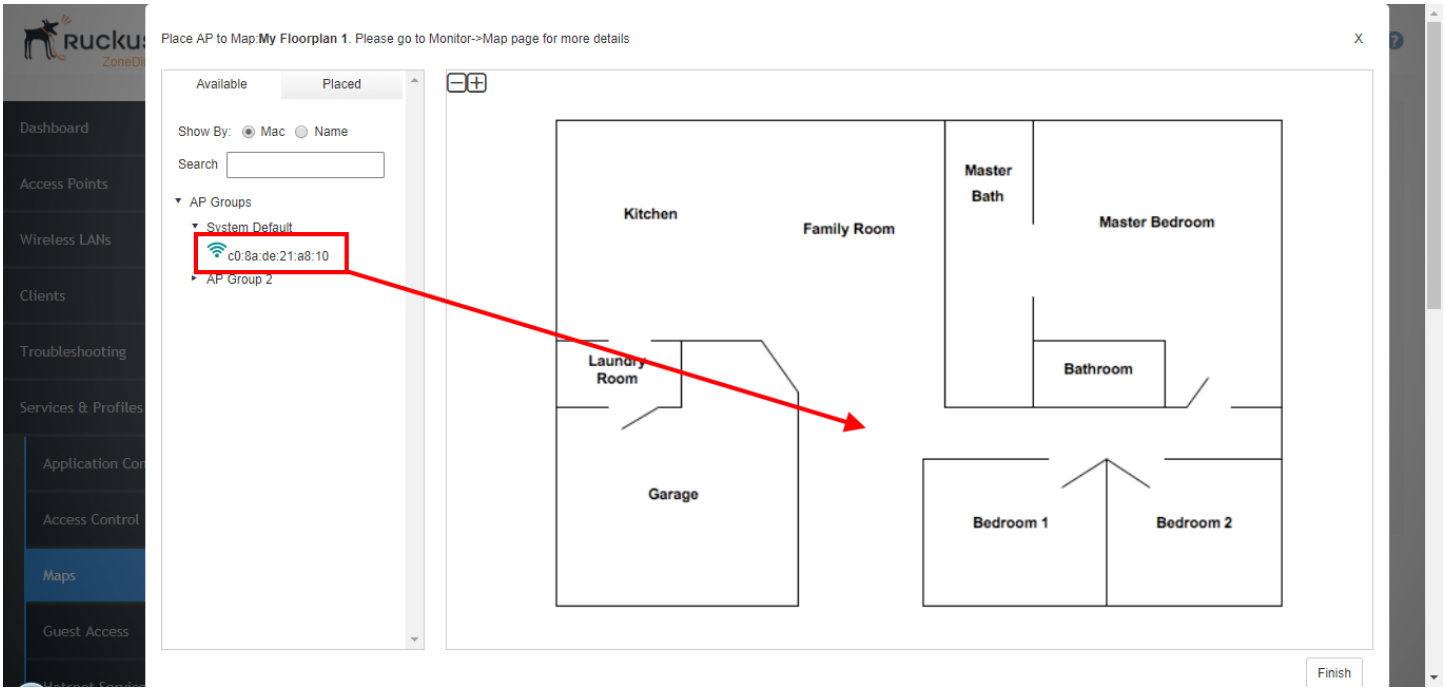
Click two points on the map between which the distance is known, and enter the **Physical Distance** in meters or feet.

FIGURE 191 Create a floorplan map



Click **Next**. On the next screen, drag APs from the list on the left onto the map to represent their actual physical locations.

FIGURE 192 Drag an AP on to the map



Click **Finish**.

Guest Access

The *Services & Profiles > Guest Access* page provides options for configuring access to your guest networks.

For information on guest access configuration, see Configuring Guest Access on page 125.

Hotspot Services

The *Services & Profiles > Hotspot Services* and *Hotspot 2.0 Services* pages provide options for configuring guest hotspot service.

For more information on Hotspot and Hotspot 2.0 configuration, see Creating a Hotspot Service on page 185.

Mesh Configuration

The *Services & Profiles > Mesh* page provides options for enabling and configuring mesh settings.

For more information, see Deploying a Smart Mesh Network on page 383.

Using an External AAA Server

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 ZoneDirector to the AAA server so that requests will be passed through ZoneDirector before access is granted.

This section describes the tasks that you need to perform on ZoneDirector to ensure ZoneDirector can communicate with your AAA server.

> **NOTE**
> For specific instructions on AAA server configuration, refer to the documentation that is supplied with your server.

ZoneDirector supports the following types of AAA server:

- Active Directory for Web Portal
- Active Directory for 802.1X
- LDAP
- RADIUS
- RADIUS Accounting
- TACACS+

A maximum of 32 AAA server entries can be created, regardless of server type.

Active Directory

Microsoft Active Directory (AD) is a directory service for Windows domains that stores information about members of the domain, such as users and devices, and verifies their login credentials and controls their access privileges.

In Active Directory, objects are organized in a number of levels such as domains, trees and forests.

At the top of the structure is the forest. A forest is a collection of multiple trees that share a common global catalog, directory schema, logical structure, and directory configuration. In a multi-domain forest, each domain contains only those items that belong in that domain. Global Catalog servers provide a global list of all objects in a forest.

ZoneDirector support for Active Directory authentication includes the ability to query multiple Domain Controllers using Global Catalog searches. To enable this feature, you will need to enable Global Catalog support and enter an Admin DN (distinguished name) and password.

Depending on your network structure, you can configure ZoneDirector to authenticate users to an Active Directory server in one of the following ways:

- Active Directory for 802.1X
- Single Domain Active Directory Authentication for Web Portal
- Multi-Domain Active Directory Authentication for Web Portal

Active Directory for 802.1X

AD for 802.1X allows 802.1X authentication with a back-end Active Directory server.

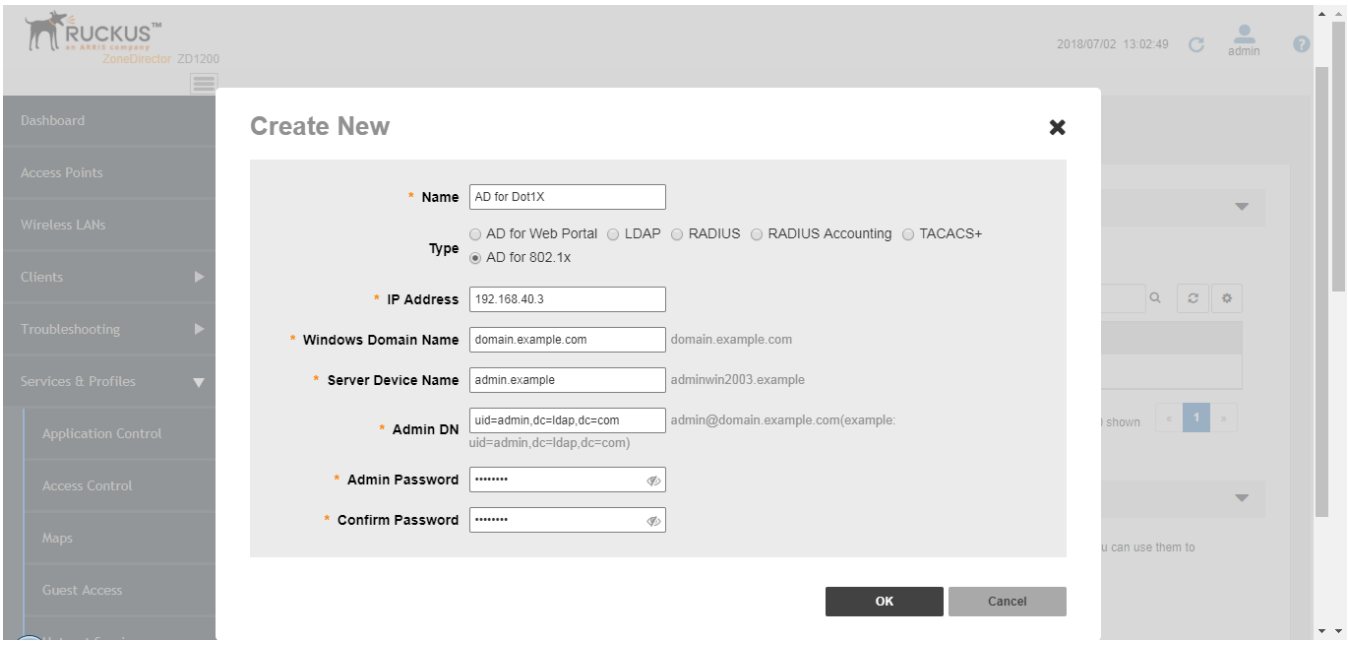
In this type of authentication, the client's login credentials pass from the AP to ZoneDirector (using MS-CHAPv2), then to a RADIUS server using 802.1X, and then to a back-end AD server for authentication.

To configure Active Directory for 802.1X:

1. Go to **Services & Profiles > AAA Servers**.
2. In *Authentication/Accounting Servers*, click **Create** to create a new AAA server entry.
3. In the *Create New* form, enter a **Name** for the AAA server.

4. In *Type*, select **AD for 802.1X**.
5. Enter the following AD server details according to your network configuration:
   - IP Address
   - Windows Domain Name
   - Server Device Name
   - Admin DN
   - Admin Password
   - Confirm Password
6. Click **OK** to save your changes. The new AAA server entry is added to the table.

FIGURE 193 Active Directory for 802.1X



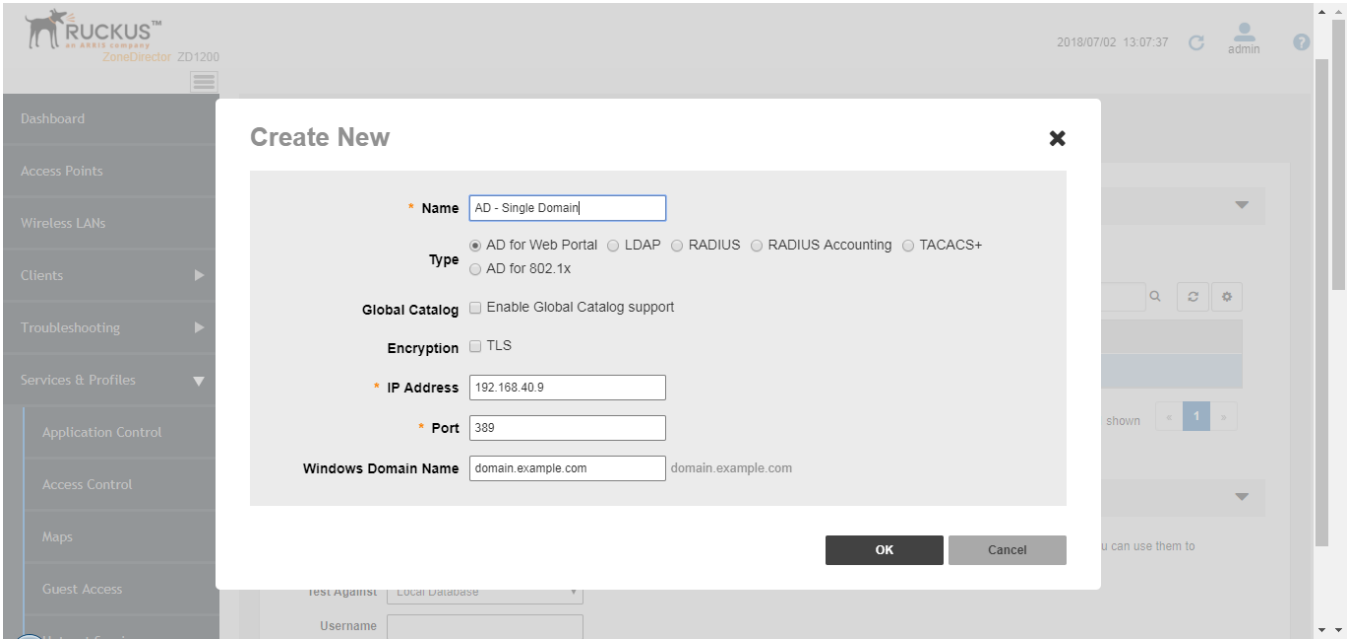
Single Domain Active Directory Authentication

To enable Active Directory authentication for a single domain:

1. Go to **Services & Profiles** > **AAA Servers**, and click **Create New** under **Authentication/Accounting Servers**. The **Create New** form appears.
2. In **Type**, Select **Active Directory**.
   - In Encryption, select Enable TLS encryption if you want to encrypt all authentication traffic between the client and the Active Directory server. The AD server must support TLS1.0/TLS1.1/TLS1.2.
3. Do not enable **Global Catalog** support.
4. Enter the **IP address** and **Port** of the AD server. 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.
5. Enter the **Windows Domain Name** (e.g., domain.ruckuswireless.com).

6. Click **OK**.

FIGURE 194 Enable Active Directory for a single domain



For single domain authentication, admin name and password are not required.

Multi-Domain Active Directory Authentication

For multi-domain AD authentication, an Admin account name and password must be entered so that ZoneDirector can query the Global Catalog.

To enable Active Directory authentication for multiple domains:

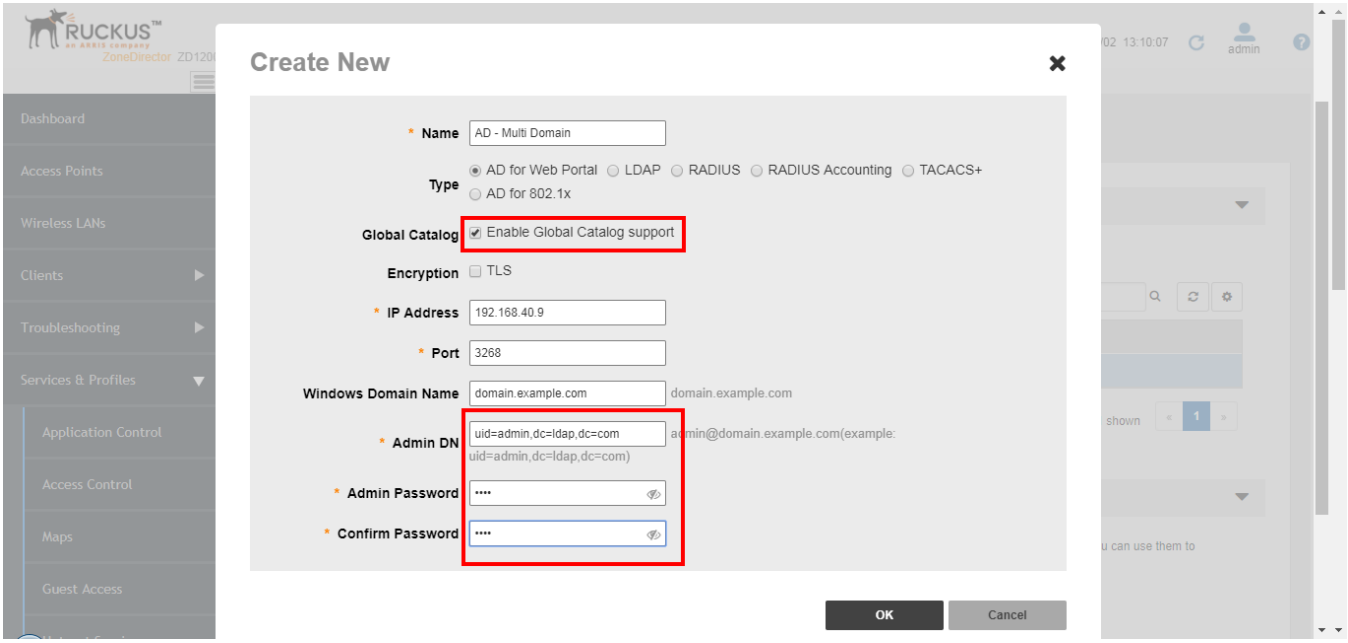
1. Go to **Services & Profiles** > **AAA Servers**, and click **Create New** under **Authentication/Accounting Servers**. The **Create New** form appears.
2. In **Type**, Select **Active Directory**
   - In Encryption, select Enable TLS encryption if you want to encrypt all authentication traffic between the client and the Active Directory server. The AD server must support TLS1.0/TLS1.1/TLS1.2.

     NOTE
     Note that Secure Active Directory requires the import of a root CA for TLS encryption. The import option is provided on the **Adminster** > **Certificate** > **Advanced Options** page.

3. Select the **Global Catalog** check box next to **Enable Global Catalog** support.
4. The default port changes to 3268, and the fields for Admin DN and password appear. The default port number (3268, or 636 if you have enabled TLS encryption) should not be changed unless you have configured your AD server to use a different port.
5. Leave the **Windows Domain Name** field empty to search all domains in the forest. Leave the **Windows Domain Name** field empty to search all domains in the forest.
6. Enter an **Admin DN** (distinguished name) in **Active Directory** format (name@xxx.yyy).
7. Enter the admin **Password**, and re-enter the same password for confirmation. The Admin account need not have write privileges, but must able to read and search all users in the database.

8. Click **OK** to save changes.
9. To test your authentication settings, see Testing Authentication Settings on page 264.

FIGURE 195 Active Directory with Global Catalog enabled



LDAP

In addition to Microsoft Active Directory, ZoneDirector supports several of the most commonly used LDAP servers, including:

- OpenLDAP
- Apple Open Directory
- Novell eDirectory
- Sun JES (limited support)

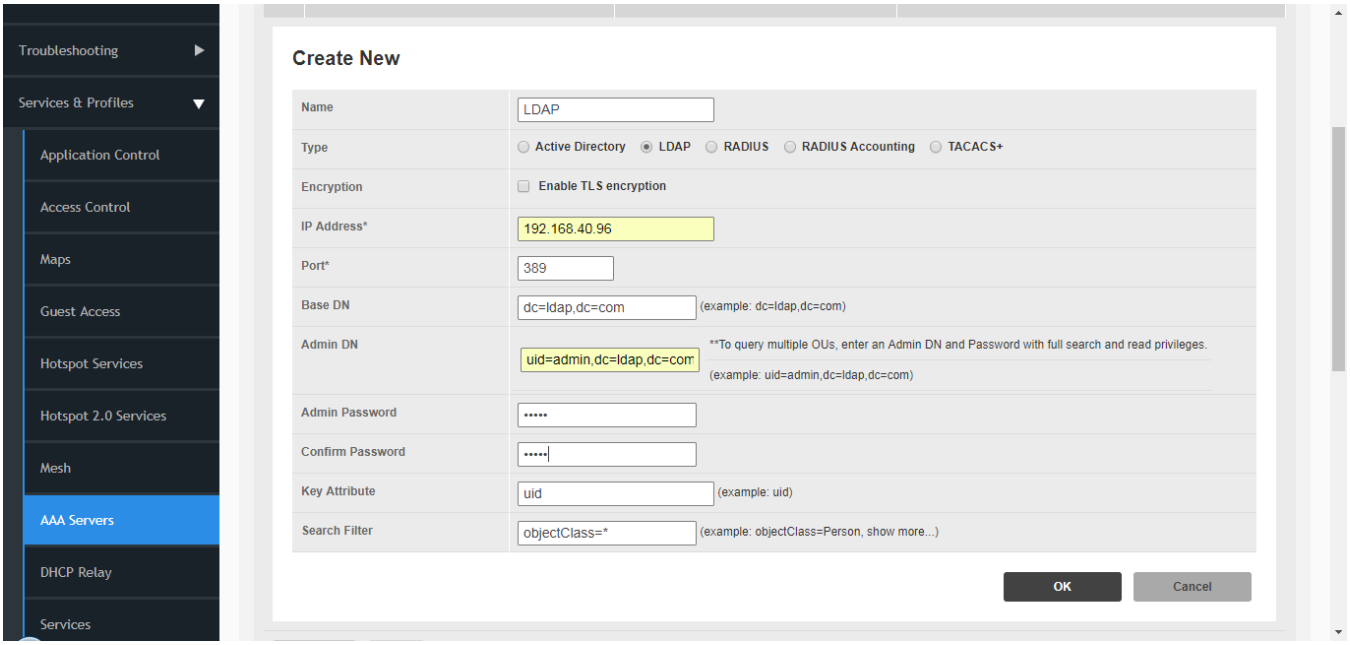
To configure an LDAP server for user authentication:

1. Go to **Services & Profiles** > **AAA Servers**, and click **Create New** under Authentication/Accounting Servers. The **Create New** form appears.
2. In **Type**, Select **LDAP**.
   - In Encryption, select Enable TLS encryption if you want to encrypt all LDAP authentication traffic between the LDAP client and the LDAP server. The LDAP server must support TLS1.0/TLS1.1/TLS1.2.

     NOTE
     Note that Secure LDAP requires the import of a root CA for TLS encryption. The import option is provided on the **Administer** > **Certificate** > **Advanced Options** page
3. Enter the **IP address** and **Port** of your LDAP server. The default port (389 for unencrypted, 636 for encrypted) should not be changed unless you have configured your LDAP server to use a different port.
4. Enter a **Base DN** in LDAP format for all user accounts.
5. Format: **cn=Users;dc=<Your Domain>,dc=com**

6. Enter an **Admin DN** in LDAP format. Format: **cn=Admin;dc=<Your Domain>,dc=com**
7. Enter the **Admin Password**, and reenter to confirm.
8. Enter a **Key Attribute** to denote users (default: uid).
9. Click **OK** to save your changes.
10. If you want to filter more specific settings, see Advanced LDAP Filtering on page 252. The Admin account need not have write privileges, but must able to read and search all users in the database.

FIGURE 196 Creating a new LDAP server object in ZoneDirector

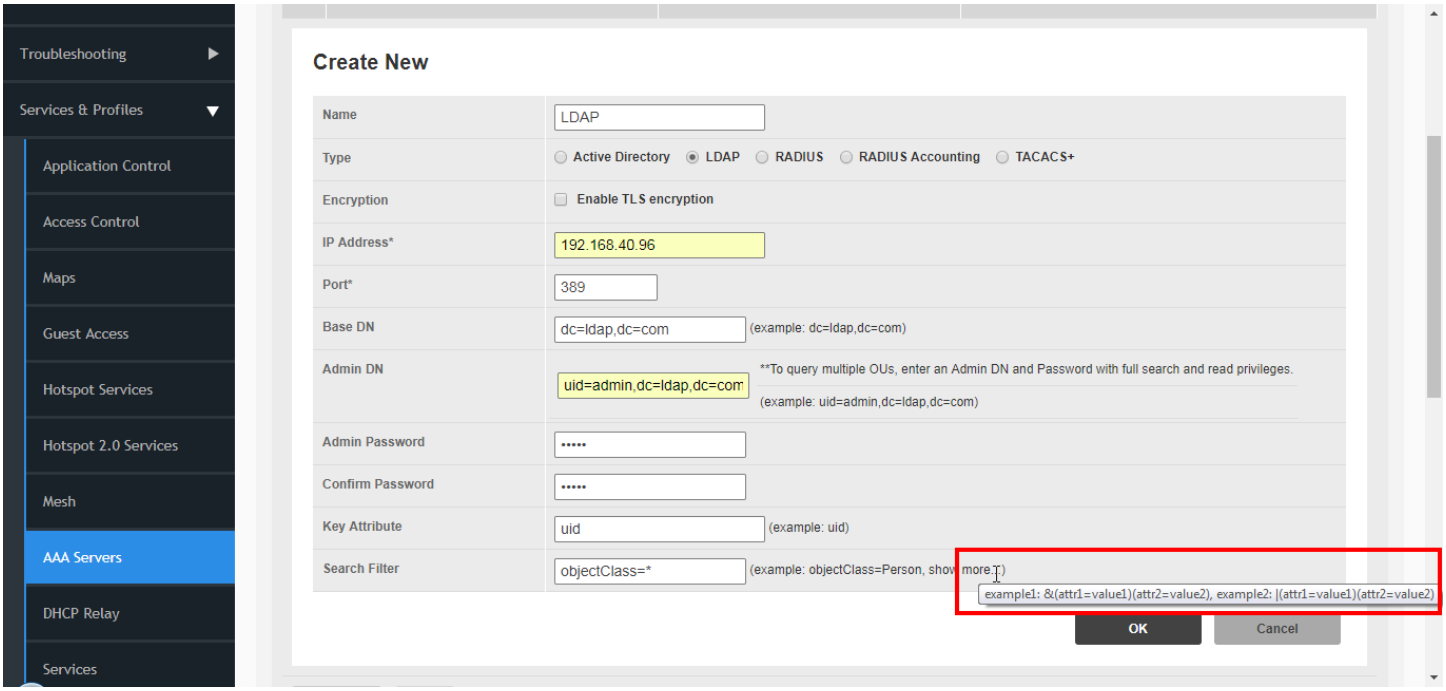


Advanced LDAP Filtering

A search string in LDAP format conforming to RFC 4515 can be used to limit search results. For example, objectClass=Person limits the search to those whose “objectClass” attribute is equal to “Person”.

More complicated examples are shown when you mouse over the “show more” section, as shown in the figure below.

FIGURE 197 LDAP search filter syntax examples



Group Extraction

By using the Search Filter, you can extract the groups to which a user belongs, as ZoneDirector to members of specific groups.

For example, in a school setting, if you want to assign members of the group “students” to a Student role, you can enter a known student’s name in the Test Authentication Settings section, click Test, and return the groups that the user belongs to. If everything is configured correctly, the result will display the groups associated with the student, which should include a group called “student” (or whatever was configured on your LDAP server).

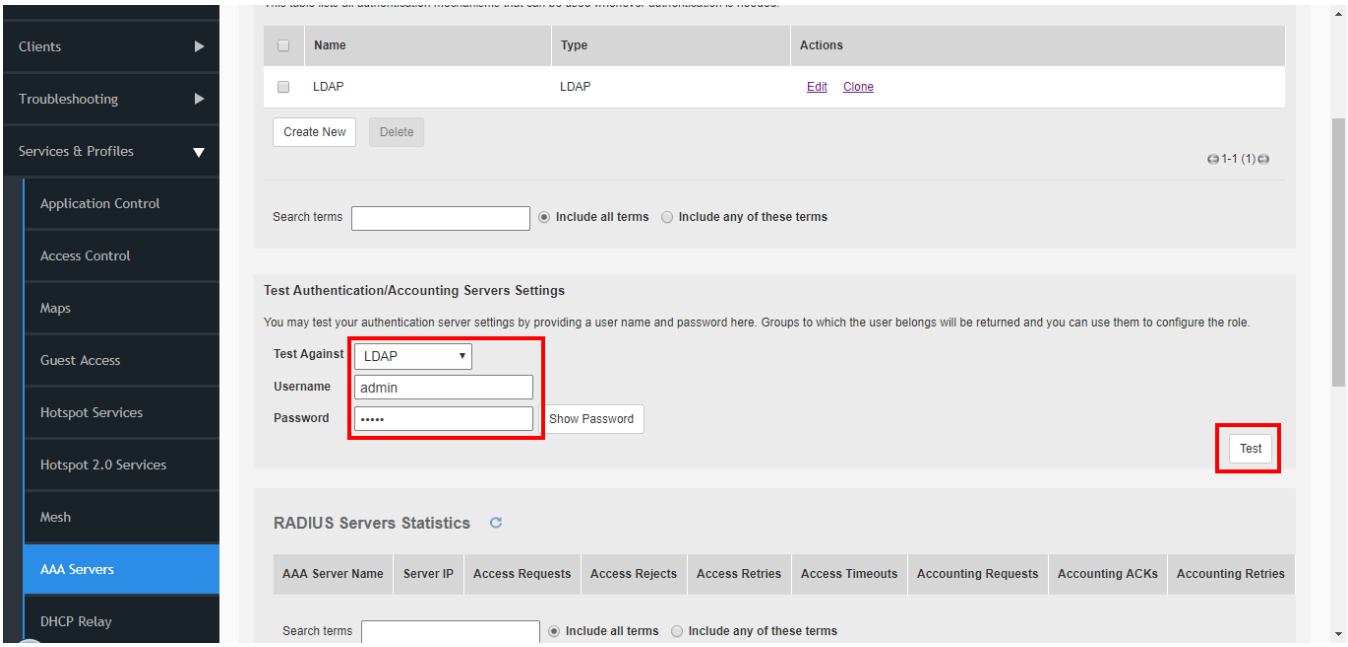
Next, go to the *Services & Profiles* > *Roles* page, create a Role named “Student,” and enter “student” in the Group Attributes field. Then you can select which WLANs you want this Role to have access to, and decide whether this Role should have Guest Pass generation privileges and ZoneDirector administration privileges. From here on, any user associated to the Group “student” will be given the same privileges when he/she is authenticated against your LDAP server.

To configure user roles based on LDAP group:

1. Go to **Services & Profiles** > **AAA Servers**.
2. In **Test Against**, select your LDAP server from the drop-down menu.
3. Enter the **User Name** and **Password** for a known member of the relevant group.
4. Click **Test**.

5. Note the Groups associated with this user.

FIGURE 198 Test authentication settings



6. Go to **Services & Profiles** > **Roles**, and create a Role based on this User Group (see Creating New User Roles on page 116).
   - Click the **Create New** link in the **Roles** section
   - In the **Group Attributes** field, enter Group attributes exactly as they were returned from the **Test Authentication Settings** dialog.
   - Specify WLAN access, Guest Pass generation and ZoneDirector administration privileges as desired for this Role.

At this point, any user who logs in and is authenticated against your LDAP server with the same Group credentials will automatically be assigned to this Role.

RADIUS /RADIUS Accounting

Remote Authentication Dial In User Service (RADIUS) user authentication requires that ZoneDirector know the IP address, port number and Shared Secret of the RADIUS/RADIUS Accounting server.

When an external RADIUS/RADIUS Accounting server is used for authentication or accounting, user credentials can be entered as a standard username/password combination, or client devices can be limited by MAC address. If using MAC address as the authentication method, you must enter the MAC addresses of each client on the AAA server, and any clients attempting to access your WLAN with a MAC address not listed will be denied access.

A RADIUS/RADIUS Accounting server can be used with 802.1X, MAC authentication, Web Authentication (Captive Portal) and Hotspot WLAN types. To configure a RADIUS/RADIUS Accounting server entry in ZoneDirector:

1. Go to **Services & Profiles** > **AAA Servers**.
2. Click the **Create New** link under Authentication/Accounting Servers.

3. Select **Radius** or **Radius Accounting** for the AAA server type.
   - If you want to enable encryption of RADIUS packets using Transport Layer Security (TLS), select the TLS check box next to Encryption. This allows RADIUS authentication and accounting data to be passed safely across insecure networks such as the Internet.

     NOTE
     Note that Secure RADIUS requires the import of a root CA for TLS encryption. The RADIUS or RADIUS Accounting server must support TLS1.1/TLS1.2. The import option is provided on the **Administer** > **Certificate** > **Advanced Options** page.

4. Choose **PAP** or **CHAP** according to the authentication protocol used by your RADIUS server.
5. Enter the **IP Address**, **Port** number and **Shared Secret**.
6. Click **OK** to save changes.

Configuring a Backup RADIUS/RADIUS Accounting Server

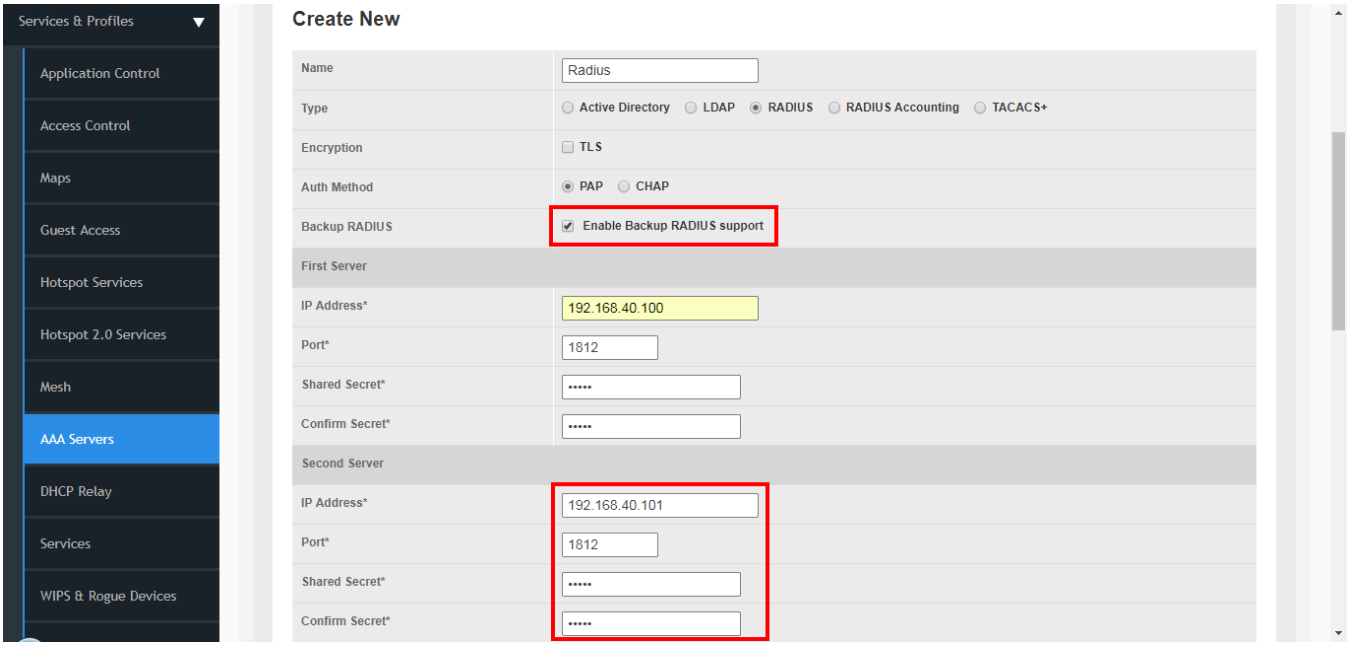
If a backup RADIUS or RADIUS Accounting server is available, enable the check box next to Backup RADIUS and additional fields appear. Enter the relevant information for the backup server and click **OK**. When you have configured both a primary and backup RADIUS server, an additional option will be available in the **Test Authentication Settings** .

To configure a backup RADIUS / RADIUS Accounting server:

1. Click the check box next to **Enable Backup RADIUS** support.
2. Enter the **IP Address**, **Port** number and **Shared Secret** for the backup server (these fields can neither be left empty nor be the same values as those of the primary server).
3. In **Request Timeout**, enter the timeout period (in seconds) after which an expected RADIUS response message is considered to have failed.
4. In **Max Number of Retries**, enter the number of failed connection attempts after which ZoneDirector will failover to the backup RADIUS server.
5. In **Max Number of Consecutive Drop Packets**, enter a value from 1-10 consecutive dropped packets, after which ZoneDirector will failover to the backup RADIUS server.

6. In **Reconnect Primary**, enter the number of minutes after which ZoneDirector will attempt to reconnect to the primary RADIUS server after failover to the backup server

FIGURE 199 Enable backup RADIUS server



MAC Authentication with an External RADIUS Server

To begin using MAC authentication:

1. Ensure that a RADIUS server is configured in ZoneDirector (**Services & Profiles** > **AAA Servers** > **RADIUS Server**). See Using an External AAA Server on page 248.
2. Create a user on the RADIUS server using the MAC address of the client as both the user name and password. The MAC address format can be configured in one of the following formats:
   - A single string of characters without punctuation: aabbccddeeff
   - Colon separated: aa:bb:cc:dd:ee:ff
   - Hyphen separated: aa-bb-cc-dd-ee-ff
   - All caps: AABBCCDDEEFF
   - All caps hyphenated: AA-BB-CC-DD-EE-FF
   - All caps colon separated: AA:BB:CC:DD:EE:FF
3. Log in to the ZoneDirector web interface, and go to **Wireless LANs**.
4. Click the **Edit** link next to the WLAN you would like to configure.
5. Under **Authentication Options: Method** , select **MAC Address**
6. Under **Authentication Server**, select your RADIUS Server.
7. Select the **MAC Address Format** according to your RADIUS server's requirements.
8. Click **OK** to save your changes

You have completed configuring the WLAN to authenticate users by MAC address from a RADIUS server.

Using 802.1X EAP + MAC Address Authentication

With the 802.1X EAP + MAC address authentication method, the clients configured with either the open or the EAP-MD5 authentication methods are both supported on the same WLAN, where the encryption method is limited to none and an external RADIUS server is required.

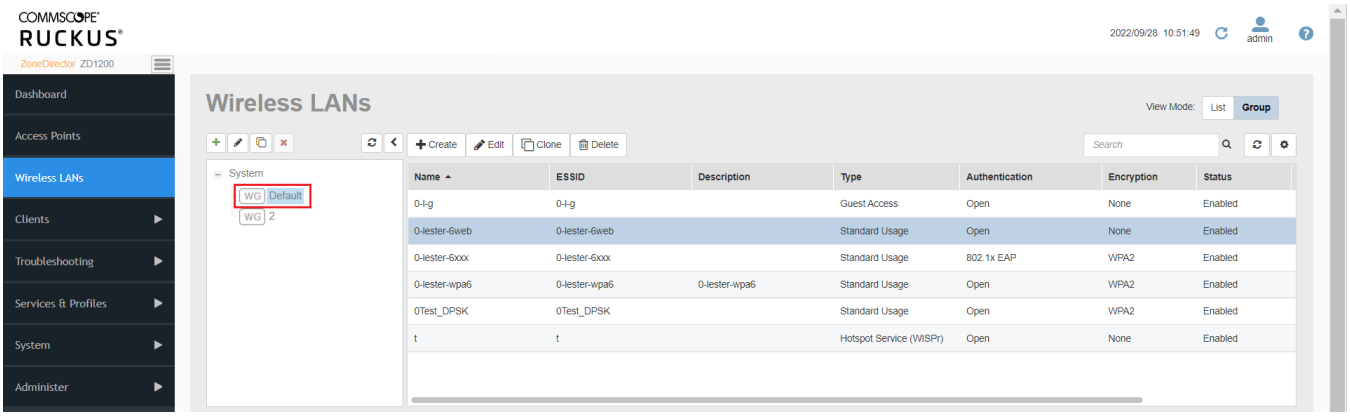
> **NOTE**
> The 802.1X EAP + MAC address authentication method works only if you have a supplicant that supports this behavior (and currently no known public domain supplicants support this behavior).

Complete the following steps to configure a WLAN for 802.1X EAP MAC authentication.

1. Go to **Wireless LANs** and select a WLAN group from the left pane.

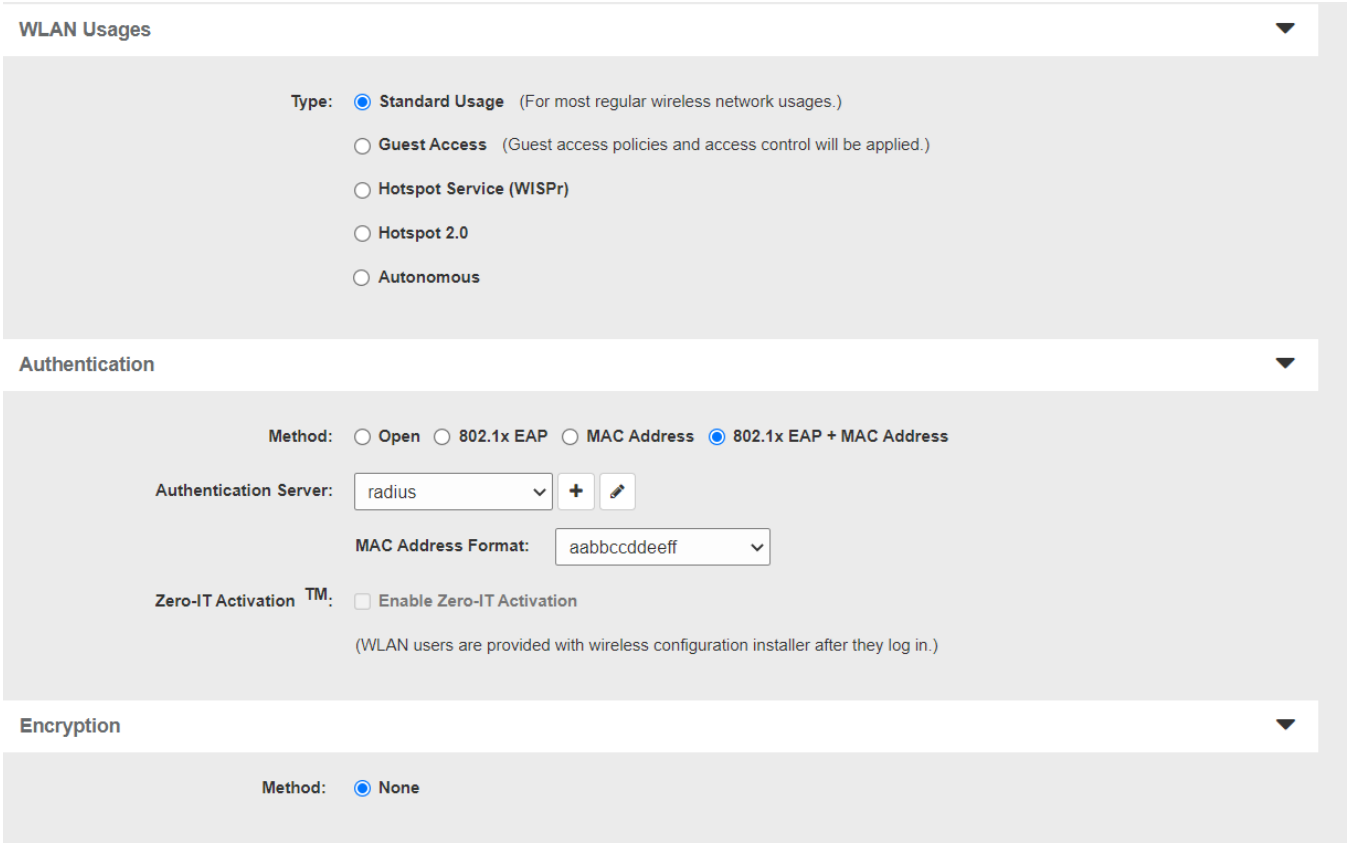
   The WLAN table displays all the WLANs created in that group in ZoneDirector.

   FIGURE 200 Configuring a WLAN



2. Select the WLAN that you want to configure and click **Edit** (or click **Create** to create a new WLAN, refer to Creating a Wireless LAN on page 65).
3. Under **WLAN Usages**, for **Type**, select **Standard Usage**.
4. Under **Authentication**, for **Method**, select **802.1X EAP + MAC Address**.

FIGURE 201 Configuring a WLAN Using the 802.1X EAP MAC Address Authentication Method



5. For **Authentication Server**, select a previously configured external RADIUS server (**Services & Profiles** > **AAA Servers**). Alternatively, click the **Create New (+)** icon to create a new AAA server object from within the WLAN configuration window.
6. Under **Encryption**, for **Method**, select **None**.
7. Click **OK** to save your changes.

When ZoneDirector authenticates a client, MAC authentication is checked first followed by the EAP authentication process. When the client tries to associate, if MAC authentication succeeds, the client is authorized directly and allowed to pass traffic without any further EAP authentication required.

If MAC authentication fails, the EAP authentication process begins and the client must provide a valid EAP account before access is granted.

You can view the actual authentication method used (MAC address or EAP) from the **Clients > Wireless Clients** page.

Using 802.1X with EAP-MD5

EAP-MD5 differs from other EAP methods in that it only provides authentication of the EAP peer to the EAP server but not mutual authentication. ZoneDirector supports 802.1X authentication with EAP-MD5 using either ZoneDirector's internal database or an external RADIUS server.

To configure a WLAN for EAP-MD5 authentication:

1. Go to **Wireless LANs** and click the **Configure** icon for the WLAN you would like to configure.
2. Under **Authentication Options: Method**, select **802.1X EAP**
3. Under **Encryption Options: Method**, select **None**

4. Under **Authentication Server**, select either **Local Database** or a previously configured RADIUS server from the list.
5. Click **OK** to save your changes.

RADIUS Attributes

Ruckus products communicate with an external RADIUS server as a RADIUS client. Packets from Ruckus products are called "access-request" or "accounting-request" messages. The RADIUS server, in turn, sends an "access-challenge", "access-accept" or "access-reject" message in response to an access-request, and an "accounting-response" message in response to an accounting-request.

RADIUS Attribute Value Pairs (AVP) carry data in both the request and the response messages. The RADIUS protocol also allows vendor specific attributes (VSA) to extend the functionality of the protocol. The following tables list the RADIUS attributes used in these messages between ZoneDirector and the RADIUS/RADIUS Accounting server based on which type of authentication is used for the WLAN.

ZoneDirector will terminate a user session if it receives a Change of Authorization-Disconnect Message (COA-DM) from the RADIUS server. The COA-DM message may be used when a client changes service levels. For instance, a new user may initially connect to a free, low-rate service on one WLAN. When they purchase access on a higher-rate service, RADIUS will send a COA-DM message to ZoneDirector, causing the user to re-connect to an alternative WLAN. COA-DM may also be used to remove a client if a user exceeds their total bandwidth allowance or time on the network.

NOTE
In addition to COA-DM messages, as of release 10.0, ZoneDirector also supports the following COA messages:

- Idle timeout
- Session Timeout
- Accounting interval
- Uplink rate limit
- Downlink rate limit
- Filter ID (ACL ID)

Notation "==>" below indicates this value is generated external to AP/ZoneDirector.

- In the case of EAP payload, this is generated by a wireless client and encapsulated in the RADIUS access-request packet.
- In the case of a "state" attribute, it indicates that an access-request packet is a response to the last received access-challenge packet by copying the "state" AVP unmodified.
- As for the "class" attribute, it is parsed and stored from an access-accept packet and then subsequently used in accounting-request packets.

RADIUS Authentication attributes

TABLE 22 RADIUS attributes used in authentication

WLAN Type	Attributes
802.1X / MAC Auth	Sent from ZoneDirector in Access Request messages: (1) User name (4) NAS IP Address (optional; prefer sending NAS ID) (5) NAS Port (6) Service Type: hard-coded to be Framed-User(2) (12) Framed MTU: hard-coded to be 1400 (30) Called Station ID: user configurable (31) Calling Station ID: format is sta's mac (32) NAS Identifier: user configurable (61) NAS Port Type: hard-coded to be 802.11 port (19) (77) Connection Info: indicates client radio type ==> (79) EAP payload ==> (24) State: if radius access-challenge in last received radius msg from AAA (80) Message Authenticator (95) NAS IPv6 address (if using/talking to an IPv6 RADIUS server) Ruckus private attribute: Vendor ID: 25053 Vendor Type / Attribute Number: 3 (Ruckus-SSID) Sent from RADIUS server in Access Accept messages: (1) User name (7) WISPr Bandwidth-Max-Up: Maximum transmit rate (bits/second) (8) WISPr Bandwidth-Max-Down: Maximum receive rate (bits/second) (25) Class (27) Session-timeout & (29) Termination-action: Session-timeout event becomes a disconnect event or re-authentication event if termination-action indicates "(1) radius-request" (85) Acct-interim-interval For Dynamic VLAN application: (64) Tunnel-Type: value only relevant if it is (13) VLAN (65) Tunnel-Medium-Type: value only relevant if it is (6) 802 (as in all 802 media plus ethernet) (81) Tunnel-Private-Group-ID: this is the VLAN ID assignment (per RFC, this is between 1 and 4094) Administrator Authentication: Ruckus private attribute: Vendor ID: 25053 Vendor Type / Attribute Number: 1 (Ruckus-User-Groups) Value Format: group_attr1, group_attr2, group_attr3, ... Cisco private attribute: Vendor ID: 9 Vendor Type/ Attribute Number: 1 (Cisco-AVPair) Value Format: shell:roles="group_attr1 group_attr2 group_attr3 ..."
WISPr / Web Auth / Guest	Additional attributes supported in WISPr WLANs (**generic attributes NOT the same as non-WISPr/802.1X): (1) User name (2) Password or (3) CHAP-Password (4) NAS IP Address (6) Service Type: hardcoded to be Framed-User(2) (8) Framed IP address (30) Called Station ID: user configurable (31) Calling Station ID: format is sta's mac (32) NAS Identifier: user configurable (44) Account session ID Ruckus private attribute: Vendor ID: 25053 Vendor Type / Attribute Number: 3 (Ruckus-SSID) WISPr vendor specific attribute (vendor id = 14122) (1) WISPr location id (2) WISPr location name (4) WISPr redirection URL (7) WISPr Bandwidth-Max-Up: Maximum transmit rate (bits/second) (8) WISPr Bandwidth-Max-Down: Maximum receive rate (bits/second) (80) Message Authenticator

RADIUS Accounting attributes

The following table lists attributes used in RADIUS accounting messages.

TABLE 23 RADIUS attributes used in Accounting

WLAN Type	Attribute
802.1X / MAC Auth	Common to Start, Interim Update, and Stop messages: (1) User Name (4) NAS IP Address (5) NAS Port (8) Framed IP (30) Called Station ID: user configurable (31) Calling Station ID: format is sta's mac (32) NAS Identifier: user configurable (40) Status Type: start, stop, interim-update (45) Authentic: radius-auth (1) (50) Acct-Multi-Session-ID (61) NAS Port Type: hard-coded to be 802.11 port (19) (77) Connection Info: indicates client radio type ==> (25) Class: if received in radius-accept message from AAA Ruckus private attribute: Vendor ID: 25053 Vendor Type / Attribute Number: 3 (Ruckus-SSID)

TABLE 23 RADIUS attributes used in Accounting (continued)

WLAN Type	Attribute
802.1X / MAC Auth	Specific to Interim Update and Stop messages: (8) Ruckus private attribute: Vendor ID: 25053 Vendor Type / Attribute Number: 2 (Ruckus-Sta-RSSI) (42) Input Octets (43) Output Octets (44) Session ID (46) Session Time (47) Input Packets (48) Output Packets (52) Input Gigawords (only appears when received bytes > 4 GB) (53) Output Gigawords (only appears when transmitted bytes > 4 GB) (55) Event Timestamp Specific to Stop messages: (49) Terminate Cause: user-request, lost-carrier, lost-service, session-timeout, admin-reset, admin-reboot, supplicant-restart, idle timeout
802.1X / MAC Auth	Sent from RADIUS server in Accept messages: (1) User name (25) Class (85) Acct-interim-interval (27) Session-timeout & (29) Termination-action: Session-timeout event becomes a disconnect event or re-authentication event if termination-action indicates "(1) radius-request" For Dynamic VLAN application: (64) Tunnel-Type: value only relevant if it is (13) VLAN (65) Tunnel-Medium-Type: value only relevant if it is (6) 802 (as in all 802 media plus Ethernet) (81) Tunnel-Private-Group-ID: this is the VLAN ID assignment (per RFC, this is between 1 and 4094)
WISPr / Web Auth / Guest Access	Common to Start, Interim Update, and Stop messages: (1) User name (2) Password (4) NAS IP address (5) NAS port (8) Framed-IP (30) Called station ID: user configurable (31) Calling station ID (32) NAS Identifier: user configurable (45) Acct authentic (50) Acct-Multi-Session-Id (61) NAS port type (77) Connection Info: indicates client radio type Ruckus private attribute: Vendor ID: 25053 Vendor Type / Attribute Number: 3 (Ruckus-SSID) Additional attributes supported in WISPr WLANs: WISPr vendor specific attributes (vendor id = 14122) (1) WISPr location id (2) WISPr location name (4) WISPr redirection URL (7) WISPr Bandwidth-Max-Up: Maximum transmit rate (bits/second) (8) WISPr Bandwidth-Max-Down: Maximum receive rate (bits/second) Specific to Interim Update and Stop messages: (42) Acct input octets (43) Acct output octets(44) Acct session ID (46) Acct session time (47) Acct input packets (48) Acct output packets (52) Acct input giga words (53) Acct output giga words Ruckus private attribute: Vendor ID: 25053 Vendor Type / Attribute Number: 2 (Ruckus-Sta-RSSI) Additional attributes supported in WISPr WLANs: WISPr vendor specific attributes (vendor id = 14122) (1) WISPr location id (2) WISPr location name

Configuring Microsoft IAS for PAP Authentication

If you are using Microsoft Internet Authentication Service (IAS) as your RADIUS server and PAP authentication, you will need to configure your user/group profiles to use only PAP authentication rather than the default (MS-CHAP). If you selected CHAP under “RADIUS / RADIUS Accounting”, you do not need to configure IAS for PAP authentication.

To configure user/group profiles for PAP authentication:

1. From the **Internet Authentication Service** main page, select the user or group for which you want to configure PAP authentication.
2. Right-click the user or group and select **Properties** to open the [user/group name] **Properties** dialog box.
3. In the **Properties** dialog box, click **Edit Profile....** The **Edit Dial-in Profile** dialog box opens.
4. Click the **Authentication** tab at the top of the screen.
5. Select **Unencrypted authentication (PAP, SPAP)**.
6. Click **OK**.

7. Repeat this procedure for additional users or groups.

FIGURE 202 On the Microsoft IAS page, right-click the user/group and select Properties.

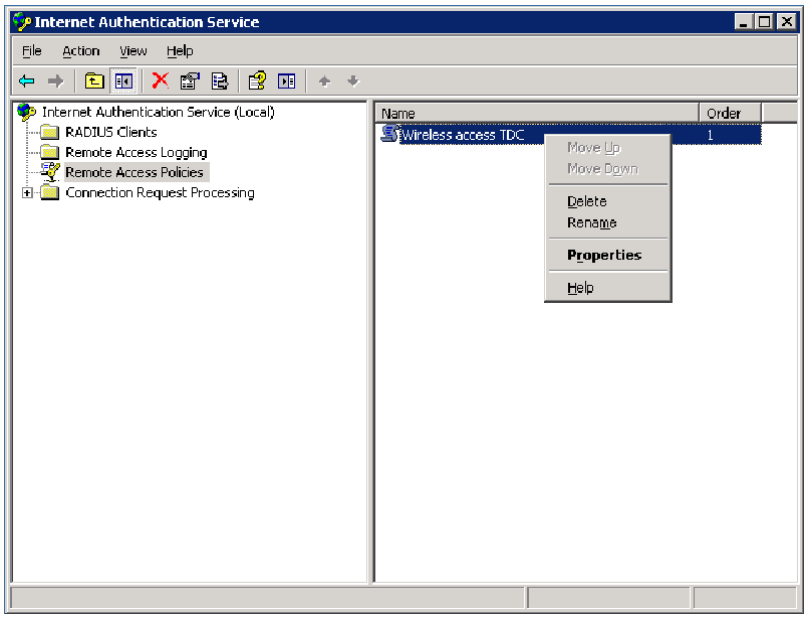


FIGURE 203 On the Properties page, click Edit Profile...

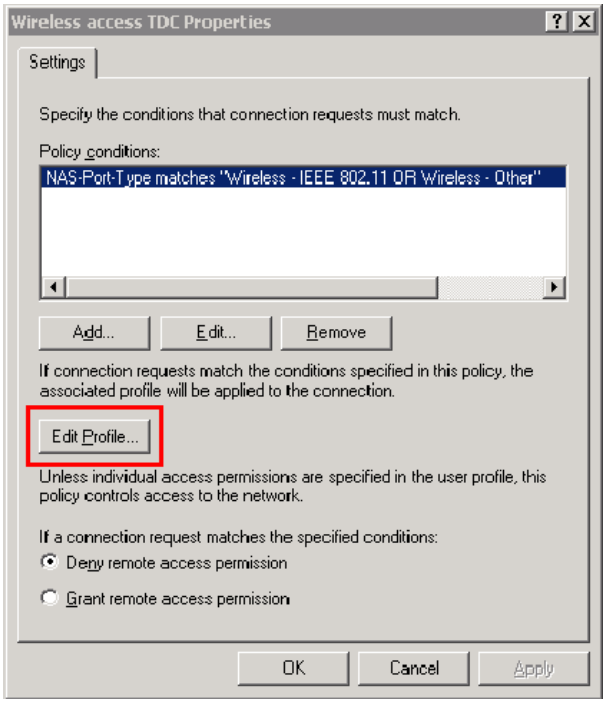
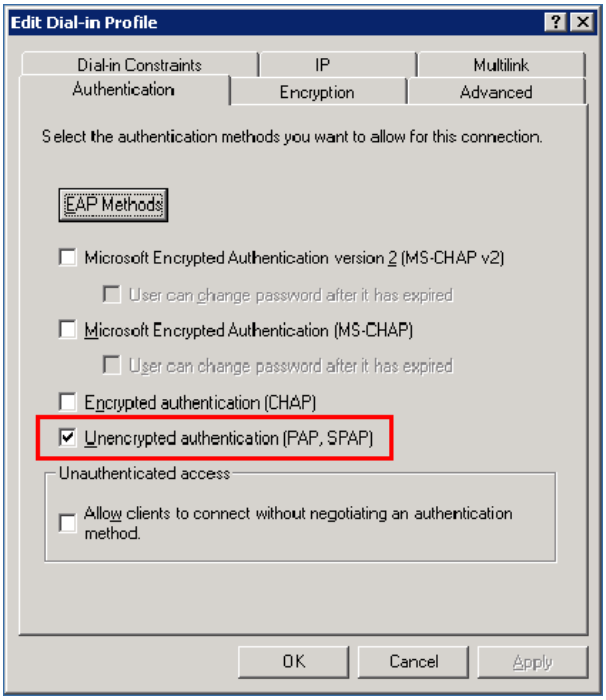


FIGURE 204 On the Authentication tab of the Edit Dial-in Profile dialog, select Unencrypted authentication (PAP, SPAP)



You have completed configuring Microsoft IAS for PAP authentication.

TACACS+

Terminal Access Controller Access-Control System Plus (TACACS+) is an Authentication, Authorization and Accounting protocol used to authenticate ZoneDirector administrators.

ZoneDirector admins can be assigned any of the same three administration privilege levels that can be set manually on the **Services & Profiles** > **Roles** page:

- Super Admin (Perform all configuration and management tasks)
- Operator Admin (Change settings affecting single AP's only)
- Monitoring Admin (Monitoring and viewing operation status only)

TACACS+ is an extensible AAA protocol that provides customization and future development features, and uses TCP to ensure reliable delivery. The daemon should listen at port 49 which is the "login" port assigned for the TACACS protocol. To authenticate ZoneDirector admins using a TACACS+ AAA server:

1. Go to **Services & Profiles** > **AAA Servers**
2. In **Authentication/Accounting Servers**, click **Create New**
3. Enter a **Name** for the TACACS+ server, and select **TACACS+** for Type.
4. Enter the server's **IP address** and do not change the **Port** setting from the default port 49 (in general).
5. In TACACS+ Service, enter a string of up to 64 characters. This name must match the name of the service configuration table on the TACACS+ server. Click **OK** to save your changes.

Once your TACACS+ server is configured on the AAA Servers page, you can select it from the list of servers used to authenticate ZoneDirector administrators on the **Administer** > **Preferences** page.

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 ZoneDirector.

After you have configured one or more authentication servers in ZoneDirector, perform this task to ensure that ZoneDirector can connect to the authentication server and retrieve the groups/attributes that you have configured for each user account. If testing against a RADIUS server, this feature uses PAP or CHAP depending on the RADIUS server configuration and the choice you made in “RADIUS / RADIUS Accounting” above. Make sure that either PAP or CHAP is enabled on the Remote Access Policy (assuming Microsoft IAS as the RADIUS server) before continuing with testing authentication settings.

1. On the **Services & Profiles > AAA Servers** page, locate the **Test Authentication Settings** section.
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, LDAP or RADIUS user name and password.
4. Click **Test**. If ZoneDirector 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 ZoneDirector 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 three 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
   - Search filter syntax invalid (LDAP only)

These results can be used to troubleshoot the reasons for failure to authenticate users from an AAA server through ZoneDirector.

> **NOTE**
> If you choose CHAP as the auth method when setting up an AAA server, this test feature will fail as the CHAP verification requires reversible encryption to be enabled for storing user passwords. Reversible encryption can be enabled in two different ways in Active Directory: 1) at the user level and 2) at the group level. Refer to your Active Directory documentation for instructions on enabling reversible encryption if you encounter this issue.

Services

Self Healing

ZoneDirector has the capability to perform automatic network adjustments to enhance performance and improve coverage by dynamically modifying power output and channel selection.

These features are called "Self Healing."

Automatically Adjust AP Power

ZoneDirector provides an option 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:

1. The power is set to Auto in the AP configuration.
2. The AP can hear another AP that is on the same channel and same ZoneDirector.

3. The AP can hear the other AP at a minimum of 50dB which means the Access Points are very close to each other.

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 sub-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.

Automatic Channel Selection

ZoneDirector offers two methods of automatic channel selection for spectrum utilization and performance optimization:

- Background Scanning on page 265
- ChannelFly on page 267

While Background Scanning must be enabled for rogue AP detection, AP location detection and radio power adjustment, either can be used for automatic channel optimization.

Background Scanning

Using Background Scanning, ZoneDirector regularly samples the activity in all Access Points to assess RF usage, to detect rogue APs and to determine which APs are near each other for mesh optimization.

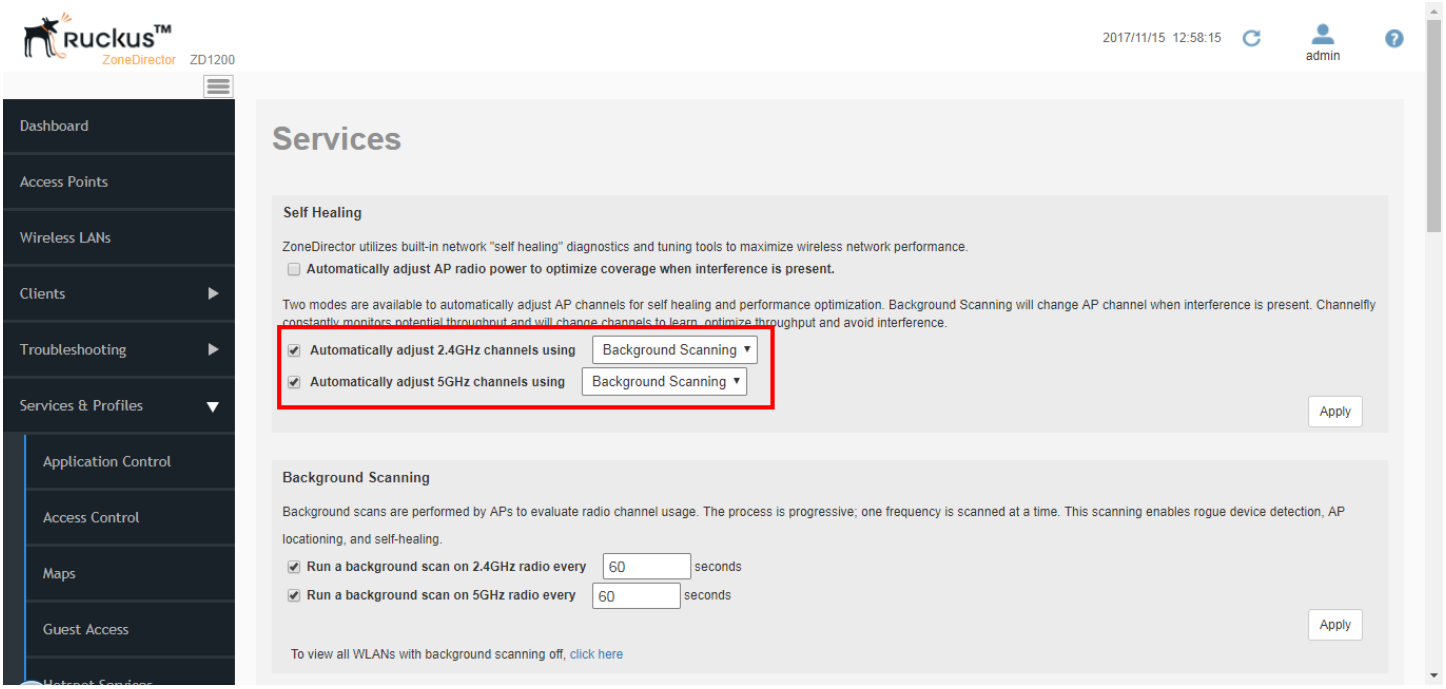
These scans sample one channel at a time in each AP so as not to interfere with network use. This information is then applied in AP Monitoring and other ZoneDirector monitoring features. You can, if you prefer, customize the automatic scanning of RF activity, deactivate it if you feel it's not helpful, or adjust the frequency, if you want scans at greater or fewer intervals.

> **NOTE**
> Background Scanning must be enabled for ZoneDirector to detect rogue APs on the network.

Background Scanning can be configured independently for the 2.4 and 5 GHz radios. Additionally, you can configure the frequency at which scans are run.

- **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.

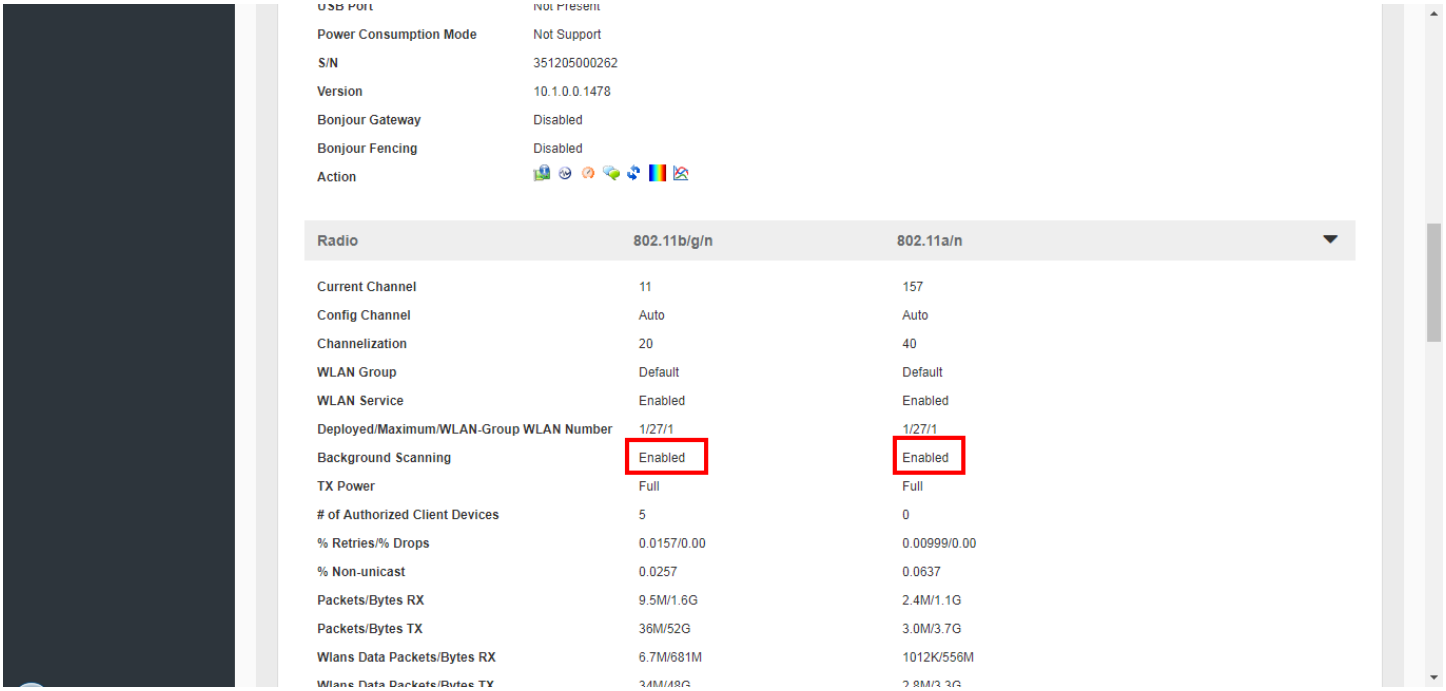
FIGURE 205 Background Scanning options



You can also disable Background Scanning on a per-WLAN basis from the **Wireless LANS** page. To disable scanning for a particular WLAN, click the **Edit** button for the WLAN for which you want to disable scanning, open **Advanced Options**, and click the check box next to **Disable Background Scanning**.

To see whether Background Scanning is enabled or disabled for a particular AP, go to **Access Points**, and select the AP from the list. Scroll down to the *General* > *Radio* section. The access point detail screen displays the Background Scanning status for each radio.

FIGURE 206 Viewing whether Background Scanning is enabled for an AP



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

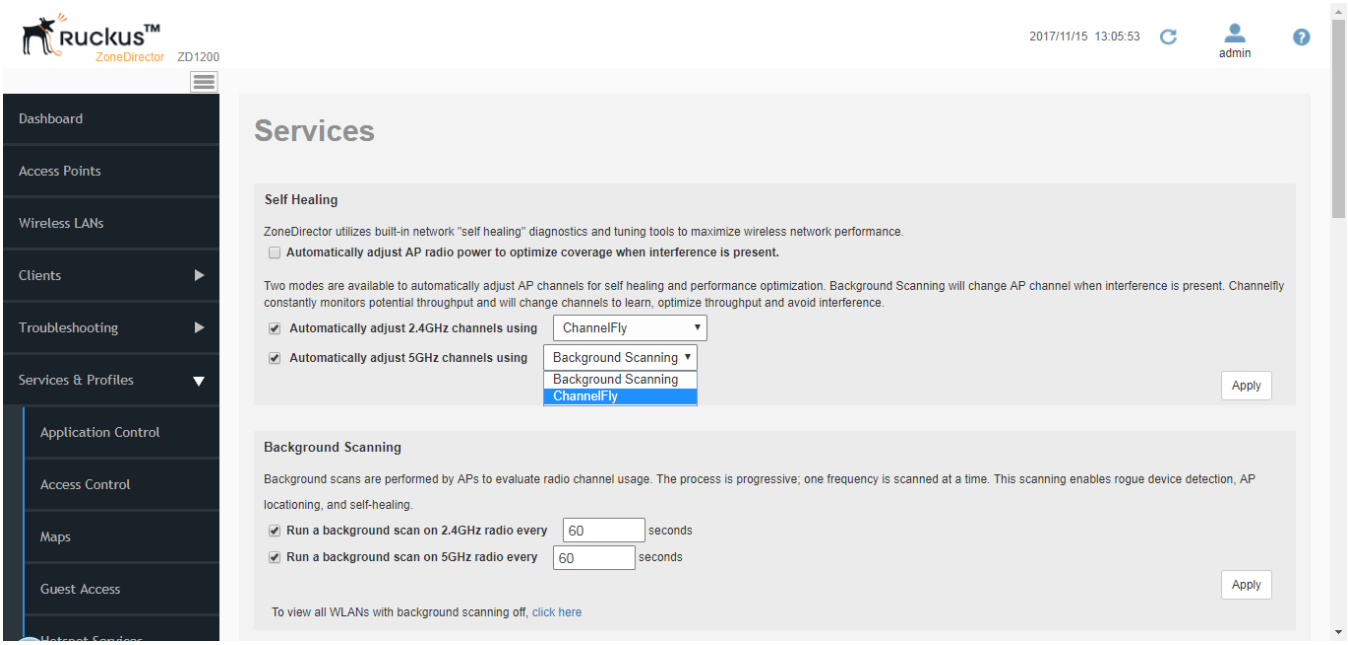
Compared to Background Scanning, ChannelFly takes considerably longer for the network to settle down. If you will be adding and removing APs to your network frequently, Background Scanning may be preferable. Additionally, if you have clients that do not support the 802.11h standard, ChannelFly may cause significant 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.

To configure the self healing options:

1. Go to **Services & Profiles** > **Services**
2. Review and change the following self-healing options:
   - **Automatically adjust AP radio power to optimize coverage where interference is present**: Enable automatic radio power adjustment based on Background Scanning
   - Automatically adjust 2.4 GHz channels using
     - Background Scanning
     - ChannelFly
   - Automatically adjust 5 GHz channels using
     - Background Scanning
     - ChannelFly
3. Click the **Apply** button in the same section to save your changes.

FIGURE 207 Enabling ChannelFly



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 ZoneDirector's web interface to balance the number of clients per radio on adjacent APs. "Adjacent APs" are determined by ZoneDirector at startup by measuring the RSSI during channel scans. After startup, ZoneDirector 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, ZoneDirector immediately updates the list of adjacent radios and refreshes the client limits at each affected AP.

Once ZoneDirector 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.

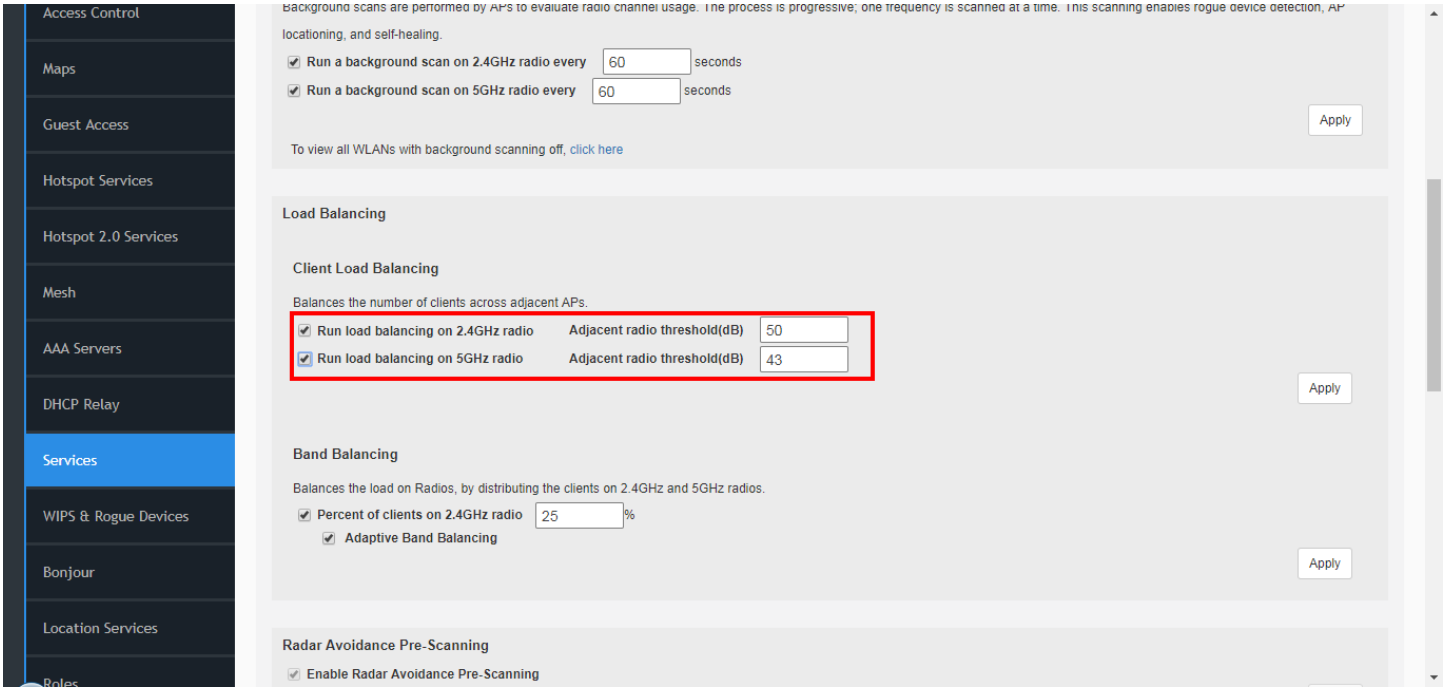
Key points on load balancing:

- These rules apply only to client devices; the AP always responds to another AP that is attempting to set up or maintain a mesh network.
- 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 and ZoneDirector.
- 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.

To enable Load Balancing globally:

1. Go to **Services & Profiles** > **Services**.
2. In **Load Balancing**, choose to perform load balancing on either the 2.4 or 5 GHz radio.
3. Enter Adjacent Radio Threshold (in dB), and click **Apply**.

FIGURE 208 Enable Load Balancing globally

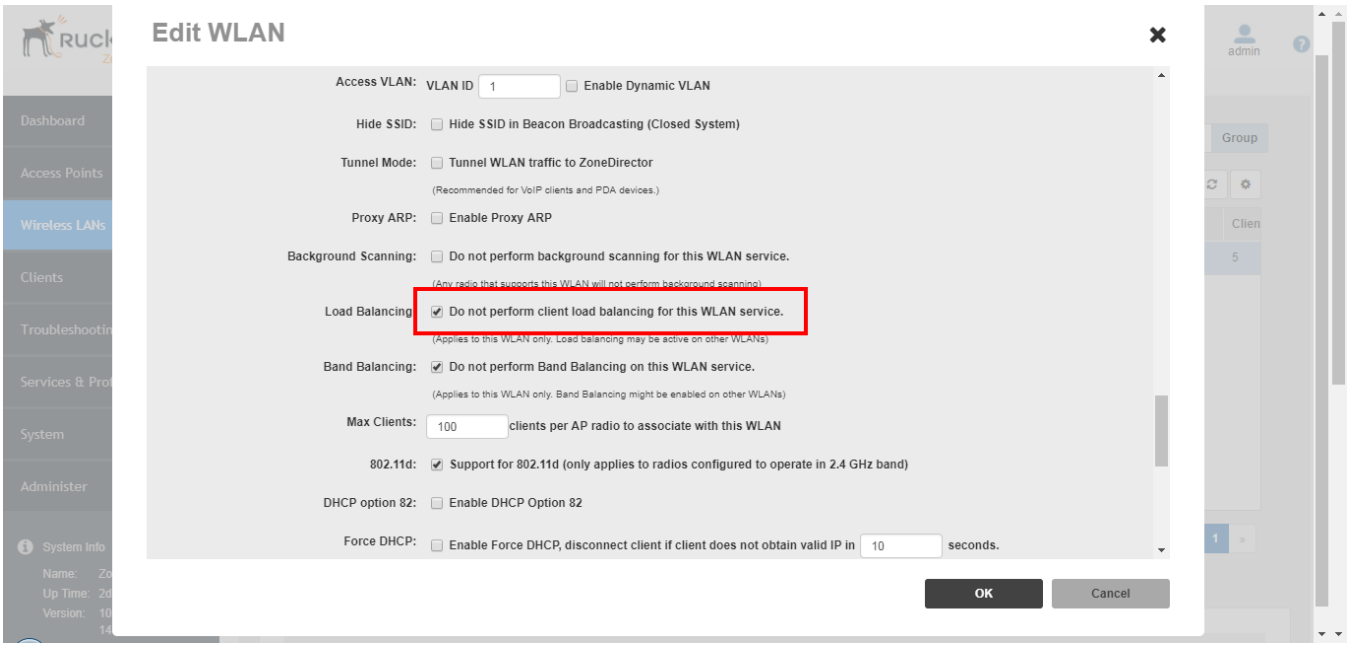


To disable Load Balancing on a per-WLAN basis

1. Go to **Wireless LANs**.
2. Click the **Edit** link for the WLAN for which you want to disable load balancing.
3. Click the **Advanced Options** link to expand the options.

4. Select **Do not perform load balancing for this WLAN service** next to **Load Balancing**.

FIGURE 209 Disable Load Balancing for a WLAN

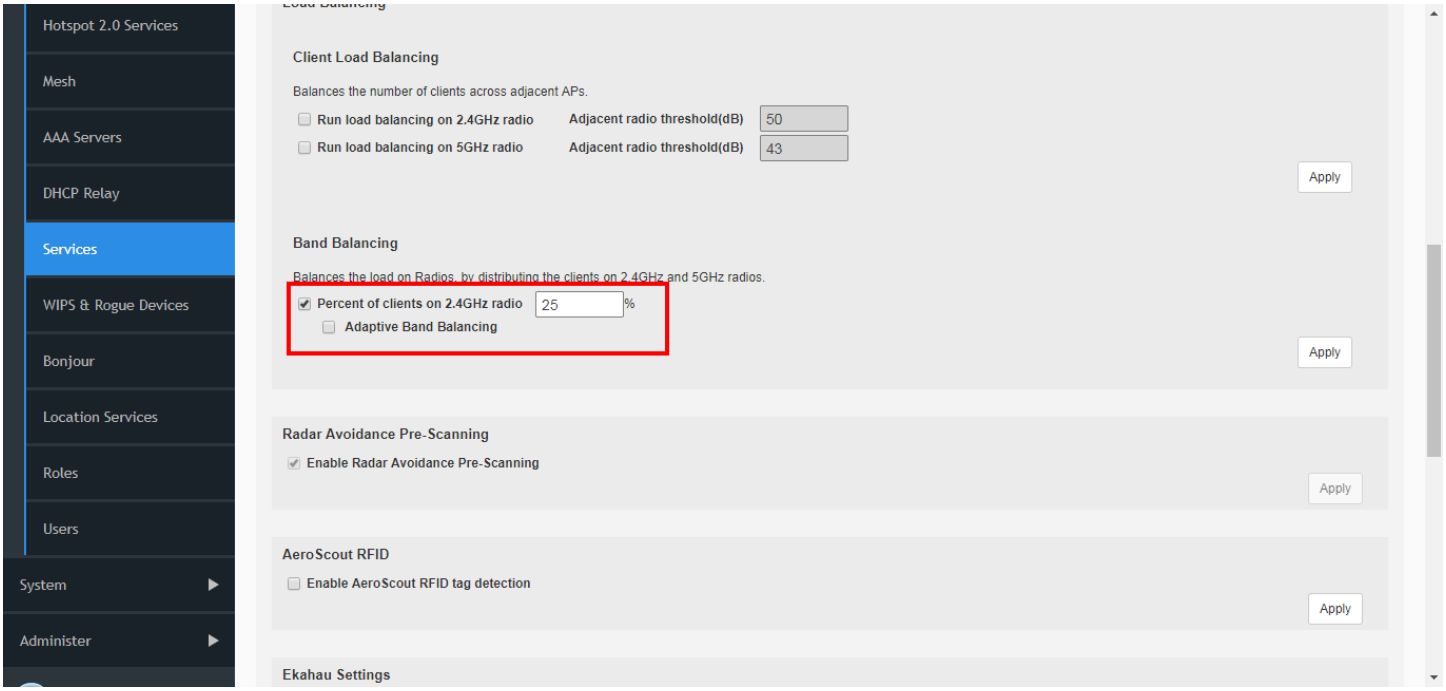


Band Balancing

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 and set to a target of 25% of clients connecting to the 2.4 GHz band. 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.

FIGURE 210 Band Balancing



Adaptive Band Balancing

This feature enhances the existing Band Balancing feature by allowing client redistribution dynamically after association, rather than only once during the initial association.

Using the Adaptive Band Balancing feature, ZoneDirector attempts to dynamically balance clients between the 2.4 and 5 GHz radios and thereby provide better Wi-Fi service to clients with weaker signals.

Many wireless clients tend to connect to the 2.4 GHz radio even when they are capable of connecting to the 5 GHz radio (which results in over-use of the 2.4 GHz band and underutilization of the 5 GHz band). There are several reasons for this:

- APs band balance clients at association time. At association, an AP may miss some clients because it does not know if the client is 5 GHz capable or not.
- Some clients do not respond to association-time Band Balancing.
- Many clients have a weak initial signal (far away from AP) and can only communicate with the 2.4GHz radio.

Adaptive Band Balancing attempts to mitigate these problems by employing BSS Fast Transition (802.11r) to encourage to clients to switch to the 5 GHz radio when appropriate.

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.

If a channel is blocked by this feature, it will be listed as “DFS Block Radar” in the AP monitoring page. This setting affects select outdoor dual band 802.11n 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*).

AeroScout RFID Tag Detection

AeroScout Tags are lightweight, battery-powered wireless devices that accurately locate and track people and assets.

AeroScout Tags, which can be mounted on valuable equipment or carried by personnel, send periodic data to the AeroScout Engine, the software component of the AeroScout visibility system that produces accurate location and presence data. If you are using AeroScout Tags in your organization, you can use the APs that are being managed by ZoneDirector to relay data from the AeroScout Tags to the AeroScout Engine. You only need to enable AeroScout tag detection on ZoneDirector to enable APs to relay data to the AeroScout engine.

To enable AeroScout RFID tag detection on ZoneDirector:

1. Go to **Services & Profiles** > **Services**.
2. Scroll down to the AeroScout RFID section (near the bottom of the page).
3. Select the **Enable AeroScout RFID tag detection** check box.
4. Click the **Apply** button in the same section to save your changes.

ZoneDirector enables AeroScout RFID tag detection on all its managed APs that support this feature.

> **NOTE**
> Tag locations are not accurate if the 2.4 GHz band is noisy or if the AP setup is not optimal (according to AeroScout documents). For more information on AeroScout Tags and the AeroScout Engine, refer to your AeroScout documentation.

Ekahau Tag Detection

Utilizing Wi-Fi wireless network as an infrastructure, the Ekahau Real Time Location battery-powered devices that can be mounted on equipment or carried by personnel, and send out periodic Ekahau Blink frames. Wi-Fi Access Points receive and forward the Ekahau Blink frames to the Ekahau RTLS Controller, which calculates accurate locations for the tags.

To enable Ekahau tag detection on ZoneDirector:

1. Go to **Services & Profiles** > **Services**.
2. Scroll down to the **Ekahau Settings** section (near the bottom of the page).
3. Select the **Enable Ekahau tag detection** check box.
4. Enter the **Ekahau Controller IP address** and **Ekahau Controller Port**.
5. Click the **Apply** button in the same section to save your changes.

ZoneDirector enables Ekahau tag detection on all its managed APs that support this feature.

Active Client Detection

Enabling active client detection allows ZoneDirector to trigger an event when a client with a low signal strength joins the network.

To enable active client detection:

1. Go to **Services & Profiles** > **Services**, and scroll down to the **Active Client Detection** section.
2. Click the check box next to **Enable client detection ...** and enter an RSSI threshold, below which an event will be triggered.
3. Click **Apply** to save your changes.

A low severity event is now triggered each time a client connects with an RSSI lower than the threshold value entered. Go to **System** > **All Events/ Activities** to monitor these events.

Tunnel Configuration

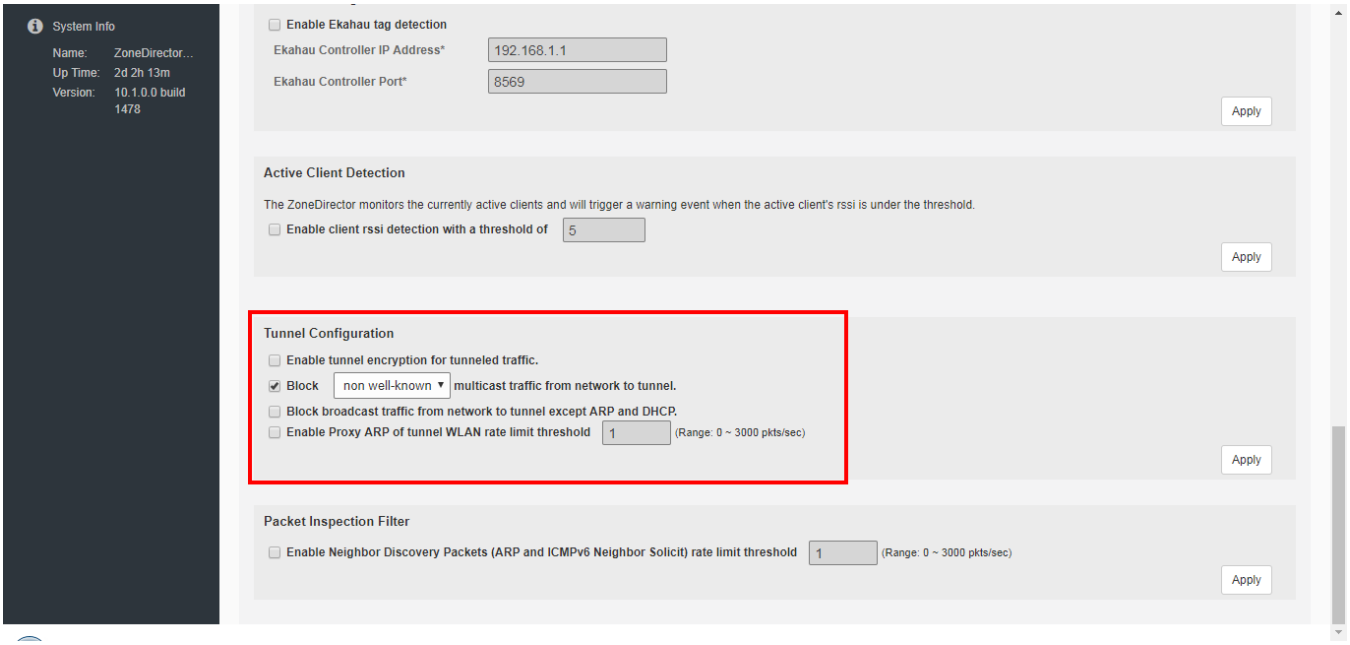
Only WLANs with Tunnel Mode enabled are affected.

See Advanced WLAN Options on page 72 in the WLAN configuration section for information on enabling Tunnel Mode.

To configure data encryption and filtering for tunneled WLANs:

1. Go to **Services & Profiles** > **Services**
2. Scroll down to the bottom of the page and locate the **Tunnel Configuration** section.
3. Enable the check boxes next to the features you want to enable.
   - **Enable tunnel encryption for tunneled traffic**: By default, when WLAN traffic is tunneled to ZoneDirector, 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 then use an AES-encrypted tunnel to send them to ZoneDirector.
   - **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 ZoneDirector 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 (see Packet Inspection Filter on page 275).
4. Click **Apply** in the same section to save your changes.

FIGURE 211 Set tunnel configuration parameters for all WLANs with tunnel mode enabled



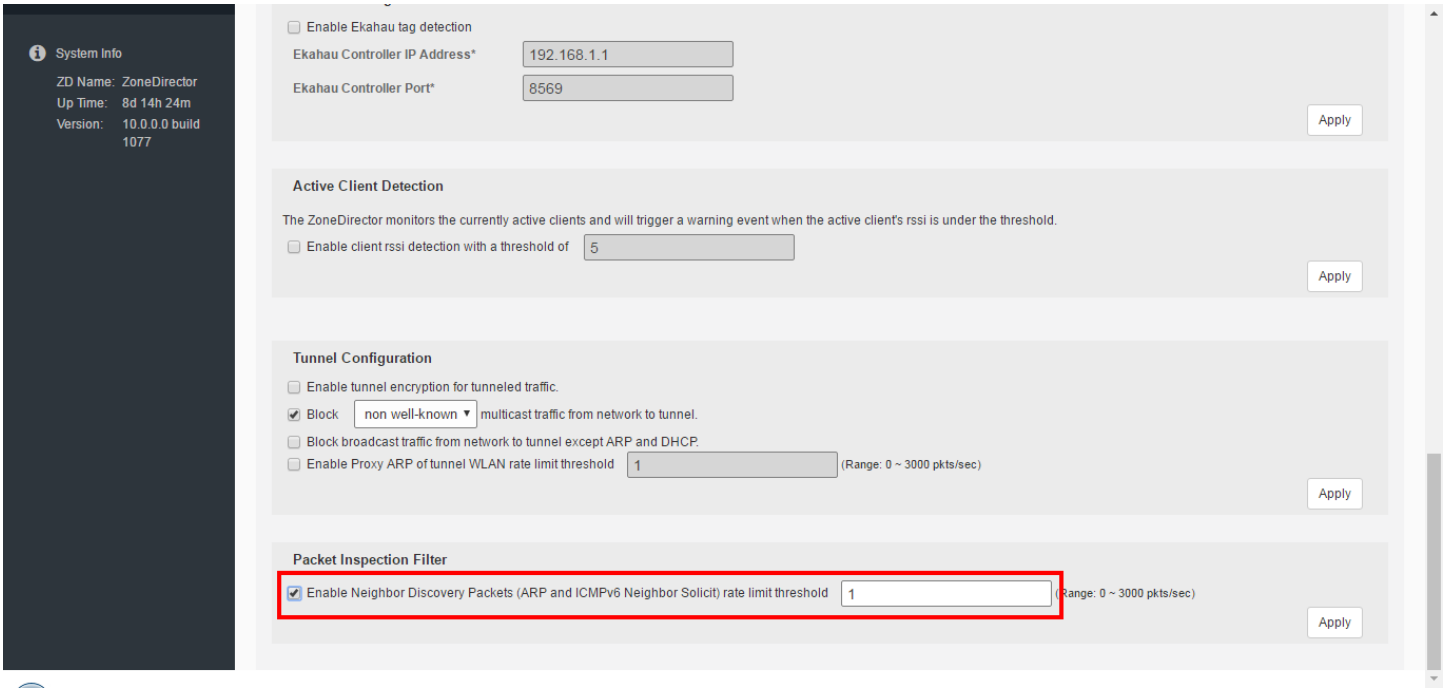
Packet Inspection Filter

The Packet Inspection Filter (PIF) allows configuration of rate limits for broadcast neighbor discovery (IPv4 Address Resolution Protocol and IPv6 Neighbor Solicit) packets. The PIF rate limiting threshold affects the following services:

- ARP Broadcast Filter for Mesh links (see Optional Mesh Configuration Features on page 397)
- Proxy ARP for WLAN interfaces (see Advanced WLAN Options on page 72 under Creating a WLAN)
- Proxy ARP for Tunneled WLANs (see Tunnel Configuration on page 274)

When Proxy ARP or ARP Broadcast Filter services are enabled, the AP attempts to reduce neighbor discovery traffic over the air by replacing broadcast messages with unicast messages for known hosts. When these packets are received for an unknown host, the Packet Inspection Filter supplements this functionality by limiting the rate at which these packets are delivered.

FIGURE 212 Packet Inspection Filter



Configuring Wireless Intrusion Prevention

ZoneDirector provides several built-in intrusion prevention features designed to protect the wireless network from security threats such as Denial of Service (DoS) attacks and 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.

DoS Protection

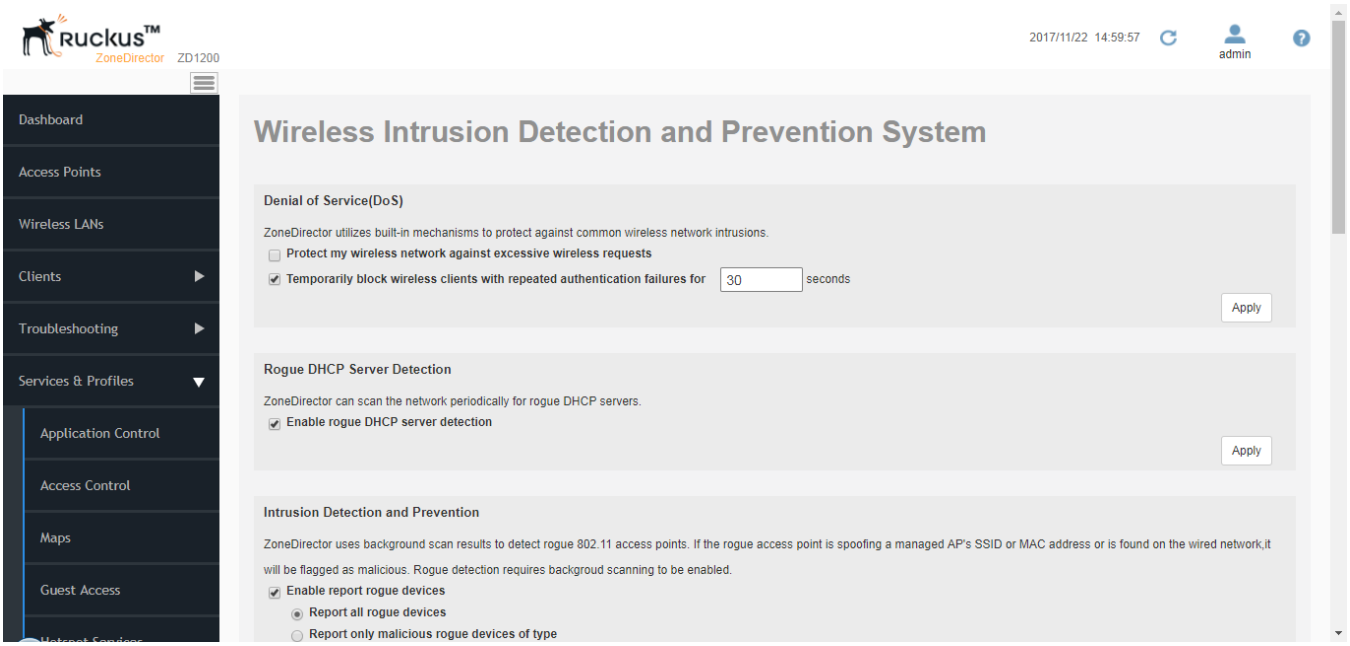
Two options are provided to protect the wireless network from Denial of Service attacks.

To configure the DoS protection options:

1. Go to **Services & Profiles** > **WIPS & Rogue Devices**

2. In the *Denial of Service (DoS)* section, configure the following settings:
   - **Protect my wireless network against excessive wireless requests**: If this capability is activated, excessive 802.11 probe request frames and management frames launched by malicious attackers will be discarded.
   - **Temporarily block wireless clients with repeated authentication failures for [ ] second**s: 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). Clients temporarily blocked by the **Intrusion Prevention** feature are not added to the **Blocked Clients** list on the **Services & Profiles** > **Access Control** page, **Blocked Clients** section.
3. Click **Apply** to save your changes.

FIGURE 213 Denial of Service (DoS) prevention options



Intrusion Detection and Prevention

ZoneDirector's 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 a ZoneDirector-managed access point that is not part of the wireless network managed by ZoneDirector.

Rogue devices are detected during off channel scans (background scanning) and are simply other access points that are not being managed by ZoneDirector (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 by ZoneDirector as "malicious rogue APs." The three automatically identified malicious access point categories are as follows:

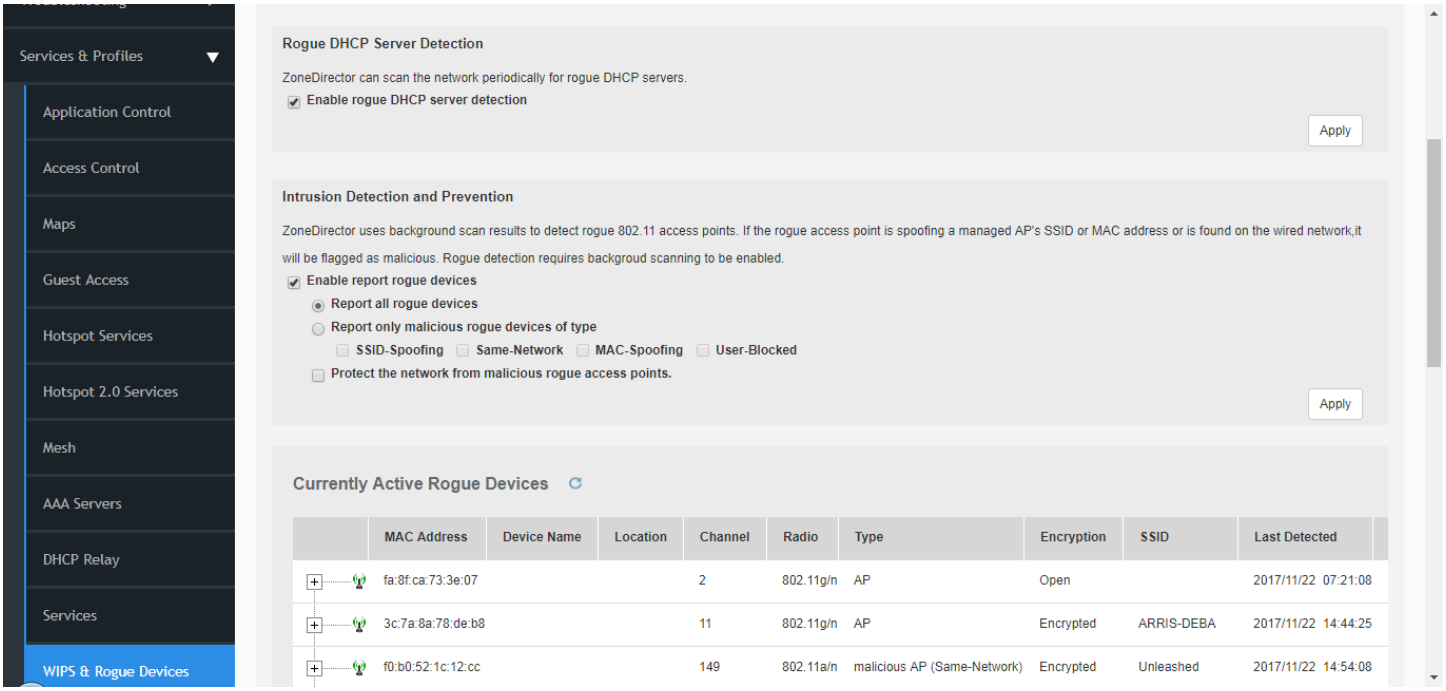
- SSID-Spoofing: These are rogue access points that are beaconing the same SSID name as a ZoneDirector-managed access point. They pose a threat as someone may be attempting to use them as a honey pot to attract your clients into their network to attempt hacking or man-in-the-middle attacks to exploit 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 ZoneDirector-managed 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 a ZoneDirector-managed 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.

The last type of malicious rogue device is "User Marked." These are devices that are manually marked as malicious rogues by a ZoneDirector administrator using the **Mark as Malicious** button on the **WIPS & Rogue Devices** page.

To configure intrusion detection and prevention options:

1. Go to **Services & Profiles > WIPS & Rogue Devices**.
2. In the **Intrusion Detection and Prevention** section, configure the following settings:
   - **Enable report rogue devices**: Enabling this check box allows ZoneDirector to include rogue device detection in logs and email alarm event notifications.
     - **Report all rogue devices**: Send alerts for all rogue AP events.
     - **Report only malicious rogue devices of type**: Select which event types to report.
   - **Protect the network from malicious rogue access points**: Enable this feature to automatically protect your network from network connected rogue APs, SSID-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 BSSID (MAC) to prevent wireless clients from connecting to the malicious rogue AP. This option is disabled by default.
3. Click the **Apply** button in the same section to save your changes.

FIGURE 214 Intrusion Detection and Prevention settings



See Detecting Rogue Access Points on page 379 for more information on monitoring and handling rogue devices.

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. ZoneDirector has a rogue DHCP server detection feature that can help you prevent connectivity and security issues that rogue DHCP servers may cause. When this feature is enabled, ZoneDirector scans the network every five seconds for unauthorized DHCP servers and generates an event every time it detects a rogue DHCP server.

The conditions for detecting rogue DHCP servers depend on whether ZoneDirector's own DHCP server is enabled:

- If the built-in DHCP server is enabled, ZoneDirector will generate an event when it detects any other DHCP server on the network.
- If the built-in DHCP server is disabled, ZoneDirector will generate events when it detects two or more DHCP servers on the network. You will need to find these DHCP servers on the network, determine which ones are rogue, and then disconnect them or shut down the DHCP service on them.

The Rogue DHCP Server Detection feature is enabled by default. If it is disabled, use the following procedure to re-enable:

To enable rogue DHCP server detection on ZoneDirector (enabled by default):

1. Go to **Services & Profiles** > **WIPS & Rogue Devices**.
2. In the Rogue **DHCP Server Detection** section, select the **Enable rogue DHCP server detection** check box.
3. Click the **Apply** button that is in the same section.

You have completed enabling rogue DHCP server detection. Ruckus recommends checking the **System** > **All Events/Activities** page periodically to determine if ZoneDirector has detected any rogue DHCP servers. When a rogue DHCP server is detected, the following event appears on the **All Events/Activities** page:

```
Rogue DHCP server on [IP_address] has been detected.
```

If the check box is cleared, ZoneDirector will not generate these events.

NOTE
Rogue DHCP server detection only works on the ZoneDirector's management IP subnet.

DHCP Relay

ZoneDirector's DHCP Relay agent improves network performance by converting DHCP broadcast traffic to unicast to prevent flooding the Layer 2 network (when Layer 3 Tunnel Mode is enabled -- DHCP Relay only applies to Tunnel Mode WLANs.)

Typically, when mobile stations acquire IP addresses through DHCP, the DHCP request and acknowledgment traffic is broadcast to any devices in the same Layer 2 environment. With Tunnel Mode WLANs, this traffic flood is wasteful in terms of bandwidth and computing power. When DHCP Relay is enabled on a WLAN, the ZoneDirector relay agent converts DHCP Discover / Request traffic to unicast UDP packets and sends them to the DHCP servers, then delivers DHCP Offer / Ack messages from the DHCP server back to the client.

The traffic flow is as follows:

1. Client sends DHCP discover broadcast.
2. AP tunnels this DHCP discover frame to ZoneDirector.
3. DHCP Relay Agent sends unicast DHCP discover packet to DHCP server.
4. DHCP server sends DHCP offer to Relay Agent on ZoneDirector.
5. ZoneDirector sends DHCP Offer back to the AP.
6. AP sends this Offer to client.

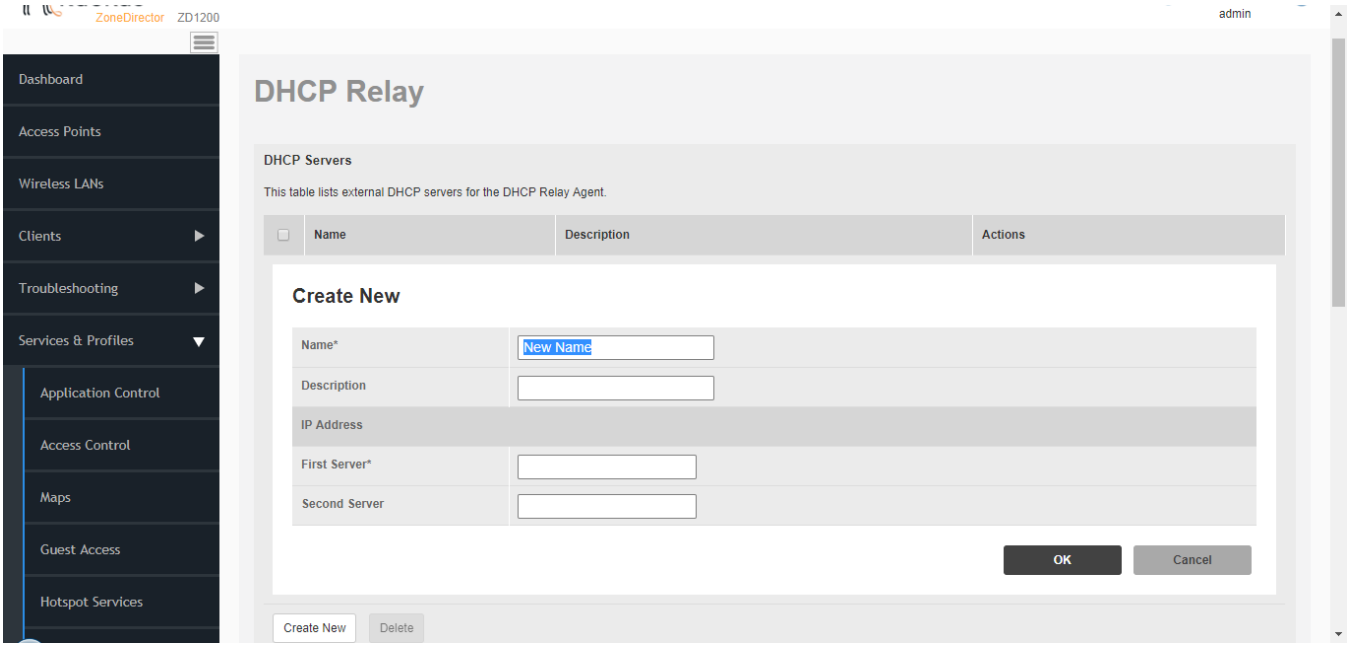
By reducing broadcast flooding, this option allows for higher client capacity in tunneled WLANs designed for VoIP phones, for example. It also allows for DHCP discovery across multiple subnets and limits DHCP broadcasts to the client's AP tunnel and radio.

To configure DHCP Relay for tunneled WLANs:

1. Go to **Services & Profiles** > **DHCP Relay**.
2. Click **Create New**.
3. Enter a **Name** and **IP address** for the server.

4. Click **OK** to save your changes. The new server appears in the list.

FIGURE 215 Creating a DHCP Relay server

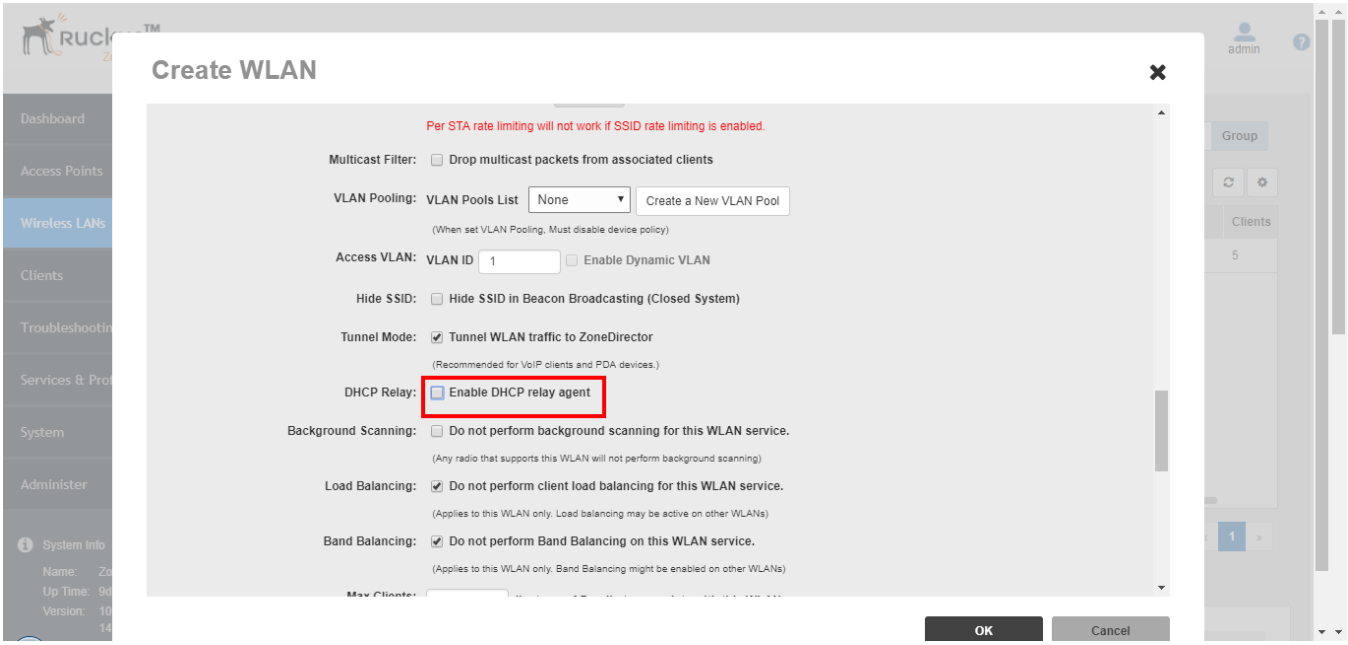


To enable DHCP Relay for a WLAN:

1. Go to**Wireless LANs**.
2. If creating a new WLAN, click **Create New**. Otherwise, click **Edit** for the WLAN you want to configure.
3. Under **Advanced Options**, when Tunnel Mode is enabled, the DHCP Relay option becomes available.
4. Under **DHCP Relay**, select **Enable DHCP relay agent with __ DHCP** server and select the server you created earlier from the list.

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

FIGURE 216 Enabling DHCP Relay agent for a Tunnel Mode WLAN



Bonjour Gateway

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

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.

ZoneDirector's Bonjour Gateway feature addresses this requirement by providing an mDNS proxy service configurable from the web interface to allow administrators to specify which types of Bonjour services can be accessed from/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 SSIDs.
- 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.

NOTE
Note the following considerations when deploying Bonjour Gateway rules:

- *Bridge Service Rules*
- *Bridge Service Records*

Bridge Service Rules

Creating a large number of Bonjour Gateway Bridge Service Rules can have a negative impact on memory and CPU resources.

The maximum number of Bonjour Gateway Rules that ZoneDirector can support is 256. If the maximum number of Bonjour service rules is exceeded, users can edit and delete existing rules, but are not allowed to create new rules until the total number is lower than the maximum.

Bridge Service Records

Common Bonjour Bridge Services include multiple service types, and each takes up one service record.

Each ZoneDirector or AP serving as a Bonjour Gateway is limited to a maximum of 500 Bridge Service Records. Some Bonjour services use more than one service record. For example, AirPlay takes two service records (for audio and video), and AirPrint can use up to four service records.

If you multiply the number of service records by the number of printers and Apple TVs, the total may easily exceed the 500 service record limit. Admins must therefore be aware of how many Bonjour servers/services are advertised per broadcast domain.
Each AirPrinter may take up to 4 service entries if it supports **_ipp._tcp**, **_printer._tcp**, and **_universal._ipp._tcp**.

```
<mdnsservice name="AirPrint" id="4">
    <service type="_ipp._tcp."/>
    <service type="_ipps._tcp."/>
    <service type="_universal._ipp._tcp."/>
    <service type="_printer._tcp."/>
  </mdnsservice>
```

Each Airplay will have 2 service entries:

```
<mdnsservice name="AirPlay" id="2">
    <service type="_airplay._tcp."/>
    <service type="_raop._tcp."/>
  </mdnsservice>
```

Apple File Server will have at least one service entry depending on what is enabled:

```
<mdnsservice name="Apple File Sharing" id="6">
    <service type="_afpovertcp._tcp."/>
  </mdnsservice>
```

In heavy use and if using AirPrint, AirPlay, and AppleTV at a site/location, consider defining one service on each of three different AP Bonjour Gateways to distribute the memory/CPU utilization.

> **NOTE**
> Consider using higher end model APs for dedicated AP Bonjour Gateways.

Creating a Bonjour Gateway Rule - ZD Site

The Bonjour Gateway service on ZoneDirector is essentially a list of rules for mapping services from one VLAN to another. Using the ZD Site Bonjour Gateway feature, ZoneDirector serves as the Bonjour proxy for forwarding Bonjour packets to the designated VLANs.

Layer 2 switch between ZoneDirector and APs. The maximum number of ZD site Bonjour Gateway rules is as follows:

TABLE 24 Max Bonjour rules per controller

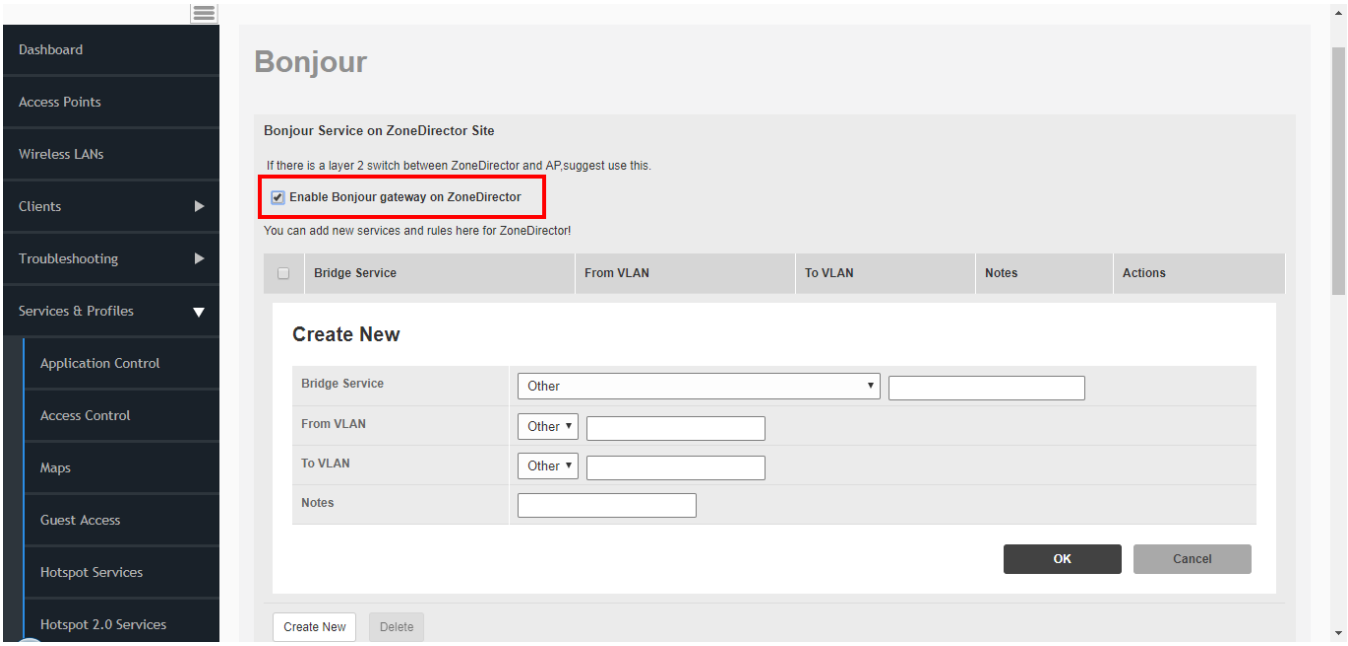
ZoneDirector Model	Max Rules
ZoneDirector 1200	256

To configure rules for bridging Bonjour services across VLANs:

1. Go to **Services & Profiles** > **Bonjour**.

2. In the **Bonjour Service on ZoneDirector Site** section, click **Create New** to create a new Bonjour service rule.
3. 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.
4. Click **OK**.
5. Repeat for any additional rules.
6. Select the check box next to **Enable Bonjour gateway on ZD** and click the **Apply** button.

FIGURE 217 Creating a ZD Site Bonjour Gateway rule



Creating a Bonjour Gateway Rule AP Site

Using the AP Site Bonjour Gateway feature, Bonjour bridging service is performed on a designated AP rather than on ZoneDirector.

Offloading the Bonjour policy to an AP is necessary if a Layer 3 switch or router exists between ZoneDirector and the APs. ZoneDirector identifies a single AP that meets the memory/processor requirements (this feature is only supported on certain APs), and delivers a set of service rules - a Bonjour policy - to the AP to perform the VLAN bridging.

Requirements and limitations:

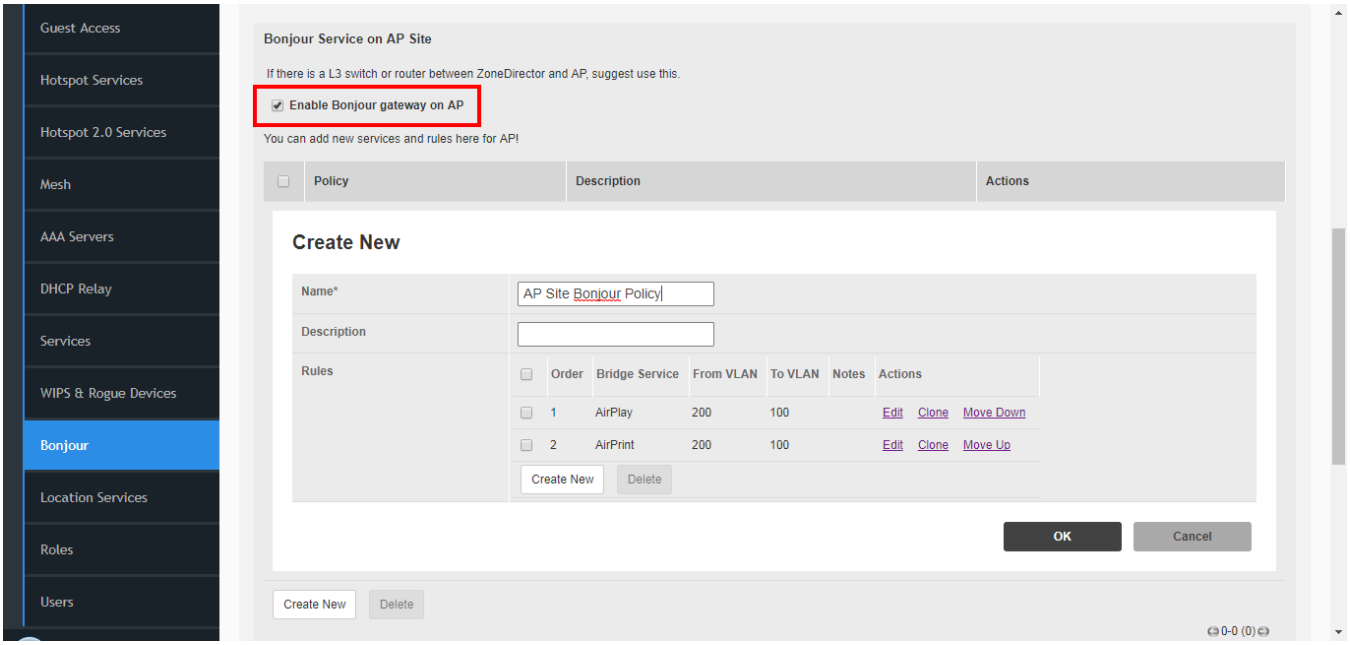
- Bonjour policy deployment to an AP takes effect after the AP joins ZoneDirector.

- Some APs of one local area link must be in one subnet. The switch interfaces connected to these APs in a local area link to must be configured in VLAN-trunk mode. Only by doing so can the designated AP can receive all the multicast Bonjour protocol packets from other VLANs.
- Dynamic VLANs are not supported.
- Some AP models are incompatible with this feature due to memory requirements.

To configure rules for AP site bridging Bonjour services across VLANs:

1. Go to **Services & Profiles** > **Bonjour**.
2. In the **Bonjour Service on AP Site** section, click **Create New** to create a new Bonjour service policy.
3. Type a name for the policy, then click **Create New** to create a new rule.
4. In the **Create New** form, configure the following options:
   - **Name**: Enter a name for the proxy.
   - **Description**: Optionally, enter a description for the rule.
   - **Order**: Choose the order in which to apply rules.
   - **Bridge Service**: Select the Bonjour service from the list.
   - **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.
5. Click **OK** to save your changes.
6. Repeat for any additional rules.
7. Select the check box next to **Enable Bonjour gateway on AP** and click the **OK** button.

FIGURE 218 Create an AP site Bonjour policy



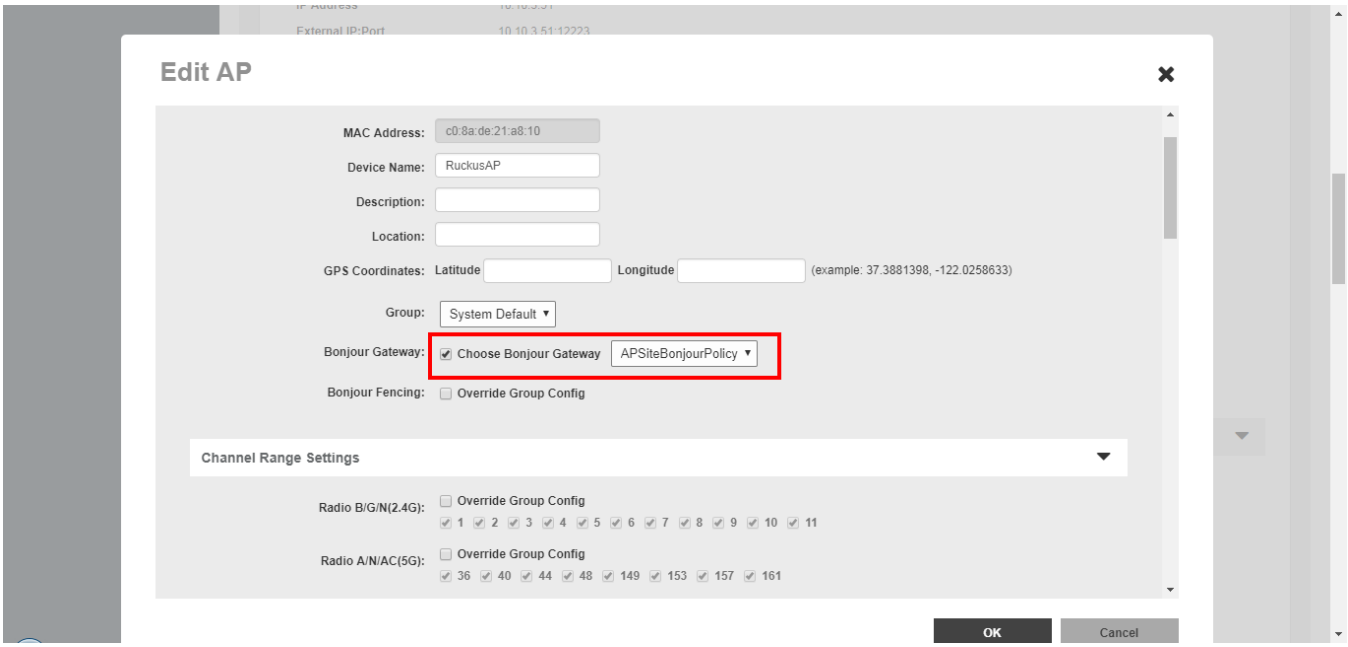
Applying a Bonjour Policy to an AP

Once you have created an AP site Bonjour policy, you will need to designate the AP that will be responsible for implementing this policy.

To enable Bonjour policy on an AP:

1. Go to **Access Points**.
2. Click **Configure** for the AP you want to configure.
3. In **Bonjour Gateway**, enable the check box and select a Bonjour policy that you created on the **Services & Profiles** > **Bonjour** page from the list.
4. Click **OK** to save your changes.

FIGURE 219 Designate an AP as a Bonjour Gateway



Example Network Setup

The following example illustrates how ZoneDirector's Bonjour Gateway can be used to allow users to access Bonjour resources on different VLANs in a school setting, where access to certain resources must generally be separated between teachers and students, but where sharing may sometimes be necessary.

Assume a network with three VLANs mapped to separate SSIDs, all on separate subnets or multicast domains. The three segments host different devices for different users:

- Classroom SSID (VLAN 100): WEP authentication, includes an iMac desktop for file sharing and iOS Sync for backup, and an Apple TV attached to a projector.
- Teachers SSID (VLAN 200): 802.1X authentication for a MacBook and iPad, needs to have access to all classroom resources.
- Students SSID (VLAN 300): Students have a separate SSID with no authentication, they must be able to backup their iPads to the classroom iMac but should not have access to the Apple TV or File Sharing services.

In this example, the teacher gains access to AirPlay, AirPrint, iCloud Sync and File Sharing, while students are given access to iCloud Sync and AirPrint only.

Bonjour Fencing

Bonjour Fencing provides a mechanism to limit the scope of Bonjour (mDNS) service discovery in the physical/spatial domain.

While Bonjour Fencing is related to Bonjour Gateway, they are two separate features designed for different purposes. Bonjour Gateway bridges mDNS services across VLANs, and is useful because Bonjour is designed as a same-VLAN protocol.

Bonjour Fencing limits the range of Bonjour service discovery within physical space, which is useful because logical network boundaries (e.g. VLANs) do not always correlate well to physical boundaries within a building/floor.

Configuring Bonjour Fencing Policies

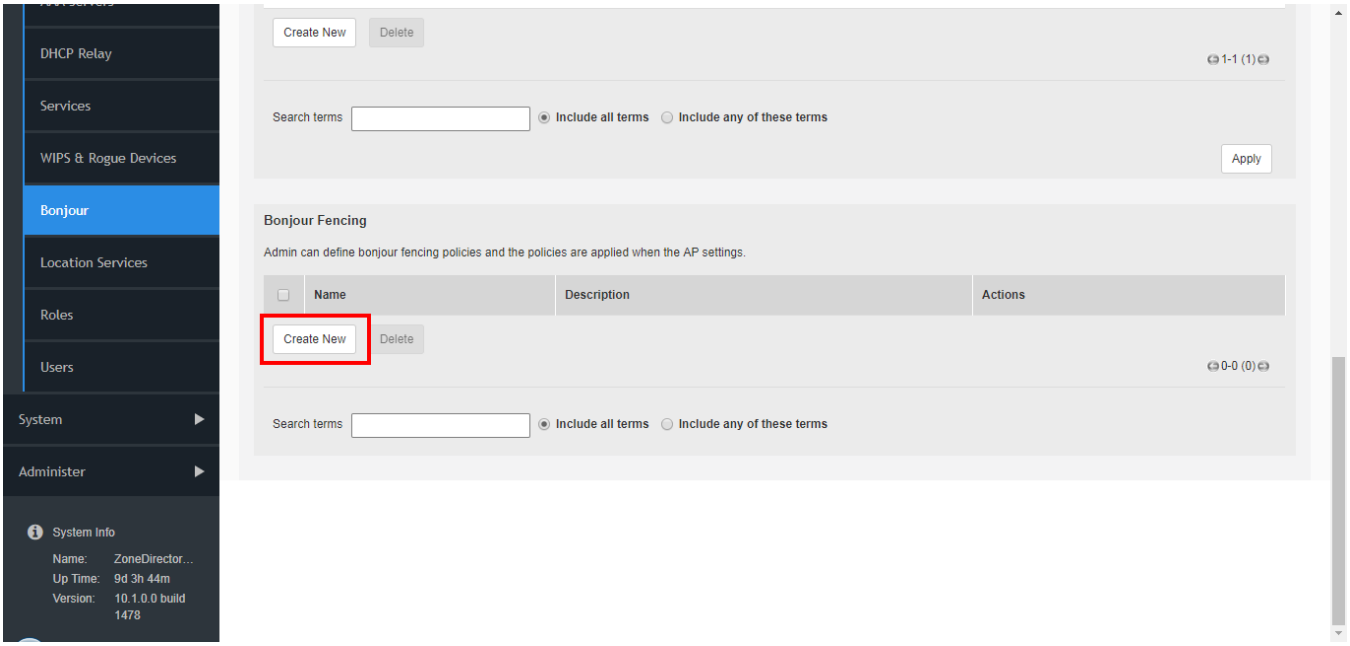
Bonjour Fencing requires a two-step process: create a policy, and then apply it to either an AP or an AP Group that will serve as the "anchor" for the Bonjour services.

To create a Bonjour Fencing policy:

1. Go to **Services & Profiles** > **Bonjour**.
2. In the **Bonjour Fencing** section, click **Create New**.

   The **Create Bonjour Fencing Policy** page appears.

   FIGURE 220 Creating a Bonjour Fencing Policy



3. Configure the following:
   a. **Name**: Type a name for the policy.
   b. **Description**: Type a description for the policy.
   c. **Fencing Rule**: Create the policy rule by configuring the following:
      1. Click **Create**. The **Create New (Fencing Rule)** screen appears.
      2. Configure the following options:
         - **Source Type**: Select **Wireless** or **Wired** network connection method for the device advertising bonjour services.

           When you select Wired, you must also specify the MAC address of the device advertising bonjour services in **Device MAC**, and the access point that is physically closest to the wired device in **Closest AP**. Setting the closest AP creates a physical anchor point for fencing, and the closest AP is auto-detected for wireless devices, based on the AP association.
         - **Service**: Select one of the Bonjour services from the drop-down list.

           NOTE
           If *Google Chrome Cast* service is selected for Bonjour fencing, then SSDP port 1900 will be blocked to prevent ChromeCast from initiating device discovery through SSDP protocol.
         - **Fencing Range**: Select the fencing range to be restricted to either the Same AP or 1-Hop AP Neighbors.
         - **Description**: Enter an optional description to describe the rule.
      3. Click **OK**.

         You have created the Bonjour Fencing policy rule.
   d. Click **OK** again to save the Bonjour Fencing Policy.

You have created a Bonjour Fencing policy with rules.

Next, you must configure an AP or AP group as the anchor for the policy, as described in Applying a Bonjour Fencing Policy to an AP or AP Group on page 287.

Applying a Bonjour Fencing Policy to an AP or AP Group

Once you have created a Bonjour Fencing policy, you will need to apply the policy to either an individual AP or an AP group.

To apply a Bonjour Fencing policy to an AP or AP group:

1. Go to **Access Points**.
2. Click **Configure** for the AP you want to configure as the "anchor" for the Bonjour service policy.
3. In **Bonjour Fencing**, enable the **Override Group Config** check box and select a Bonjour Fencing policy that you created on the **Services & Profiles** > **Bonjour** page from the list.
4. Click **OK** to save your changes.
5. To configure an AP group with a fencing policy, click **Edit** next to the AP group you want to use as the anchor, and select the **Policy** from the list of existing policies or click **Create New** to create a new fencing policy.

SPoT Location Services

To take advantage of Ruckus SmartPositioning Technology (SPoT) location services, ZoneDirector must be configured with the Venue information that is displayed in the SPoT Administration Portal.

After completing purchase of the SPoT location service, you will be given account login information that you can use to log into the SPoT Administration Portal. The Admin Portal provides tools for configuring and managing all of your "Venues" (the physical locations in which SPoT service is deployed). After a Venue is successfully set up, you will need to enter the same Venue information in ZoneDirector.

The following section lists the steps required for configuring ZoneDirector to communicate with the SPoT Location Server.

To configure ZoneDirector for SPoT communication:

1. Log in to the SPoT Administration Portal.
2. On the **Venues** page, click **Config** next to the venue for which you want to configure ZoneDirector Location Services.
3. Take note of the four values in **Controller Settings**.
4. In the ZoneDirector web interface, go to **Services & Profiles** > **Location Services**.
5. In **Location Services**, click **Create New**.
6. Enter the information from the **SPot Admin Portal** nto the four fields provided.
7. Click **OK** to save your changes.
8. Go to **Access Points**, and in **Access Point Groups**, click **Create New** or **Edit** to configure one or more AP groups for SPoT location services.
9. Configure the AP group for SPoT communications. You will need to select 1 channel per radio for calibration, then after calibration is complete, select 3 channels per radio for normal operation (see *SPoT User Guide* for details).
10. In **Location Services**, click **Enable**, then select the **Venue** you created on the **Services & Profiles** > **Location Services** page.
11. Click **OK** to save the AP group. ZoneDirector will begin trying to communicate with the SPoT Location Server.

12. Once the APs have successfully connected to the SPoT server, you can view the status of your SPoT-enabled APs on the *Location Services* page.

FIGURE 221 SPoT Administration Portal Venue Config page

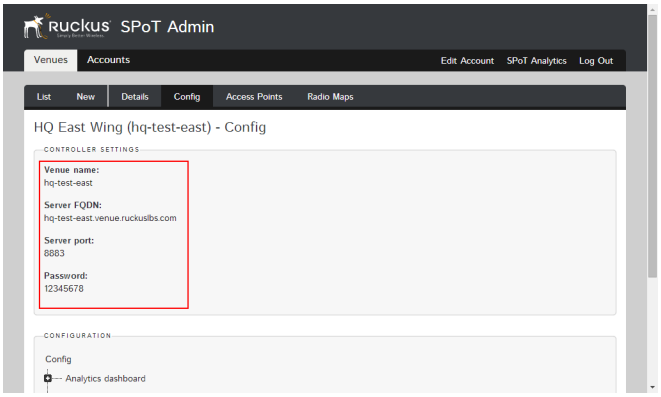
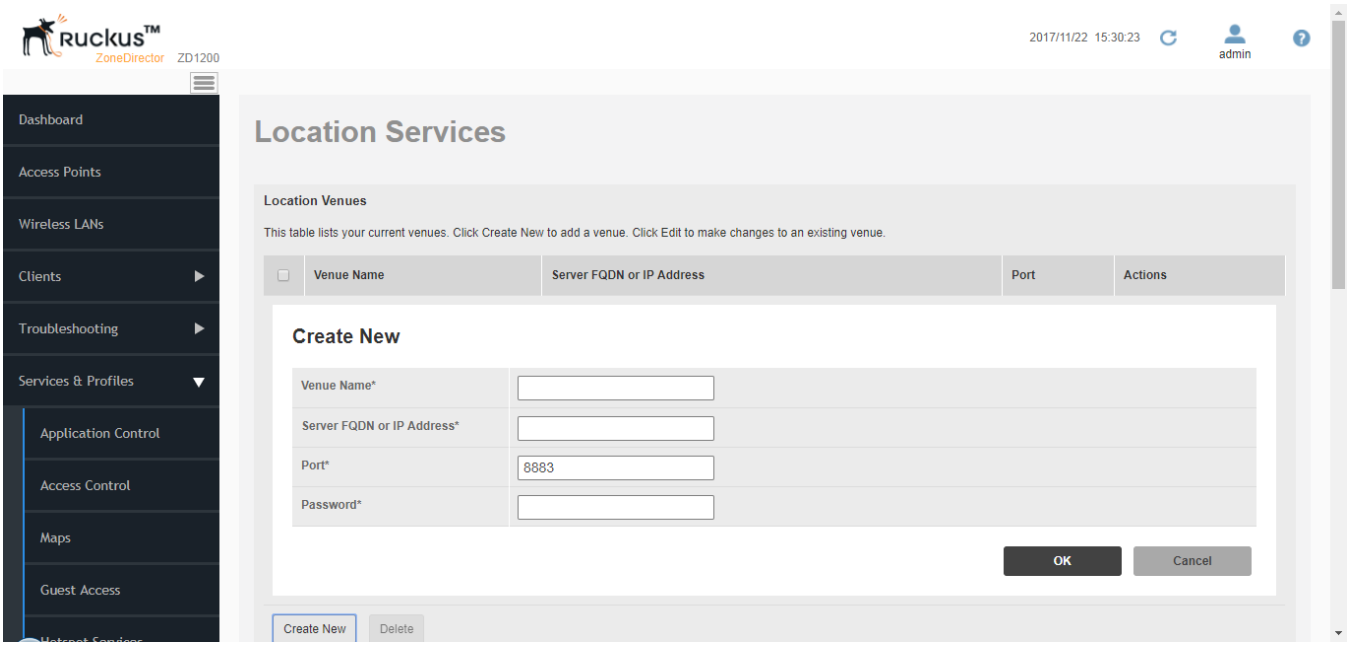


FIGURE 222 Enter the venue information in ZoneDirector's Services & Profiles > Location Services page



For more information on configuration and management of your SPoT Location Services, see the *SPoT User Guide*, available from: https://support.ruckuswireless.com.

Configuring System Settings

- System Configuration Overview 291
- Changing the Network Addressing 291
- Creating Static Route Entries 294
- Enabling Smart Redundancy 296
- Configuring the Built-in DHCP Server 300
- Controlling ZoneDirector Management Access 302
- Setting the System Time 303
- Setting the Country Code 305
- Configuring System Log Settings 307
- Setting Up Email Alarm Notifications 312
- Configuring SMS Settings for SMS Guest Pass Delivery 315
- Enabling Login Warning Messages 316
- Configuring Dashboard Map Settings 317
- Enabling Network Management Systems 318

System Configuration Overview

The majority of ZoneDirector's general system settings can be accessed from the **System** section in the web interface. A basic set of parameters was configured during the Setup Wizard process. These parameters and others can be customized in this section.

> **NOTE**
> When making any changes in the web interface, you must click **Apply** before you navigate away from the page or your changes will not be saved.

Changing the System Name

When you first worked through the Setup Wizard, you were prompted for a network-recognizable system name for ZoneDirector.

If needed, you can change that name by following these steps:

1. Go to **System** > **System Settings**
2. In **System Name** (under Identity), 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.

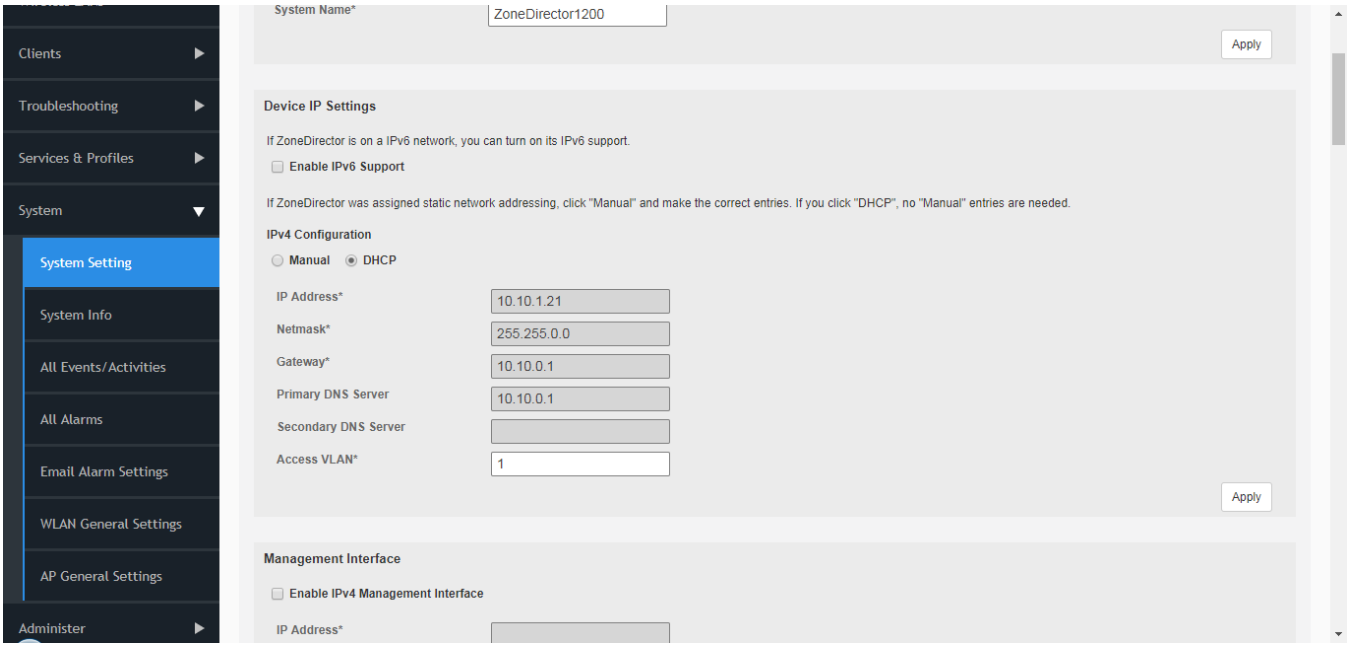
Changing the Network Addressing

IIf you need to update the IP address and DNS server settings of ZoneDirector, follow the steps outlined below.

1. Go to **System > System Settings**.

2. Review the **Device IP Settings** options.

FIGURE 223 The Device IP options



3. Select one of the following:
   - **Enable IPv6 Support**: By default, ZoneDirector operates in IPv4 mode. If your network uses IPv6, select Enable IPv6 Support and enter configuration settings for either IPv6 only or dual IPv4/IPv6 support. See IPv6 Configuration on page 292 for more information.
   - **Manual**: If you select Manual, enter the correct information in the now-active fields (IP Address, Netmask, and Gateway are required).
   - **DHCP**: If you select DHCP, no further information is required.
4. Click **Apply** to save your settings. You will lose connection to ZoneDirector.
5. To log back into the web interface, use the newly assigned IP address in your web browser or use the UPnP application to rediscover ZoneDirector.

IPv6 Configuration

ZoneDirector supports IPv6 and dual IPv4/IPv6 operation modes. If both IPv4 and IPv6 are used, ZoneDirector will keep both IP addresses. Ruckus APs operate in dual IPv4/v6 mode by default, so you do not need to manually set the mode for each AP.

If you enable IPv6, you have the option to manually configure an IP address in IPv6 format (128 bits separated by colons instead of decimals) or to choose **Auto Configuration**. If you choose **Manual**, you will need to enter **IP Address**, **Prefix Length** and **Gateway** address.

TABLE 25 Default static IPv4 and IPv6 addresses

	AP default IP address	ZoneDirector default IP address
IPv4	192.168.0.1	192.168.0.2
IPv6	fc00::1	fc00::2

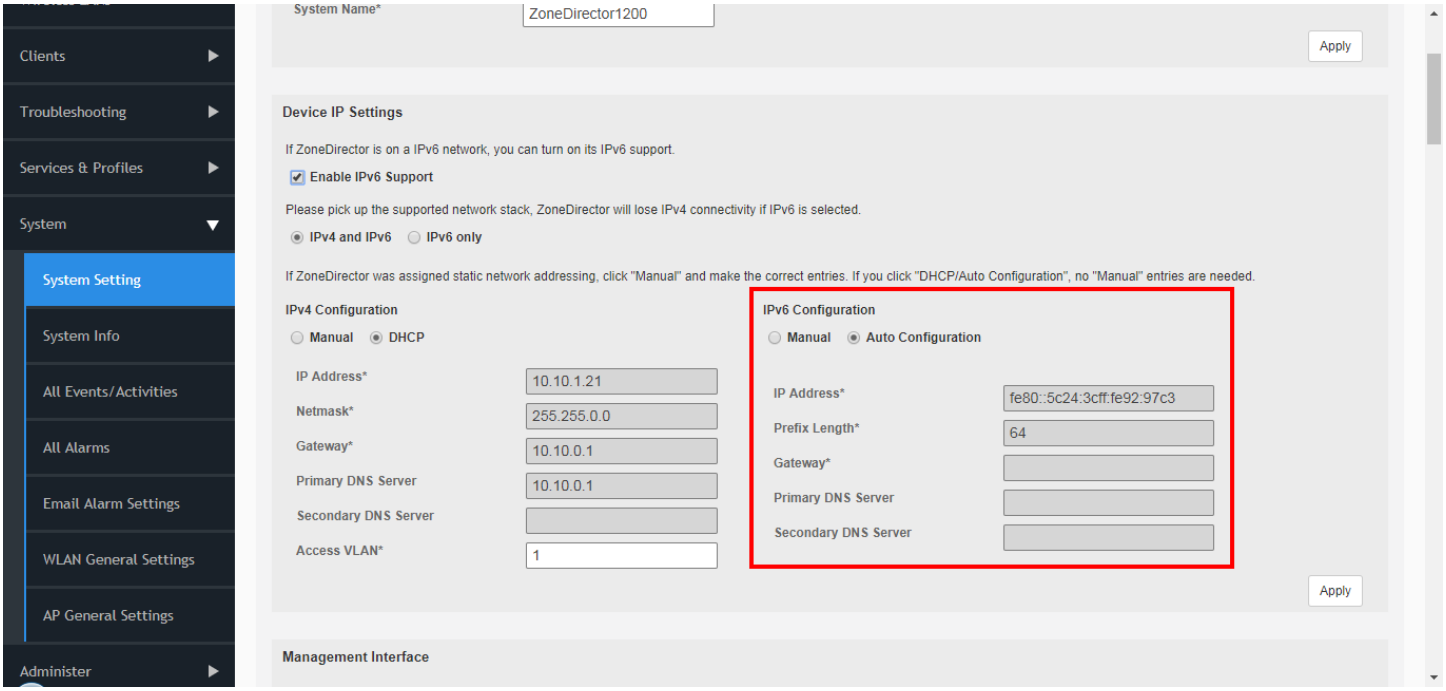
DNS Address can be configured manually or obtained automatically by the DHCPv6 client.

> **NOTE**
> If you switch from IPv4 to IPv6, you will need to manually change a number of settings that may have previously been configured, such as Access Control Lists (ACLs), AAA server addresses, Syslog server, SNMP trap receiver, etc.

When IPv6 is enabled, the other fields where IP addresses are entered (such as Additional Management Interface) automatically change to allow entry of IPv6 format addresses, as shown in Figure 24.

Note that some features are not supported when in IPv6 mode. Specifically, internal DHCP server, LAN rogue AP detection, DHCPv6 vendor specific options, Aeroscout RFID tag detection, SSL certificate generation, UPnP, remote access to ZD, and L2TP and WISPr in standalone APs are not supported when in IPv6 mode.

FIGURE 224 Enabling IPv6 automatically changes other fields to allow IPv6 addresses



Enabling an Additional Management Interface

The additional management interface is created for receiving and transmitting management traffic only.

The management IP address can be configured to allow an administrator to manage ZoneDirector from its management VLAN, thereby separating management traffic from LWAPP traffic between the controller and the access points. The Management IP can be reached from anywhere on the network as long as it is routable via the default Gateway configured in **Device IP Settings**.

It can also be used for Smart Redundancy -- when two redundant ZoneDirectors are deployed, you can create a separate management interface to be shared by both devices. Then, you only have to remember one IP address that you can log into regardless of which ZoneDirector is the active unit. This shared management IP address must be configured identically on both ZoneDirectors (see Enabling Smart Redundancy on page 296).

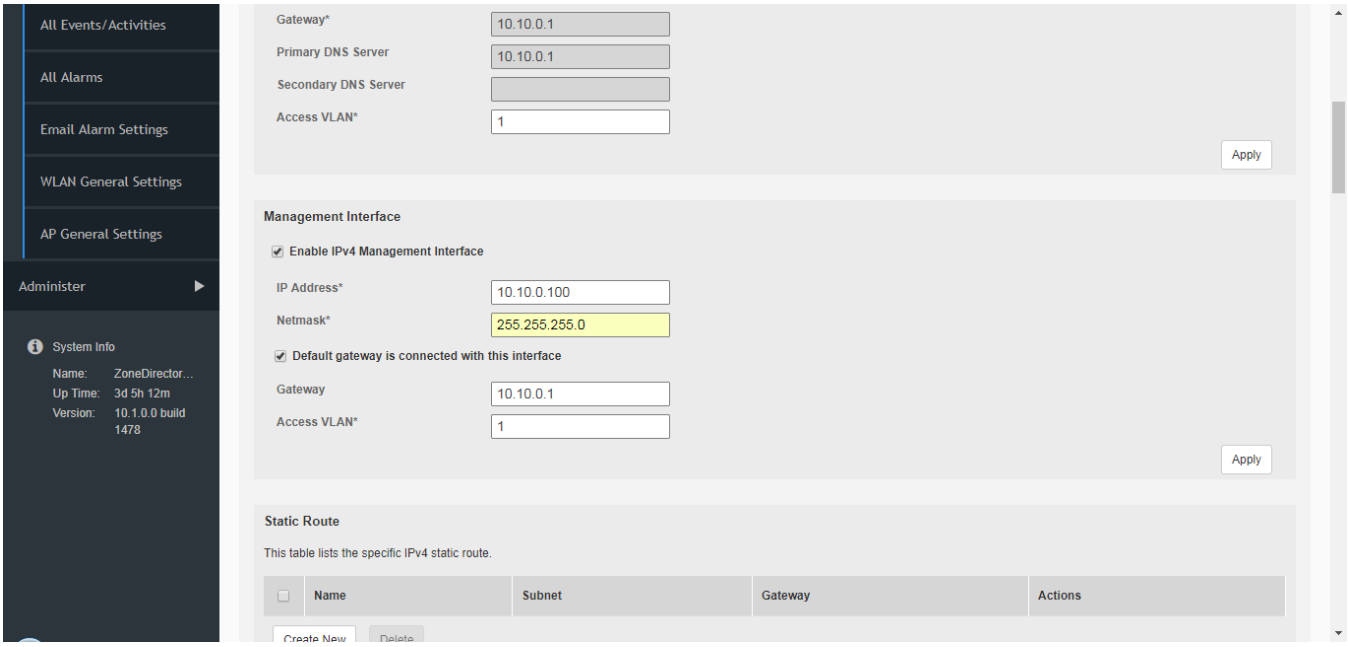
To enable an additional management interface:

1. Go to **System** > **System Settings**.

2. Locate the **Management Interface** section and click the check box next to **Enable IPv4 Management Interface** or **Enable IPv6 Management Interface**.
3. Enter the **IP Address**, **Netmask** and **Access VLAN** information for the additional interface. (If IPv6, enter *Prefix Length* instead of *Netmask*).
4. (Optional) If you want to configure this management interface with a different gateway from the gateway configured under "Device IP Settings", select **Default gateway is connected with this interface**, and enter the gateway IP address in the field provided. Enable this option if you want to change the default gateway of the ZoneDirector to be in your management subnet. Changing the default gateway to be in the management subnet will cause all traffic to be routed via this gateway.
5. **NOTE**
   If the Management Interface is to be shared by two Smart Redundancy ZoneDirectors, repeat these steps for the other ZoneDirector.

   Click **Apply** to save your settings.

FIGURE 225 Enabling an additional management interface



NOTE
If a management interface is used for web UI management, the actual IP address must still be used when configuring ZoneDirector as a client for a backend RADIUS server, UMM server or in any SNMP systems. If two ZoneDirectors are deployed in a Smart Redundancy configuration, both of the actual IP addresses must be used rather than the management IP address.

Creating Static Route Entries

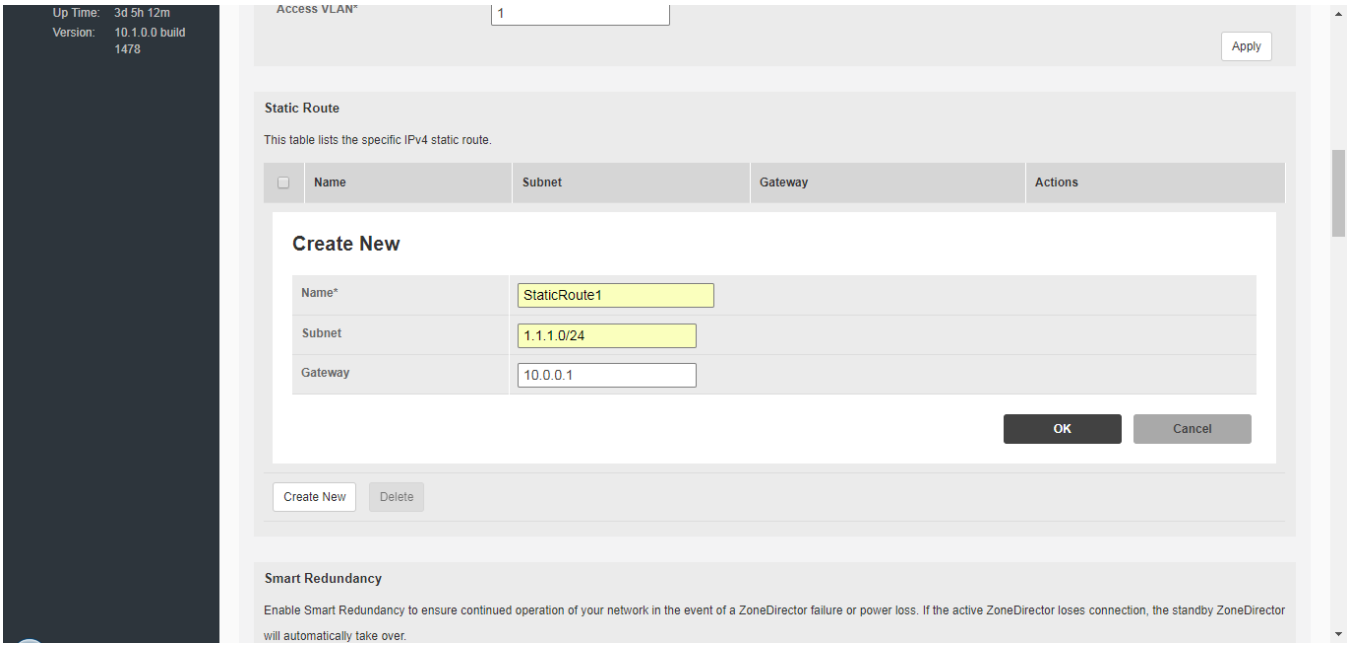
Static routes can be created to allow ZoneDirector to reach remote networks which can only be reached via a gateway other than default gateway. The gateway you use must be in the same subnet as either the ZoneDirector primary IP address or the Management IP address.

To create a static route to an additional gateway

1. Go to **System** > **System Settings** and locate the **Static Route** section.

2. Click **Create New** to create a new static route.
3. Enter a **Name** for this access route.
4. Enter a **Subnet** (in the format A.B.C.D/M (where M is the netmask).
5. Enter the **Gateway** address.
6. Click **OK** to save your changes. You can create up to 4 static route entries.

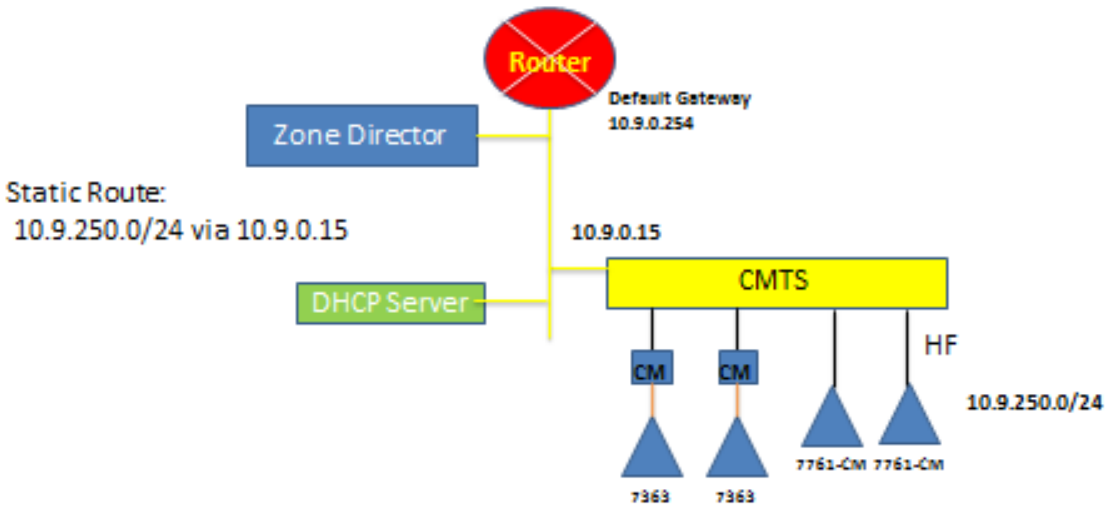
FIGURE 226 Creating a static route entry



Static Route Example

As an example, in a network where the APs are connected to ZoneDirector via a cable modem termination system, the APs are in a different subnet and not found via the default gateway. A static route would therefore be needed to allow ZoneDirector to AP connectivity.

FIGURE 227 A static route is needed when APs are reachable only through a non-default gateway



Enabling Smart Redundancy

ZoneDirector's Smart Redundancy feature allows two ZoneDirectors to be configured as a redundant pair, with one unit actively managing your network while the other serves as a backup in standby mode, ready to take over if the first unit fails or loses power.

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

The ZoneDirector in active state manages all APs and client connections. The ZoneDirector in standby state is responsible for monitoring the health of the active unit and periodically synchronizing its settings to match those of the active device. The ZoneDirector in standby state will not respond to Discovery requests from APs and changing from active to standby state will release all associated APs.

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

When two ZoneDirectors are connected in a Smart Redundancy configuration, the standby ZD will send heartbeats and the active will send discover messages at 6 second intervals. If after 15 seconds no reply is seen, each controller will assume disconnection from its peer, and the standby ZD will change to active state. At this point both devices are in active state and will accept join requests from APs.

When the two ZoneDirectors are communicating again, one active ZD will change to standby state and an auto-synchronization process will be started. A timestamp is used to determine which ZD should sync its latest configuration changes to those of its peer. They will continue trying to communicate, sending discover messages every 6 seconds, until the ZDs are communicating again, at which point they will determine active/standby roles based on: 1) most managed APs, and/or 2) lower MAC address.

Configuring ZoneDirector for Smart Redundancy

For management convenience, both ZoneDirectors in a Smart Redundancy deployment can be managed via a single shared IP address.

To manage two ZoneDirector devices, three IP addresses would need to be configured:

- Primary ZoneDirector's real address
- Backup ZoneDirector's real address
- Management address

All configuration changes are made to the active ZoneDirector and synchronized to the standby unit. The user can access the web interface from any of the three IP addresses, however not all configuration options are available from the standby device.

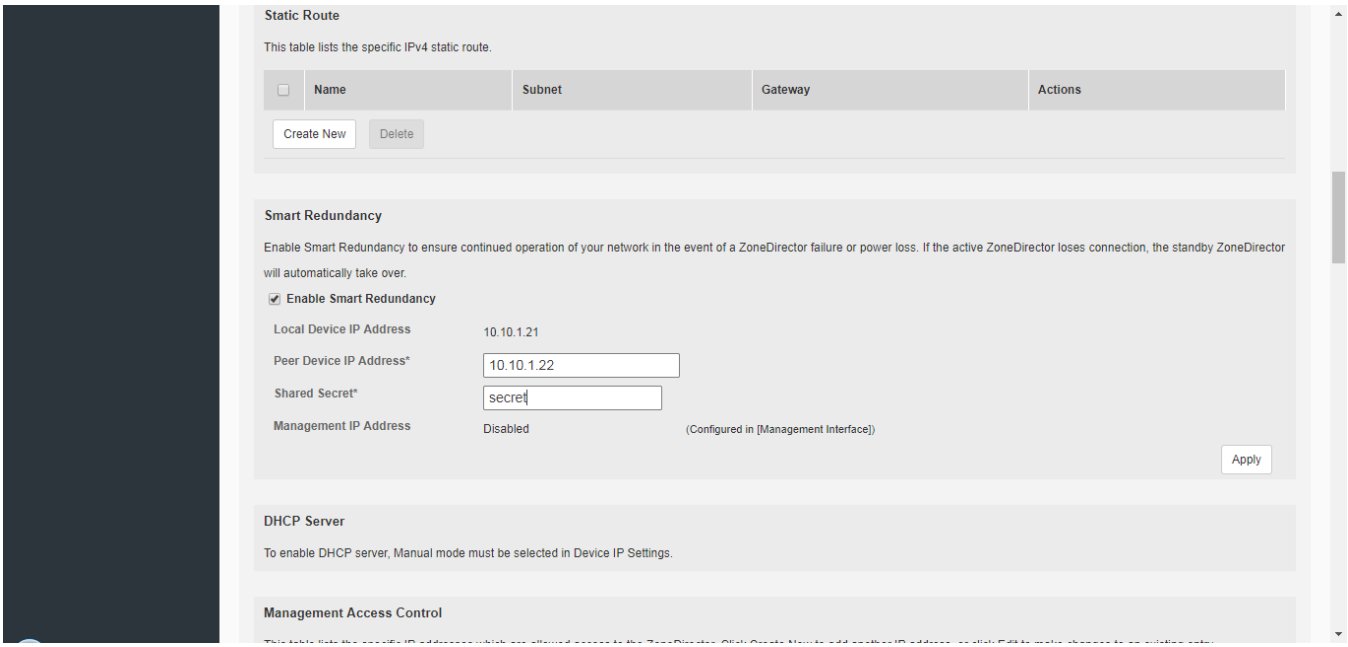
> **NOTE**
> If you will be deploying the two ZoneDirectors on different Layer 3 networks, you must ensure that Port 443 and Port 33003 are open in any routers and firewalls located between the two ZoneDirectors.

To enable Smart Redundancy:

1. Log in to the web interface of the ZoneDirector you will initially designate as the primary unit.
2. Go to **System** > **System Settings**, and set a static IP address under Device IP Settings, if not already configured.
3. Click **Apply**. You will need to log in again using the new IP address (if changed).

4. On the same **System** > **System Settings** page, locate the Smart Redundancy section.

   FIGURE 228 Enable Smart Redundancy



5. Enable the check box next to **Enable Smart Redundancy**.
6. Enter the IP address of the backup unit under **Peer Device IP Address**. If you have configured Limited ZD Discovery under *Access Points* > *Access Point Policies*, you must identify the IP address of both ZoneDirectors that the APs should connect to when Smart Redundancy is active. If the Limited ZD Discovery and Smart Redundancy information you enter is inconsistent, a warning message will be displayed asking you to confirm. Note that Ruckus recommends using the Smart Redundancy feature instead of the Limited ZD Discovery feature whenever possible.
7. Enter a **Shared Secret** for two-way communication between the two ZoneDirectors (up to 15 alphanumeric characters).
8. Click **Apply** to save your changes and prompt ZoneDirector to immediately attempt to discover its peer on the network.
9. If discovery is successful, the details of the peer device will be displayed to the right.
10. If discovery is unsuccessful, you will be prompted to retry discovery or continue configuring the current ZoneDirector.
11. Install the second ZoneDirector and complete the **Setup Wizard**.
12. Go to **System** > **System Settings**, enable **Smart Redundancy** and enter the primary ZoneDirector's IP address in **Peer Device IP address**.

13. Click **Apply**. If an active ZoneDirector is discovered, the second ZoneDirector will assume the standby state. If an active device is not discovered, you will be prompted to retry discovery or to continue configuring the current device.

    NOTE
    If you want to use the same SSL certificate for both devices in a Smart Redundancy pair, you can back up the certificate/private key from one device and import it into the other. See Working with SSL Certificates on page 346 for more information.

    NOTE
    If you disable Smart Redundancy after it has been enabled, both ZoneDirectors will revert to active state, which could result in unpredictable network topologies. Therefore, Ruckus recommends first factory resetting the standby ZoneDirector before disabling Smart Redundancy.

    NOTE
    If the active and standby ZoneDirector are on different IP subnets, APs need to know the IP addresses of both ZoneDirectors to quickly find the active ZoneDirector after a Smart Redundancy failover. You can do this by configuring the IP addresses of both devices on the **Access Points** > **Limited ZD Discovery** page. Specify one ZoneDirector as Primary, the other as Secondary. Alternatively, you can also specify the IP addresses of both ZoneDirectors using DHCP Option 43.

Managing Smart Redundancy AP License Pools

If two Smart Redundancy ZoneDirectors have different license levels (number of licensed APs), the total number of licenses is displayed in the Smart Redundancy dashboard widget, in the “License Pool” entry. When one device is disconnected, the remaining active ZD will continue to use the previous total license pool and start a 60-day timer. When the timer expires, the ZD will use its own license number (the license pool is reduced to the number of APs licensed for the currently active device only) until its Smart Redundancy peer comes back online.

If a third ZoneDirector connects, the license pool will reflect the new total license pool if the sum of the two licenses is higher than the original pair. If the sum is less than the previous license pool (within the 60-day timer), the user will be prompted to choose whether the license pool will be derived from the active + original disconnected device, or from the currently active + current standby device. License pools cannot exceed the maximum individual ZD license limit. ZoneDirectors with temporary licenses cannot be configured as part of a Smart Redundancy pair.

FIGURE 229 Smart Redundancy status degraded (peer is disconnected, license pool remains valid for 60 days

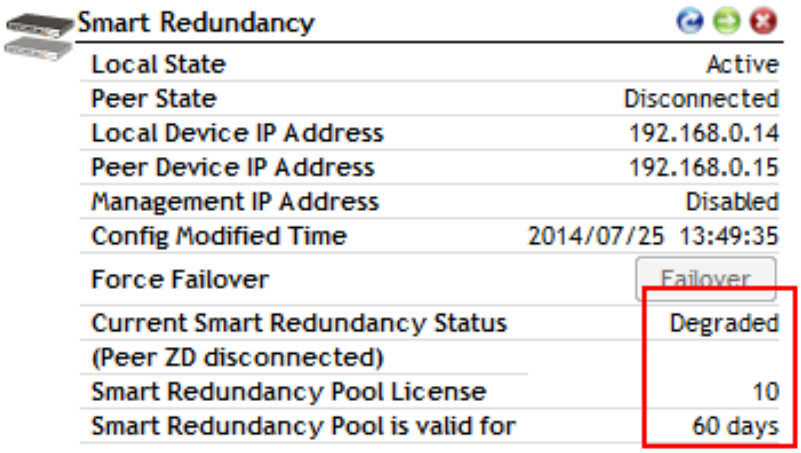


FIGURE 230 After 60 day grace period expires, license pool is revoked and AP license count reverts to active device license level only

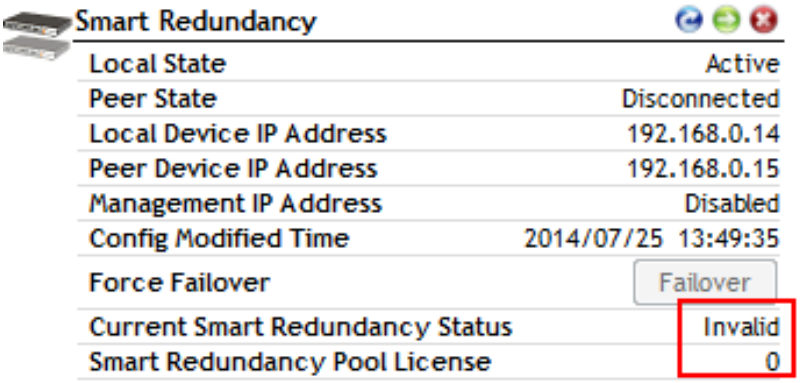


FIGURE 231 If a third ZD connects with a lower license level than the 2nd (disconnected) ZD, the user can choose to use the original license pool for up to 60 days

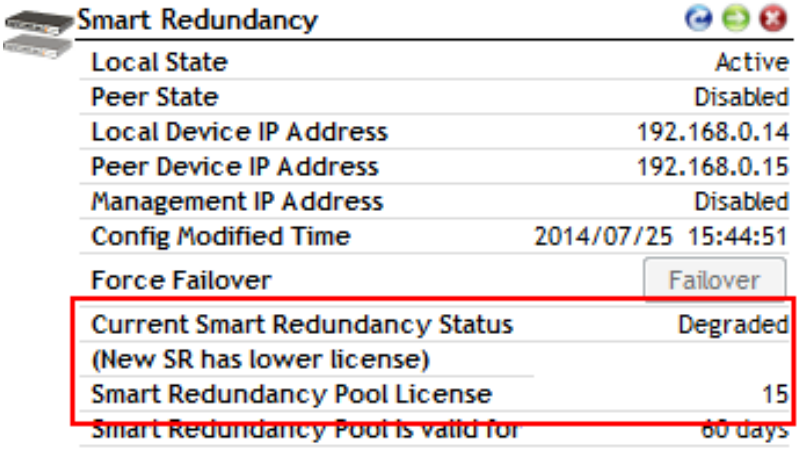


TABLE 26 Max AP Licenses by ZoneDirector Model

Model	Max AP Licenses
ZoneDirector 1200	150

Configuring the Built-in DHCP Server

ZoneDirector comes with a built-in DHCP server that you can enable to assign IP addresses to devices that are connected to it. ZoneDirector's DHCP server will only assign addresses to devices that are on its own subnet and part of the same VLAN.

Note that before you can enable the built-in DHCP server, ZoneDirector must be assigned a manual (static) IP address. If you configured ZoneDirector 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 System Configuration page.

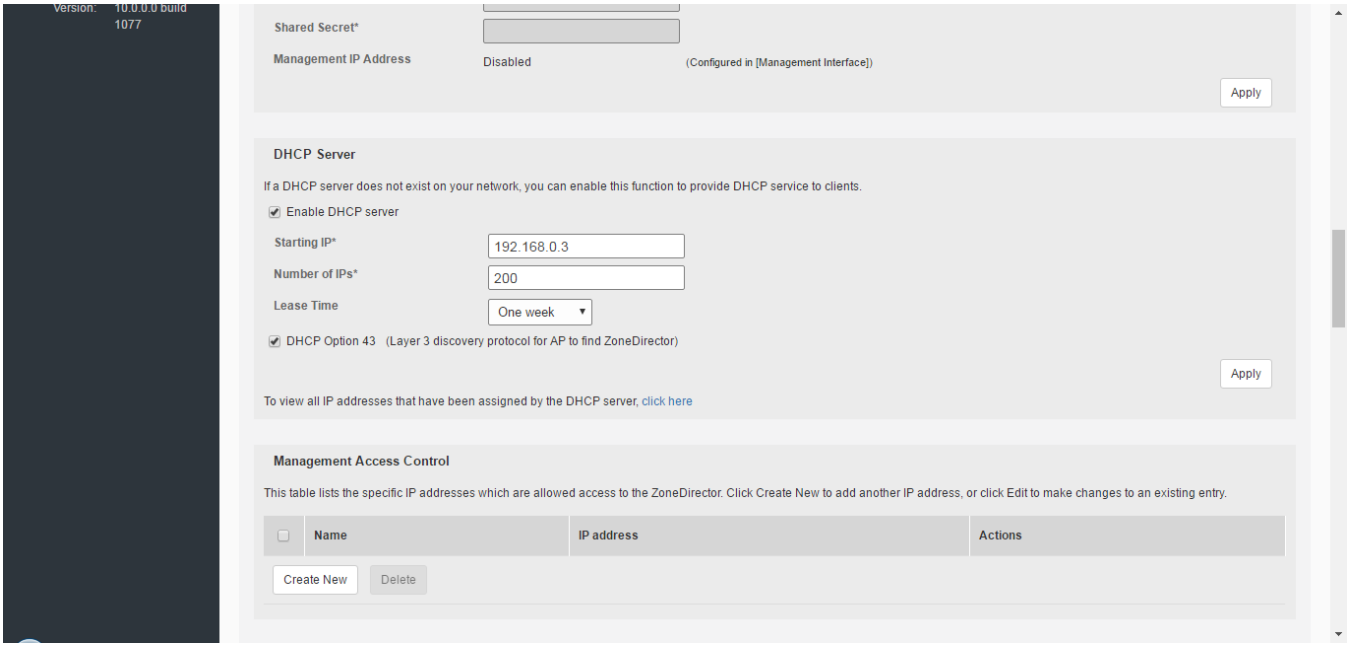
Enabling the Built-in DHCP server

Ruckus recommends that you only enable the built-in DHCP server if there are no other DHCP servers on the network.

ZoneDirector's internal DHCP server can service only a single subnet (the one it's in) and not other VLANs that may be associated with client WLANs. If you enable the built-in DCHP server, Ruckus also recommends enabling the rogue DHCP server detector. For more information, refer to Rogue DHCP Server Detection on page 278.

1. Go to **System > System Settings**.
2. In the **DHCP Server** section, select the **Enable DHCP Server** check box.
3. In **Starting IP**, type the first IP address that the built-in DHCP server will allocate to DHCP clients. The starting IP address must be on the same subnet as the IP address assigned to ZoneDirector. If the value that you typed is invalid, an error message appears and prompts you to let ZoneDirector automatically correct the value. Click **OK** to automatically correct the entry.
4. In **Number of IPs**, type the maximum number of IP addresses 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 ZoneDirector. The default value is 200.
5. In **Lease Time**, select a time period for which IP addresses will be allocated to DHCP clients. Options range from six hours to two weeks (default is one week).
6. If your APs are on different subnets from ZoneDirector, click the check box next to **DHCP Option 43** to enable Layer 3 discovery of ZoneDirector by the APs.
7. Click **Apply**. If you typed an invalid value in any of the text boxes, an error message appears and prompts you to let ZoneDirector automatically correct the value. Click **OK** to change it to a correct value.

FIGURE 232 The DHCP Server options

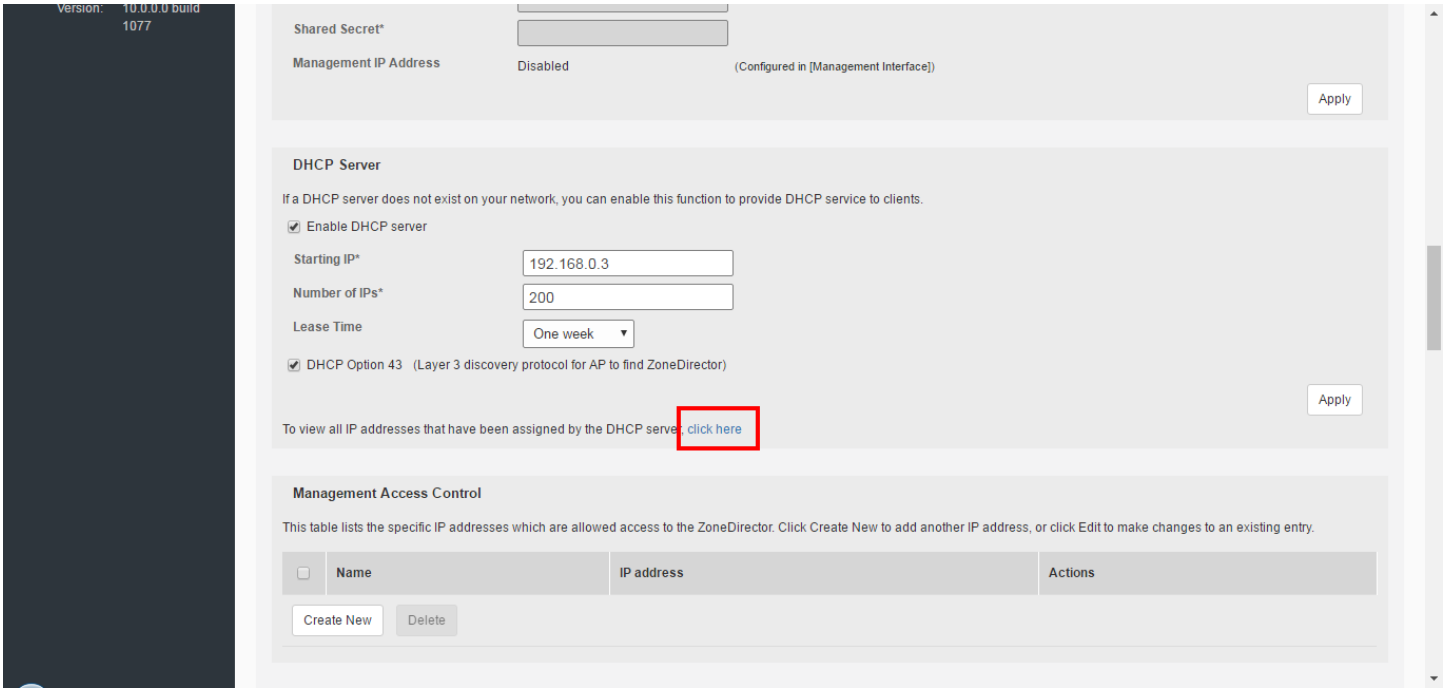


Viewing DHCP Clients

To view a list of current DHCP clients, click the **click here** link at the end of the "To view all currently assigned IP addresses that have been assigned by the DHCP server..." sentence. A table appears and lists all current DHCP clients with their MAC address, IP address and the remaining lease time.

You can clear DHCP leases on ZoneDirector by disabling and re-enabling the DHCP service.

FIGURE 233 To view current DHCP clients, click the "click here" link



Controlling ZoneDirector Management Access

The **Management Access Control** option can be used to control access to ZoneDirector's management interface.

The **Management Access Control** interface is located on the **System** > **System Settings** screen. Options include limiting access by subnet, single IP address and IP address range. When you create a management access control rule, all IP addresses and subnets other than those specifically listed will be blocked from accessing ZoneDirector's web interface.

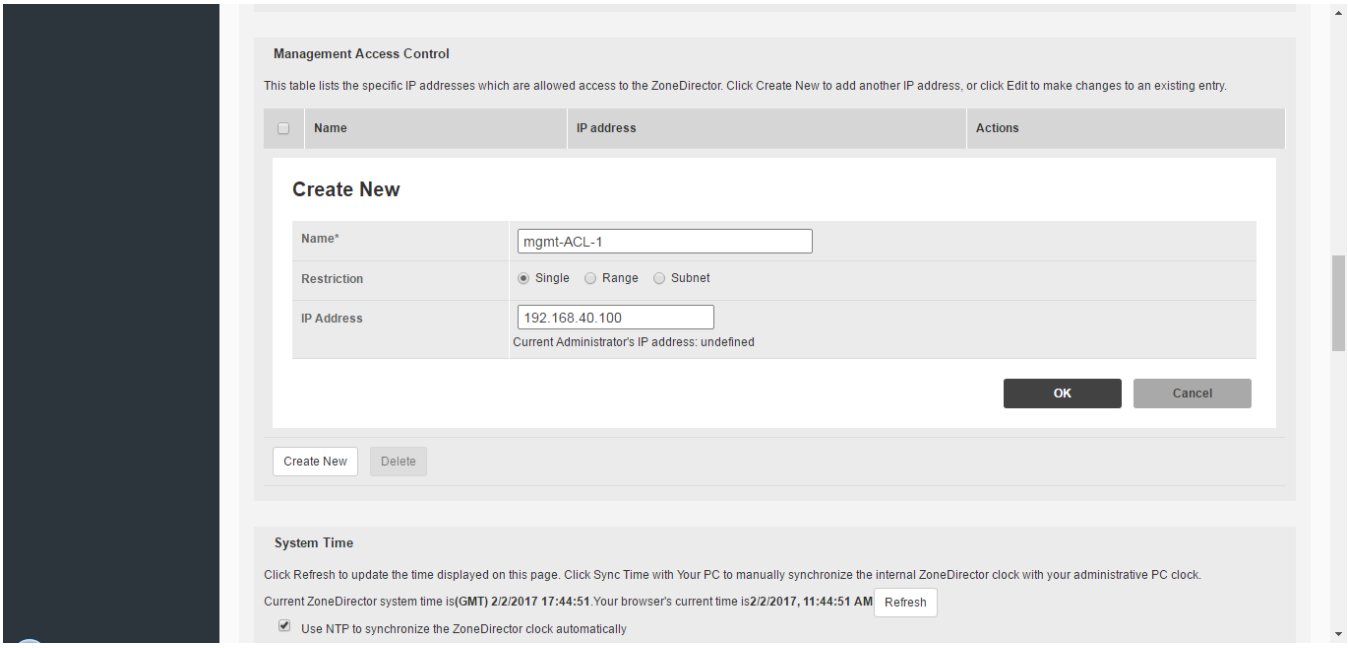
To restrict access to ZoneDirector's web interface:

1. Go to **System** > **System Settings**.
2. Locate the **Management Access Control** section, and click the **Create New link**.
3. In the **Create New** menu that appears, enter a name for the user(s) that you want to allow access to ZoneDirector's web interface.
4. Enter an IP address, address range or subnet. The administrator's current IP address is shown for convenience.

CAUTION
Be sure that you do not create an ACL that blocks the admin's own IP address from accessing the web interface.

5. Click **OK** to confirm. You can create up to 16 entries to the Management ACL.

FIGURE 234 Creating a new ZoneDirector management ACL



Setting the System Time

Many ZoneDirector features require that the controller 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.

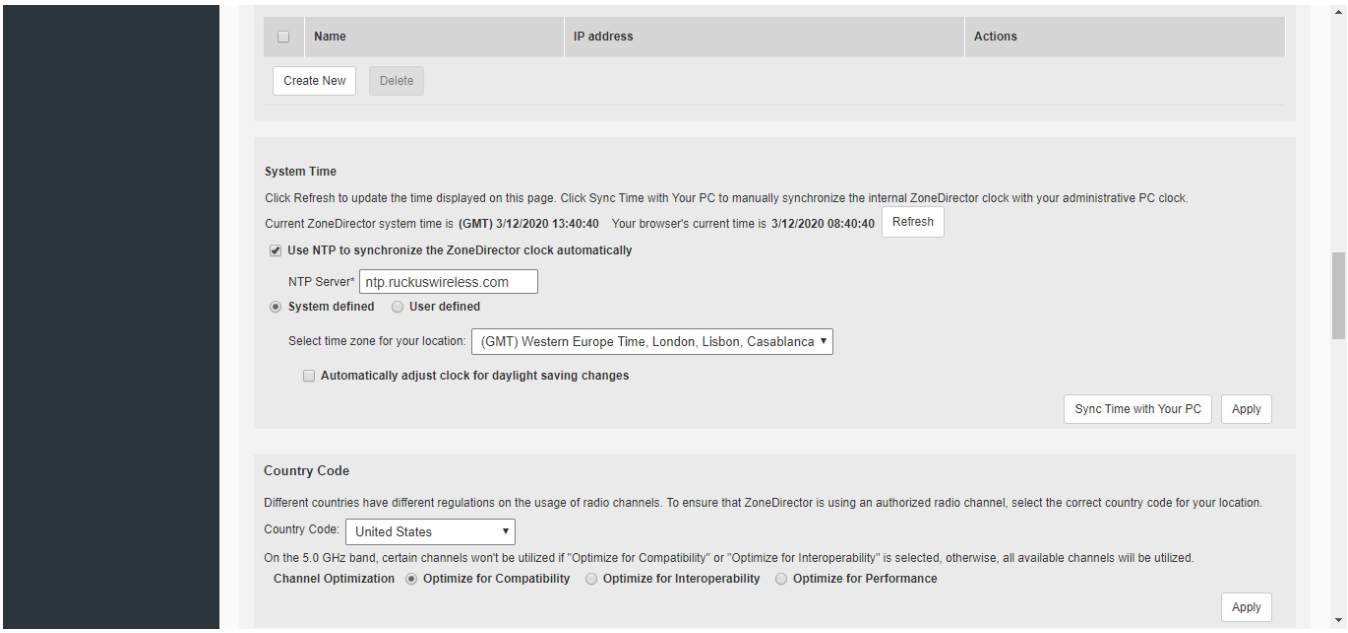
During the initial setup, the internal clock is automatically synchronized with the clock on your administration PC. You can use the web interface to check the current time on the internal clock, which shows up as a static notation in the Configure tab workspace. If this notation is incorrect, you can re-synchronize the internal clock to your PC clock immediately by clicking the **Sync Time with Your PC** button.

A preferable option is to link your ZoneDirector to an NTP server (as detailed below), which provides continual updating with the latest time.

1. Go to **System** > **System Settings**, and locate the *System Time* section.
2. Click **Refresh** to update the ZoneDirector display (a static snapshot) from the internal clock.
3. In **Sync Time with your PC**, if needed, click this to update the internal clock with the current time settings from your administration PC.
4. In **Use NTP server to synchronize the ZoneDirector clock automatically** (enabled by default), clear this check box to disable this option, or enter the DNS name or IP address of your preferred NTP server to use a different one.
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 304.
6. **Select time zone for your location**: Choose your time zone from the drop-down menu.
7. **Automatically adjust clock for daylight saving changes**: Enable to adjust for DST where applicable.

8. Click **Apply** to save any changes.

FIGURE 235 The System Time options



Configuring a User-Defined Time Zone

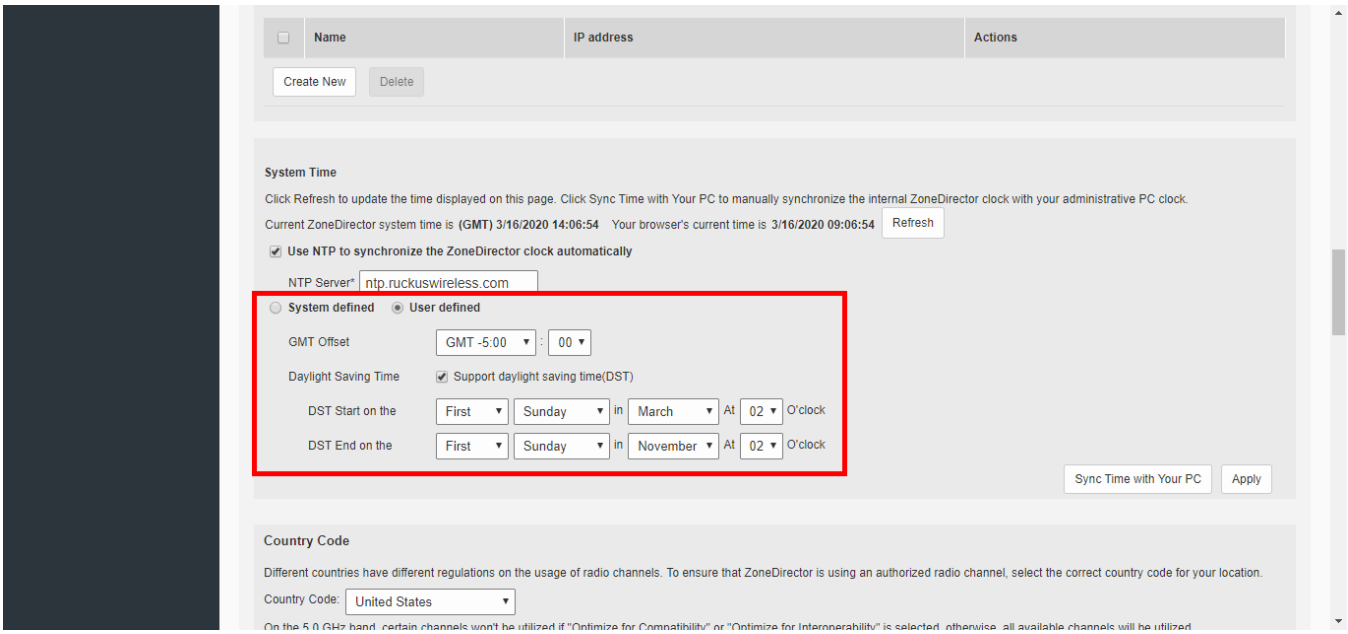
The user-defined time zone option allows admins to customize the time zone and daylight savings time start and end times.

To configure a user-defined time zone:

1. Go to **System > System Settings**, and locate the *System Time* section.
2. Enable **Use NTP to synchronize the ZoneDirector 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 236 User-defined time zone



Setting the Country Code

Different countries and regions maintain different rules that govern which channels can be used for wireless communications.

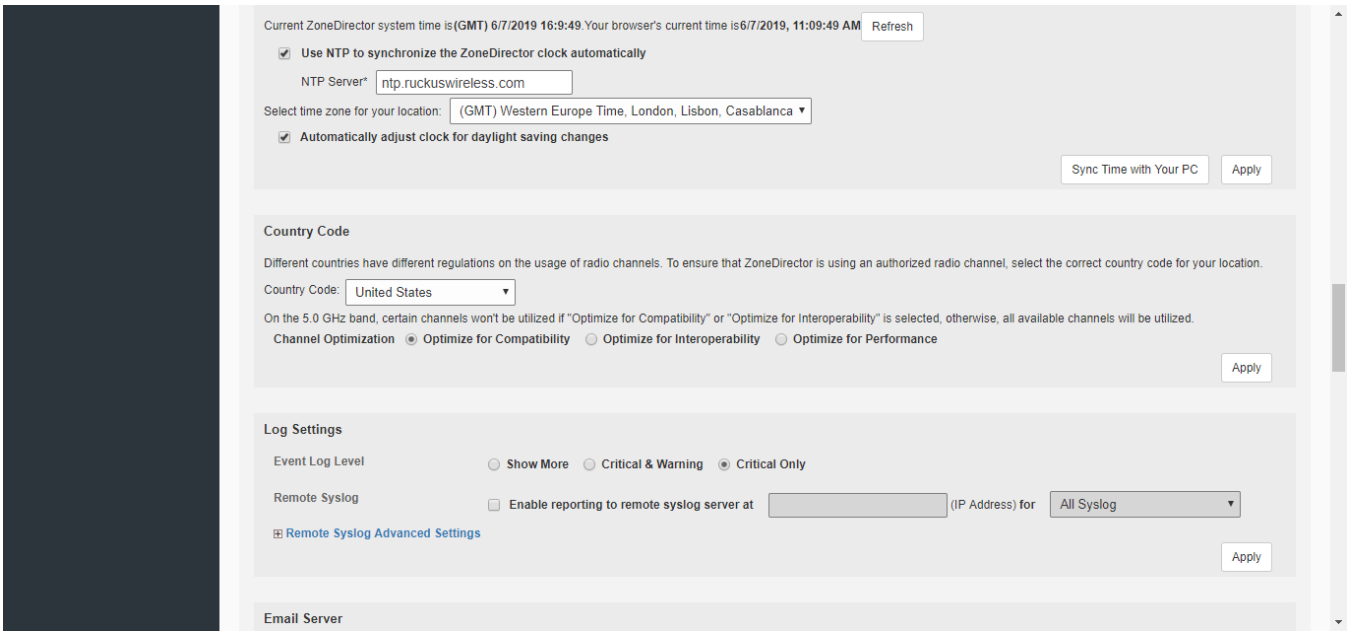
Setting the Country Code to the proper regulatory region ensures that your wireless network does not violate local and national regulatory restrictions. ZoneDirector's web interface can be used to define the country code for all APs under its control.

To set the Country Code to the proper location:

1. Go to **System** > **System Settings**.
2. Locate the **Country Code** section, and choose your location from the pull-down menu.

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

FIGURE 237 The Country Code settings



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
Note that these settings only affect Ruckus APs that support the extended DFS channel list.

Channel Optimization settings are described in the following table.

TABLE 27 Channel Optimization settings for US Country Code

Setting	Description	Use this setting when
Optimize for Compatibility	DFS-capable 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 APs that do not support DFS channels in a Smart Mesh configuration.
Optimize for Interoperability	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	APs can use all available DFS and non-DFS channels, without regard for compatibility or interoperability.	You have only DFS-capable APs in your deployment, you are not concerned with DFS compatibility of client devices, and you want to make the maximum use of all available channels.

NOTE
If you are located in the United States and have a DFS-capable AP that is expected to serve as an uplink AP with a non-DFS-capable Mesh AP as its downlink, you will need to set the Channel Optimization setting to "Optimize for Compatibility." This is due to the DFS-capable AP's ability to use more channels than the non-DFS-capable APs, which could result in the uplink choosing a channel that is not available to the mesh AP. Alternatively, manually set the channel for the Root AP to one of the non-DFS channels. Specifically, choose one of the following channels: 36, 40, 44, 48, 149, 153, 157, 161, 165.

The 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, including 100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140.

Configuring System Log Settings

ZoneDirector maintains an internal log of current events and alarms.

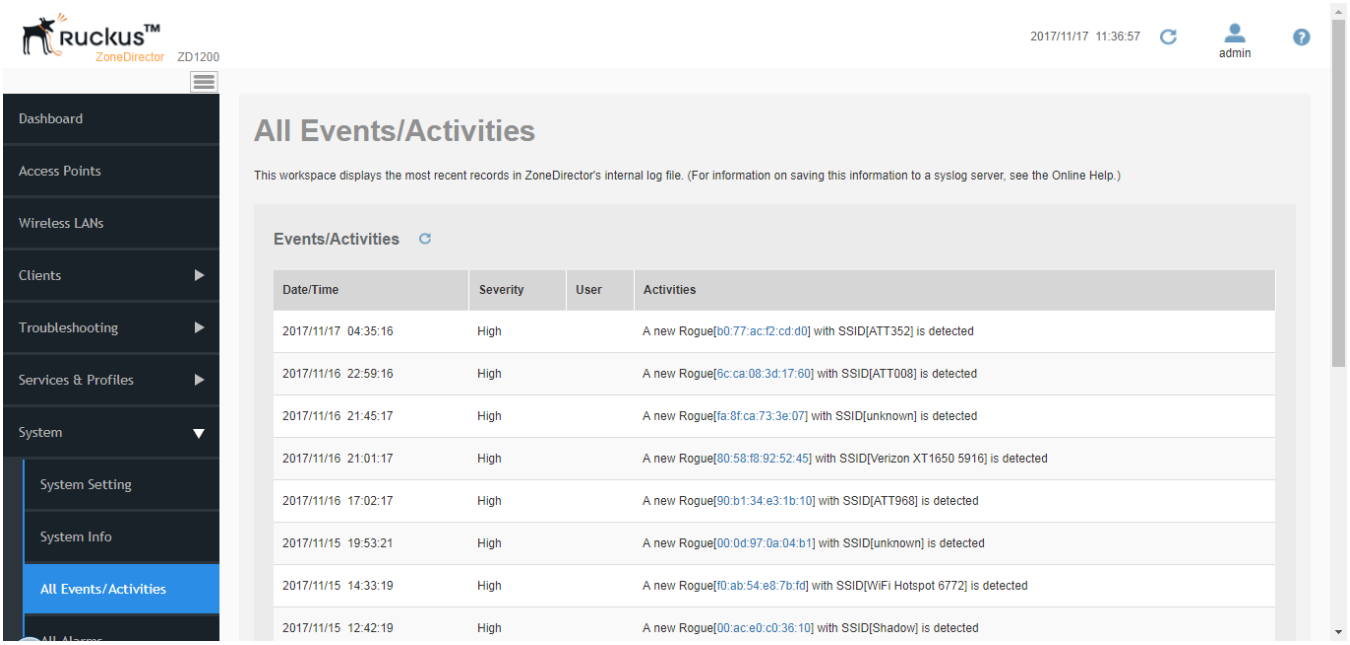
This file has a fixed capacity; at a certain level, ZoneDirector will start deleting the oldest entries to make room for the newest. This log is volatile, and the contents will be deleted if ZoneDirector is powered down. If you want a permanent record of all logging activities, you can set up your syslog server to receive log contents from ZoneDirector, and then use the web interface to direct all logging to the syslog server.

Reviewing the Current Log Contents

1. Go to **System** > **All Events/Activities**
2. Review the events and alarms listed below. Log entries are listed in reverse chronological order (with the latest logs at the top of the list).
3. Click a column header to sort the contents by that category.

4. Click any column twice to switch chronological or alphanumeric sorting modes.

FIGURE 238 The All Events/Activities page



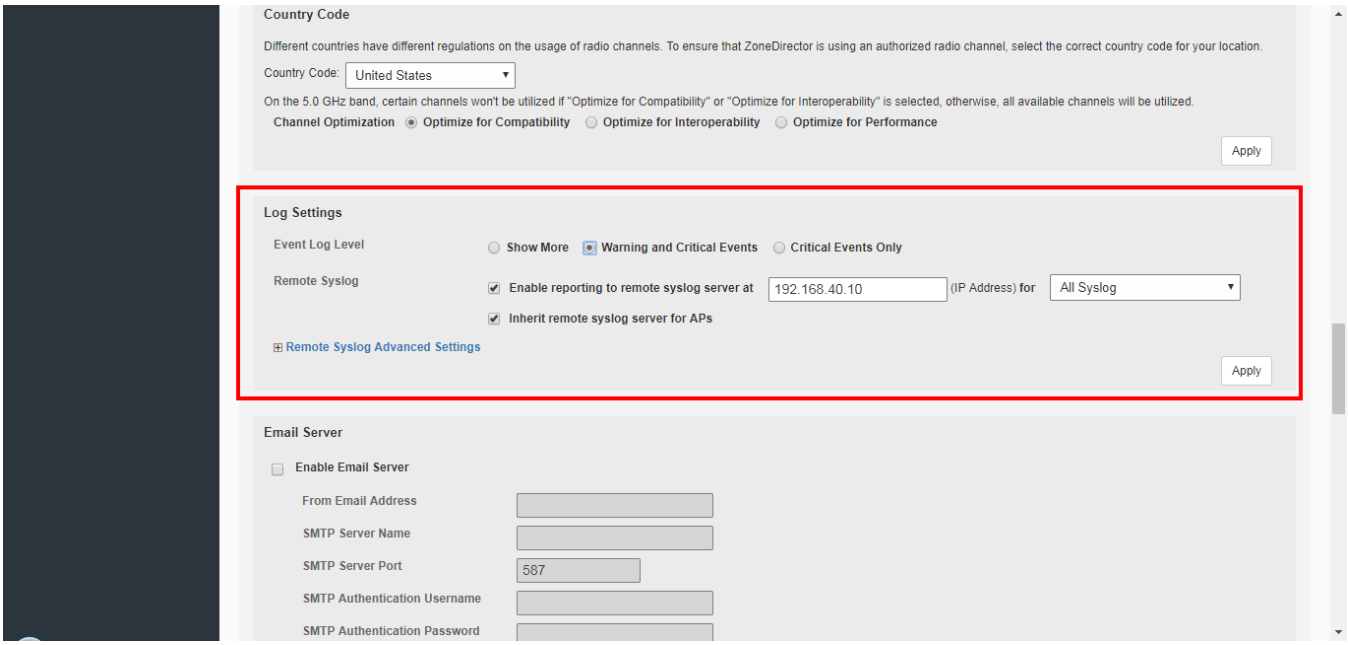
Customizing the Current Log Settings

Customize the log settings to control which categories and severity levels of event logs to collect and where to send them.

1. Go to **System** > **System Settings**.
2. Scroll down to the **Log Settings** section.
3. In **Event Log Level**, select one of the three logging levels: “Show More,” “Warning and Critical Events,” or “Critical Only.”
4. To enable event log delivery to a syslog server, enable the **Enable reporting to remote syslog server at** option in **Remote Syslog**.
5. Enter the **IP address** of the syslog server in the (IP address) box provided.
6. Select whether the logs will contain all syslog events or client connection events only:
   - **All Syslog**: ZoneDirector sends all syslog messages configured in the *Debug Logs* section of the *Troubleshooting* > *Diagnostics* page.
   - **Client Connection Logs Only**: ZoneDirector sends client connection event logs only to the syslog server.
   - **Client Flow Data Only**: ZoneDirector sends client flow data only to the syslog server.
7. **Inherit remote syslog server for APs __ (IP Address)**: Enabling this feature allows ZoneDirector 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, ZoneDirector 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.

8. Click **Apply** to save your settings. The changes go into effect immediately.

FIGURE 239 The Log Settings options



Configuring Remote Syslog Advanced Settings

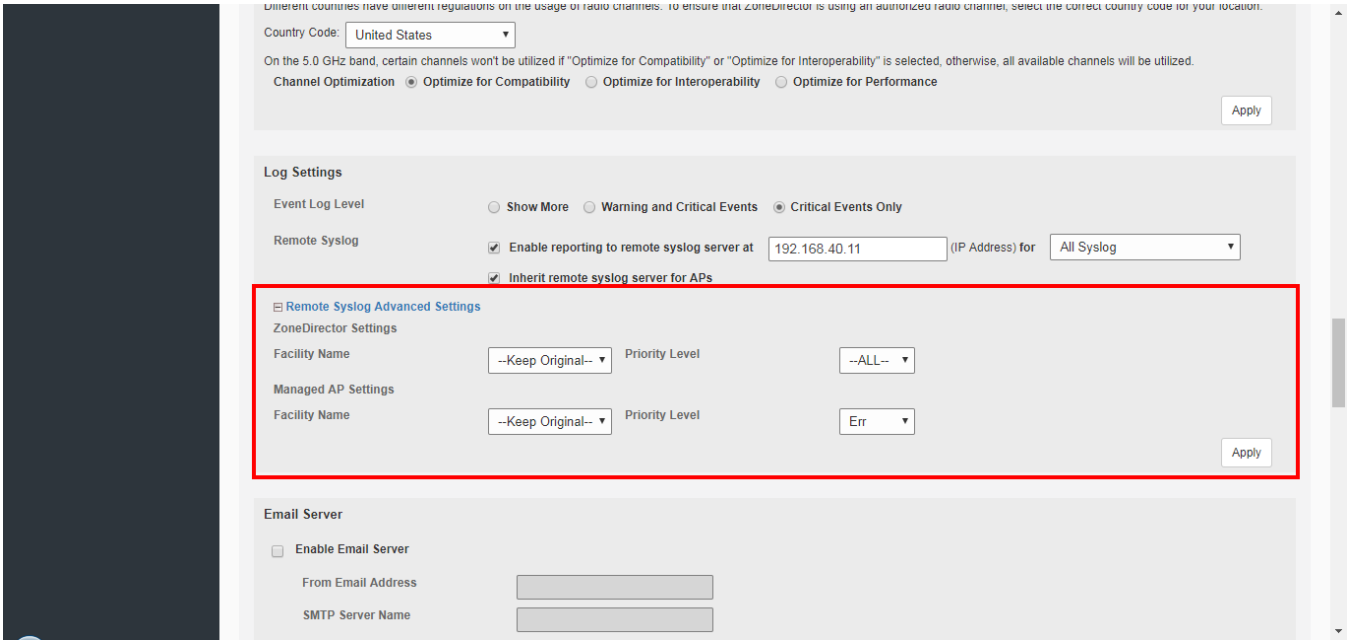
Advanced Syslog settings allow you to override the default Facility Name and Priority Level of messages sent to the syslog server. In this way, users can separate different kinds of syslogs according to the facility name on the syslog server side.

To configure remote syslog advanced settings:

1. Go to **System** > **System Settings**.
2. Scroll down to **Log Settings**, and expand the **Remote Syslog Advanced Settings** section.
3. In **ZoneDirector Settings**, set the facility name as follows:
   - **Keep Original**: Retain the original facility name.
   - **local0** - **local7**: Specify facility name.
4. Set the priority level as follows:
   - **All**: Include all syslog messages.
   - 0(emerg), 1(alert), 2(crit), 3(err), 4(warning), 5(notice), 6(info), 7(debug): Lower numbers indicate higher priority. The syslog server will only receive logs whose priority levels are the same as or higher than the configured level.

5. Repeat step 4 for **Managed AP Settings**. ZoneDirector and Access Points can use different facility and priority settings. All managed APs share the same facility and priority settings.

FIGURE 240 Remote Syslog Advanced Settings



Configuring Syslogs for Firewall Integration

If enabled, ZoneDirector generates syslog messages upon acquisition, update or deletion of an IP address by a wireless station, which allows for enhanced integration with third-party firewall products for implementing client-specific security rules.

Station information is conveyed through a syslog message containing the following information: IPv4/v6 address, User name, MAC address, Operation Type (Add, Update, Del), AP/ZD MAC, OS Type.

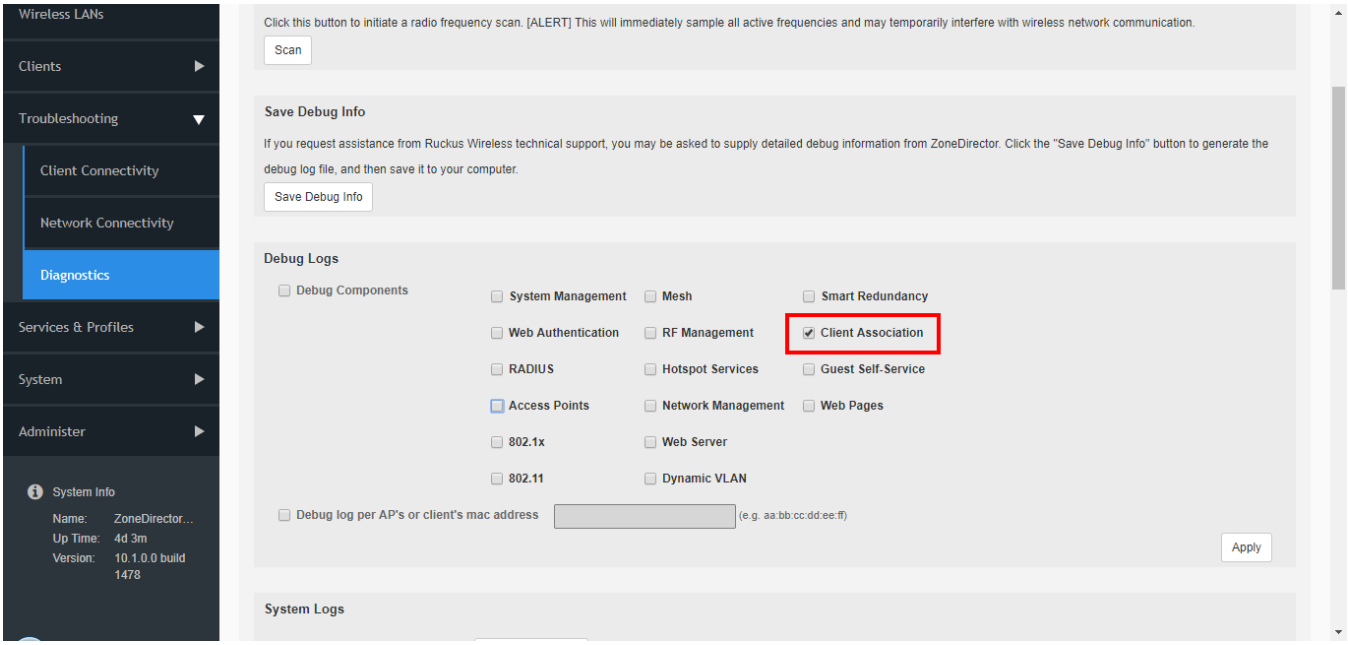
To enable inclusion of client association logs in syslog messages:

1. Go to **Troubleshooting** > **Diagnostics**.
2. In *Debug Logs*, select the **Client Association** check box.

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

NOTE
You must also ensure that syslog delivery is enabled on the *System > System Settings > Log Settings* page and that the **Priority** level in *Remote Syslog Advanced Settings* is set to **Info** or **All**.

FIGURE 241 Enable client association logs in syslog for firewall integration



User Data Flow

The flow of user data from the end point to the firewall will use the following path:

1. The user authenticates to an authentication server via the AP.
2. ZoneDirector verifies the user's identity.
3. After the station authenticates successfully and gets an IP address, ZoneDirector generates a syslog message.
4. The log is sent to a syslog server in real time.
5. The script on the syslog server extracts user information from the log message and sends it to the firewall.

   A similar flow can be used to remove user mappings if the station sends a disconnect message.

Log Format

The log format consists of the following fields:

- **operation**: Indicates whether to add, delete or update client association information.
- **sta_ip**: Indicates the IP address of station.
- **sta_name**: Indicates the station's account name supplied by the client when being authenticated. The user name is used for 802.1X and Web Auth WLANs. The MAC address of the client will be used as the user name for Open, MAC Address and 802.1X + MAC Address WLAN types.

- **sta_mac**: The station's MAC address.
- **sta_oriip**: Only takes effect when the operation is "update" in order to indicate the original IP of the station.
- **ap_mac**: Shows the MAC address of the AP to which the station is currently connected.
- **seq**: Indicates the sequence number of the log message. It is increased by one after a log is sent. The UDP packet can be adjusted to the right order by this field in the log server.
- **sta_ostype**: Indicates the station's OS type. Will be filled with "unknown" if the OS type is unobtainable.

Examples

- Add

```
operation=add;seq=1;sta_ip=192.168.120.16;sta_mac=60:36:dd:19:17:ac;zd/
ap=00:0c:29:11:5a:0b/58:93:96:29:4c:60;sta_ostype=Windows7/
Vista;sta_name=60:36:dd:19:17:ac;stamgr_handle_remote_ipc
```

- Delete

```
operation=del;seq=4;sta_ip=192.168.120.30;sta_mac=60:36:dd:19:17:ac;zd/
ap=00:0c:29:11:5a:0b/58:93:96:29:4c:60;sta_ostype=Windows 7/
Vista;sta_name=60:36:dd:19:17:ac;stamgr_sta_log_disconnect
```

- Update

```
operation=update;seq=2;sta_ip=192.168.120.30;sta_oriip=
192.168.120.16;sta_mac=60:36:dd:19:17:ac;zd/ap=00:0c:29:11:5a:0b/
58:93:96:29:4c:60;sta_ostype=Windows 7/
Vista;sta_name=60:36:dd:19:17:ac;stamgr_handle_remote_ipc
```

Setting Up Email Alarm Notifications

If an alarm condition is detected, ZoneDirector will record it in the event log. If you prefer, an email notification can be sent to a configured email address of your choosing.

To activate this option, follow these steps:

1. Go to **System** > **Email Alarm Settings**.
2. To enable email notification, select the **Send an email message when an alarm is triggered** check box.
3. Enter the recipient email address in the **Email Address** box provided, and click **Apply**.
4. Go to **System** > **System Settings**, and scroll down to the **Email Server** section.

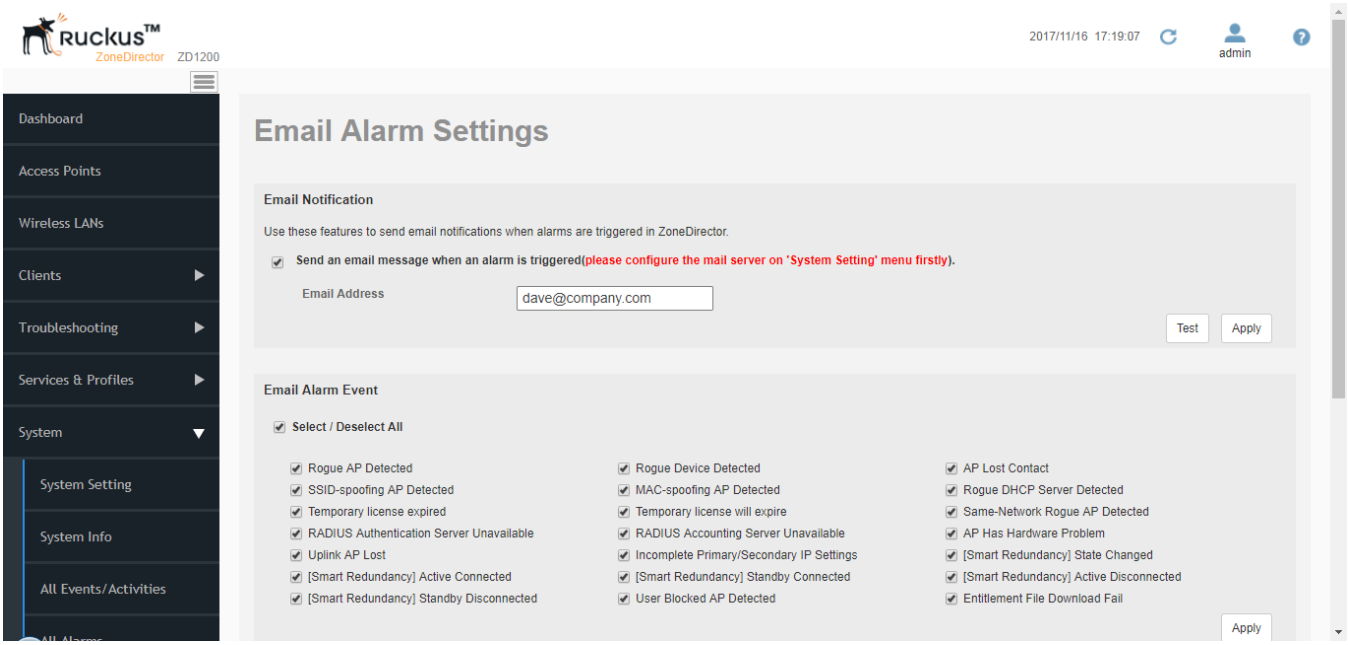
5. Configure the settings listed in the following **SMTP settings for email notification** table.

SMTP Setting	Description
From email address	Type the email address from which ZoneDirector will send alarm 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**. For Hotmail addresses, the SMTP server name is smtp.live.com.
SMTP Server Port	Type the SMTP port number provided by your ISP or mail administrator. Often, the SMTP port number is **25** 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. If using a Yahoo! email account, **STARTTLS** must be disabled. If using a Hotmail account, both **TLS** and **STARTTLS** must be enabled.

6. To verify that ZoneDirector can send alarm messages using the SMTP settings you configured, click the **Test** button.
   - If ZoneDirector is able to send the test message, the message **Success!** appears at the bottom of the Email Notification page. Continue to Step 7.
   - If ZoneDirector is unable to send the test message, the message **Failed!** appears at the bottom of the **Email Notification** page. Go back to Step 5, and then verify that the SMTP settings are correct.

7. Click **Apply**. The email notification settings you configured become active immediately.

FIGURE 242 The Alarm Settings page



NOTE
If the **Test** button is clicked, ZoneDirector will attempt to connect to the mail server for 10 seconds. If it is unable to connect to the mail server, it will stop trying and quit.

NOTE
When the alarm email is first enabled, the alarm recipient may receive a flood of alarm notifications. This may cause the mail server to treat the email notifications as spam and to temporarily block the account.

NOTE
ZoneDirector sends email notifications for a particular alert only once, unless (1) it is a new alert of the same type but for a different device, or (2) existing alert logs are cleared.

Customizing Email Alarms

Using the Alarm Event section of the **System** > **Email Alarm Settings** page, you can choose which types of events will trigger ZoneDirector to send an email notification.

1. Click **Select/Deslect All** to select/deselect all alarm types.
2. Select or deselect those for which you want or don't want to receive emails.

3. Click **Apply** to save your changes. When any of the selected events occur, ZoneDirector sends an email notification to the email address that you specified in the section.

> **NOTE**
> With the exception of the *Lost contact with AP* event, ZoneDirector only sends one email alarm notification for each event. If the same event happens again, no alarm will be sent until you clear the alarm on the *System* > *All Alarms* page. On the other hand, ZoneDirector sends a new alarm notification each time the *Lost contact with AP* event occurs.

Configuring SMS Settings for SMS Guest Pass Delivery

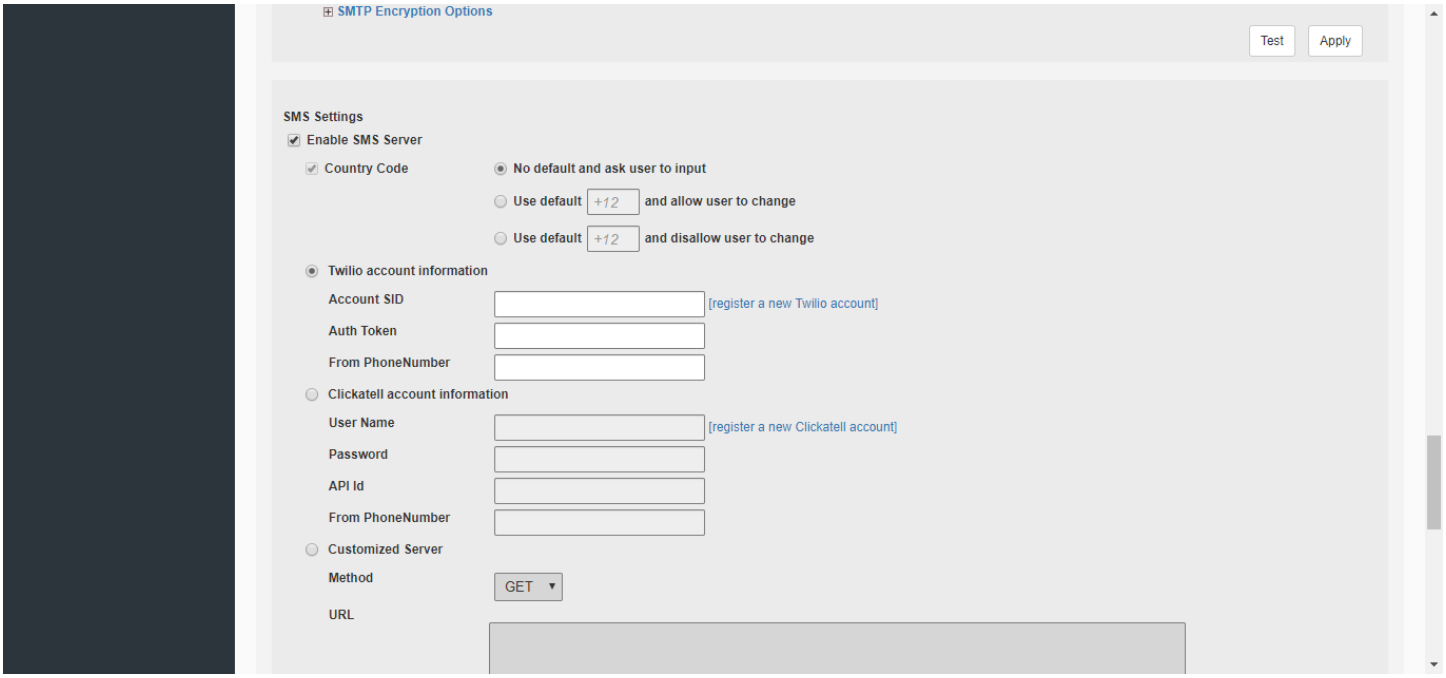
If you want to deliver Guest Passes to your guests via SMS, you can configure ZoneDirector to use an existing third-party SMS delivery service account for SMS delivery.

The first step is to inform ZoneDirector of the account information for your Twilio, Clickatell, or other SMS service provider account.

1. Go to **System** > **System Settings**.
2. Locate the **SMS Settings** section, and enable the check box next to **Enable SMS Server**.
3. In **Country Code**, select one of the following options:
   - **Country Code**: 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.

You can now allow guest pass generators to deliver guest pass codes to guests using the SMS button when generating a new guest pass. (You must also enter a phone number for receiving the SMS messages for each guest pass created.).

FIGURE 243 Configuring SMS Settings



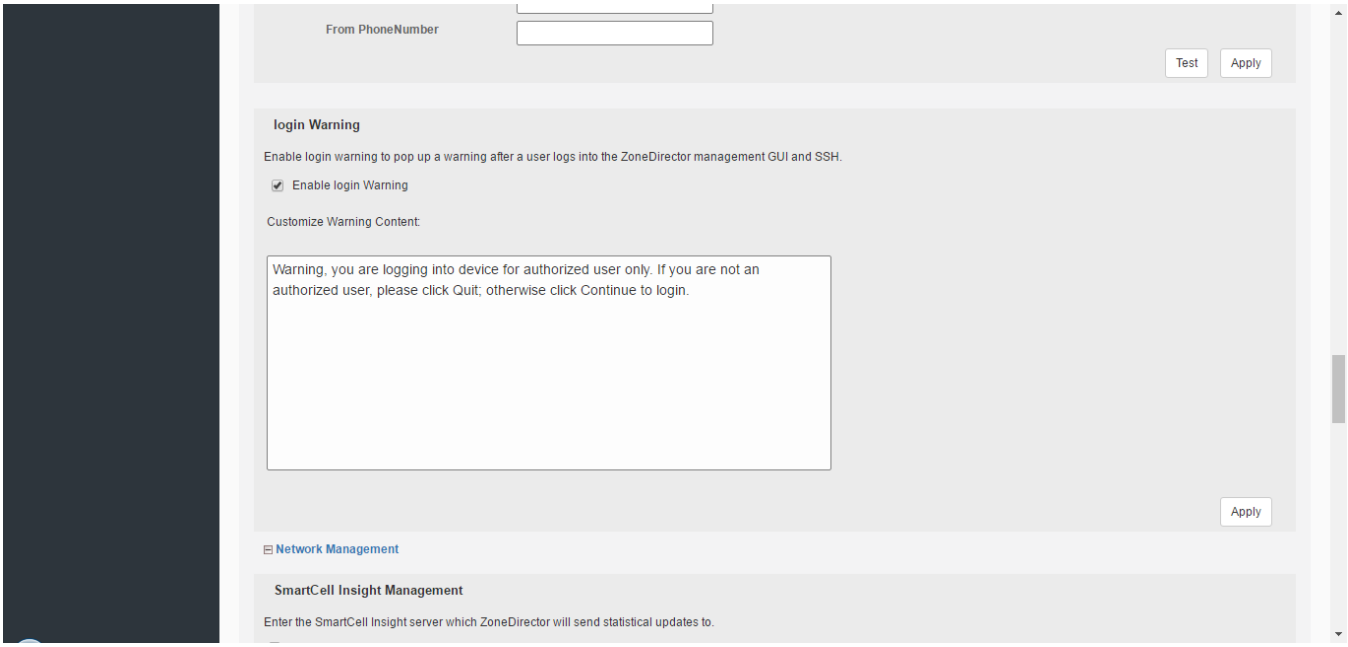
Enabling Login Warning Messages

If you want to display a warning message upon login to the ZoneDirector web UI or CLI, you can do so using the following procedure:

1. Go to **System** > **System Settings**, and scroll down to the **Login Warning** section.
2. Click **Enable login warning**, and replace the text in the **Customize warning content** text box according to your preferences.

3. Click **Apply** to save your changes. The next time a user attempts to login to ZoneDirector, they will be presented with the warning message you configured.

FIGURE 244 Enabling and configuring a login warning message



Configuring Dashboard Map Settings

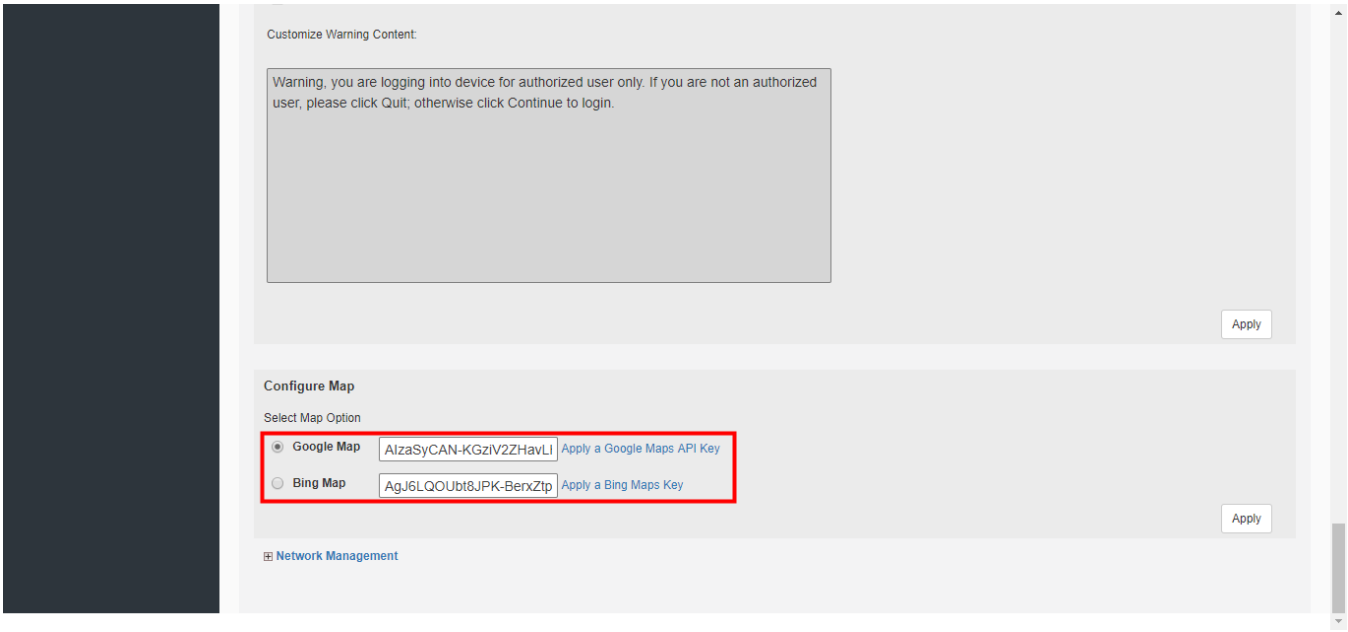
The Dashboard Health overview map requires the import of either a Google Maps or Bing Maps API key.

To configure the Dashboard map, use the following procedure:

1. Go to **System > System Setting**, and scroll down to the **Configure Map** section.
2. Select either **Google Map** or **Bing Map**, and enter your Google or Bing maps API key. If you do not have an API key, click the link to either the Google or Microsoft developer site, where you can apply for an API key.
3. Follow the instructions on the developer site to generate an API key, and copy/paste the key into the **Configure Map** text field.

4. Click **Apply** to import your API key. If successful, the Dashboard will now display a world map from either Google Maps or Bing Maps. You can display the locations of your APs on this map using the **Access Points** configuration page.

FIGURE 245 Configuring Google Maps or Bing Maps for Dashboard world map display



Enabling Network Management Systems

ZoneDirector supports several external network management options including Ruckus SmartCell Insight, Northbound Portal, Unleashed Multisite Manager (UMM), SNMPv2, SNMPv3 and Telnet. These options are configured from the **System** > **System Settings** page by expanding the **Network Management** link.

The following section describes how to enable these network management systems.

Enabling SmartCell Insight Communication

If your ZoneDirector will be used as a data source for Ruckus SmartCell Insight (SCI) analytics engine, you can enable the SmartCell Insight Management feature to allow ZoneDirector to initiate communications with SCI at set 15 minute intervals. In this way, if ZoneDirector is behind a firewall or NAT device, it can still communicate with SCI without having to reconfigure your firewalls and NAT devices to allow SCI to contact the ZoneDirector.

This feature only needs to be enabled if ZoneDirector is inaccessible by SCI (e.g., ZoneDirector is behind a firewall/NAT device). Otherwise, configuration only needs to be done on SCI.

NOTE
This feature is compatible with SCI version 2.0 and later.

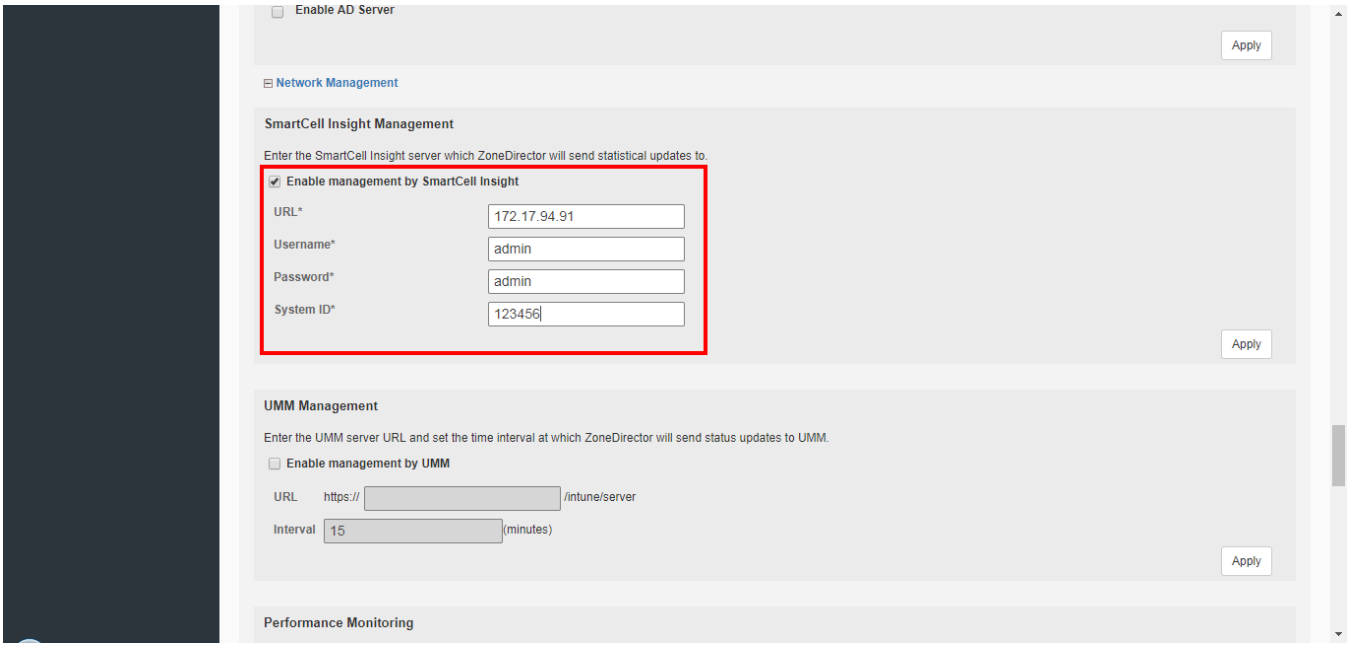
NOTE
Beginning in release 10.2, ZoneDirector can also send application recognition statistics to SCI for analysis, for monitoring application reports such as top applications by client count and top applications by traffic volume. You must enable Application Recognition & Control for any WLANs for which you want to report application data (**Wireless LANs > Create/Edit > Advanced Options > Application Recognition & Control > Enable**).

NOTE
SCI server version 5.1.1 and later is required to support ARC data.

To enable SmartCell Insight Management:

1. Go to **System** > **System Settings**, and expand the **Network Management** section.
2. Enable the check box next to **Enable management by SmartCell Insight**.
3. Enter the following information for your SCI system:
   - **URL**: Enter the SCI URL (e.g., https://[SCI IP address]/pentaho/Home)
   - **User Name**: Enter the SCI login user name used for ZD-SCI communications.
   - **Password**: Enter the SCI login password used for ZD-SCI communications.
   - **System ID**: Enter the System ID that you used for the ZD data source on the SCI System Setup page (see *SCI User Guide* for details).
4. Click **Apply** to save your changes.

FIGURE 246 Config SCI server



Enabling Management via UMM

If you have a Ruckus Unleashed Multi-site Manager (UMM; formerly known as FlexMaster) server installed on the network, you can enable UMM management to centralize monitoring and administration of multiple ZoneDirector controllers and other supported Ruckus devices.

This version of ZoneDirector supports the following UMM-deployed tasks:

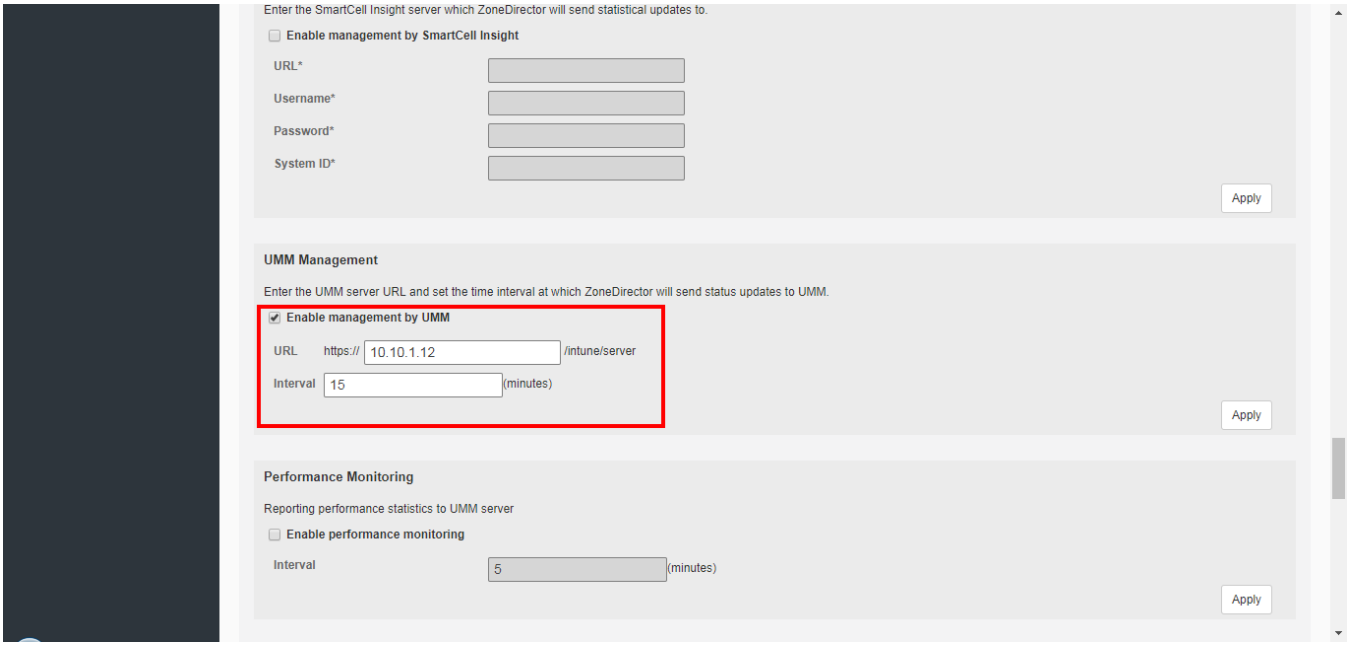
- Firmware upgrade for both ZoneDirector and the APs that report to them
- Reboot
- Backup of ZoneDirector settings
- Performance monitoring

When the UMM management option is enabled, you will still be able to access the ZoneDirector web interface to perform other management tasks. By default, UMM management is disabled.

To enable UMM management:

1. Click **System** > **System Settings**.
2. Scroll down to the bottom of the page.
3. Click the **Network Management** link to expand the section.
4. Under **UMM Management**, select the **Enable management by UMM** check box.
5. In **URL**, type the **UMM DNS** host name or IP address of the UMM server.
6. In **Interval**, type the time interval (in minutes) at which ZoneDirector will send status updates to the UMM server. The default interval is 15 minutes
7. Click **Apply**. The message **Setting Applied** appears.

FIGURE 247 Unleashed Multi-site Manager (UMM) management options



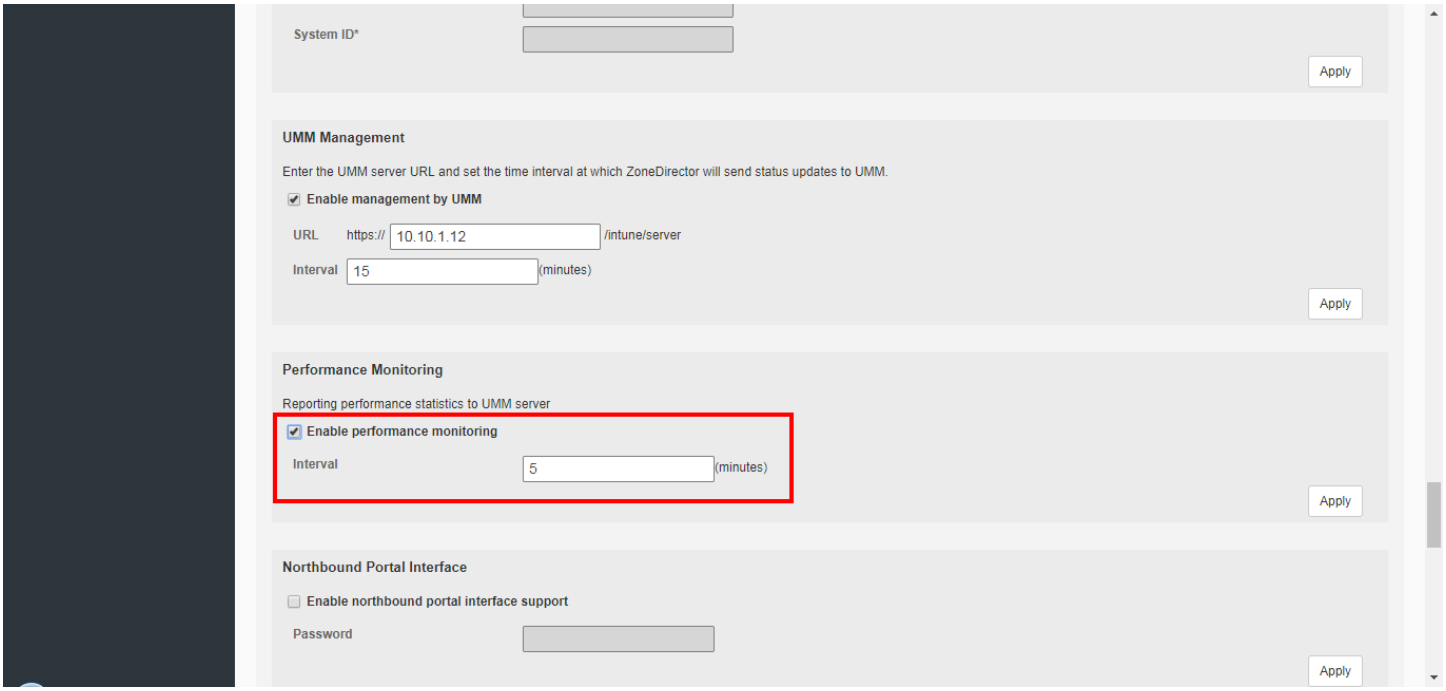
You have completed enabling UMM management on ZoneDirector. For more information on how to configure ZoneDirector from the UMM web interface, refer to the UMM documentation, available from *https://suppport.ruckuswireless.com*.

Monitoring ZoneDirector Performance from UMM

If you want to monitor ZoneDirector's performance statistics from UMM, select **Enable Performance Monitoring**, enter an update interval, and click **Apply**.

This option is disabled by default.

FIGURE 248 Enable UMM performance monitoring



Enabling Northbound Portal Interface Support

The Northbound Portal interface allows the use of DPSKs on open authentication WLANs meant for public access.

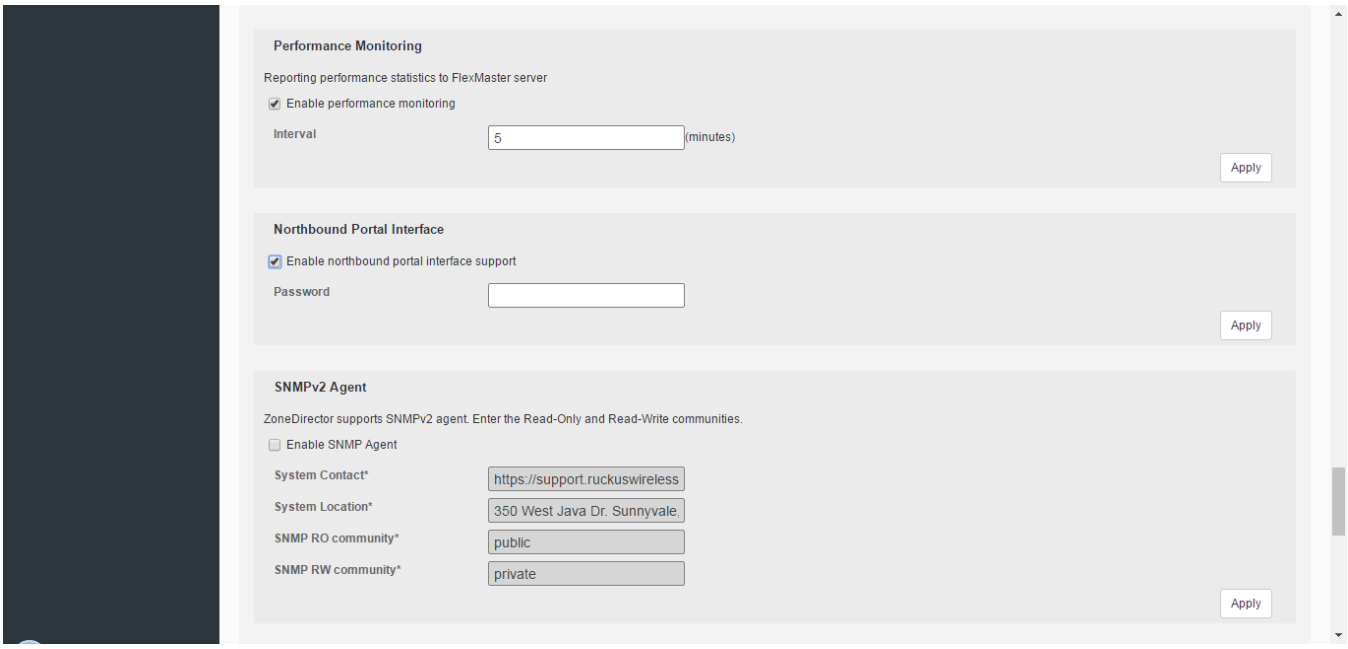
By enabling the Northbound Portal Interface, a wireless service provider can provide simple but secure Wi-Fi access without pre-registration, account setup or authentication. ZoneDirector redirects authentication requests to an outside portal. If access is granted, ZoneDirector provides a unique dynamic PSK. The DPSK can be delivered in a prov.exe file, which automatically configures the user's device with the relevant wireless settings or displayed on the portal screen for manual entry.

To enable Northbound Portal interface support:

1. Go to **System** > **System Settings** > **Network Management**.
2. Click **Enable northbound portal interface support**.
3. Enter a **Password** for API to portal communication.
4. Click **Apply** in the same section to save changes.

5. Configure the portal to display the key to the user or to push the prov.exe file to the client.

FIGURE 249 Enabling Northbound Portal interface



Configuring SNMP Support

ZoneDirector provides support for Simple Network Management Protocol (SNMP v2 and v3), which allows you to query ZoneDirector information such as system status, WLAN list, AP list, and clients list, and to set a number of system settings using a Network Management System (NMS) or SNMP MIB browser.

You can also enable SNMP traps to receive immediate notifications for possible AP and client issues.

Enabling the SNMP Agent

The procedure for enabling ZoneDirector's 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 ZoneDirector with SNMPv3 enabled. For a list of the MIB variables that you can get and set using SNMP, check the related SNMP documentation on the Ruckus Support site at *http://support.ruckuswireless.com/documents*.

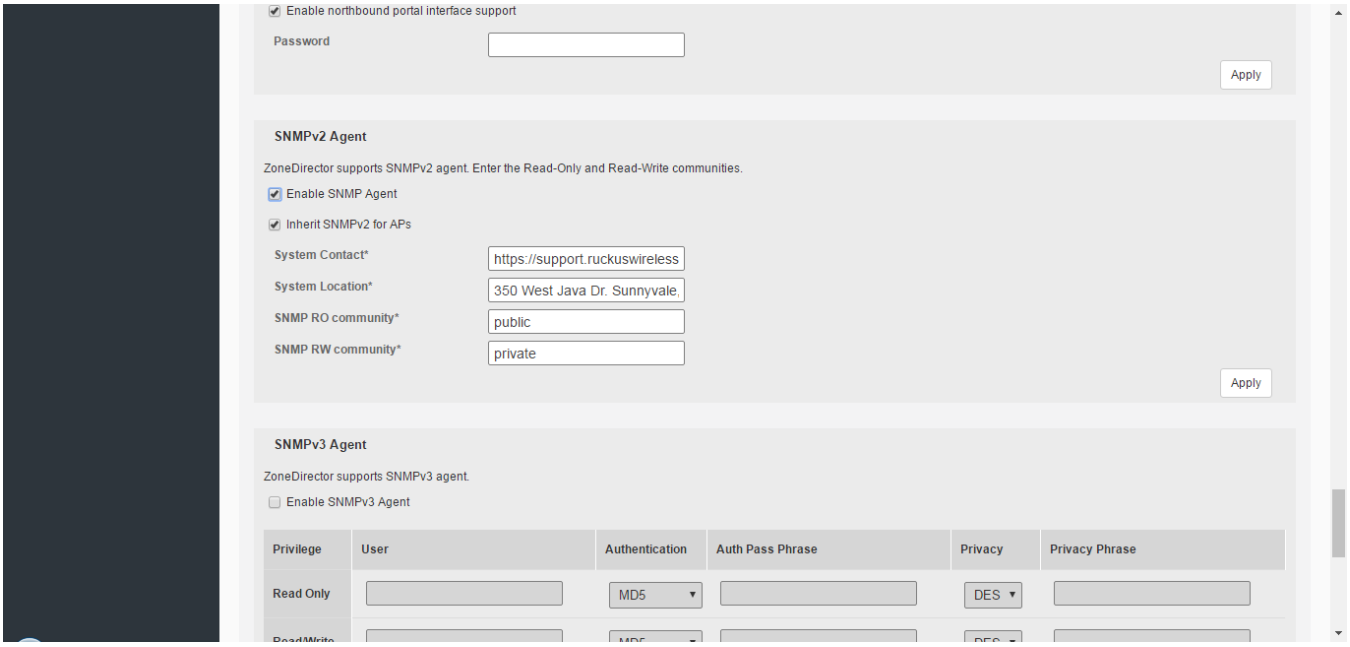
If your network uses SNMPv2

To enable SNMPv2 management:

1. Go to **System** > **System Settings**. Scroll down to the bottom of the page and click the **Network Management** link to open the **Network Management** section.
2. Under the **SNMPv2 Agent** section, select the **Enable SNMP Agent** check box.

3. When the SNMPv2 Agent is enabled, the Inherit SNMPv2 for APs option appears. This option is enabled by default. Disabling it allows you to disable SNMP traps on all APs.
4. Enter the following information:
   - In **SNMP RO community** (required), set the read-only community string. Applications that send SNMP Get-Requests to ZoneDirector (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 ZoneDirector (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**.
   - In **System Contact**, type your email address (optional).
   - In **System Location**, type the location of the ZoneDirector device (optional).
5. Click **Apply** to save your changes.

FIGURE 250 Enabling the SNMPv2 agent



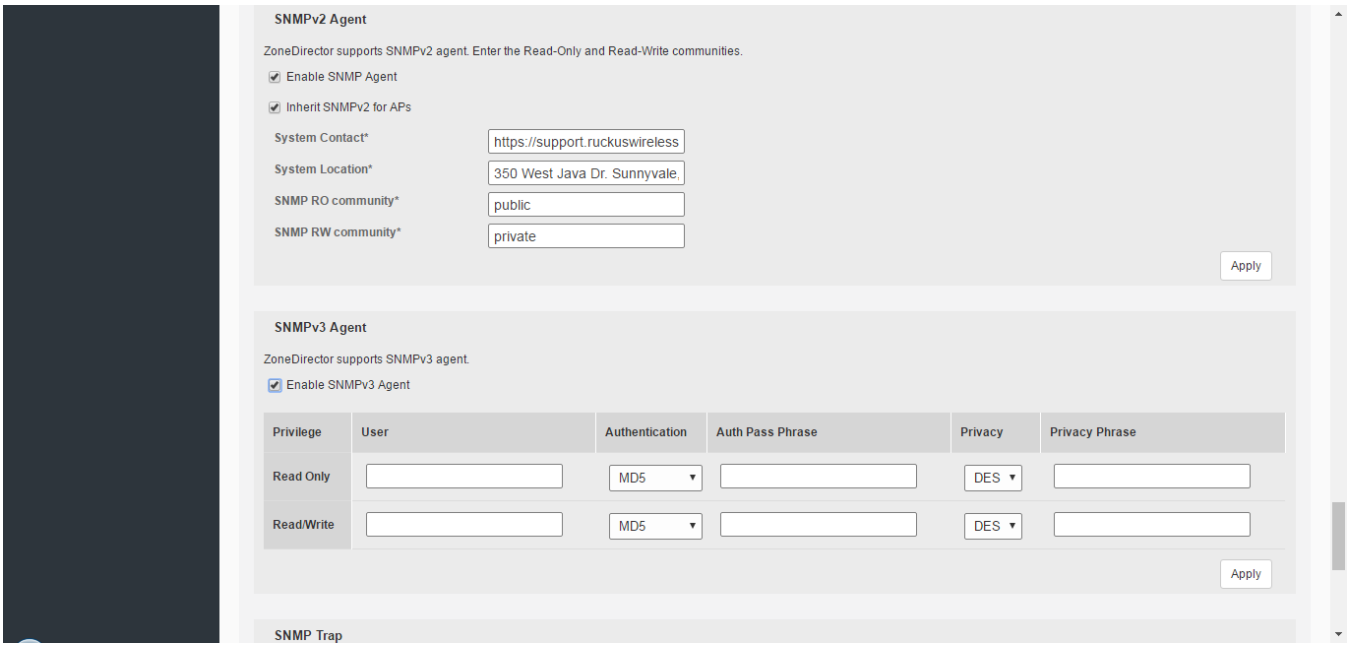
If your network uses SNMPv3

To enable SNMPv3 management:

1. Go to **System** > **System Settings**. Scroll down to the bottom of the page and click the **Network Management** link to open the **Network Management** section.
2. Under the **SNMPv3 Agent** section, select the **Enable SNMP 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
     - **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 251 Enabling the SNMPv3 agent



Enabling SNMP Trap Notifications

If you have an SNMP trap receiver on the network, you can configure ZoneDirector 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. In the **Network Management** section of the **System > System Settings** page, scroll down to the bottom of the page.
2. Under **SNMP Trap**, 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 252 Enabling SNMPv2 trap notifications

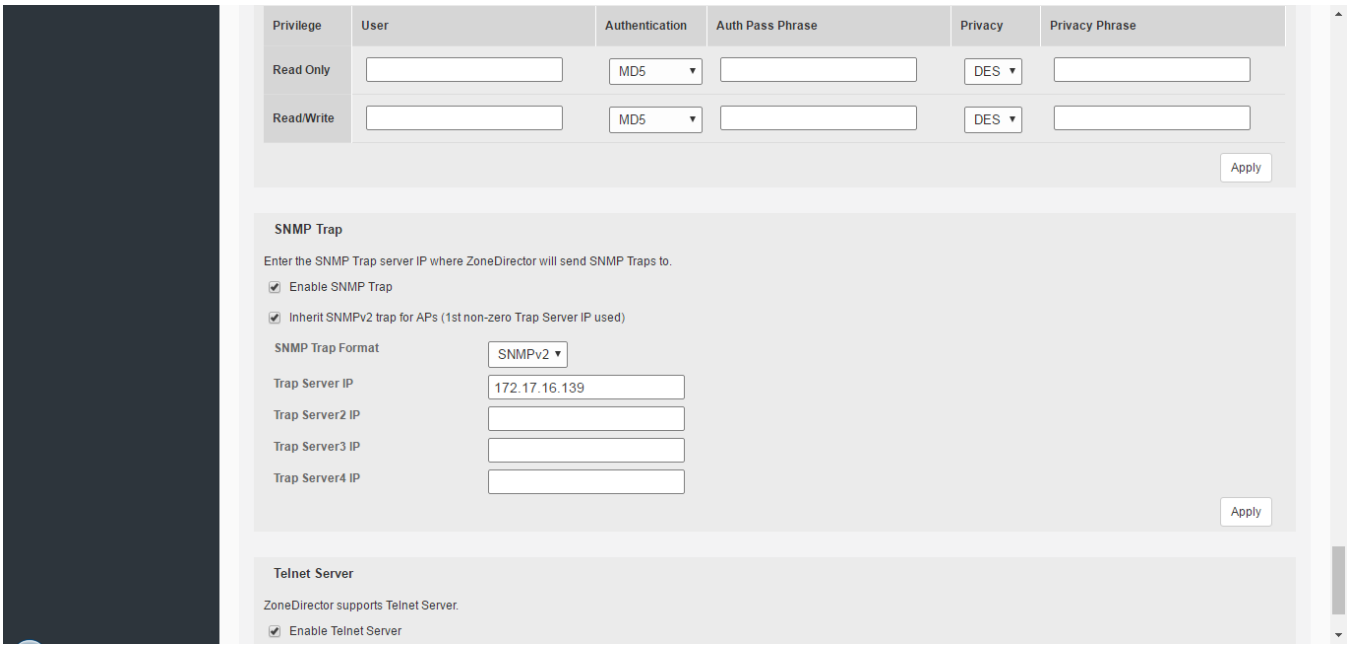
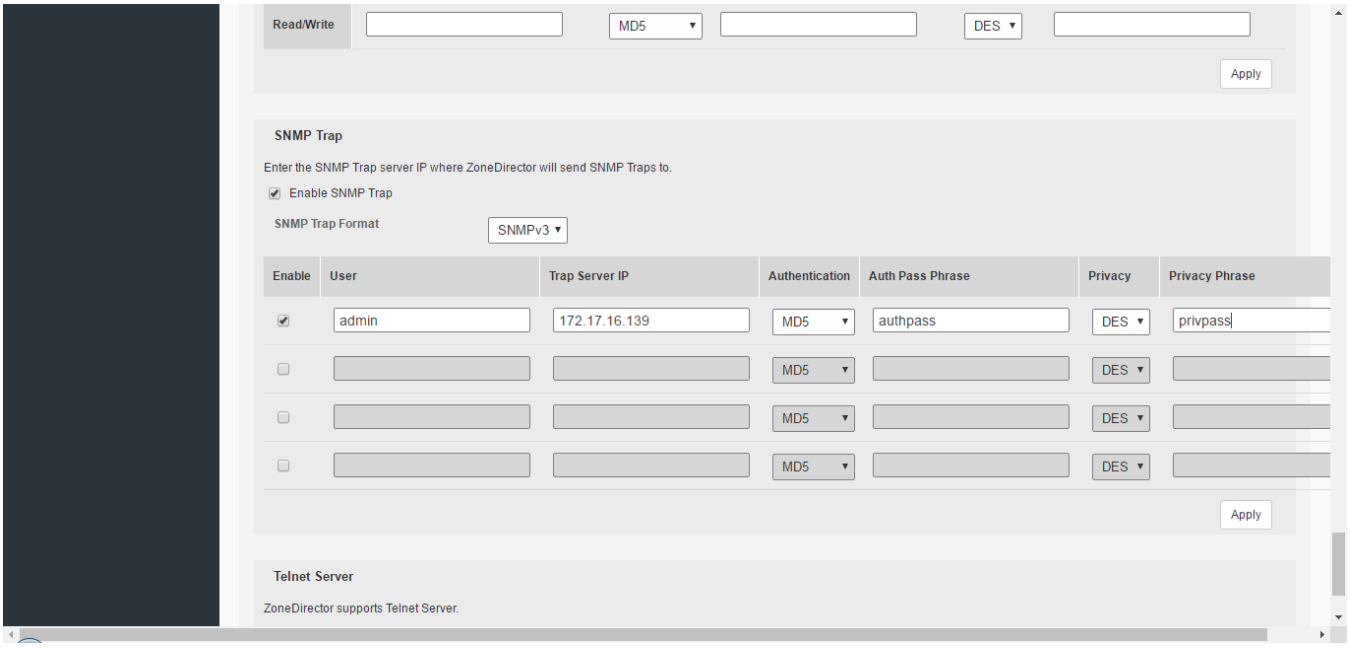


FIGURE 253 Enabling SNMP trap notifications with SNMPv3



Trap Notifications That ZoneDirector Sends

There are several events for which ZoneDirector will send trap notifications to the SNMP server that you specified.

The following table lists the trap notifications that ZoneDirector sends and when they are sent.

TABLE 28 Trap notifications

Trap Name	Description
ruckusZDEventAPJoinTrap	An AP has joined ZoneDirector. The AP's MAC address is included in the trap notification.
ruckusZDEventSSIDSpoofTrap	An SSID-spoofing rogue AP has been detected on the network. The rogue AP's MAC address and SSID are included in the trap notification.
ruckusZDEventMACSpoofTrap	A MAC-spoofing rogue AP has been detected on the network. The rogue AP's MAC address and SSID are included in the trap notification.
ruckusZDEventRogueAPTrap	A rogue AP has been detected on the network. The rogue AP's MAC address and SSID are included in the trap notification.
ruckusZDEventAPLostTrap	An AP has lost contact with ZoneDirector. The AP's MAC address is included in the trap notification.
ruckusZDEventAPLostHeartbeatTrap	An AP's heartbeat has been lost. The AP's MAC address is included in the trap notification.
ruckusZDEventClientAuthFailBlockTrap	A wireless client repeatedly failed to authenticate with an AP. The client's MAC address, AP's MAC address and SSID are included in the trap notification.
ruckusZDEventClientJoin	A client has successfully joined an AP. The client's MAC address, the AP's MAC address and SSID are included in the trap notification.
ruckusZDEventClientJoinFailed	A client has attempted and failed to join an AP. The client's MAC address, the AP's MAC address and SSID are included in the trap notification.
ruckusZDEventClientJoinFailedAPBusy	A client attempt to join an AP failed because the AP was busy. The client's MAC address, AP's MAC address and SSID are included.
ruckusZDEventClientDisconnect	A client has disconnected from the AP. The client's MAC address, AP's MAC address and SSID are included.
ruckusZDEventClientRoamOut	A client has roamed away from an AP. The client's MAC address, AP's MAC address and SSID are included.
ruckusZDEventClientRoamIn	A client has roamed in to an AP. The client's MAC address, AP's MAC address and SSID are included.
ruckusZDEventClientAuthFailed	A client authentication attempt has failed. The client's MAC address, AP's MAC address, SSID and failure reason are included.
ruckusZDEventClientAuthorizationFailed	A client authorization attempt to join an AP has failed. The client's MAC address, AP's MAC address and SSID are included.
ruckusZDEventAPcoldstart	An AP has been cold started.
ruckusZDEventAPwarmstart	An AP has been warm started.
ruckusZDEventAPclientValve	Triggered when an AP's online client limit has been exceeded.
ruckusZDEventAPCPUvalve	An AP's CPU utilization has exceeded the set value.
ruckusZDEventAPMEMvalve	An AP's memory utilization has exceeded the set value.
ruckusZDEventSmartRedundancy ChangetoActive	The standby Smart Redundancy ZoneDirector has failed to detect its active peer, system changed to active state.
ruckusZDEventSmartRedundancy ActiveConnected	The active Smart Redundancy ZoneDirector has detected its peer and is in active/connected state
ruckusZDEventSmartRedundancy ActiveDisconnected	The active Smart Redundancy ZoneDirector has not detected its peer and is in active/disconnected state.

TABLE 28 Trap notifications (continued)

Trap Name	Description
ruckusZDEventSmartRedundancy StandbyConnected	The standby ZoneDirector has detected its peer and is in standby/connected state.
ruckusZDEventSmartRedundancy StandbyDisconnected	The standby ZoneDirector has not detected its peer and is in standby/ disconnected state.

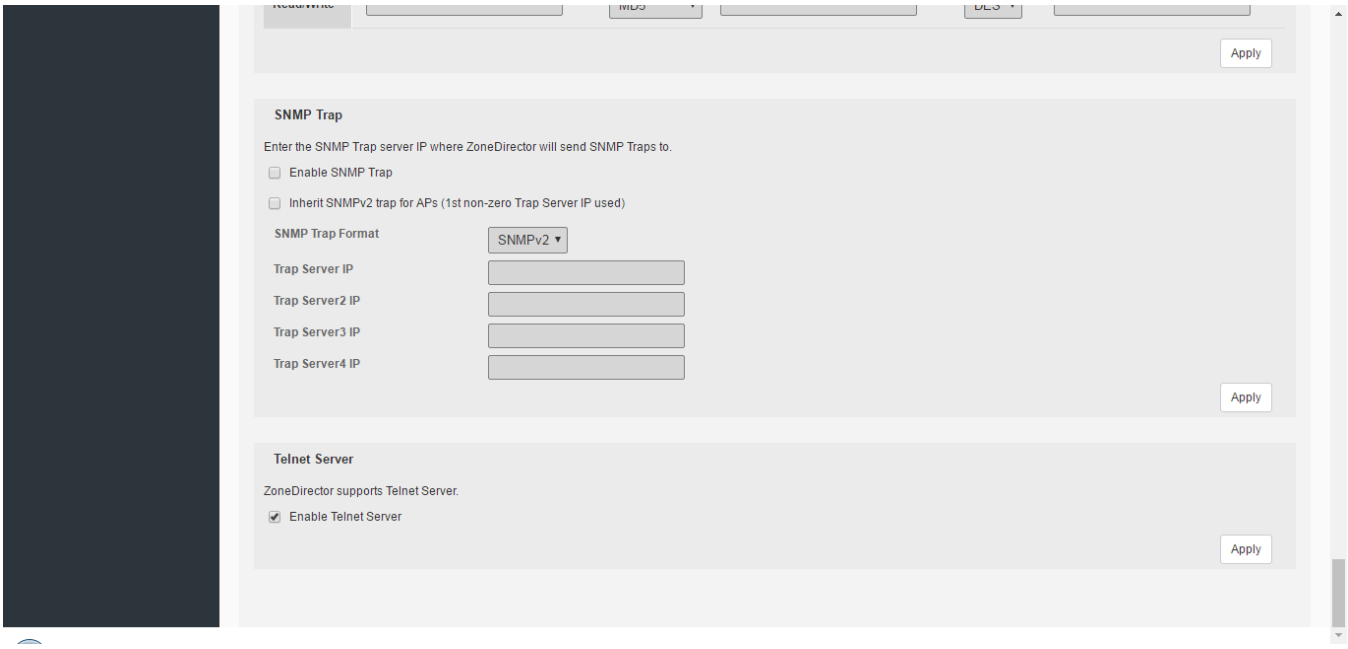
Enabling Telnet

By default, Telnet is disabled due to security considerations, as SSH is the preferred method if you need to access the ZoneDirector CLI. In some situations however, you may want to enable Telnet.

To enable Telnet:

1. Go to **System** > **System Settings**.
2. Scroll down to the bottom of the page and expand the **Network Management** section.
3. Locate the **Telnet Server** section, and click the box next to **Enable Telnet Server**.
4. Click **Apply** to save your changes.

FIGURE 254 Enabling Telnet server



Setting Administrator Preferences

- Changing the Web Interface Display Language..... 329
- Changing the ZoneDirector Administrator User Name and Password..... 331
- Working with Backup Files..... 334
- Restoring ZoneDirector to Default Factory Settings..... 337
- Upgrading ZoneDirector and Connected APs..... 339
- Working with Licenses and Support..... 343
- Working with SSL Certificates..... 346

Changing the Web Interface Display Language

Depending on your preferences, you can change the language in which the web interface is displayed in your web browser. The default is English.

This change only affects how the web interface appears, and does not modify either OS/system or browser settings (which are managed through other processes).

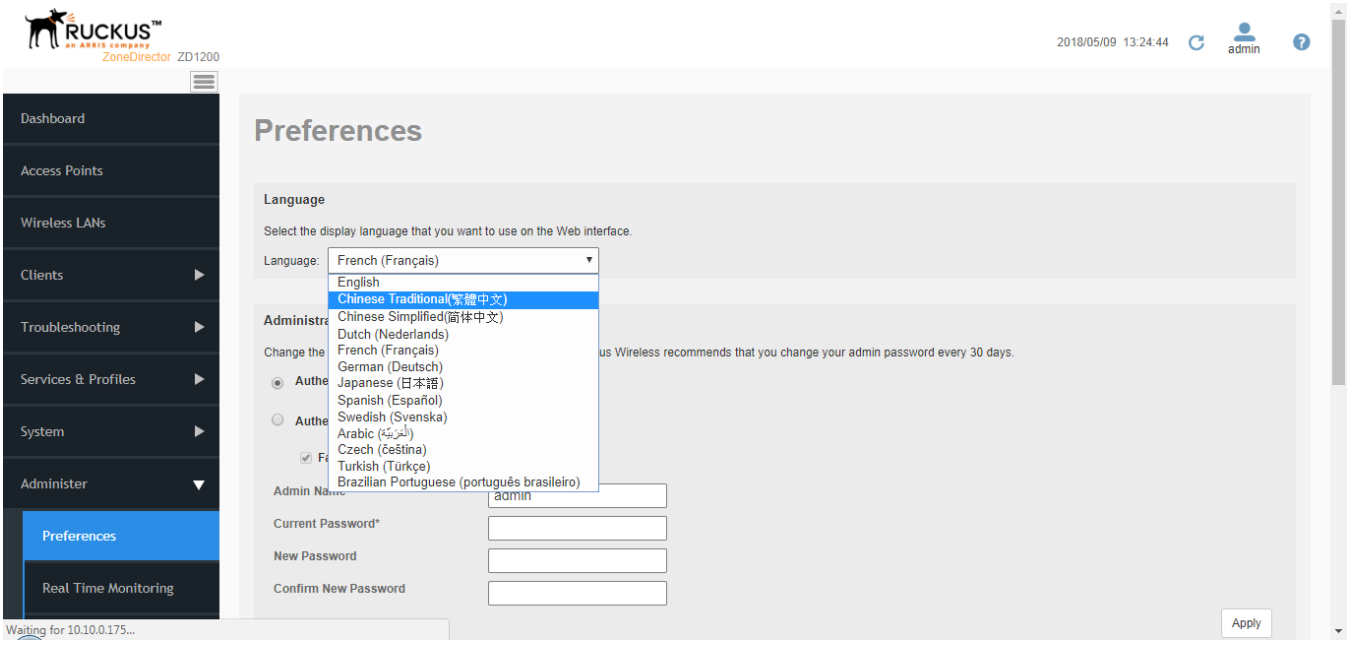
1. Go to **Administer** > **Preferences**.
2. Choose your preferred language from the **Language** drop-down menu.

3. Click **Apply** to save your settings. The changes go into effect immediately.

   Current web interface languages supported:

   - English
   - Chinese Traditional
   - Chinese Simplified
   - Dutch
   - French
   - German
   - Japanese
   - Spanish
   - Swedish
   - Arabic
   - Czech
   - Turkish
   - Brazilian Portuguese

   FIGURE 255 Select UI display language



Changing the ZoneDirector Administrator User Name and Password

You should change your ZoneDirector administrator login password on a monthly basis, but the administrator user name should be changed only if necessary.

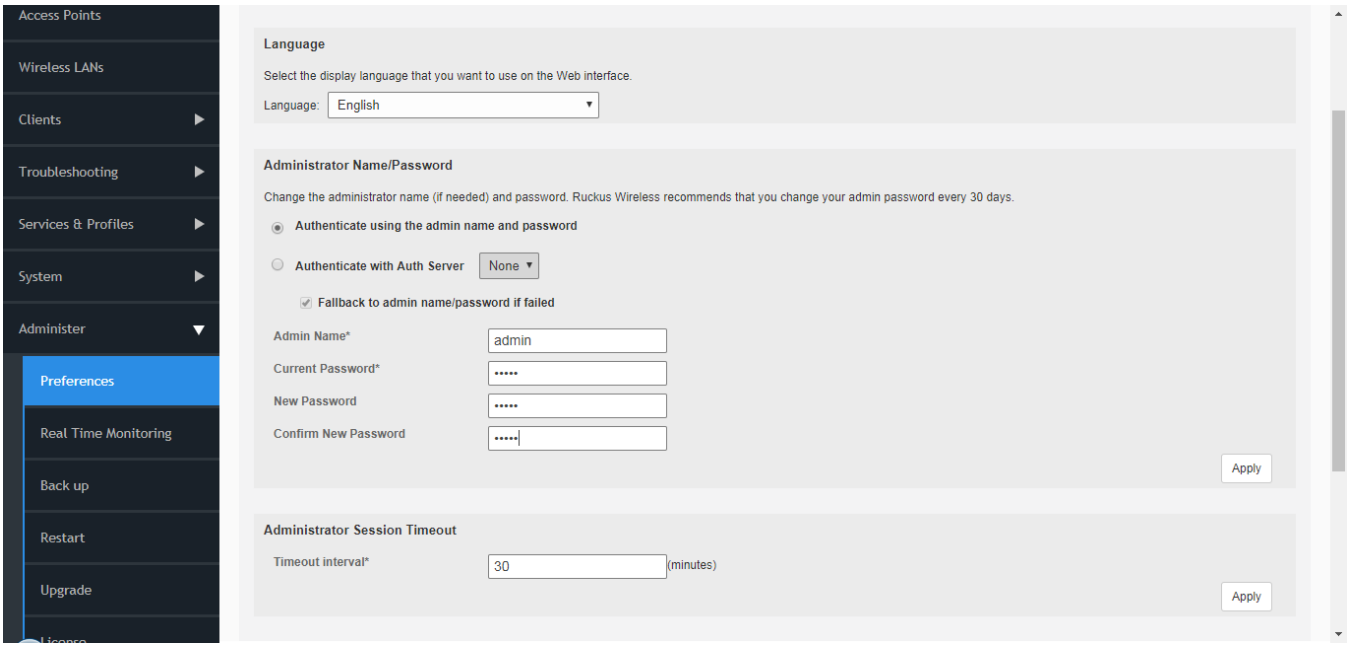
> **NOTE**
> If authentication with an external server is enabled and the **Fallback to admin name/password if failed check box** is disabled, you will be unable to edit the user name and password.

To edit or replace the current name or password:

1. Go to **Administer** > **Preferences**.
2. When the **Preferences** page appears, you have the following options under Administrator Name/Password:
   - **Authenticate using the admin name and password**: The default option, should be enabled if you are not using an external server for administrator authentication.
   - **Authenticate with Auth server**: Select an authentication server from the list, if you have configured one on the **Services & Profiles** > **AAA Servers** page.
     - **Fallback to admin name/password if failed**: Enable this check box to ensure you will be able to log in when the AAA server is unreachable.
   - **Admin Name**: Delete the text in this field and type the new administrator account name (used solely to log into ZoneDirector via the web interface).
   - **Current Password**: Enter the current admin password.
   - **New Password/Confirm Password**: Delete the text in the fields and type the same text for a new password.

3. Click **Apply** to save your settings. The changes go into effect immediately.

FIGURE 256 The Admin Preferences page



Using an External Server for Administrator Authentication

ZoneDirector supports additional administrator accounts that can be authenticated using an external authentication server such as RADIUS, LDAP, Active Directory or TACACS+. Three types of administrative privileges can be assigned to these administrator accounts:

- Super Admin - Allows all types of configuration and management tasks
- Operator Admin - Allows AP configuration only
- Monitoring Admin – Allows monitoring operations only

This section provides basic instructions for setting up ZoneDirector to authenticate additional administrator accounts with an external authentication server. For more information on AAA server configuration, see Using an External AAA Server on page 248.

To authenticate ZoneDirector administrators using an AAA server:

1. Set up Group Attributes on the AAA server:
   - RADIUS:
     - Ruckus private attribute
       - Vendor ID: 25053
       - Vendor Type/Attribute Number: 1 (Ruckus-User-Groups)
       - Value Format: group_attr1,group_attr2,group_attr3,...
   - Cisco private attribute (if your network is using a Cisco access control server)
     - Vendor ID: 9
     - Vendor Type / Attribute Number: 1 (Cisco-AVPair)
     - Value Format: shell:roles="group_attr1 group_attr2 group_attr3 ..."
   - Active Directory or LDAP:
     - Set up administrator groups.
     - Populate these groups with users to whom you want to grant administrator access. One way to do this is to edit each user's Member of profile and add the group to which you want the user to belong. Remember the group names that you set; you will enter this information when you create administrator roles in ZoneDirector (see Step 3).
     - TACACS+: See TACACS+ on page 263 for more information.
2. Set up ZoneDirector to use an AAA server (Services & Profiles > AAA Servers).
3. Create an Administrator Role in ZoneDirector (Services & Profiles > Roles).
   - Allow access to all/specific WLANs.
   - Allow/deny Guest Pass Generation.
   - Ensure that Allow ZoneDirector Administration is enabled, and choose the level of administration privileges you want to allow for this role.

     NOTE
     If you do not select the Allow ZoneDirector Administration check box, administrators that are assigned this role will be unable to log into ZoneDirector even if all other settings are configured correctly.

4. Test your authentication settings (Services & Profiles > AAA Servers > Test Authentication Settings).
5. Specify AAA server to use (Administer > Preferences > Authenticate with Auth Server).
   - Verify that the Fallback to admin name/password if failed check box is selected. Keeping this check box selected ensures that administrators will still be able to log into the ZoneDirector web interface even when the authentication server is unavailable.

Congratulations! You have completed setting up ZoneDirector to use external servers for administrator authentication. Whenever a user with administrator privileges logs into the ZoneDirector web interface, an event will be recorded. The following is an example of the event details that you will see:**Admin [user_name] login (authenticated by {Authentication Server} with {Role}).**

Setting Administrator Login Session Timeout

By default, administrators logged into the web interface are automatically logged out after 30 minutes of inactivity.

This timeout can be configured with a value between 1 and 1440 minutes (24 hours). To change the admin idle timeout period, enter a new value in **Administer** > **Preferences** > **Timeout interval**, and click **Apply**.

Working with Backup Files

After you have set up and configured your wireless network, you may want to back up the full ZoneDirector configuration for future use.

The resulting archive can be used to restore your ZoneDirector to the saved settings after a factory reset. Whenever you make additions or changes to the setup, you can create new backup files, so that in case of any configuration errors, you can always revert to the last known good settings using the backup file.

Backing Up a Network Configuration

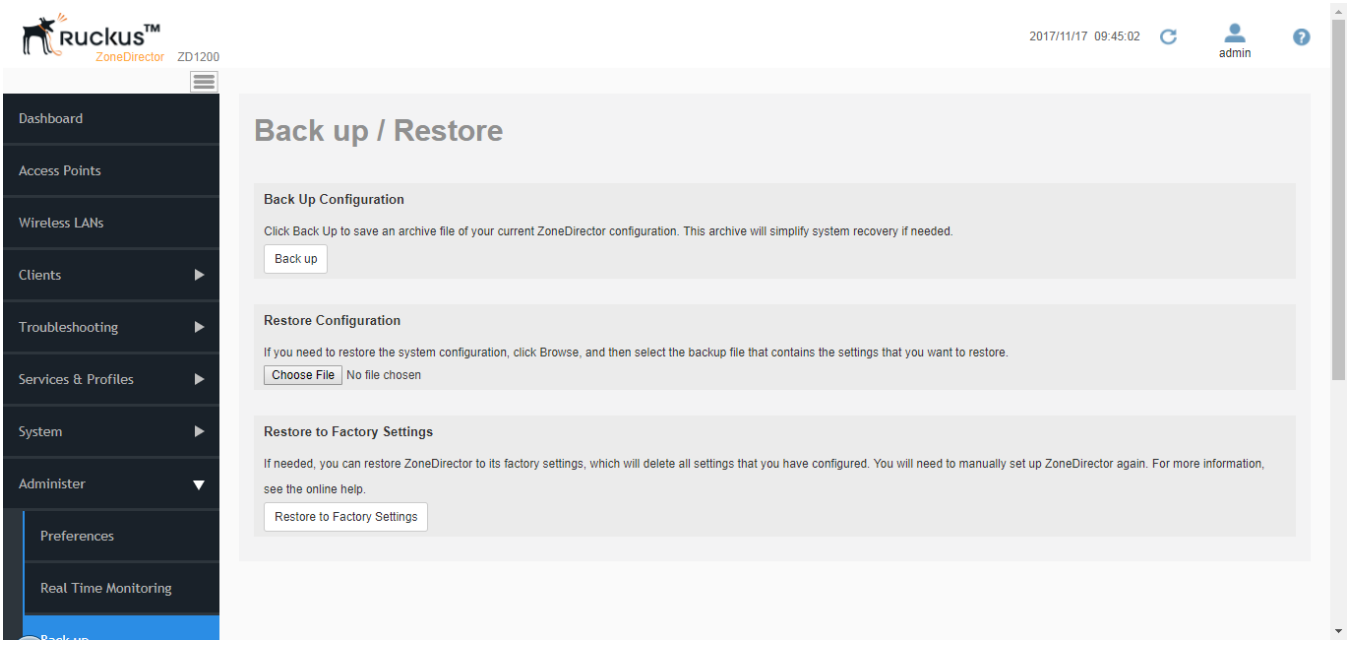
To back up your current ZoneDirector configuration to a backup file:

1. Go to **Administer** > **Backup**.
2. Under the **Backup Configuration** sections, click **Back Up**. The **File Download** dialog box appears.
3. Click **Save**.
4. When the **Save As** dialog box appears, enter a name for this archive file, pick a destination folder, then click **Save**.

   NOTE
   Ruckus recommends adding the firmware version number to the backup file name so that you can easily identify which backup files were created on which firmware version. By default, only the backup date is included in the file name.

5. Make sure the filename ends in a ".bak" extension.
6. When the **Download Complete** dialog box appears, click **Close**.

FIGURE 257 The Back Up Configuration option



Restoring Archived Settings to ZoneDirector

Restoring a backup file will automatically reboot ZoneDirector and all APs that are currently associated with it. Users associated with these APs will be temporarily disconnected; wireless access will be restored automatically after ZoneDirector and the APs have completed booting up.

To restore ZoneDirector configuration settings from a backup file:

1. Go to **Administer** > **Backup**.
2. Under **Restore Configuration**, click **Choose File**.
3. Locate a previously saved backup file, select the file, and then click **Open**.
4. Three restore options appear:
   - **Restore everything**: Select this option if you want the device to use all the settings configured in the backup file (including the IP address, wireless settings, access control lists, AP and WLAN group configurations, etc.).

     NOTE
     If you use the Restore everything option to restore settings from one ZoneDirector unit to another, note that wireless clients reporting to the AP managed by the first ZoneDirector unit will need to go through Zero-IT activation again to obtain new client certificates. Zero-IT activation is enabled by default, therefore no manual configuration is required from you.

   - **Restore everything, except system name and IP address settings** (for failover deployment at the same site): Select this option to import settings saved from a primary to a backup ZoneDirector for Smart Redundancy deployment.

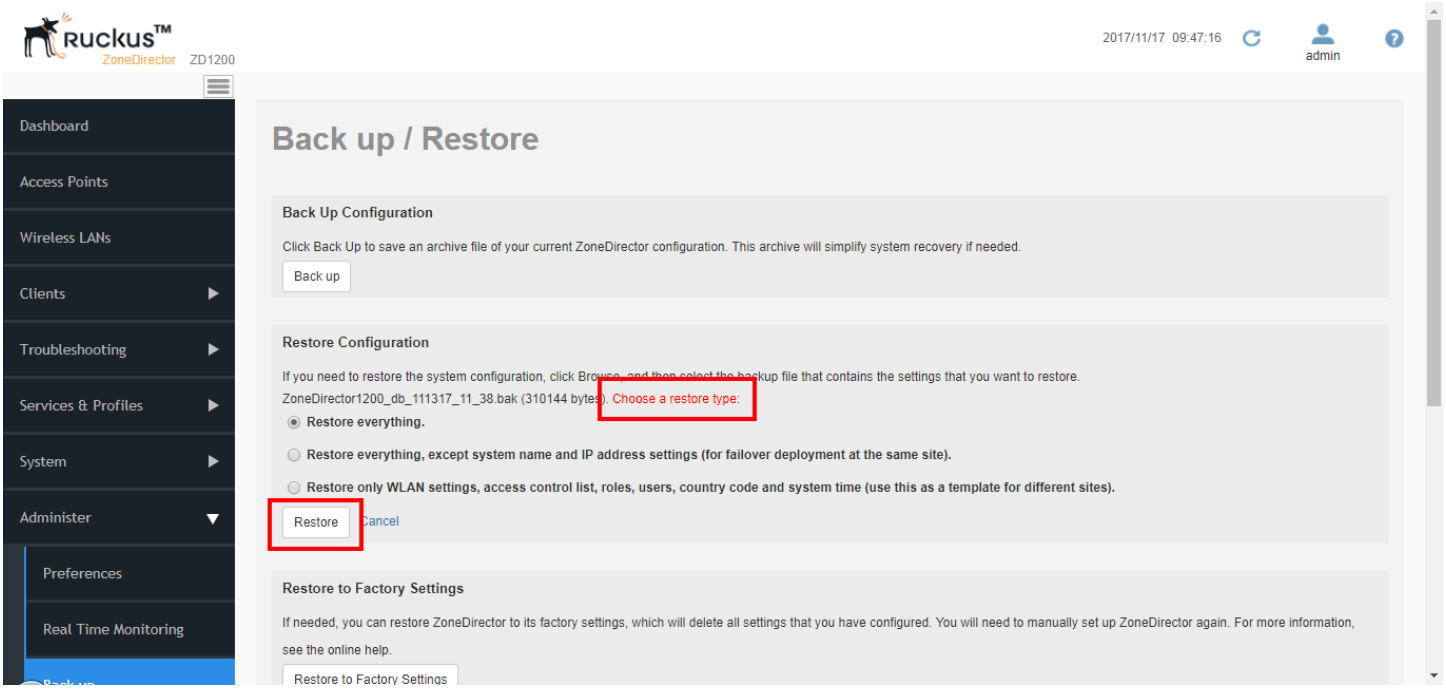
     NOTE
     In addition to system name and IP address, this option restores everything except for the following configuration settings:

     a. VLAN settings.
     b. Management IP address and VLAN settings.
     c. Smart Redundancy settings.
     d. DHCP server settings.
     e. Session timeout.
     f. Limited ZD Discovery and Management VLAN settings in Access Point Policies.

   - **Restore only WLAN settings, access control list, roles, and users** (use this as a template for different sites): Select this option if you want to use the backup file as a configuration template.
5. Click the **Restore** button.

ZoneDirector restores the backup file. During this process, ZoneDirector automatically logs you out of the web interface. When the restore process is complete, ZoneDirector automatically restarts and your wireless network will be ready for use again.

FIGURE 258 Select the restore level for restoring from a backup file



Restoring AP Configuration Settings Only

You can also restore previously saved access point configurations from a backup file without restoring any other ZoneDirector configuration settings.

This feature can be useful in deploying N+1 redundancy. For example, if three ZoneDirector controllers are deployed in different locations, plus one ZoneDirector serving as a backup, you can use this feature to export the AP lists from the three primary controllers and import them one by one into the backup ZD.

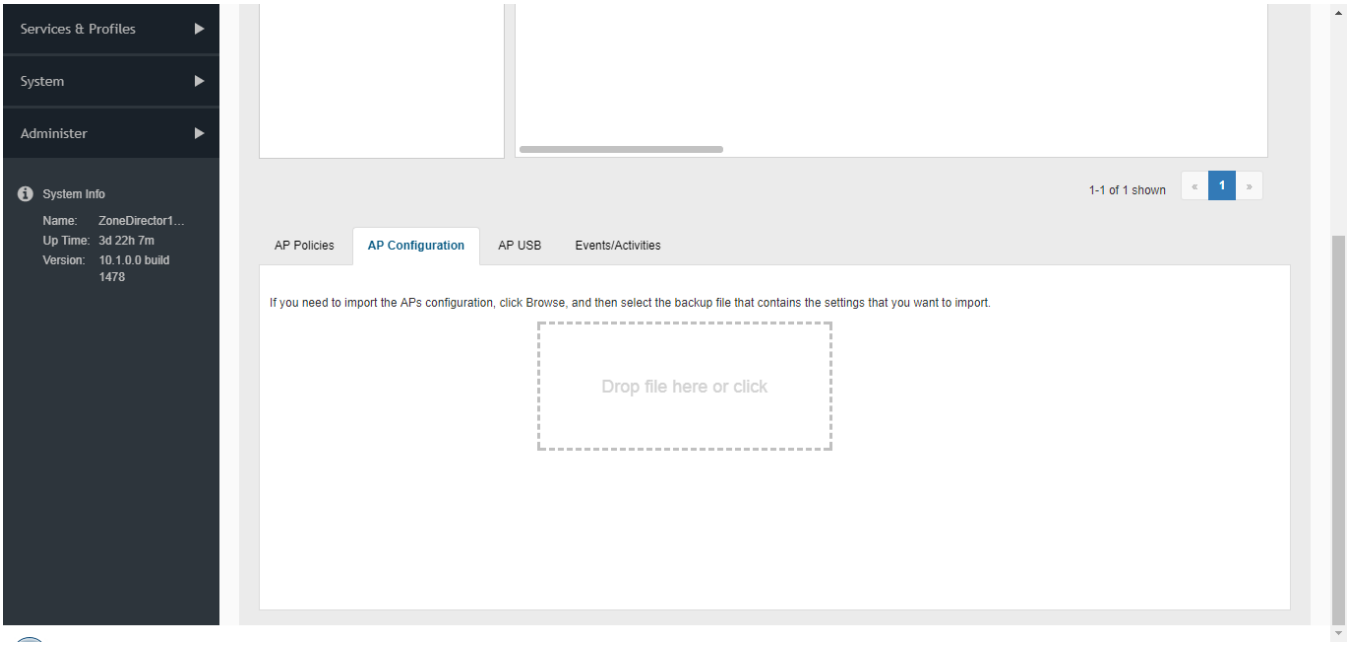
For more information on N+1 redundancy deployment, see Using Limited ZD Discovery for N+1 Redundancy on page 55.

To restore an AP list from a backup file without altering ZoneDirector settings:

1. Go to **Access Points**, and click the **AP Configuration** tab.
2. Drag and drop a previously saved backup file to the **Drop file here or click** box, or click to browse and locate a file on your local computer.
3. Click **Open**. The page refreshes and the name of the backup file you selected is displayed, along with the option to either import this file and reboot, or import this file and continue importing additional files before reboot.
   - To import this file only, select **Import this backup file and then reboot**. ZoneDirector will reboot after loading your AP list.
   - To import this file and continue importing AP lists from other backup files, select **Import this backup file and additional backup file(s)**. Then click **Import**. When the import is complete, you will be prompted to import AP configurations from additional backup files.
4. When finished, click **Import**. ZoneDirector will import all AP configurations from any backup files selected and reboot automatically. You must wait for the reboot process to complete before being able to log back into ZoneDirector.

5. When the reboot process is complete, the restored APs appear in the Access Points table at the top of the page.

FIGURE 259 Importing AP lists only from a backup file



Restoring ZoneDirector to Default Factory Settings

In certain extreme conditions, you may want to re-initialize ZoneDirector and reset it to factory default state.

In this state, the network is almost ready for use, but all your user/guest/log and other records, accounts and preference configurations would need to be manually reconfigured.

NOTE
Resetting ZoneDirector to factory default settings will erase all configuration changes that you made, except for AP licenses and SSL certificates.

NOTE
When this procedure is complete, you will need to redo a complete setup. If ZoneDirector is on a live network, a new IP address may be assigned to the system. In this case, the system can be discovered by a UPnP client application, such as Windows “My Network Places.” If there is no DHCP server on the connected network, the system's default IP address is 192.168.0.2 with subnet mask 255.255.255.0.

NOTE
A complete set of instructions is available in the ZoneDirector Quick Start Guide (QSG). Before restoring ZoneDirector to factory default settings, you should open and print out the QSG pages. You can follow those instructions to set up ZoneDirector after restoring factory defaults.

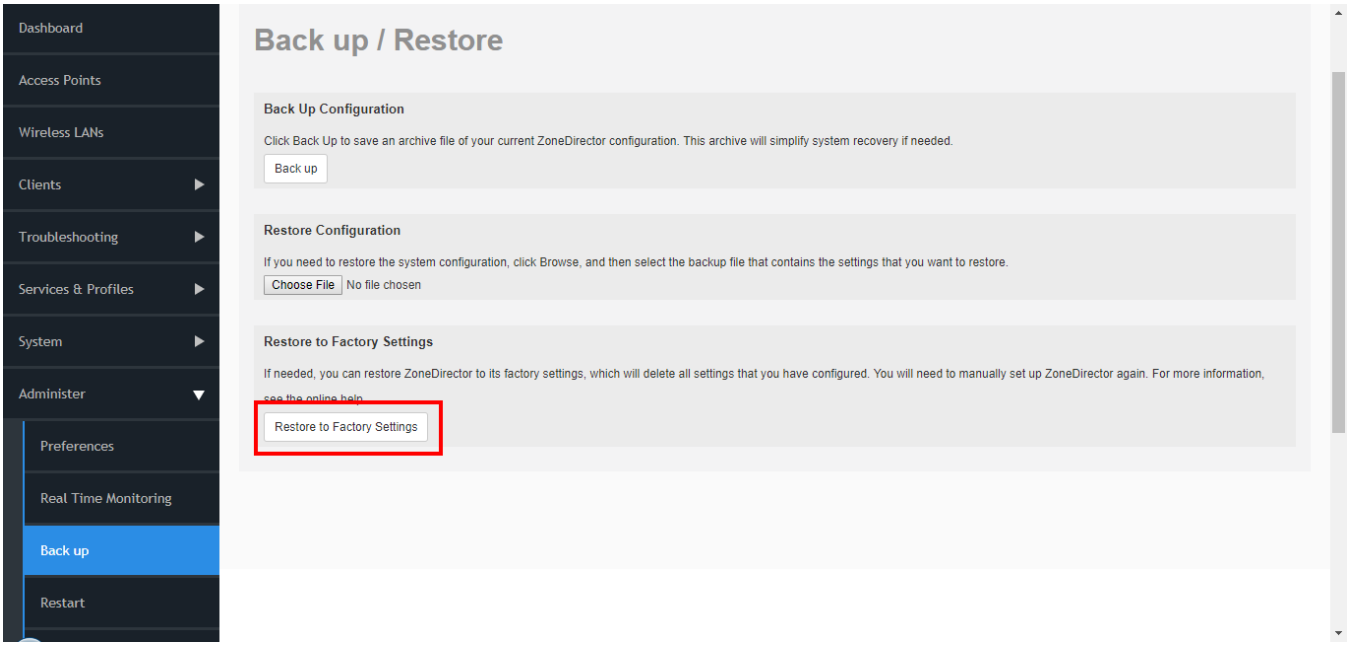
1. Go to **Administer** > **Backup**.

2. Locate the **Restore to Factory Settings** and click the button.

   NOTE
   Owing to the drastic effect of this operation, one or more confirmation dialog boxes will appear. Click **OK** to confirm this operation.

3. When this factory reset process begins, you will be logged out of the web interface.
4. When the reset is complete, the Status LED begins blinking green, indicating that the system is in the "factory default" state. After you complete the Setup Wizard, the Status LED will be steady green.

FIGURE 260 The Restore to Factory Settings section



Alternate Factory Default Reset Method

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

NOTE
Do not disconnect ZoneDirector from its power source until this procedure is complete.

1. Locate the **Reset** pin hole on the front panel of ZoneDirector.
2. Insert a straightened paper clip in the hole and press for at least 5 seconds. After the reset is complete, the Status LED blinks red, then blinks green, indicating that the system is in factory default state. After you complete the Setup Wizard, the Status LED will be steady green.

Upgrading ZoneDirector and Connected APs

Consult the Ruckus Support website on a regular basis for updates that can be applied to your Ruckus network devices.

> **NOTE**
> For information and detailed instructions (including video tutorials) on upgrading ZoneDirector, visit the Ruckus Support How-To Hub at *https://support.ruckuswireless.com/how-to-hub*.

Ruckus strongly recommends reading the *Release Notes* for the release that you plan to upgrade to prior to beginning the upgrade.

Release Notes contain important information related to upgrading to the current release, including:

- Supported platforms
- Supported upgrade paths
- Enhancements
- Resolved issues
- Known open issues
- Client interoperability

Review the Release Notes to ensure that the ZoneDirector and AP models in your deployment are supported in the release. Release Notes and firmware image files are both available at *https://support.ruckuswireless.com*. You will need a valid Ruckus support site account to access these resources.

After downloading an update package to a convenient folder on your administrative PC, you can complete the network upgrade (of both ZoneDirector and the APs) by performing the following steps.

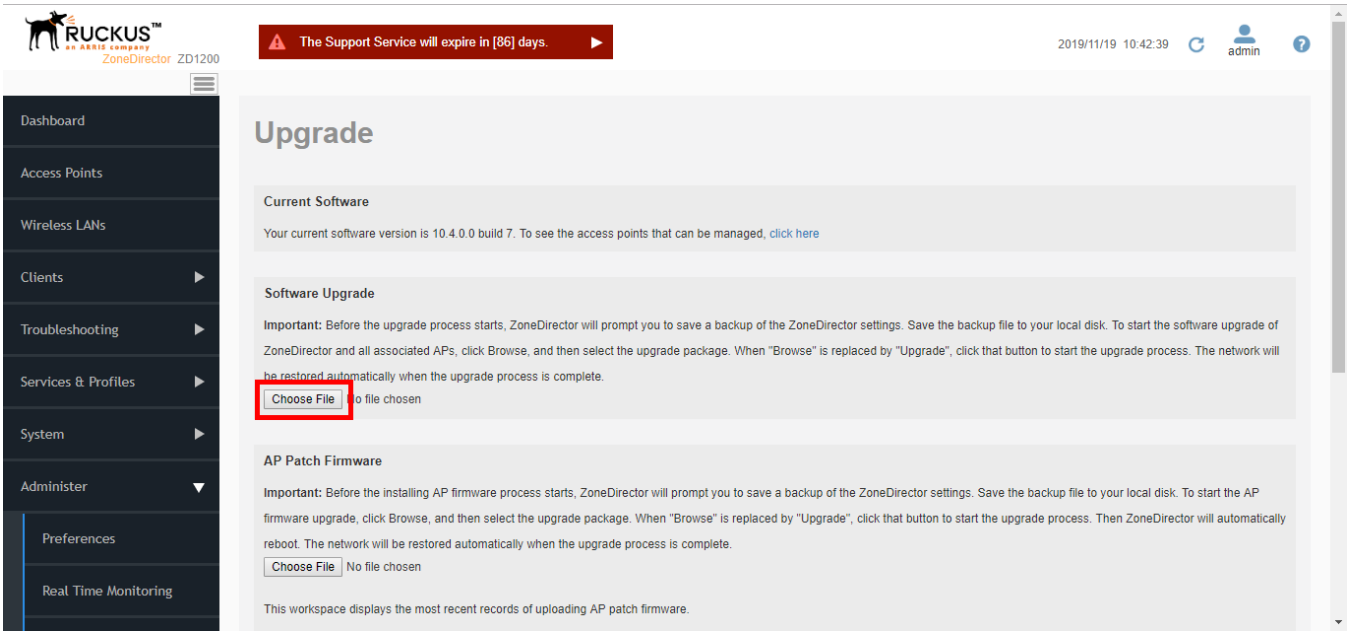
The full network upgrade is successive in sequence. After ZoneDirector is upgraded, it contacts each active AP, upgrades it, and restores it to service. The APs use FTP to download firmware updates from ZoneDirector by default. If you have an access control list (ACL) or firewall between ZoneDirector and the APs, make sure that FTP traffic is allowed to ensure that the APs can successfully download the updated firmware.

> **NOTE**
> Upgrading ZoneDirector and the APs temporarily disconnects them (and any associated clients) from the network. To minimize network disruption, Ruckus recommends performing the upgrade procedure at an off-peak time.

1. Back up your existing configuration.
2. Go to **Administer** > **Upgrade**.

3. In the *Software Upgrade* section, click **Choose File**.

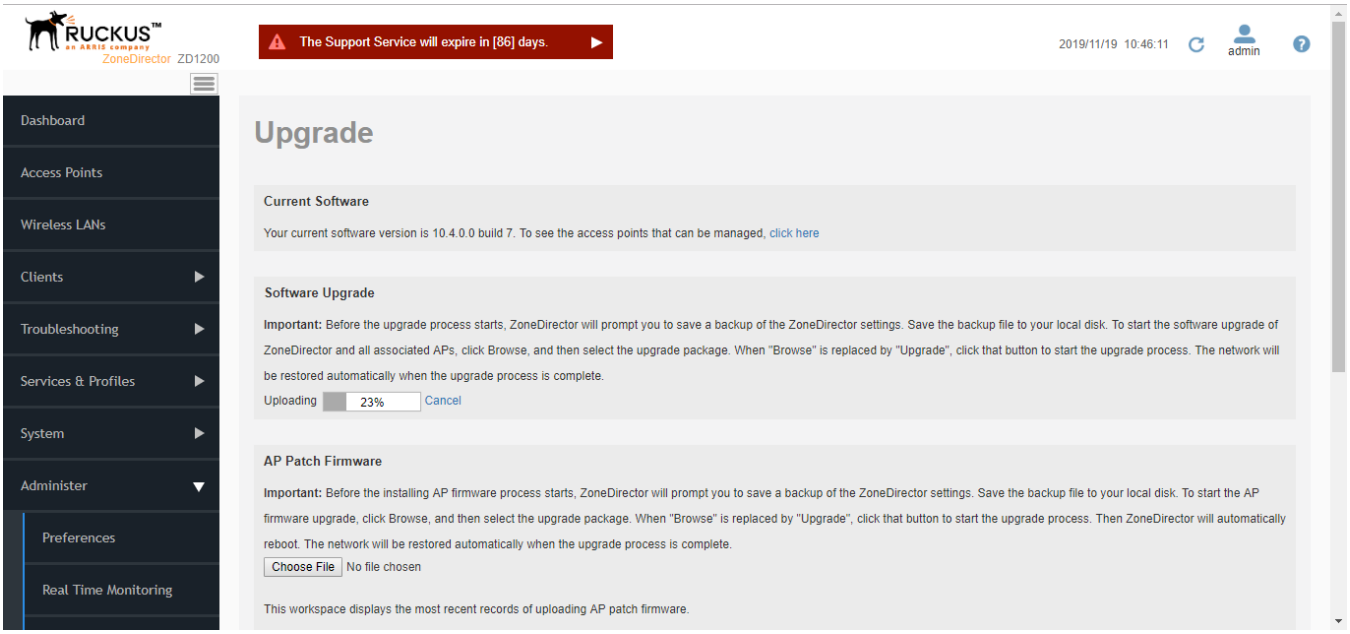
FIGURE 261 Upgrade Page



4. Browse to the location where you saved the upgrade package, and click **Open**.

The firmware image file upload progress is displayed.

FIGURE 262 Firmware upload in progress



5. When the file is finished uploading, the upgrade file name appears in the text field, and the **Upgrade** button appears.

6. Click **Upgrade**. ZoneDirector performs the upgrade and restarts. When the upgrade process is complete, the Status LED on ZoneDirector is steadily lit. You may now log in to the web interface as Administrator to confirm the new build number.

Importing an AP Firmware Bundle

Beginning with ZoneDirector release 10.0, administrators can import a new AP model patch file to ZoneDirector without performing a full upgrade of the controller. In this way, new AP models can be introduced without the need to wait for the next ZoneDirector firmware release.

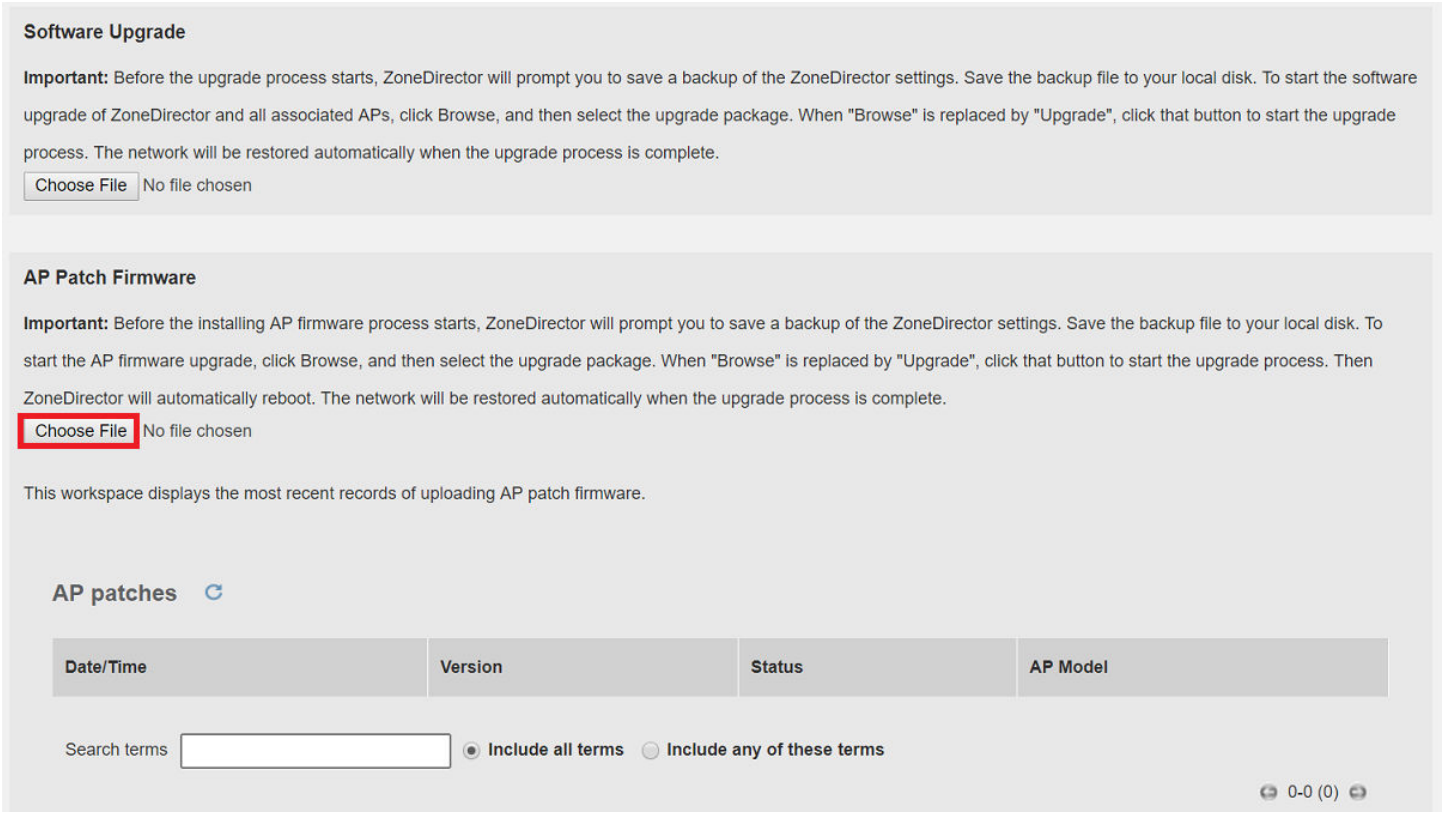
When Ruckus introduces a new AP model, an AP firmware bundle (or new AP model patch) is made available for download from the Ruckus Support website. Visit the Support site to download the AP firmware bundle to a local computer, import it into ZoneDirector, and the new AP model is now supported after a reboot.

NOTE
Upgrading ZoneDirector to a new release deletes all imported AP firmware bundles. Install the required AP firmware bundles only after upgrading ZoneDirector firmware.

The steps required for importing an AP firmware bundle are similar to the steps in Upgrading ZoneDirector and Connected APs on page 339.

NOTE
Importing an AP firmware bundle automatically reboots the ZoneDirector to affect the patch, temporarily disconnecting APs (and any associated clients) from the network. To minimize network disruption, Ruckus recommends performing the upgrade procedure at an off-peak time.

FIGURE 263 Importing an AP Firmware Bundle

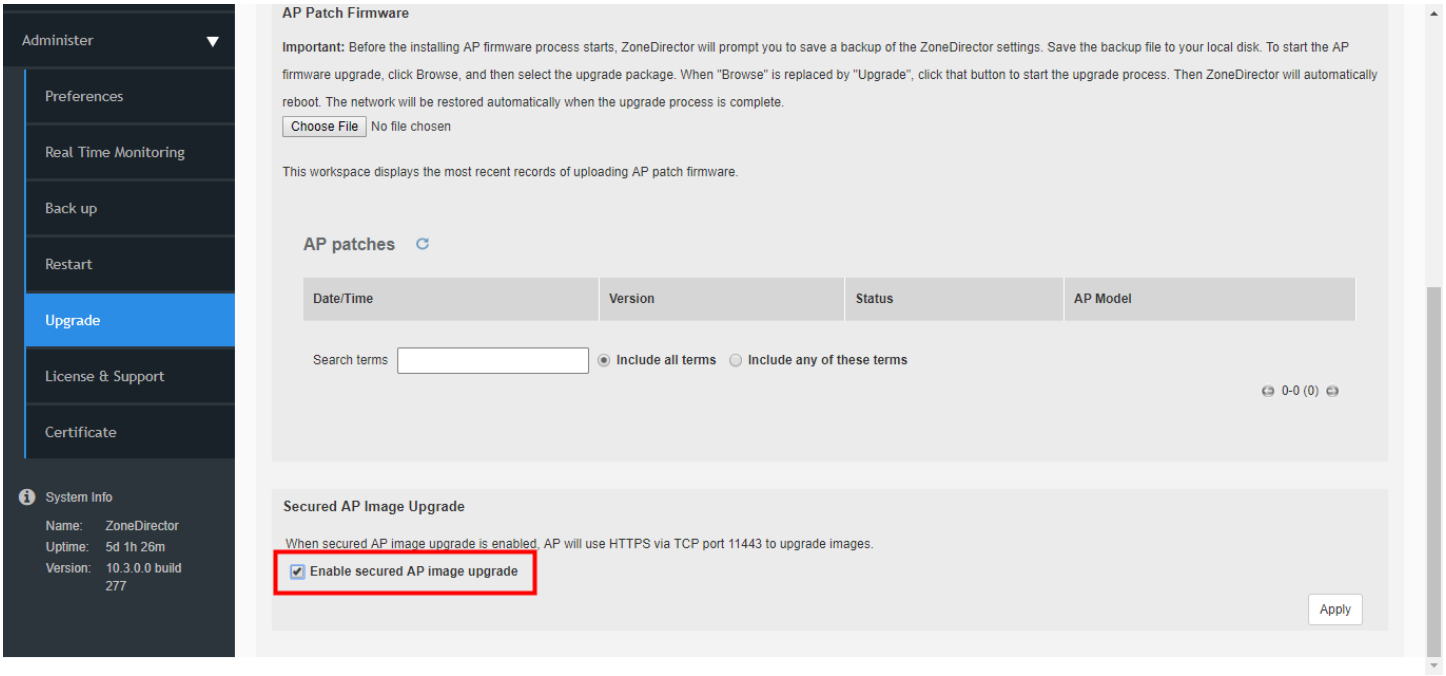


Enabling Secured AP Image Upgrade

Beginning with ZoneDirector release 9.13, AP firmware image upgrades can be performed using HTTPS via TCP port 11443 rather than FTP.

Select the check box next to **Enable secured AP image upgrade** to enable HTTPS upgrade. If HTTPS upgrade is not supported by the specific AP model, the upgrade will fall back to FTP.

FIGURE 264 Secure AP image upgrade



Performing an Upgrade with Smart Redundancy

If you have two ZoneDirectors in a Smart Redundancy configuration, the upgrade procedure is similar to upgrading a single controller.

Note however, that the active and standby ZoneDirectors will reverse roles during the upgrade.

To upgrade both ZoneDirectors in a Smart Redundancy configuration, complete the following steps:

1. Log in to the **active** ZoneDirector.

   NOTE
   Do not attempt to manually upgrade the standby ZoneDirector before the active unit. If you do so, some configuration options may be lost during the upgrade process. Be sure to begin the upgrade process from the web interface of the active ZoneDirector (or the shared Management Interface, if configured).

2. Go to **Administer** > **Upgrade**.
3. In the **Software Upgrade** area, click **Browse**. The **Browse** dialog box appears.
4. Browse to the location where you saved the upgrade package, and click **Open**.

   When the upgrade file name appears in the text field, the **Browse** button becomes the **Upgrade** button.
5. Click **Upgrade**.

   The standby ZoneDirector is upgraded first.

6. When the standby ZoneDirector upgrade is complete, the standby ZoneDirector reboots and becomes the active controller (begins accepting AP requests), while the original active device enters standby state and begins its own upgrade process.
7. All APs are now associated to the original standby ZoneDirector (now the active ZoneDirector), and begin downloading and upgrading AP firmware to the new version.
8. Each AP reboots after the upgrade is complete, and reconnects to the new active ZoneDirector.

Working with Licenses and Support

The *License & Support* page provides options for managing AP licenses, URL filtering licenses, and Ruckus customer support services.

Upgrading the AP License

Depending on the number of Ruckus APs you need to manage with your ZoneDirector, you may need to upgrade your license as your network expands.

Contact your authorized Ruckus reseller to purchase an upgrade license. Once you load the license via the web interface, it takes effect immediately.

Current license information (description, PO number, status, etc.) is displayed on the web interface.

> **NOTE**
> The system does not reboot or reset after a license is imported.

To import a new license file:

1. Go to **Administer** > **License & Support**.
2. In *AP License*, click **Update Services By File**.
3. In the *Import a new license* section that appears, drag and drop a file into the window or click the text box to upload a file.

4. Once your license file has been uploaded, ZoneDirector immediately attempts to validate and install the license.

FIGURE 265 Importing a new AP license file

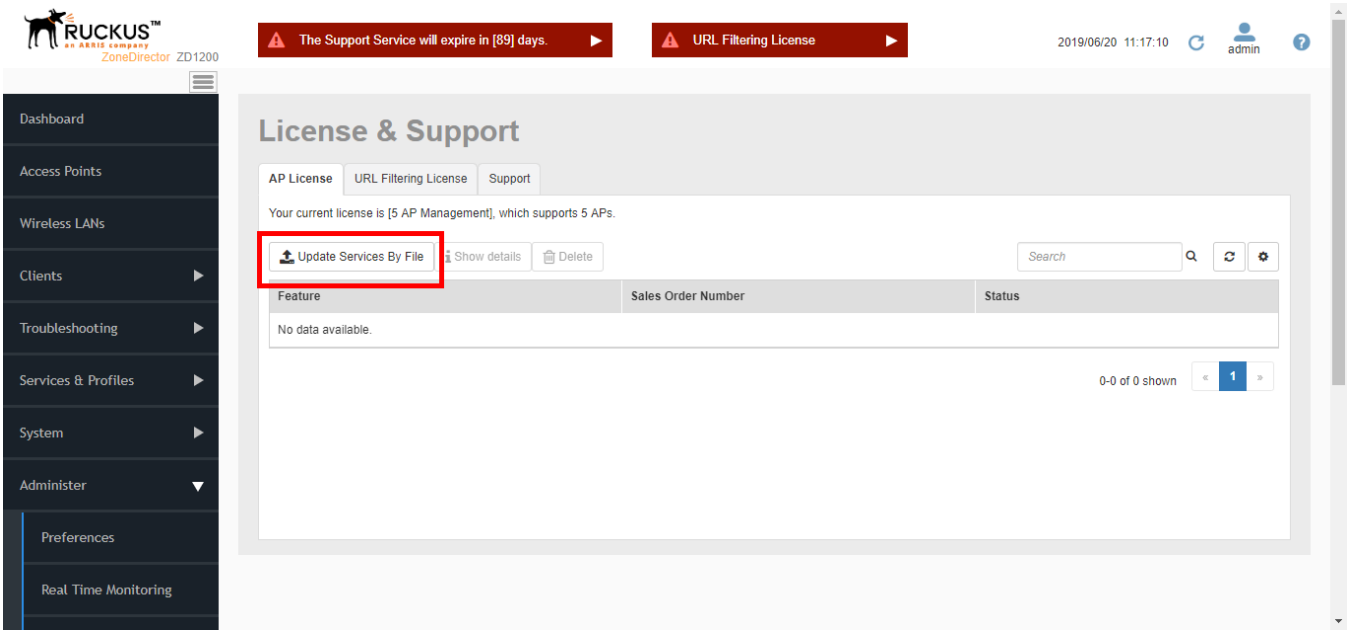
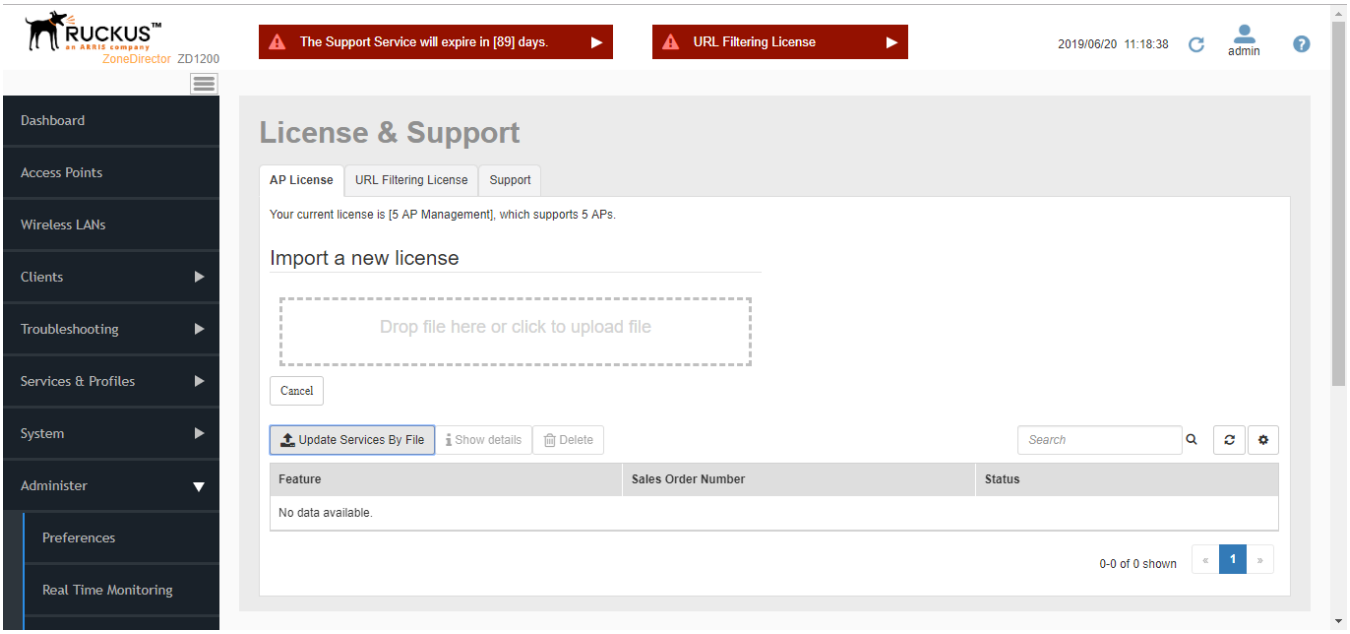


FIGURE 266 The License page



Support Entitlement

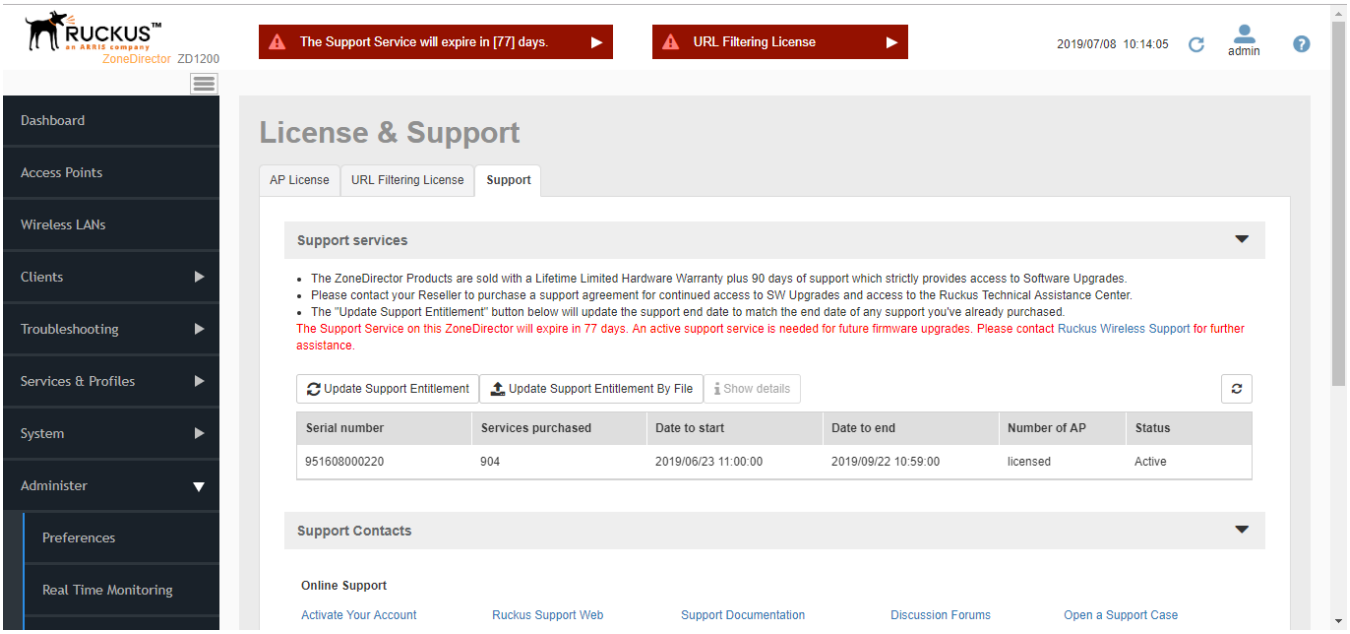
A Support Entitlement license allows you to extend the period for which you are allowed to continue upgrading your ZoneDirector when newer versions are released.

If your support contract has expired, you can contact your Ruckus customer service representative or Ruckus reseller to purchase additional support service. After you have purchased a support contract, you can download the entitlement file and automatically import into your ZoneDirector or manually download the file and upload it to ZoneDirector.

To import a new Support entitlement file:

1. Go to **Administer** > **License & Support**.
2. In the **Support Services** section, click **Update Services by File** to import a locally saved support activation file, or click **Renew Services Online** to download and install a new support service automatically.
3. Click **Show Details** to display support service status information.

FIGURE 267 Activating Support Entitlement



Working with URL Filtering Licenses

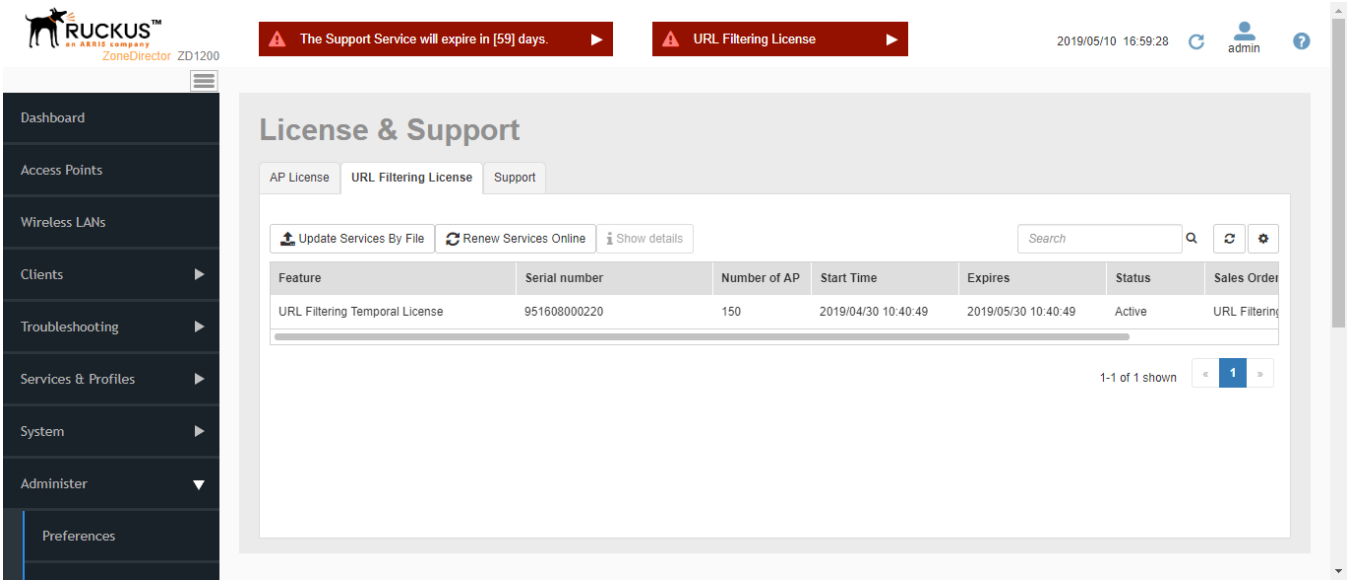
URL Filtering service requires an active URL filtering license on the ZoneDirector to function. URL filtering licenses can be purchased from Ruckus partners and distributors, and a temporary license is also available to allow customers to try out the service for a limited time before purchasing.

To manage URL filtering licenses:

1. Go to **Administer > License & Support**.

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

FIGURE 268 Working with URL filtering licenses



Working with SSL Certificates

SSL certificates enable device or user identification, as well as secure communications. ZoneDirector captive portal services and the web UI use an SSL certificate when establishing HTTPS connections.

The default SSL certificate that is installed on the ZoneDirector is self-signed and therefore not trusted by any browser. This is the reason why the SSL security warnings appear when establishing an HTTPS connection to the ZoneDirector.

To eliminate the security warnings, administrators may purchase a trusted SSL certificate from a public Certificate Authority (CA) such as VeriSign and install it on the ZoneDirector.

Basic Certificate Installation

The 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 ZoneDirector.

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 ZoneDirector 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 **Administer** > **Certificate** form allows 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.

To create a certificate request file (CSR):

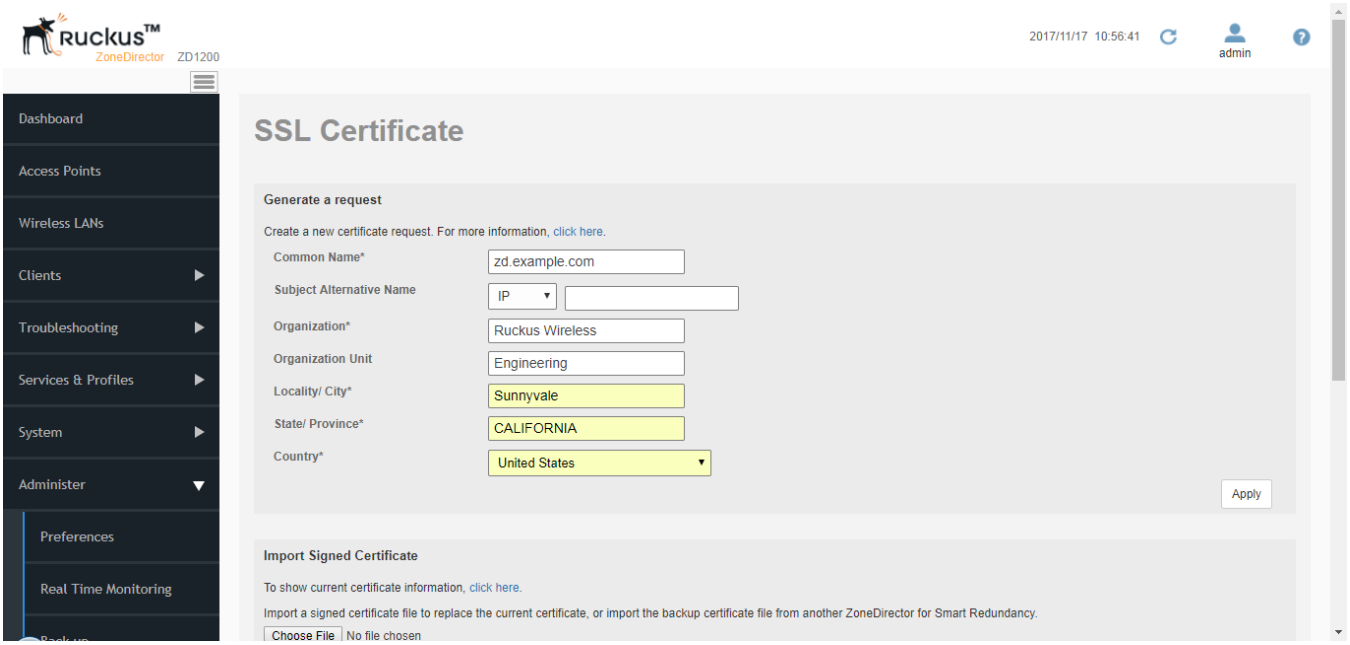
1. Go to **Administer** > **Certificate**
2. In the **Generate a Request** section, complete the following options:
   - **Common Name***: Enter ZoneDirector's Fully Qualified Domain Name (FQDN). Typically, this will be "zonedirector.[your company].com". You can also enter ZoneDirector's IP address (e.g., "192.168.0.2"), or a familiar name by which the ZoneDirector will be accessed in your browser (e.g., by device name such as "").

     NOTE
     Ruckus recommends using the FQDN as the Common Name if possible. If your network does not have a DNS server, you may use ZoneDirector's IP address instead. However, note that some CA's may not allow this.

     - If you wish to access ZoneDirector 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 ZoneDirector's IP address.
     - If you use a familiar name, this name will be shown in the browser's URL whenever accessing ZoneDirector (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**: (Optional) Type the name of the division, department, or section in your organization that manages network security (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 269 Generating a CSR file



5. Go to a certificate authority's web site and follow the instructions for purchasing an SSL certificate.
6. When you are prompted for the certificate signing request, copy and paste the content of the text file that you saved to your local computer, and then complete the certificate purchase. After the certificate authority approves your CSR, you will receive the SSL certificate via email. The following is an example of a signed certificate that you will receive from a certificate authority:
7. Copy the content of the signed certificate, and then paste it into a text file.
8. Save the file.

You may now import the signed certificate into ZoneDirector.

Importing an SSL Certificate

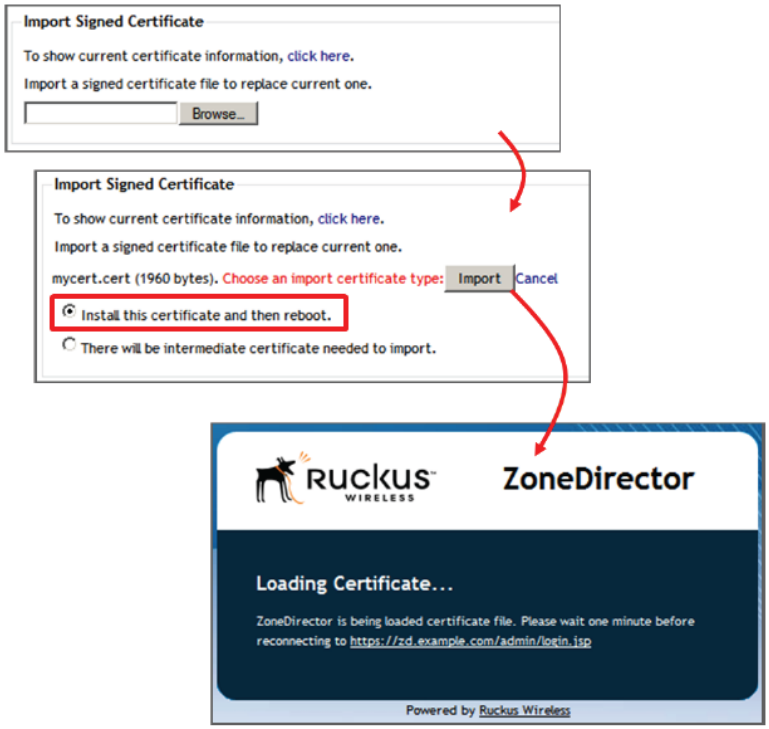
After you receive the signed certificate from the Certificate Authority, you must import it into ZoneDirector.

To import a signed certificate:

1. Click on the **Browse** button and select the file that contains the certificate (in PEM format) to upload it.

2. If there are no intermediate CA certificates, then click on the **Import** button to install the uploaded certificate. If the certificate does not match the currently installed private key you will be prompted to upload the correct private key.

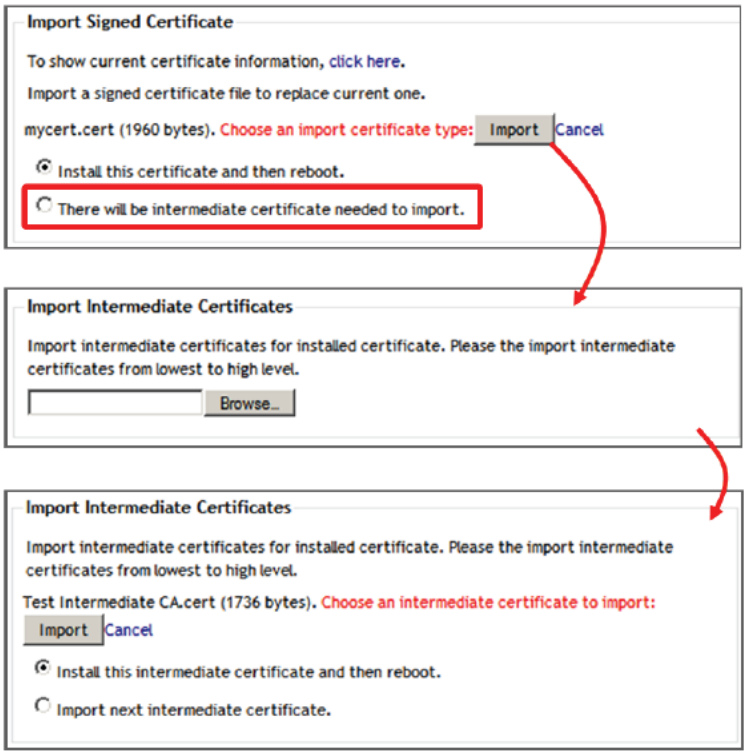
   FIGURE 270 Importing a signed SSL Certificate



3. If your ZoneDirector certificate was issued by an intermediate CA, then you must also import the intermediate CA's certificate (as well as all other intermediate CA certificates in the path to the root CA). In that event, you would receive an intermediate certificate:
   - After selecting the end certificate, click on the intermediate certificate import option.
   - Click the **Import** button to reveal the form.
   - Click the **Browse** button and select the file containing the intermediate certificate (PEM format) to upload it.
   - If there are no additional intermediate certificates, click the **Import** button to install the uploaded certificate.

4. Alternatively, you can simplify this process by appending the intermediate CA certificate(s) to the ZoneDirector certificate file. Then, you just need to import a single file. The intermediate certificate(s) will be imported automatically. In this case, you will see multiple ---BEGIN CERTIFICATE--- and ---END CERTIFICATE--- pairs in the file.

FIGURE 271 Importing a signed certificate (continued)



SSL Certificate Advanced Options

The **Advanced Options** section allows you to perform additional certificate management functions. These include the following:

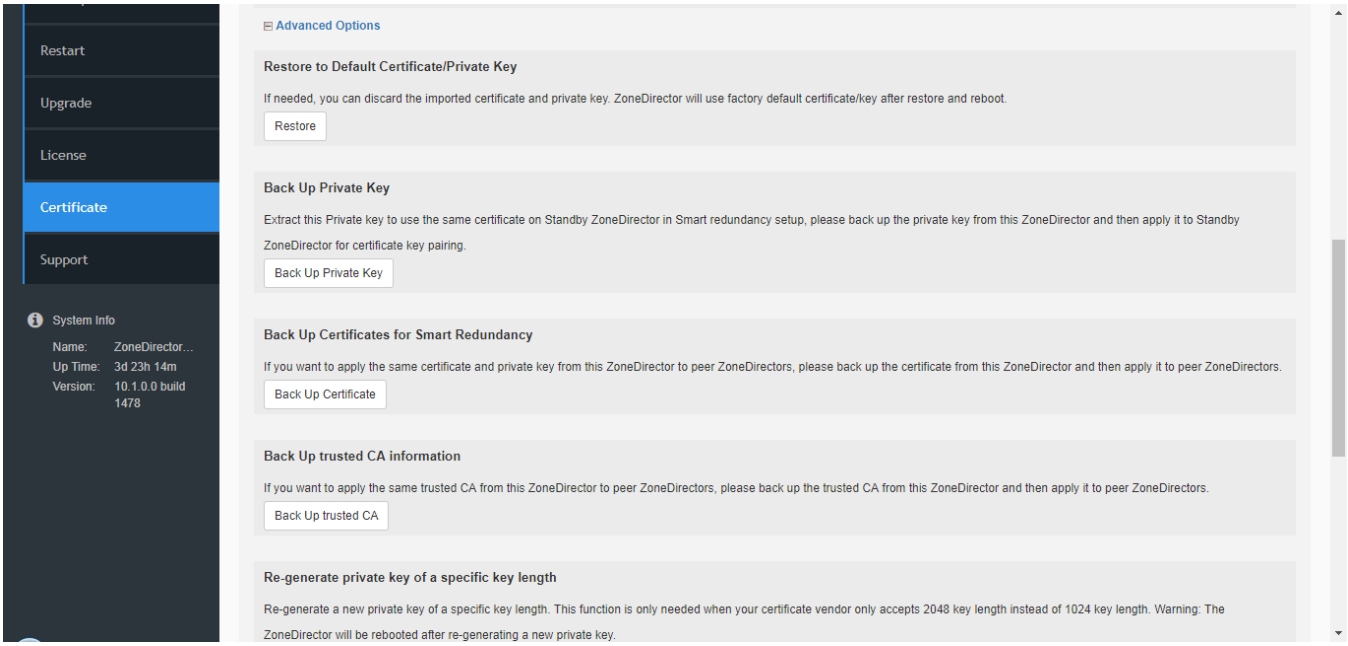
- Restore to Default Certificate/Private Key: This deletes any certificate and private key that has been imported, and restores the factory default certificate/private key after restore and reboot.

  NOTE
  Restoring ZoneDirector to factory defaults 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 ZoneDirector. If your ZoneDirector 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 two ZoneDirectors in a Smart Redundancy configuration, you can install the same SSL certificate/private key pair advertised in DNS for the same FQDN without seeing the security warning. If you wish to also use certificates in a Smart Redundancy configuration with captive portals such as Guest Access, Web Portal and Hotspot, see Wildcard Certificate Installation on page 355.

- Back Up Trusted CA Informationthis ZoneDirector to peer ZoneDirectors. The file is output as a .tar.gz file containing all trusted Certificate Authoritiy information currently installed on this ZoneDirector. This compressed file must be decompressed and the files imported into the peer ZoneDirector 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.
- Import Ruckus PKI Certificate Package: As of ZoneDirector release 9.13, all affected Ruckus APs can be upgraded with the new Ruckus Public Key Infrastructure (RPKI) certificate and key. See Importing Ruckus PKI Certificate Packages on page 351.

FIGURE 272 SSL Certificate Advanced Options



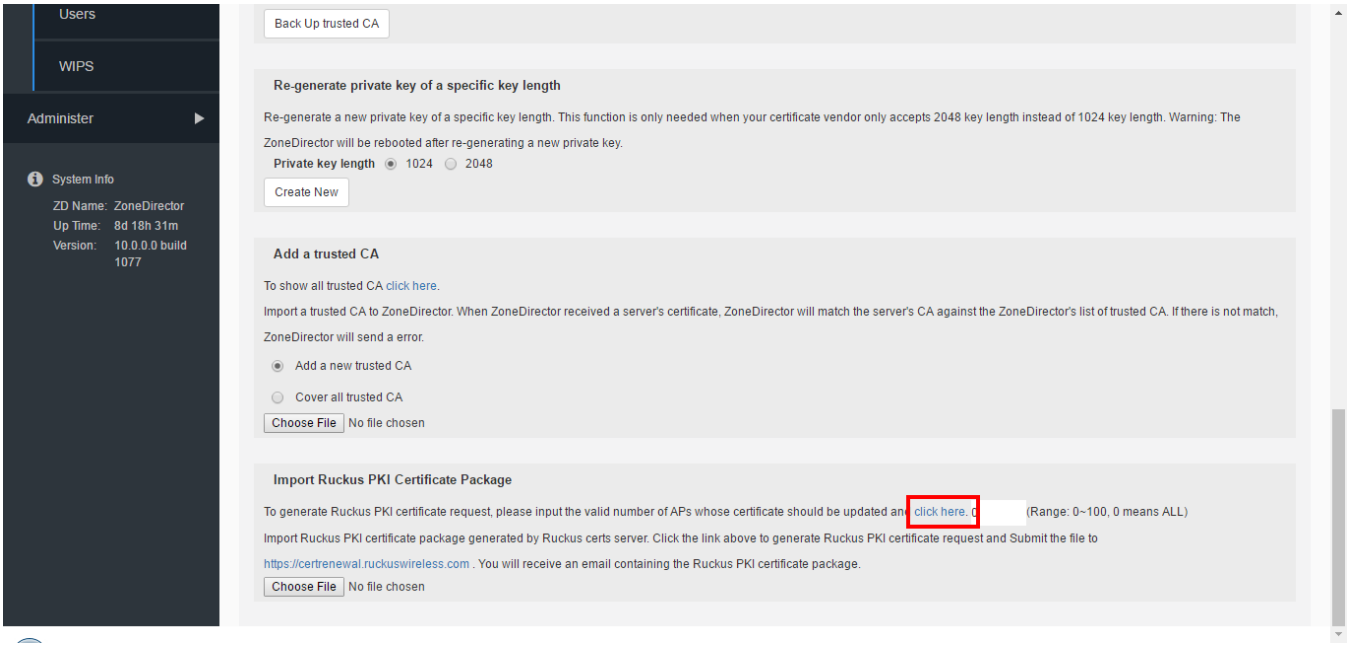
Importing Ruckus PKI Certificate Packages

To generate a Ruckus PKI certificate request:

1. Go to **Administer** > **Certificate**.

2. Locate the *Import Ruckus PKI Certificate Package* section, and click the **click here** link. The content of the current certificate file is displayed.

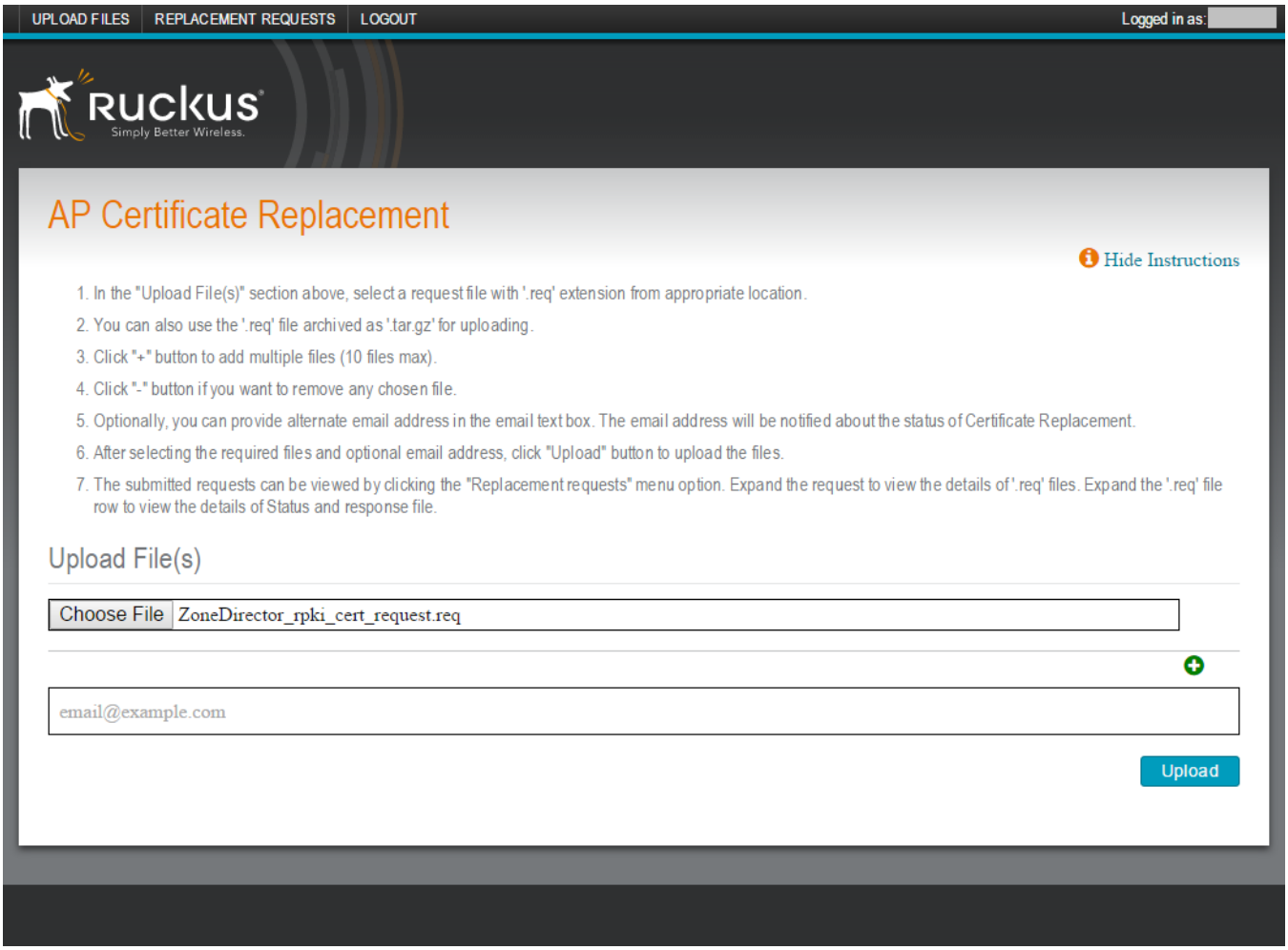
FIGURE 273 Import Ruckus PKI Certificate Package



3. A file named "ZoneDirector1200_rpki_cert_request.req" (or similar) will be generated. Save the file to your local computer.
4. Launch a web browser, and go to the following URL: *https://certrenewal.ruckuswireless.com/certificate_renewal_requests/new*. You will need to login to the Ruckus Support portal to continue.

5. Once logged in, you will be redirected to the **AP Certificate Replacement** page.

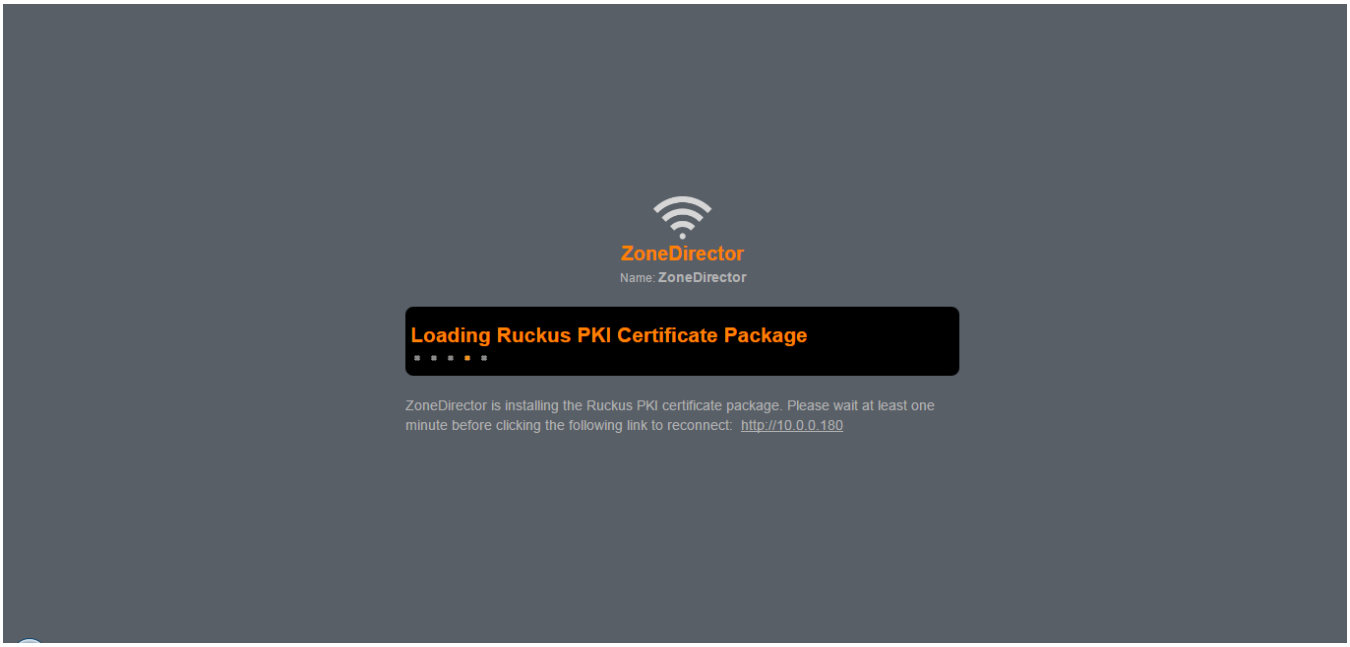
FIGURE 274 AP Certificate Replacement page



6. In the **Upload Files** section, click **Choose File**, and locate the text file you saved to your local computer.
7. Click **Upload**. Your request will be delivered to Ruckus, and you will receive an email confirmation.
8. Once Ruckus has completed the processing of your request, Ruckus will send another email with a link to download the certificate package.
9. Click the link in the email and download the package to your local computer. (The file name will be similar to: `ZoneDirector_rpki_cert_request_20160405191623397.res`.)
10. On the SSL Certificate Advanced Options click **Choose File** to import the new certificate package (*.res file). The file is uploaded to ZoneDirector.
11. Click **Import** to import the new certificate package.

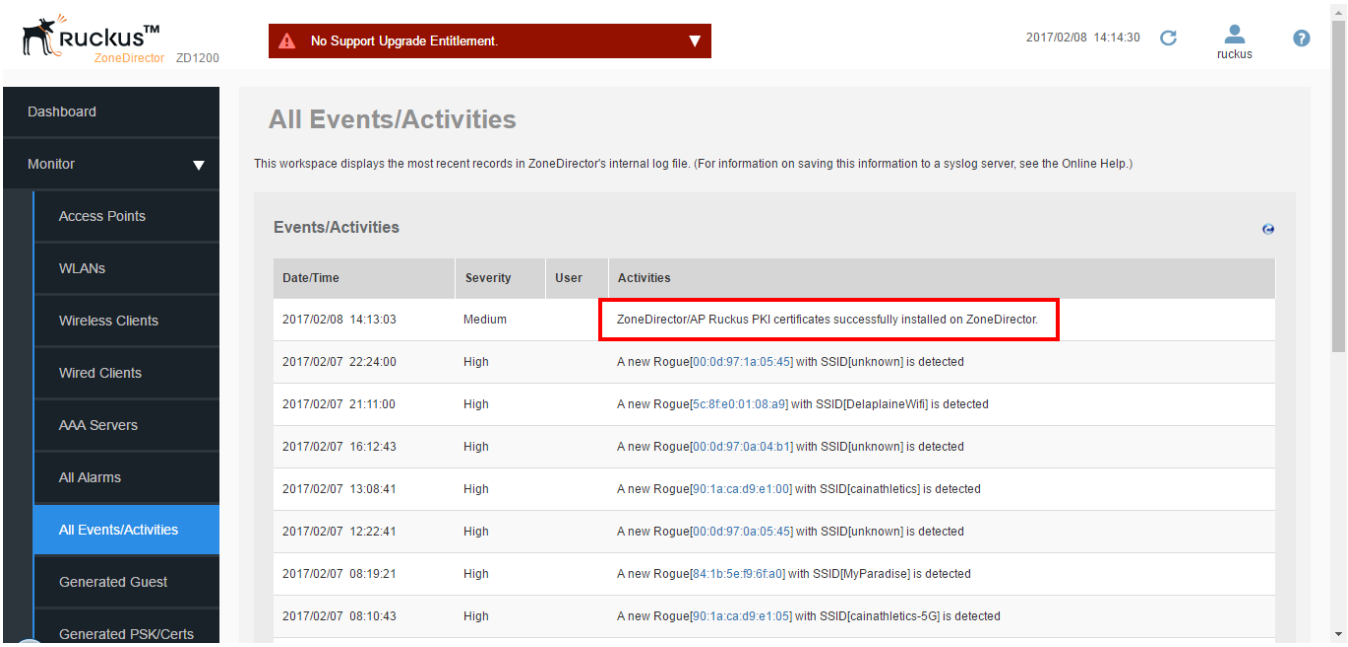
12. A “Loading Ruckus PKI Certificate Package…progress screen to complete importing the new package (this process should take approximately one minute).

FIGURE 275 Loading Ruckus PKI Certificate Package



13. Once complete, log back into ZoneDirector, and on the **System > All Events/Activities** page, you should see the following event message: "ZoneDirector/AP Ruckus PKI certificates successfully installed on ZoneDirector."

FIGURE 276 Ruckus PKI certificates successfully installed



You have completed upgrading your ZoneDirector and connected APs with the new RPKI certificates and keys.

Wildcard Certificate Installation

A wildcard certificate is a generic certificate that can be used for multiple devices in a specific domain. This is useful for Smart Redundancy installations where you have two ZoneDirectors. You can purchase and install two certificates, or use a wildcard certificate.

When you try to import a wildcard certificate, the ZoneDirector will notify you that it does not have the matching private key. At this point, click on the “click here” link to import the private key. Once the private key is imported, try to import the certificate again. The ZoneDirector will prompt you for the host name. Enter the hostname and ensure that your DNS server is configured to resolve that name to the IP address of ZoneDirector.

Wildcard Certificates In Smart Redundancy With Captive Portals

In order to prevent redirect loops when deploying SSL certificates in a Smart Redundant following wildcard certificate procedure:

1. Purchase or generate a self-signed wildcard certificate such as *.acompany.com and install it on both ZoneDirectors in the Smart Redundant pair.
2. In DNS, add 3 host/IP entries similar to the following
   - management.acompany.com; 192.168.0.100: This is the FQDN you wish to use for reaching the shared virtual management interface and is mapped to its configured IP address
   - primary-zd.acompany.com; 192.168.0.98: This is the FQDN for the primary ZD controller and its physical IP address.
   - backup-zd.acompany.com; 192.168.0.99: This is the FQDN for the backup ZD controller and its physical IP address
3. When you import the wildcard certificate into the ZoneDirectors you will be prompted to enter the host name – make sure you use the same host name as you will advertise in DNS for that ZoneDirector (the default is the same configured ZoneDirector name).

NOTE
Currently it is not possible to support this configuration with the Hotspot captive portal when it is being used for Zero-IT activation through the ZoneDirector because the FQDN for the “/activate” URL is identical on both ZoneDirectors. To achieve this use the Onboarding Portal feature for Zero-IT activation.

Monitoring Your Wireless Network

- Reviewing the ZoneDirector Monitoring Options....357
- Monitoring Access Points....357
- Monitoring WLAN Status....366
- Reviewing Current User Activity....367
- Monitoring Wired Clients....373
- Monitoring AAA Server Statistics....373
- Reviewing Recent System Events....374
- Reviewing Current Alarms....374
- Monitoring Location Services....375
- Monitoring Mesh Status....376
- Real Time Monitoring....377
- Detecting Rogue Access Points....379
- Monitoring System Information....381

Reviewing the ZoneDirector Monitoring Options

The ZoneDirector web interface provides many options for monitoring all aspects of your wireless networks, including the controller itself, all connected APs, wireless LANs, wireless clients, applications, guest passes, alarms and events, and rogue devices.

Monitoring Access Points

ZoneDirector provides several features for monitoring the status and performance of your APs.

The following are a few ways you can quickly locate information on the APs that ZoneDirector is managing:

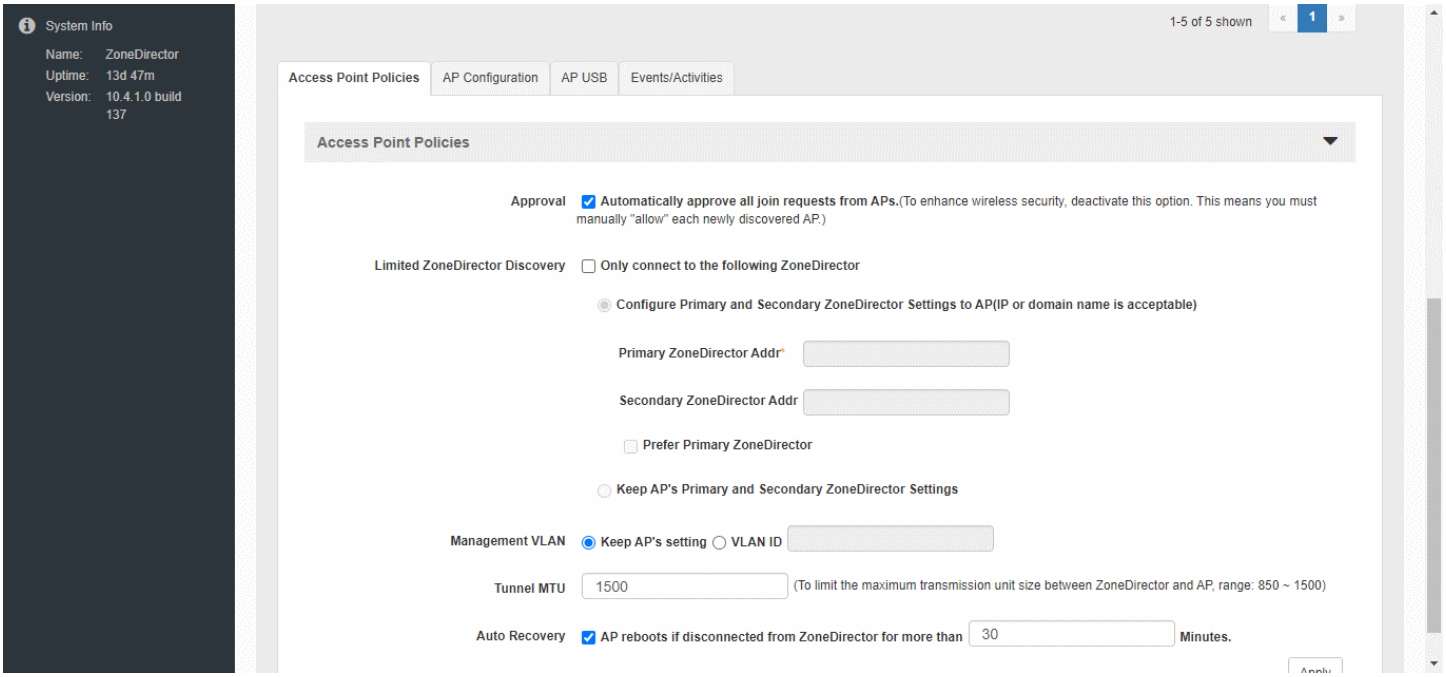
1. Locate APs on the map view of the **Dashboard**. Zoom in to any venue map, and click the MAC address link of any AP record to see more details.
2. Go to **Access Points** and review the usage and coverage of your APs. Click the MAC address link of any listed AP to see more details.

Using the AP Status Overview Page

The *Access Points* page provides an overview of currently managed APs.

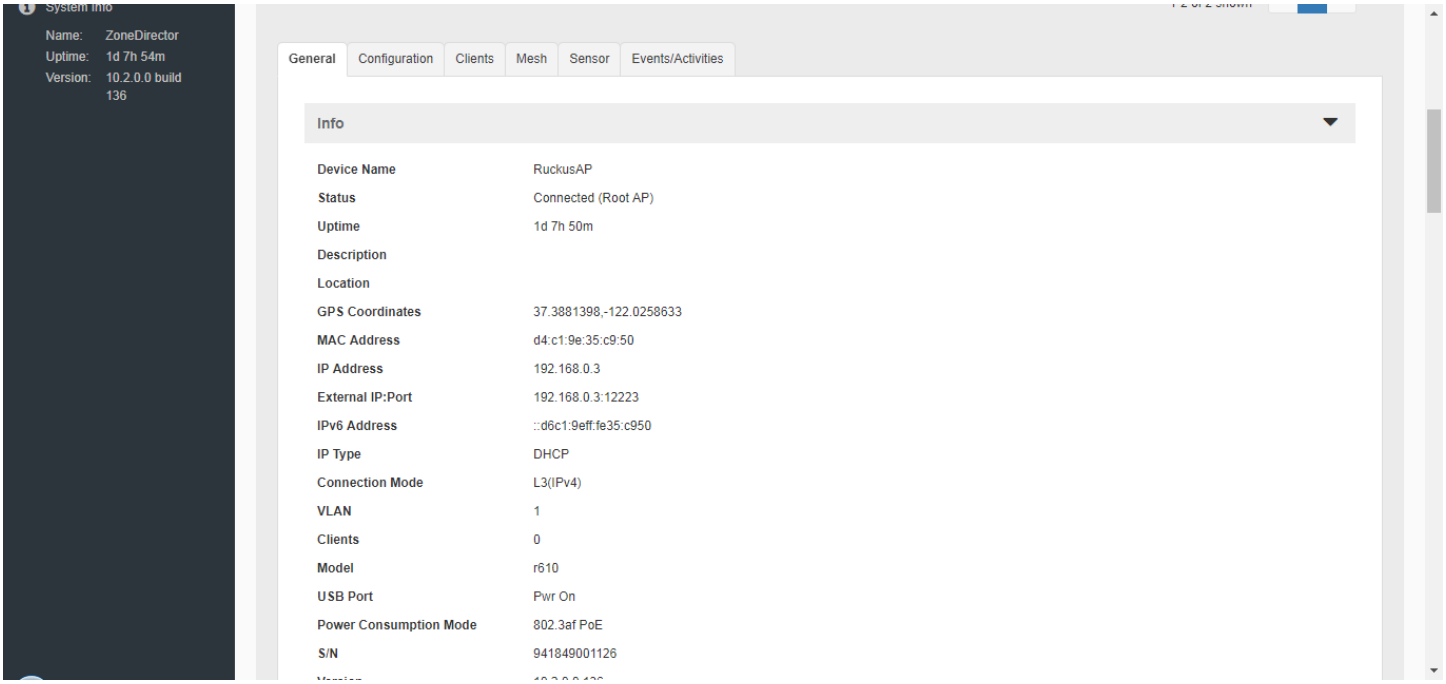
When no AP is selected, the bottom section of the page contains global configuration options including AP policies, importing an AP configuration file, importing an AP USB software package, and viewing a list of AP-related events/activities.

FIGURE 277 AP global options



Click on an AP from the list, and the bottom section of the page changes to display detailed information on that AP. Click any of the tabs to monitor or configure AP-specific information and settings.

FIGURE 278 Monitoring an AP's general information



Currently Managed APs

Click on any AP in the *Access Points* list to view details on that specific AP.

The *General* tab provides the following information:

TABLE 29 Access Points page AP details information

Heading	Description
Device Name	The AP's "name."
Status	Displays the current status of the AP from ZoneDirector's perspective: • Approval Pending • Connected • Disconnected • Root AP • Mesh AP • eMesh AP • Number of hops
Uptime	The amount of time since the last AP reboot or power cycle.
Description	The AP's description, if configured.
Location / GPS Coordinates	The AP's location, if configured. This can be modified by configuring GPS coordinates on the AP configuration page.
MAC Address	The AP's MAC address.
IP Address	The IP address of the AP.
External IP: Port	The public IP address and port number for APs connected via Layer 3 behind a NAT device.
IPv6 Address	The AP's IPv6 address, if IPv6 addressing is enabled.
IP Type	The IP address acquisition method; dynamic (DHCP) or manual.
Connection Mode	Layer 2 or Layer 3/4 connection method.
VLAN	The VLAN ID, if configured.
Clients	The number of clients currently connected to this AP.
Model	The AP's model number.
USB Port	USB port power status; on or off.
LACP/LAG	Link aggregation status; enabled or disabled.
Power Consumption Mode	The current AP power mode; DC power, 802.3af, 802.3at, etc.
S/N	The AP's serial number.
Version	The current firmware version on the AP.
Bonjour Gateway	Indicates whether Bonjour Gateway service is enabled, disabled or not supported on this AP.
Bonjour Fencing	Indicates whether Bonjour Fencing is enabled, disabled or not supported on this AP.
Action	These icons allow you to configure and troubleshoot APs individually. See *Using Action Icons to Configure APs*.

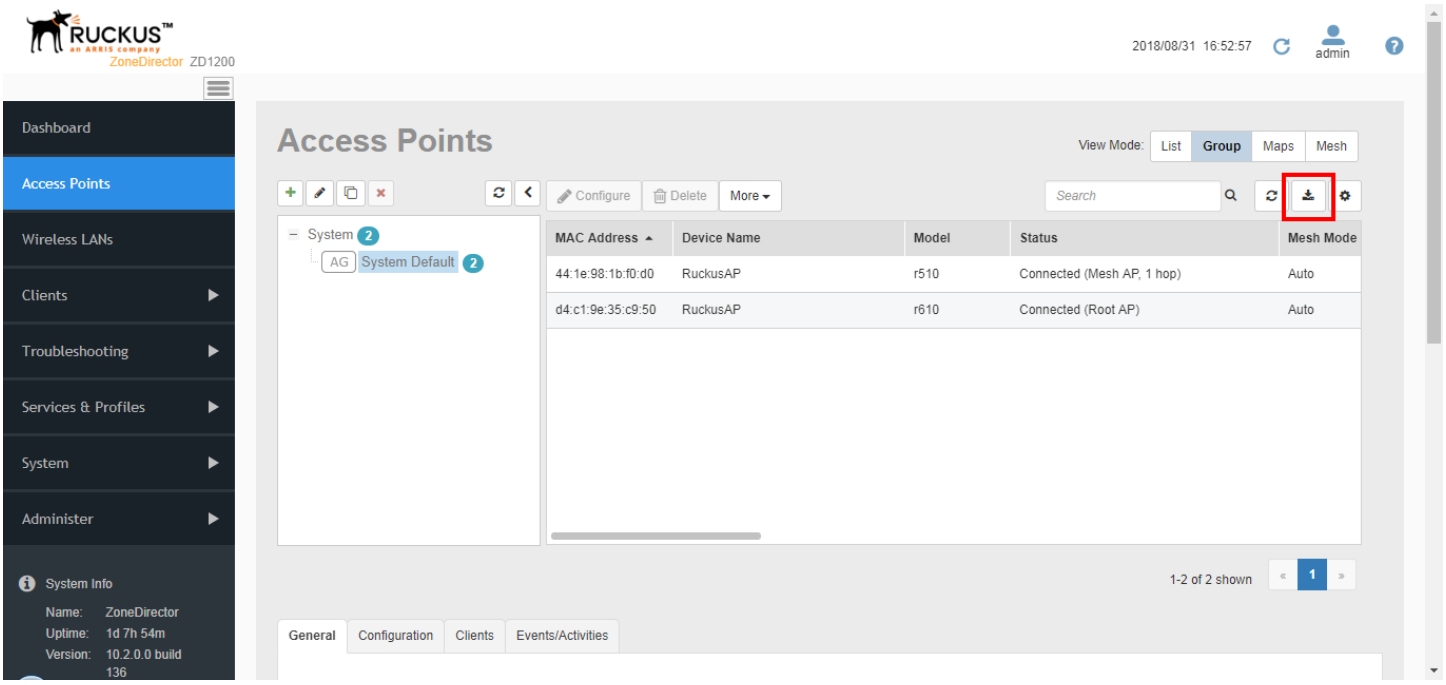
Exporting the AP List to a CSV File

The Access Points table can be exported as a CSV file, which can be opened in a spreadsheet program such as Microsoft Excel.

If the search box is empty, all APs will be saved to the CSV file. If you enter text in the search box, only the APs currently matching the search text will be exported.

Click **Export to CSV** to download the AP list.

FIGURE 279 Exporting the AP list to a CSV file

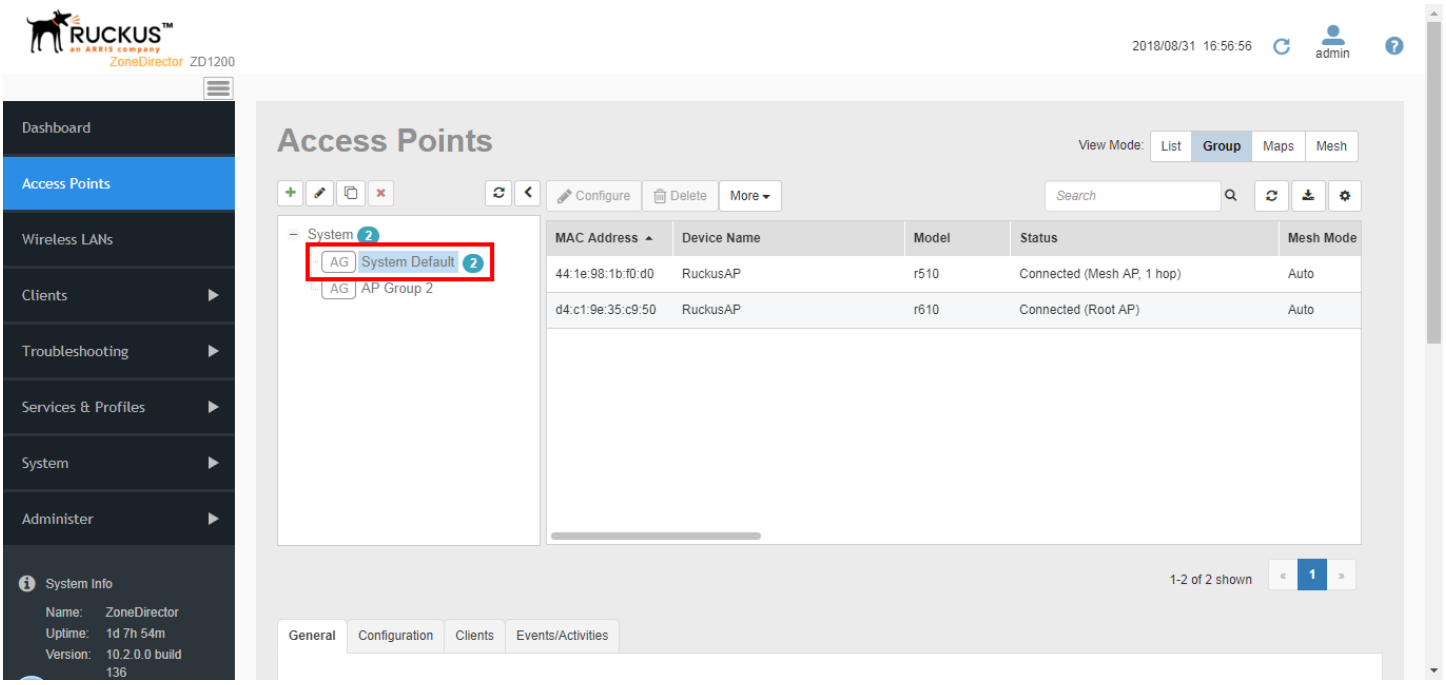


Currently Managed AP Groups

Click on an AP Group from the list of AP Groups (beginning with "System Default" AP Group) on the left side of the *Access Points* page to display all members of the group.

When an AP Group is selected, the bottom section of the page changes to display detailed information about that AP Group. View group status details in the **General** tab, configure group settings in the **Configuration** tab, manage clients in the **Client** tab and view group-related events in the **Events** tab.

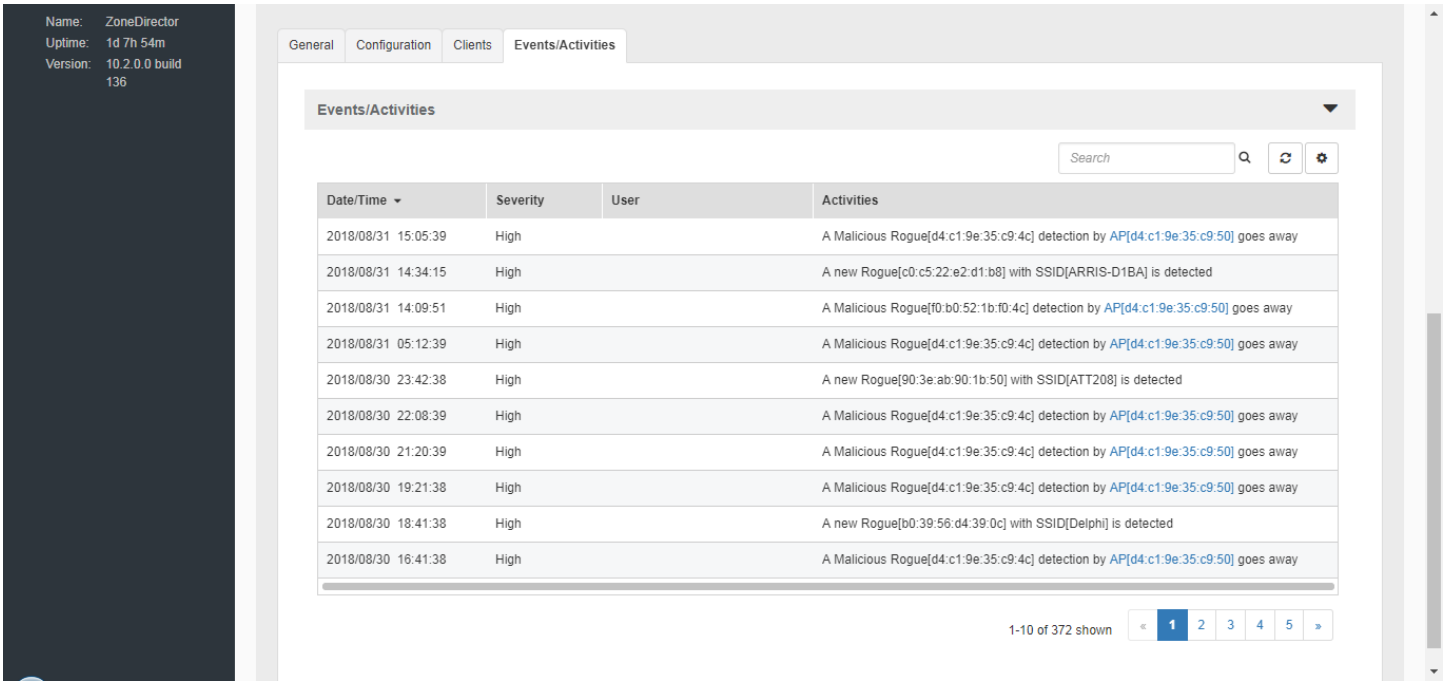
FIGURE 280 Selecting an AP Group



Events/Activities

The *Events/Activities* table displays an AP-specific or AP-group-specific subset of the events listed on the *All Events/Activities* page.

FIGURE 281 AP-specific events



Monitoring Individual APs

When you click on the MAC address of any AP, the Access Points page changes to a detailed view of information related to that specific AP.

The **Access Points** page provides the following details on the specific AP:

TABLE 30 AP Information details

Heading	Description
General Information	Displays general information on the AP, including software version, IP address and model number, uptime, clients and mesh status.
Actions	Action icons provide tools for managing the AP (see *Using Action Icons to Manage APs*).
Radio 802.11(b/g/n or 11a/n/ac)	Displays details on the 2.4 GHz (b/g/n) and 5 GHz (a/n/ac) radios. Transmission statistics are totals since last radio restart. Airtime % statistics represent the time spent sending (Tx) and receiving (Rx) 802.11 frames, plus the time spent waiting for non-802.11 interference to avoid collision (busy). Free airtime is 100% - total. High numbers indicate contention in the channel.
LAN Port Configuration	Displays the current configuration of the AP's LAN ports, including their enabled state, type (Access Port or Trunk Port), and Access VLAN ID.
LAN Port Status	Displays the status of the Ethernet ports, whether the link is up or down and the speed/duplex status.
Neighbor APs	Displays nearby APs, their channel and signal strength.
WLANs	Displays the WLANs that this AP is supporting, including SSID name, BSSID MAC address, radio type and up/down status.
Performance	Displays a graphical view of AP performance and RF environment statistics. Three Performance analysis graphs plot the capacity, throughput, associated clients and RF contention in the channel as a function of time. The estimated capacity is of downlink traffic and is updated only when the AP transmits more than 1000 packets, each containing at least 1024 bytes of data, within a one-minute measurement interval. The uplink and downlink throughput curves show the actual throughput of a particular client or the current mix of clients. These curves are influenced by the user session, and they vary as a function of gaps in browsing activity and internet server response times. The RF Pollution graph plots a proprietary metric describing the impediment due to other RF signals competing for use of the channel over time. (See RF Pollution FAQ on page 364 for more information)
Mesh-related Information	Displays uplink/downlink information, transmission statistics and details on mesh signal strength and stability (if mesh is enabled).
Sensor Information	Displays AP orientation and temperature details as reported by the AP's internal sensors (not supported on all APs). See Access Point Sensor Information on page 366 for more information.
Clients	Displays a list of the currently connected clients. Action icons can be used to configure or troubleshoot a client from this list.
Events/Activities	Displays an AP-related subset of the All Events / Activities table.

Using Action Icons to Manage and Troubleshoot APs

The following action icons can be used to perform configuration and troubleshooting tasks on a specific AP.

TABLE 31 Action icons

Icon	Icon Name	Action
	System Info	Generate a log file (support.txt) containing system information on this AP.
	RF Info	Generates a log file called info.txt, containing radio frequency data that can be used for troubleshooting the RF environment.
	Configure	Go to the **Access Points** page and edit the configuration settings for this AP.
	SpeedFlex	Launch the SpeedFlex performance test tool to measure uplink/downlink speeds to/from this AP.

TABLE 31 Action icons (continued)

Icon	Icon Name	Action
	Mesh View	Open a "Mesh View" screen with this AP highlighted in a Mesh tree that also shows any uplink and downlink APs connected to this AP.
	Troubleshoot	Troubleshoot connectivity issues using Ping and Traceroute.
	Restart	Initiate a reboot of this AP.
	Recover	Recover an isolated Mesh AP
	Allow	Allow this AP to be managed by ZoneDirector. This icon will only appear if you have disabled automatic approval under "Access Point Policies" on the **Access Points** page.
	Join Another Controller	Click this button to migrate an AP to another controller.
	Spectrum Analysis	Launch the Spectrum Analysis window.
	Performance	Launch the AP Performance window.

Migrating an AP from ZoneDirector to Another Controller

The Migrate (join another controller) button allows you to migrate ZD-controlled APs to SmartZone or Ruckus Cloud control. When clicked, the AP is blocked from joining ZoneDirector, enables a SmartZone discovery client and reboots. After the reboot it begins searching for a new controller, either on premises or in the cloud.

Once the **Migrate** button is clicked, the following two actions will be taken:

1. The AP's SmartZone discovery process - called "wsgclient" - will be started.
2. Zonedirector will ignore this AP's discovery requests; ZD blocks the AP from joining until the block is manually removed.

The AP can discover SZ as usual, via any of the following methods:

- mDNS discovery on local IP subnet
- DHCP Option 43 sub-option 6
- DHCPv6 Option 17 sub-option 6
- DHCPv6 Option 52
- DNS entry named "ruckuscontroller.<local domain>"
- AP CLI command "set scg ip"

For more information on these SmartZone discovery methods, refer to the *SmartZone Admin Guide*.

NOTE
If you have blocked an AP this way and want to allow it to join ZoneDirector again, go to **Access Points**, select the AP from the AP list, and click the **Allow** button.

RF Pollution FAQ

What is RF Pollution?

- "RF Pollution" is a linear index used to describe the level of performance-impacting RF contention and interference that an AP is experiencing. It distills several low-level MAC and PHY-level error metrics into a single parameter. Values can range from 0 to infinity, although in most normal environments the RF Pollution index will average between 10 and 100. Higher values indicate a noisier environment.
- What is RF Pollution measuring? It is measuring the level of RF contention and interference experienced by the AP. It distills several low-level MAC and PHY-level error metrics into a single parameter.
- How is RF Pollution different than noise? Noise may or may not have an impact on performance. RF Pollution is a measure of noise or other interference that is in fact impacting performance.
- How do customers use this new concept to understand and manage their WiFi networks? RF Pollution is an informational metric. BeamFlex and ChannelFly use a variant of this metric and other throughput-based metrics internally to optimize the RF so that you don't have to.
- Why is Ruckus using this new term vs. the existing measurements such as PHY errors, CRC errors, etc.? PHY Errors and CRC errors can be very misleading metrics because there is no standard way for the chipset to report them. Different chipsets can report these errors in different ways and certain types of noise can even mask these errors entirely. RF Pollution is a more stable metric that will never produce misleading results.

Spectrum Analysis

Spectrum analysis provides two real time views of the RF environment using data generated by the AP to chart power levels across the 2.4 and 5GHz frequency bands.

- **Instantaneous Samples View** (top view): The instantaneous samples plot provides a real time display of signal power across the entire 2.4 or 5GHz frequency bands. The plot is color-coded based on the signal power within each part of the frequency band. Red represents stronger signals while weaker signals are closer to blue.
- **CDF of Samples View** (bottom view): This graph displays the concentration of signal power readings within each portion of the frequency band in a cumulative distribution format. The CDF plot is color-coded based upon the frequency with which each point is observed during consecutive spectral sweeps of the entire 2.4/5Ghz frequency band. Frequently occurring points are marked 'red', moderately occurring points are marked 'yellow', and occasionally occurring points are marked 'green'.

To view spectrum analysis data for an access point:

1. Go to **Access Points** and click the MAC address of the AP to view the AP detailed information.
2. Click the **Spectrum Analysis** icon in the "Actions" table. (APs that do not support this feature do not display this icon).
3. The **Spectrum Analysis** display opens in a new window.
4. Select **2.4G** or **5G** to choose the frequency band for which spectrum analysis data will be collected, and click **Start Monitoring** to begin.

FIGURE 282 APs that support spectrum analysis display an extra icon in the Actions table

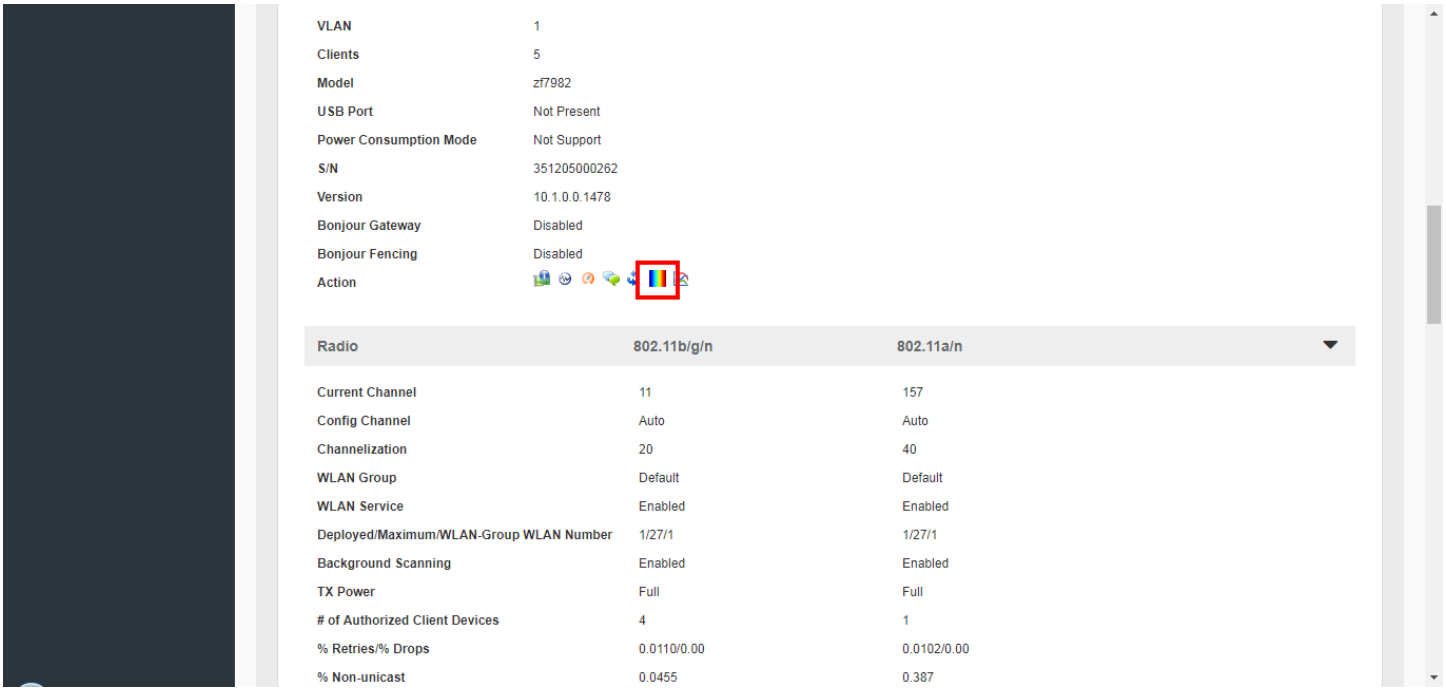
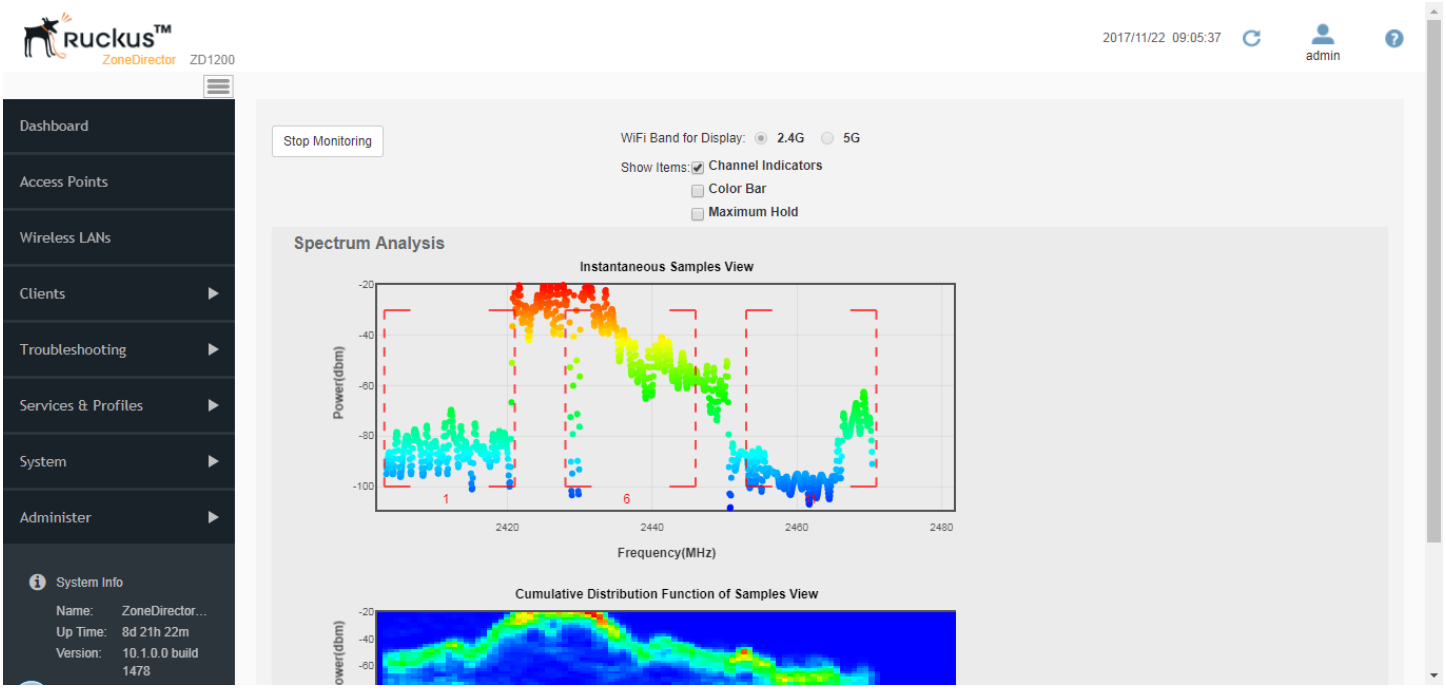


FIGURE 283 Performing Spectrum Analysis on the 2.4 GHz radio



Neighbor APs

ZoneDirector uses several calculations to determine which APs are in proximity to one another. This information can be useful in planning or redesigning your Smart Mesh topology or in troubleshooting link performance issues.

Details on neighbor APs include:

- Access Point: The AP's description, if configured, or the MAC address if no name or description is available.
- Channel: The channel that the neighbor AP is currently using.
- SNR (dB): Signal to Noise Ratio. SNR is the difference between the received signal from the neighbor AP and the noise floor. A higher number indicates a better signal. For example, if the AP you are currently viewing receives a signal of -30 dBm and the noise floor is measured at -90 dBm, the SNR is 60 dB.
- Path Score (status): A higher score indicates better performance over the link between this AP and its neighbor.

Access Point Sensor Information

If your APs include internal sensors, ZoneDirector will display the AP's status in this section. Temperature and orientation sensors are available on most Ruckus outdoor APs.

Orientation

- Desktop/Horizontal Mount
- Ceiling/Horizontal Mount
- Wall/Vertical Mount

Temperature

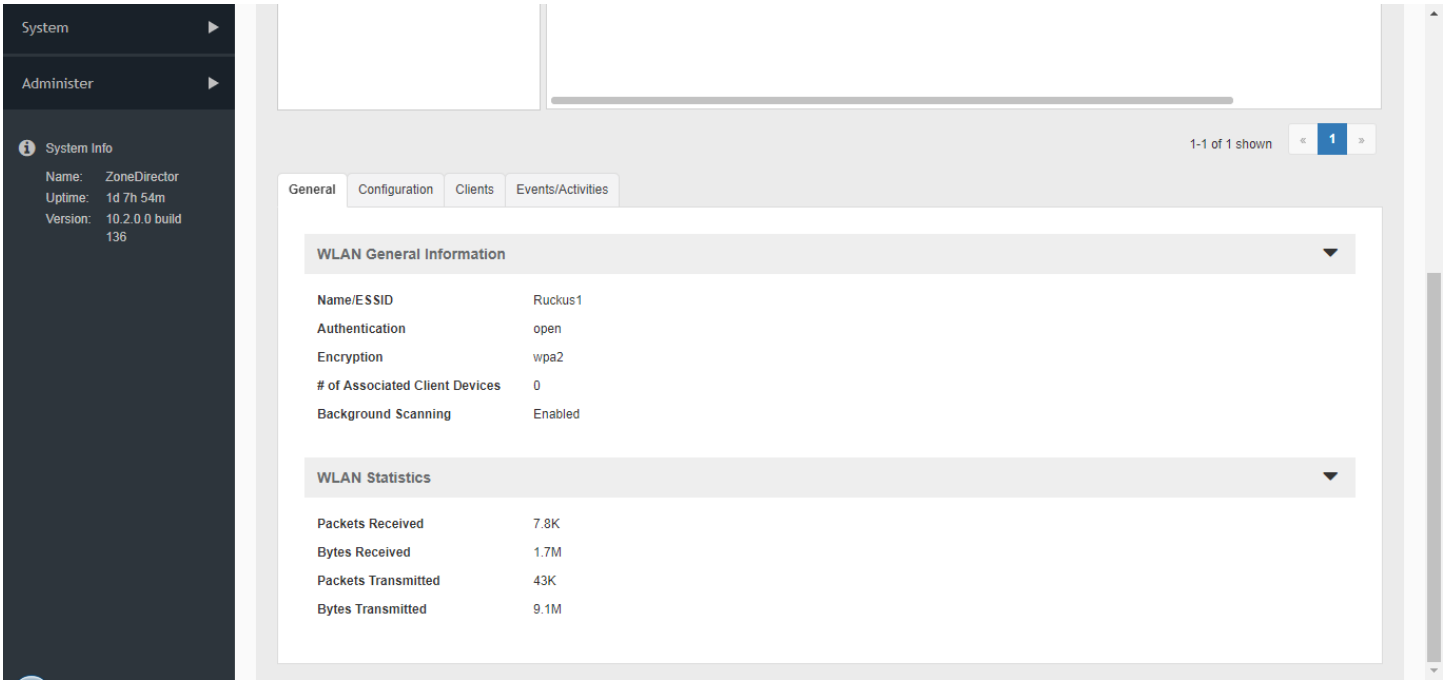
This sensor displays the temperature statistics as reported by the AP.

Monitoring WLAN Status

The **Wireless LANs** page lists the currently deployed WLANs, WLAN Groups, VLAN Pools, Events/Activities and RADIUS statistics (for WLANs that use RADIUS authentication).

Click on a WLAN **Name** to view detailed information on a specific WLAN. Click any of the **General**, **Configuration**, **Clients** or **Events/Activities** tabs to view further details.

FIGURE 284 Viewing WLAN general information



Reviewing Current User Activity

You can monitor current wireless users by viewing a general overview of all currently connected clients, and on a per-client basis.

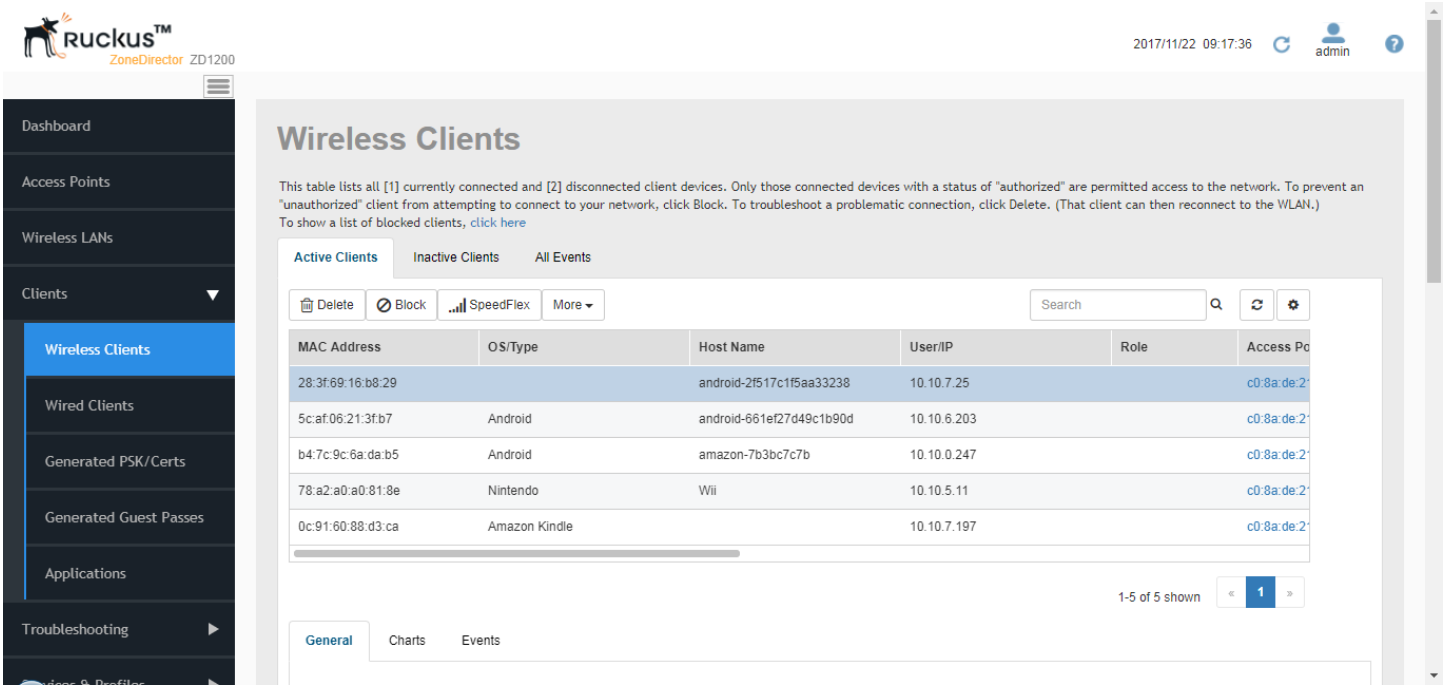
1. Go to **Clients** > **Wireless Clients**.
2. In the **Active Clients** table, click any client's device **MAC address** link to monitor that client in more detail.

Additionally, you can perform a number of actions on individual clients from this page, including blocking unauthorized clients, deleting clients from the table (which will allow them to attempt to reconnect), testing throughput using SpeedFlex, and testing connectivity using Ping and Traceroute, using the Action icons.

The Wireless Clients monitoring page also includes the following details on active and recently active clients:

- **Active Clients**: The Active Clients tab displays a list of active wireless clients. You can customize the columns displayed by clicking the **Configure Table** button. You can also delete, block, run SpeedFlex and test connectivity using the action icons in this table.
- **Inactive Clients**: The Inactive Clients tab displays a list of inactive clients and can be used to view usage statistics of recently disconnected clients.
- **All Events**: The All Events tab displays a client-specific subset of the events listed on the All Events/Activities page.

FIGURE 285 Monitoring Wireless Clients



Active Client Action Icons

The following Action icons can be used for configuration and troubleshooting of an individual client.

TABLE 32 Client Action Icons

Icon	Name	Description
	Delete	Delete a client record. See Temporarily Disconnecting Specific Client Devices on page 233.
	Block	Permanently block a client device. See Permanently Blocking Specific Client Devices on page 234.
	SpeedFlex	Launch the SpeedFlex performance test tool to measure uplink/downlink speeds to/from this client. See Measuring Wireless Network Throughput with SpeedFlex on page 205.
	Network Connectivity	Troubleshoot connectivity issues using Ping and Traceroute. See Using the Ping and Traceroute Tools on page 202.

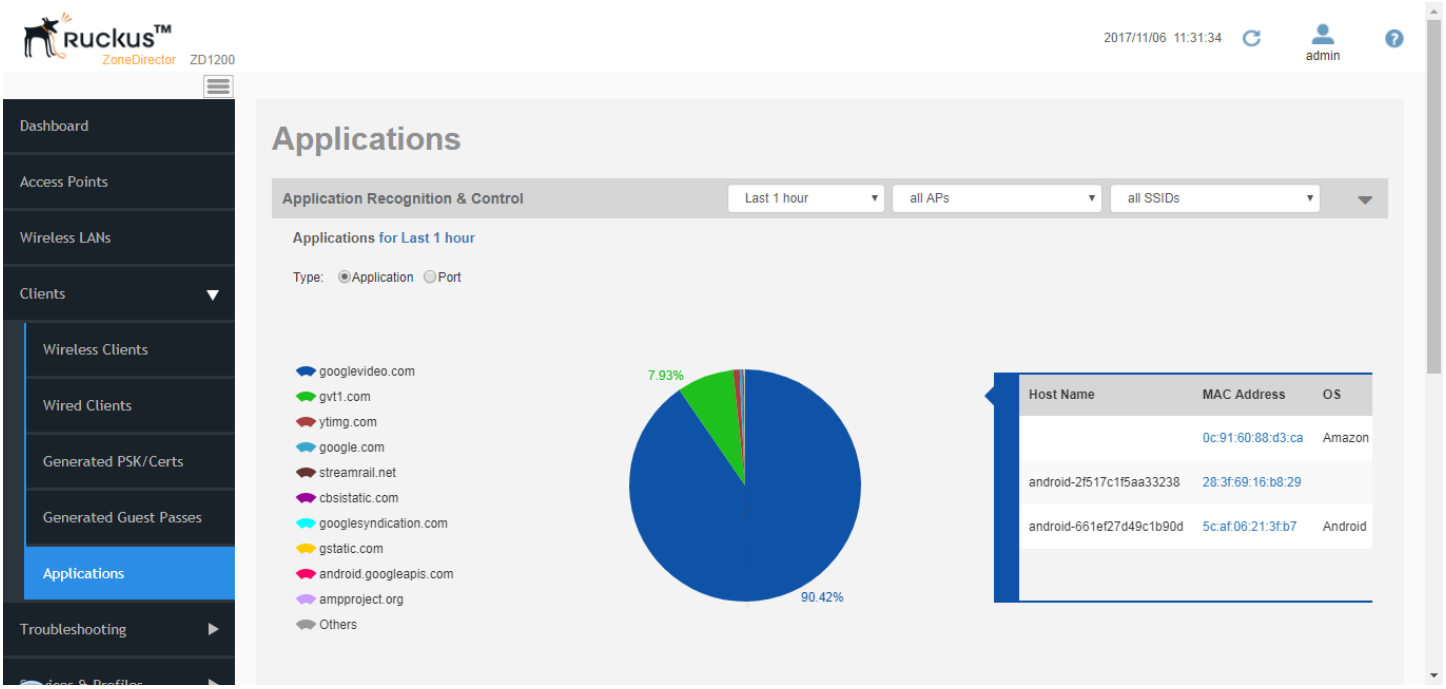
Viewing Application Usage Statistics

The Applications/Ports pie chart displays user activity by application or port for the selected time span. The Application Performance chart displays uplink and downlink throughput over time.

Select time span, AP group and SSID to change or filter the values displayed in the charts.

Click the **Show Details** button to display detailed application or port usage percentages. Click **Top 10 Clients** to view applications used by the top 10 clients only.

FIGURE 286 Monitoring Applications for the last 1 hour



Viewing Application Usage by Client

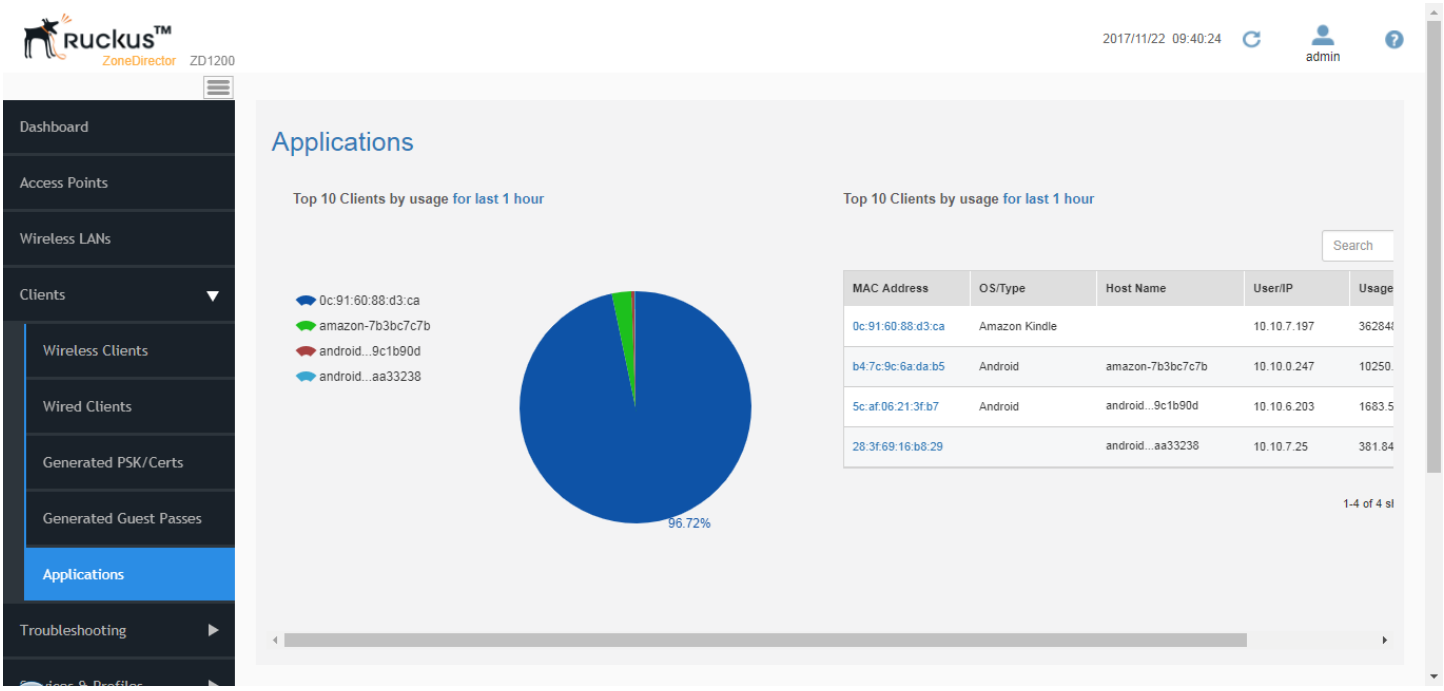
The Applications pie chart can also be used to discover which clients are using the most used applications.

When you mouse over a section of the pie chart, a table is displayed to the right providing a list of the top clients responsible for this traffic.

Viewing the Top 10 Clients by Usage

Clicking the Top 10 Clients button launches a new web page with a pie chart and table displaying the top 10 clients by traffic volume.

FIGURE 287 Viewing the top 10 clients by usage for the last 1 hour



Monitoring Individual Clients

You can monitor individual wireless clients by clicking on the MAC address of any connected client from the *Clients* page, the *All Events/Activities* page and other tables where client information is displayed.

To view detailed information about a specific client:

1. Go to **Clients** > **Wireless Clients**.
2. Click the client you want to monitor. The bottom part of the page refreshes to display a page of client specific information and statistics. The wireless client details contains the following tabs, which can be used to access additional information about the connected client.

Heading	Description
General	• Displays general information on the client, including Host Name, OS, AP, WLAN, channel, traffic and signal strength statistics. • The general tab also displays current AP receive signal strength (in dB), as well as AP transmit data rate. The Tx Data Rate value consists of the MCS value (Modulation and Coding Scheme; for a list of MCS codes, see http://en.wikipedia.org/wiki/IEEE_802.11n-2009), the channel width (20S or 40S), and the data rate in Mbps. • Contains a **Client Performance** icon (see Monitoring Client Performance on page 371).
Charts	Displays client application usage and throughput in pie chart and time graph formats.
Events/Activities	Displays a client-specific subset of the events in the All Events/Activities table.

Monitoring Client Performance

The Client Performance graph can be used to track the uplink/downlink throughput and estimated capacity of a specific client over time.

To monitor a client's performance:

1. Go to **Clients** > **Wireless Clients** and select the client from the Active Clients list.

2. Click the **Client Performance** icon to launch a new browser page displaying client throughput and capacity over time. Select a time increment and the chart updates immediately.

FIGURE 288 Click the Client Performance icon to view performance statistics

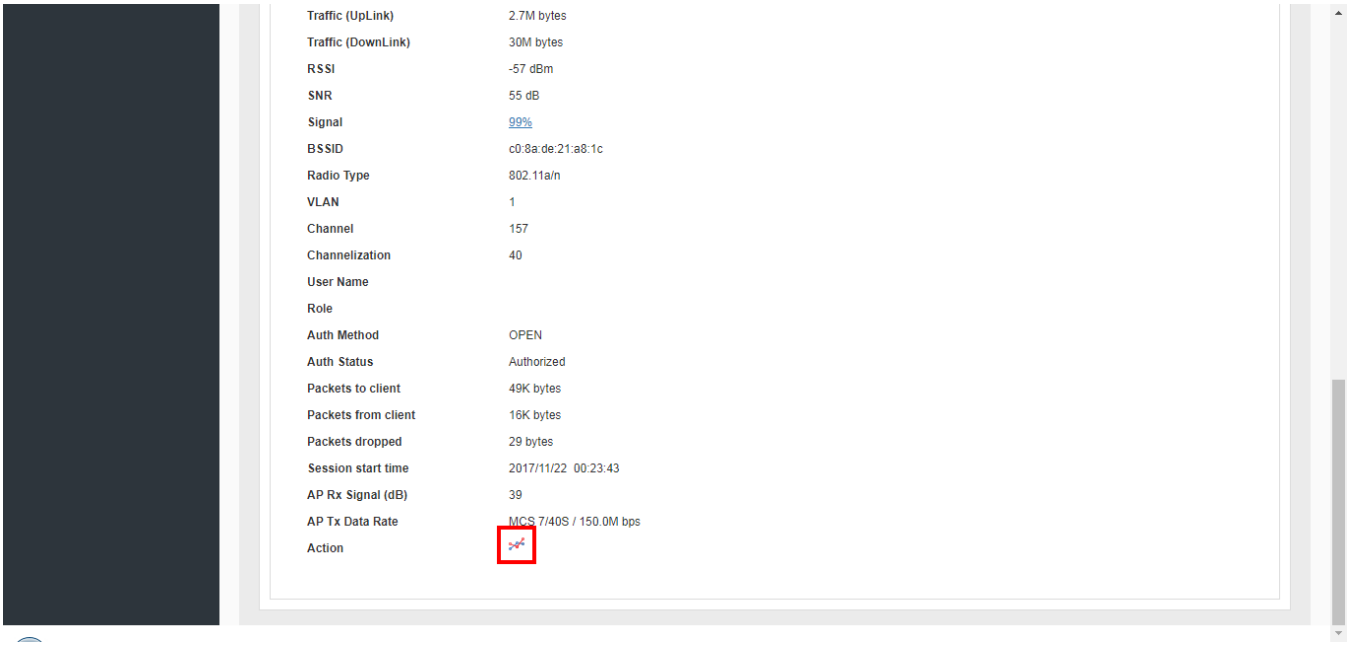
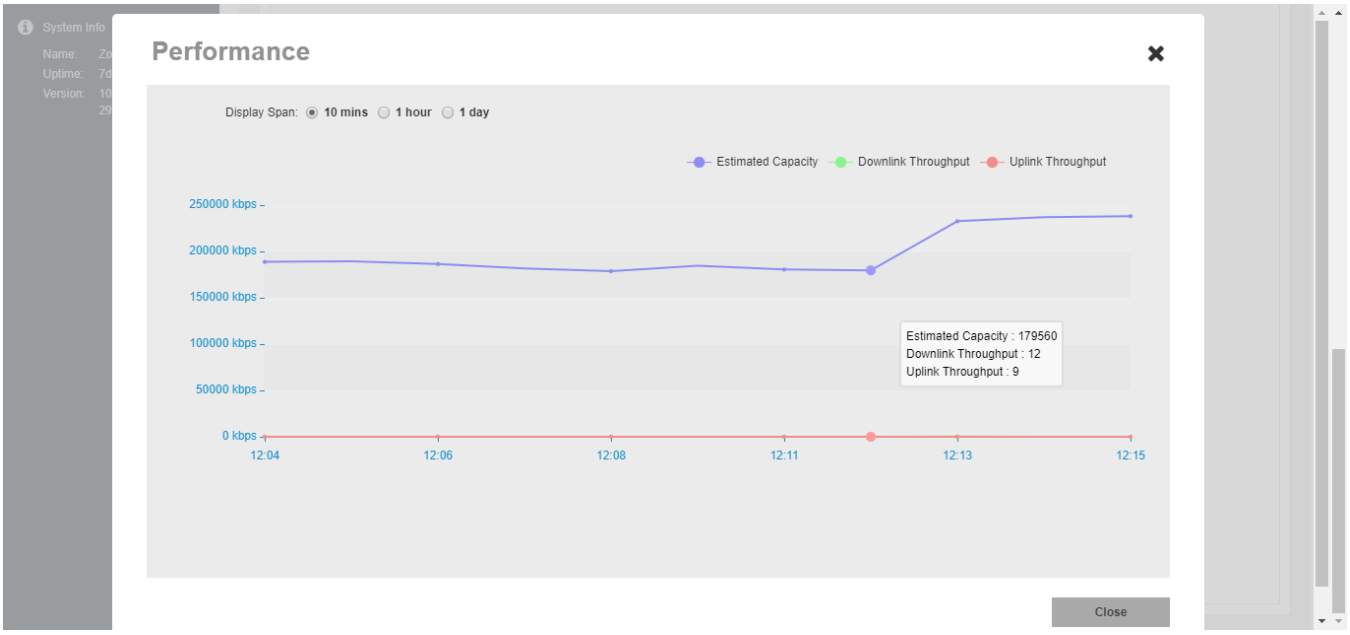


FIGURE 289 Wireless client performance over time



The Estimated Capacity is the maximum potential throughput of a particular client. Estimated capacity or estimated throughput is the short-time averaged MSDU throughput the client is receiving when the AP is actually transmitting to that client. It is measured in bits/s and takes into account the PHY rate, error rate, and all contention due to 802.11 and non-802.11 transmitters. Because it takes into account every source of link

impairment, estimated throughput is the best possible way of numerically characterizing client performance in a single number. This estimate is based on measurements of downlink traffic and is updated only when the AP transmits more than 1000 packets, each containing at least 1024 bytes of data, within a one-minute measurement interval. The uplink and downlink throughput curves show the actual throughput of the client as measured by the AP. These curves are influenced by the user session, and they vary as a function of gaps in browsing activity and internet server response times.

Monitoring Wired Clients

You can monitor currently connected wired clients using the *Clients > Wired Clients* page.

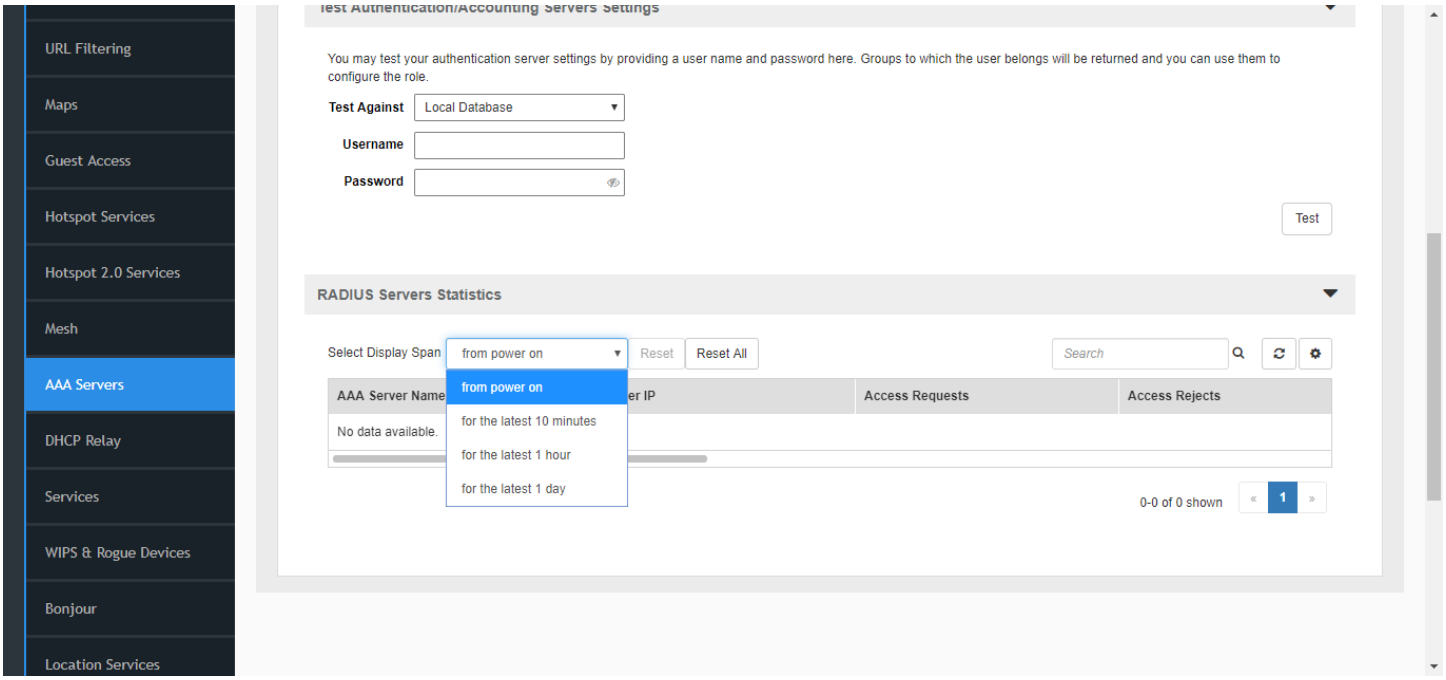
This page displays all currently connected 802.1X or tunneled wired client devices. Only devices with an "authorized" status are permitted access to the network. The **Clients** table lists the wired client's MAC address, user name or IP address, the AP it is connected to, the LAN, VLAN and authorization status. The **Events / Activities** table displays recent connection and authentication events related to wired clients only.

Monitoring AAA Server Statistics

To monitor AAA server (RADIUS) statistics, go to *Services & Profiles > AAA Servers*.

In **RADIUS Server Statistics**, select a time span to display, or click **Reset** to reset a specific time span or **Reset All** to reset all server statistics.

FIGURE 290 Monitoring RADIUS server access and accounting request statistics



Reviewing Recent System Events

The *System > All Events/Activities* page displays the most recent records in ZoneDirector's internal log file.

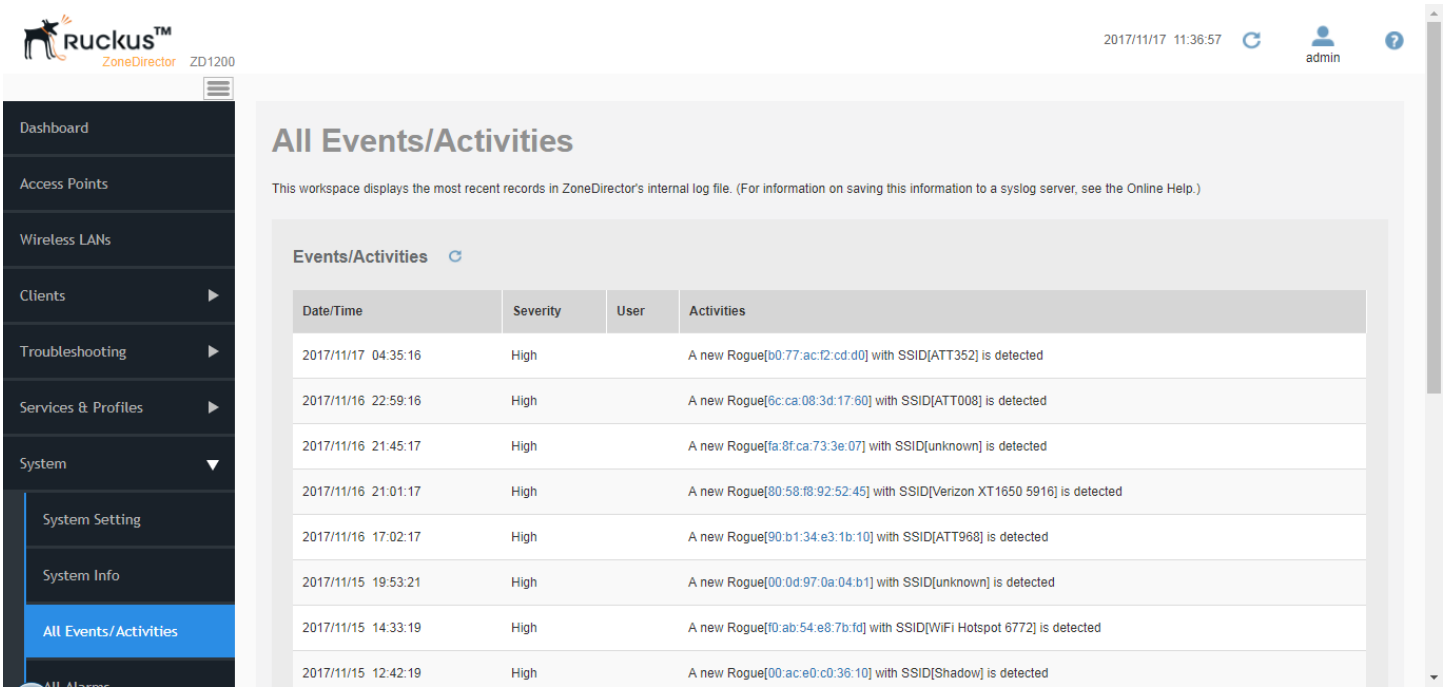
To view a list of recent events/activities:

1. Go to **System > All Events/Activities**.
2. Review the details displayed in the **Events/Activities** table.
3. The first 15 entries are displayed by default. Click **Show More** to expand the display.
4. Click **Clear All** to delete all entries in the table.

NOTE
AP events display the first 17 characters of an AP name (if AP names are used).

NOTE
The **All Events/Activities** table displays a maximum of 2,500 events. When this limit is reached, the oldest events will be overwritten when new events occur.

FIGURE 291 The System > All Events/Activities page



Reviewing Current Alarms

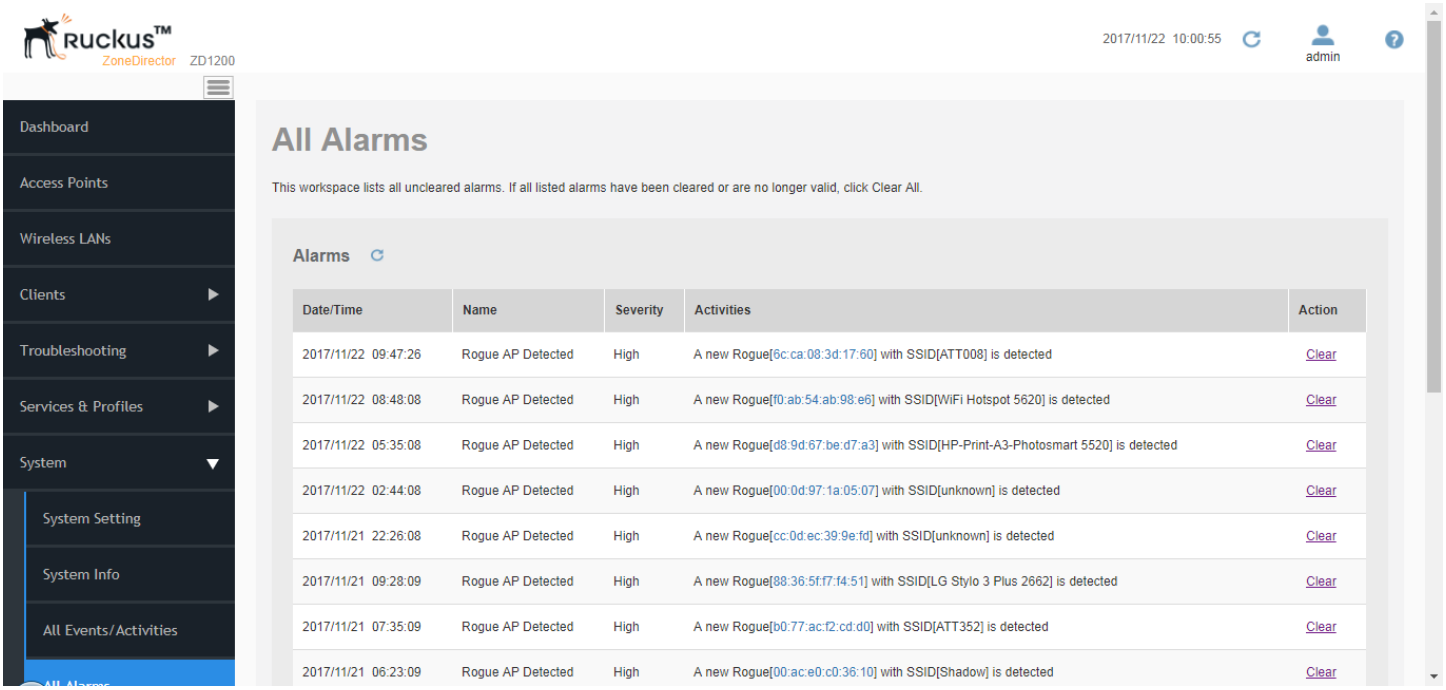
If an alarm condition is detected, ZoneDirector will record it in the events log, and if configured, will send an email warning.

To review the current alarms and clear all resolved alarm records, follow these steps:

1. Go to **System** > **All Alarms**.
2. The **Alarms** table lists the unresolved alarms, the most recent at the top.

3. Review the contents of this table.
4. If a listed alarm condition has been resolved, click the **Clear** link to the right. You also have the option to click **Clear All** to resolve all alarms at once.

FIGURE 292 The **System > All Alarms** page

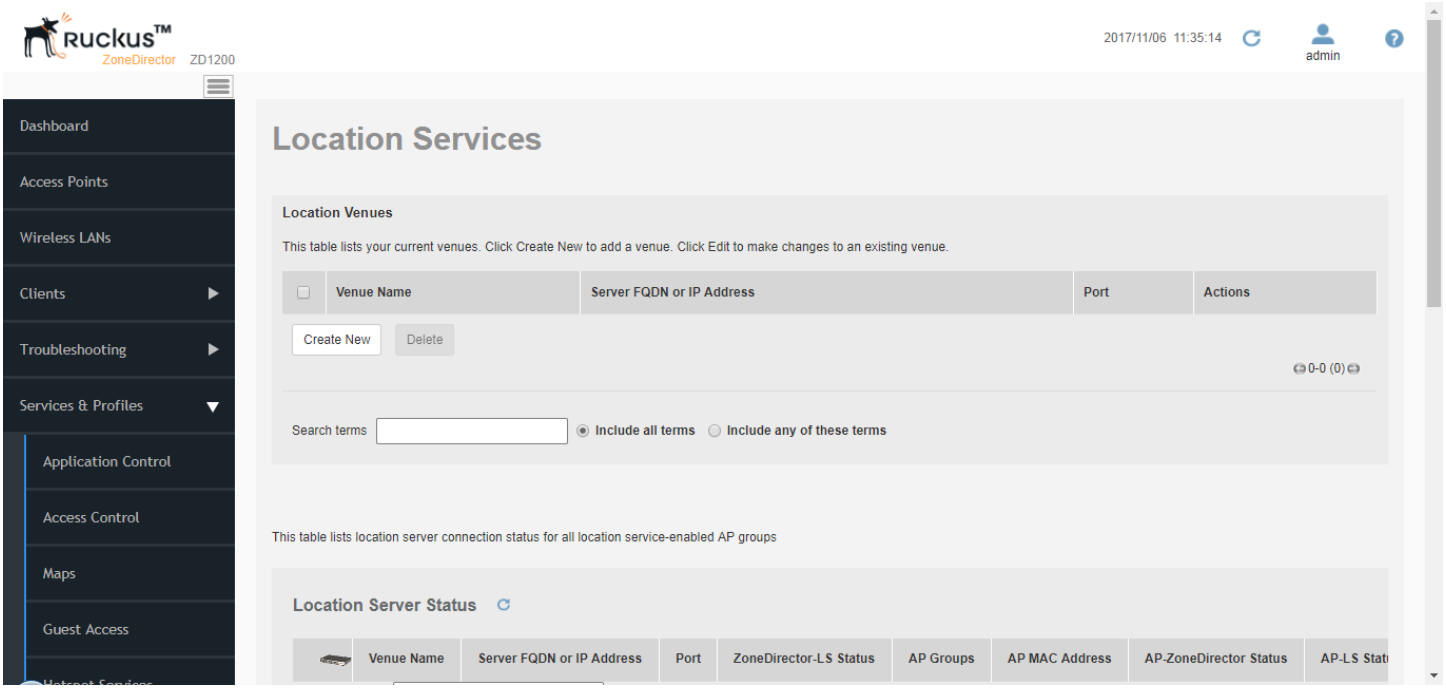


Monitoring Location Services

To monitor SmartPositioning location servers, go to *Services & Profiles > Location Services*.

NOTE
For information on configuration and administration of Ruckus SmartPositioning Technology (SPoT) service, please refer to the *SPoT User Guide*, available from the Ruckus support site: *support.ruckuswireless.com*.

FIGURE 293 Monitoring Location Services

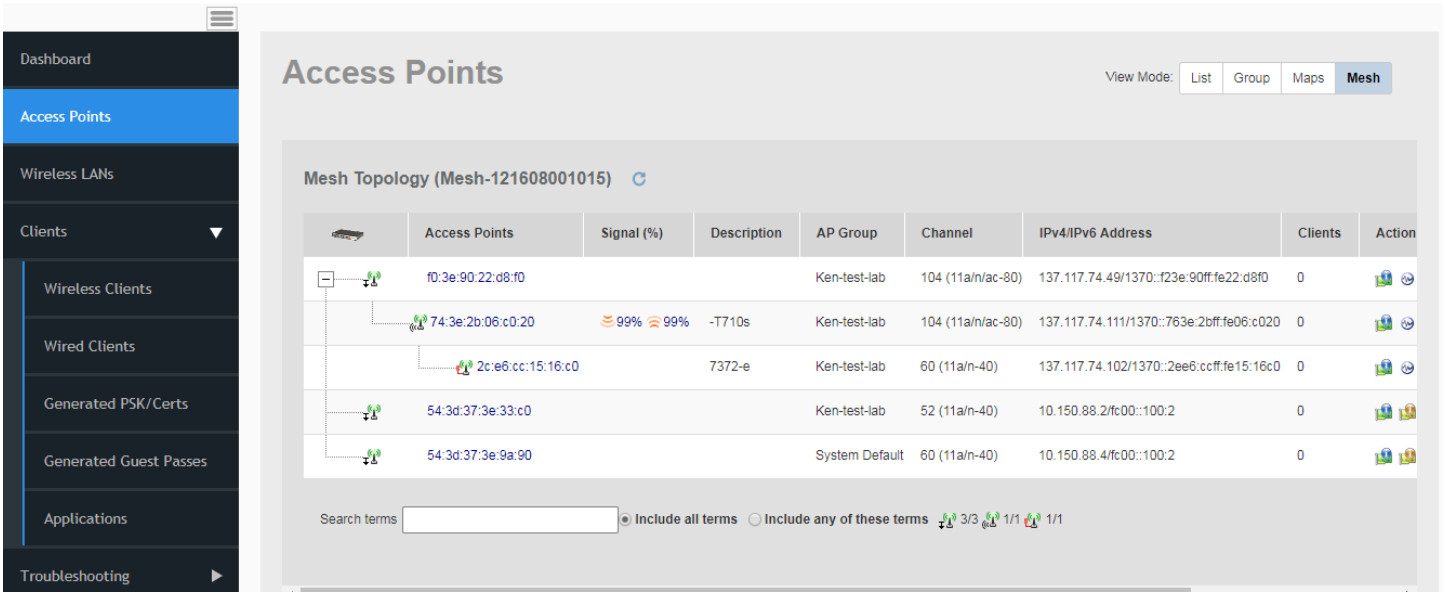


Monitoring Mesh Status

The *Access Points* > *Mesh* view can be used to view Smart Mesh topologies of any mesh trees present on your network.

This page also displays non-meshing APs controlled by ZoneDirector and provides action icons to troubleshoot and diagnose mesh-related problems.

FIGURE 294 Reviewing Mesh status of APs using the Access Points > Mesh page



Real Time Monitoring

The Real Time Monitoring tool provides a convenient at-a-glance overview of performance statistics such as CPU and memory utilization, number of APs and clients on the network, and number of packets transmitted.

Go to **Administer > Real Time Monitoring**, select a time period for display (five minutes, one hour, or one day), and click **Start Monitoring** to start.

FIGURE 295 Real Time Monitoring



Click the **Add Widgets** link to view available widgets, and drag and drop icons onto the dashboard to customize the display.

FIGURE 296 Add Widgets



FIGURE 297 Drag widgets to display on the dashboard



Detecting Rogue Access Points

"Rogue" (unauthorized) APs pose problems for a wireless network in terms of airtime contention as well as security.

Usually, a rogue AP appears in the following way: an employee obtains another manufacturer's AP and connects it to the LAN, to gain wireless access to other LAN resources. This would potentially allow even more unauthorized users to access your corporate LAN - posing a security risk. Rogue APs also interfere with nearby Ruckus APs, thus degrading overall wireless network coverage and performance.

ZoneDirector's rogue AP detection features help in identifying the presence of a rogue AP, categorizing it as either a known neighbor AP or as a malicious rogue, and locating it on your worksite floorplan prior to its physical removal.

To detect a rogue AP:

1. Go to **Services & Profiles** > **WIPS & Rogue Devices**.
2. There are three sections related to rogue devices:
   - **Currently Active Rogue Devices**: Lists all currently detected rogue APs.
   - **Known/Recognized Rogue Devices**: Lists rogue APs that have been marked as known, typically neighbor APs.
   - **User Blocked Rogue Devices**: Lists devices that have been marked as malicious by the user.
3. Review the **Currently Active Rogue Devices** table. The following types of Rogue APs generate an alarm when ZoneDirector detects them (if the alarm has been enabled):
   - AP: A normal rogue AP. This rogue AP has not yet been categorized as malicious or non-malicious.
   - Malicious AP (SSID-spoof): A malicious rogue AP that uses the same SSID as ZoneDirector's AP, also known as an "Evil-twin" AP.
   - Malicious AP (Same-Network): A malicious rogue AP that is connected to the same wired network.
   - Malicious AP (MAC-spoof): A malicious rogue AP that has the same BSSID (MAC) as one of the virtual APs managed by ZoneDirector.
   - Malicious AP (User-Blocked): A rogue AP that has been marked as malicious by the user.

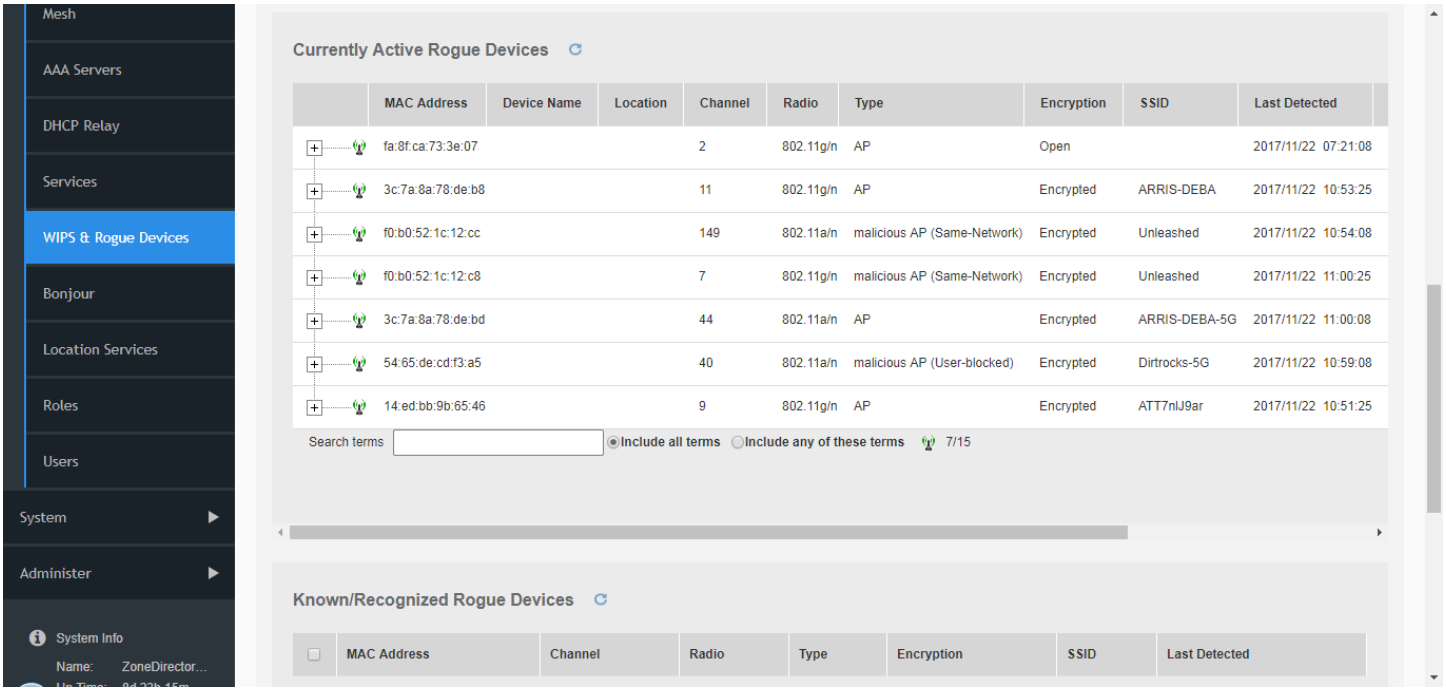
4. To mark an AP as malicious, click **Mark as Malicious**. This AP will now be blocked and listed in the **User Blocked Rogue Devices** table. The malicious rogue AP protection mechanisms are automatically applied to all rogue APs categorized as "malicious," whether user-blocked or another type.
5. If a listed AP is part of another, known neighbor network, click **Mark as Known**. This identifies the AP as posing no threat, while copying the record to the **Known/Recognized Rogue Devices** table.

You can now find the rogue APs and disconnect them. Or, if a rogue AP is actually a component of a neighboring network, you can mark it as "known."

NOTE
If your office or worksite is on a single floor in a multistory building, your upper- and lower-floor neighbors' wireless access points may show up on the Map View, but seemingly in your site. As the Map View cannot locate them in vertical space, you may mark them as "Known."

NOTE
To assist in physically locating rogue devices, click the plus sign (+) icon next to a detected rogue AP. This expands a list to display which APs have detected this rogue, sorted according to signal strength.

FIGURE 298 Monitoring Rogue Access Points



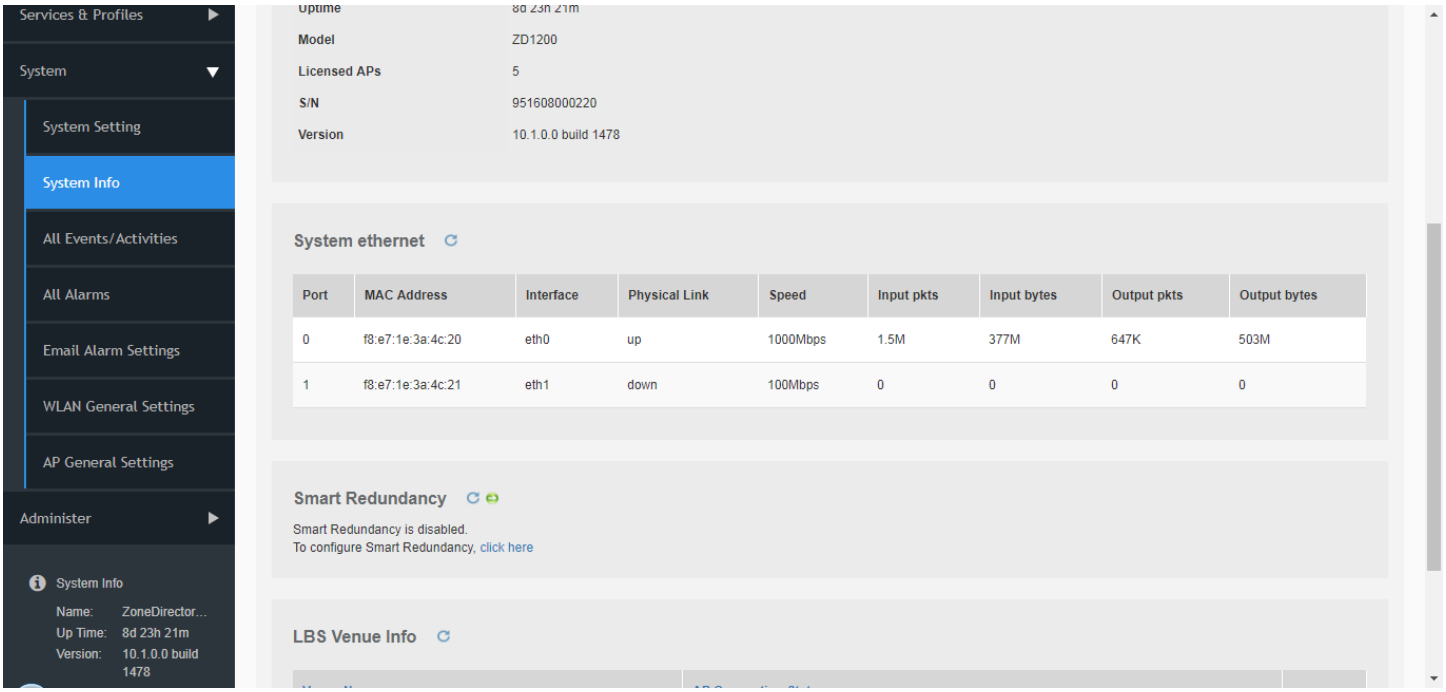
Monitoring System Information

The *System* > *System Info* page provides general overview of the ZoneDirector, as well as information on Ethernet port status, Smart Redundancy status, and Location Services status, if any.

Monitoring System Ethernet Port Status

To view the status of ZoneDirector's Ethernet ports, go to *System* > *System Info*. The table displays the MAC address, Interface ID, physical link status, link speed, and total packets/bytes received/transmitted on the port since last restart.

FIGURE 299 Monitoring ZoneDirector Ethernet port information



Deploying a Smart Mesh Network

- Overview of Smart Mesh Networking 383
- Smart Mesh Networking Terms 384
- Supported Mesh Topologies 384
- Viewing the Mesh Topology 387
- Deploying a Wireless Mesh via ZoneDirector 388
- Optional Mesh Configuration Features 397
- Understanding Mesh-related AP Statuses 397
- Using the AP LEDs to Determine the Mesh Status 397
- Using Action Icons to Configure and Troubleshoot APs in a Mesh 399
- Setting Mesh Uplinks Manually 400
- Troubleshooting Isolated Mesh APs 401
- Best Practices and Recommendations 403

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 Ruckus APs forming the network), or “mesh nodes,” form the network's backbone. Clients (laptops and other mobile devices) connect to the mesh nodes and use the backbone to communicate with one another, and, if permitted, with nodes on the internet.

In a 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, Ruckus APs communicate with ZoneDirector through a wired LAN connection or through a wireless connection with other Ruckus access points. The mesh network enables clients to reach other systems by creating a path that 'hops' between nodes.

Smart Mesh networking offers many advantages:

- Fast deployment: Mesh nodes can be easily installed to construct a wireless mesh network in a short time, much shorter than the construction period of a traditional WLAN.
- Dynamic coverage area expansion: As more mesh nodes are deployed, the coverage area can be rapidly expanded.
- 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.
- Robustness: A mesh network is a peer-to-peer network that will not be affected by the failure of a single node. If a node fails, packets are forwarded to the destination node along other paths.
- Flexible networking: An AP can join or leave a mesh network easily, allowing for flexible networking.
- Various application scenarios: Besides traditional WLAN scenarios such as enterprise networks, hospitality and higher education, a mesh network also applies to scenarios such as large-scale warehouses, docks and marinas, Smart Cities, and emergency communications.
- Cost-effectiveness: Only Root APs need to connect to the wired network, which minimizes the dependency on wired devices and saves costs in wired device purchasing and cable deployment.

NOTE
For best practices and recommendations on planning and deploying a Smart Mesh network, refer to *Mesh Networking Best Practices*.

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 33 Mesh networking terms

Term	Definition
Mesh Node	A Ruckus AP with mesh capability enabled.
Root AP (RAP)	A mesh node that communicates with ZoneDirector through its Ethernet (that is, wired) interface.
Mesh AP (MAP)	A mesh node that communicates with ZoneDirector through its wireless interface.
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 ZoneDirector can manage more than one mesh tree. There is no limit on the number of mesh trees per ZoneDirector. For example, a ZoneDirector 1206 (license for 6 APs) can manage 1 mesh tree of 6 APs, 2 mesh trees of 3 APs each, or 3 mesh trees of 2 APs each.
Hop	The number of wireless mesh links a data packet takes from one Mesh AP to the Root AP. For example, if the Root AP is the uplink of Mesh AP 1, then Mesh AP 1 is one hop away from the Root AP. In the same scenario, if Mesh AP 1 is the uplink of Mesh AP 2, then Mesh AP 2 is two hops away from the Root AP. A maximum of 8 hops is supported.

Supported Mesh Topologies

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

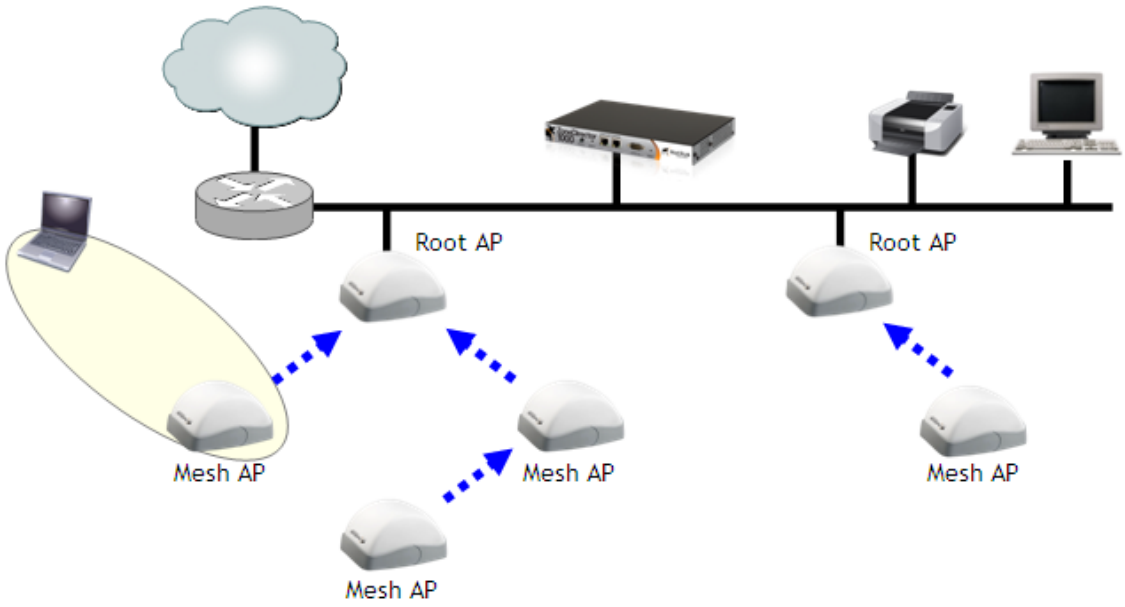
- Standard Topology on page 384
- Wireless Bridge Topology on page 385
- Hybrid Mesh Topology on page 386

Standard Topology

The standard Smart Mesh topology consists of ZoneDirector and a number of Root APs and Mesh APs. In this topology, ZoneDirector 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 300 Mesh - standard topology

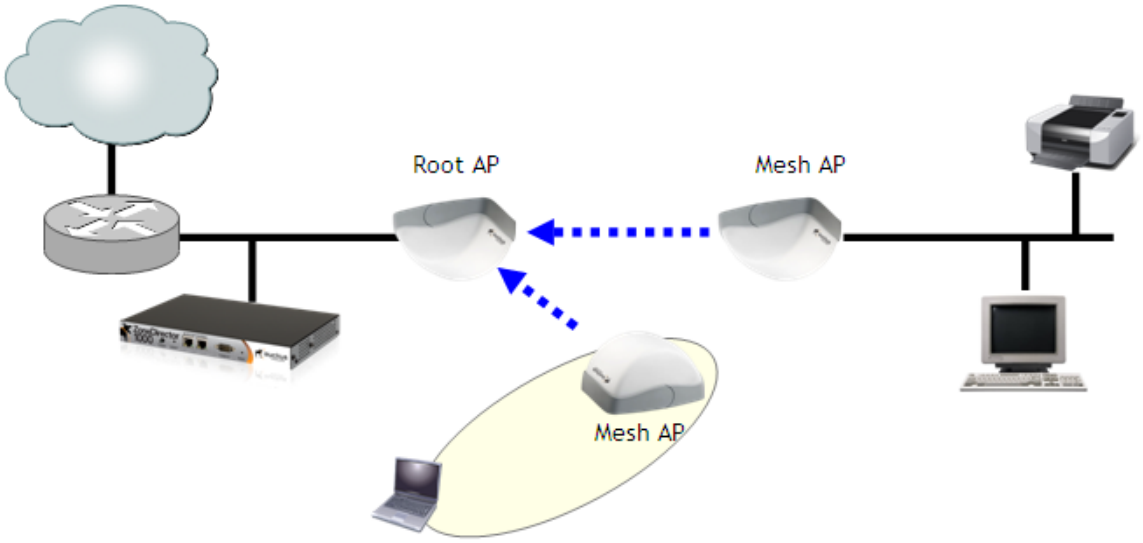


Wireless Bridge Topology

If you need to bridge isolated wired LAN segments, you can set up a mesh network using the wireless bridge topology.

In this topology, ZoneDirector 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 301 Mesh - wireless bridge topology



Hybrid Mesh Topology

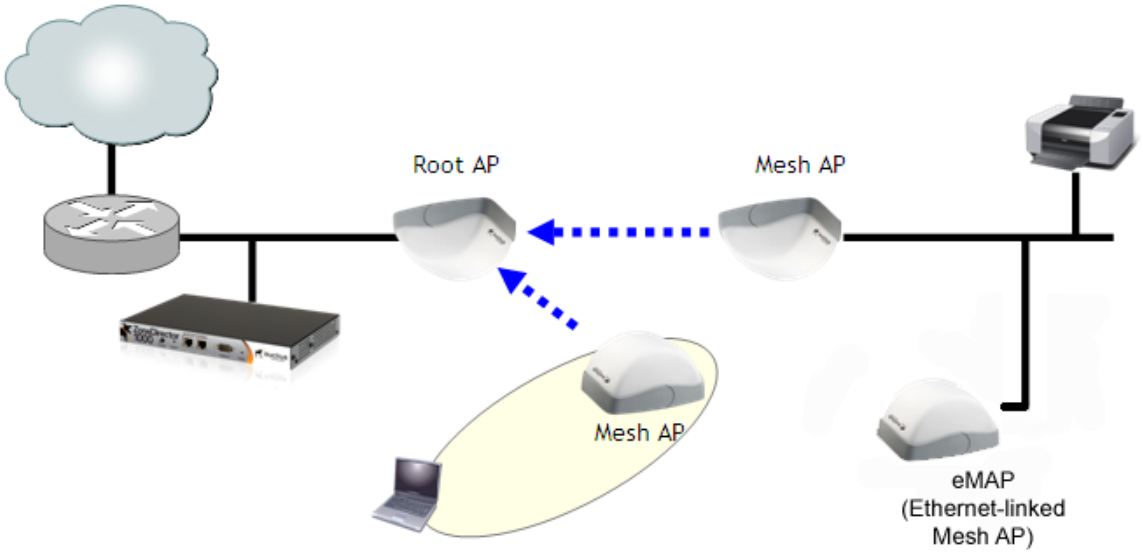
A third type of network topology can be configured using the Hybrid Mesh concept.

Ethernet-connected 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 ZoneDirector 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 wireless traffic can be set to different channels to take advantage of spectrum reuse.

FIGURE 302 eMAP - Hybrid Mesh topology



Use the **Access Points** > **Mesh** page to see a tree diagram of your Smart Mesh network.

Icon	Meaning
	Root AP (RAP)
	Mesh AP (MAP)
	eMesh AP (eMAP)

Viewing the Mesh Topology

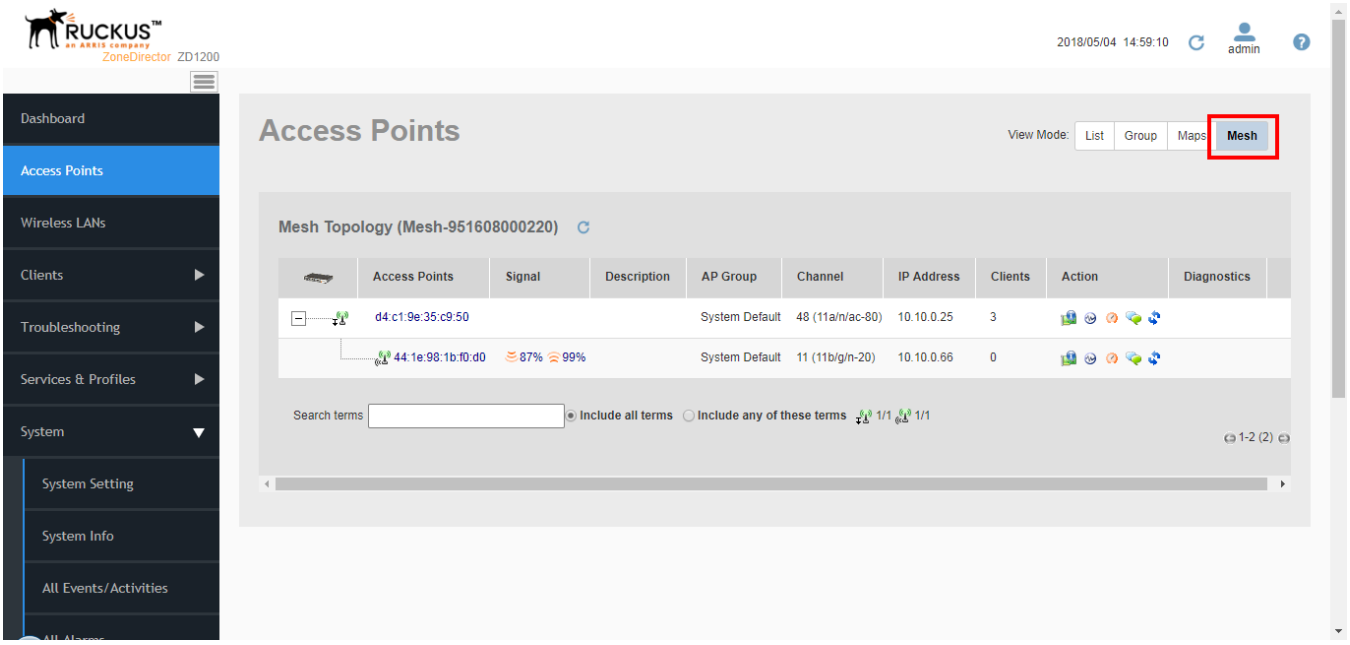
You can view the current mesh topology from the Access Points page.

To monitor the current mesh topology:

1. Go to **Access Points**.

2. In *View Mode*, click **Mesh**. Mesh APs are displayed beneath and connected to their uplink APs. You can also view the signal strength of the mesh link and perform troubleshooting tasks such as reboot an AP, ping an AP, and perform a SpeedFlex performance test on a mesh link from this view.

FIGURE 303 Click Mesh to view mesh topology



Deploying a Wireless Mesh via ZoneDirector

Deploying a wireless mesh via ZoneDirector involves the following steps:

- Step 1: Prepare for Wireless Mesh Deployment
- Step 2: Enable Mesh Capability on ZoneDirector
- Step 3: Provision and Deploy Mesh Nodes
- Step 4: Verify That the Wireless Mesh Network Is Up

Step 1: Prepare for Wireless Mesh Deployment

Before starting with your wireless mesh deployment, Ruckus recommends performing a number of tasks that can help ensure a smooth deployment.

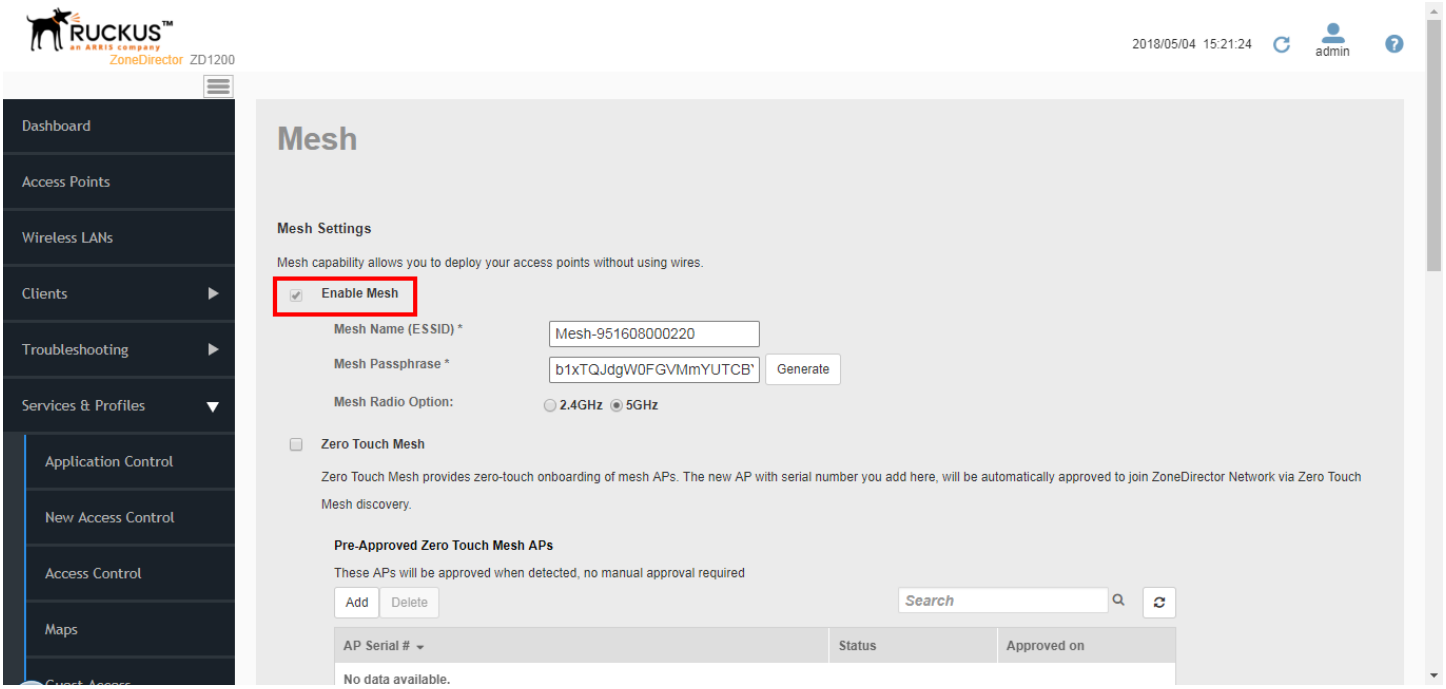
- Ensure that the APs that will form the mesh are of the same radio type:
  - Single-band APs can only mesh with other single-band APs.
  - Dual-band APs can only mesh with other dual-band APs.
- Plan your wireless mesh network - perform a site survey of your deployment site, decide on the number of APs that you will deploy (including the number of root APs and mesh APs), and then create a sketch of where you will deploy each root AP and mesh AP. Remember that root APs need to be connected to ZoneDirector via their Ethernet ports. Make sure that the root AP locations can be wired easily, if cabling is not yet available.

- In general, it is desirable to have as many root APs as possible to maximize overall network performance and reliability.
- Enable Auto Approval - If you do not want to have to manually approve the join requests from each mesh AP when they start forming the wireless mesh, you can enable Auto Approval. For instructions on how to enable Auto Approval, see Adding New Access Points to the Network on page 35.

Step 2: Enable Mesh Capability on ZoneDirector

If you did not enable mesh capability on ZoneDirector when you completed the Setup Wizard, you can enable it on the **Services & Profiles** > **Mesh screen** page.

FIGURE 304 Enable Mesh from the Services & Profiles > Mesh page



To enable Smart Mesh:

1. Log into the ZoneDirector web interface.
2. Click the **Services & Profiles** tab.
3. On the menu, click **Mesh**.
4. Under **Mesh Settings**, select the **Enable Mesh** check box.

   NOTE
   You cannot disable Smart Mesh once you enable it. This is by design, to prevent isolating nodes. If you want to disable Smart Mesh once it has been enabled, you will have to factory reset ZoneDirector, or disable mesh for each AP, as described in *Managing Access Points Individually*.

5. In **Mesh Name (ESSID)**, type a name for the mesh network. Alternatively, do nothing to accept the default mesh name that ZoneDirector has generated.

6. In **Mesh Passphrase**, type a passphrase that contains at least 12 characters. This passphrase will be used by ZoneDirector to secure the traffic between Mesh APs. Alternatively, click **Generate** to generate a random passphrase with 32 characters or more.
7. In **Mesh Radio Option**, select whether to transmit the mesh SSID over the 2.4 or 5 GHz radio. By default, mesh is enabled on the 5 GHz radio.

   NOTE
   If mesh is enabled and you want to switch the mesh radio between 5 GHz and 2.4 GHz, make sure all APs are Root APs before switching the mesh radio, all APs will reboot to make the mesh changes effective.

   NOTE
   Zero Touch Mesh is not supported when the 2.4 GHz mesh radio option is selected.

8. In the **Mesh Settings** section, click **Apply** to save your settings and enable Smart Mesh.

You have completed enabling mesh capability on ZoneDirector. You can now start provisioning and deploying the APs that you want to be part of your wireless mesh network.

Step 3: Provision and Deploy Mesh Nodes

In this step, you will connect each AP to the same wired network as ZoneDirector to provision it with mesh-related settings. After you complete provisioning an AP, you must reboot it for the mesh-related settings to take effect.

NOTE
Beginning with release 10.2, ZoneDirector also provides a "Zero Touch Mesh" option, which alleviates the need to perform this manual provisioning procedure. For more information, see Zero Touch Mesh on page 391.

To provision and deploy a mesh node:

1. Using one of the AP's Ethernet ports, connect it to the same wired network to which ZoneDirector is connected, and then power it on. The AP detects ZoneDirector and sends a join request.
2. If Auto Approval is enabled, continue to Step 3. If Auto Approval is disabled, log into ZoneDirector, check the list of currently active access points for the AP that you are attempting to provision, and then click the corresponding **Allow** link to approve the join request.

3. After the AP has been provisioned, disconnect it from the wired network, unplug the power cable, and then move the device to its deployment location.
   - If you want the AP to be a Root AP, reconnect it to the wired network using one of its Ethernet ports, and then power it on. When the AP detects ZoneDirector again through its Ethernet port, it will set itself as a Root AP, and then it will start accepting mesh association requests from Mesh APs.
   - If you want the AP to be a Mesh AP, power it on but do not reconnect it to the wired network. When it does not detect ZoneDirector through its Ethernet port within 90 seconds, it will search for potential uplink APs and, once mesh neighbor relationships are established, form a mesh tree.

     NOTE
     After an AP in its factory default state has been provisioned, you need to reboot it to enable mesh capability.

     NOTE
     If you are located in the United States and have a DFS-capable AP that is expected to serve as a Root AP (or eMAP), with a non-DFS-capable Mesh AP as its downlink, you will need to set the channel for the Root AP to one of the non-DFS channels. Specifically, choose one of the following channels: 36, 40, 44, 48, 149, 153, 157, 161, 165. This is due to the DFS-capable AP's ability to use more channels than the non-DFS-capable AP, which could result in the RAP choosing a channel that is not available to the MAP. Alternatively, go to *System > System Settings > Country Code*, and set the *Channel Optimization* setting to "Optimize for Compatibility."

Repeat Steps 1 to 3 for each AP that you want to be part of your wireless mesh network. After you complete provisioning and deploying all mesh nodes, verify that the wireless mesh has been set up successfully.

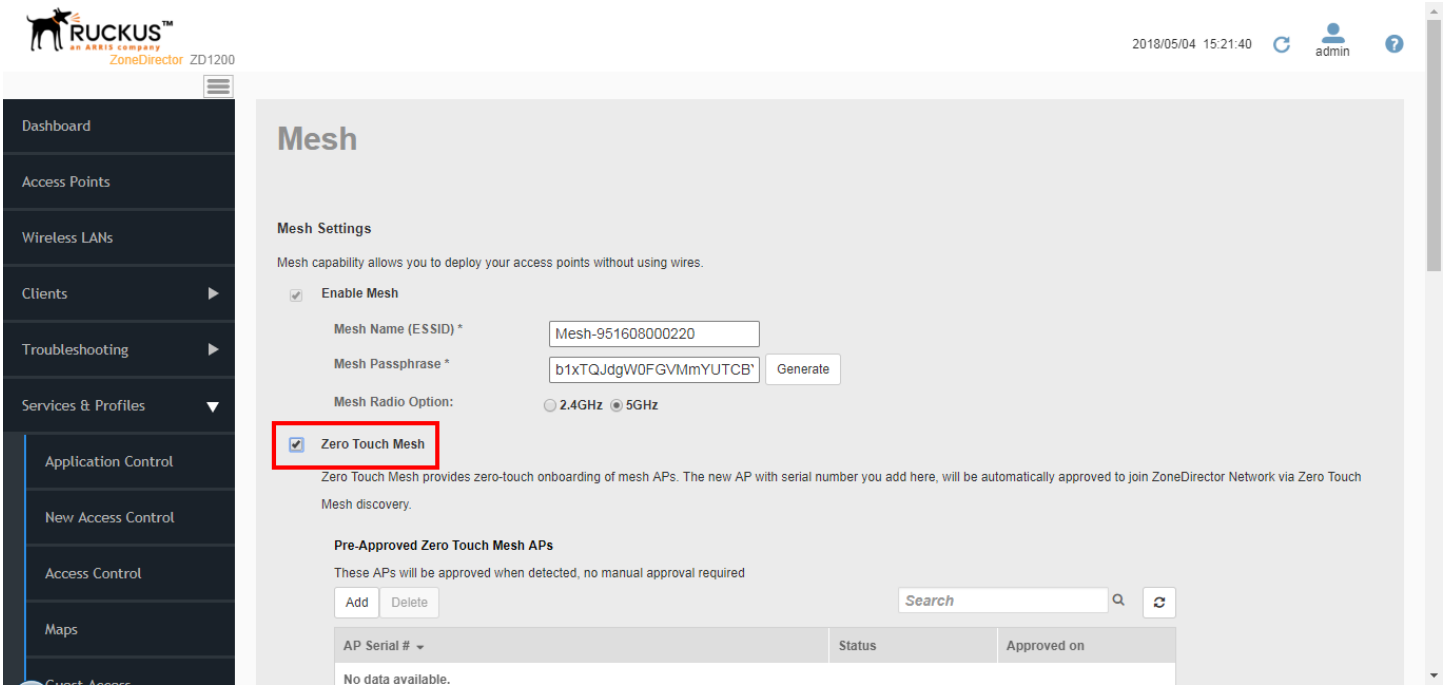
Zero Touch Mesh

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, APs that are destined to become Mesh APs (MAPs) need to first be primed prior to deployment. They are first manually connected to the controller via Ethernet to receive the provisioning parameters (Mesh SSID and PSK passphrase), and then unplugged from Ethernet and installed at their desired locations. Once installed, Mesh APs perform network discovery and associate to another 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 305 Zero Touch Mesh



Zero Touch Mesh Limitations

Please be aware of the following limitations of the ZTM feature:

- Zero Touch Mesh AP needs a new version certification.

  User can use "get rpki-cert issuer" command via AP CLI to get the version of certification.

  The new version certification must be like ：

  Issuer: RuckusPKI-DeviceSubCA-**N** (**N** can be 1 、 2 or 3)
- Zero Touch Mesh only supports 5GHz.
- Zero Touch Mesh only supports solo AP 110.0+ and ZD AP 10.2+.
- When a solo AP is upgraded from a previous release (for example 104 or 106) to 110 or 10.2, the AP must be factory reset to activate Zero Touch Mesh.
- When a solo AP has updated configuration (for example, WLAN configuration), the AP must be factory reset to activate Zero Touch Mesh.
- Zero Touch Mesh cannot work if root APs are fixed working on some channels out of the below range in some countries.

  Available channel list for Zero Touch Mesh:

  * 36 (5180 MHz) HT20 HT40 HT80

  * 40 (5200 MHz) HT20 HT40 HT80

  * 44 (5220 MHz) HT20 HT40 HT80

  * 48 (5240 MHz) HT20 HT40 HT80

  * 52 (5260 MHz) HT20 HT40 HT80

  * 56 (5280 MHz) HT20 HT40 HT80

* 60 (5300 MHz) HT20 HT40 HT80
* 64 (5320 MHz) HT20 HT40 HT80
* 100 (5500 MHz) HT20 HT40 HT80
* 104 (5520 MHz) HT20 HT40 HT80
* 108 (5540 MHz) HT20 HT40 HT80
* 112 (5560 MHz) HT20 HT40 HT80
* 116 (5580 MHz) HT20 HT40 HT80
* 120 (5600 MHz) HT20 HT40 HT80
* 124 (5620 MHz) HT20 HT40 HT80
* 128 (5640 MHz) HT20 HT40 HT80
* 132 (5660 MHz) HT20 HT40 HT80
* 136 (5680 MHz) HT20 HT40 HT80
* 140 (5700 MHz) HT20
* 149 (5745 MHz) HT20 HT40 HT80
* 153 (5765 MHz) HT20 HT40 HT80
* 157 (5785 MHz) HT20 HT40 HT80
* 161 (5805 MHz) HT20 HT40 HT80
* 165 (5825 MHz) HT20

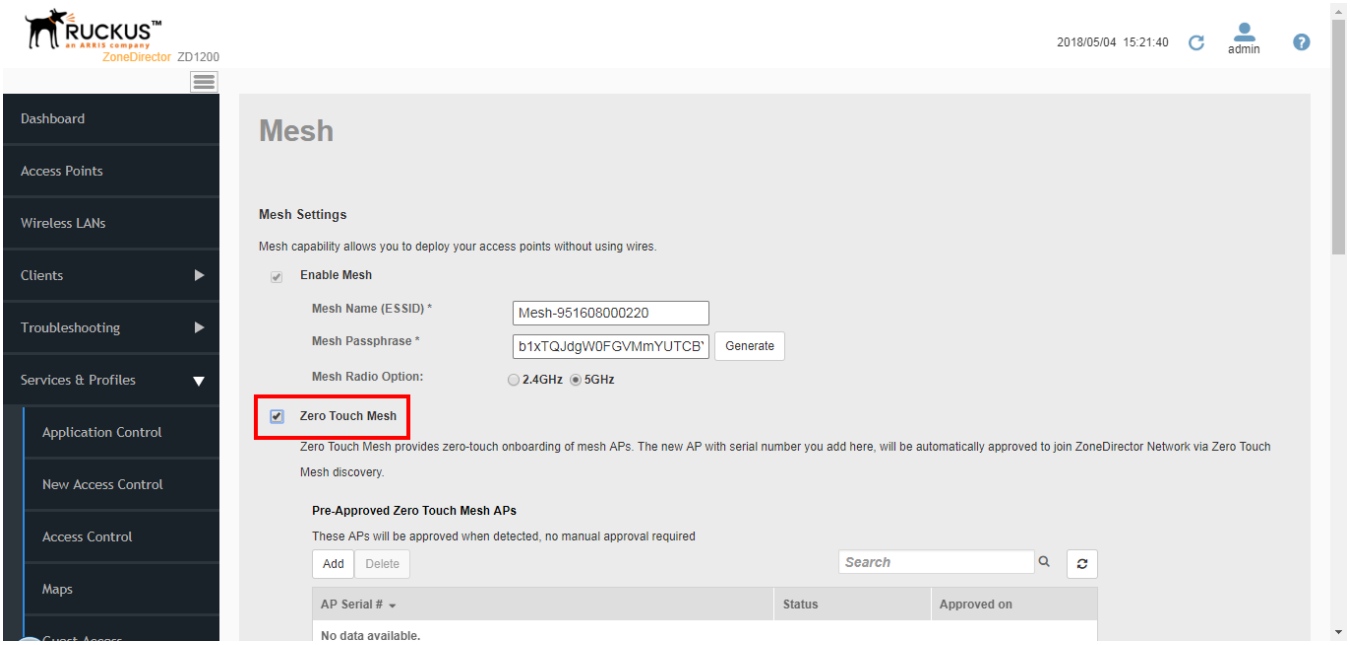
Onboarding Mesh APs with Zero Touch Mesh

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

1. Go to **Services & Profiles > 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.

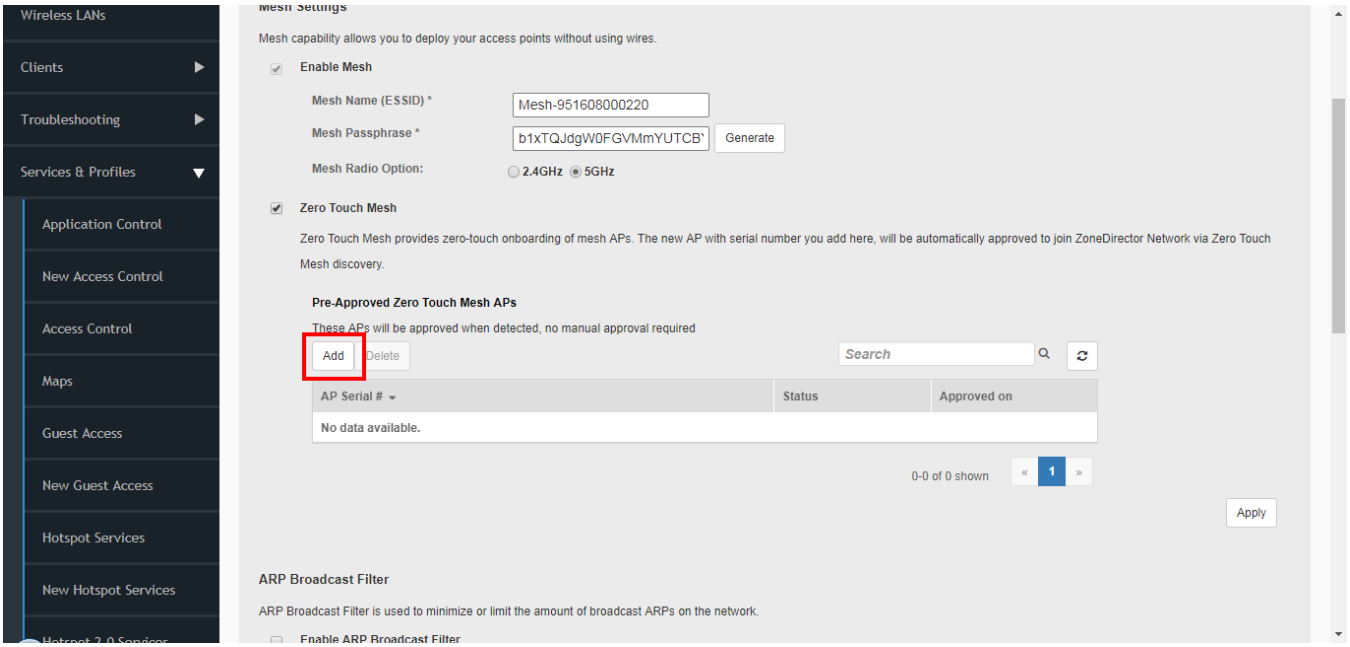
FIGURE 306 Enable Zero Touch Mesh



4. Go to **Access Points**.
5. When a supported AP attempts to join, it will appear in *Disconnected* state in the AP table. Click the **Approve** button to approve the AP.
6. To pre-approve APs by serial number, go to **Services & Profiles > 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 or multiple APs to the list of pre-approved Zero Touch Mesh APs.

FIGURE 307 Click Add to add APs to the list of pre-approved Zero Touch Mesh APs

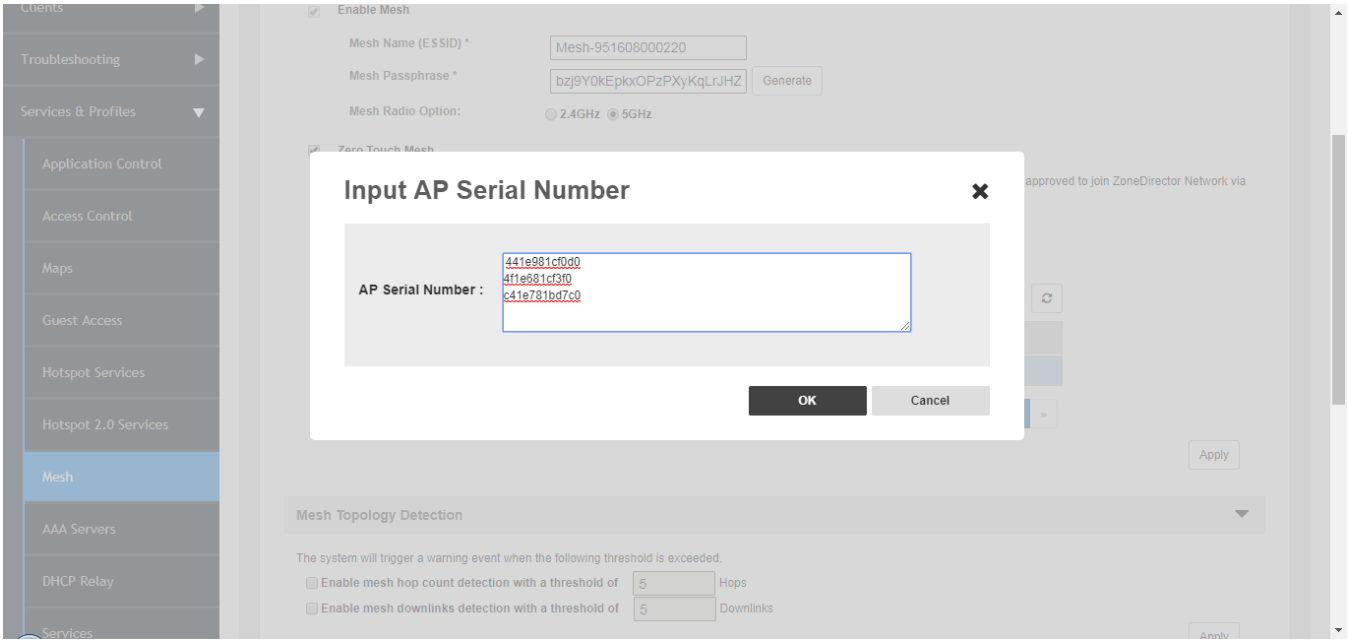


The *Input AP Serial Number* window appears.

8. Enter the AP Serial Numbers of the APs to auto-provision, and click **OK**.

   NOTE
   You can enter multiple serial numbers. Each serial number must be exactly 12 characters (no colons), and each must be on its own separate line. You can also copy/paste many serial numbers from a text editor. Empty lines are invalid.

   FIGURE 308 Input AP Serial Number



   The AP serial numbers are added to the list.

9. Click **Apply**. A message box appears notifying you that the process may take several minutes for the changes to propagate through the mesh network.
10. 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 on the network.

Step 4: Verify That the Wireless Mesh Network Is Up

After you complete deploying all mesh nodes to their locations on the network, you can check the *Access Points* page to verify that mesh associations have been established and mesh trees formed.

1. Go to **Access Points**.
2. In *View Mode*, click **Mesh**.
3. Check if all the mesh nodes that you have provisioned and deployed appear in the **Mesh Topology** section.

Optional Mesh Configuration Features

The following settings are disabled by default and are not necessary for standard mesh configuration. These settings can be used to fine-tune your mesh network to prevent issues such as excessive broadcast ARP (Address Resolution Protocol) requests, traffic looping and excessive number of mesh hops.

- **ARP Broadcast Filter**: The ARP Broadcast filter is designed to reduce IPv4 Address Resolution Protocol (ARP) and IPv6 Neighbor Discovery Protocol (NDP) broadcasts over the air. Once enabled, access points will sniff ARP/NDP responses and maintain a table of IP addresses to MAC address entries. When the AP receives an ARP/NDP 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. If the AP receives a request from an unknown host, it forwards the request at the rate limit specified in the Packet Inspection Filter.
- **Mesh Topology Detection**: Set the number of mesh hops and mesh downlinks after which ZoneDirector should trigger warning messages.

Understanding Mesh-related AP Statuses

You can use the *Access Points* page for viewing and mesh-related AP statuses.

In the *Access Points* table, the mesh status of each AP is displayed in the *Status* column, along with the *Mesh Mode* and other details.

The table below lists possible AP statuses that are related to mesh networking in the *Status* column, including any actions that you may need to perform to resolve mesh-related issues.

Status	Description	Recommended Action
Connected	AP is connected to ZoneDirector, but mesh is disabled	If mesh is enabled on the AP, you may need to reboot it to activate the mesh.
Connected (Root AP)	AP is connected to ZoneDirector via its Ethernet port	
Connected (Mesh AP, n hops)	AP is connected to ZoneDirector via its wireless interface and is n hops away from the Root AP.	
Connected (eMesh AP, n hops	AP is connected to ZoneDirector via its Ethernet port, but acts as a Mesh AP using another Mesh AP as its uplink	
Isolated Mesh AP	AP is disconnected from the ZoneDirector mesh	• The AP may be configured incorrectly. Verify that the mesh SSID and passphrase configured on the AP are correct. • If Uplink Selection is set to Manual, the uplink AP specified for this AP may be off or unavailable.

Using the AP LEDs to Determine the Mesh Status

In addition to checking the AP's mesh status from the ZoneDirector web interface, you can also check the LEDs on the APs.

On Dual-band Ruckus APs

On dual-band APs, mesh networking is enabled on the 5 GHz radio by default.

Refer to the following sections for information on how to check the LEDs on dual-band APs for their mesh status.

- *Indoor Dual-Band APs*
- *Outdoor Dual-Band APs*

Indoor Dual-band APs

On dual-band indoor APs, the 5G LED indicates the status of the mesh downlink, and the AIR LED indicates the status of the mesh uplink.

See the table below for more information.

LED	Root AP / eMAP	Mesh AP
5G LED	Solid Green: • Solid Green: 5G radio is up • No Mesh APs are connected • At least one client is connected	Mesh AP 5G LED is consistent with Root AP behavior
	Amber: • 5G radio is up • No Mesh APs/clients connected	
	Slow Flashing Green (one flash every two seconds): • 5G radio is up • At least one MAP is connected • No clients are associated	
	Fast Flashing Green (two flashes every second) • 5G radio is up • At least one MAP is connected • At least one client is connected	
AIR LED	Off	Solid Green: • Connected to an uplink AP • Signal quality is good • Fast flashing green (two flashes every second): • Connected to a uplink AP • Signal quality is fair • Slow flashing green (one flash every two seconds): • Mesh network is enabled • Not connected to an uplink AP, searching for a mesh uplink

Outdoor Dual-band APs

On outdoor APs, the STATUS LED indicates the AP's mesh status.

See the table below for more information.

LED Color/Behavior	Description
Solid Green	• This is a Root AP or eMAP, or • This is a Mesh AP and is connected to a Root AP with good signal
Fast blinking green	• This is a Mesh AP, and • The Root AP signal is fair
Slow blinking green	• This is a Mesh AP that is currently searching for a Root AP, or • This AP is currently searching for ZoneDirector

Using Action Icons to Configure and Troubleshoot APs in a Mesh

The following action icons are used to perform configuration and troubleshooting tasks on the respective AP. The icons are displayed next to APs on the **Access Points** page.

TABLE 34 Action icon

Icon	Icon Name	Action
	System Info	Generate a log file (support.txt) containing system information on this AP.
	Configure	Go to the *Access Points* page and edit the configuration settings for this AP.
	Mesh View	Open a "Mesh View" screen with this AP highlighted in a Mesh tree that also shows the uplink and downlink APs connected to this AP.
	SpeedFlex	Launch the SpeedFlex performance test tool to measure uplink/downlink speeds to/from this AP.
	Troubleshoot	Troubleshoot connectivity issues using Ping and Traceroute.
	Restart	Initiate a reboot of this AP.
	Recover	Recover an isolated Mesh AP
	Allow	Allow this AP to be managed by ZoneDirector. This icon will only appear if you have disabled automatic approval under **Access Point Policies** on the **Access Points** page.
	RF Info	Generates a log file called info.txt, containing radio frequency data that can be used for troubleshooting the RF environment.

TABLE 34 Action icon (continued)

Icon	Icon Name	Action
	Join Another Controller	Click this button to migrate an AP to another controller. For more information, see Migrating an AP from ZoneDirector to Another Controller on page 363.

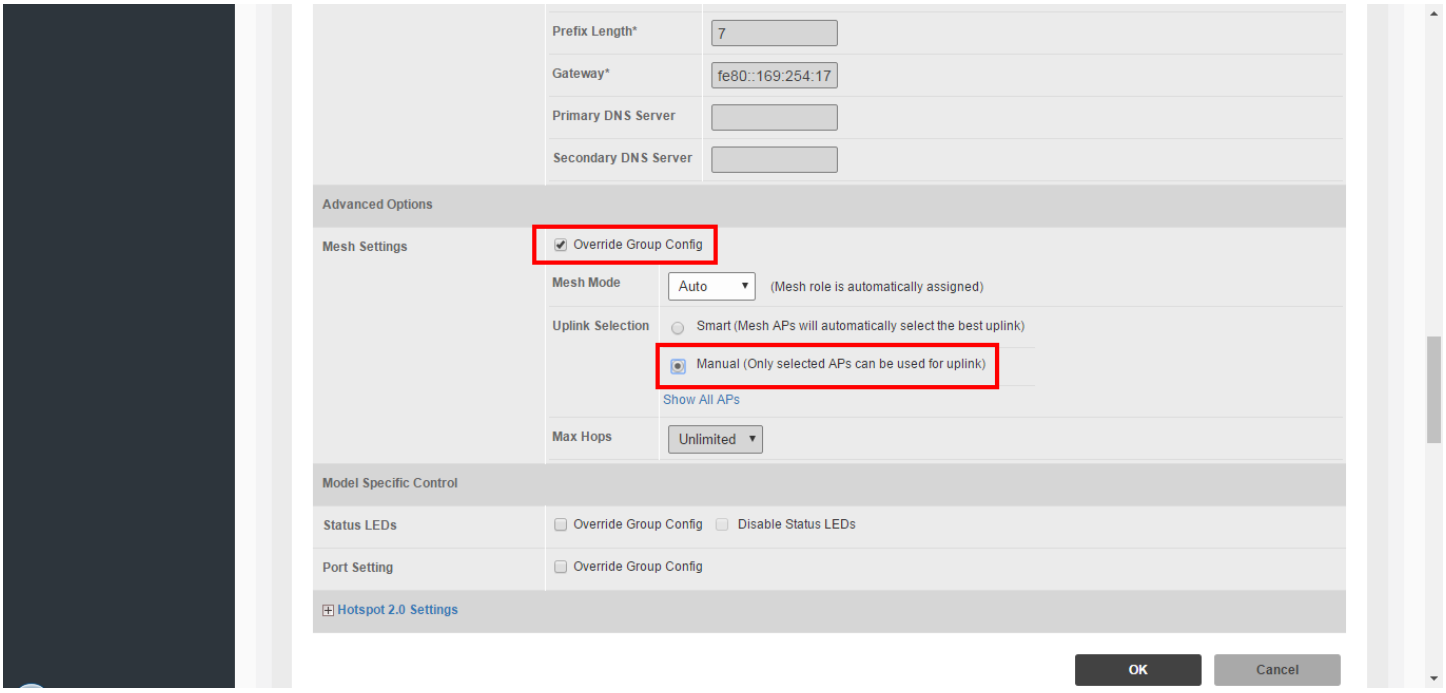
Setting Mesh Uplinks Manually

In a wireless mesh network, the default behavior of Mesh APs is to connect automatically to a mesh node (either Mesh AP or Root AP) that provides the highest throughput. This automatic connection is called "Smart Uplink Selection."

If you want to shape your mesh network or force a certain topology, you will need to disable Smart Uplink Selection and manually set the mesh nodes to which an AP can connect.

NOTE
Note that in most situations, Ruckus recommends against manually changing the roles of APs in a mesh, because it can result in isolated Mesh APs.

FIGURE 309 Setting Uplink Selection to Manual



NOTE
Do not manually set a Mesh AP as a Root AP. Only APs that are connected to ZoneDirector via Ethernet (and on the same LAN segment) should be configured as Root APs. Mis-configuring a Mesh AP or an eMAP as a Root AP can cause the AP to become isolated, or, in the case of eMAP, can result in a network loop.

To set the mesh uplink for an AP manually:

1. On the ZoneDirector web interface, click the **Access Points** tab.

2. In the **Access Points** table, find the AP you want to restrict, and click **Edit** under the **Actions** column. The editing form appears below your selection.
3. Under **Advanced Options** > **Uplink Selection**, select the **Manual** radio button. The other APs in the mesh appear below the selection.
4. Select the check box for each AP that the current AP can use as uplink. If you set Uplink Selection for an AP to Manual and the uplink AP that you selected is off or unavailable, the AP status on the *Access Points* page will appear as *Isolated Mesh AP*.
5. Click **OK** to save your settings.

Troubleshooting Isolated Mesh APs

Isolated Mesh APs are those that were once managed by ZoneDirector but are now unreachable. They are up and running and constantly searching for mesh uplinks, but are unable to connect to any root AP. You can check if you have any isolated mesh APs on the network by checking the **Access Points** page.

NOTE
A mesh network is dynamic in nature. Before attempting to resolve any mesh-related issue, please wait 15 minutes to allow the mesh network to stabilize. Some mesh-related issues are automatically resolved once the mesh network stabilizes.

Understanding Isolated Mesh AP Statuses

There are several possible reasons for a mesh AP to become isolated. The table below lists possible Isolated Mesh AP statuses that may appear on the *Access Points* page, and provides possible reasons for the isolation and the recommended steps for resolving the issue.

Status	Possible Reason
No APs in manual uplink selection	You have set uplink selection to Manual, but none of the uplink APs you specified is available or reachable. To resolve this, go to the *Access Points* page on the ZoneDirector web interface, select the AP and click the Configure button, and then click SmartSelect in the Mesh settings.
No APs within hop-limit	The AP cannot find other APs within the internally defined limit to the number of hops. The hop limit mechanism helps ensure that mesh APs maintain reasonable network performance. To resolve this, add additional Root APs near this isolated Mesh AP.
Searching for uplinks	The AP is still searching for uplinks. This is usually a temporary state and is typically resolved automatically within 15 minutes as the mesh network stabilizes. If there is a significant number of APs on the network, it might take longer for the AP to resolve uplinks.
Config error	The AP attempted to establish the mesh uplink but was unsuccessful. If you recently updated the mesh SSID and passphrase, it is likely that your changes have not propagated correctly to this AP (for example, the AP was offline when you updated the mesh SSID and passphrase). To resolve this, follow the instructions in *Recovering an Isolated Mesh AP*.
No APs with matching radio type	The AP is unable to find an uplink AP with the same radio type. Ruckus Smart Mesh APs must use the same radio type to be able connect to each other via the mesh network. For example, an 802.11n/ac/ax Mesh AP will only connect to another 802.11n/ac/ax AP, and an 802.11b/g

Status	Possible Reason
	Mesh AP will only connect to another 802.11b/g AP. To resolve this, place additional wired APs or Mesh APs that use the same radio type near this AP.

Recovering an Isolated Mesh AP

When a Mesh AP becomes isolated, it begins broadcasting a recovery SSID (named “recover.me-<last 6 digits of AP’s MAC address>”), which you can use to connect directly to the AP and make configuration changes.

Note that this SSID is not bridged to the local network for security reasons.

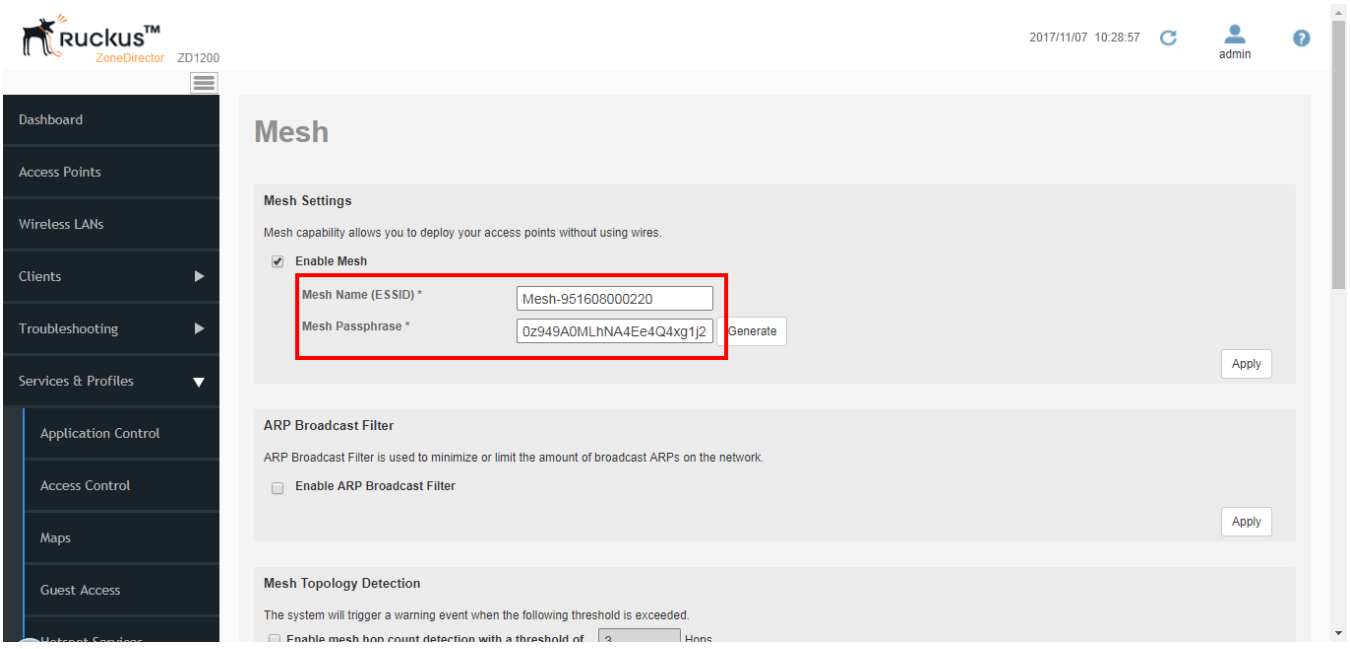
To perform these procedures, you will need:

- A notebook computer with wireless capability.
- The current ZoneDirector mesh configuration (steps for obtaining this information are provided below).
- An SSH client, such as PuTTY or OpenSSH.
- A text editor such as Notepad.

Step 1: Obtain the Mesh SSID and Passphrase

1. On the ZoneDirector web interface, click the **Services & Profiles** tab, and then click **Mesh** on the menu.
2. Under **Mesh Settings**, copy the contents of the **Mesh Name** and **Mesh Passphrase** fields into a text editor.

FIGURE 310 The Mesh Name and Mesh Passphrase you will use to configure the AP



Step 2: Ensure that the AP's Mesh Mode is set to Auto

1. Go to **Access Points** and click the **Edit** link next to the AP you want to recover.
2. Under **Advanced Options** > **Mesh Mode**, select **Auto** and click **OK**.

Step 3: Locate the AP's Mesh Recovery SSID

1. In your notebook's wireless connection list, locate the Mesh recovery SSID. The SSID will be named "Recover.Me-xxxxxx" (where xxxxxx is the last 6 digits of the AP's MAC address).
2. Connect to this WLAN using WPA and the passphrase ruckus-<admin password>. (The admin password is the same as that used to log into ZoneDirector.)

   NOTE
   ZoneDirector allows passwords of less than 8 characters, but the recovery password has to be at least 8 characters. Therefore, if the password is less than 8 characters, hyphens (-) will be added to the passphrase to reach the 8 character minimum. For example, if the admin password is "admin", the recovery passhphrase would be "admin---".

3. You can now access the AP's web interface by entering the AP's recovery IP address **10.154.231.125** in the browser.

   NOTE
   Note that because the AP is still in ZoneDirector-managed state, you cannot make configuration changes via the web interface. Therefore you will need to proceed to the next step and connect to the AP's CLI to make changes.

Step 4: Connect to the AP and update its Mesh settings

1. Launch your SSH client and enter the IP address **10.154.231.125**.
2. Log into the AP via SSH using the same user name and password that you use to log into the ZoneDirector web interface.
3. Enter the command **set meshcfg ssid <current_ssid>**, where "current_ssid" is the SSID that the mesh network is currently using.
4. Enter the command **set meshcfg passphrase <current_passphrase>**, where "current_passphrase" is the passphrase that the mesh network is currently using. To paste text into PuTTY, press ctrl+v to paste, then click the right mouse button.
5. Enter the command **set mesh auto**.
6. If there are multiple ZoneDirectors on the network, you may need to specify which ZoneDirector the AP should connect to, using the command **set director ip <ZoneDirector's IP address>**.
7. If a management VLAN is used for ZoneDirector-AP management traffic, enter the following command: **set ipaddr wan vlan <vlan ID>**.
8. Enter the command **reboot** to restart the AP with the new configuration changes.
9. Close the SSH client.

You have completed recovering the isolated mesh AP. You should be able to manage this AP again shortly. Please wait at least 15 minutes (to allow the mesh network to stabilize), and then try managing this AP again via ZoneDirector.

Best Practices and Recommendations

For recommendations and best practices in planning and deploying a Ruckus Smart Mesh network, refer to Mesh Networking Best Practices on page 405.

Mesh Networking Best Practices

- Calculating the Number of APs Required..... 405
- Placement and Layout Considerations..... 405
- Signal Quality Verification..... 406
- Mounting and Orientation of APs..... 407
- Mesh Best Practice Checklist..... 408

Calculating the Number of APs Required

This is an important step in planning your mesh network. You will need to calculate the number of total APs (Root APs and Mesh APs) that are needed to provide adequate coverage and performance for a given property.

Performing a site survey to determine the coverage for your particular installation environment is essential. Once the coverage area is sufficiently covered with Root APs to meet your bandwidth and throughput requirements, you will need to adjust the number and placement to compensate for APs that will serve as Mesh APs.

If you plan to support Internet grade connections for casual web browsing, plan for a design that delivers 1Mbps of throughput in the entire coverage area. For enterprise-grade connections, plan for 10Mbps of throughput.

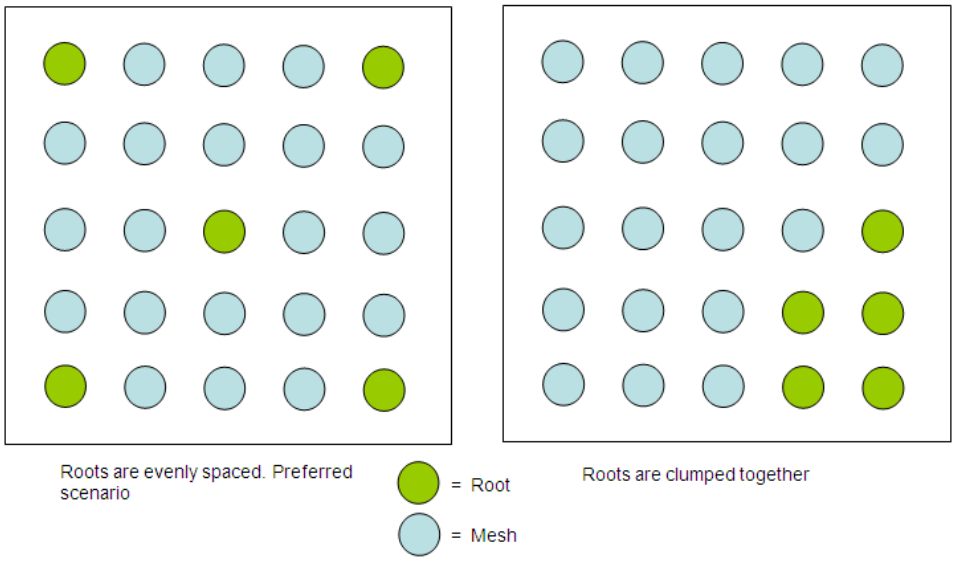
Wi-Fi is a shared medium, of course, so this aggregate bandwidth will be shared amongst the concurrent users at any given time. In other words, if the network is designed to support 10Mbps, for example, it would support 1 user at 10Mbps, or 10 users at 1Mbps each. In reality, due to statistical multiplexing (just like the phone system - the fact that not all users are using the network concurrently), if you use an oversubscription ratio of 4:1, such a network could actually support 40 users at 1Mbps.

In a Smart Mesh network, the Root AP (RAP) has all its wireless bandwidth available for downlink, because the uplink is wired. For Mesh APs (MAPs), the available wireless bandwidth has to be shared between the uplink and the downlink. This degrades performance of a Mesh AP as compared to a Root. This problem is mitigated somewhat by dual radio APs when the uplink and downlink traffic can be sent/received on two separate radios.

Placement and Layout Considerations

- Utilize two or more RAPs: To prevent having a single point-of-failure, it is always best to have 2 or more RAPs so that there are alternate paths back to the wired network.
- More roots are better: The more Root APs in the design, the higher the performance. Therefore, as far as possible, try to wire as many APs as is convenient.
- Design for max 3 hops: Avoid an excessive number of hops in your mesh topology. In general, the goal should be to have the lowest number of hops, provided other considerations (like Signal >= 25%) are met. Limiting the number of hops to 3 or less is best practice.
- Place a Root towards the middle of a coverage area to minimize the # hops required to reach some MAPs.
- If there are multiple Roots, ensure that the Roots are distributed evenly throughout the coverage area (not clumped up close together in one area). Shown in the figure below is an ideal scenario, along with a not-so-ideal scenario. Of course, the whole purpose of mesh is to provide coverage in areas that are hard to wire, therefore the ideal may not be possible. But as far as possible, evenly spaced Root APs are preferable.

FIGURE 311 Root Placement



- If the customer's network utilizes a wireless backhaul technology for broadband access, it is recommended to not mount the broadband wireless modem right next to a Wi-Fi Access Point. A distance of 10 feet or more would be desirable.

Signal Quality Verification

Signal Quality is a measurement of the link quality of the MAP's uplink, and is available on the ZoneDirector web interface.

The above guidelines for planning will result in a well-designed mesh. However, it is advisable to place the APs in the planned locations temporarily using a tripod stand or other means, and actually checking the Signal Quality throughout the mesh network. In addition, once the mesh is deployed, the Signal Quality should be periodically monitored to make sure the mesh is operating optimally.

To view the Signal parameter in the ZoneDirector web interface, go to **Access Points**, and click on the Mesh AP being tested (click the MAC address) to see the Access Point detail screen. There are two best practice observations that should be met:

- Ensure Signal >= 25%: The Signal value under Neighbor APs that shows "Connected" should be 25% or better. If it is lower, you need to bring the AP closer, or move it to avoid an obstruction, such that the Signal value becomes 25% or better. For a more conservative design, you may use 35% as your Signal benchmark.
- Ensure Minimum 2 Uplink options for every MAP: In addition, under Neighbor APs, it is best practice that there exists an alternate path for this mesh uplink. This alternate path should also have a Signal of 25% or better. Stated differently, there should be at least 2 possible links that the MAP can use for uplink, and both should have a Signal value of 25% or better. For a more conservative design, you may use 35% as your Signal benchmark.

Mounting and Orientation of APs

Ruckus APs are very tolerant to a variety of mounting and orientation options due to Ruckus' use of its unique BeamFlex technology, in which the RF signal is dynamically concentrated and focused towards the other end of the RF link.

The bottom line regarding orientation and placement is that during the planning phase, it is advisable to use the Signal Quality as your benchmark, as explained in Signal Quality Verification on page 406. Ensure that the Signal is better than 25% for trouble-free operation.

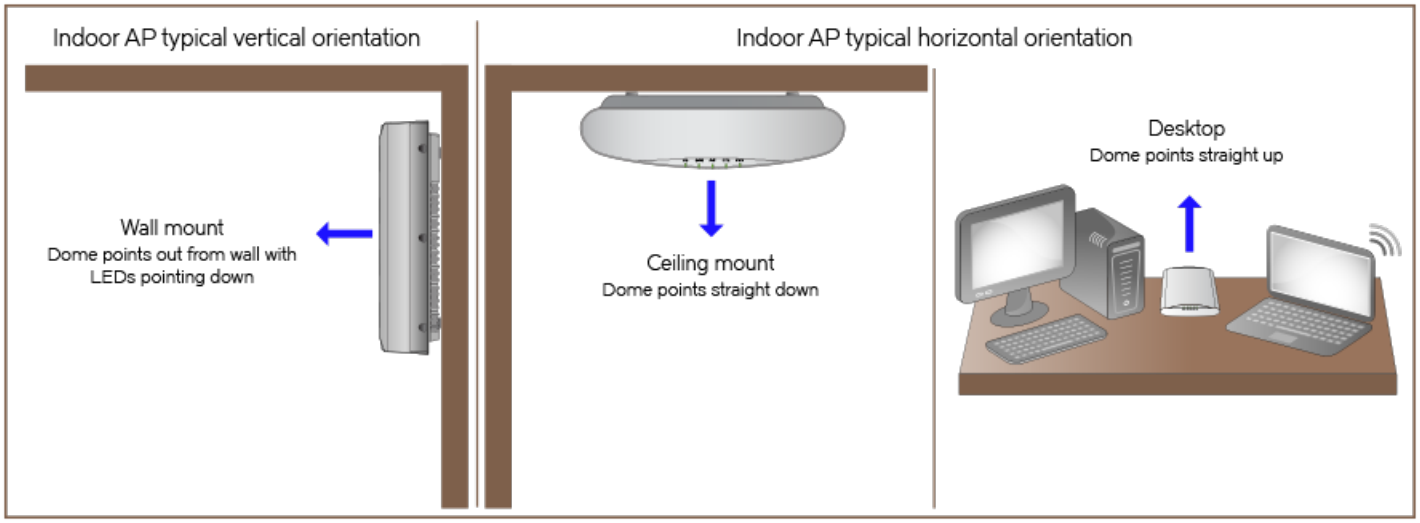
For additional mounting details, please also consult the *Quick Setup Guide* or *Mounting Guide* that came in the AP box.

Indoor APs - Typical Orientation

Ruckus indoor APs are typically oriented such that the dome of the AP is pointing straight down, if ceiling mounted, or away from the wall if wall mounted.

Indoor APs are also frequently installed in desktop scenarios with the dome pointed straight up.

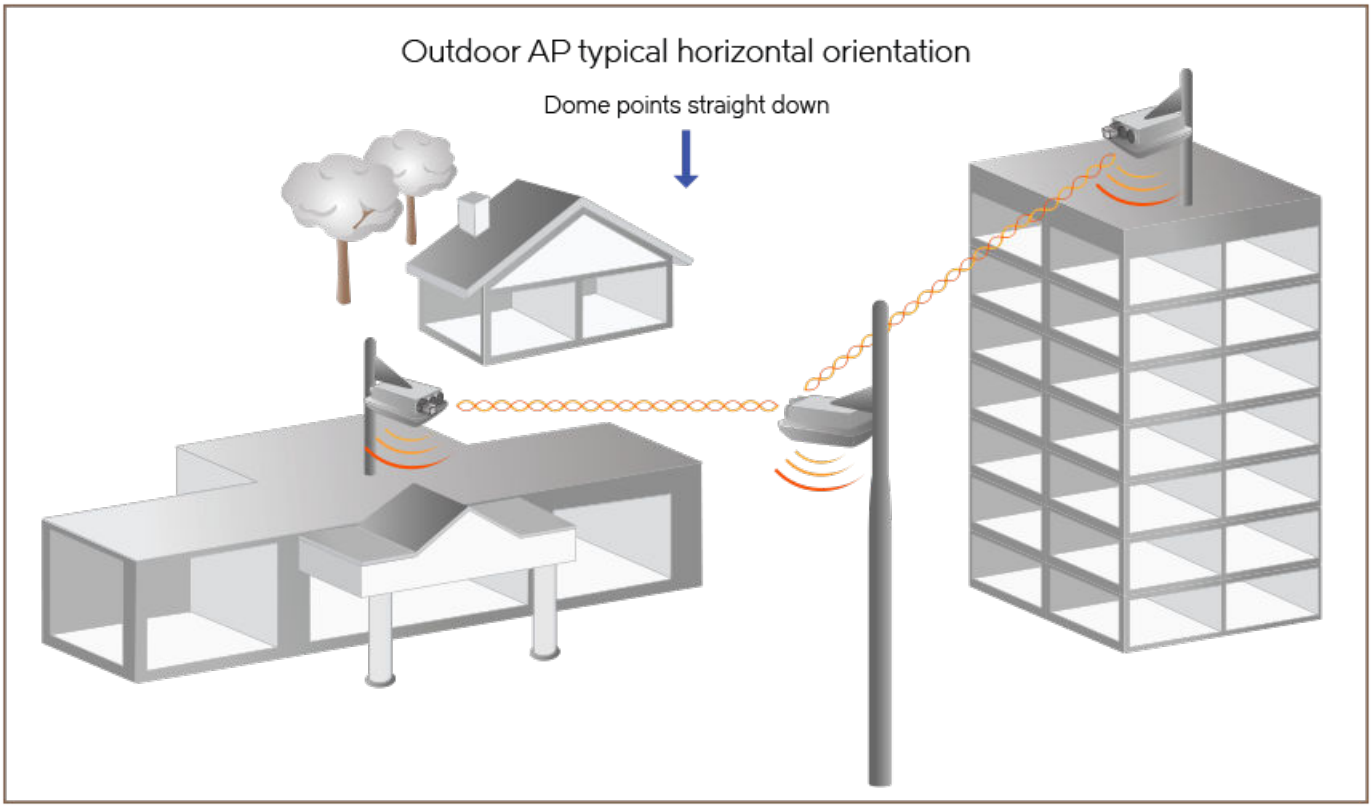
FIGURE 312 Indoor AP typical orientation



Outdoor APs - Typical Horizontal Orientation

Outdoor APs are typically mounted in a horizontal orientation. A less typical orientation would be vertically mounted.

FIGURE 313 Outdoor AP typical horizontal orientation



Elevation of RAPs and MAPs

In addition to orientation, it is important to also pay attention to the elevation of an AP for reliable mesh operation.

More specifically, large differences in elevation should be avoided. So whether you are deploying an indoor mesh, an outdoor mesh, or a mixed indoor-outdoor mesh, you should ensure that as far as convenient and possible, MAPs and RAPs should all be at a similar elevation from the ground. For example, for an indoor-outdoor mesh, if all your indoor RAPs and MAPs are at ceiling height (standard 15-foot ceiling), then you would not want to mount the outdoor MAPs on 40-foot poles. You would want to keep all MAPs and RAPs at around the same elevation from the ground.

Mesh Best Practice Checklist

Following the mesh best practices will ensure that your mesh is well-designed, and have the capacity and reliability required for your enterprise applications. The best practices are summarized below as a checklist for quick review.

1. Avoid an excessive number of hops. Ideally keep hop count to 3 or less.
2. Having more RAPs is better for performance.
3. Ensure that there are RAPs near the middle of a coverage area so as to minimize the number of hops to reach a given MAP.

4. Where possible, ensure that the RAPs are distributed evenly throughout the coverage area rather than clumped together.
5. Once the APs are mounted on a test-basis or permanently, use the Signal quality measurement to ensure that the uplink signal quality from MAP to RAP is 25% or better.
6. Ideally there should be at least one alternate uplink path for each MAP for reliability, and the signal quality of that alternate path should also be 25% or better.

Access Point Power Supply Considerations

- AP Power Warnings..... 411
- Power Limitations by PoE Mode and AP Model..... 413

AP Power Warnings

Beginning with release 10.4, the ZoneDirector dashboard displays warning icons when an AP is operating in reduced power mode.

FIGURE 314 Warning icons indicate an AP is operating in reduced power mode

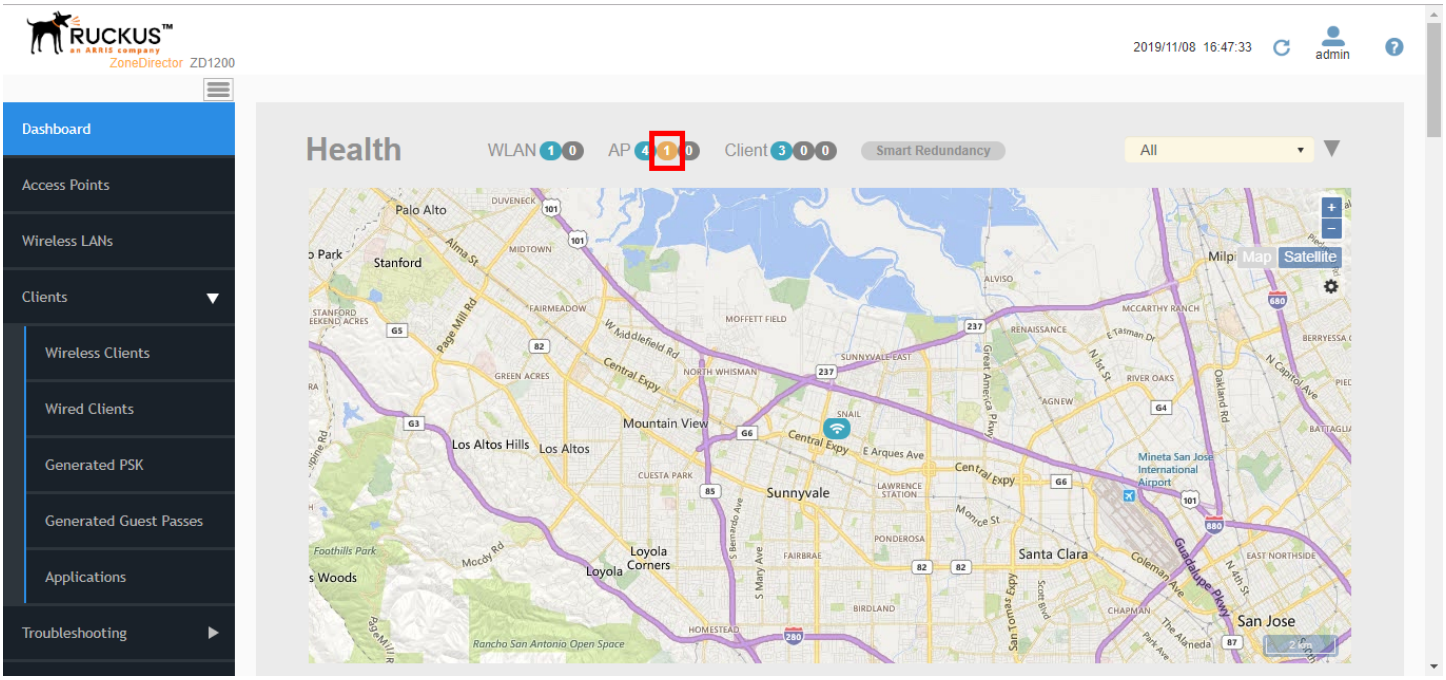
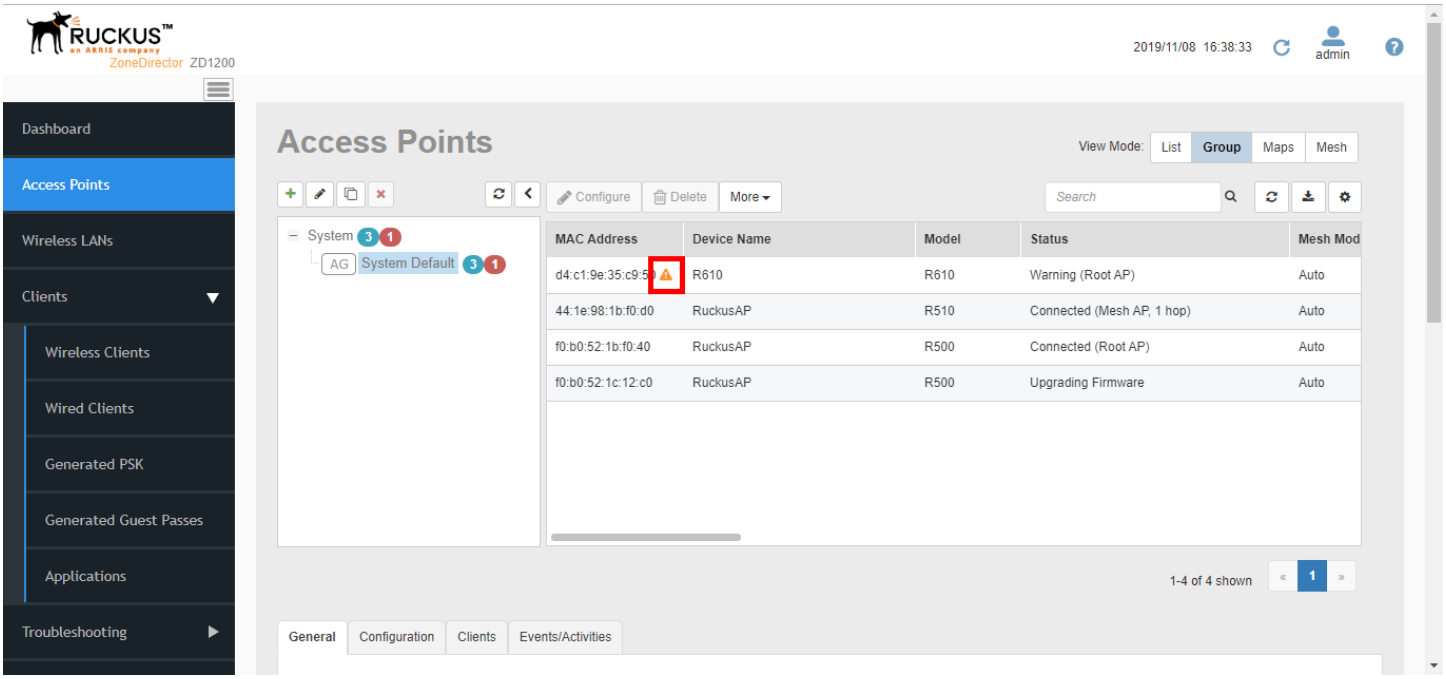


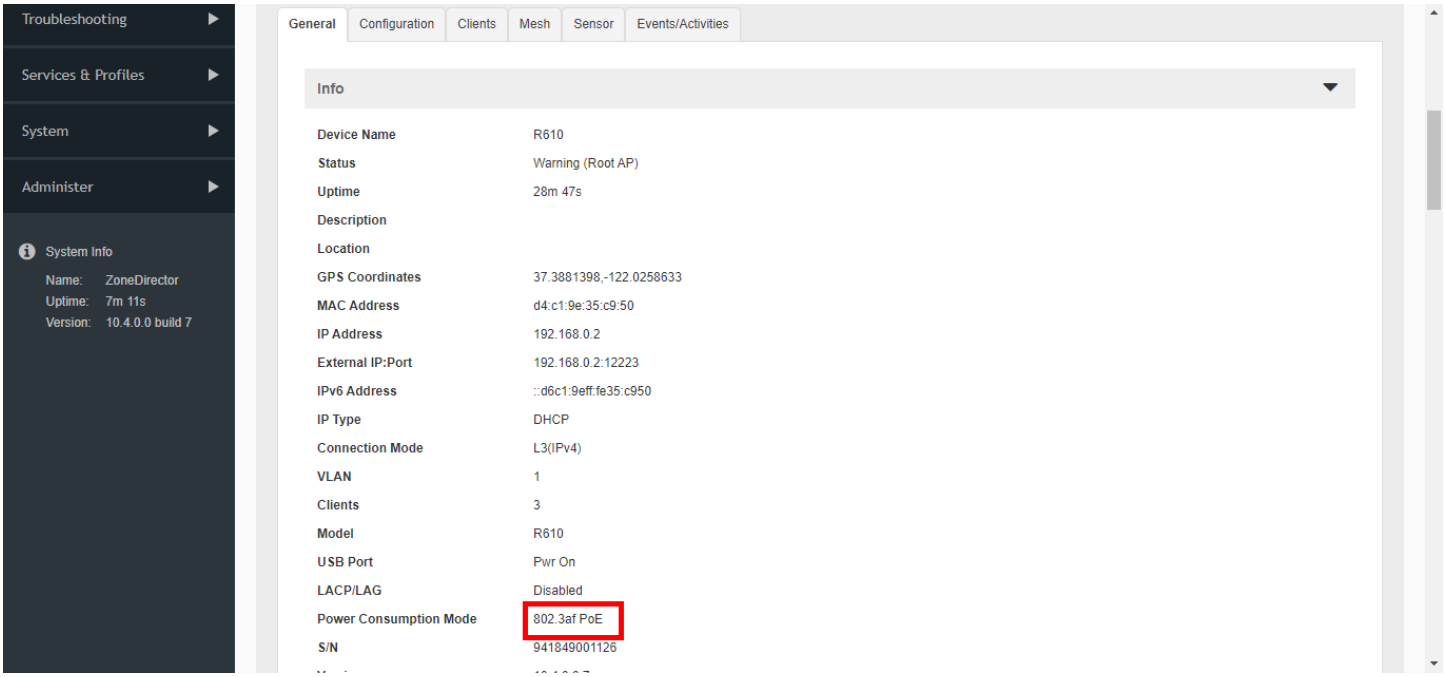
FIGURE 315 Warning icons on the Access Points page



If a warning icon appears, select the AP from the list and scroll down to locate the **Power Consumption Mode** entry in the *General* tab.

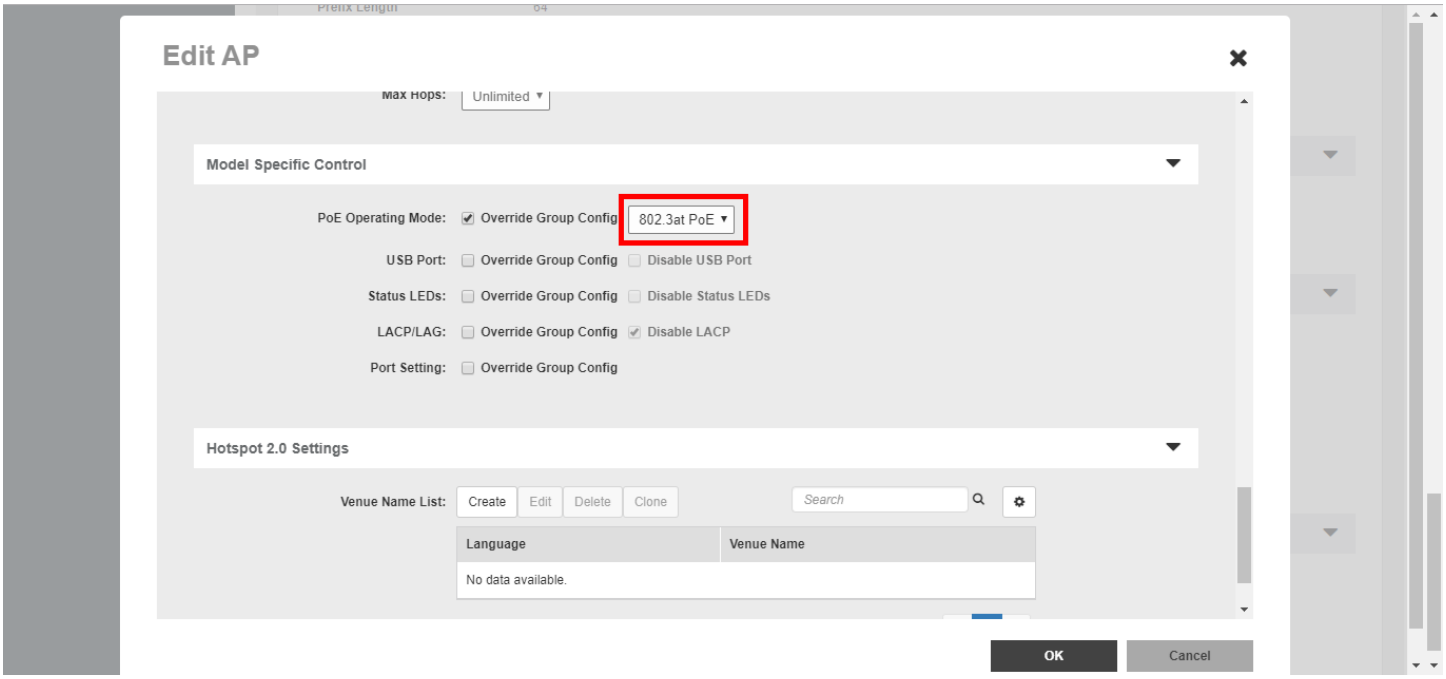
Refer to *Power Limitations by PoE Mode and AP Model* to see what limitations are in effect.

FIGURE 316 Show AP power consumption mode



If power supply deficiency is caused by incorrect power level negotiation between the AP and the switch/PoE injector, you can enforce the AP Power Level on the AP's configuration page. Go to **Access Points > [AP] > Configure > Model Specific Control > PoE Operating Mode**. Enable **Override Group Config** and select a power mode from the menu.

FIGURE 317 Override PoE operating mode



NOTE
If the AP is not receiving full power from the switch, verify that LLDP is enabled on the PoE switch.

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.

TABLE 35 AP Power Limitations

Indoor AP	Outdoor AP
R850	T610
R750	M510
R730	T750
R720	R850
R710	
R650	
R610	
R550	

R850

TABLE 36 R850 PoE Modes

	LLDP Power Ask	2.4G Tx/Rx	5G Tx/Rx	5Gbps Eth	1Gbps Eth	USB	IoT	Comments
DC		4/4	8/8	Enabled	Enabled	Enabled	N/A	
802.3af		1/4	1/8	Enabled	Disabled	Disabled	N/A	Not supported operation mode
802.3at	25W	4/4	4/8	Enabled	Enabled	Enabled (0.5W)	N/A	
802.3bt/Class 5	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/Class 5 from GUI

R750

TABLE 37 R750 PoE Modes

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

R730

TABLE 38 R730 PoE Modes

	LLDP Power Ask	2.4G Tx/Rx	5G Tx/Rx	5Gbps Eth	1Gbps Eth	USB	IoT	Comments
DC		4/4	8/8	Enabled	Enabled	Enabled	N/A	
802.3af		1/4	1/8	Enabled	Disabled	Disabled	N/A	Not supported operation mode
802.3at	25W	4/4	4/8	Enabled	Enabled	Enabled (0.5W)	N/A	
802.3bt/Class 5	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/Class 5 from GUI

R720

TABLE 39 R720 PoE Modes

	LLDP Power Ask	2.4G Tx/Rx	5G Tx/Rx	2.5Gbps Eth	1Gbps Eth	USB	Comments
DC		4/4 (22dBm)	4/4 (23dBm)	Enabled	Enabled	Enabled	
802.3af		1/4 (20dBm)	1/4 (18dBm)	Enabled	Disabled	Disabled	

TABLE 39 R720 PoE Modes (continued)

802.3at	25W	4/4 (20dBm)	4/4 (18dBm)	Enabled	Disabled	Disabled	
802.3bt/Class 5	35W	4/4 (22dBm)	4/4 (23dBm)	Enabled	Enabled	Enabled	
PoE injector (Model 480125A) 60W		4/4	4/4	Enabled	Enabled	Enabled	Force to 802.3bt/ Class 5 from GUI

R710

TABLE 40 R710 PoE Modes

	LLDP Power Ask	2.4G Tx/Rx	5G Tx/Rx	1Gbps Eth (PoE)	1Gbps Eth	USB
DC		4/4 (22dBm)	4/4 (20dBm)	Enabled	Enabled	Enabled
802.3af		2/4 (20dBm)	4/4 (19dBm)	Enabled	Disabled	Disabled
802.3at/Injector (Model 480125A)	25W	4/4 (22dBm)	4/4 (20dBm)	Enabled	Enabled	Enabled

R650

TABLE 41 R650 PoE Modes

	LLDP Power Ask	2.4G Tx/Rx	5G Tx/Rx	2.5Gbps Eth (PoE)	1Gbps Eth	USB	IoT
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 42 R610 PoE Modes

	LLDP Power Ask	2.4G Tx/Rx	5G Tx/Rx	1Gbps Eth (PoE)	1Gbps Eth	USB
DC		4/4	4/4	Enabled	Enabled	Enabled
802.3af		2/4	4/4	Enabled	Disabled	Disabled
802.3at/Injector (Model 480125A)	24W	4/4	4/4	Enabled	Enabled	Enabled

R550

TABLE 43 R550 PoE Modes

	LLDP Power Ask	2.4G Tx/Rx	5G Tx/Rx	1Gbps Eth (PoE)	1Gbps Eth	USB	IoT
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
PoE Injector (Model 480125A)		2/2 (22 dBm)	2/2 (22 dBm)	Enabled	Enabled	Enabled	Enabled

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

FIGURE 318 T750 and T750-SE PoE Modes

	LLDP Power Ask	2.4G Tx/Rx	5G Tx/Rx	2.5Gbps Eth	1Gbps Eth	USB	IoT	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



© 2023 CommScope, Inc. All rights reserved.
350 West Java Dr., Sunnyvale, CA 94089 USA
https://www.commscope.com