



# Ruckus Wireless™ ZoneDirector™

## Release 9.13 User Guide

Part Number 800-71222-001 Rev D  
Published August 2016

[www.ruckuswireless.com](http://www.ruckuswireless.com)



# Copyright Notice and Proprietary Information

Copyright 2016. Ruckus Wireless, Inc. All rights reserved.

No part of this documentation may be used, reproduced, transmitted, or translated, in any form or by any means, electronic, mechanical, manual, optical, or otherwise, without prior written permission of Ruckus Wireless, Inc. ("Ruckus"), or as expressly provided by under license from Ruckus.

## Destination Control Statement

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

## Disclaimer

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

## Limitation of Liability

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

## Trademarks

Ruckus Wireless, Ruckus, the bark logo, ZoneFlex, FlexMaster, ZoneDirector, SmartMesh, Channelfly, Smartcell, Dynamic PSK, and Simply Better Wireless are trademarks of Ruckus Wireless, Inc. in the United States and other countries. All other product or company names may be trademarks of their respective owners.



# Contents

## Copyright Notice and Proprietary Information

### About This Guide

Document Conventions . . . . .	16
Related Documentation . . . . .	17
Documentation Feedback . . . . .	17
Online Training Resources . . . . .	17

## 1 Introducing Ruckus Wireless ZoneDirector

Overview of ZoneDirector . . . . .	20
ZoneDirector Physical Features . . . . .	21
ZoneDirector 1200 . . . . .	21
ZoneDirector 3000 . . . . .	24
ZoneDirector 5000 . . . . .	27
Introduction to the Ruckus Wireless Network . . . . .	32
Ensuring That APs Can Communicate with ZoneDirector . . . . .	32
How APs Discover ZoneDirector on the Network . . . . .	33
How to Ensure that APs Can Discover ZoneDirector on the Network . . . . .	34
Firewall Ports that Must be Open for ZoneDirector Communications . . . . .	43
Installing ZoneDirector . . . . .	46
Accessing ZoneDirector's Command Line Interface . . . . .	47
Using the ZoneDirector Web Interface . . . . .	49
Navigating the Dashboard . . . . .	50
Using Indicator Widgets . . . . .	51
Real Time Monitoring . . . . .	55
Stopping and Starting Auto Refresh . . . . .	57
Registering Your Product . . . . .	58

## 2 Configuring System Settings

System Configuration Overview . . . . .	62
Changing the System Name . . . . .	62
Changing the Network Addressing . . . . .	63
IPv6 Configuration . . . . .	64

Enabling an Additional Management Interface . . . . .	66
Creating Static Route Entries . . . . .	68
Static Route Example. . . . .	69
Enabling Smart Redundancy. . . . .	70
Configuring ZoneDirector for Smart Redundancy. . . . .	71
Forcing Failover to the Backup ZoneDirector . . . . .	74
Managing Smart Redundancy AP License Pools . . . . .	74
Configuring the Built-in DHCP Server . . . . .	76
Enabling the Built-in DHCP server . . . . .	76
Viewing DHCP Clients . . . . .	78
Controlling ZoneDirector Management Access . . . . .	78
Setting the System Time. . . . .	80
Setting the Country Code . . . . .	81
Channel Optimization. . . . .	82
Channel Mode . . . . .	84
Changing the System Log Settings. . . . .	84
Reviewing the Current Log Contents . . . . .	84
Customizing the Current Log Settings . . . . .	85
Setting Up Email Alarm Notifications . . . . .	90
Customizing Email Alarms that ZoneDirector Sends . . . . .	93
Configuring SMS Settings for Guest Pass Delivery via SMS . . . . .	93
Enabling Login Warning Messages . . . . .	94
Enabling Network Management Systems . . . . .	96
Enabling SmartCell Insight Communication . . . . .	96
Enabling Management via FlexMaster . . . . .	97
Enabling Northbound Portal Interface Support . . . . .	99
Configuring SNMP Support . . . . .	100
Enabling Telnet . . . . .	108
Configuring DHCP Relay. . . . .	108
Enabling Bonjour Gateway . . . . .	111
Bridge Service Rules . . . . .	112
Bridge Service Records . . . . .	112
Creating a Bonjour Gateway Rule - ZD Site . . . . .	113
Creating a Bonjour Gateway Rule - AP Site . . . . .	115
Applying a Bonjour Policy to an AP . . . . .	117
Example Network Setup . . . . .	118
Configuring SPoT Location Services . . . . .	119

### 3 Configuring Security and Other Services

Configuring Self Healing Options . . . . .	126
Automatically Adjust AP Power . . . . .	126
Automatic Channel Selection . . . . .	126
Load Balancing . . . . .	131
Band Balancing . . . . .	134
Radar Avoidance Pre-Scanning . . . . .	135
AeroScout RFID Tag Detection . . . . .	136
Ekahau Tag Detection . . . . .	137
Active Client Detection . . . . .	138
Tunnel Configuration . . . . .	139
Packet Inspection Filter . . . . .	141
Ethernet Port Redundancy . . . . .	142
Configuring Wireless Intrusion Prevention . . . . .	144
DoS Protection . . . . .	144
Intrusion Detection and Prevention . . . . .	145
Rogue Access Points . . . . .	145
Rogue DHCP Server Detection . . . . .	147
Controlling Network Access Permissions . . . . .	150
Creating Layer 2/MAC Address Access Control Lists . . . . .	150
Creating Layer 3/Layer 4/IP Address Access Control Lists . . . . .	151
Configuring Device Access Policies . . . . .	153
Configuring Precedence Policies . . . . .	156
Blocking Client Devices . . . . .	157
Configuring Client Isolation White Lists . . . . .	161
Application Recognition and Filtering . . . . .	164
Using an External AAA Server . . . . .	171
Active Directory . . . . .	171
LDAP . . . . .	174
RADIUS / RADIUS Accounting . . . . .	178

### 4 Managing a Wireless Local Area Network

Overview of Wireless Networks . . . . .	200
About Ruckus Wireless WLAN Security . . . . .	201
Creating a WLAN . . . . .	202
General Options . . . . .	203
WLAN Usage Types . . . . .	204
Authentication Method . . . . .	224
Fast BSS Transition . . . . .	224

Encryption Options . . . . .	225
Options . . . . .	226
Advanced Options . . . . .	229
Creating a Copy of an Existing WLAN for Workgroup Use. . . . .	236
Customizing WLAN Security . . . . .	237
Reviewing the Initial Security Configuration. . . . .	237
Fine-Tuning the Current Security Mode . . . . .	238
Switching to a Different Security Mode. . . . .	238
Using the Built-in EAP Server . . . . .	240
Authenticating with an External RADIUS Server . . . . .	240
If You Change the Internal WLAN to WEP or 802.1X . . . . .	241
Working with WLAN Groups . . . . .	241
Creating a WLAN Group . . . . .	242
Assigning a WLAN Group to an AP . . . . .	243
Viewing a List of APs That Belong to a WLAN Group . . . . .	244
Deploying ZoneDirector WLANs in a VLAN Environment . . . . .	245
Tagging Management Traffic to a VLAN . . . . .	247
How Dynamic VLAN Works . . . . .	249
Working with VLAN Pools . . . . .	252
Working with Hotspot Services . . . . .	255
Creating a Hotspot Service . . . . .	255
Assigning a WLAN to Provide Hotspot Service. . . . .	259
Common WISPr Attribute Abbreviations. . . . .	260
Creating a Hotspot 2.0 Service . . . . .	261
Create a Service Provider Profile . . . . .	261
Working with Dynamic Pre-Shared Keys . . . . .	267
Enabling Dynamic Pre-Shared Keys on a WLAN . . . . .	268
Setting Dynamic Pre-Shared Key Expiration. . . . .	270
Generating Multiple Dynamic PSKs . . . . .	271
Creating a Batch Dynamic PSK Profile . . . . .	273
Bypass Apple CNA . . . . .	275

## 5 Managing Access Points

Adding New Access Points to the Network. . . . .	278
Connecting the APs to the Network . . . . .	278
Verifying/Approving New APs. . . . .	279
Working with Access Point Groups. . . . .	281
Modifying the System Default AP Group. . . . .	282
Creating a New Access Point Group . . . . .	284



Modifying Access Point Group Membership . . . . .	284
Modifying Model Specific Controls . . . . .	285
Configuring AP Ethernet Ports . . . . .	287
Viewing AP Ethernet Port Status . . . . .	297
Reviewing Current Access Point Policies . . . . .	299
Using Limited ZD Discovery for N+1 Redundancy . . . . .	301
Importing a USB Software Package . . . . .	303
Managing Access Points Individually . . . . .	305
Configuring Hotspot 2.0 Venue Settings for an AP . . . . .	308
Optimizing Access Point Performance . . . . .	309
Assessing Current Performance Using the Map View . . . . .	309
Improving AP RF Coverage . . . . .	310
Assessing Current Performance Using the Access Point Table . . . . .	310
Adjusting AP Settings . . . . .	310
Prioritizing WLAN Traffic . . . . .	311

## 6 Monitoring Your Wireless Network

Reviewing the ZoneDirector Monitoring Options . . . . .	314
Importing a Map View Floorplan Image . . . . .	315
Requirements . . . . .	315
Importing the Floorplan Image . . . . .	315
Placing the Access Point Markers . . . . .	316
Using the Map View Tools . . . . .	317
AP Icons . . . . .	319
Evaluating and Optimizing Network Coverage . . . . .	320
Moving the APs into More Efficient Positions . . . . .	320
Reviewing Current Alarms . . . . .	321
Reviewing Recent Network Events . . . . .	321
Clearing Recent Events/Activities . . . . .	322
Monitoring WLAN Status . . . . .	322
Reviewing Current User Activity . . . . .	324
Viewing Application Usage Statistics . . . . .	324
Active Clients . . . . .	329
Inactive Clients . . . . .	329
Events/Activities . . . . .	329
Monitoring Individual Clients . . . . .	331
Monitoring Client Performance . . . . .	332
Monitoring Wired Clients . . . . .	334
Monitoring Access Point Status . . . . .	334

Using the AP Status Overview Page . . . . .	335
Monitoring Individual APs . . . . .	339
Using Action Icons to Manage and Troubleshoot APs . . . . .	340
RF Pollution FAQ . . . . .	342
Spectrum Analysis . . . . .	345
Neighbor APs. . . . .	347
Access Point Sensor Information . . . . .	348
Monitoring Mesh Status . . . . .	348
Detecting Rogue Access Points . . . . .	349
Monitoring System Ethernet Port Status . . . . .	352
Monitoring AAA Server Statistics. . . . .	352
Monitoring Location Services . . . . .	353

## 7 Managing User Access

Enabling Automatic User Activation with Zero-IT . . . . .	356
Clients that Support Zero-IT . . . . .	357
Self-Provisioning Clients with Zero-IT . . . . .	358
Self-Provisioning Clients without Ethernet Ports . . . . .	359
Provisioning Clients that Do Not Support Zero-IT . . . . .	359
Adding New User Accounts to ZoneDirector. . . . .	360
Internal User Database. . . . .	360
Managing Current User Accounts . . . . .	362
Changing an Existing User Account . . . . .	362
Deleting a User Record . . . . .	363
Creating New User Roles . . . . .	363
Role Based Access Control Policy . . . . .	365
Managing Automatically Generated User Certificates and Keys. . . . .	366
Using an External Server for User Authentication. . . . .	367
Activating Web Authentication. . . . .	369
Captive Portal Redirect on Initial Browser HTTPS Request. . . . .	370

## 8 Managing Guest Access

Configuring Guest Access. . . . .	374
Creating a Guest Access Service . . . . .	374
Using Guest Pass Self-Service. . . . .	376
Configuring Guest Subnet Restrictions. . . . .	387
Creating a Guest WLAN . . . . .	388
Using the BYOD Onboarding Portal . . . . .	389
Working with Guest Passes . . . . .	393

Configuring Guest Pass Generation . . . . .	393
Generating and Delivering a Single Guest Pass . . . . .	397
Generating and Printing Multiple Guest Passes at Once . . . . .	401
Monitoring Generated Guest Passes . . . . .	403
Customizing the Guest Login Page . . . . .	404
Creating a Custom Guest Pass Printout . . . . .	405
Delivering Guest Passes via Email . . . . .	407
Delivering Guest Passes via SMS . . . . .	408
<b>9 Deploying a Smart Mesh Network</b>	
Overview of Smart Mesh Networking . . . . .	412
Smart Mesh Networking Terms . . . . .	412
Supported Mesh Topologies . . . . .	413
Standard Topology . . . . .	413
Wireless Bridge Topology . . . . .	414
Hybrid Mesh Topology . . . . .	415
Deploying a Wireless Mesh via ZoneDirector . . . . .	416
Step 1: Prepare for Wireless Mesh Deployment . . . . .	417
Step 2: Enable Mesh Capability on ZoneDirector . . . . .	417
Step 3: Provision and Deploy Mesh Nodes . . . . .	419
Step 4: Verify That the Wireless Mesh Network Is Up . . . . .	420
Understanding Mesh-related AP Statuses . . . . .	422
Using the ZoneFlex LEDs to Determine the Mesh Status . . . . .	423
On Single-band ZoneFlex APs . . . . .	423
On Dual-band ZoneFlex APs . . . . .	424
Using Action Icons to Configure and Troubleshoot APs in a Mesh . . . . .	427
Setting Mesh Uplinks Manually . . . . .	428
Troubleshooting Isolated Mesh APs . . . . .	430
Understanding Isolated Mesh AP Statuses . . . . .	430
Recovering an Isolated Mesh AP . . . . .	431
Best Practices and Recommendations . . . . .	433
<b>10 Setting Administrator Preferences</b>	
Changing the ZoneDirector Administrator User Name and Password . . . . .	436
Setting Administrator Login Session Timeout . . . . .	437
Changing the Web Interface Display Language . . . . .	437
Upgrading ZoneDirector and ZoneFlex APs . . . . .	438
Importing a Default Application Package . . . . .	439
Enabling Secure AP Image Upgrade . . . . .	439

Performing an Upgrade with Smart Redundancy . . . . .	440
Working with Backup Files . . . . .	440
Backing Up a Network Configuration . . . . .	441
Restoring Archived Settings to ZoneDirector . . . . .	441
Restoring ZoneDirector to Default Factory Settings. . . . .	445
Alternate Factory Default Reset Method . . . . .	446
Working with SSL Certificates . . . . .	447
Basic Certificate Installation . . . . .	447
Generating a Certificate Signing Request . . . . .	447
Importing an SSL Certificate. . . . .	450
SSL Certificate Advanced Options . . . . .	452
Using an External Server for Administrator Authentication . . . . .	459
Upgrading the License . . . . .	461
Support Entitlement . . . . .	462

## 11 Troubleshooting

Troubleshooting Failed User Logins . . . . .	466
Fixing User Connections . . . . .	467
If WLAN Connection Problems Persist . . . . .	468
Measuring Wireless Network Throughput with SpeedFlex. . . . .	468
Using SpeedFlex in a Multi-Hop Smart Mesh Network . . . . .	472
Allowing Users to Measure Their Own Wireless Throughput . . . . .	474
Diagnosing Poor Network Performance . . . . .	475
Starting a Radio Frequency Scan . . . . .	475
Using the Ping and Traceroute Tools . . . . .	476
Generating a Debug File . . . . .	478
Viewing Current System and AP Logs. . . . .	478
Packet Capture and Analysis . . . . .	480
Local Capture . . . . .	481
Streaming Mode . . . . .	481
AP Diagnostic Information. . . . .	484
Importing a Script . . . . .	485
Enabling Remote Troubleshooting . . . . .	485
Restarting an Access Point . . . . .	486
Restarting ZoneDirector . . . . .	487

## 12 Smart Mesh Networking Best Practices

Choosing the Right AP Model for Your Mesh Network . . . . .	490
Calculating the Number of APs Required . . . . .	490

Placement and Layout Considerations . . . . .	491
Signal Quality Verification . . . . .	492
Mounting and Orientation of APs . . . . .	494
Indoor APs - Typical Case: Horizontal Orientation . . . . .	494
Indoor APs - Vertical Orientation . . . . .	495
Outdoor APs - Typical Horizontal Orientation . . . . .	496
Elevation of RAPs and MAPs . . . . .	496
Best Practice Checklist . . . . .	497

## Appendix: Zone 2 APs

### Index



# About This Guide

This *User Guide* describes how to install, configure and manage the Ruckus Wireless™ ZoneDirector™ version 9.13.

This guide is intended for use by those responsible for managing Ruckus Wireless 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 Reader Portable Document Format (PDF) or HTML on the Ruckus Wireless Support website at <https://support.ruckuswireless.com/documents>.

---

**NOTE:** By downloading this software and subsequently upgrading the ZoneDirector to version 9.13, 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.

---

# Document Conventions

Table 1 and Table 2 list the text and notice conventions that are used throughout this guide.

Table 1. Text conventions

Convention	Description	Example
monospace	Represents information as it appears on screen	[Device name] >
<b>monospace bold</b>	Represents information that you enter	[Device name] > <b>set ipaddr 10.0.0.12</b>
<b>default font bold</b>	Keyboard keys, software buttons, and field names	On the <b>Start</b> menu, click <b>All Programs</b> .
<i>italics</i>	Screen or page names	Click <b>Advanced Settings</b> . The <i>Advanced Settings</i> page appears.

Table 2. Notice conventions

Notice Type	Description
<b>Note</b>	Information that describes important features or instructions
<b>Caution</b>	Information that alerts you to potential loss of data or potential damage to an application, system, or device
<b>Warning</b>	Information that alerts you to potential personal injury



## Related Documentation

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

- *Online Help*: Provides instructions for performing tasks using the web interface. The online help is accessible from the web interface and is searchable.
- *Release Notes*: Provide information about the current software release, including new features, enhancements, and known issues.

## Documentation Feedback

Ruckus Wireless is interested in improving its documentation and welcomes your comments and suggestions. You can email your comments to Ruckus Wireless at:

[docs@ruckuswireless.com](mailto:docs@ruckuswireless.com)

When contacting us, please include the following information:

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

For example:

- ZoneDirector 9.13 User Guide
- Part number: 800-71222-001 Revision D
- Page 88

## Online Training Resources

To access a variety of online Ruckus Wireless training modules, including free introductory courses to wireless networking essentials, site surveys, and Ruckus Wireless products, visit the Ruckus Wireless Training Portal at:

<https://training.ruckuswireless.com>



# Introducing Ruckus Wireless ZoneDirector

# 1

In this chapter:

- [Overview of ZoneDirector](#)
- [ZoneDirector Physical Features](#)
- [Introduction to the Ruckus Wireless Network](#)
- [Ensuring That APs Can Communicate with ZoneDirector](#)
- [Installing ZoneDirector](#)
- [Accessing ZoneDirector's Command Line Interface](#)
- [Using the ZoneDirector Web Interface](#)
- [Registering Your Product](#)

## Overview of ZoneDirector

Ruckus Wireless ZoneDirector serves as a central control system for Ruckus ZoneFlex Access Points (APs). ZoneDirector provides simplified 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 Wireless ZoneFlex APs allows deployment of a Smart Mesh network, to extend wireless coverage throughout a location without having to physically 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 WLAN, in addition to providing much greater flexibility in AP placement.

ZoneDirector also integrates network monitoring, sophisticated user access controls, integrated Wi-Fi client performance 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 802.11 ac, are used.

This user guide provides complete instructions for using the Ruckus Wireless web interface, the wireless network management interface for ZoneDirector. With the web interface, you can customize and manage all aspects of ZoneDirector and your ZoneFlex network.

# ZoneDirector Physical Features

Three models of ZoneDirector are currently available:

- [ZoneDirector 1200](#)
- [ZoneDirector 3000](#)
- [ZoneDirector 5000](#)

This section describes the physical features of these ZoneDirector models.

---

**NOTE:** ZoneDirector 1100 is discontinued (EOL) as of release 9.12 and cannot be upgraded to 9.12 or later.

---

## ZoneDirector 1200

This section describes the following physical features of ZoneDirector 1200:

- [Buttons, Ports, and Connectors](#)
- [Front Panel LEDs](#)

Figure 1. ZoneDirector 1200



### Buttons, Ports, and Connectors

[Table 1](#) describes the buttons, ports and connectors on ZoneDirector 1200.

Table 1. 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. For information on what the two Ethernet LEDs indicate, refer to <a href="#">Table 2</a> .
Console	RJ-45 Console port for accessing the ZoneDirector command line interface.
F/D	<p>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 <a href="#">Alternate Factory Default Reset Method</a>.</p> <p><i>WARNING: Resetting ZoneDirector to factory default settings will erase all configuration changes that you made, except for AP licenses and SSL certificates.</i></p>

## Front Panel LEDs

[Table 2](#) describes the LEDs on the front panel of ZoneDirector 1200.

Table 2. 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.

<b>LED Label</b>	<b>State</b>	<b>Meaning</b>
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.

## ZoneDirector 3000

This section describes the following physical features of ZoneDirector 3000:

- [Buttons, Ports, and Connectors](#)
- [Front Panel LEDs](#)

Figure 2. ZoneDirector 3000



### Buttons, Ports, and Connectors

[Table 3](#) describes the buttons, ports and connectors on ZoneDirector 3000.

Table 3. ZoneDirector 3000 front panel elements

Label	Meaning
Power	(Located on the rear panel) Press this button to power on ZoneDirector.
F/D	To reset ZoneDirector to factory default settings, press the F/D button for at least five (5) seconds. For more information, refer to <a href="#">Alternate Factory Default Reset Method</a> .  <i>WARNING: Resetting ZoneDirector to factory default settings will erase all configuration changes that you have made, except for AP licenses and SSL certificates.</i>



Label	Meaning
Reset	To restart ZoneDirector, press the Reset button once for less than two seconds.
USB	For Ruckus Wireless Support use only
Console	RJ-45 port for accessing the ZoneDirector command line interface.
10/100/1000 Ethernet	Two auto negotiating 10/100/1000Mbps Ethernet ports. For information on what the two Ethernet LEDs indicate, refer to <a href="#">Table 4</a> .

## Front Panel LEDs

[Table 4](#) describes the LEDs on the front panel of ZoneDirector 3000.

Table 4. ZoneDirector 3000 LED descriptions

LED Label	State	Meaning
Power	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.
	Solid Red	ZoneDirector has shut down (but is still connected to a power source).
	Flashing Red	ZoneDirector is starting up or shutting down.

<b>LED Label</b>	<b>State</b>	<b>Meaning</b>
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	Amber	The port is connected to a 1000Mbps device.
	Green	The port is connected to a 100Mbps device.
	Off	The port is connected to a 10Mbps device.

## ZoneDirector 5000

This section describes the following physical features of ZoneDirector 5000:

- [Front Panel Features](#)
- [Front Panel \(Bezel Removed\)](#)
- [Control Panel](#)
- [Rear Panel Features](#)

Figure 3. ZoneDirector 5000 Front Panel



### Front Panel Features

Table 5. ZoneDirector 5000 front panel features

Feature	Description
Control Panel	See <a href="#">Control Panel</a> description below.
RJ45 Serial Port	COM 2 / Serial B port for accessing the ZoneDirector command line interface.
USB Port	Not used.
Front Bezel Lock	Remove this bezel lock to remove the front bezel and gain access to the hard drive bays.

## Front Panel (Bezel Removed)

Figure 4. ZoneDirector 5000 front panel (bezel removed)

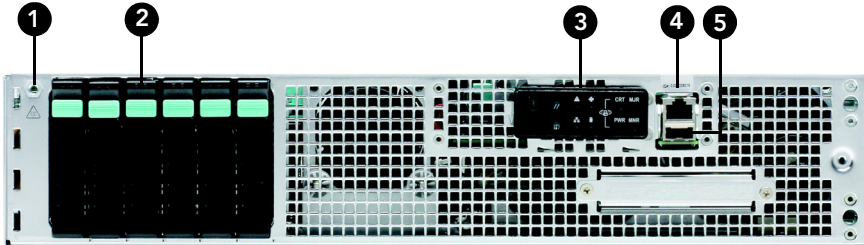


Table 6. ZoneDirector front panel elements

Number	Feature
1	ESD ground strap attachment
2	Hard drive bays (not used)
3	Control panel
4	RJ45 serial port for accessing the ZoneDirector command line interface.
5	USB port (not used).

## Control Panel

Figure 5. Control panel buttons and indicators

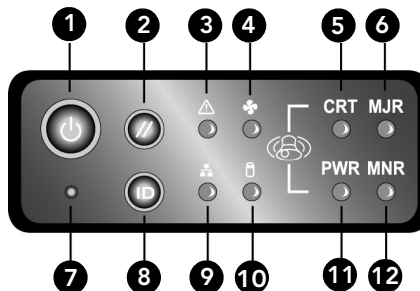


Table 7. ZoneDirector 5000 control panel

Number	Feature
1	Power button
2	System reset button
3	System status LED (see <a href="#">Table 8</a> )
4	Fan status LED
5	Critical alarm (not used)
6	MJR alarm (not used)
7	NMI pin hole button (factory reset button)
8	Chassis ID button
9	NIC 1 / NIC 2 activity LED
10	HDD activity LED (not used)
11	PWR alarm LED (not used)
12	MNR alarm (Amber: system unavailable; OFF: system available)

Table 8. System status LED definitions

LED Status	Definition
Off	No power supply detected, or two power supplies detected and system is off
Green On	System ready/normal operation, two power supplies detected
Green Blinking	<ol style="list-style-type: none"> <li>1. System ready but degraded</li> <li>2. One power supply connected</li> <li>3. One fan failure detected</li> </ol>
Amber On	<ol style="list-style-type: none"> <li>1. Critical or non-recoverable condition</li> <li>2. Power up in progress, only one power source detected</li> <li>3. More than one fan failure detected</li> </ol>
Amber Blinking	Non-critical alarm

## Rear Panel Features

Figure 6. ZoneDirector 5000 rear panel features

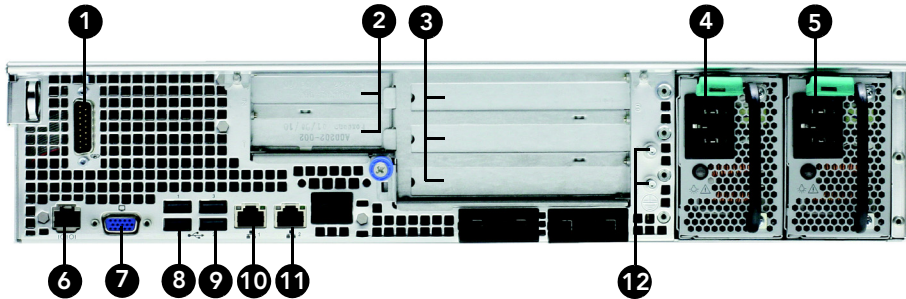


Table 9. Rear panel features

Number	Feature
1	Alarms cable connector (not used)
2	Two low-profile PCIe add-in cards (not used)
3	Three full-length PCIe add-in cards (not used)
4	Power supply 2 (backup AC power)
5	Power supply 1 (primary AC power)
6	RJ45 serial port (COM2/serial B)
7	Video connector (not used)
8	USB 0 and 1 (#1 on top)
9	USB 2 and 3 (#3 on top)
10	GbE NIC #1 connector
11	GbE NIC #2 connector
12	Two ground studs (used for DC-input system)

Table 10. NIC status LEDs

<b>LED Color</b>	<b>LED State</b>	<b>NIC State</b>
Green/Amber (Left)	Off	10Mbps
	Green	100Mbps
	Amber	1000Mbps
Green (Right)	On	Active connection
	Blinking	Transmit / Receive activity

# Introduction to the Ruckus Wireless Network

Your new Ruckus Wireless network starts when you disperse a number of Ruckus Wireless access points (APs) to efficiently cover your worksite. After connecting the APs to ZoneDirector (through network hubs or switches), running through the Setup Wizard and completing the “Zero-IT” setup, you have a secure wireless network for both registered users and guest users.

---

**NOTE:** “Zero-IT” refers to ZoneDirector’s simple setup and ease-of-use features, which allow end users to automatically self-configure wireless settings on Windows and Mac OS clients as well as many mobile devices including iOS, Windows Phone and Android OS devices.

---

After using the web interface to set up user accounts for staff and other authorized users, your WLAN can be put to full use, enabling users to share files, print, check email, and more. And as a bonus, guest workers, contractors and visitors can be granted limited controlled access to a separate “Guest WLAN” with minimal setup. You can now fine-tune and monitor your network through the web interface, which enables you to customize additional WLANs for authorized users, manage your users, monitor the network’s security and performance, and expand your radio coverage, if needed.

## 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](#)), 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 (over a locally connected ZoneDirector).

- 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 attempt to discover ZoneDirector again by repeating the same discovery cycle. The AP will continue to repeat this 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](#)
- [Option 2: Customize Your DHCP Server](#)
- [Option 3: Register ZoneDirector with a DNS Server](#)

---

**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 Server. If your DHCP server is running on a different operating system, the procedure may be different.

---

**NOTE:** For ZD 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 Wireless 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 Wireless 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.

For example: If 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 FlexMaster information (sub-option code 01)**

- **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.

For example: If the Flex Master 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 FlexMaster 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, FlexMaster 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
FlexMaster	<code>http://192.168.10.1/intune/server</code> (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 servers 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 Wireless 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 Wireless 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 and appears in the DHCP Vendor Class dialogue list. Click **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 **03** 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 Reservation, just like any other DHCP option, using **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 7. Ensuring that DHCPv6 Option 17 is configured correctly

```
▼ Vendor-specific Information
  Option: Vendor-specific Information (17)
  Length: 76
  Value: 000061dd000600202001192001cf000000000000000001...
  Enterprise ID: Ruckus Wireless, Inc. (25053)
▼ option
  Option code: 6
  Option length: 32
  Option data: 2001192001cf0000000000000000000012001192001cf0000...
▼ option
  Option code: 3
  Option length: 32
  Option data: 2001192001cf0000000000000000000032001192001cf0000...
```

### 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.

---

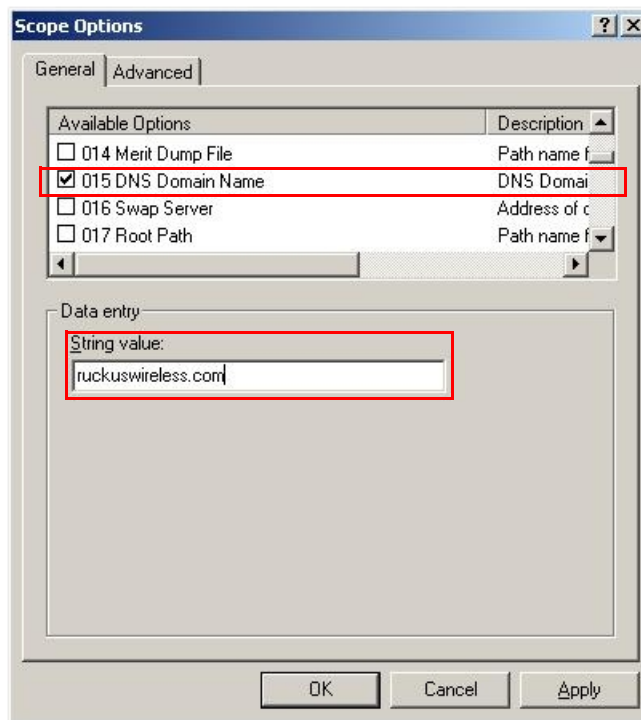
#### ***Step 1: Set the DNS Domain Name on the DHCP Server***

- 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 8. Select the 015 DNS Domain Name check box, and then type your company domain name in String value

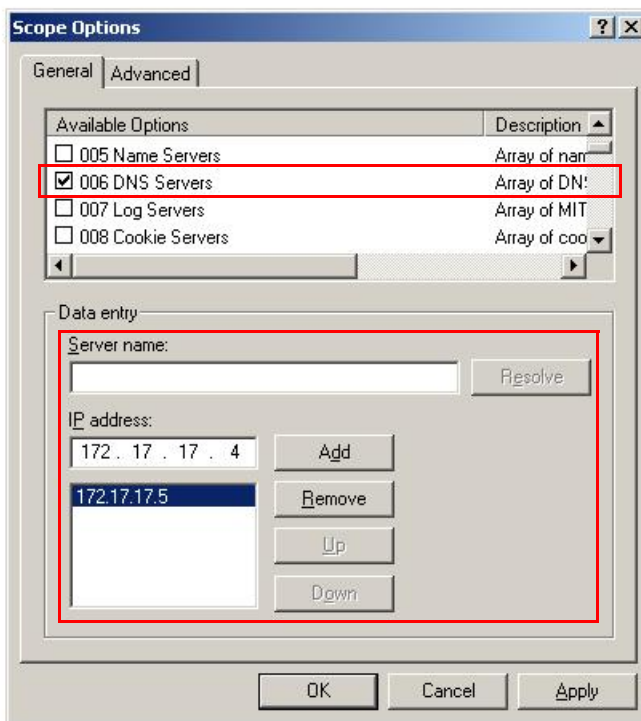


### ***Step 2: Set the DNS Server IP Address on the DHCP Server***

- 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 **General** 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 9. 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 firewalls located between ZoneDirector, FlexMaster or the access points. The following table lists the ports that need to be open for different types of communications.

Table 11. Firewall ports that must be open for ZoneDirector communications

<b>Communication</b>	<b>Ports</b>
ZoneDirector Web UI access	TCP destination ports 80 and 443 (HTTP and HTTPS)
AP > ZoneDirector LWAPP	UDP destination ports 12222 and 12223
AP > ZoneDirector SpeedFlex	UDP port 18301
AP > ZoneDirector (AP) firmware upgrade	TCP port 21 (the firewall must be stateful for PASV FTP transfers)
AP > ZoneDirector application statistics reporting	TCP port 21 (FTP) TCP port: Random port higher than 1024
ZoneDirector > ZoneDirector Smart Redundancy	TCP destination port 443 and port 33003

ZoneDirector > FlexMaster registration/inform/firmware upgrade	TCP destination port 443
FlexMaster > ZoneDirector management interface	TCP destination port as specified in FM Inventory 'Device Web Port Number Mapping'
ZoneDirector CLI access	TCP destination port 22 (SSH)
TACACS+ server < > ZoneDirector	TCP destination port 49 (TACACS+) (default)

---

**NOTE:** Additionally, TCP port 1883 is used for AP to AP communication, for infrastructure services shared by many applications/features, such as avpd, nbrd, ftromd, and so on. However, this communication is only between adjacent APs, which are normally not separated by firewalls/ACLs. Therefore this should not have any impact on customer network infrastructure.

---

## NAT Considerations

Beginning with version 9.2, ZoneDirector can be deployed in a private network behind a NAT (Network Address Translation) device. When ZoneDirector is deployed on an isolated private network where NAT is used, administrators can manually configure a port-mapping table on the NAT device to allow remote access into ZoneDirector. This allows APs to establish an LWAPP connection with ZoneDirector, as well as allowing remote HTTPS and SSH management access to ZoneDirector. [Table 11](#) lists the ports that must be open for trans-NAT communications.

Specifically, the following ports must be mapped to ZoneDirector's private IP address on the NAT device's port mapping table: ports 21, 22, 80, 443, 12222, 12223.

Note that there are some limitations with this configuration, including:

- SpeedFlex performance test tool will not work (ZoneDirector needs to know the IP addresses of the APs).
- Deploying two ZoneDirectors behind the same NAT in a Smart Redundancy configuration requires creation of two port forwarding rules (one for each ZoneDirector physical IP address), and that the APs are configured with both ZoneDirectors' public IP addresses as primary and secondary ZD IPs.

- An active ZoneDirector behind NAT will be unable to perform upgrades to the standby ZoneDirector on the other side of the NAT device.

# 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 7 and Windows 8, you may need to **Turn on network discovery** in the *Network and Sharing Center > Advanced Sharing Settings*.
- 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 worksite, connect them to power and to your LAN.
- 6 Begin using your ZoneFlex network.

Figure 10. Discover ZoneDirector using UPnP

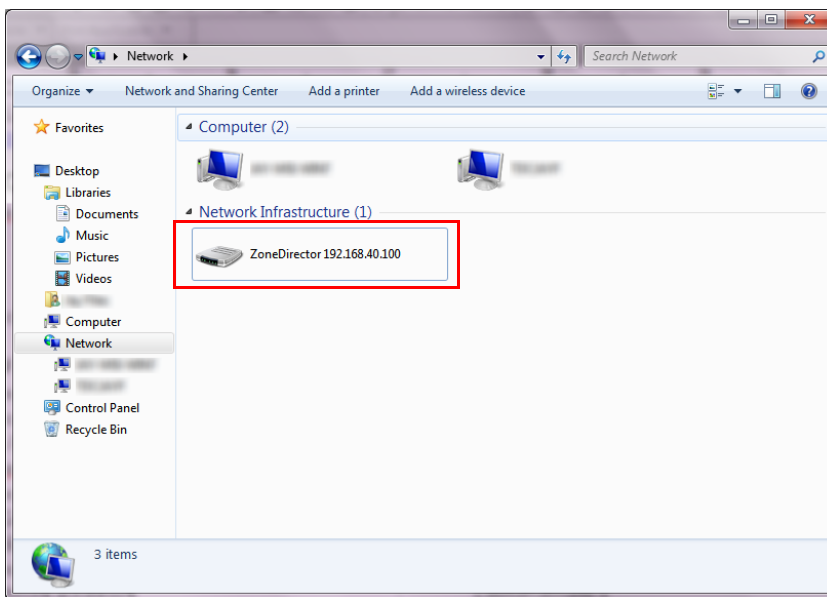
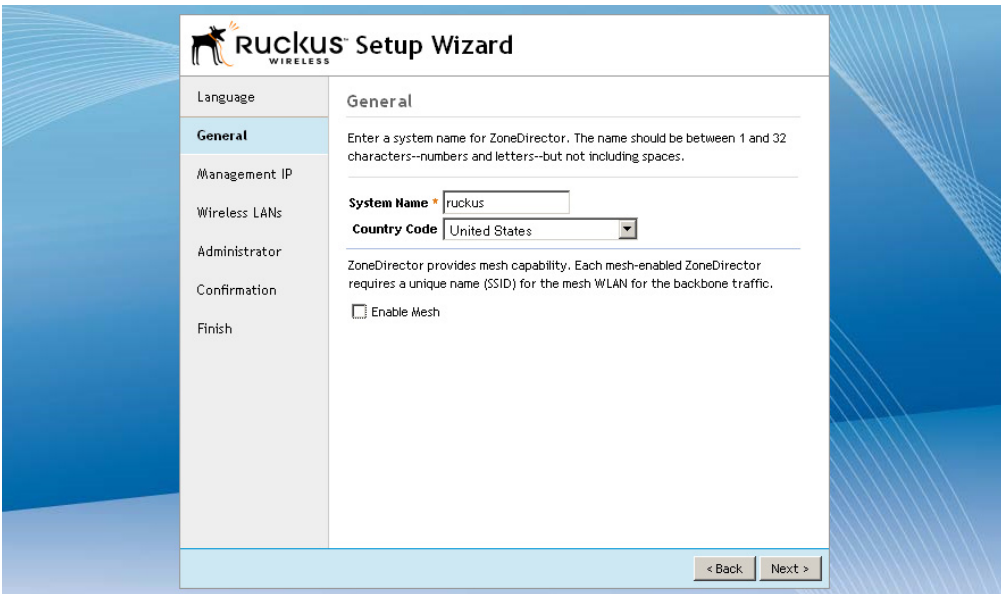


Figure 11. ZoneDirector Setup Wizard



## Accessing ZoneDirector's Command Line Interface

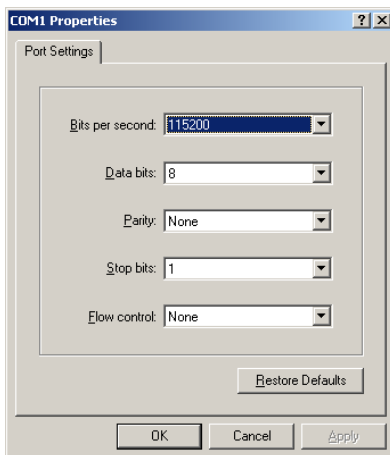
In general, this User Guide provides instructions for managing ZoneDirector and your ZoneFlex network using the ZoneDirector web interface. You can also perform many management and configuration tasks using the ZoneDirector Command Line Interface (CLI) by connecting directly to the Console port or an 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 12. 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 and monitor your Ruckus Wireless WLANs (including ZoneDirector and all APs).

Dashboard	<p>When you first log into your ZoneDirector using the web interface, the Dashboard appears, displaying a number of widgets containing indicators and tables that summarize the network and its current status. Each indicator, gauge or table provides links to more focused, detailed views on elements of the network.</p> <p>TIP: You can minimize (hide) any of the tables or indicators on the Dashboard, then reopen them by means of the Add Widget options in the lower left corner.</p>
Widgets	<p>Widgets are Dashboard components, each containing a separate indicator or table as part of the active dashboard. Each widget can be added or removed to enhance your ZoneDirector Dashboard summary needs.</p>
Tabs	<p>Click any of the four tabs (Dashboard, Configure, Monitor, and Administer) to take advantage of related sets of features and options. When you click a tab, ZoneDirector displays a collection of tab-specific buttons. Each tab's buttons are a starting point for Ruckus Wireless network setup, management, and monitoring.</p>
Buttons	<p>The left-side column of buttons varies according to which tab has been clicked. The buttons provide features that assist you in managing and monitoring your network. Click a button to see related options in the workspace to the right.</p>
Workspace	<p>The large area to the right of the buttons will display specific sets of features and options, depending on which tab is open and which button was clicked.</p>
Toolbox	<p>The drop-down menu at the top right corner provides access to the Real Time Monitoring, Auto-Refresh and Network Connectivity tools, used for diagnosing and monitoring your ZoneFlex network. It also provides a tool to stop and start automatically refreshing the web interface pages.</p>
Help and Log Out	<p>Clicking Help launches the online Help - which is an HTML-based subset of the information contained in this User Guide. Click Log Out to exit the web interface.</p>

## Navigating the Dashboard

The Dashboard offers a number of self-contained indicators and tables that summarize the network and its current status. Some indicators have fields that link to more focused, detailed views on elements of the network.

Figure 13. The Dashboard

The screenshot shows the ZoneDirector web interface dashboard. The top navigation bar includes 'Dashboard', 'Monitor', 'Configure', and 'Administer'. The main content area is divided into several sections:

- System Overview:** Displays system name (ZoneDirector), IP address (192.168.40.100), MAC address (6C:AA:B3:00:00:A0), uptime (10d 23h 59m), model (ZD1200), licensed APs (5), S/N (123456789012), and version (9.13.0.0 build 87).
- Devices Overview:** Shows the number of APs (1), authorized client devices (0), total client devices (0), and rogue devices (13).
- Usage Summary:** Provides statistics for concurrent users (0), bytes transmitted (93K), average signal (N/A), and rogue devices (13).
- Currently Managed APs:** A table listing APs with columns for MAC Address, Device Name, Model, Status, Mesh Mode, IP Address, Channel, Clients, Application Capability, and Action. Two APs are shown, both with status 'Disconnected'.
- Most Recent User Activities:** A table showing user activities with columns for Date/Time, Severity, and User Activities.
- Most Active Client Devices (since the last connection):** A table listing active client devices with columns for MAC Address, IP Address, and User Usage.
- Currently Active WLANs:** A table listing active WLANs with columns for Name, ESSID, Authentication, Encryption, VLAN, and Clients.
- Mesh Topology (Mesh-123456789012):** A table listing mesh topology details with columns for Access Points, Signal (%), Description, AP Group, Channel, IP Address, Clients, Action, and Diagnostics.
- Most Recent System Activities:** A table showing system activities with columns for Date/Time, Severity, and Activities.
- Most Frequently Used Access Points:** A table listing frequently used access points with columns for MAC Address, IP Address, Description, Model, and Clients.
- Support:** A section providing links for Company, Warranty Info, Online Support, Product Registration, Activate Your Account, Ruckus Support Web, Support Documentation, Discussion Forums, and Open a Support Case.

**NOTE:** Some indicators may not be present upon initial view. The Add Widgets feature, located at the bottom left area of the screen, enables you to show or hide indicators. See [Using Indicator Widgets](#).

**NOTE:** You can sort the information (in ascending or descending order) that appears on the dashboard by clicking the column headers. Some widgets (such as *Currently Managed APs*) can also be customized to hide columns so that the tables do not run off the page. Click the **Edit Columns** button to customize the widget according to your preferences.

## Using Indicator Widgets

Dashboard widgets represent the indicators displayed as part of the active dashboard. Indicator widgets can be added or removed to enhance your ZoneDirector summary needs.

The following indicators are provided:

- *System Overview*: Shows ZoneDirector system information including its IP address, MAC address, model number, maximum number of licensed APs, serial number, software version number, and others.
- *Devices Overview*: Shows the number of APs being managed by ZoneDirector, the number of authorized clients, and the total number of clients connected to the managed APs (authorized and unauthorized). It also shows the number of rogue devices that have been detected by ZoneDirector.
- *Usage Summary*: Shows usage statistics for the last hour and the last 24 hours.
- *Mesh Topology*: Shows the mesh status and topology of all APs connected via mesh uplinks or downlinks.
- *Most Active Client Devices*: Identifies the most active clients by MAC address, IP address, and user name. Bandwidth usage is calculated in megabytes (MB) and is based on the total number of bytes sent (Tx) and received (Rx) by each client from the time it associated with the managed AP.
- *Most Recent User Activities*: Shows activities performed by users on client machines.
- *Most Recent System Activities*: Shows system activities related to ZoneDirector operation.
- *Most Frequently Used Access Points*: Lists the access points that are serving the most client requests.
- *Currently Active WLANs*: Shows details of currently active WLANs.
- *Currently Active WLAN Groups*: Shows details of available WLAN groups. If you have not created any WLAN groups, only the *Default WLAN* group appears.
- *Currently Managed APs*: Shows details of access points that ZoneDirector is currently managing.
- *Currently Managed AP Groups*: Shows details of the System Default and user-defined AP groups. Click the + button next to an AP group to expand the group to display all members of the AP group.
- *Support*: Shows contact information for Ruckus Wireless support, product registration and support account activation.

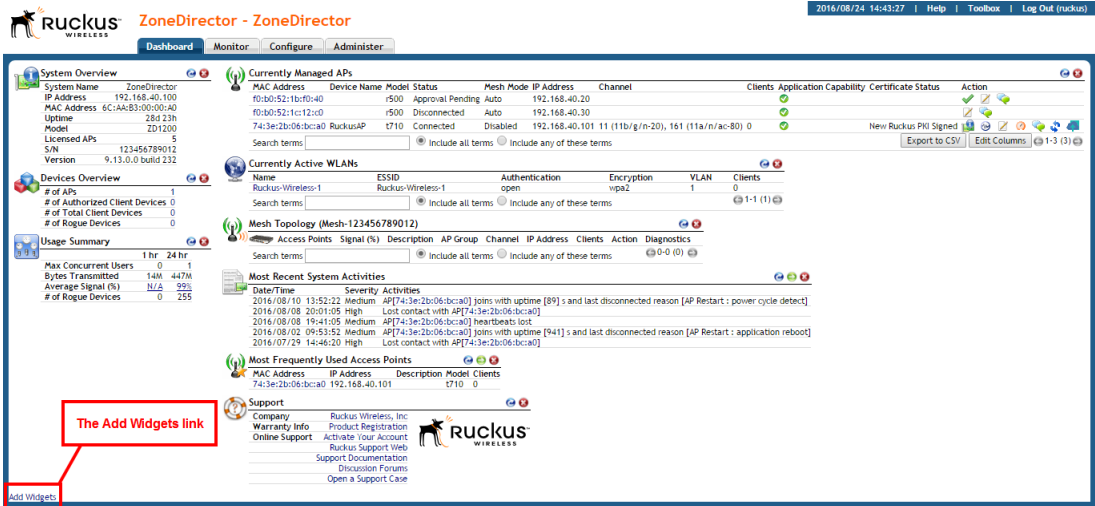
- *Smart Redundancy*: Displays the status of primary and backup ZoneDirector devices, if configured.
- *AP Activities*: Shows a list of recent log events from APs.
- *Client Device Type*: Displays a pie chart of currently connected client devices by OS type as a percentage of the total.
- *Top 10 Applications by Usage*: Lists the top 10 applications, their total usage in KB and percent of the total.
- *Top 10 APs by Usage*: Lists the top 10 APs, their total usage in KB and percent of the total.
- *Top 10 Clients by Usage*: Lists the top 10 clients, their total usage in KB and percent of the total.
- *Top 10 SSIDs by Usage*: Lists the top 10 SSIDs, their total usage in KB and percent of the total.
- *Applications*: Displays a pie chart of the top applications as a percent of the total traffic volume.
- *LBS Venue Info*: Displays status of Location Based Services (SPoT) venues configured for this ZoneDirector.

## Adding a Widget

To add a widget:

- 1 Go to the **Dashboard**.
- 2 Click the **Add Widgets** link located at the bottom left corner of the Dashboard page.

Figure 14. The Add Widgets link is at the bottom-left corner of the Dashboard



The Widgets pane opens at the upper-left corner of the Dashboard.

- 3 Select any widget icon and drag and drop it onto the Dashboard to add the widget. If you have closed a widget, it appears in this pane.

Figure 15. The widget icons appear at the top-left corner of the Dashboard

The screenshot shows the Ruckus ZoneDirector web interface. At the top left, there is a 'Finish' button and a vertical pane of widget icons. A red box highlights these icons with the label 'Widget Icons'. The main dashboard area displays various system overview metrics, tables for managed APs, user activities, active WLANs, mesh topology, and system activities.

**System Overview**

System Name	ZoneDirector
IP Address	192.168.40.100
MAC Address	6C:AA:B3:00:00:40
Uptime	11d 5m
Model	ZD1200
Licensed APs	5
S/N	123456789012
Version	9.13.0.0 build 87

**Usage Summary**

Max Concurrent Users	0	0
Bytes Transmitted	115K	11M
Average Signal (%)	N/A	N/A
# of Rogue Devices	14	37

**Currently Managed APs**

MAC Address	Device Name	Model	Status	Mesh Mode	IP Address	Channel	Clients	Application Capability	Action
f0:b0:52:1b:f0:40	r500	r500	Disconnected	Auto	192.168.40.16				
cd:c5:20:3b:91:f0	RuckusAP	z7372	Connected	Disabled	192.168.40.10	11 (11b/g/n-20), 36 (11a/n-40)	0		
f0:b0:52:1c:12:c0	r500	r500	Disconnected	Auto	192.168.40.18				

**Most Recent System Activities**

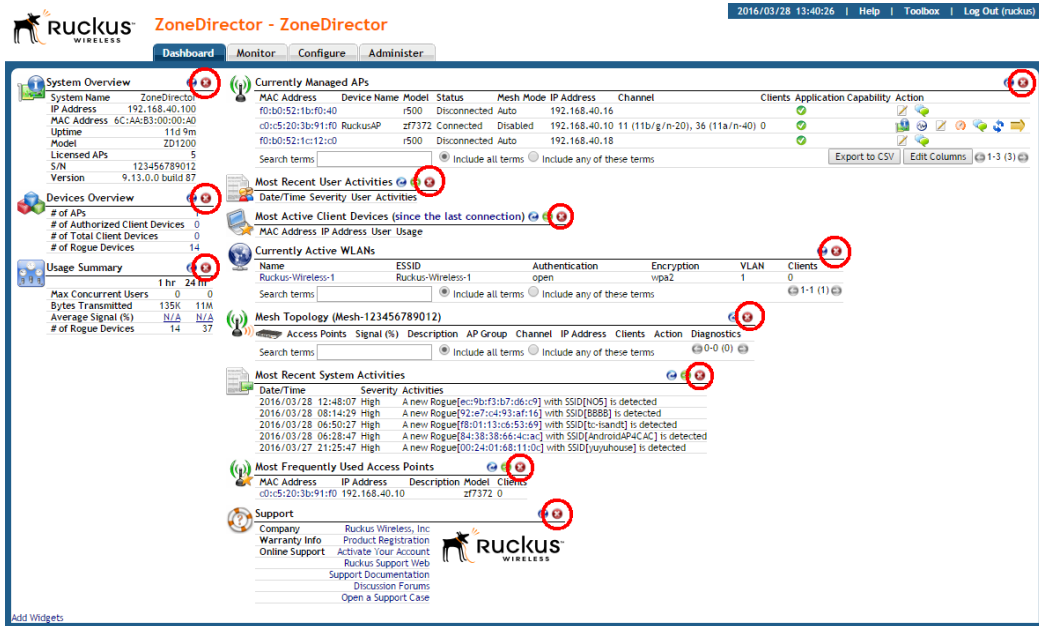
Date/Time	Severity	Activities
2016/03/28 12:48:07	High	A new Rogue[ec:9b:f3:b7:dc:c9] with SSID[NOS] is detected
2016/03/28 08:14:29	High	A new Rogue[92:e7:c4:93:af:16] with SSID[B88B] is detected
2016/03/28 06:50:27	High	A new Rogue[8:01:13:c6:53:69] with SSID[ro-learn] is detected
2016/03/28 06:28:47	High	A new Rogue[84:38:38:66:4c:ac] with SSID[AndroidAP4CAC] is detected
2016/03/27 21:25:47	High	A new Rogue[00:24:01:68:11:0c] with SSID[yuuhouse] is detected

4 Click **Finish** in the Widgets pane to close it.

## Removing a Widget

To remove a widget from the Dashboard, click the icon for any of the widgets currently open on the Dashboard. The Dashboard refreshes and the widget that you removed disappears from the page.

Figure 16. To remove a widget, click the corresponding red X icon

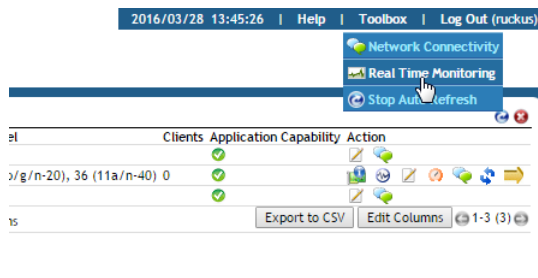


## Real Time Monitoring

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.

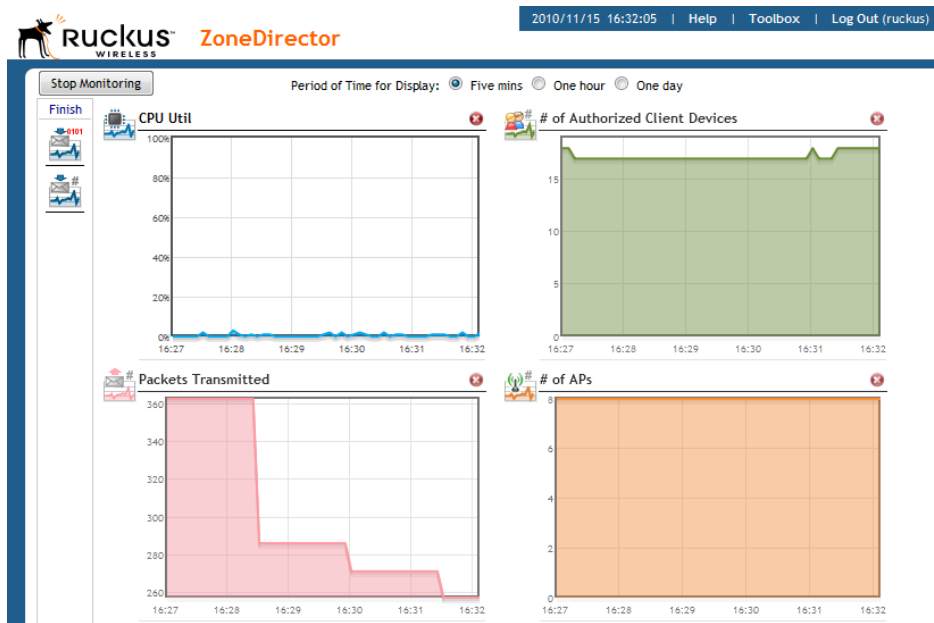
To view the Real Time Monitoring page, locate the **Toolbox** link at the top of the page and select **Real Time Monitoring** from the pull-down menu. You can also access the Real Time Monitoring page from the **Monitor > Real Time Monitoring** tab.

Figure 17. Select Real Time Monitoring from the Toolbox



Like the Dashboard, you can drag and drop Widgets onto the Real Time Monitoring page to customize the information you want to see.

Figure 18. The Real Time Monitoring screen



Select a time increment to monitor statistics by (5 minutes, 1 hour or 1 day) and click **Start Monitoring** to begin.

## Real Time Monitoring Widgets

- *CPU Util*: Displays the % utilization of ZoneDirector's CPU.
- *Memory Util*: Displays the % utilization of ZoneDirector's memory.
- *# of APs*: Displays the number of APs being managed by ZoneDirector.
- *# of Client Devices*: Displays the number of client devices associated to APs being managed by ZoneDirector.
- *Bytes Received*: Total bytes received by all APs being managed by ZoneDirector.
- *Bytes Transmitted*: Total bytes received by all APs being managed by ZoneDirector.



- *Packets Received*: Total packets received by all APs being managed by Zone-Director.
- *Packets Transmitted*: Total packets transmitted by all APs being managed by ZoneDirector.

## Stopping and Starting Auto Refresh

By default, ZoneDirector web interface pages automatically refresh themselves periodically depending on activity. You can pause auto-refresh on any page in the web interface from the Toolbox. After clicking **Stop Auto Refresh**, ZoneDirector pauses automatic updating of all widgets on the current page and the refresh icons on the widgets are disabled (greyed out). To restart auto refresh, click **Start Auto Refresh** from the Toolbox.

Figure 19. Stopping and starting automatic page refreshing

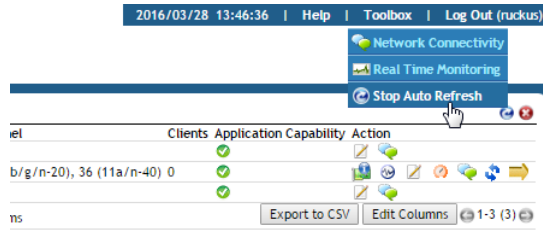
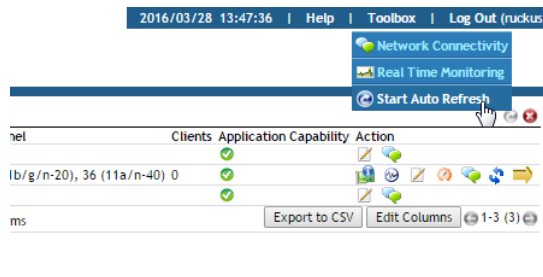


Figure 20. The Refresh icon on all widgets is disabled when auto refresh is stopped



# Registering Your Product

**NOTE:** Ruckus Wireless 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 Click the **Product Registration** link in the *Support* widget on the Dashboard, or
- 2 Go to **Administer > Registration**.
- 3 Enter your contact information on the Registration page, 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](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.

Figure 21. Support Widget on the Dashboard



Figure 22. The Product Registration page

2016/03/28 13:52:41 | Help | Toolbox | Log Out (ruckus)

**ruckus** WIRELESS **ZoneDirector - ZoneDirector**

Dashboard Monitor Configure **Administer**

### Product Registration

**Required fields**

To start the registration process, fill out the required information, and then click Apply to generate the registration request file (.csv). Save the file, and then go to [https://support.ruckuswireless.com/warranty\\_registration](https://support.ruckuswireless.com/warranty_registration) to upload the device registration file.

If you need to create an account first, go to [https://support.ruckuswireless.com/get\\_access\\_now](https://support.ruckuswireless.com/get_access_now)

Name*	<input type="text" value="John Doe"/>
Email*	<input type="text" value="jdoe@abc.com"/>
Phone*	<input type="text" value="123412341234"/>
Company Name*	<input type="text" value="AAA"/>
Company Address*	<input type="text" value="1234 Road Rd."/>

Your ZoneDirector is now registered with Ruckus Wireless.

## Registering Your Product

Stopping and Starting Auto Refresh

# Configuring System Settings

# 2

In this chapter:

- [System Configuration Overview](#)
- [Changing the Network Addressing](#)
- [Creating Static Route Entries](#)
- [Enabling Smart Redundancy](#)
- [Configuring the Built-in DHCP Server](#)
- [Controlling ZoneDirector Management Access](#)
- [Setting the System Time](#)
- [Setting the Country Code](#)
- [Changing the System Log Settings](#)
- [Setting Up Email Alarm Notifications](#)
- [Configuring SMS Settings for Guest Pass Delivery via SMS](#)
- [Enabling Login Warning Messages](#)
- [Enabling Network Management Systems](#)
- [Configuring DHCP Relay](#)
- [Enabling Bonjour Gateway](#)
- [Configuring SPoT Location Services](#)

# System Configuration Overview

The majority of ZoneDirector's general system settings can be accessed from the *Configure > System* page in the web interface. A basic set of parameters is configured during the Setup Wizard process. These parameters and others can be customized on this page.

---

**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.

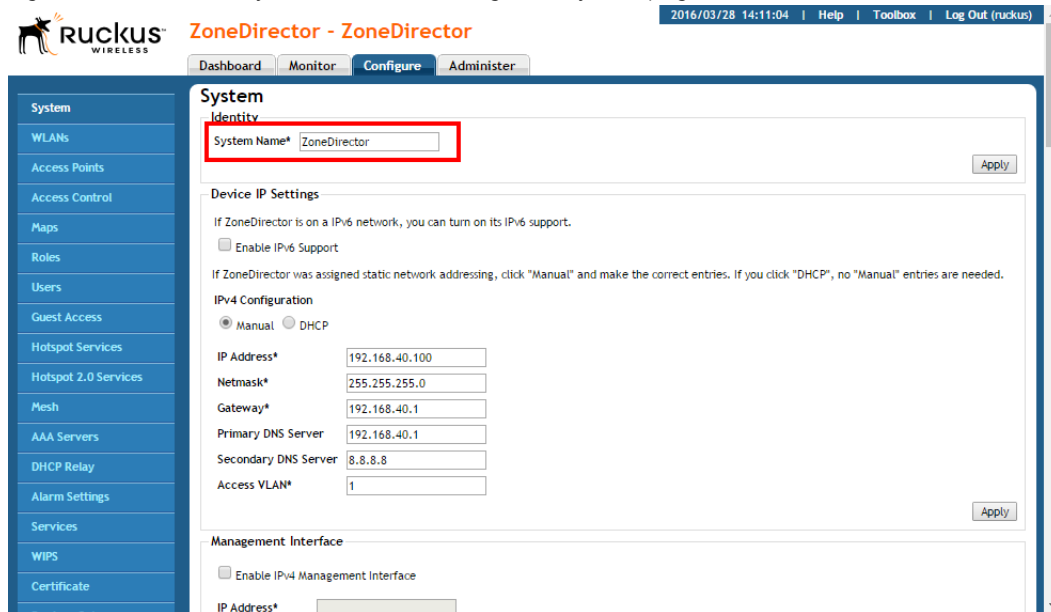
---

## 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 **Configure > System**.
- 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.

Figure 23. The Identity section on the Configure &gt; System page



The screenshot shows the Ruckus ZoneDirector web interface. The top navigation bar includes the Ruckus logo, the title "ZoneDirector - ZoneDirector", and a status bar with the date "2016/03/28 14:11:04" and links for "Help", "Toolbox", and "Log Out (ruckus)". Below the navigation bar are tabs for "Dashboard", "Monitor", "Configure", and "Administer". The left sidebar contains a menu with categories like "System", "WLANs", "Access Points", "Access Control", "Maps", "Roles", "Users", "Guest Access", "Hotspot Services", "Hotspot 2.0 Services", "Mesh", "AAA Servers", "DHCP Relay", "Alarm Settings", "Services", "WIPS", and "Certificate". The main content area is titled "System Identity" and contains the following fields and options:

- System Name\***: A text input field containing "ZoneDirector", highlighted with a red box. An "Apply" button is to its right.
- Device IP Settings**: A section with a note: "If ZoneDirector is on a IPv6 network, you can turn on its IPv6 support." Below this is a checkbox for "Enable IPv6 Support".
- IPv4 Configuration**: A section with a note: "If ZoneDirector was assigned static network addressing, click 'Manual' and make the correct entries. If you click 'DHCP', no 'Manual' entries are needed." Below this are radio buttons for "Manual" (selected) and "DHCP".
- IP Address\***: A text input field containing "192.168.40.100".
- Netmask\***: A text input field containing "255.255.255.0".
- Gateway\***: A text input field containing "192.168.40.1".
- Primary DNS Server**: A text input field containing "192.168.40.1".
- Secondary DNS Server**: A text input field containing "8.8.8.8".
- Access VLAN\***: A text input field containing "1".
- An "Apply" button is located at the bottom right of this section.
- Management Interface**: A section with a checkbox for "Enable IPv4 Management Interface".
- IP Address\***: A text input field, currently empty.

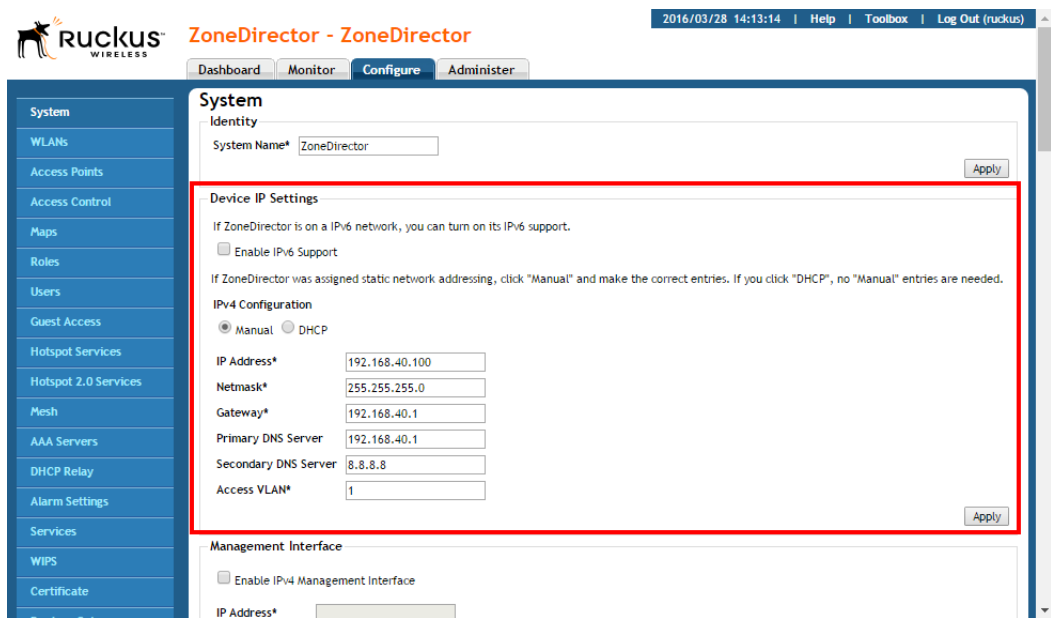
## Changing the Network Addressing

If you need to update the IP address and DNS server settings of ZoneDirector, follow the steps outlined below.

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

- 1 Go to **Configure > System**.
- 2 Review the Device IP Settings options.

Figure 24. 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](#) below 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 ZoneFlex 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**.

Table 12. Default static IPv4 and IPv6 addresses

	<b>AP default IP address</b>	<b>ZoneDirector default IP address</b>
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.

---

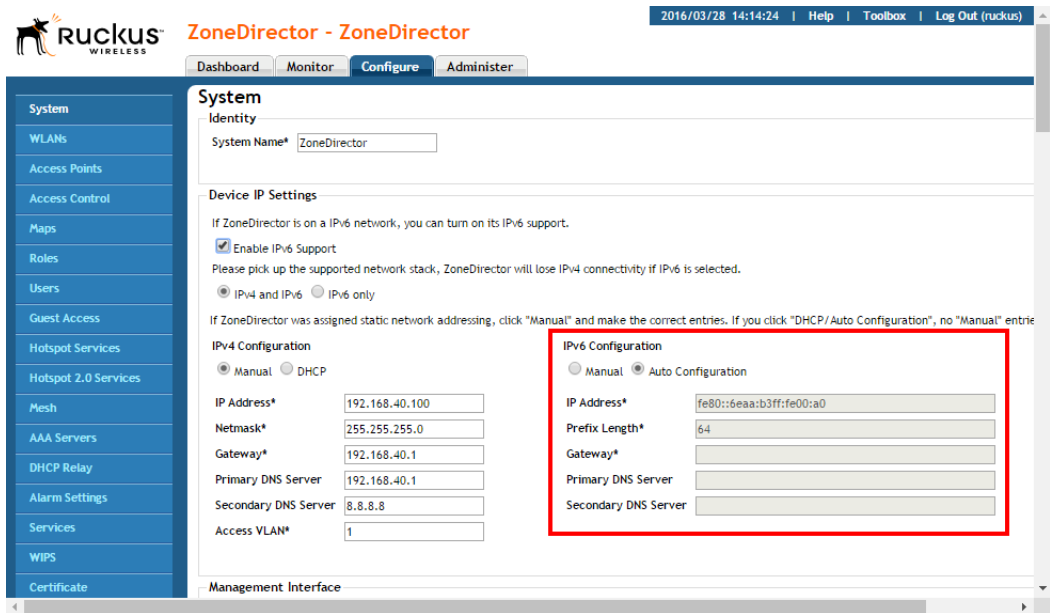
**NOTE:** If you switch from IPv4 to IPv6, you will need to manually change a number of settings that may have previously been configured, such as Access Control Lists (ACLs), AAA server addresses, Syslog server, SNMP trap receiver, etc.

---

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 25](#).

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 25. 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 [Configuring ZoneDirector for Smart Redundancy](#)).

To enable an additional management interface:

- 1 Go to **Configure > System**.
- 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 Click **Apply** to save your settings.

**NOTE:** If the Management Interface is to be shared by two Smart Redundancy ZoneDirectors, repeat these steps for the other ZoneDirector.

Figure 26. Enabling an additional management interface

The screenshot shows the configuration page for enabling an additional management interface. On the left is a navigation menu with items: AAA Servers, DHCP Relay, Alarm Settings, Services, WIPS, Certificate, Bonjour Gateway, and Location Services. The main content area is divided into sections: Primary DNS Server (192.168.40.1), Secondary DNS Server (8.8.8.8), and Access VLAN\* (1). Below this is the Management Interface section, where the checkbox 'Enable IPv4 Management Interface' is checked and highlighted with a red box. Other fields in this section include IP Address\* (192.168.40.101), Netmask\* (255.255.255.0), a checked checkbox for 'Default gateway is connected with this interface', Gateway (192.168.40.1), and Access VLAN\* (1). An 'Apply' button is at the bottom right of this section. The Static Route section contains a table with columns Name, Subnet, Gateway, and Actions, and a 'Create New' button. The Smart Redundancy section has an unchecked checkbox for 'Enable Smart Redundancy', Local Device IP Address (192.168.40.100), Peer Device IP Address\* (a greyed-out field), Shared Secret\* (a greyed-out field), and Management IP Address (Disabled, with a note '(Configured in [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, FlexMaster 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 **Configure > System** 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.

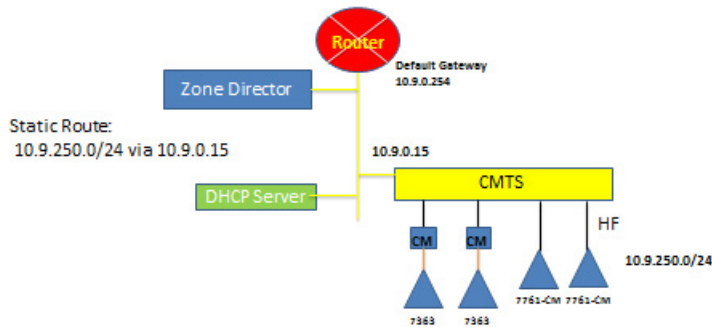
Figure 27. Creating a static route entry

The screenshot shows the ZoneDirector configuration interface. At the top, there is a section for the default gateway with a checked box "Default gateway is connected with this interface", a "Gateway" field containing "192.168.40.1", and an "Access VLAN\*" field containing "1". An "Apply" button is to the right. Below this is the "Static Route" section, which is highlighted with a red border. It contains a table header with columns "Name", "Subnet", "Gateway", and "Actions". Below the header is a "Create New" button. A form for creating a new static route is open, with fields for "Name\*" (containing "Static Route 1"), "Subnet" (containing "1.1.1.0/24"), and "Gateway" (containing "192.168.11.2"). There are "OK" and "Cancel" buttons at the bottom of the form. Below the "Static Route" section is the "Smart Redundancy" section, which has an unchecked "Enable Smart Redundancy" checkbox and fields for "Local Device IP Address" (192.168.40.100), "Peer Device IP Address\*", "Shared Secret\*", and "Management IP Address" (Disabled).

## 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. (See [Figure 28](#)).

Figure 28. 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 ZoneFlex 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. In this situation, 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 **Configure > System**, 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 **Configure > System** page, locate the *Smart Redundancy* section.

Figure 29. Enable Smart Redundancy

Default gateway is connected with this interface  
Access VLAN\* 1 Apply

**Static Route**  
This table lists the specific IPv4 static route.  

Name	Subnet	Gateway	Actions
------	--------	---------	---------

  
[Create New](#) [Delete](#)

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

Enable Smart Redundancy

Local Device IP Address 192.168.40.100  
Peer Device IP Address\* 192.168.40.102  
Shared Secret\* secret  
Management IP Address Disabled (configured in [management interface]) Apply

**DHCP Server**  
If a DHCP server does not exist on your network, you can enable this function to provide DHCP service to clients.

Enable DHCP server

Starting IP\* 192.168.0.3  
Number of IPs\* 200  
Lease Time One week  
 DHCP Option 43 (Layer 3 discovery protocol for AP to find ZoneDirector) Apply

- 5 Enable the check box next to **Enable Smart Redundancy**.
- 6 Enter the IP address of the backup unit under **Peer Device IP Address**.

---

**NOTE:** If you have configured Limited ZD Discovery under Configure > 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.

---

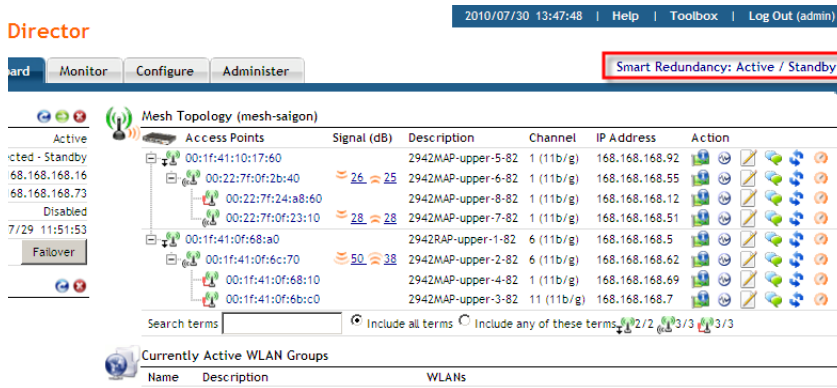
- 7 Enter a **Shared Secret** for two-way communication between the two ZoneDirectors (up to 15 alphanumeric characters).
- 8 Click **Apply** to save your changes and prompt ZoneDirector to immediately attempt to discover its peer on the network.
- 9 If discovery is successful, the details of the peer 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 **Configure > System**, 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.

Once Smart Redundancy has been enabled, a status link is displayed at the top of the web interface.

Figure 30. Smart Redundancy status link



---

**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](#) 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 Wireless 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 **Configure > Access Points > Limited ZD**

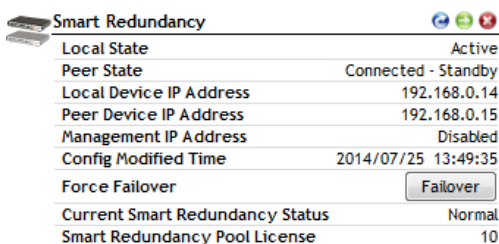
Discovery page. Specify one ZoneDirector as Primary, the other as Secondary. Alternatively you can specify the IP addresses of both ZoneDirectors through DHCP Option 43 (see [Option 2: Customize Your DHCP Server](#)).

---

## Forcing Failover to the Backup ZoneDirector

After Smart Redundancy has been enabled, you can view the status of both the primary and backup units from the Dashboard by dragging the Smart Redundancy widget onto the workspace.

Figure 31. The Smart Redundancy widget



The screenshot shows a 'Smart Redundancy' widget with a title bar containing a close button and two status icons (green and red). The widget displays the following information:

Local State	Active
Peer State	Connected - Standby
Local Device IP Address	192.168.0.14
Peer Device IP Address	192.168.0.15
Management IP Address	Disabled
Config Modified Time	2014/07/25 13:49:35
Force Failover	<input type="button" value="Failover"/>
Current Smart Redundancy Status	Normal
Smart Redundancy Pool License	10

The **Failover** button can be used to force a role reversal making the standby ZoneDirector the active unit. This widget also displays the state (active, standby or disconnected) of both devices, as well as their IP addresses and the Management IP address, if configured.

## 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 32. Smart Redundancy status degraded (peer is disconnected, license pool remains valid for 60 days)

Smart Redundancy	
Local State	Active
Peer State	Disconnected
Local Device IP Address	192.168.0.14
Peer Device IP Address	192.168.0.15
Management IP Address	Disabled
Config Modified Time	2014/07/25 13:49:35
Force Failover	Failover
Current Smart Redundancy Status (Peer ZD disconnected)	Degraded
Smart Redundancy Pool License	10
Smart Redundancy Pool is valid for	60 days

Figure 33. After 60 day grace period expires, license pool is revoked and AP license count reverts to active device license level only

Smart Redundancy	
Local State	Active
Peer State	Disconnected
Local Device IP Address	192.168.0.14
Peer Device IP Address	192.168.0.15
Management IP Address	Disabled
Config Modified Time	2014/07/25 13:49:35
Force Failover	Failover
Current Smart Redundancy Status	Invalid
Smart Redundancy Pool License	0

Figure 34. 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

Smart Redundancy	
Local State	Active
Peer State	Disabled
Local Device IP Address	192.168.0.14
Peer Device IP Address	192.168.0.15
Management IP Address	Disabled
Config Modified Time	2014/07/25 15:44:51
Force Failover	Failover
Current Smart Redundancy Status (New SR has lower license)	Degraded
Smart Redundancy Pool License	15
Smart Redundancy Pool is valid for	60 days

Table 13. Max AP Licenses by ZoneDirector Model

Model	Max AP Licenses
ZoneDirector 1200	75
ZoneDirector 3000	500
ZoneDirector 5000	1,000

## 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

---

**NOTE:** Ruckus Wireless 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 DHCP server, Ruckus Wireless also recommends enabling the rogue DHCP server detector. For more information, refer to [Rogue DHCP Server Detection](#).

---

- 1 Click the **Configure** tab. The *System* page appears.
- 2 Under the **DHCP Server** section, select the **Enable DHCP** check box.
- 3 In **Starting IP Address**, 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**.

**NOTE:** 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 35. The DHCP Server options

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

Enable Smart Redundancy

Local Device IP Address 192.168.40.100

Peer Device IP Address\* 192.168.40.102

Shared Secret\* secret

Management IP Address Disabled (configured in [Management Interface])

---

**DHCP Server**

If a DHCP server does not exist on your network, you can enable this function to provide DHCP service to clients.

Enable DHCP server

Starting IP\* 192.168.0.3

Number of IPs\* 200

Lease Time One week ▾

DHCP Option 43 (Layer 3 discovery protocol for AP to find ZoneDirector)

To view all IP addresses that have been assigned by the DHCP server, [click here](#)

---

**Management Access Control**

This table lists the specific IP addresses which are allowed access to the ZoneDirector. Click [Create New](#) to add another IP address, or click [Edit](#) to make changes to an existing entry.

<input type="checkbox"/>	Name	IP address	Actions
<a href="#">Create New</a>			<input type="button" value="Delete"/>

---

**System Time**

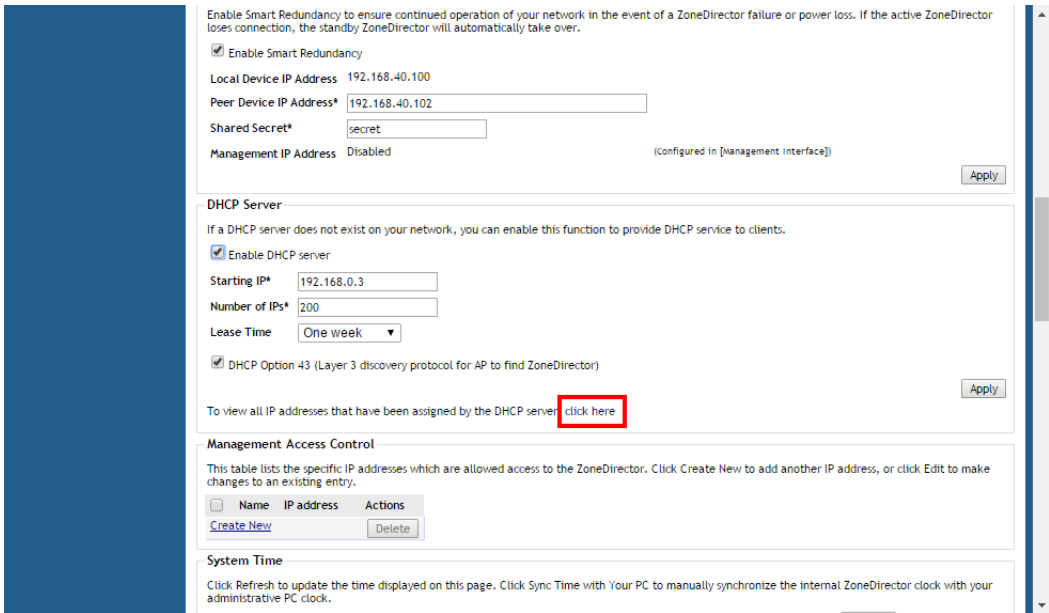
Click [Refresh](#) to update the time displayed on this page. Click [Sync Time with Your PC](#) to manually synchronize the internal ZoneDirector clock with your administrative PC clock.

## 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, assigned IP address, and the remaining lease time.

You can clear DHCP leases on ZoneDirector by disabling and re-enabling the DHCP service.

Figure 36. 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 *Configure > System* screen. Options include limiting access by subnet, single IP address and IP address range.

**NOTE:** 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 **Configure > System**.
- 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--be sure not to create an ACL that prevents 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 37. Management Access Control

If a DHCP server does not exist on your network, you can enable this function to provide DHCP service to clients.

Enable DHCP server

Starting IP\*

Number of IPs\*

Lease Time

DHCP Option 43 (Layer 3 discovery protocol for AP to find ZoneDirector)

To view all IP addresses that have been assigned by the DHCP server, [click here](#)

**Management Access Control**

This table lists the specific IP addresses which are allowed access to the ZoneDirector. Click **Create New** to add another IP address, or click **Edit** to make changes to an existing entry.

<input type="checkbox"/>	Name	IP address	Actions
<input type="button" value="Create New"/>			<input type="button" value="Delete"/>

**System Time**

Click **Refresh** to update the time displayed on this page. Click **Sync Time with Your PC** to manually synchronize the internal ZoneDirector clock with your administrative PC clock.

Current ZoneDirector system time is (GMT +8:00) 3/29/2016 5:35:13. Your browser's current time is 3/28/2016, 2:35:13 PM

Use NTP to synchronize the ZoneDirector clock automatically

NTP Server\*

Select time zone for your location:

**Country Code**

Different countries have different regulations on the usage of radio channels. To ensure that ZoneDirector is using an authorized radio channel, select the correct country code for your location.

Country Code:

On the E-90 GHz band, certain channels won't be utilized if "Options for Compatibility" or "Options for Interoperability" is selected. Otherwise, all

Figure 38. Creating a new ZoneDirector management ACL

DHCP Option 43 (Layer 3 discovery protocol for AP to find ZoneDirector) Apply

To view all IP addresses that have been assigned by the DHCP server, [click here](#)

**Management Access Control**

This table lists the specific IP addresses which are allowed access to the ZoneDirector. Click Create New to add another IP address, or click Edit to make changes to an existing entry.

<input type="checkbox"/>	Name	IP Address	Actions
<div style="border: 1px solid #ccc; padding: 5px;"> <p><b>Create New</b></p> <p>Name* <input type="text" value="Mgmt ACL 1"/></p> <p>Restriction <input checked="" type="radio"/> Single <input type="radio"/> Range <input type="radio"/> Subnet</p> <p>IP Address <input type="text" value="192.168.11.5"/></p> <p>Current Administrator's IP address: 192.168.11.5</p> <p style="text-align: right;"><input type="button" value="OK"/> <input type="button" value="Cancel"/></p> </div>			
<a href="#">Create New</a>		<input type="button" value="Delete"/>	

**System Time**

Click Refresh to update the time displayed on this page. Click Sync Time with Your PC to manually synchronize the internal ZoneDirector clock with your administrative PC clock.

Your current system time is Mon May 23 2011 15:57:03 GMT+0800 (Taipei Standard Time)

Use NTP to synchronize the ZoneDirector clock automatically.

## Setting the System Time

The internal clock in ZoneDirector is automatically synchronized with the clock on your administration PC during the initial setup. 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 **Configure > System**.
- 2 In the *System Time* features you have the following options:
  - *Refresh*: Click this to update the ZoneDirector display (a static snapshot) from the internal clock.
  - *Synch Time with your PC Now*: If needed, click this to update the internal clock with the current time settings from your administration PC.



- *Use NTP... (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.
- *Select time zone for your location*: Choose your time zone from the drop-down menu. Setting the proper time zone ensures that timestamps on log files are in the proper time zone.

3 Click **Apply** to save the results of any resynchronization or NTP links.

Figure 39. The System Time options

To view all IP addresses that have been assigned by the DHCP server, [click here](#)

**Management Access Control**

This table lists the specific IP addresses which are allowed access to the ZoneDirector. Click Create New to add another IP address, or click Edit to make changes to an existing entry.

<input type="checkbox"/>	Name	IP address	Actions
<a href="#">Create New</a>			<a href="#">Delete</a>

**System Time**

Click Refresh to update the time displayed on this page. Click Sync Time with Your PC to manually synchronize the internal ZoneDirector clock with your administrative PC clock.

Current ZoneDirector system time is (GMT +8:00) 3/29/2016 5:35:13. Your browser's current time is 3/28/2016, 2:35:13 PM [Refresh](#)

Use NTP to synchronize the ZoneDirector clock automatically

NTP Server\*

Select time zone for your location:

[Sync Time with Your PC](#) [Apply](#)

**Country Code**

Different countries have different regulations on the usage of radio channels. To ensure that ZoneDirector is using an authorized radio channel, select the correct country code for your location.

Country Code:

On the 5.0 GHz band, certain channels won't be utilized if "Optimize for Compatibility" or "Optimize for Interoperability" is selected, otherwise, all available channels will be utilized.

Channel Optimization  Optimize for Compatibility  Optimize for Interoperability  Optimize for Performance

Channel Mode  Allow indoor channels (allows ZoneFlex Outdoor APs to use channels regulated as indoor use-only)

[Apply](#)

**Log Settings**

Event Log Level  Show More  Warning and Critical Events  Critical Events Only

Remote Syslog  Enable reporting to remote syslog server at  (IP Address)

## 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 ZoneFlex 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 **Configure > System**.

- 2 Locate the *Country Code* section, and choose your location from the pull-down menu.
- 3 Click **Apply** to save your settings.

Figure 40. The Country Code settings

**System Time**  
 Click Refresh to update the time displayed on this page. Click Sync Time with Your PC to manually synchronize the internal ZoneDirector clock with your administrative PC clock.  
 Current ZoneDirector system time is (GMT +8:00) 3/29/2016 5:35:13. Your browser's current time is 3/28/2016, 2:35:13 PM   
 Use NTP to synchronize the ZoneDirector clock automatically  
 NTP Server\*   
 Select time zone for your location: (GMT +8:00) Beijing, Perth, Singapore, Hong Kong

**Country Code**  
 Different countries have different regulations on the usage of radio channels. To ensure that ZoneDirector is using an authorized radio channel, select the correct country code for your location.  
 Country Code:   
 On the 5.0 GHz band, certain channels won't be utilized if "Optimize for Compatibility" or "Optimize for Interoperability" is selected, otherwise, all available channels will be utilized.  
 Channel Optimization  Optimize for Compatibility  Optimize for Interoperability  Optimize for Performance  
 Channel Mode  Allow indoor channels (allows ZoneFlex Outdoor APs to use channels regulated as indoor use-only)

**Log Settings**  
 Event Log Level  Show More  Warning and Critical Events  Critical Events Only  
 Remote Syslog  Enable reporting to remote syslog server at:  (IP Address)

**Email Server**  
 Enable Email Server  
 From Email Address   
 SMTP Server Name

## Channel Optimization

If your Country Code is set to “United States,” an additional configuration option, Channel Optimization, is shown. This feature allows you to choose whether additional DFS (Dynamic Frequency Selection) channels in the 5 GHz band should be available for use by your APs.

Note that these settings only affect Ruckus Wireless APs that support the extended DFS channel list. Channel Optimization settings are described in the following table.

Table 14. Channel Optimization settings for US Country Code

Setting	Description	Use this setting when
Optimize for Compatibility	DFS-capable ZoneFlex APs are limited to the same channels as all other APs (non-DFS channels only).	You have a mixture of APs that support DFS channels and other Ruckus APs that do not support DFS channels in a Smart Mesh configuration.
Optimize for Interoperability	ZoneFlex 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	ZoneFlex APs can use all available DFS and non-DFS channels, without regard for compatibility or interoperability.	You have only DFS-capable APs in your network, you are not concerned with DFS compatibility of client devices, and you want to make the maximum use of all possible available channels.

**NOTE:** If you are located in the United States and have a DFS-capable ZoneFlex 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 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 RAP choosing a channel that is not available to the MAP. 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.

## Channel Mode

Some countries restrict certain 5 GHz channels to indoor use only. For instance, Germany restricts channels in the 5.15 GHz to 5.25 GHz band to indoor use. When ZoneFlex Outdoor APs and Bridges with 5 GHz radios (ZoneFlex 7731, 7782, P300, T300 series and T710 series) are set to a country code where these restrictions apply, the AP or Bridge can no longer be set to an indoor-only channel and will no longer select from amongst a channel set that includes these indoor-only channels when SmartSelect or Auto Channel selection is used, unless the administrator configures the AP to allow use of these channels.

For instance, if the AP is installed in a challenging indoor environment such as a warehouse, the administrator may want to allow the AP to use an indoor-only channel. These channels can be enabled for use through the AP CLI or ZoneDirector web interface by configuring *Configure > System > Country Code > Channel Mode* and checking **Allow indoor channels (allows ZoneFlex Outdoor APs to use channels regulated as indoor use only)**. If you have a dual-band ZoneFlex Indoor AP functioning as a RAP with dual-band ZoneFlex Outdoor APs functioning as MAPs, the mesh backhaul link must initially use a non-indoor-only channel. Your ZoneFlex Outdoor MAPs may fail to join if the mesh backhaul link is using a restricted indoor-only channel.

## Changing the 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—as detailed in this topic.

## Reviewing the Current Log Contents

- 1 Go to **Monitor > All Events/Activities**.
- 2 Review the events and alarms listed below.

---

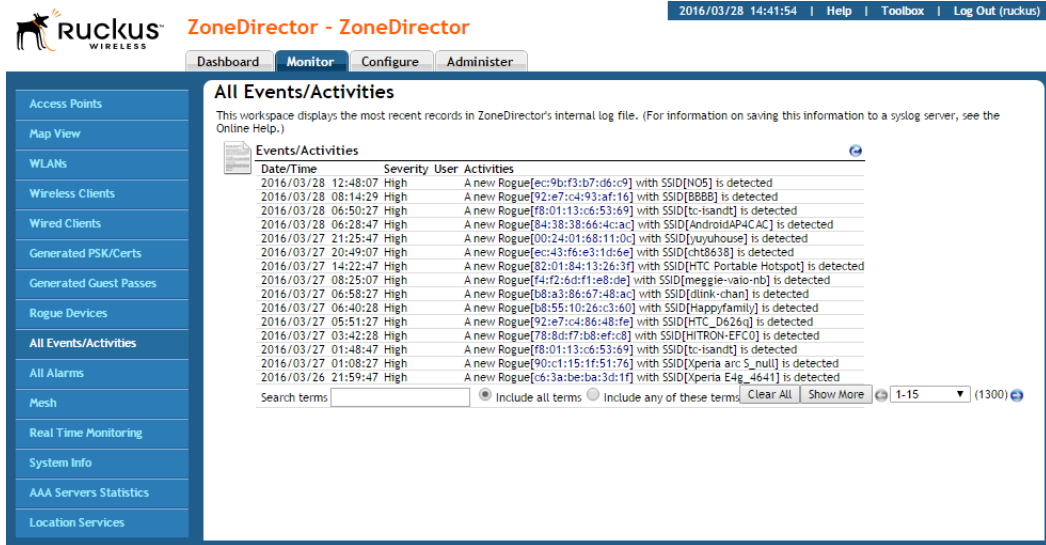
**NOTE:** Log entries are listed in reverse chronological order (with the latest logs at the top of the list).

---

- 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 41. The All Events/Activities page



## Customizing the Current Log Settings

You can review and customize the log settings by following these steps:

- 1 Go to **Configure > System**.
- 2 Scroll down to *Log Settings*.
- 3 Make your selections from these syslog server options:
  - *Event Log Level*: Select one of the three logging levels: “Show More,” “Warning and Critical Events,” or “Critical Events Only.”
  - *Remote Syslog*: To enable syslog logging, select the “Enable reporting to remote syslog server at” check box, and then type the IP address in the box provided.
  - *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 it to the firewall for access restriction based on client association information.

- 4 Click **Apply** to save your settings. The changes go into effect immediately.

Figure 42. The Log Settings options

Different countries have different regulations on the usage of radio channels. To ensure that ZoneDirector is using an authorized radio channel, select the correct country code for your location.

Country Code:

On the 5.0 GHz band, certain channels won't be utilized if "Optimize for Compatibility" or "Optimize for Interoperability" is selected, otherwise, all available channels will be utilized.

Channel Optimization  Optimize for Compatibility  Optimize for Interoperability  Optimize for Performance

Channel Mode  Allow indoor channels (allows ZoneFlex Outdoor APs to use channels regulated as indoor use-only)

**Log Settings**

Event Log Level  Show More  Warning and Critical Events  Critical Events Only

Remote Syslog  Enable reporting to remote syslog server at  (IP Address)

Remote Syslog Advanced Settings

**Email Server**

Enable Email Server

From Email Address

SMTP Server Name

SMTP Server Port

SMTP Authentication Username

SMTP Authentication Password

Confirm SMTP Authentication Password

SMTP Encryption Options

**SMS settings**

Enable SMS Server

twilio account information

## Configuring Syslogs for Firewall Integration

Starting with release 9.8, ZoneDirector will generate syslog messages upon acquisition, update or deletion of an IP address by a wireless station. This feature allows enhanced integration with popular firewalls from vendors including Barracuda and Palo Alto Networks for implementing client-specific security rules.

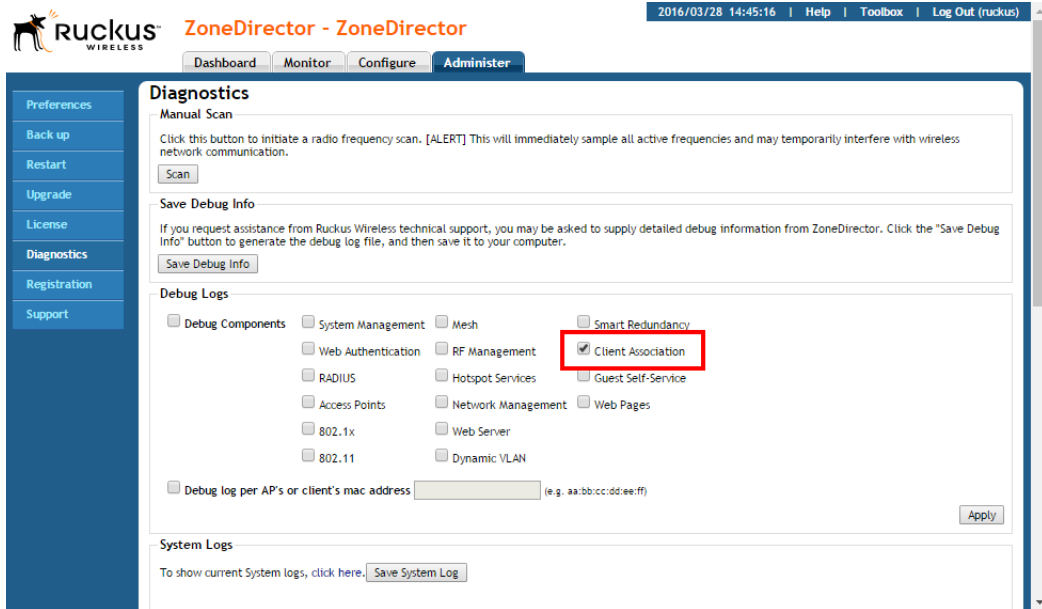
Station information is conveyed through a syslog message containing the following information: IPv4/v6 address, User name, MAC address, Operation Type (Add, Update, Del), AP/ZD MAC, OS Type.

To enable inclusion of client association logs in syslog messages:

- 1 Go to **Administer > Diagnostics**.
- 2 In **Debug Logs**, select the **Client Association** check box.
- 3 Click **Apply** to save your changes.

- 4 You must also ensure that syslog delivery is enabled on the **Configure > System** page and that the **Priority** level in **Remote Syslog Advanced Settings** is set to **Info** or **All**.

Figure 43. Enable client association logs in syslog for firewall integration



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 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_o-  
riip=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
```



## 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 **Configure > System**.
- 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 44. Remote Syslog Advanced Settings

On the 5.0 GHz band, certain channels won't be utilized if "Optimize for Compatibility" or "Optimize for Interoperability" is selected, otherwise, all available channels will be utilized.

Channel Optimization  Optimize for Compatibility  Optimize for Interoperability  Optimize for Performance

Channel Mode  Allow indoor channels (allows ZoneFlex Outdoor APs to use channels regulated as indoor use-only)

Apply

Log Settings

Event Log Level  Show More  Warning and Critical Events  Critical Events Only

Remote Syslog  Enable reporting to remote syslog server at: \_\_\_\_\_ (IP Address)

Remote Syslog Advanced Settings

ZoneDirector Settings

Facility Name:  Priority Level:

Managed AP Settings

Facility Name:  Priority Level:

Apply

Email Server

Enable Email Server

From Email Address: \_\_\_\_\_

SMTP Server Name: \_\_\_\_\_

SMTP Server Port:

SMTP Authentication Username: \_\_\_\_\_

SMTP Authentication Password: \_\_\_\_\_

Confirm SMTP Authentication Password: \_\_\_\_\_

SMTP Encryption Options

Test Apply

## 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 **Configure > 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 **Configure > System**, and scroll down to the *Email Server* section.
- 5 Configure the settings listed in [Table 15](#).

Table 15. SMTP settings for email notification

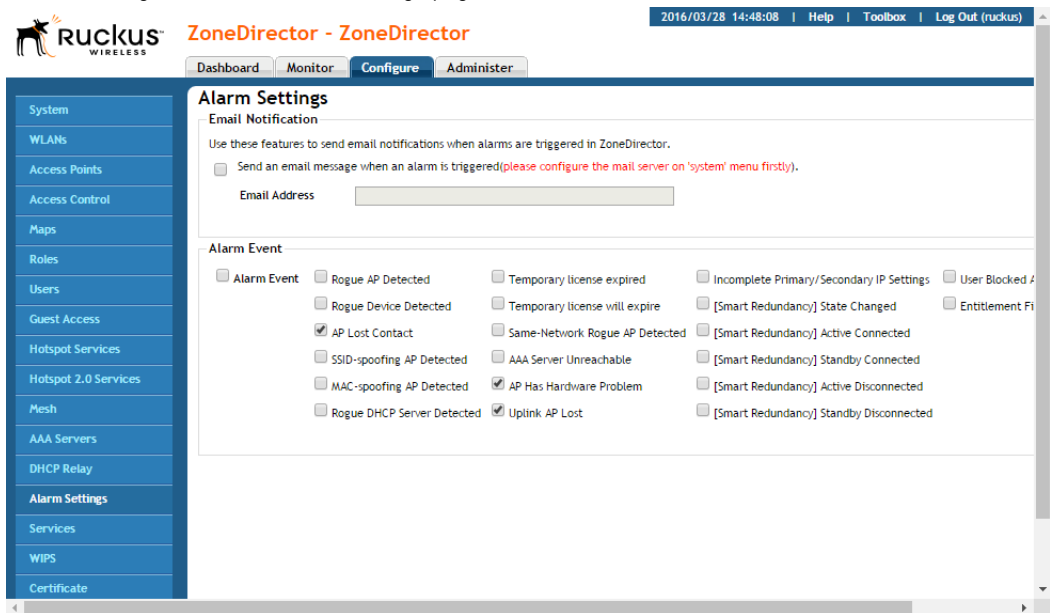
SMTP Setting	Description
From email address	Type the email address from which ZoneDirector will send alarm messages.
SMTP Server Name	Type the full name of the server provided by your ISP or mail administrator. Often, the SMTP server name is in the format <b>smtp . company . com .</b> . For Hotmail addresses, the SMTP server name is <i>smtp.live.com</i> .
SMTP Server Port	Type the SMTP port number provided by your ISP or mail administrator. Often, the SMTP port number is <b>25</b> or <b>587</b> . The default SMTP port value is <b>587</b> .
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 <b>SMTP Encryption Options</b> link, and then select the <b>TLS</b> check box. Additionally, select the <b>STARTTLS</b> check box that appears after you select the <b>TLS</b> 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.

## Setting Up Email Alarm Notifications

Customizing the Current Log Settings

- 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 45. 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 that ZoneDirector Sends

Using the Alarm Event section of the *Configure > Alarm Settings* page, you can choose which types of events will trigger ZoneDirector to send an email notification.

- 1 Click **Alarm Event** 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 *Email Notification* 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 **Monitor > 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 Guest Pass Delivery via SMS

If you want to deliver Guest Passes to your guests via SMS, you can configure ZoneDirector to use an existing Twilio or Clickatell account for SMS delivery. The first step is to inform ZoneDirector of your Twilio or Clickatell account information.

- 1 Go to **Configure > System**.
- 2 Locate the **SMS Settings** section, and select either **Twilio account information** or **Clickatell account information**.
- 3 Enter your **Account SID**, **Auth Token** and **From Phone Number** (Twilio) or your **User Name**, **Password** and **API ID** (Clickatell).
- 4 Click the **Test** button to test your settings.
- 5 Once confirmed, click **Apply** to save your changes.

## Enabling Login Warning Messages

Customizing Email Alarms that ZoneDirector Sends

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 46. Configuring SMS Settings

The screenshot displays the configuration interface for SMS settings and login warnings. At the top, there are fields for SMTP Authentication Username, Password, and Confirmation, along with a link to SMTP Encryption Options. Below this is the 'SMS settings' section, which is highlighted with a red border. It includes a checked 'Enable SMS Server' option and two radio buttons for account providers: 'twilio account information' (selected) and 'clickatell account information'. Each provider has fields for Account SID, Auth Token, From Phone Number, User Name, Password, and API Id. Below the SMS settings is the 'login Warning' section, which has an unchecked 'Enable login Warning' option and a text box for 'Customize Warning Content' containing a default warning message.

## 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 **Configure > System**, 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 47. Enabling and configuring a login warning message

The screenshot displays the configuration page for enabling login warning messages. It is divided into two main sections: account information and warning configuration.

**twilio account information**

- Account SID:  [register a new twilio account]
- Auth Token:
- From PhoneNumber:

**clickatell account information**

- User Name:  [register a new clickatell account]
- Password:
- API Id:
- From PhoneNumber:

Buttons:

**login Warning**

Enable login warning to pop up a warning after a user logs into the ZD management GUI and SSH.

Enable login Warning

Customize Warning Content:

Warning, you are logging into device for authorized user only. If you are not an authorized user, please click Quit; otherwise click Continue to login.

Buttons:

Network Management

# Enabling Network Management Systems

ZoneDirector supports several external network management systems including Ruckus Wireless SmartCell Insight, FlexMaster server, SNMPv2, SNMPv3 and Telnet server. These options are configured from the Configure > System 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.

---

**NOTE:** 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 only available as of SCI version 2.0 and later.

---

To configure SCI Management:

- 1 Go to **Configure > System**, 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])
  - **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 48. Config SCl server

The screenshot shows the configuration page for ZoneDirector. The 'SmartCell Insight Management' section is highlighted with a red border. It includes a checkbox for 'Enable management by SmartCell Insight' which is checked. Below this are input fields for 'URL\*', 'User Name\*', 'Password\*', and 'System ID\*'. There are 'Apply' buttons at the end of each section. Other sections visible include 'FlexMaster Management' with a URL of 'https://192.168.0.44/intune/server' and an interval of 15 minutes, 'Performance Monitoring' with an interval of 5 minutes, and 'Northbound Portal Interface'.

## Enabling Management via FlexMaster

If you have a Ruckus Wireless FlexMaster server installed on the network, you can enable FlexMaster management to centralize monitoring and administration of ZoneDirector and other supported Ruckus Wireless devices. This version of ZoneDirector supports the following FlexMaster-deployed tasks:

- Firmware upgrade for both ZoneDirector and the APs that report to them
- Reboot
- Backup of ZoneDirector settings
- Performance monitoring

When the FlexMaster management option is enabled, you will still be able to access the ZoneDirector web interface to perform other management tasks. By default, FlexMaster management is disabled.

To enable FlexMaster management:

- 1 Click **Configure > System**.
- 2 Scroll down to the bottom of the page.

- 3 If you see **+ Network Management** (section is collapsed) at the bottom of the page, click the **Network Management** link to expand the section.
- 4 Under *FlexMaster Management*, select the **Enable management by FlexMaster** check box.
- 5 In **URL**, type the **FlexMaster DNS** host name or IP address of the FlexMaster server.
- 6 In **Interval**, type the time interval (in minutes) at which ZoneDirector will send status updates to the FlexMaster server. The default interval is 15 minutes.
- 7 Click **Apply**. The message *Setting Applied* appears.

You have completed enabling FlexMaster management on ZoneDirector. For more information on how to configure ZoneDirector from the FlexMaster web interface, refer to the FlexMaster documentation.

Figure 49. The FlexMaster Management options

The screenshot shows the 'Network Management' section of the ZoneDirector web interface. The 'FlexMaster Management' section is highlighted with a red box. It contains the following fields and options:

- SmartCell Insight Management:** A checkbox for 'Enable management by SmartCell Insight' is unchecked. Below it are input fields for 'URL\*', 'User Name\*', 'Password\*', and 'System ID\*'. An 'Apply' button is located to the right.
- FlexMaster Management:** A checkbox for 'Enable management by FlexMaster' is checked. The 'URL' field contains 'https://192.168.0.44/intune/server'. The 'Interval' field is set to '15' minutes. An 'Apply' button is located to the right.
- Performance Monitoring:** A checkbox for 'Enable performance monitoring' is unchecked. The 'Interval' field is set to '5' minutes. An 'Apply' button is located to the right.
- Northbound Portal Interface:** A checkbox for 'Enable northbound portal interface support' is unchecked.

## Monitoring ZoneDirector Performance from FlexMaster

If you want to monitor ZoneDirector's performance statistics from FlexMaster, select **Enable Performance Monitoring**, enter an update interval, and click **Apply**. This option is disabled by default.

## 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 **Configure > System > 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 50. Enabling Northbound Portal interface

The screenshot shows a configuration page with several sections:

- System ID\***: A text input field.
- FlexMaster Management**: Includes a checkbox for 'Enable management by FlexMaster', a URL field (https://192.168.0.44/intune/server), and an interval field (15 minutes).
- Performance Monitoring**: Includes a checkbox for 'Enable performance monitoring' and an interval field (5 minutes).
- Northbound Portal Interface**: This section is highlighted with a red box. It contains a checked checkbox for 'Enable northbound portal interface support' and a password field with masked characters (\*\*\*\*\*).
- SNMPv2 Agent**: Includes a checkbox for 'Enable SNMP Agent', a 'System Contact\*' field (https://support.ruckuswireless.com/contact), a 'System Location\*' field (350 West Java Dr. Sunnyvale, CA 94089 L), and fields for 'SNMP RO community\*' (public) and 'SNMP RW community\*' (private).

## 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.

---

**NOTE:** For a list of the MIB variables that you can get and set using SNMP, check the related SNMP documentation on the Ruckus Wireless Support Web site at <http://support.ruckuswireless.com/documents>.

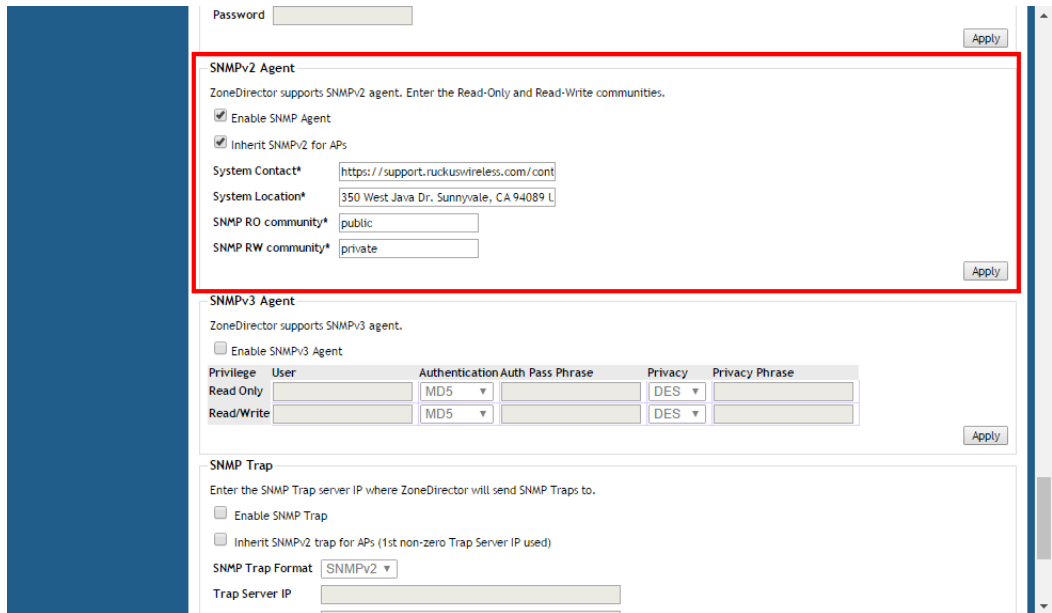
---

### ***If your network uses SNMPv2***

To enable SNMPv2 management:

- 1 Go to **Configure > System**. 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 51. Enabling the SNMPv2 agent



***If your network uses SNMPv3***

To enable SNMPv3 management:

- 1 Go to **Configure > System**. 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 output.
    - **SHA:** Secure Hash Algorithm, message hash function with 160-bit output.
  - **Auth Pass Phrase:** Enter a passphrase between 8 and 32 characters in length.
  - **Privacy:** Choose DES, AES or None.
    - **DES:** Data Encryption Standard, data block cipher.

- **AES**: Advanced Encryption Standard, data block cipher.
- **None**: No Privacy passphrase is required.
- **Privacy Phrase**: If either DES or AES is selected, enter a Privacy phrase between 8 and 32 characters in length.

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

Figure 52. Enabling the SNMPv3 agent

The screenshot shows the configuration page for enabling the SNMPv3 agent. The page is divided into several sections:

- Password**: A text input field with an **Apply** button.
- SNMPv2 Agent**: A section with the text "ZoneDirector supports SNMPv2 agent. Enter the Read-Only and Read-Write communities." It includes checkboxes for "Enable SNMP Agent" and "Inherit SNMPv2 for APs". Below are text input fields for "System Contact\*" (https://support.ruckuswireless.com/cont), "System Location\*" (350 West Java Dr. Sunnyvale, CA 94089 L), "SNMP RO community\*" (public), and "SNMP RW community\*" (private). An **Apply** button is at the bottom right.
- SNMPv3 Agent**: This section is highlighted with a red box. It starts with "ZoneDirector supports SNMPv3 agent." and a checked "Enable SNMPv3 Agent" checkbox. Below is a table for configuring users:

Privilege	User	Authentication	Auth Pass Phrase	Privacy	Privacy Phrase
Read Only	<input type="text"/>	MD5	<input type="text"/>	DES	<input type="text"/>
Read/Write	<input type="text"/>	MD5	<input type="text"/>	DES	<input type="text"/>

An **Apply** button is located at the bottom right of this section.

- SNMP Trap**: A section with the text "Enter the SNMP Trap server IP where ZoneDirector will send SNMP Traps to." It includes checkboxes for "Enable SNMP Trap" and "Inherit SNMPv2 trap for APs (1st non-zero Trap Server IP used)". Below are a dropdown for "SNMP Trap Format" (SNMPv2) and a text input for "Trap Server IP".

## 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 (see [Trap Notifications That ZoneDirector Sends](#)).

To enable SNMP trap notifications

- 1 In the Network Management section of the System 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 53. Enabling SNMPv2 trap notifications

The screenshot displays the configuration interface for ZoneDirector, divided into three main sections: SNMPv3 Agent, SNMP Trap, and Telnet Server. The SNMP Trap section is highlighted with a red border.

**SNMPv3 Agent**  
ZoneDirector supports SNMPv3 agent.  
 Enable SNMPv3 Agent

Privilege	User	Authentication	Auth Pass Phrase	Privacy	Privacy Phrase
Read Only	<input type="text"/>	MD5	<input type="text"/>	DES	<input type="text"/>
Read/Write	<input type="text"/>	MD5	<input type="text"/>	DES	<input type="text"/>

**SNMP Trap**  
Enter the SNMP Trap server IP where ZoneDirector will send SNMP Traps to.  
 Enable SNMP Trap  
 Inherit SNMPv2 trap for APs (1st non-zero Trap Server IP used)

SNMP Trap Format:

Trap Server IP:

Trap Server 2 IP:

Trap Server 3 IP:

Trap Server 4 IP:

**Telnet Server**  
ZoneDirector supports Telnet Server.  
 Enable Telnet Server



Figure 54. Enabling SNMP trap notifications with SNMPv3

**SNMPv3 Agent**  
ZoneDirector supports SNMPv3 agent.

Enable SNMPv3 Agent

Privilege	User	Authentication	Auth Pass Phrase	Privacy	Privacy Phrase
Read Only	readonly	MD5	readonly	DES	privacy
Read/Write	admin	MD5	adminadmin	DES	privacy

**SNMP Trap**  
Enter the SNMP Trap server IP where ZoneDirector will send SNMP Traps to.

Enable SNMP Trap

SNMP Trap Format: **SNMPv3**

Enable	User	Trap Server IP	Authentication	Auth Pass Phrase	Privacy	Privacy Phrase
<input checked="" type="checkbox"/>	admin	172.17.16.139	MD5	authpass	DES	privacypass
<input type="checkbox"/>			MD5		DES	
<input type="checkbox"/>			MD5		DES	
<input type="checkbox"/>			MD5		DES	

**Telnet Server**  
ZoneDirector supports Telnet Server.

Enable Telnet Server

### Trap Notifications That ZoneDirector Sends

There are several events for which ZoneDirector will send trap notifications to the SNMP server that you specified. [Table 16](#) lists the trap notifications that ZoneDirector sends and when they are sent.

Table 16. 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.

Table 16. Trap notifications

Trap Name	Description
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.

Table 16. Trap notifications

Trap Name	Description
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.
ruckusZDEventSmartRedundancyChangeToActive	The standby Smart Redundancy ZoneDirector has failed to detect its active peer, system changed to active state.
ruckusZDEventSmartRedundancyActiveConnected	The active Smart Redundancy ZoneDirector has detected its peer and is in active/connected state.
ruckusZDEventSmartRedundancyActiveDisconnected	The active Smart Redundancy ZoneDirector has not detected its peer and is in active/disconnected state.
ruckusZDEventSmartRedundancyStandbyConnected	The standby ZoneDirector has detected its peer and is in standby/connected state.
ruckusZDEventSmartRedundancyStandbyDisconnected	The standby ZoneDirector has not detected its peer and is in standby/disconnected state.

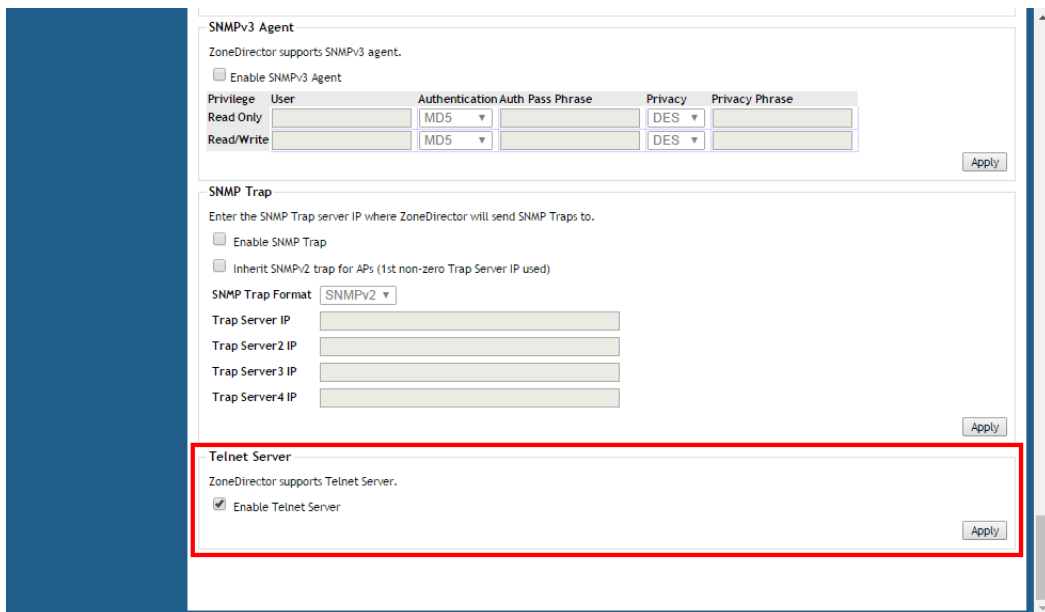
## Enabling Telnet

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 **Configure > System**.
- 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 55. Enabling Telnet server



The screenshot displays the configuration page for the ZoneDirector system, specifically the Network Management section. It is divided into three main sections: SNMPv3 Agent, SNMP Trap, and Telnet Server. The Telnet Server section is highlighted with a red rectangular box. In this section, the text "ZoneDirector supports Telnet Server." is followed by a checked checkbox labeled "Enable Telnet Server" and an "Apply" button. The SNMPv3 Agent section includes a table for configuring user privileges and authentication. The SNMP Trap section includes fields for enabling traps and specifying trap server IP addresses.

Privilege	User	Authentication	Auth Pass Phrase	Privacy	Privacy Phrase
Read Only		MD5		DES	
Read/Write		MD5		DES	

## Configuring 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:

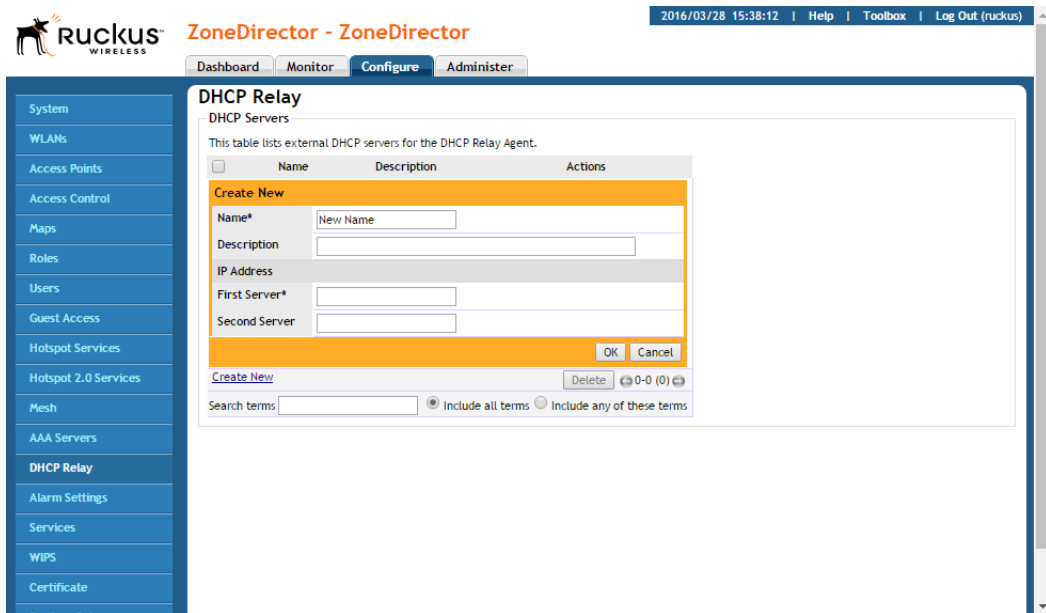
- 1 Client sends DHCP discover broadcast.
- 2 AP tunnels this DHCP discover frame to ZoneDirector.
- 3 DHCP Relay Agent sends unicast DHCP discover packet to DHCP server.
- 4 DHCP server sends DHCP offer to Relay Agent on ZoneDirector.
- 5 ZoneDirector sends DHCP Offer back to the AP.
- 6 AP sends this 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 **Configure > 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.

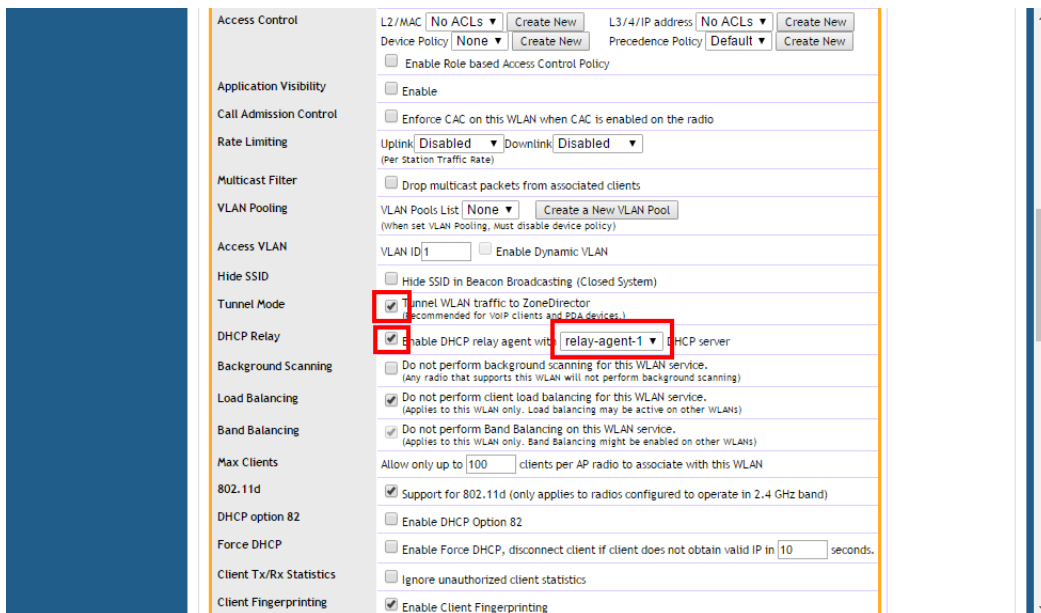
Figure 56. Creating a DHCP Relay server



To enable DHCP Relay for a WLAN:

- 1 Go to **Configure > WLANs**.
- 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 57. Enabling DHCP Relay agent for a Tunnel Mode WLAN



## Enabling 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:

- 1 The target networks must be segmented into VLANs.
- 2 VLANs must be mapped to different SSIDs.
- 3 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

The number of ZoneDirector Bonjour Gateway Bridge Service Rules that you create can have a negative impact on memory and CPU resources.

Maximum Bonjour Gateway Rules:

- ZoneDirector 1100 (without Smart Redundancy): 64
- ZoneDirector 1100 (with Smart Redundancy): 32
- ZoneDirector 1200/3000/5000: 256

If a user has created more than the max number of Bonjour Gateway rules in a previous release, all existing rules will be kept after upgrading to 9.9+. Users can edit and delete the existing rules, but are not allowed to create new rules until the total number is lower than these maximums.

## 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.

## Examples

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 3 different AP Bonjour Gateways to distribute the memory/CPU utilization. Consider 7982 and higher 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.

Requirements:

- Layer 2 switch between ZoneDirector and APs

The maximum number of ZD site Bonjour Gateway rules is as follows:

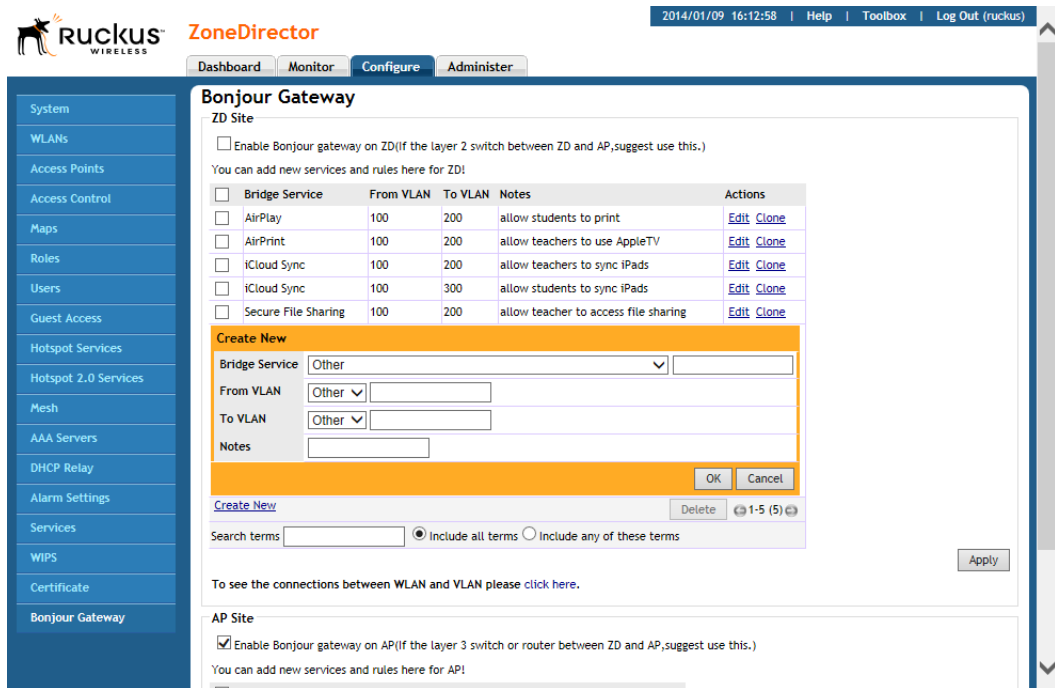
Table 17. Max Bonjour rules per controller

<b>ZoneDirector Model</b>	<b>Max Rules</b>
ZoneDirector 1200	256
ZoneDirector 3000	256
ZoneDirector 5000	256

To configure rules for bridging Bonjour services across VLANs:

- 1** Go to **Configure > Bonjour Gateway**.
- 2** Click **Create New** in the *ZD Site* table 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** to save your changes.
- 5** Repeat for any additional rules.
- 6** Select the check box next to **Enable Bonjour gateway on ZD** and click the **Apply** button.

Figure 58. 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.

**NOTE:** This feature is only supported on the following access points: T300 series, T710, T710s, R310, H500, R500, R510, R600, R700, R710, 7055, 7352, 7372, 7782/81, 7982.

Requirements and limitations:

- Bonjour policy deployment to an AP takes effect after the AP joins ZoneDirector.

## Enabling Bonjour Gateway

Creating a Bonjour Gateway Rule - AP Site

- 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 **Configure > Bonjour Gateway**.
- 2 Click **Create New** in the *AP Site* table 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 **Apply** button.

Figure 59. Create an AP site Bonjour policy

The screenshot displays the 'AP Site' configuration page in the ZoneDirector interface. On the left is a navigation menu with 'Bonjour Gateway' selected. The main content area shows a table of existing Bonjour policies:

<input type="checkbox"/>	Bridge Service	From VLAN	To VLAN	Notes	Actions
<input type="checkbox"/>	AirPlay	100	200	allow students to use AppleTV	<a href="#">Edit</a> <a href="#">Clone</a>
<input type="checkbox"/>	AirPrint	100	200	allow teachers to print	<a href="#">Edit</a> <a href="#">Clone</a>
<input type="checkbox"/>	iCloud Sync	100	200	allow teachers to sync iPads	<a href="#">Edit</a> <a href="#">Clone</a>
<input type="checkbox"/>	iCloud Sync	100	300	allow students to sync iPads	<a href="#">Edit</a> <a href="#">Clone</a>
<input type="checkbox"/>	Secure File Sharing	100	200	allow teachers to access file sharing	<a href="#">Edit</a> <a href="#">Clone</a>

Below the table are 'Create New' and 'Delete' buttons, and a search bar with radio buttons for 'Include all terms' (selected) and 'Include any of these terms'. An 'Apply' button is on the right.

The 'AP Site' section has a checked box for 'Enable Bonjour gateway on AP'. Below it is a 'Create New' dialog box:

**Create New**

Name\*

Description

Rules

<input type="checkbox"/>	Order	Bridge Service	From VLAN	To VLAN	Notes	Actions
<input type="checkbox"/>	1	AirPlay	100	200	allow students to use AppleTV	<a href="#">Edit</a> <a href="#">Clone</a>
<input type="checkbox"/>	2	AirPrint	100	200	allow students to print	<a href="#">Edit</a> <a href="#">Clone</a>

The dialog box also has 'Create New', 'Delete', 'OK', and 'Cancel' buttons, and a search bar with radio buttons for 'Include all terms' (selected) and 'Include any of these terms'. An 'Apply' button is on the right.

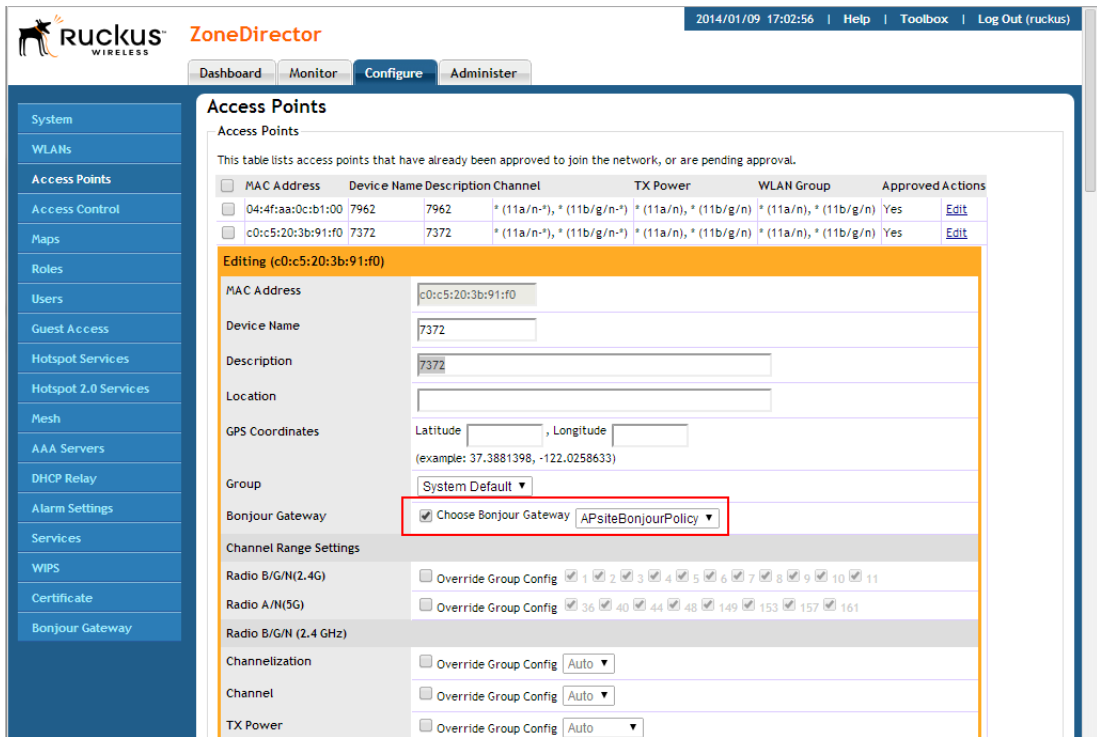
## Applying a Bonjour Policy to an AP

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 **Configure > Access Points**.
- 2 Click **Edit** next to the AP you want to configure.
- 3 in *Bonjour Gateway*, enable the check box and select a Bonjour policy that you created on the *Configure > Bonjour Gateway* page from the list.
- 4 Click **OK** to save your changes.

Figure 60. 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.

Figure 61. Sample Bonjour Gateway configuration for a classroom scenario

The screenshot shows the Ruckus ZoneDirector web interface. The top navigation bar includes the Ruckus logo, the ZoneDirector title, and a status bar with the date/time (2014/01/02 12:19:55), Help, Toolbox, and Log Out (ruckus) links. Below the navigation bar are tabs for Dashboard, Monitor, Configure, and Administer. The left sidebar contains a menu with items like System, WLANs, Access Points, Access Control, Maps, Roles, Users, Guest Access, Hotspot Services, Hotspot 2.0 Services, Mesh, AAA Servers, DHCP Relay, Alarm Settings, Services, WIPS, Certificate, and Bonjour Gateway. The main content area is titled "Bonjour Gateway" and is split into two sections: "ZD Site" and "AP Site".

**ZD Site Configuration:**

- Enable Bonjour gateway on ZD (If the layer 2 switch between ZD and AP, suggest use this.):
- You can add new services and rules here for ZD!

Bridge Service	From VLAN	To VLAN	Notes	Actions
<input type="checkbox"/> AirPlay	100	200	allow students to print	<a href="#">Edit</a> <a href="#">Clone</a>
<input type="checkbox"/> AirPrint	100	200	allow teachers to use AppleTV	<a href="#">Edit</a> <a href="#">Clone</a>
<input type="checkbox"/> iCloud Sync	100	200	allow teachers to sync iPads	<a href="#">Edit</a> <a href="#">Clone</a>
<input type="checkbox"/> iCloud Sync	100	300	allow students to sync iPads	<a href="#">Edit</a> <a href="#">Clone</a>
<input type="checkbox"/> Secure File Sharing	100	200	allow teacher to access file sharing	<a href="#">Edit</a> <a href="#">Clone</a>

- Search terms:   Include all terms  Include any of these terms

**AP Site Configuration:**

- Enable Bonjour gateway on AP (If the layer 3 switch or router between ZD and AP, suggest use this.):
- You can add new services and rules here for AP!

Policy	Description	Actions
<input type="checkbox"/>		<a href="#">Delete</a>

- Search terms:   Include all terms  Include any of these terms

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.

## Configuring SPoT Location Services

To take advantage of Ruckus Wireless 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 **Configure > Location Services**.
- 5 In *Location Services*, click **Create New**.
- 6 Enter the information from the SPoT Admin Portal into the four fields provided.
- 7 Click **OK** to save your changes.
- 8 Go to **Configure > 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.

---

**NOTE:** 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 *Configure > 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 *Monitor > Location Services* page.

For more information on configuration and management of your SPoT service, see the *SPoT User Guide*, available from [support.ruckuswireless.com](http://support.ruckuswireless.com).



Figure 62. SPoT Administration Portal Venue Config page

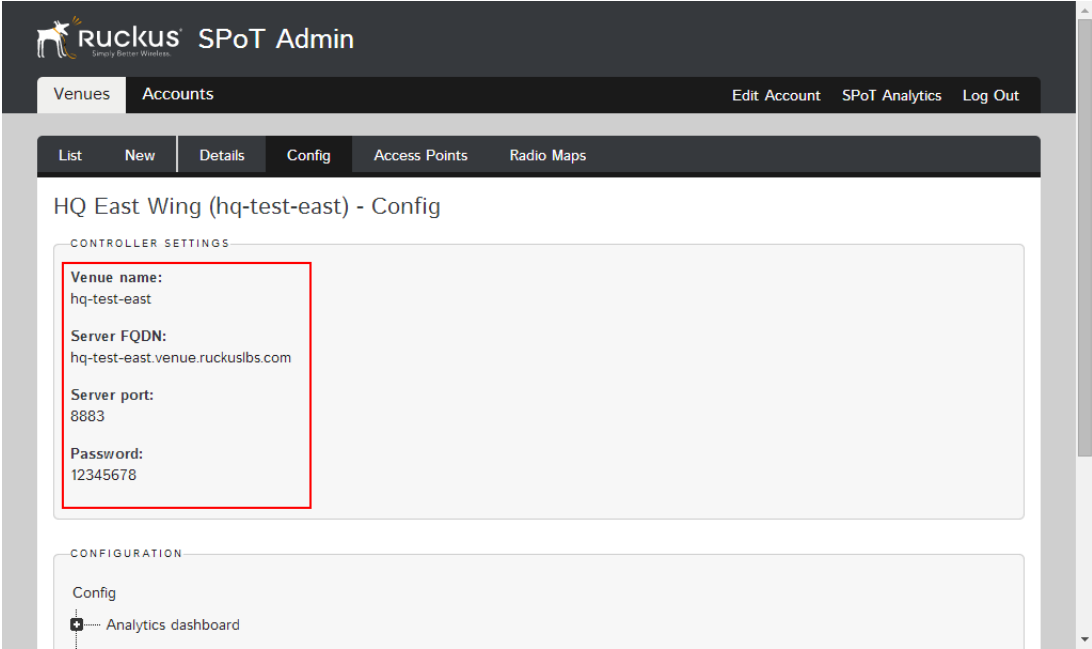


Figure 63. Enter the venue information in ZoneDirector's Configure > Location Services page

The screenshot displays the ZoneDirector web interface. At the top left is the Ruckus logo and the text 'ZoneDirector - ZoneDirector'. The top right shows the date and time '2014/08/07 20:36:29' along with links for 'Help', 'Toolbox', and 'Log Out (ruckus)'. Below the header is a navigation bar with tabs for 'Dashboard', 'Monitor', 'Configure', and 'Administer'. The 'Configure' tab is active. On the left is a vertical sidebar with various system configuration options. The main content area is titled 'Location Services' and contains a table listing current venues. Below the table is a 'Create New' form with the following fields:

<input type="checkbox"/>	Venue Name	Server FQDN or IP Address	Port	Actions
<b>Create New</b>				
	Venue Name*	hq-test-east		
	Server FQDN or IP Address*	hq-test-east.venue.ruckuslbs.com		
	Port*	8883		
	Password*	12345678		
				OK Cancel

Below the form, there is a 'Create New' link, a 'Delete' button, and a count '0-0 (0)'. At the bottom, there is a search bar and radio buttons for 'Include all terms' (selected) and 'Include any of these terms'.

Figure 64. Configure an AP Group for SPoT location services

The screenshot displays the 'Create New' configuration page for an AP Group. The interface includes a left-hand navigation menu with options: Alarm Settings, Services, WIPS, Certificate, Bonjour Gateway, and Location Services. The main configuration area is titled 'Create New' and contains the following sections:

- Name:** SPoT AP Group
- Description:** AP group for Location Services
- Channel Range Settings:** This section is highlighted with a red box. It includes three rows of radio settings, each with an 'Override System Default' checkbox and a list of channel numbers:
  - Radio B/G/N(2.4G):  Override System Default. Channels: 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11. Channel 6 is selected.
  - Radio A/N/AC(5G) Indoor:  Override System Default. Channels: 36, 40, 44, 48, 149, 153, 157, 161. Channel 161 is selected.
  - Radio A/N/AC(5G) Outdoor:  Override System Default. Channels: 149, 153, 157, 161.
- Radio Settings:** This section is divided into two columns: Radio B/G/N (2.4 GHz) and Radio A/N/AC (5.0 GHz). Each column has settings for Channelization, Channel, TX Power, 11n/ac only Mode, WLAN Group, Call Admission Control, and SpectraLink Compatibility, each with an 'Override System Default' checkbox and a dropdown menu.
- Network Setting:** IP Mode:  Override System Default. Dropdown: IPv4 and IPv6.
- Location Services:** Enable/Disable:  Enable. Venue Name\*:  (highlighted with a red box).

## Configuring SPoT Location Services

Example Network Setup

# Configuring Security and Other Services

# 3

In this chapter:

- [Configuring Self Healing Options](#)
- [Configuring Wireless Intrusion Prevention](#)
- [Controlling Network Access Permissions](#)
- [Using an External AAA Server](#)

# Configuring Self Healing Options

ZoneDirector has the capability to perform automatic network adjustments to enhance performance and improve coverage by dynamically modifying power output and channel selection settings for each AP, depending on the actual RF environment. These features are called “Self Healing.”

## Automatically Adjust AP Power

ZoneDirector provides a feature to automatically adjust AP radio power to optimize coverage when interference is present. This feature is designed to turn down the power of an access point if the following conditions are met:

- 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.

Note that the 2.4G and 5G radio bands are considered independently. If all conditions are met, the AP will reduce its power by half. The other AP may or may not necessarily reduce its power simultaneously.

---

**NOTE:** In general, Ruckus does NOT recommend enabling this feature as it can lead to non-optimal AP power levels. With BeamFlex access points, Ruckus' general guidelines are to run access points at full power to maximize the throughput and SINR levels, thus maximizing data rates and performance.

---

## Automatic Channel Selection

ZoneDirector offers two methods of automatic channel selection for spectrum utilization and performance optimization:

- [ChannelFly](#)
- [Background Scanning](#)

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.

## ChannelFly

The main difference between ChannelFly and Background Scanning is that ChannelFly determines the optimal channel based on real-time statistical analysis of actual throughput measurements, while Background Scanning uses channel measurement and other techniques to estimate the impact of interference on Wi-Fi capacity based on progressive scans of all available channels.

---

**NOTE:** If you enable ChannelFly, Background Scanning can still be used for adjusting radio power and rogue detection while ChannelFly manages the channel assignment. Both cannot be used at the same time for channel management.

---

### ***Benefits of ChannelFly***

With ChannelFly, the AP intelligently samples different channels while using them for service. ChannelFly assesses channel capacity every 15 seconds and changes channel when, based on historical data, a different channel is likely to offer higher capacity than the current channel. Each AP makes channel decisions based on this historical data and maintains an internal log of channel performance individually.

When ChannelFly changes channels, it utilizes 802.11h channel change announcements to seamlessly change channels with no packet loss and minimal impact to performance. The 802.11h channel change announcements affect both wireless clients and Ruckus mesh nodes in the 2.4 GHz and/or 5 GHz bands.

Initially (in the first 30-60 minutes) there will be more frequent channel changes as ChannelFly learns the environment. However, once an AP has learned about the environment and which channels are most likely to offer the best throughput potential, channel changes will occur less frequently unless a large measured drop in throughput occurs.

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

### ***Disadvantages of ChannelFly***

Compared to Background Scanning, ChannelFly takes considerably longer for the network to settle down. If you will be adding and removing APs to your network frequently, Background Scanning may be preferable. Additionally, if you have clients that do not support the 802.11h standard, ChannelFly may cause significant connectivity issues during the initial capacity assessment stage.

You can enable/disable ChannelFly per band. If you have 2.4 GHz clients that do not support 802.11h, Ruckus recommends disabling ChannelFly for 2.4 GHz but leaving it enabled for the 5 GHz band.

To configure the self healing options:

- 1 Go to **Configure > 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 65. Self Healing options

The screenshot displays the Ruckus ZoneDirector web interface. The top navigation bar includes the Ruckus logo, the title "ZoneDirector - ZoneDirector", and a status bar with the date "2016/03/28 16:19:58" and links for "Help", "Toolbox", and "Log Out (ruckus)". Below the navigation bar are tabs for "Dashboard", "Monitor", "Configure", and "Administer". The left sidebar contains a menu with categories like System, WLANs, Access Points, Access Control, Maps, Roles, Users, Guest Access, Hotspot Services, Hotspot 2.0 Services, Mesh, AAA Servers, DHCP Relay, Alarm Settings, Services, WIPS, and Certificate. The main content area is titled "Services" and contains the "Self Healing" section, which is highlighted with a red border. This section includes a description of ZoneDirector's self-healing capabilities and three configuration options: "Automatically adjust AP radio power to optimize coverage when interference is present" (unchecked), "Automatically adjust 2.4GHz channels using Background Scanning" (checked), and "Automatically adjust 5GHz channels using Background Scanning" (checked). Below this section are "Background Scanning" and "Load Balancing" sections, each with their own "Apply" buttons. The "Background Scanning" section includes options to run scans every 20 seconds for both 2.4GHz and 5GHz. The "Load Balancing" section includes options for client load balancing on 2.4GHz and 5GHz radio, with adjacent radio thresholds of 50 dB and 43 dB respectively.



## 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 that Background Scanning must be enabled for ZoneDirector to detect rogue APs on the network.

To configure Background Scanning:

- 1 Go to **Configure > Services**.
- 2 In the *Background Scanning* section, configure the following options:
  - **Run a background scan on the 2.4 GHz radio every [ ]**: Select this check box enter the time interval (1~65535 seconds, default is 20) that you want to set between each scan.
  - **Run a background scan on the 5 GHz radio every [ ]**: Select this check box enter the time interval (1~65535 seconds, default is 20) that you want to set between each scan.

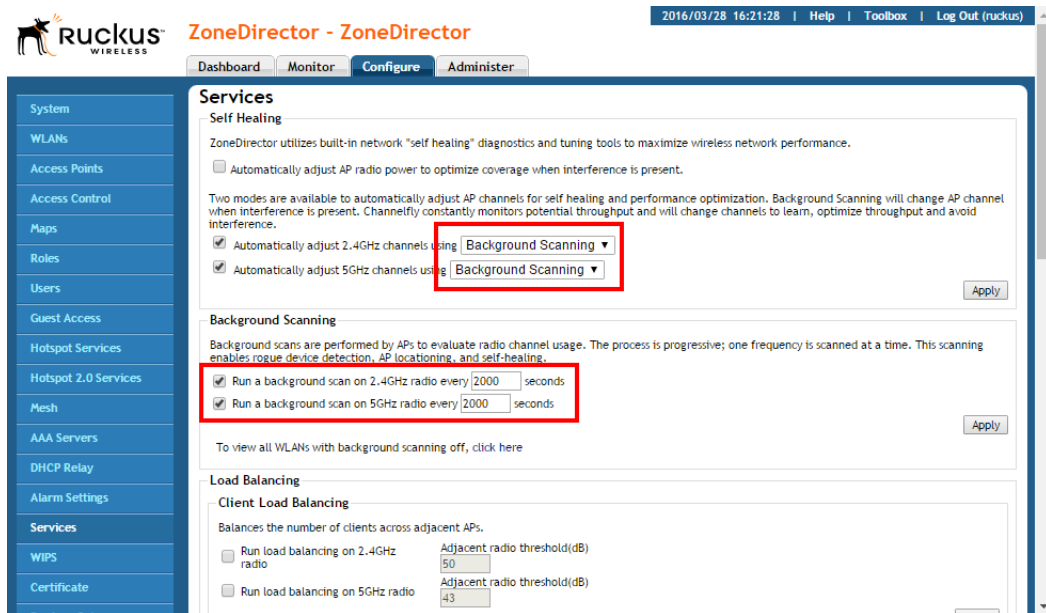
---

**NOTE:** If you want to disable Background Scanning, clear the check box; this should result in a minor increase in AP performance, but removes the detection of rogue APs from ZoneDirector monitoring. You can also decrease the scan frequency, as less frequent scanning improves overall AP performance.

---

- 3 Click the **Apply** button in the same section to save your settings.

Figure 66. Background scanning options



**NOTE:** You can also disable Background Scanning on a per-WLAN basis from the **Configure > WLANs** page. To disable scanning for a particular WLAN, click the **Edit** link next to the WLAN for which you want to disable scanning, open **Advanced Options**, 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 **Monitor > Access Points**, and click on the AP's MAC address. The access point detail screen displays the Background Scanning status for each radio.

Figure 67. Viewing whether Background Scanning is enabled for an AP

The screenshot shows the ZoneDirector web interface. The left sidebar contains navigation menus for Access Points, WLANs, Clients, and other system components. The main content area displays the configuration for a selected AP. The 'Background Scanning' status is highlighted in a red box, showing it is 'Enabled'. Other configuration details include device name, location, IP address, and various performance metrics.

General		Info		WLANs	
Device Name	7982	Status	Connected (Root AP)	Name/ESSID	BSSID
Description		Uptime	5d 1h 7m	Ruckus1	c4:10
Location		Connection Mode	L3 (IPv4)	Ruckus1	c4:10
GPS Coordinates		VLAN	1		
MAC Address	c4:10:8a:1f:d1:f0	Associated Clients	1		
IP Address	192.168.40.64	Bonjour Gateway			
External IP:Port	192.168.40.64:12223				
IP Type	DHCP	Actions			
Model	z7982				
S/N	501155001774				
Version	9.8.0.0.104				
Radio 802.11a/n		Radio 802.11b/g/n		LAN Port Configur	
Current Channel	149	Current Channel	1	LAN State	Typ
Channelization	40	Channelization	20	LAN1	Enabled Tru
WLAN Group	Default	WLAN Group	Default	LAN2	Enabled Tru
SpectralLink Compatibility	Use Parent Configuration	SpectralLink Compatibility	Use Parent Configuration	LAN Port Status	
Deployed/Maximum/WLAN-Group WLAN Number	1/27/1	Deployed/Maximum/WLAN-Group WLAN Number	1/27/1	Port Interface	Dr
Background Scanning	Enabled	Background Scanning	Enabled	eth0	Nc
TX Power	Full	TX Power	Full	eth1	Nc
# of Authorized Client Devices	1	# of Authorized Client Devices	0	Neighbor APs	
% Retries/% Drops	0.0025 / 0.00	% Retries/% Drops	1.12 / 0.00	Access Point	
% Non-unicast	0.0188	% Non-unicast	0.0853	c0:c5:20:3b:91:f0	
Packets/Bytes Received	36M/36G	Packets/Bytes Received	4.4M/890M	04:4f:aa:0c:b1:00	
Packets/Bytes Transmitted	19M/7.4G	Packets/Bytes Transmitted	634K/329M		
Wlans Data Packets/Bytes Received	45K/4.7M	Wlans Data Packets/Bytes Received	190K/19M		
Wlans Data Packets/Bytes Transmitted	54K/52M	Wlans Data Packets/Bytes Transmitted	317K/246M		
Noise Floor	-112	Noise Floor	-107		
PHY Errors	0	PHY Errors	62		
% AirTime (total/busy/RX/TX)	0.0/0.0/0.0/0.0	% AirTime (total/busy/RX/TX)	8.0/0.5/8.0/0.0		
Available Channel	36,40,44,48,149,153,157,161	Available Channel	1,2,3,4,5,6,7,8,9,10,11		

## 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 **Configure > 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 68. Enable Load Balancing across adjacent APs by radio type

To view all WLANs with background scanning off, [click here](#)

**Load Balancing**

**Client Load Balancing**

Balances the number of clients across adjacent APs.

Run load balancing on 2.4GHz radio  Adjacent radio threshold(dB)

Run load balancing on 5GHz radio  Adjacent radio threshold(dB)

**Band Balancing**

Balances the load on Radios, by distributing the clients on 2.4GHz and 5GHz radios.

Percent of clients on 2.4GHz radio  %

**Radar Avoidance Pre-Scanning**

Enable Radar Avoidance Pre-Scanning

**AeroScout RFID**

Enable AeroScout RFID tag detection

**Ekahau Settings**

Enable Ekahau tag detection

Ekahau Controller IP Address\*

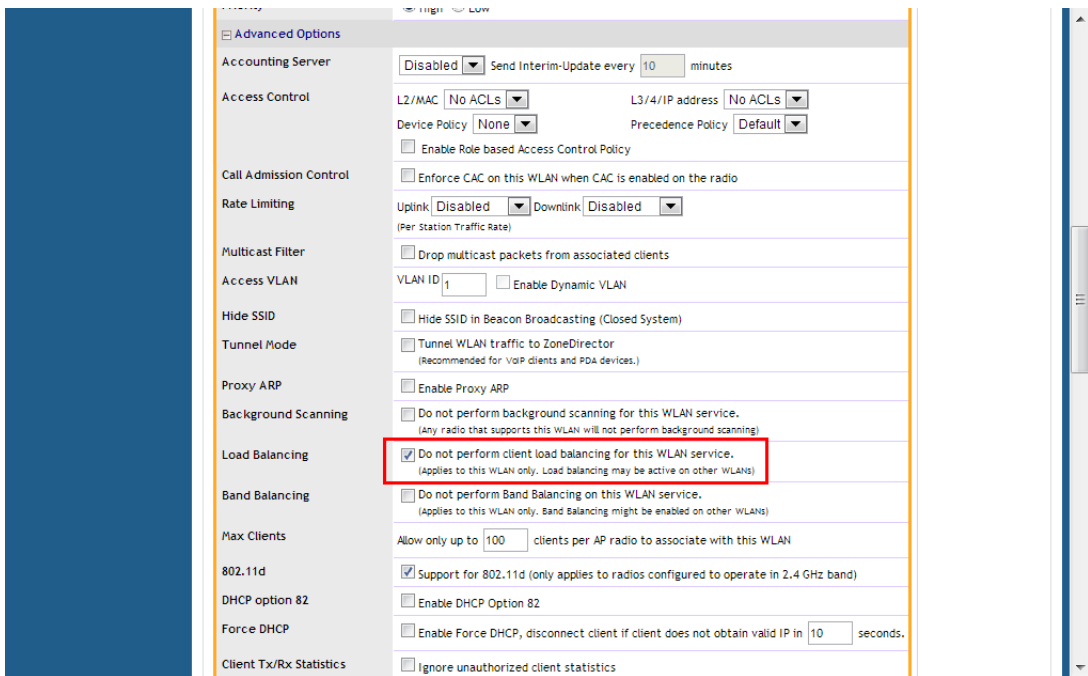
Ekahau Controller Port\*

**Active Client Detection**

To disable Load Balancing on a per-WLAN basis:

- 1 Go to **Configure > WLANs**.
- 2 Click the **Edit** link beside 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*.

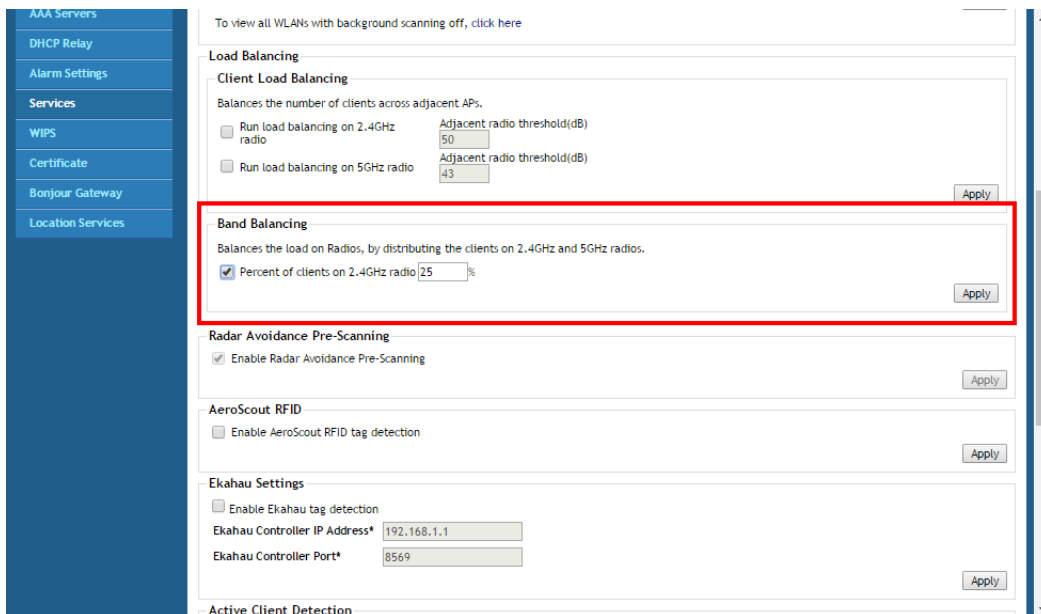
Figure 69. Disable load balancing on a specific WLAN



## 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 70. Distributing clients between the 2.4 and 5 GHz radios



## 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](#)).

Figure 71. Enabling Radar Avoidance Pre-Scanning

The screenshot shows the configuration page for services in ZoneDirector. The left sidebar contains a navigation menu with items: AAA Servers, DHCP Relay, Alarm Settings, Services (highlighted), WIPS, Certificate, Bonjour Gateway, and Location Services. The main content area is titled 'To view all WLANs with background scanning off, click here'. It contains several sections: 'Load Balancing' with 'Client Load Balancing' (radio buttons for 2.4GHz and 5GHz, and adjacent radio threshold inputs of 50 and 43 dB) and 'Band Balancing' (radio button for 2.4GHz and a percentage input of 25%). The 'Radar Avoidance Pre-Scanning' section is highlighted with a red box and contains a checked checkbox 'Enable Radar Avoidance Pre-Scanning' and an 'Apply' button. Below it is the 'AeroScout RFID' section with an unchecked checkbox 'Enable AeroScout RFID tag detection' and an 'Apply' button. The 'Ekahau Settings' section includes an unchecked checkbox 'Enable Ekahau tag detection', an 'Ekahau Controller IP Address\*' field with '192.168.1.1', and an 'Ekahau Controller Port\*' field with '8569', both with 'Apply' buttons. At the bottom, there is a partially visible 'Active Client Detection' section.

## 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.

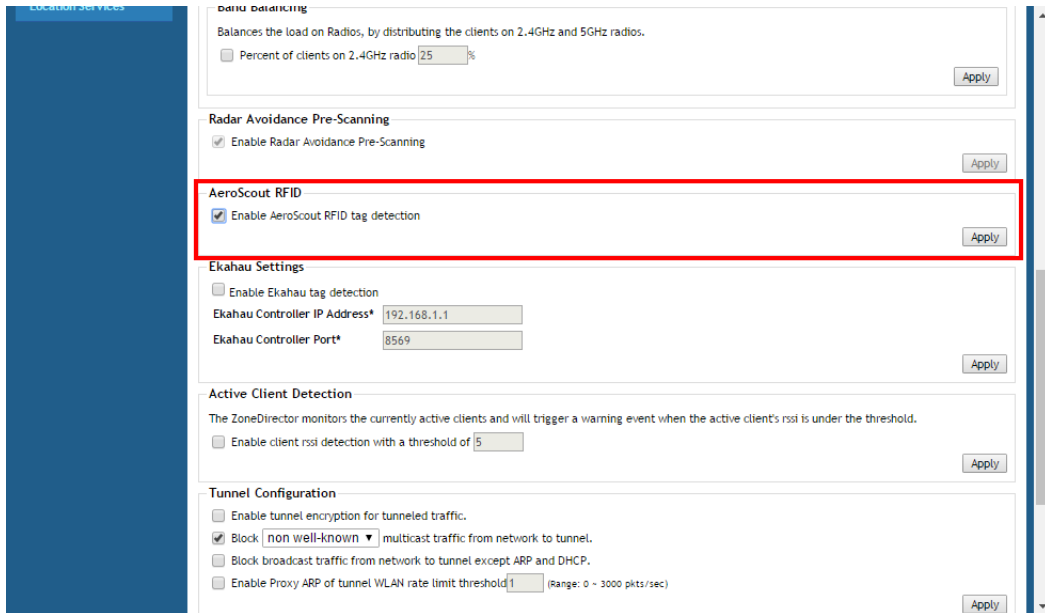
To enable AeroScout RFID tag detection on ZoneDirector:

- 1 Go to **Configure > 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.



Figure 72. Enabling AeroScout Tag detection



The screenshot shows the configuration page for ZoneDirector. The 'AeroScout RFID' section is highlighted with a red box. It contains a checked checkbox for 'Enable AeroScout RFID tag detection' and an 'Apply' button. Other sections include 'Data Balancing', 'Radar Avoidance Pre-Scanning', 'Ekahau Settings', 'Active Client Detection', and 'Tunnel Configuration'.

---

**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 System locates and tracks assets with attached Ekahau Tags. Ekahau Tags are small, 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 **Configure > 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.

Figure 73. Enabling Ekahau tag detection

The screenshot displays the configuration page for 'Location Services'. The 'Ekahau Settings' section is highlighted with a red border. It includes the following fields and options:

- Enable Ekahau tag detection
- Ekahau Controller IP Address\*: 192.168.1.1
- Ekahau Controller Port\*: 8569
- Apply button

Other visible sections include:

- Radio Balancing**: Balances the load on Radios, by distributing the clients on 2.4GHz and 5GHz radios. Includes a checkbox for 'Percent of clients on 2.4GHz radio' set to 25% and an Apply button.
- Radar Avoidance Pre-Scanning**: Includes a checked checkbox for 'Enable Radar Avoidance Pre-Scanning' and an Apply button.
- AeroScout RFID**: Includes a checkbox for 'Enable AeroScout RFID tag detection' and an Apply button.
- Active Client Detection**: The ZoneDirector monitors the currently active clients and will trigger a warning event when the active client's rssi is under the threshold. Includes a checkbox for 'Enable client rssi detection with a threshold of' set to 5 and an Apply button.
- Tunnel Configuration**: Includes checkboxes for 'Enable tunnel encryption for tunneled traffic.', 'Block non well-known multicast traffic from network to tunnel.', 'Block broadcast traffic from network to tunnel except ARP and DHCP.', and 'Enable Proxy ARP of tunnel WLAN rate limit threshold' set to 1 (Range: 0 - 3000 pkts/sec) with an Apply button.

## 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 **Configure > 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.

Figure 74. Enabling active client detection

The screenshot shows the configuration page for ZoneDirector. The 'Active Client Detection' section is highlighted with a red border. It contains the following text and controls:

- Active Client Detection**
- The ZoneDirector monitors the currently active clients and will trigger a warning event when the active client's rssi is under the threshold.
- Enable client rssi detection with a threshold of
- 

Other sections visible include:

- Ekahau Settings**:  Enable Ekahau tag detection; Ekahau Controller IP Address\* ; Ekahau Controller Port\* ;
- Tunnel Configuration**:  Enable tunnel encryption for tunneled traffic.;  Block  multicast traffic from network to tunnel.;  Block broadcast traffic from network to tunnel except ARP and DHCP.;  Enable Proxy ARP of tunnel WLAN rate limit threshold  (Range: 0 - 3000 pkts/sec);
- Packet Inspection Filter**:  Enable Neighbor Discovery Packets (ARP and ICMPv6 Neighbor Solicit) rate limit threshold  (Range: 0 - 3000 pkts/sec);
- Ethernet Port Redundancy**:  Enable Active-standby mode on Ethernet ports; Primary ethernet port will be Up after delay:  (Range: 0 - 1000000 ms); Primary ethernet port will be Down after delay:  (Range: 0 - 1000000 ms);

A low severity event is now triggered each time a client connects with an RSSI lower than the threshold value entered. Go to **Monitor > All Events/Activities** to monitor these events.

## Tunnel Configuration

Only WLANs with *Tunnel Mode* enabled are affected. See [Advanced Options](#) in the WLAN configuration section for information on enabling Tunnel Mode.

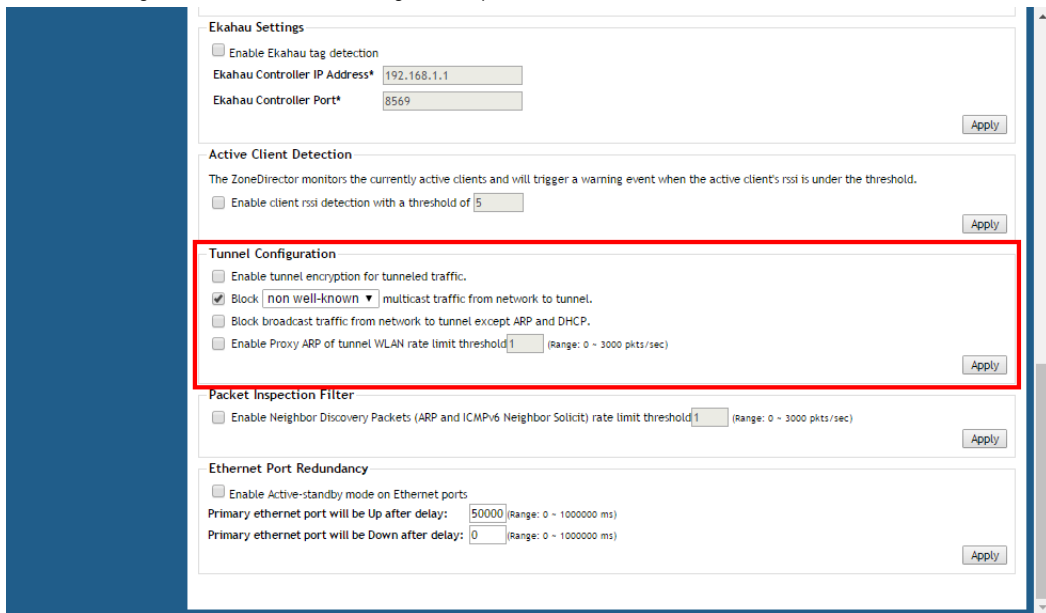
To configure data encryption and filtering for tunneled WLANs:

- 1 Go to **Configure > 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 broadcast neighbor discovery packets (ARP and ICMPv6 Neighbor Solicit) over 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 specified. If ZoneDirector receives a broadcast ARP request for an unknown host, 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](#)).

4 Click **Apply** in the same section to save your changes.

Figure 75. 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](#)).
- Proxy ARP for WLAN interfaces (see [Advanced Options](#) under [Creating a WLAN](#)).
- Proxy ARP for Tunneled WLANs (see [Tunnel Configuration](#)).

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 76. Packet Inspection Filter

The screenshot shows the configuration interface for the Packet Inspection Filter. The 'Packet Inspection Filter' section is highlighted with a red border. It contains the following settings:

- Enable Neighbor Discovery Packets (ARP and ICMPv6 Neighbor Solicit) rate limit threshold  (Range: 0 - 3000 pkts/sec)

Other sections visible include:

- Ekahau Settings:**  Enable Ekahau tag detection; Ekahau Controller IP Address\* ; Ekahau Controller Port\*
- Active Client Detection:** The ZoneDirector monitors the currently active clients and will trigger a warning event when the active client's rssi is under the threshold.  Enable client rssi detection with a threshold of
- Tunnel Configuration:**  Enable tunnel encryption for tunneled traffic.  Block  multicast traffic from network to tunnel.  Block broadcast traffic from network to tunnel except ARP and DHCP.  Enable Proxy ARP of tunnel WLAN rate limit threshold  (Range: 0 - 3000 pkts/sec)
- Ethernet Port Redundancy:**  Enable Active-standby mode on Ethernet ports. Primary ethernet port will be Up after delay:  (Range: 0 - 1000000 ms). Primary ethernet port will be Down after delay:  (Range: 0 - 1000000 ms)

## Ethernet Port Redundancy

Ethernet Port Redundancy, or NIC bonding, provides a method for aggregating Zonedirector network interfaces into a single logical “bonded” interface. With port redundancy enabled, one of the two network interfaces will be in active state while the other is in standby state. When the active interface physical link is down and the standby interface physical link is up, the two interfaces will fail over within 3 seconds, and the original active interface becomes the standby interface, while the original standby interface becomes the active port.

---

**NOTE:** This feature is currently only available on ZoneDirector 3000/5000. ZD 1200 does not support port redundancy.

---

Port redundancy is disabled by default. If enabled, you can specify the time (in milliseconds) after which the standby port will be enabled after a link recovery has been detected, and after which the inactive port will be disabled after a link failure has been detected.

To enable Ethernet Port Redundancy:

- 1 Go to **Configure > Services**.
- 2 Locate the **Ethernet Port Redundancy** section at the bottom of the page.
- 3 **Enable** the check box, and enter the **Up Delay Time** and **Down Delay Time** in the text boxes.
  - **Up Delay Time:** Specifies the time, in milliseconds, to wait before enabling a slave after a link recovery has been detected. The default value is 50000, range is 0~1000000.
  - **Down Delay Time:** Specifies the time, in milliseconds, to wait before disabling a slave after a link failure has been detected. The default value is 0, range is 0~1000000.
- 4 Click **Apply** to save your changes.

Figure 77. Ethernet Port Redundancy

The screenshot displays the configuration interface for Ethernet Port Redundancy. The interface is organized into several sections, each with an 'Apply' button. The 'Ethernet Port Redundancy' section is highlighted with a red border.

- Enable Ekahau tag detection:** . Ekahau Controller IP Address\*: 192.168.1.1. Ekahau Controller Port\*: 8569.
- Active Client Detection:** The ZoneDirector monitors the currently active clients and will trigger a warning event when the active client's rssi is under the threshold.  Enable client rssi detection with a threshold of 5.
- Tunnel Configuration:**
  - Enable tunnel encryption for tunneled traffic.
  - Block non well-known multicast traffic from network to tunnel.
  - Block broadcast traffic from network to tunnel except ARP and DHCP.
  - Enable Proxy ARP of tunnel WLAN rate limit threshold 1 (Range: 0 - 3000 pkts/sec).
- Packet Inspection Filter:**  Enable Neighbor Discovery Packets (ARP and ICMPv6 Neighbor Solicit) rate limit threshold 1 (Range: 0 - 3000 pkts/sec).
- Ethernet Port Redundancy:**  Enable Active-standby mode on Ethernet ports.
  - Primary ethernet port will be Up after delay: 50000 (Range: 0 - 1000000 ms)
  - Primary ethernet port will be Down after delay: 0 (Range: 0 - 1000000 ms)
  -

# 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 intrusion attempts. These features, called Wireless Intrusion Prevention System (WIPS), allow you to customize the actions to take and the notifications you would like to receive when each of the different threat types is detected.

## 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 **Configure > WIPS**.
- 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 [ ] seconds:** If this capability is activated, any clients that repeatedly fail in attempting authentication will be temporarily blocked for a period of time (10~1200 seconds, default is 30). Clients temporarily blocked by the Intrusion Prevention feature are not added to the Blocked Clients list on the *Configure > Access Control* page, *Blocked Clients* section.
- 3 Click **Apply** to save your changes.



Figure 78. Denial of Service (DoS) prevention options

The screenshot displays the ZoneDirector configuration page for the Wireless Intrusion Detection and Prevention System. The 'Denial of Service(DoS)' section is highlighted with a red box. It includes the following options:

- Protect my wireless network against excessive wireless requests
- Temporarily block wireless clients with repeated authentication failures for  seconds

Below the DoS section are two other sections:

- Intrusion Detection and Prevention:**
  - Enable report rogue devices
    - Report all rogue devices
    - Report only malicious rogue devices of type
      - SSID-Spoofing
      - Same-Network
      - MAC-Spoofing
      - User-Blocked
  - Protect the network from malicious rogue access points.
- Rogue DHCP Server Detection:**
  - Enable rogue DHCP server detection

## 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 ZoneFlex 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 *Monitor > Rogue Devices* page.

To configure intrusion detection and prevention options:

- 1 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.
- 2 Click the **Apply** button that is in the same section to save your changes.

Figure 79. Intrusion Prevention options

The screenshot shows the Ruckus ZoneDirector configuration interface. The top navigation bar includes 'Dashboard', 'Monitor', 'Configure', and 'Administer'. The left sidebar lists various system settings like System, WLANs, Access Points, etc. The main content area is titled 'Wireless Intrusion Detection and Prevention System' and contains three sections:

- Denial of Service(DoS)**: Includes options to protect against excessive requests and temporarily block clients with repeated authentication failures for 30 seconds.
- Intrusion Detection and Prevention** (highlighted with a red box): Includes options to enable reporting of rogue devices, with sub-options for reporting all devices or only malicious ones of specific types (SSID-Spoofing, Same-Network, MAC-Spoofing, User-Blocked). It also has an option to protect the network from malicious rogue access points.
- Rogue DHCP Server Detection**: Includes an option to enable rogue DHCP server detection.

See [Detecting Rogue Access Points](#) 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 **Configure > WIPS**.
- 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 Wireless recommends checking the *Monitor > 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:

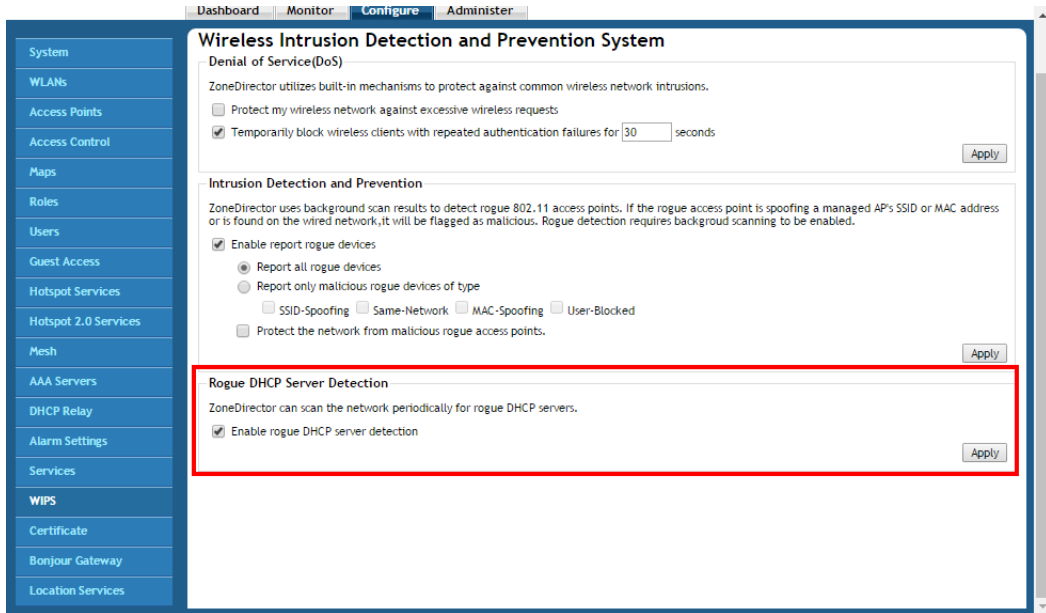
Rogue DHCP server on [IP\_address] has been detected  
If the check box is cleared, ZoneDirector will not generate these events.

---

**NOTE:** Rogue DHCP server detection only works on the ZoneDirector's management IP subnet.

---

Figure 80. Enabling Rogue DHCP server detection



# Controlling Network Access Permissions

ZoneDirector provides several options for controlling client 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 **Configure > Access Control** page:

- [Creating Layer 2/MAC Address Access Control Lists](#)
- [Creating Layer 3/Layer 4/IP Address Access Control Lists](#)
- [Configuring Device Access Policies](#)
- [Configuring Precedence Policies](#)
- [Blocking Client Devices](#)
- [Configuring Client Isolation White Lists](#)
- [Application Recognition and Filtering](#)

## 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 **Configure > Access Control**.
- 2 Expand the **L2-L7 Access Control** section.
- 3 In *L2/MAC Access Control*, click **Create New**.

---

**NOTE:** Alternatively, you can create a Layer 2/MAC ACL from the WLAN creation page while creating a new WLAN or modifying an existing WLAN (**Configure > WLANs > Edit > Advanced Options > Access Control > L2/MAC > Create New**.)

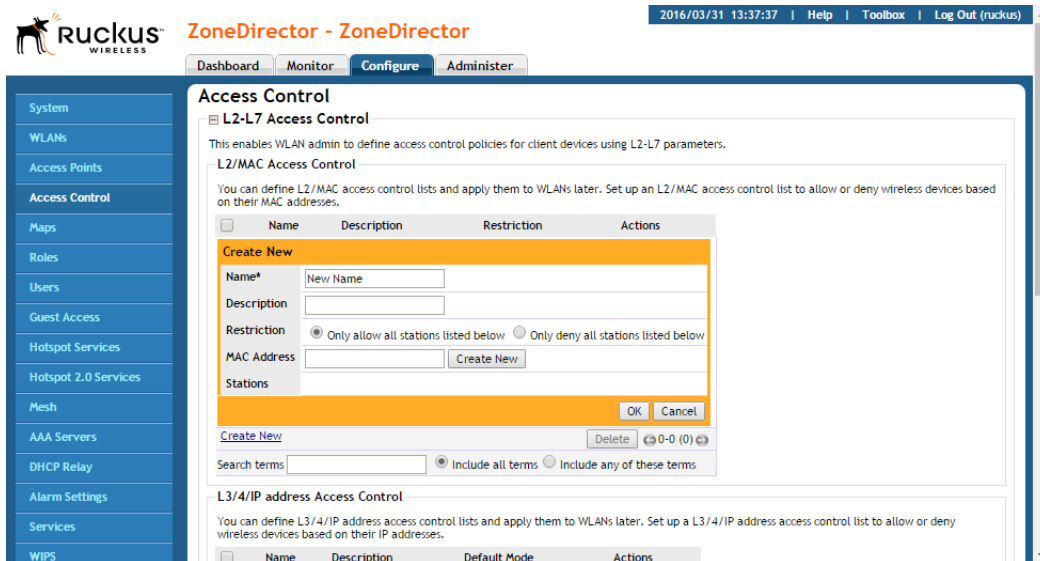
---

- 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 81. 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 provides access control options at Layer 3 and Layer 4. This means that you can configure the access control options based on a set of criteria, including:

- Destination Address
- Application
- Protocol
- Destination Port

To create an L3/L4/IP address based ACL:

- 1 Go to **Configure > Access Control**.
- 2 Expand the **L2-L7 Access Control** section.
- 3 In *L3/4/IP address Access Control*, click **Create New**.

---

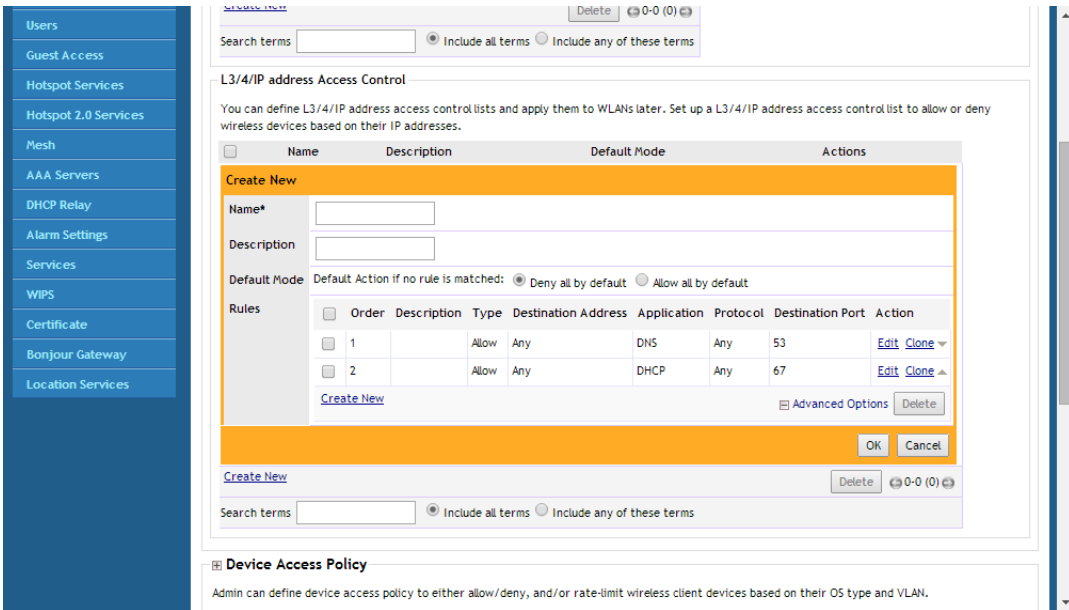
**NOTE:** Alternatively, you can create a Layer 3/Layer 4/IP Address ACL from the WLAN creation page while creating a new WLAN or modifying an existing WLAN (**Configure > WLANs > Edit > Advanced Options > Access Control > L3/4/IP Address > Create New.**)

---

- 4 Type a **Name** for the ACL.
- 5 Type a **Description** for the ACL.
- 6 In **Default Mode**, set the default access privilege (allow all or deny all) that you want to grant all users by default.
- 7 In **Rules**, click **Create New** or click **Edit** to edit an existing rule.
- 8 Define each access policy by configuring a combination of the following:
  - *Type*: The access privilege (allow or deny) that this policy grants.
  - *Destination Address*: Enter an IP subnet and netmask of the network target to which you want to allow or deny access. (IP address must be in the format *A.B.C.D/M*, where *M* is the subnet mask.) Otherwise, select *Any*. For example, if you enter 192.168.0.1/24, the rule would allow or deny the entire Class C subnet. To allow/deny a single host, use /32 as the netmask.
  - *Application*: If you select a specific application from the menu, the Protocol and Destination Port options are automatically filled with the relevant values and are not configurable.
  - *Protocol*: Enter a network protocol number (0-254), as defined by the IANA (<http://www.iana.org/assignments/protocol-numbers/protocol-numbers.xhtml>) to allow or deny. Otherwise, select *Any*.
  - *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 82. Configuring an L3/L4 access control list



## Configuring Device Access Policies

In response to the growing numbers of personally owned mobile devices such as smart phones and tablets being brought into the network, IT departments are requiring more sophisticated control over how devices connect, what types of devices can connect, and what they are allowed to do once connected.

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

Once a Device Access Policy has been created, you can apply the policy to any WLANs for which you want to control access by device type. You could, for example, allow only Apple OS devices on one WLAN and only Linux devices on another.

To create a Device Access Policy:

- 1 Go to **Configure > Access Control**.
- 2 Expand the *Device Access Policy* section, and click **Create New**.

---

**NOTE:** Alternatively, you can create a Device Access Policy from the WLAN creation page while creating a new WLAN or modifying an existing WLAN (**Configure > WLANs > Edit > Advanced Options > Access Control > Device Policy > Create New.**)

---

- 3 Enter a **Name** and optionally a description for the access policy.
- 4 In *Default Mode*, select **Deny all by default** or **Allow all by default**.
- 5 In *Rules*, you can create multiple OS-specific rules for each access policy.
  - **Description:** Description of the rule.
  - **OS/Type:** Select from any of the supported client types.
  - **Type:** Select rule type (allow or deny).
  - **Uplink/Downlink:** Set rate limiting for this client type.
  - **VLAN:** Segment this client type into a specified VLAN (1~4094; if no value entered, this policy does not impact device VLAN assignment).
- 6 Click **Save** to save the rule you created. You can create up to 10 rules per access policy (one for each OS/Type).
- 7 To change the order in which rules are implemented, click the up or down arrows in the *Action* column. You can also **Edit** or **Clone** rules from the *Action* column. To delete a rule, select the box next to the rule and click **Delete**.
- 8 Click **OK** to save the access policy. You can create up to 32 access policies (one access policy per WLAN).

Figure 83. Creating a Device Access Policy

The screenshot shows the ZoneDirector web interface. On the left is a navigation menu with items: DHCP Relay, Alarm Settings, Services, WIPS, Certificate, Bonjour Gateway, and Location Services. The main content area is titled 'Device Access Policy' and contains the following elements:

- A search bar with the text 'Search terms' and two radio buttons: 'Include all terms' (selected) and 'Include any of these terms'.
- A section titled 'Device Access Policy' with a sub-header 'Admin can define device access policy to either allow/deny, and/or rate-limit wireless client devices based on their OS type and VLAN.'
- A 'Create New' dialog box with the following fields and options:
  - Name\*: Deny iOS
  - Description: Deny all iOS devices
  - Default Mode: Default Action if no rule is matched:  Deny all by default  Allow all by default
  - Rules table:

Order	Description	OS/Type	Type	Uplink	Downlink	VLAN	Action
1	Deny iOS	Apple iOS	Deny	DISABLE	DISABLE		<a href="#">Edit</a> <a href="#">Clone</a>

Below the table are links for [Create New](#), [Advanced Options](#), and [Delete](#).
  - Buttons for 'OK' and 'Cancel'.
- Below the dialog box are links for [Create New](#), [Delete](#), and a counter '0-0 (0)'.
- A second search bar with the same radio buttons as above.
- A section titled 'Precedence Policy' with the text: 'Precedence policies are used to define the order in which VLAN and rate limiting policies are applied when the WLAN settings, AAA server configuration or Device Policy settings conflict.'
- A section titled 'Blocked Clients'.

To apply a Device Access Policy to a WLAN:

- 1 Go to **Configure > WLANs**.
- 2 To edit an existing WLAN, click **Edit** next to the WLAN you want to edit.
- 3 Expand the **Advanced Options**, and locate the *Access Control* section.
- 4 In **Device Policy**, select the policy you created from the list.
- 5 Click **OK** to save your changes.

Figure 84. Applying a device access policy for a WLAN

The screenshot displays the configuration page for a WLAN. On the left is a navigation sidebar with 'Location Services' selected. The main content area is divided into several sections:

- Authentication Server:** Local Database (dropdown), Create New (button).
- Wireless Client Isolation:**
  - Isolate wireless client traffic from other clients on the same AP.
  - Isolate wireless client traffic from all hosts on the same VLAN/subnet. (No WhiteList dropdown, Create New button)
  - (Requires whitelist for gateway and other allowed hosts.)
- Zero-IT Activation™:**
  - Enable Zero-IT Activation (WLAN users are provided with wireless configuration installer after they log in.)
- Priority:** High (selected), Low (radio button).
- Advanced Options:**
  - Accounting Server:** Disabled (dropdown), Create New (button), Send Interim-Update every 10 minutes (input).
  - Access Control:**
    - Device Policy:** None (dropdown), Create New (button)
    - Enable R:**  None (dropdown), Control Policy (dropdown)
    - Enable deny IQS (button, highlighted by mouse cursor)
  - Application Visibility:**  Enable
  - Call Admission Control:**  Enforce CAC on this WLAN when CAC is enabled on the radio
  - Rate Limiting:** Uplink: Disabled (dropdown), Downlink: Disabled (dropdown), (Per Station Traffic Rate)
  - Multicast Filter:**  Drop multicast packets from associated clients
  - VLAN Pooling:** VLAN Pools List: None (dropdown), Create a New VLAN Pool (button), (When set VLAN Pooling, must disable device policy)
  - Access VLAN:** VLAN ID: 1 (input),  Enable Dynamic VLAN
  - Hide SSID:**  Hide SSID in Beacon Broadcasting (Closed System)
  - Tunnel Mode:**  Tunnel WLAN traffic to ZoneDirector (Recommended for VoIP clients and PDA devices.)
  - Proxy ARP:**  Enable

## 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 **Configure > 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.

**NOTE:** Alternatively, you can create a Precedence Policy from the WLAN creation page while creating a new WLAN or modifying an existing WLAN (**Configure > WLANs > 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 85. Precedence Policy settings

The screenshot shows the Ruckus ZoneDirector web interface. The top navigation bar includes the Ruckus logo, the title 'ZoneDirector - ZoneDirector', and a status bar with the date '2016/03/28 16:52:07', 'Help', 'Toolbox', and 'Log Out (ruckus)'. Below the navigation bar are tabs for 'Dashboard', 'Monitor', 'Configure', and 'Administer'. The left sidebar contains a menu with options like System, WLANs, Access Points, Access Control, Maps, Roles, Users, Guest Access, Hotspot Services, Hotspot 2.0 Services, Mesh, AAA Servers, DHCP Relay, Alarm Settings, Services, WIPS, and Certificate. The main content area is titled 'Access Control' and contains several sections:

- L2-L7 Access Control**: This enables WLAN admin to define access control policies for client devices using L2-L7 parameters.
- Device Access Policy**: Admin can define device access policy to either allow/deny, and/or rate-limit wireless client devices based on their OS type and VLAN.
- Precedence Policy** (highlighted with a red box): Precedence policies are used to define the order in which VLAN and rate limiting policies are applied when the WLAN settings, AAA server configuration or Device Policy settings conflict. It includes a table with columns for Name, Description, and Actions. The table has one row with 'Default' in the Name column and 'Edit Clone' in the Actions column. Below the table are buttons for 'Create New', 'Delete', and a pagination control showing '1-1 (1)'. There is also a search bar and radio buttons for 'Include all terms' (selected) and 'Include any of these terms'.
- Blocked Clients**: This table lists client devices that are blocked from the WLAN. To unblock a client and allow it to access the WLAN, delete it from the list. To view a list of currently active clients, click here.
- Client Isolation White List**: Admin can configure the IP and MAC information of the reachable wired network hosts in the local network. Clients on the port configured with this list are prevented from spoofing any IP in this list.
- Application Recognition and Filtering**: [1] This enables admin to define list of applications and application port maps and apply it to Clients later. This information is used for generating of pie chart in Clients. To download the port list, click here.

## 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 to monitor, block and unblock client devices manually from the ZoneDirector web interface.

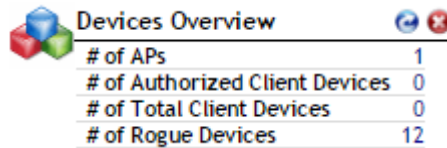
Note the following considerations when managing the Blocked Clients list:

- 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.

## Monitoring Client Devices

- 1 Go to the Dashboard, if it's not already in view.
- 2 Under *Devices Overview*, look at # of Total Client Devices.

Figure 86. The Device Overview widget



Devices Overview	
# of APs	1
# of Authorized Client Devices	0
# of Total Client Devices	0
# of Rogue Devices	12

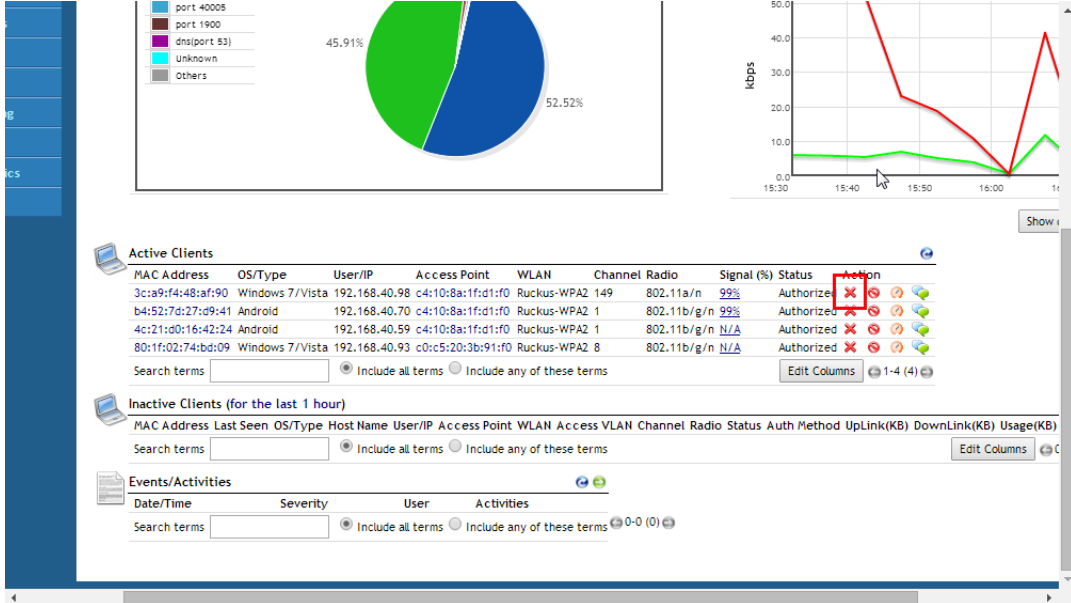
- 3 Click the current number, which is also a link. The Wireless Clients page (on the Monitor tab) appears, showing the first 15 clients that are currently connected to ZoneDirector. If there are more than 15 currently active clients, the Show More button at the bottom of the page will be active. To display more clients in the list, click **Show More**. When all active clients are displayed on the page, the Show More button disappears.
- 4 To block any listed client devices, follow the next set of steps.

## 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 Look at the *Status* column to identify any “Unauthorized” users.
- 2 Click the **Delete** button in the *Action* column in a specific user row. The entry is deleted from the *Active/Current Client* list, and the listed device is disconnected from your Ruckus Wireless WLAN.

Figure 87. Click the Delete button to temporarily delete a client. The client will be able to reconnect.



**NOTE:** 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](#).

## Permanently Blocking Specific Client Devices

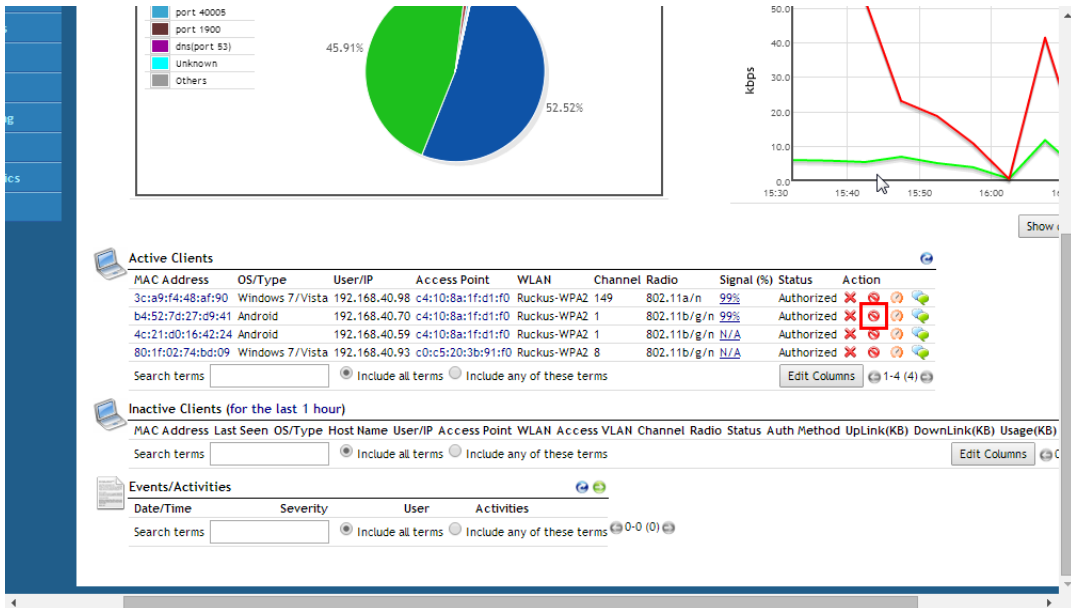
Follow these steps to permanently block a client device from WLAN connections.

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

2 Click the **Block** button in the *Action* column in a specific user row.

The status is changed to *Blocked*. This will prevent the listed device from using your Ruckus Wireless WLANs.

Figure 88. Click the Block button to permanently delete a client

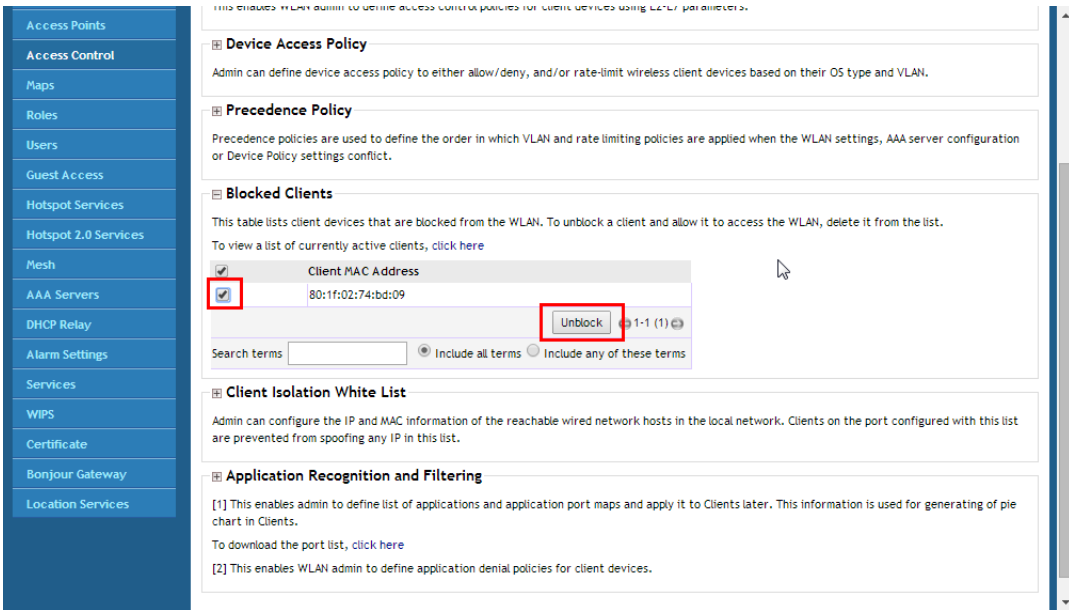


## Reviewing a List of Previously Blocked Clients

- 1 Go to **Configure > Access Control**.
- 2 Review the *Blocked Clients* table.
- 3 You can unblock any listed MAC address by clicking the **Unblock** button for that address.



Figure 89. 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 **Configure > Access Control**.
- 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 (**Configure > WLANs > 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-down menu in the *Order* column. You can also **Edit** or **Clone** rules from the *Action* column. To delete a rule, select the box next to the rule and click **Delete**.
- 7 Click **OK** to save the white list.

Figure 90. Creating a Client Isolation White List

The screenshot displays the 'Client Isolation White List' configuration interface. On the left is a blue sidebar with navigation links: Guest Access, Hotspot Services, Hotspot 2.0 Services, Mesh, AAA Servers, DHCP Relay, Alarm Settings, Services, WIPS, Certificate, Bonjour Gateway, and Location Services. The main content area is titled 'Client Isolation White List' and includes the following sections:

- Blocked Clients:** A section with a title and a description: 'This table lists client devices that are blocked from the WLAN. To unblock a client and allow it to access the WLAN, delete it from the list. To view a list of currently active clients, [click here](#)'.
- Client Isolation White List:** A section with a title and a description: 'Admin can configure the IP and MAC information of the reachable wired network hosts in the local network. Clients on the port configured with this list are prevented from spoofing any IP in this list.' Below this is a table with columns: Name, Description, and Actions.
 

Name	Description	Actions			
<b>Create New</b>					
Name*	<input type="text" value="whitelist1"/>				
Description	<input type="text"/>				
<b>Rules</b>					
<input type="checkbox"/>	Order	Description	MAC Address	IPv4 Address	Action
<input type="checkbox"/>	1	allow printer access	00:01:02:03:04:05	192.168.40.3	<a href="#">Edit</a> <a href="#">Clone</a>
<input type="checkbox"/>	2	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="button" value="Save"/> <input type="button" value="Cancel"/>
<a href="#">Create New</a> <input type="button" value="Delete"/>					
<input type="button" value="OK"/> <input type="button" value="Cancel"/>					
- Search terms:** A search bar with a dropdown menu set to 'Include all terms' and a radio button option for 'Include any of these terms'.
- Application Recognition and Filtering:** A section with a title and a footnote: '[1] This enables admin to define list of applications and application port maps and apply it to Clients later. This information is used for generating of pie'.

To apply a Client Isolation White List to a WLAN:

- 1 Go to **Configure > WLANs**.
- 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 *Configure > Access Control page*.
- 4 Click **OK** to save your changes.

Figure 91. Selecting a Client Isolation White List

The screenshot shows the 'Create New' configuration page for Client Isolation White Lists. The left sidebar contains a navigation menu with items like Maps, Roles, Users, Guest Access, Hotspot Services, Hotspot 2.0 Services, Mesh, AAA Servers, DHCP Relay, Alarm Settings, Services, WIPS, Certificate, Bonjour Gateway, and Location Services. The main content area is titled 'Create New' and contains several sections: General Options (Name/SSID, Description), WLAN Usages (Type: Standard Usage, Guest Access, Hotspot Service, Hotspot 2.0, Autonomous, Social Media), Authentication Options (Method: Open, 802.1x EAP, MAC Address, 802.1x EAP + MAC Address; Fast BSS Transition: Enable 802.11r FT Roaming), Encryption Options (Method: WPA2, WPA-Mixed, WEP-64, WEP-128, None), Options (Web Authentication: Enable captive portal), Authentication Server (Local Database, Create New), Wireless Client Isolation (Isolate wireless client traffic from other clients on the same AP, Isolate wireless client traffic from all hosts on the same VLAN/subnet), Zero-IT Activation™ (Enable Zero-IT Activation), and Priority (High, Low). The 'Wireless Client Isolation' section is highlighted, and the 'Isolate wireless client traffic from all hosts on the same VLAN/subnet' option is selected. A dropdown menu is open, showing 'No WhiteList' and 'whitelist' options. The 'whitelist' option is highlighted in blue. At the bottom of the page, there are 'Create New', 'Delete', and '1-1 (1)' buttons.

## Application Recognition and Filtering

The Application Recognition and Filtering features allow administrators to enhance ZoneDirector's built-in application identification capabilities and apply filtering policies to prevent users from accessing certain applications. These features allow administrators to perform the following tasks:

- [Configure User Defined Applications](#)
- [Configure Application Port Mapping](#)
- [Configure Application Denial Policies](#)

### Configure User Defined Applications

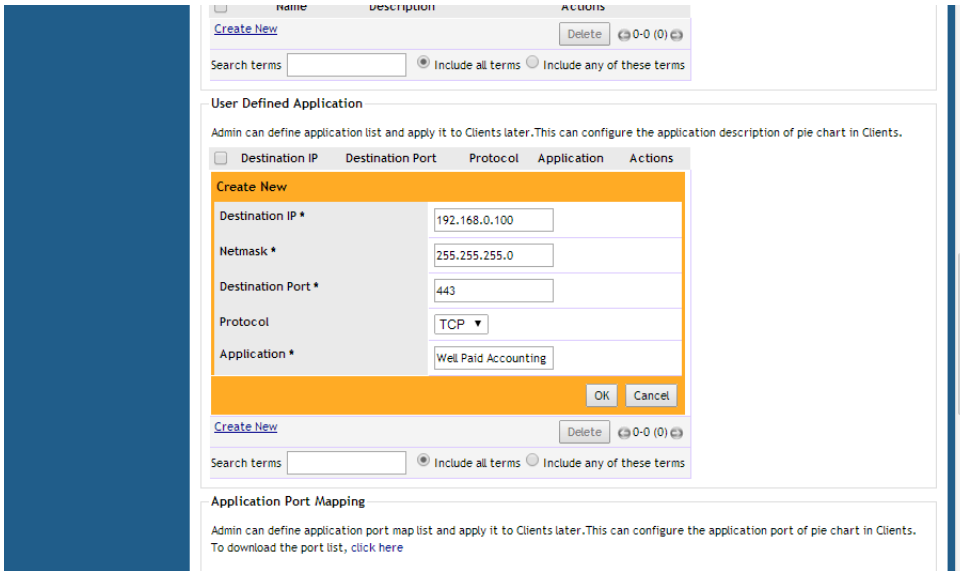
When an application is unrecognized and generically (or incorrectly) categorized, you can configure an explicit application identification policy by IP Address/Mask, Port and Protocol. Wireless traffic that matches a configured policy will be displayed using the policy's name on the Top 10 Applications widget on the Dashboard and the Applications pie charts/tables on the Wireless Clients monitoring page.

In case of a conflict, application identification policies are implemented according to the following priority order:

- 1 User Defined Applications
- 2 ZoneDirector embedded applications
- 3 Port Mapping application policies

[Figure 92](#) shows how to configure a 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 92. Defining custom applications for ZoneDirector identification



## Configure Application Port Mapping

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 widget on the Dashboard and Applications pie charts/tables on the Wireless Clients monitoring page. You can create new port-to-application name mappings individually, or you can batch upload a list in .csv format. Click the **click here** link to download a sample of the .csv file format.

This type of policy is the least granular in configuration and hence it has the lowest priority as a means of application identification. If for example you configure an Application Port Mapping Policy for port 80/TCP, any such matching wireless traffic not identified by either a User Defined Applications policy or ZoneDirector's embedded policies will be identified as belonging to this policy.

Figure 93 shows how an Application Port Mapping policy could be used to identify all port 8081 wireless traffic as "HTTP Proxy" traffic and display this name in application recognition pie charts and tables.

Figure 93. Application Port Mapping

The screenshot displays two configuration panels. The top panel, 'Application Port Mapping', includes a description, a 'Choose File' button, and a table with columns for Port, Protocol, Description, and Actions. A 'Create New' dialog box is open, showing fields for Port (8081), Protocol (TCP), and Description (HTTP Proxy), with OK and Cancel buttons. Below the table are search terms, radio buttons for 'Include all terms' and 'Include any of these terms', and a 'Delete' button with a count of 0-0. The bottom panel, 'Application Denial Policy', has a similar description and a table with columns for Name, Description, and Actions. A row for 'Facebook' is shown with a description of 'Deny Facebook' and 'Edit Clone' links. It also features search terms, radio buttons for 'Include all terms' and 'Include any of these terms', and a 'Delete' button with a count of 1-1 (1).

### ***Well-Known Service and Destination Port Mappings Defined in Application Visibility***

ZoneDirector automatically identifies several hundred applications for use in application recognition and denial policies. The following links provide lists of many the most 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](#)

## Configure Application Denial Policies

This option allows the administrator to deny application access by blocking any HTTP host name or L4 port. Using application denial policies, administrators can block specific applications if they are seen to be consuming excessive network resources, or enforce network usage policies such as blocking social media sites.

The following usage guidelines need to be taken into consideration when defining Application 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”.

### **Notes:**

- 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.
- 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.

#### ***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.

To create an Application Denial Policy:

- 1** Go to **Configure > Access Control**.
- 2** Expand the **Application Recognition and Filtering** section.
- 3** In *Application Denial Policy*, click **Create New** to create a new policy.

---

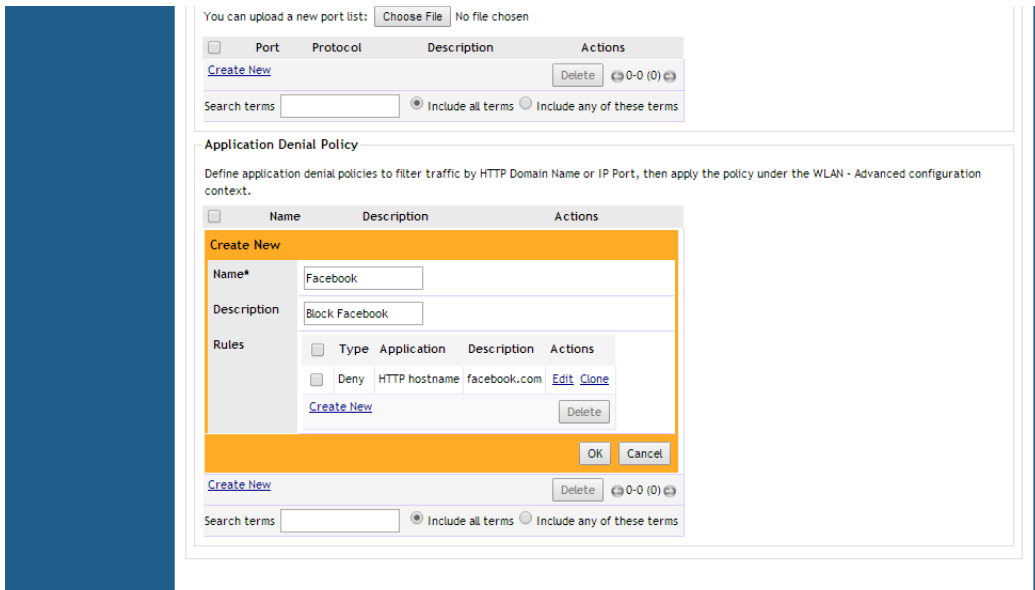
**NOTE:** Alternatively, you can create an Application Denial Policy from the WLAN creation page while creating a new WLAN or modifying an existing WLAN (**Configure > WLANs > Edit > Advanced Options > Application Visibility > Enable > Apply Policy Group > Create New.**)

---

- 4** Enter a **Name** and optionally a **Description** for the policy.
- 5** In *Rules*, click **Create New** to create a new rule for this policy.
- 6** In *Application*, Select **HTTP Domain Name** or **Port**.
- 7** In *Description*, enter the domain name or port number for the application you want to block.
- 8** Click **Save** to save the rule, and click **OK** to save the policy.



Figure 94. Blocking an application by HTTP host name



### ***Applying an Application Denial Policy to a WLAN***

Once an Application Denial Policy is created, use the following procedure to apply it to one or more WLANs:

- 1 Go to **Configure > WLANs**, and click **Edit** next to the WLAN you want to configure.
- 2 Expand the **Advanced Options** section, and locate the **Application Visibility** section.
- 3 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 95. Apply an Application Denial Policy to a WLAN

The screenshot displays a configuration page for a WLAN service. The left sidebar contains navigation options: Bonjour Gateway and Location Services. The main configuration area is divided into several sections:

- Authentication Server:** Local Database
- Wireless Client Isolation:** Includes checkboxes for isolating wireless client traffic from other clients on the same AP and from all hosts on the same VLAN/subnet. A 'No WhiteList' dropdown is present.
- Zero-IT Activation™:** Includes a checkbox for enabling Zero-IT Activation.
- Priority:** Radio buttons for High and Low.
- Advanced Options:** A collapsed section.
- Accounting Server:** Disabled, with a dropdown for Send Interim-Update every 10 minutes.
- Access Control:** Includes dropdowns for L2/MAC (No ACLs), L3/4/IP address (No ACLs), Device Policy (None), and Precedence Policy (Default). A checkbox for Enable Role based Access Control Policy is present.
- Application Visibility:** Includes a checked 'Enable' checkbox and an 'Apply policy group' dropdown set to 'deny Facebook'.
- Call Admission Control:** Includes a checkbox for Enforce CAC and a dropdown for deny Facebook.
- Rate Limiting:** Includes dropdowns for Uptlink (Disabled) and Downtlink (Disabled).
- Multicast Filter:** Includes a checkbox for Drop multicast packets from associated clients.
- VLAN Pooling:** Includes a dropdown for VLAN Pools List (None) and a 'Create a New VLAN Pool' button.
- Access VLAN:** Includes a dropdown for VLAN ID (1) and a checkbox for Enable Dynamic VLAN.
- Hide SSID:** Includes a checkbox for Hide SSID in Beacon Broadcasting (Closed System).
- Tunnel Mode:** Includes a checkbox for Tunnel WLAN traffic to ZoneDirector.
- Proxy ARP:** Includes a checkbox for Enable Proxy ARP.
- Background Scanning:** Includes a checkbox for Do not perform background scanning for this WLAN service.
- Load Balancing:** Includes a checked checkbox for Do not perform client load balancing for this WLAN service.
- Band Balancing:** Includes a checked checkbox for Do not perform Band Balancing on this WLAN service.

# 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 four types of AAA server:

- [Active Directory](#)
- [LDAP](#)
- [RADIUS / RADIUS Accounting](#)
- [TACACS+](#)

A maximum of 32 AAA server entries can be created, regardless of server type.

## Active Directory

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 against an Active Directory server in one of two ways:

- [Single Domain Active Directory Authentication](#)
- [Multi-Domain Active Directory Authentication](#)

## Single Domain Active Directory Authentication

To enable Active Directory authentication for a single domain:

- 1 Go to **Configure > 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 96. Enable Active Directory for a single domain

The screenshot shows the ZoneDirector web interface. The top navigation bar includes the Ruckus Wireless logo, the text "ZoneDirector - ZoneDirector", and a status bar with "2014/08/04 17:23:17 | Help | Toolbox | Log Out (ruckus)". Below the navigation bar are tabs for "Dashboard", "Monitor", "Configure", and "Administer". The left sidebar menu lists various system settings, with "AAA Servers" selected. The main content area is titled "Authentication/Accounting Servers" and contains a table listing authentication mechanisms. A "Create New" form is open, showing the following fields:

Name	Type	Actions
<b>Create New</b>		
Name	<input type="text" value="Ruckus AD"/>	
Type	<input checked="" type="radio"/> Active Directory <input type="radio"/> LDAP <input type="radio"/> RADIUS <input type="radio"/> RADIUS Accounting <input type="radio"/> TACACS+	
Global Catalog	<input type="checkbox"/> Enable Global Catalog support	
Encryption	<input type="checkbox"/> Enable SSL/TLS encryption	
IP Address*	<input type="text" value="192.168.11.17"/>	
Port*	<input type="text" value="389"/>	
Windows Domain Name	<input type="text" value="domain.ruckuswireless.com"/> (example: domain.ruckuswireless.com)	
		<input type="button" value="OK"/> <input type="button" value="Cancel"/>

Below the form, there is a "Create New" link, a "Delete" button, and a search bar with the text "Search terms" and radio buttons for "Include all terms" (selected) and "Include any of these terms".

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 **Configure > 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 *Configure > 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.

---

**NOTE:** Do NOT enter anything in the Windows Domain Name field. If you enter a Windows Domain Name, the search will be limited to that domain, rather than the whole 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.

---

**NOTE:** The Admin account need not have write privileges, but must be 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](#).

Figure 97. Active Directory with Global Catalog enabled

2014/08/04 17:24:17 | Help | Toolbox | Log Out (ruckus)

**Ruckus WIRELESS ZoneDirector - ZoneDirector**

Dashboard Monitor **Configure** Administer

**Authentication/Accounting Servers**

Authentication/Accounting Servers

This table lists all authentication mechanisms that can be used whenever authentication is needed.

Name	Type	Actions
<b>Create New</b>		
Name	Ruckus AD	
Type	<input checked="" type="radio"/> Active Directory <input type="radio"/> LDAP <input type="radio"/> RADIUS <input type="radio"/> RADIUS Accounting <input type="radio"/> TACACS+	
Global Catalog	<input checked="" type="checkbox"/> Enable Global Catalog support	
Encryption	<input type="checkbox"/> Enable SSL/TLS encryption	
IP Address*	192.168.11.17	
Port*	3268	
Windows Domain Name	domain.ruckuswireless.com (example: domain.ruckuswireless.com)	
Admin DN*	admin@domain.ruckus.com (example: admin@domain.ruckuswireless.com)	
Admin Password*	.....	
Confirm Password*	.....	

OK Cancel

## 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 **Configure > 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 Configure > 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](#).
- 

**NOTE:** The Admin account need not have write privileges, but must be able to read and search all users in the database.

---

Figure 98. Creating a new LDAP server object in ZoneDirector

The screenshot shows the ZoneDirector web interface with the 'Authentication/Accounting Servers' configuration page. The 'Create New' form is highlighted in orange and contains the following fields:

- Name:** Ruckus LDAP
- Type:** LDAP (selected)
- Encryption:**  Enable SSL/TLS encryption
- IP Address\*:** 192.168.11.17
- Port\*:** 389
- Base DN:** dc=idap,dc=com (example: dc=idap,dc=com)
- Admin DN:** uid=admin,dc=idap,dc= (example: uid=admin,dc=idap,dc=com)
- Admin Password:** [masked]
- Confirm Password:** [masked]
- Key Attribute:** uid (example: uid)
- Search Filter:** objectClass=\* (example: objectClass=Person, show more...)

Buttons for 'OK' and 'Cancel' are located at the bottom right of the form.

## 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 [Figure 99](#) below.



Figure 99. LDAP search filter syntax examples

**Create New**

Name: LDAP

Type:  Active Directory  LDAP  RADIUS  RADIUS Accounting

IP Address\*: 192.168.0.4

Port\*: 389

Base DN: (example: dc=idap,dc=com)

Admin DN: \*\*To query multiple OUs, enter an Admin DN and Password with full search and read privileges. (example: uid=admin,dc=idap,dc=com)

Admin Password:

Confirm Password:

Key Attribute: uid (example: uid)

Search Filter: objectClass=\* (example: objectClass=Person, show more...)

example1: &(attr1=value1)(attr2=value2), example2: !(&(attr1=value1)(attr2=value2))

Create New Delete 1-3 (3)

Search terms:  Include all terms  Include any of these terms

## Group Extraction

By using the Search Filter, you can extract the groups to which a user belongs, as categorized in your LDAP server. Using these groups, you can attribute Roles within 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 Configure > 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 Point ZoneDirector to your LDAP server:
  - Go to **Configure > AAA Servers**
  - Click **Edit** next to LDAP
  - Enter **IP address**, **Port** number, **Admin DN** and **Password**

- 2 Enter the **Key Attribute** (default: uid).
- 3 Click **OK** to save this LDAP server.
- 4 In *Test Authentication Settings*, enter the **User Name** and **Password** for a known member of the relevant group.
- 5 Click **Test**.
- 6 Note the Groups associated with this user.

Figure 100. Test authentication settings

**Test Authentication Settings**

You may test your authentication server settings by providing a user name and password here. Groups to which the user belongs will be returned and you can use them to configure the role.

Test Against: openDir

User Name: student1

Password: \*\*\*\*\* [Show Password]

Success! Groups associated with this user are student, workgroup. The user will be assigned a role of "Default".

[Test]

- 7 Go to **Configure > Roles**, and create a Role based on this User Group (see [Creating New User Roles](#)).
  - 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 **Configure > 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 Configure > 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* section to choose to test against the primary or the backup RADIUS server.

To configure a backup RADIUS / RADIUS Accounting server:

- 1 Click the check box next to **Enable Backup RADIUS support**.

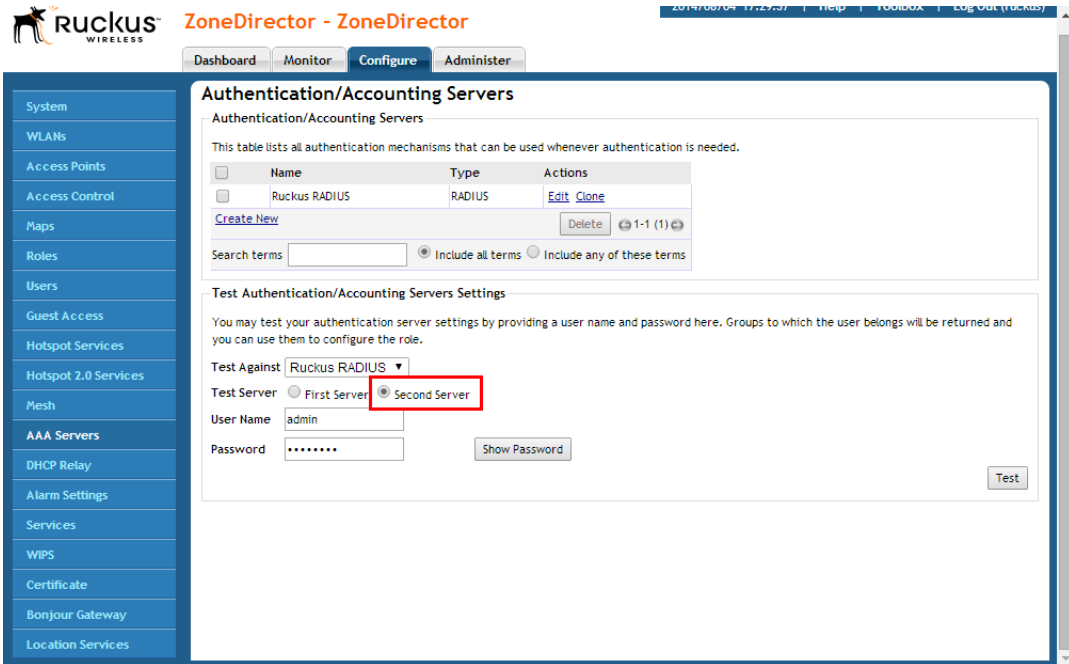
- 2 Enter the **IP Address**, **Port** number and **Shared Secret** for the backup server (these fields can neither be left empty nor be the same values as those of the primary server).
- 3 In **Request Timeout**, enter the timeout period (in seconds) after which an expected RADIUS response message is 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 101. Enable backup RADIUS server

The screenshot shows the configuration page for creating a new RADIUS server. The interface includes a sidebar on the left with navigation options like 'Access Points', 'Access Control', 'Maps', 'Roles', 'Users', 'Guest Access', 'Hotspot Services', 'Hotspot 2.0 Services', 'Mesh', 'AAA Servers', 'DHCP Relay', 'Alarm Settings', 'Services', 'WIPS', 'Certificate', 'Bonjour Gateway', and 'Location Services'. The main configuration area is titled 'Create New' and contains the following fields:

Name	Type	Actions
<b>Create New</b>		
Name	Ruckus RADIUS	
Type	<input type="radio"/> Active Directory <input type="radio"/> LDAP <input checked="" type="radio"/> RADIUS <input type="radio"/> RADIUS Accounting <input type="radio"/> TACACS+	
Encryption	<input type="checkbox"/> TLS	
Auth Method	<input checked="" type="radio"/> PAP <input type="radio"/> CHAP	
Backup RADIUS	<input checked="" type="checkbox"/> Enable Backup RADIUS support	
<b>First Server</b>		
IP Address*	192.168.11.17	
Port*	1812	
Shared Secret*	*****	
Confirm Secret*	*****	
<b>Second Server</b>		
IP Address*	192.168.11.18	
Port*	1812	
Shared Secret*	*****	
Confirm Secret*	*****	
<b>Retry Policy</b>		
Request Timeout*	3 seconds	
Max Number of Retries*	2 times	

Figure 102. Test authentication settings against 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 (**Configure > AAA Servers > RADIUS Server**). See [Using an External AAA Server](#).
- 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 **Configure > WLANs**.

- 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.

Figure 103. RADIUS authentication using MAC address

The screenshot shows the 'Create New' configuration page for a WLAN. The left sidebar contains a navigation menu with items like Roles, Users, Guest Access, Hotspot Services, Hotspot 2.0 Services, Mesh, AAA Servers, DHCP Relay, Alarm Settings, Services, WIPS, Certificate, Bonjour Gateway, and Location Services. The main content area is titled 'Create New' and has several sections:

- General Options:** Name/SSID\* (MAC Auth, ESSID: MAC Auth), Description.
- WLAN Usages:** Type (Standard Usage selected, Guest Access, Hotspot Service (WISPr), Hotspot 2.0, Autonomous).
- Authentication Options:** Method (MAC Address selected, Open, 802.1x EAP, 802.1x EAP + MAC Address).
- Encryption Options:** Method (None selected, WPA2, WPA-Mixed, WEP-64 (40 bit), WEP-128 (104 bit)).
- Options:** Authentication Server (RADIUS-MAC selected), MAC Address Format (aabbccddeeff selected), Wireless Client Isolation (No WhiteList selected), Zero-IT Activation™ (Enable Zero-IT Activation unchecked), Priority (High selected, Low).
- Advanced Options:** (indicated by a small icon).

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, clients configured with either “open” or EAP-MD5 authentication methods are both supported on the same WLAN. The encryption method is limited to “none,” and an external RADIUS server is required.



## 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. [Table 105](#) lists the attributes used in authentication, and [Table 18](#) lists those used in accounting.

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.

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***

Figure 105. RADIUS attributes used in authentication

<b>WLAN Type</b>	<b>Attributes</b>
802.1X/MAC Auth	<p>Sent from ZoneDirector in Access Request messages:</p> <ul style="list-style-type: none"> <li>(1) User name</li> <li>(4) NAS IP Address (optional; prefer sending NAS ID)</li> <li>(5) NAS Port</li> <li>(6) Service Type: hard-coded to be Framed-User(2)</li> <li>(12) Framed MTU: hard-coded to be 1400</li> <li>(30) Called Station ID: user configurable</li> <li>(31) Calling Station ID: format is sta's mac</li> <li>(32) NAS Identifier: user configurable</li> <li>(61) NAS Port Type: hard-coded to be 802.11 port (19)</li> <li>(77) Connection Info: indicates client radio type</li> <li>==&gt; (79) EAP payload</li> <li>==&gt; (24) State: if radius access-challenge in last received radius msg from AAA</li> <li>(80) Message Authenticator</li> <li>(95) NAS IPv6 address (if using/talking to an IPv6 RADIUS server)</li> </ul> <p>Ruckus private attribute:          Vendor ID: 25053          Vendor Type / Attribute Number: 3 (Ruckus-SSID)</p>

Figure 105. RADIUS attributes used in authentication

WLAN Type	Attributes
802.1X/MAC Auth	<p>Sent from RADIUS server in Access Accept messages:</p> <ul style="list-style-type: none"> <li>(1) User name</li> <li>(7) WISPr Bandwidth-Max-Up: Maximum transmit rate (bits/second)</li> <li>(8) WISPr Bandwidth-Max-Down: Maximum receive rate (bits/second)</li> <li>(25) Class</li> <li>(27) Session-timeout &amp; (29) Termination-action: Session-timeout event becomes a disconnect event or re-authentication event if termination-action indicates "(1) radius-request"</li> <li>(85) Acct-interim-interval</li> </ul> <p>For Dynamic VLAN application:</p> <ul style="list-style-type: none"> <li>(64) Tunnel-Type: value only relevant if it is (13) VLAN</li> <li>(65) Tunnel-Medium-Type: value only relevant if it is (6) 802 (as in all 802 media plus ethernet)</li> <li>(81) Tunnel-Private-Group-ID: this is the VLAN ID assignment (per RFC, this is between 1 and 4094)</li> </ul> <p>Administrator Authentication:</p> <p>Ruckus private attribute:</p> <p>Vendor ID: 25053</p> <p>Vendor Type / Attribute Number: 1 (Ruckus-User-Groups)</p> <p>Value Format: group_attr1, group_attr2, group_attr3, ...</p> <p>Cisco private attribute:</p> <p>Vendor ID: 9</p> <p>Vendor Type/ Attribute Number: 1 (Cisco-AVPair)</p> <p>Value Format: shell:roles="group_attr1 group_attr2 group_attr3 ..."</p>

Figure 105. RADIUS attributes used in authentication

<b>WLAN Type</b>	<b>Attributes</b>
WISPr / Web Auth / Guest Access	<p>Additional attributes supported in WISPr WLANs (**generic attributes NOT the same as non-WISPr/802.1X)</p> <ul style="list-style-type: none"> <li>(1) User name</li> <li>(2) Password or (3) CHAP-Password</li> <li>(4) NAS IP Address</li> <li>(6) Service Type: hardcoded to be Framed-User(2)</li> <li>(8) Framed IP address</li> <li>(30) Called Station ID: user configurable</li> <li>(31) Calling Station ID: format is sta's mac</li> <li>(32) NAS Identifier: user configurable</li> <li>(44) Account session ID</li> </ul> <p>Ruckus private attribute: Vendor ID: 25053 Vendor Type / Attribute Number: 3 (Ruckus-SSID) WISPr vendor specific attribute (vendor id = 14122)</p> <ul style="list-style-type: none"> <li>(1) WISPr location id</li> <li>(2) WISPr location name</li> <li>(4) WISPr redirection URL</li> <li>(7) WISPr Bandwidth-Max-Up: Maximum transmit rate (bits/second)</li> <li>(8) WISPr Bandwidth-Max-Down: Maximum receive rate (bits/second)</li> <li>(80) Message Authenticator</li> </ul>

### ***RADIUS Accounting attributes***

The following table lists attributes used in RADIUS accounting messages.

Table 18. 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)
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

Table 18. RADIUS attributes used in Accounting

<b>WLAN Type</b>	<b>Attribute</b>
802.1X/MAC Auth	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)

Table 18. RADIUS attributes used in Accounting

WLAN Type	Attribute
WISPr / Web Auth / Guest Access	<p>Common to Start, Interim Update, and Stop messages:</p> <ul style="list-style-type: none"> <li>(1) User name</li> <li>(2) Password</li> <li>(4) NAS IP address</li> <li>(5) NAS port</li> <li>(8) Framed-IP</li> <li>(30) Called station ID: user configurable</li> <li>(31) Calling station ID</li> <li>(32) NAS Identifier: user configurable</li> <li>(45) Acct authentic</li> <li>(50) Acct-Multi-Session-Id</li> <li>(61) NAS port type</li> <li>(77) Connection Info: indicates client radio type</li> </ul> <p>Ruckus private attribute: Vendor ID: 25053 Vendor Type / Attribute Number: 3 (Ruckus-SSID)</p> <p>Additional attributes supported in WISPr WLANs: WISPr vendor specific attributes (vendor id = 14122)</p> <ul style="list-style-type: none"> <li>(1) WISPr location id</li> <li>(2) WISPr location name</li> <li>(4) WISPr redirection URL</li> <li>(7) WISPr Bandwidth-Max-Up: Maximum transmit rate (bits/second)</li> <li>(8) WISPr Bandwidth-Max-Down: Maximum receive rate (bits/second)</li> </ul>

Table 18. RADIUS attributes used in Accounting

WLAN Type	Attribute
WISPr / Web Auth / Guest Access	<p>Specific to Interim Update and Stop messages:</p> <p>(42) Acct input octets</p> <p>(43) Acct output octets</p> <p>(44) Acct session ID</p> <p>(46) Acct session time</p> <p>(47) Acct input packets</p> <p>(48) Acct output packets</p> <p>(52) Acct input giga words</p> <p>(53) Acct output giga words</p> <p>(55) Event timestamp</p> <p>Ruckus private attribute:</p> <p>Vendor ID: 25053</p> <p>Vendor Type / Attribute Number: 2 (Ruckus-Sta-RSSI)</p> <p>Additional attributes supported in WISPr WLANs:</p> <p>WISPr vendor specific attributes (vendor id = 14122)</p> <p>(1) WISPr location id</p> <p>(2) WISPr location name</p>

## 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 On 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 106. On the Microsoft IAS page, right-click the user/group and select Properties.

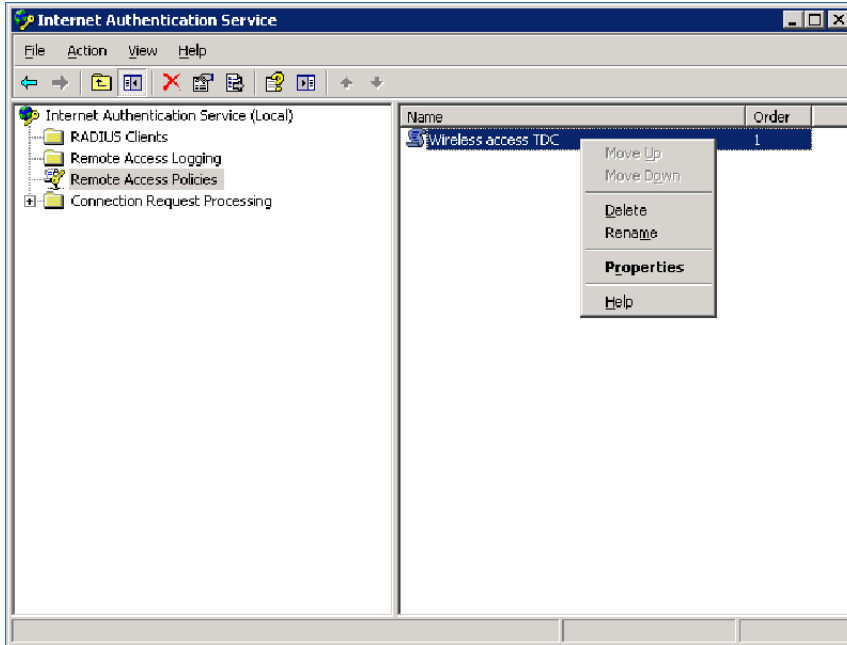




Figure 107. On the Properties page, click Edit Profile...

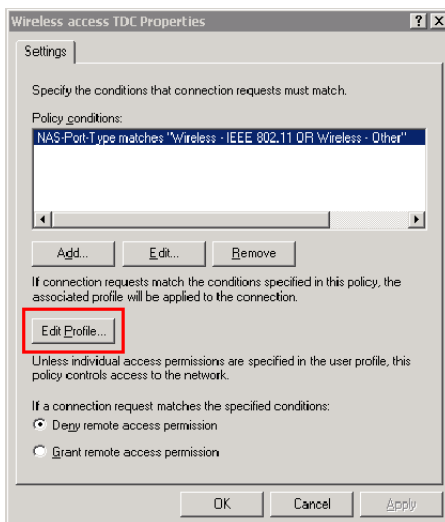
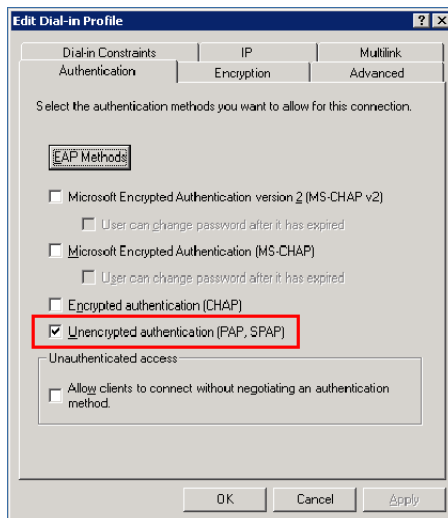


Figure 108. On the Authentication tab of the Edit Dial-in Profile dialog, select Unencrypted authentication (PAP, SPAP)



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 Configure > 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 **Configure > 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.

Figure 109. Configuring a TACACS+ AAA server

The screenshot shows the Ruckus ZoneDirector web interface. The top navigation bar includes the Ruckus logo, the text "ZoneDirector - ZoneDirector", and a status bar with the date "2014/08/04 17:35:15", "Help", "Toolbox", and "Log Out (ruckus)". Below the navigation bar are tabs for "Dashboard", "Monitor", "Configure", and "Administer". The left sidebar contains a menu with items: System, WLANs, Access Points, Access Control, Maps, Roles, Users, Guest Access, Hotspot Services, Hotspot 2.0 Services, Mesh, AAA Servers, DHCP Relay, Alarm Settings, Services, WIPS, Certificate, Bonjour Gateway, and Location Services. The main content area is titled "Authentication/Accounting Servers" and contains a table of existing servers. Below the table is a "Create New" form for configuring a TACACS+ server. The form fields are: Name (TACACS Plus), Type (radio buttons for Active Directory, LDAP, RADIUS, RADIUS Accounting, and TACACS+), IP Address\* (172.17.16.41), Port\* (49), Shared Secret\* (masked with dots), Confirm Secret\* (masked with dots), and TACACS+ Service\* (TACACS). At the bottom of the form are "OK" and "Cancel" buttons. Below the form is a "Create New" link, a "Delete" button, and a "1-1 (1)" indicator. At the bottom of the page is a "Test Authentication/Accounting Servers Settings" section with a text area for testing.

Name	Type	Actions
Ruckus RADIUS	RADIUS	<a href="#">Edit</a> <a href="#">Clone</a>

**Create New**

Name: TACACS Plus

Type:  Active Directory  LDAP  RADIUS  RADIUS Accounting  TACACS+

IP Address\*: 172.17.16.41

Port\*: 49

Shared Secret\*: .....

Confirm Secret\*: .....

TACACS+ Service\*: TACACS

OK Cancel

Create New Delete 1-1 (1)

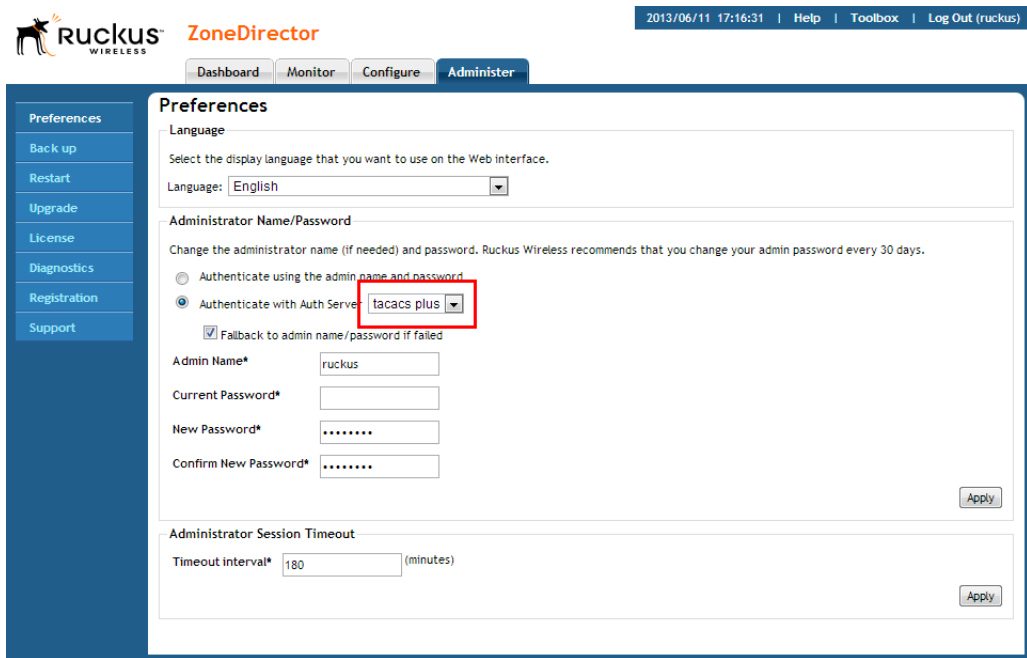
Search terms:   Include all terms  Include any of these terms

**Test Authentication/Accounting Servers Settings**

You may test your authentication server settings by providing a user name and password here. Groups to which the user belongs will be returned and you can use them to configure the role.

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.

Figure 110. Select TACACS+ for ZoneDirector administrator authentication



The screenshot shows the Ruckus ZoneDirector Administrator web interface. At the top, there is a navigation bar with the Ruckus logo, the text 'ZoneDirector', and a status bar showing '2013/06/11 17:16:31 | Help | Toolbox | Log Out (ruckus)'. Below this is a menu with 'Dashboard', 'Monitor', 'Configure', and 'Administer'. The 'Administer' tab is active, leading to the 'Preferences' page. On the left, a sidebar contains links for 'Preferences', 'Back up', 'Restart', 'Upgrade', 'License', 'Diagnostics', 'Registration', and 'Support'. The main content area is titled 'Preferences' and contains several sections: 'Language' (set to English), 'Administrator Name/Password' (with 'Authenticate with Auth Server' selected and 'tacacs plus' in the dropdown), and 'Administrator Session Timeout' (set to 180 minutes). The 'Admin Name' field contains 'ruckus'.

## 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.

---

**NOTE:** 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 **Configure > 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.

## Using an External AAA Server

RADIUS / RADIUS Accounting

# Managing a Wireless Local Area Network

# 4

In this chapter:

- [Overview of Wireless Networks](#)
- [About Ruckus Wireless WLAN Security](#)
- [Creating a WLAN](#)
- [Creating a Copy of an Existing WLAN for Workgroup Use](#)
- [Customizing WLAN Security](#)
- [Working with WLAN Groups](#)
- [Deploying ZoneDirector WLANs in a VLAN Environment](#)
- [Working with Hotspot Services](#)
- [Creating a Hotspot 2.0 Service](#)
- [Working with Dynamic Pre-Shared Keys](#)
- [Bypass Apple CNA](#)

## Overview of Wireless Networks

Once you have completed the ZoneDirector Setup Wizard, you have a fully functional wireless network, based on two secure WLANs (if you enabled the optional guest WLAN) with access for authorized users and guests. The default WLAN provides Zero-IT connectivity to allow users to automatically provision their client devices with WLAN settings the first time they connect. The guest WLAN provides visitors to your organization with a connection to the Internet, but not to your internal corporate network.

There are several scenarios in which you will want to create additional WLANs, in addition to the default internal and guest WLANs:

- 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 for wireless devices that only support WEP-key encryption.
- To create special WLANs with different settings for specific purposes. For example, a VoIP WLAN for voice traffic with Background Scanning and load balancing disabled, or a student WLAN that is only available during school hours.

In the first scenario, specific WLANs (esp. regarding authentication and encryption algorithm) can be set up that support specific groups of users. This requires a two-step process: (1) create the custom WLAN and link it to qualified user accounts by “roles,” and (2) assist all qualified users to prepare their client devices for custom WLAN connection.

As a result, you will have the default 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:

Figure 111. Max WLANs by ZoneDirector model

Model	Max WLANs
ZoneDirector 1200	256
ZoneDirector 3000	1024
ZoneDirector 5000	2048



On single and dual-band 802.11n APs, the maximum number of service WLANs deployable per AP radio is 27. These APs support maximum 32 SSIDs per radio, but five are reserved (two mesh SSIDs and one each for monitor, recovery and scan). 802.11ac APs support up to 27 service WLANs on the 2.4 GHz radio and 13 service WLANs on the 5 GHz radio.

---

**CAUTION!** Deploying a large number of WLANs per AP will have a performance impact. Ruckus Wireless recommends deploying no more than eight WLANs per AP radio.

---

## About Ruckus Wireless 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, WEP or no encryption. Open authentication/WPA2 encryption WLANs (also known as WPA-Personal) are the most common type of WLAN and should be the default configuration if there are no special requirements for authentication or encryption.

The 802.1X EAP (WPA-Enterprise) authentication method provides effective authentication regardless of whether you deploy WEP, WPA2 or no encryption, and requires a back-end authentication server.

You can also choose to authenticate clients by MAC address. MAC address 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.)

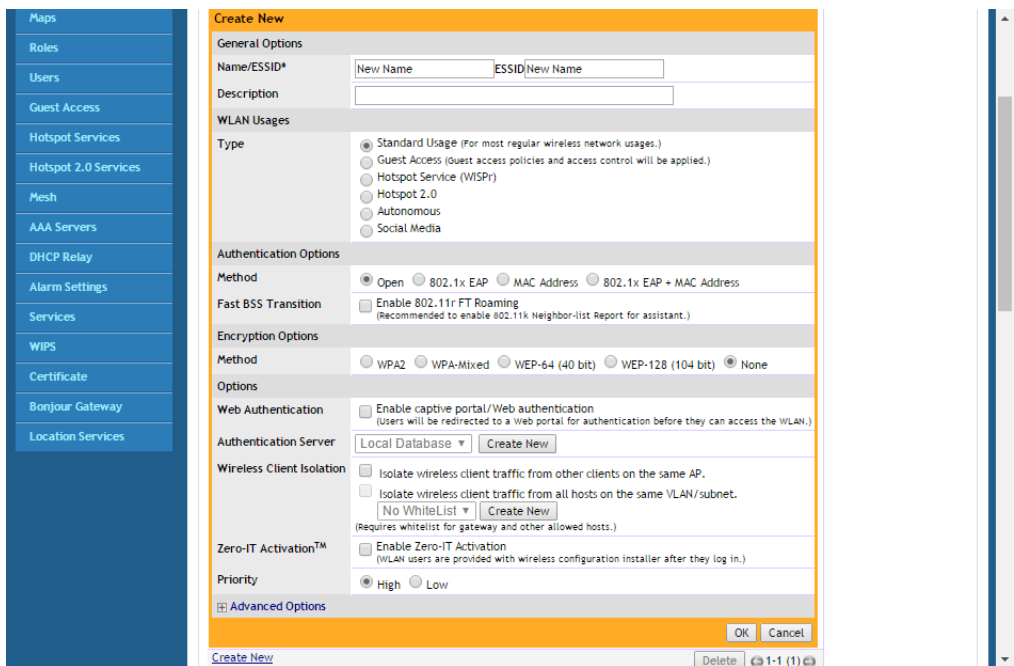
All client authentication options (Open, 802.1X, MAC, and 802.1X+MAC) are detailed in [Creating a WLAN](#), and you can learn how to apply them to your WLANs in the same section.

## Creating a WLAN

To create a new WLAN:

- 1 Go to **Configure > WLANs**. The first table displays all WLANs that have already been created in ZoneDirector.
- 2 In the top section (WLANs), click **Create New**. The *Create New* workspace displays the following:

Figure 112. Creating a new WLAN



The WLAN *Create New* workspace includes the following configuration options used to customize your new WLAN. The individual options are explained in detail in the next section, beginning with [General Options](#).

Table 19. Create new WLAN options

Option	Description
General Options	Enter WLAN name and description.
WLAN Usages	Select usage type (standard, guest access, hotspot, autonomous, social media).
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, WPA-Mixed, WEP, or None), encryption algorithm (AES or Auto AES+TKIP) and enter a WPA passphrase/WEP key.
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.

- 3 When you finish, click **OK** to save the entries. This WLAN is ready for use.
- 4 You can now select from these WLANs when assigning roles to users, as detailed in [Creating New User Roles](#).

## 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 five 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](#)). Guest WLANs are subject to guest access policies, such as redirection and subnet access restrictions.

---

**CAUTION!** When Guest Access or Wireless Client Isolation (below) is enabled, the SpeedFlex Wireless Performance tool may not function properly. 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. Before using SpeedFlex, verify that both Guest Access and Wireless Client Isolation options are disabled. For more information on SpeedFlex, refer to [Measuring Wireless Network Throughput with SpeedFlex](#).

---

- **Hotspot Service (WISPr):** Create a Hotspot WLAN. A Hotspot service must first have been created (Configure > Hotspot Services) before it will be available for selection. See [Creating a Hotspot Service](#).

- **Hotspot 2.0:** Create a Hotspot 2.0 WLAN. A Hotspot 2.0 Operator must first have been created (Configure > Hotspot 2.0 Services) before it will be available for selection. See [Creating a Hotspot 2.0 Service](#).
- **Autonomous:** Autonomous WLANs are special WLANs designed to continue providing service to clients when APs are disconnected from ZoneDirector. See [Autonomous WLANs](#).
- **Social Media:** Social Media WLANs require the visitor to log in using a social media account before being allowed Internet access. See [Social Media WLANs](#).

## 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 (*Configure > 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.

## Social Media WLANs

Social Media WLANs allow guest users to access the Internet using a social media

account instead of using a WPA password or Guest Pass to login. The following social media login methods are currently supported:

- Facebook
- Google/Google+
- LinkedIn
- Microsoft Windows Live

### ***About the Ruckus Wireless Facebook WiFi Implementation***

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

The business owner can also display advertisements and other announcements on this Facebook page, and can control the guest session length and other options using the Facebook WiFi configuration panel. For more information, see the [Facebook WiFi Help Center](#).

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

- The maximum number of Social Media WLANs that can be created per Zone-Director is four.
- 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 4 times. If there is no response after five requests, ZoneDirector will delete the related stations.

To enable a Facebook WiFi WLAN:

- 1 Go to **Configure > WLANs**.
- 2 Click **Create New** to create a a new WLAN.
- 3 Under *WLAN Usages: Type*, select **Social Media**.
- 4 Under *Social Media Login*, select **Facebook**, and click the **Configure** button.
- 5 A new browser window opens to allow you to log into your Facebook account.
- 6 Configure the Facebook WiFi settings according to your preferences:

- a *Facebook Page*: If you have multiple Facebook Pages, select the one that is associated with your business's location.
  - b *Bypass Mode*: Choose whether customers can use a WiFi code that you give them or click on a link to skip checking in.
  - c *Session Length*: Configure the length of time to allow guests to access the network without having to check in again.
  - d *Terms of Service*: Select whether to display and require users to accept a Terms of Service agreement.
  - e Click **Save Settings**.
- 7 Click **OK** to save this WLAN.

Figure 113. Configure a Facebook WiFi WLAN

The screenshot shows the 'Create New' configuration page for a WLAN. The left sidebar contains a navigation menu with items like Maps, Roles, Users, Guest Access, Hotspot Services, Hotspot 2.0 Services, Mesh, AAA Servers, DHCP Relay, Alarm Settings, Services, WIPS, Certificate, Bonjour Gateway, and Location Services. The main content area is titled 'Create New' and contains the following sections:

- General Options**: Name/ESSID\* (Ruckus Facebook), ESSID (Ruckus Facebook), Description (Facebook WiFi WLAN).
- WLAN Usages**: Type (Social Media selected, others: Standard Usage, Guest Access, Hotspot Service (WISPr), Hotspot 2.0, Autonomous).
- Authentication Options**: Method (Open selected, others: 802.1x EAP, MAC Address, 802.1x EAP + MAC Address). Fast BSS Transition (Enable 802.11r FT Roaming).
- Encryption Options**: Method (None selected, others: WPA2, WPA-Mixed, WEP-64 (40 bit), WEP-128 (104 bit)).
- Options**: Social Media Login (Facebook WiFi selected, Configure button).
- Wireless Client Isolation**: Isolate wireless client traffic from other clients on the same AP. Isolate wireless client traffic from all hosts on the same VLAN/subnet. (No WhiteList selected, Create New button).
- Priority**: High selected, Low.
- Advanced Options**: Expanded section.

Buttons: OK, Cancel, Create New, Delete, Search terms, Include all terms, Include any of these terms.

### ***Other Social Media Types***

For other Social Media login methods, you must enter an **Application ID** and **Application Secret**. 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.

The other 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>.

### ***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.

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

---

**NOTE:** Alternatively, you can click the **Click here to create a new application/project** link from within the ZoneDirector web interface, WLAN creation screen, which appears after you have selected a **Social Media Login** type.

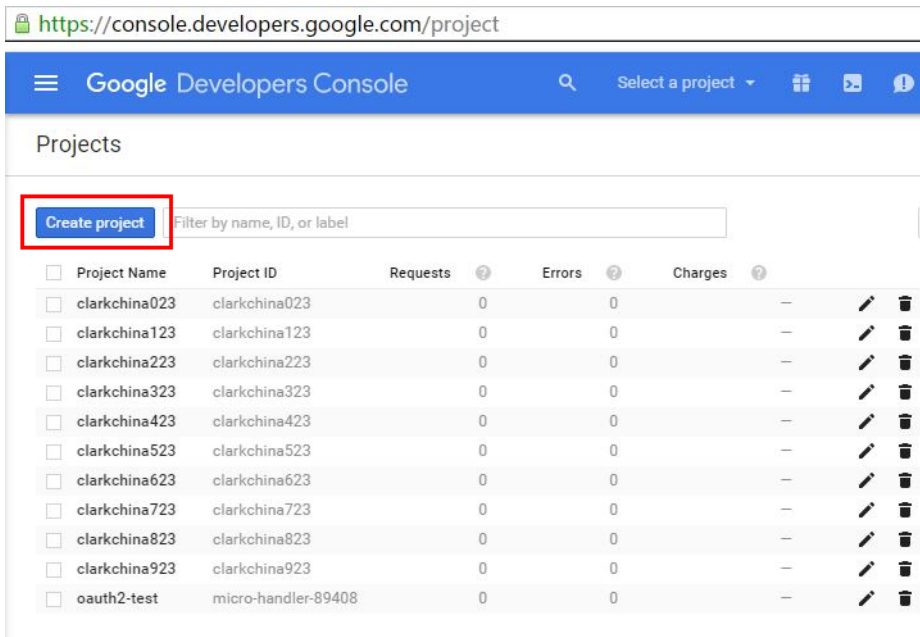
---



Figure 114. Click here link from within ZD WLAN creation screen

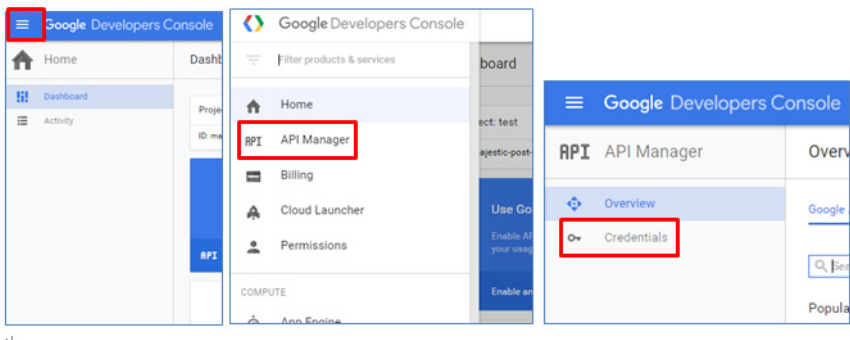
The screenshot displays the 'Create New' configuration page for a WLAN. On the left is a navigation menu with items like Maps, Roles, Users, Guest Access, Hotspot Services, Mesh, AAA Servers, DHCP Relay, Alarm Settings, Services, WIPS, Certificate, Bonjour Gateway, and Location Services. The main content area is titled 'Create New' and contains several sections: 'General Options' with fields for Name/ESSID\* (Ruckus Google) and Description (Google WLAN); 'WLAN Usages' with radio buttons for Standard Usage, Guest Access, Hotspot Service (WISPr), Hotspot 2.0, Autonomous, and Social Media (selected); 'Authentication Options' with radio buttons for Open, 802.1x EAP, MAC Address, and 802.1x EAP + MAC Address (Open is selected); 'Encryption Options' with radio buttons for WPA2, WPA-Mixed, WEP-64 (40 bit), WEP-128 (104 bit), and None (None is selected); 'Social Media Login' with a dropdown menu set to 'Google/Google+' and a red-bordered link 'Click here to create new application/project'; 'Wireless Client Isolation' with checkboxes for isolating traffic from other clients and all hosts on the same VLAN/subnet; and 'Priority' with radio buttons for High and Low. At the bottom, there are 'OK' and 'Cancel' buttons, and a search bar with 'Include all terms' selected.

Figure 115. 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 116. How to get to the Credentials page



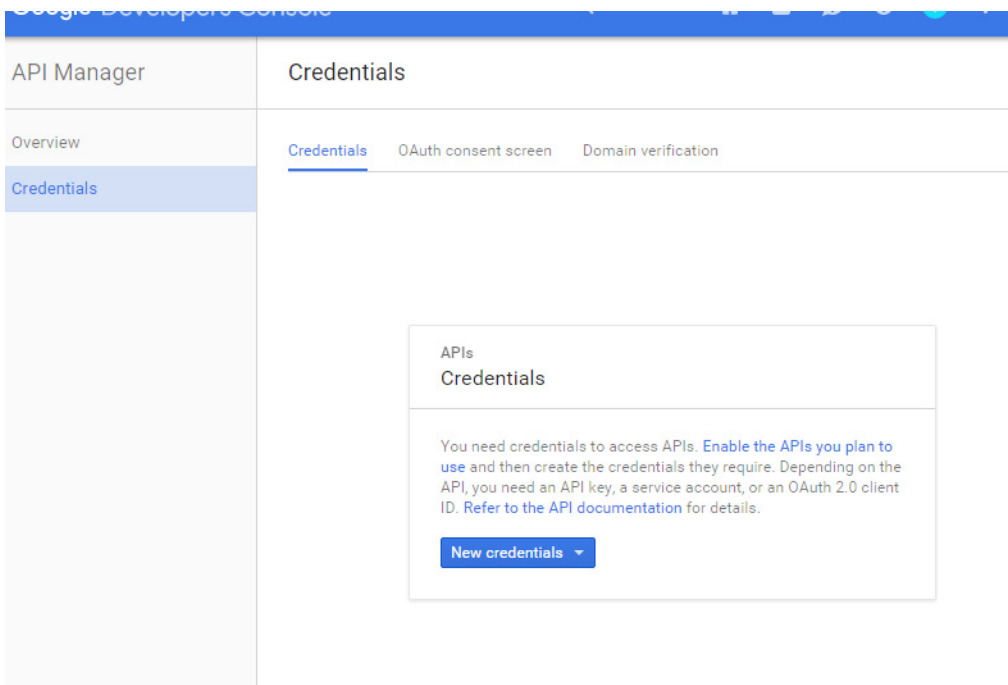
---

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

---

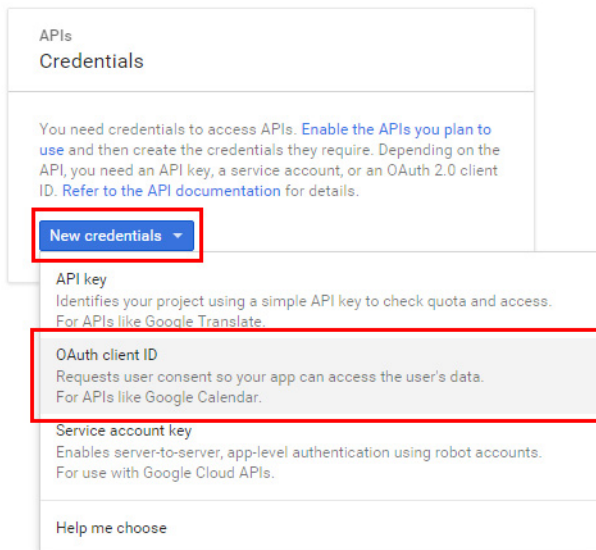
3 The *Credentials* page appears, as shown below.

Figure 117. Credentials page



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

Figure 118. 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”.

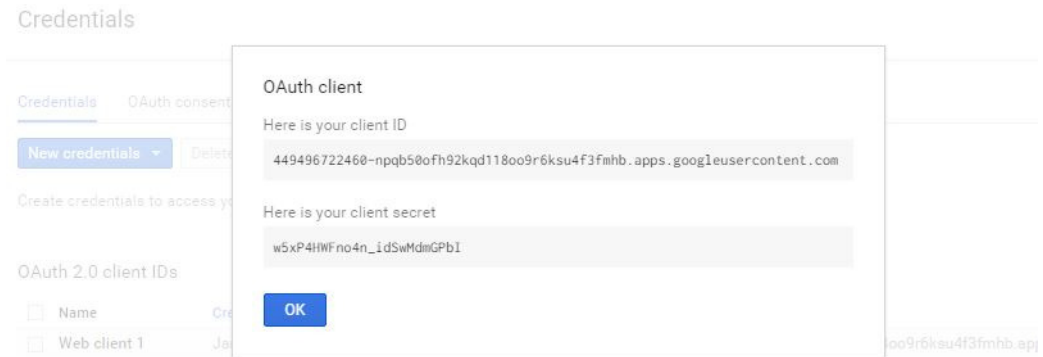
---

Figure 119. Select Web application and enter Authorized redirect URI

The screenshot shows the 'Credentials' configuration page. At the top left, there is a navigation pane with 'anager' visible. The main content area is titled 'Credentials' and includes a back arrow icon. Below the icon is the 'Create client ID' section. Under 'Application type', the 'Web application' radio button is selected and highlighted with a red box. Other options include 'Android Learn more', 'Chrome App Learn more', 'iOS Learn more', 'PlayStation 4', and 'Other'. The 'Name' field contains 'Web client 1'. The 'Restrictions' section has a sub-section 'Authorized JavaScript origins' with a text input field containing 'http://www.example.com'. Below that, the 'Authorized redirect URIs' section is highlighted with a red box and contains a text input field with 'http://zd.ruckuswireless.com/user/auth.jsp'. At the bottom, there are 'Create' and 'Cancel' buttons.

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

Figure 120. OAuth Client ID and Client Secret

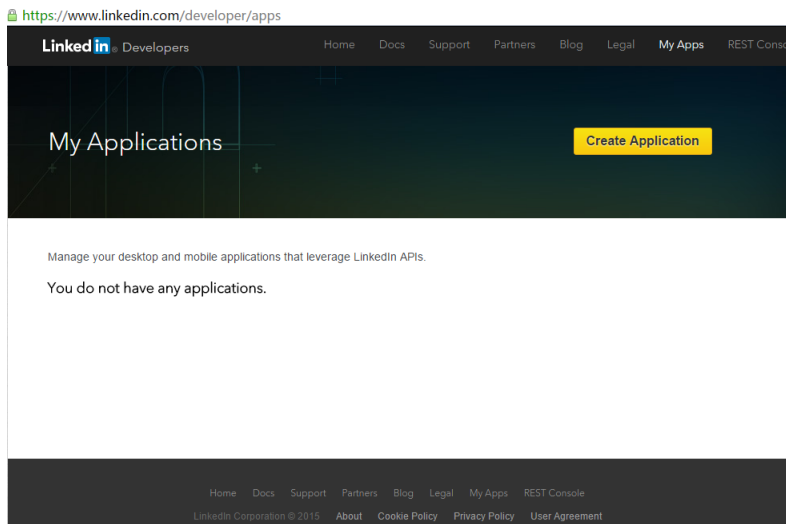


- 7 Take note of the Client ID and Client Secret. You will need to enter these values into the ZoneDirector web interface.
- 8 Continue to [Create an OAuth 2.0 WLAN on ZoneDirector](#).

### ***OAuth Setup Procedure for LinkedIn Social Media Login***

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

Figure 121. LinkedIn *My Applications* page



- 2 Click **Create application**.
- 3 Enter the required application information and click **Submit**.

Figure 122. Create a New LinkedIn Application


Create a New Application

Company Name: \*  
Create a new Company ▼

Company Name: \*

Name: \*

Description: \*

Application Logo: \*  


Application Use: \*  
Select One... ▼

Website URL: \*

Business Email: \*

Business Phone: \*

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

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

---

**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 123. LinkedIn Authentication Keys

## Authentication Keys

Client ID: 756d9w65yzy52n

Client Secret: jdFAZ3geOV9yiBbQ

## Default Application Permissions

r\_basicprofile

r\_emailaddress

rw\_company\_admin

w\_share

## OAuth 2.0

### Authorized Redirect URLs:

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

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

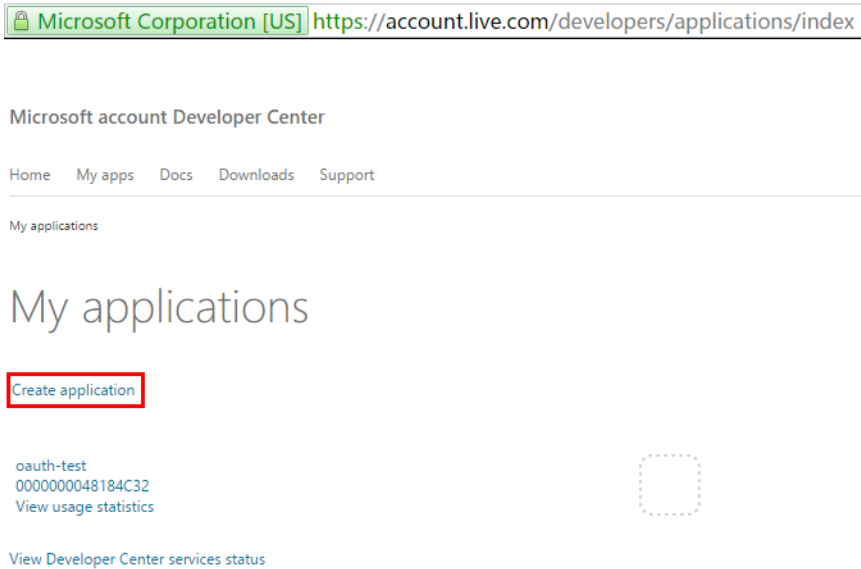
- 1 Go to the following URL to launch Microsoft Live development dashboard and create an application: <https://account.live.com/developers/applications/index>.
- 2 Click **Create application**.

---

**NOTE:** If you have not previously created any projects, you will be redirected to the application creation page directly.

---

Figure 124. Microsoft My Applications page



- 3 Enter an **Application name** and select a **Language**, then click **I accept** to create a new application.

Figure 125. Enable your application to use Microsoft accounts

Microsoft account Developer Center

Home My apps Docs Downloads Support

---

My applications

## Enable your application to use Microsoft accounts

This site will allow your web-based Android and iOS applications to authenticate users via Microsoft accounts.

**If you want to register an application for Windows 8.1 or Windows Phone 8.1, go to the [Windows Store Dashboard](#) instead.**

Provide the name of your application that users will see.

Application name\*

Language\*

Use letters, dig  
limit.

Select your ap

Clicking **I accept** means that you agree to the Microsoft services [terms of use](#). Read [Privacy & Cookies](#).

**I accept** **Cancel**

- 4 Provide a valid redirect callback URL “<http://zd.ruckuswireless.com/user/auth.jsp>”.

---

**NOTE:** If you have imported a certificate with FQDN to ZoneDirector, you should use the real FQDN instead of “[zd.ruckuswireless.com](http://zd.ruckuswireless.com)”. For example, if the FQDN is “[mydomain.com](http://mydomain.com)”, the *Authorized redirect URIs* should be “<http://mydomain.com/user/auth.jsp>”.

---

Figure 126. Enter the callback URL

Microsoft account Developer Center xuepeng.jiang | Sign out

Home My apps Docs Downloads Support

My applications > oauth-test > API Settings

## oauth-test

Settings

- Basic Information
- API Settings**
- App Settings
- Localization

Mobile or desktop client app:  
 Yes  No

Mobile client applications use a different OAuth 2.0 authentication flow. Selecting Yes will allow mobile clients to use this authentication flow. [Learn More](#)

Target domain:

This is the domain that other apps will use when they request a JWT for your app on Windows (such as www.contoso.com).

Restrict JWT issuing:  
 Yes  No

Limits the issuing of JSON Web Tokens (JWT) for your domain to exclusively this application.

Root domain:  
**zd.ruckuswireless.com**

All redirect URLs must fall within your root domain.

Redirect URLs:  
  
[Add another redirect URL](#)

Specify the exact URL you will be redirecting users to (such as http://www.contoso.com/redirect). You must provide at least one redirect URL.

For client secret and PSID information, select App Settings.

- 5 Microsoft will provide you **Client ID** and **Client secret**. Take note of these values, as you will need to enter them into the ZoneDirector web interface later.

Figure 127. Microsoft Client ID and Client secret

#### API Settings

Mobile or desktop client app:  
No

Restrict JWT issuing:  
Yes

Enhanced redirection security:  
Enabled

Target domain:

Redirect URLs:  
<http://zd.ruckuswireless.com/user/auth.jsp>

#### App Settings

Client ID:  
000000004C153DD4

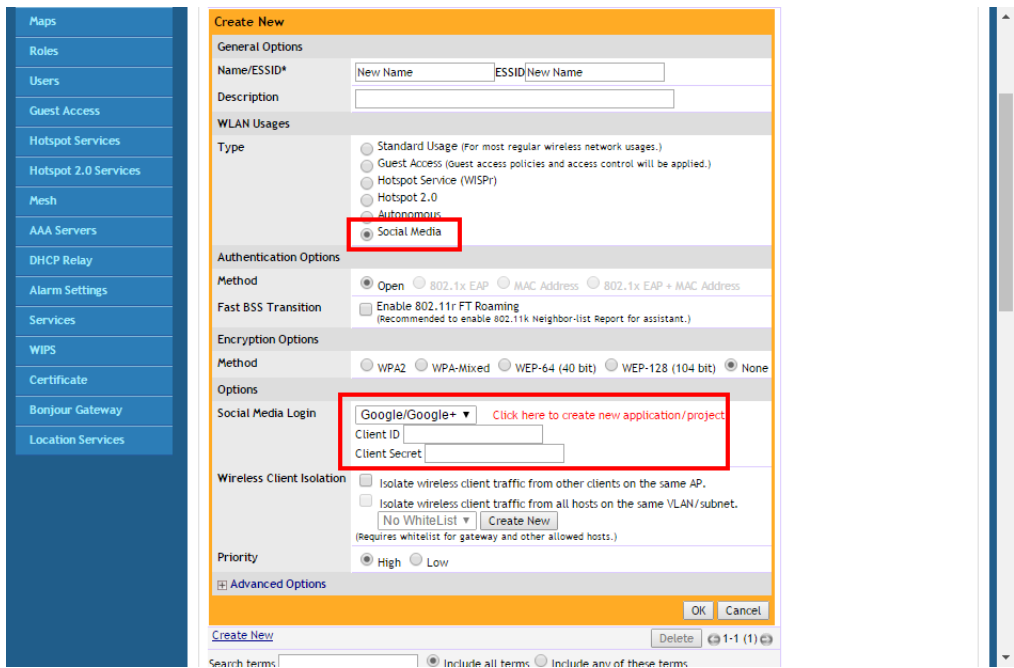
Client secret:  
HppXca7pjKXePrcSMSWpgT8O1M2gL4tZ

### ***Create an OAuth 2.0 WLAN on ZoneDirector***

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

- 1 Go to **Configure > WLANs** and create a WLAN.
- 2 In the **Type** option, select **Social Media**.
- 3 In the **Social Media Login** option, select an OAuth 2.0 provider, for example Google OAuth 2.0.
- 4 Input the **Client ID** and **Client Secret**.
- 5 Click **OK** to save your changes.

Figure 128. Creating an OAuth 2.0 Social Media WLAN on ZoneDirector

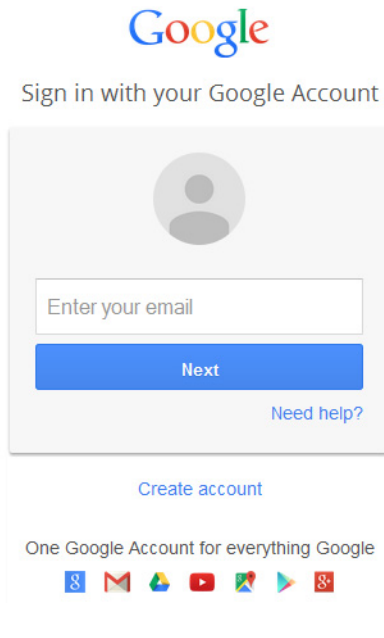


### ***User Login to Social Media WLAN***

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

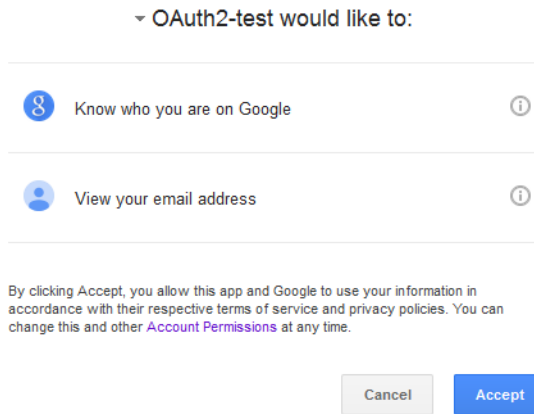
- 1 Connect to an OAuth 2.0 wlan; (for example Google OAuth 2.0 wlan)
- 2 Launch your web browser and attempt to visit any HTTP or HTTPS web page.
- 3 ZoneDirector will redirect the user to the Login page.

Figure 129. Google Login page



- 4 Enter login details and authenticate. After authentication, the end user will see the following screen.

Figure 130. 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.

## 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 dictated by the WLAN type.

ZoneDirector provides the following authentication method options:

- *Open* [Default]: No authentication mechanism is applied to connections. Any encryption method can be used.
- *802.1X/EAP*: Uses 802.1X authentication against a user database.
- *MAC Address*: Uses the device’s MAC address for both the user name and password.
- *802.1X EAP + MAC Address*: Allows the use of both authentication methods on the same WLAN. See [Using 802.1X EAP + MAC Address Authentication](#).

## 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.



## Encryption Options

Encryption choices include WPA2, WPA-Mixed, WEP-64, WEP-128 and None. WPA2 is the only encryption method certified by the WiFi Alliance and is the recommended method.

WEP has been proven to be easily circumvented, and Ruckus Wireless recommends against using WEP if possible.

### Method

- *WPA2*: Enhanced WPA encryption that complies with the 802.11i security standard.
- *WPA-Mixed*: Allows mixed networks of WPA and WPA2 compliant devices. Use this setting if your network has a mixture of older clients that only support WPA and TKIP, and newer client devices that support WPA2 and AES. *\*\*Note that selection of WPA-Mixed disables the ability to use Zero-IT for this WLAN.*
- *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.

---

**CAUTION!** If you set the encryption method to WEP-64 (40 bit) or WEP-128 (104 bit) and you are using an 802.11n or 802.11ac AP for the WLAN, the WLAN will operate in 802.11g mode.

---

### ***Algorithm (Only for WPA2 or WPA-Mixed encryption methods)***

- *AES*: This algorithm provides enhanced security over TKIP, and is the only encryption algorithm supported by the 802.11i standard. Choose AES encryption if you are confident that all of your clients will be using 802.11i-compliant NICs.
- *Auto*: 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 and you are using an 802.11n or 802.11ac AP for the WLAN, 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.

---

### ***WEP Key/Passphrase***

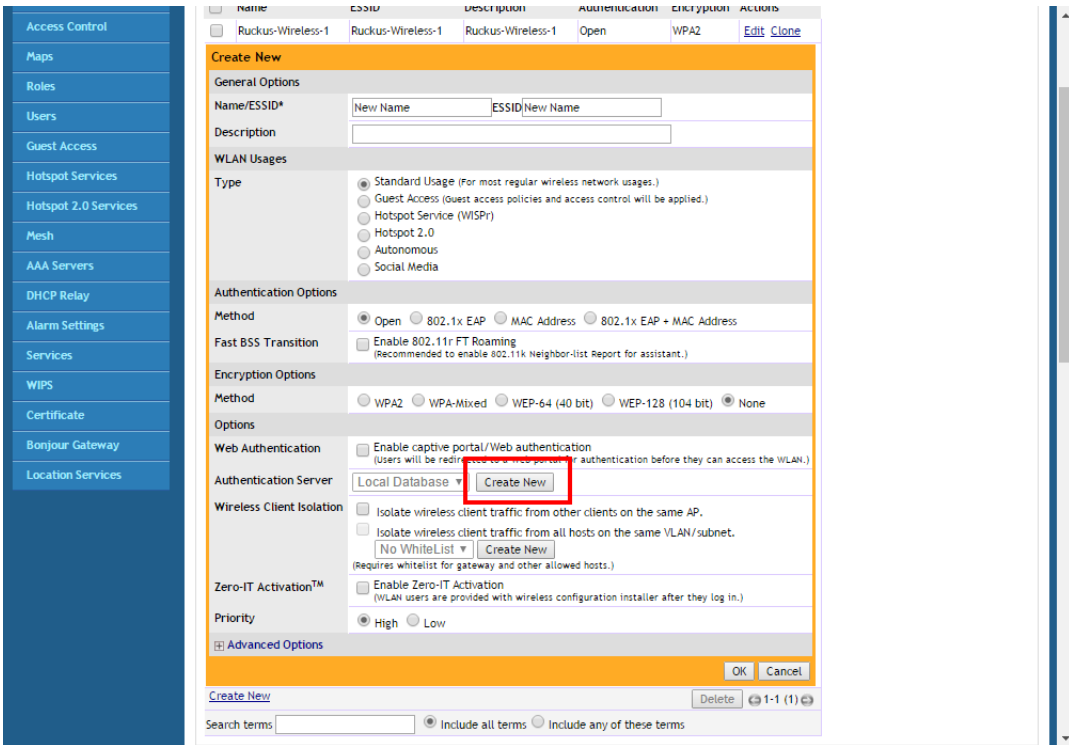
- *WEP Key:* WEP methods only. Click in the Hex field and type the required key text. If the key is for WEP-64 encryption, the key text must consist of 10 hexadecimal characters. If it is for WEP-128 encryption, enter a key 26 characters in length. Alternatively, click Generate to have ZoneDirector automatically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

## **Options**

- *Web Authentication:* [Available only with “Open” authentication.] Click the check box to require all WLAN users to complete a web-based login to this network each time they attempt to connect (see [Activating Web Authentication](#)).
- *Authentication Server:* When “Web Authentication” is active, use this option to designate the server used to authenticate web-based user login. 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, RADIUS server, Active Directory and LDAP. 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 **Configure > AAA Servers** page (see [Using an External Server for User Authentication](#)).

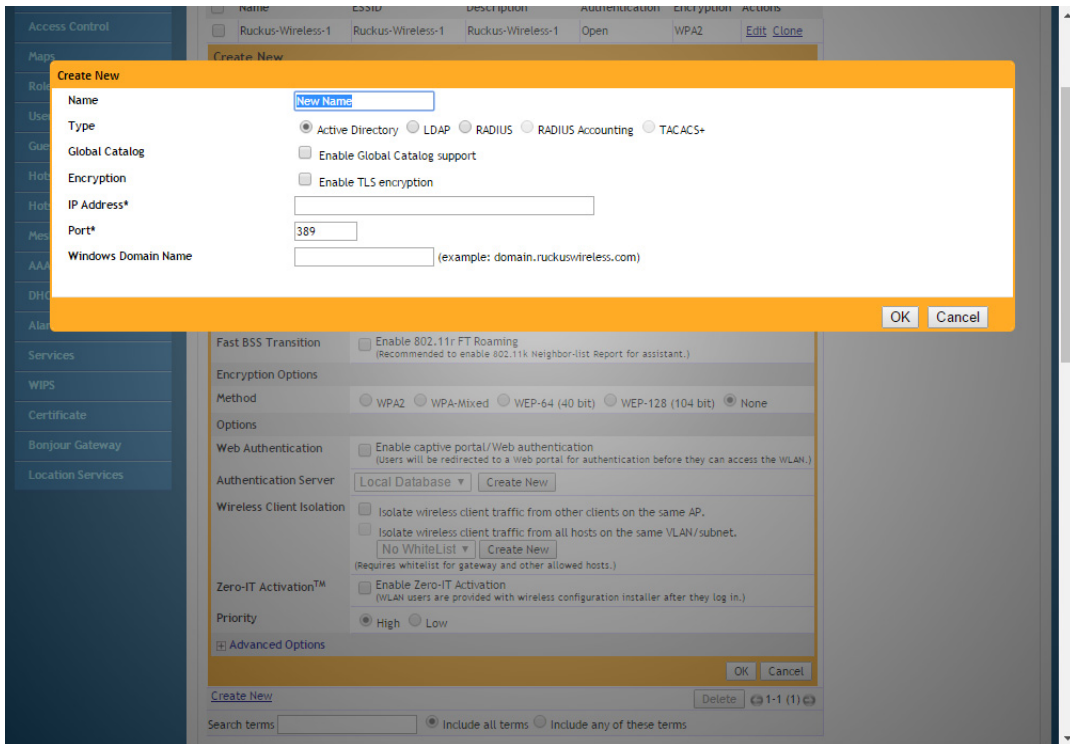
Alternatively, click the **Create New** button to create a new AAA server object from within the WLAN configuration screen.

Figure 131. Click Create New to create a new AAA server



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

Figure 132. AAA server popup



- *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 *Configure > Access Control* page before appearing here (see [Configuring Client Isolation White Lists](#)).
- *Zero-IT Activation:* Enable this option to activate ZoneDirector's share in the automatic “new user” process, in which the new user's wireless device is easily and quickly configured for WLAN use. For more information, see [Enabling Automatic User Activation with Zero-IT](#).
- *Dynamic PSK:* Dynamic PSK is available when you have enabled Zero-IT Activation. When a client is activated, ZoneDirector provisions the user with a pre-shared key. This per-user key does not expire by default. If you want to set an expiration for Dynamic PSKs, you can do so from the drop-down menu further down the page. For more information, see [Working with Dynamic Pre-Shared Keys](#).
- *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.

## Advanced 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.

- *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 Interim-Update 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.
- *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 [Controlling Network Access Permissions](#).
- *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](#).

- *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 Configure > 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.
- *Multicast Filter*: When enabled for a WLAN, all client multicast traffic will be dropped at the AP. Broadcast and unicast frames remain unchanged.
- *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. 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](#) for more information.
- *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 Wireless 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., ARP request 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 [Configuring DHCP Relay](#).
- *Background Scanning*: Background scanning enables the Ruckus Wireless 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](#)).
- *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 Wireless recommends disabling load balancing on VoIP WLANs. For more information, see [Load Balancing](#).
- *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](#).

- *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](#) 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 from a wireless client, the AP will encapsulate additional information (such as VLAN 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](#) 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.
- *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).
- *Application Visibility*: 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* widgets on the Dashboard.



---

**NOTE:** Supported APs: H500, R300, R310, R500, R510, R600, R700, R710, T300 series, T710 series, 7055, 7352, 7372, 7781/7782 series, 7982.

---

- When Application Visibility is enabled, the Apply Policy group option becomes available. Use this option to apply an Application Denial Policy to this WLAN (see [Configure Application Denial Policies](#)).
- *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.
- *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 timezone. If your browser and the target AP/WLAN are in different timezones, 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 AM and your browser was set to New York time, you would configure the WLAN service schedule to enable the WLAN at noon. When configuring the service schedule, all times are based on your browser's timezone setting.

---

- *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 [support.ruckuswireless.com](http://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 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 (Configure > Services) and Report Rogue Devices (Configure > 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.

---

**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 useful when a client reconnects to an AP that it previously roamed away from. PMK Caching is the method defined in the 802.11i specification, which also defined WPA2.

**Opportunistic Key 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).

Figure 133. Advanced options for creating a new WLAN

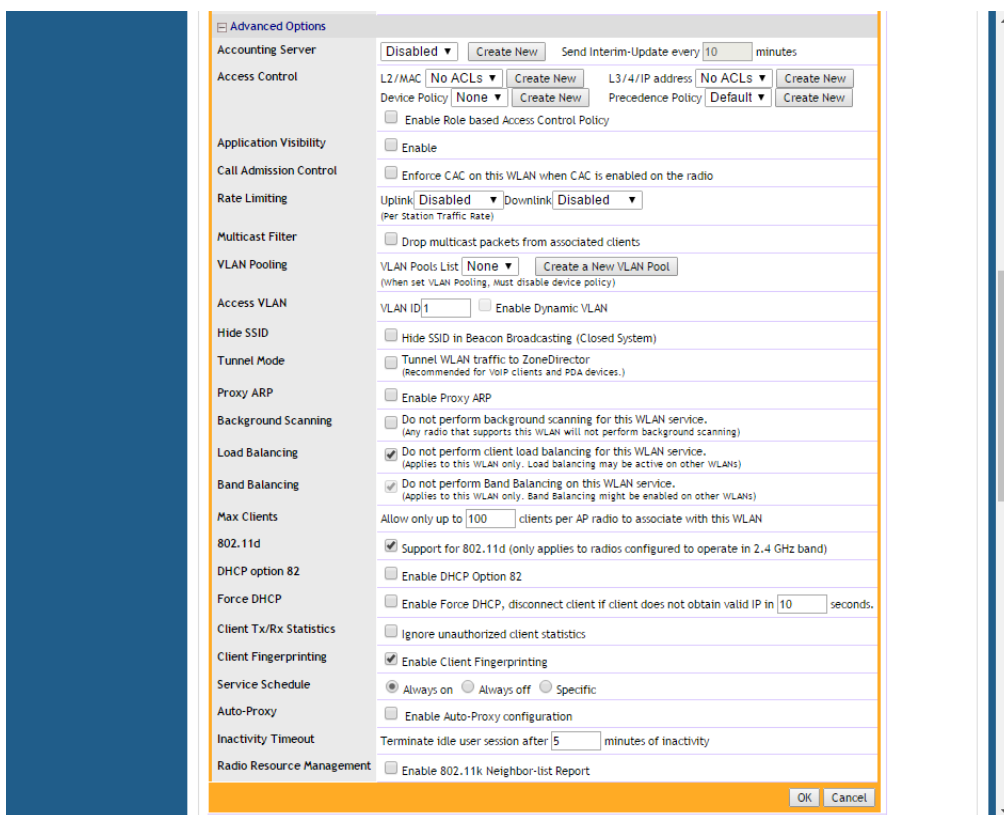
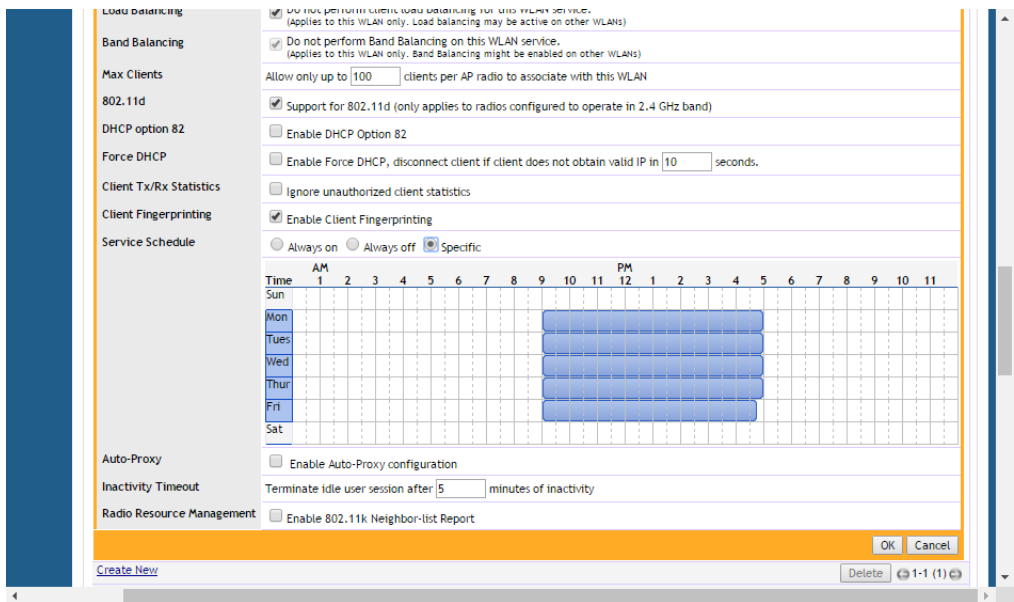


Figure 134. Configuring WLAN service schedule



## 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 **Configure > WLANs**.
- 3 When the *WLANs* page appears, the default internal and guest networks are listed in the table (once you have created a WLAN, it will appear in this table).
- 4 If you have no need for custom authentication or encryption methodologies in this new WLAN, locate the default WLAN record and click **Clone**.
- 5 A workspace appears, displaying the default settings of a new WLAN, using the same configuration settings as the default WLAN.
- 6 Type a descriptive **Name** for this WLAN, and then click **OK**. This new WLAN is ready for use by selected users.

- 7 You can now assign access to this new WLAN to a limited set of internal users, as detailed in [Creating New User Roles](#).

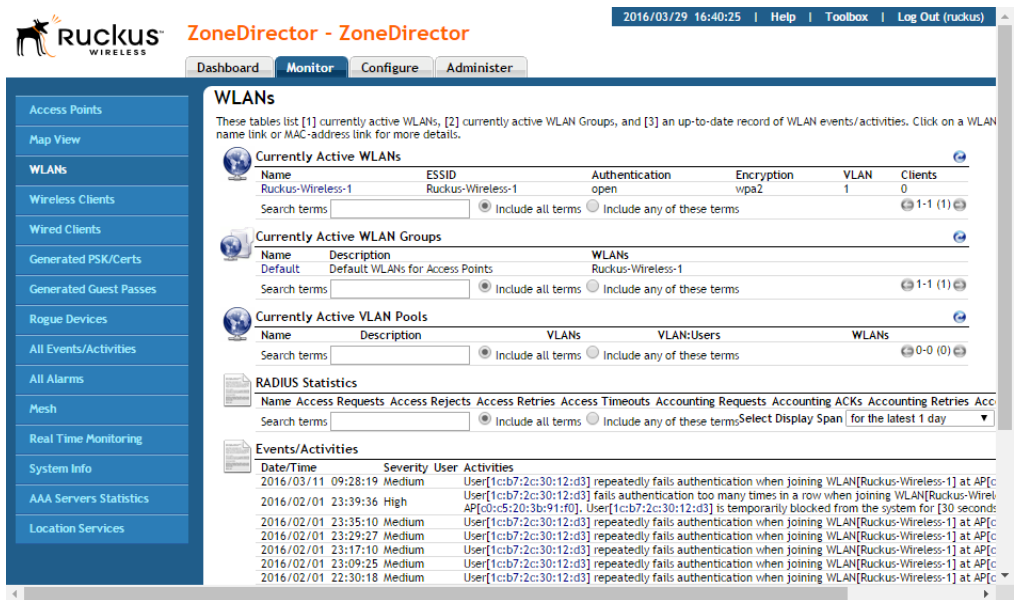
## Customizing WLAN Security

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 **Monitor > WLANs**.
- 2 The *Currently Active WLANs* table lists the WLANs created during the setup process. You can review the details of a WLAN’s configuration by clicking the WLAN name. See [Figure 135](#).
- 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 135. Viewing WLAN security configurations from the Monitor > WLANs page



## Fine-Tuning the Current Security Mode

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

- 1 Go to **Configure > WLANs**.
- 2 In the Internal WLAN row, click **Edit**.
- 3 Choose from the following options to keep the default WPA2 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/WPA 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/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.
- **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 **Configure > WLANs**.
- 2 When the *WLANs* workspace appears, you will want to review and then change the security options for the internal network. To start, click **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- 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 *Configure > 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.

---

**NOTE:** Replacing your WPA configuration with 802.1X requires the users to make changes to their Ruckus wireless connection configuration—which may include the importation of 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](#)). 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](#).



**CAUTION!** If your wireless network is using EAP/external RADIUS server for client authentication and you have Windows Vista clients, make sure that they are upgraded to Vista Service Pack 1 (SP1). SP1 includes fixes for client authentication issues when using EAP/external RADIUS server.

---

## 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 20. Maximum number of WLAN groups by ZoneDirector model

ZoneDirector Model	Max WLAN Groups
ZoneDirector 1200	256
ZoneDirector 3000	1024
ZoneDirector 5000	2048

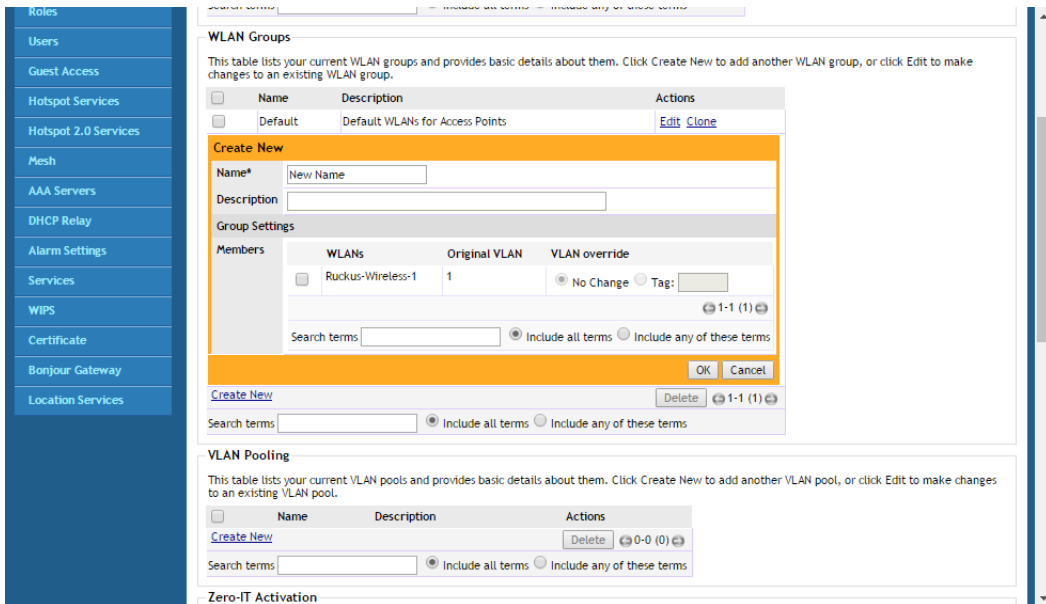
## Creating a WLAN Group

- 1 Go to **Configure > WLANs**.
- 2 In the **WLAN Groups** section, click **Create New**. The Create New 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 New 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 136. WLAN group



## Assigning a WLAN Group to an AP

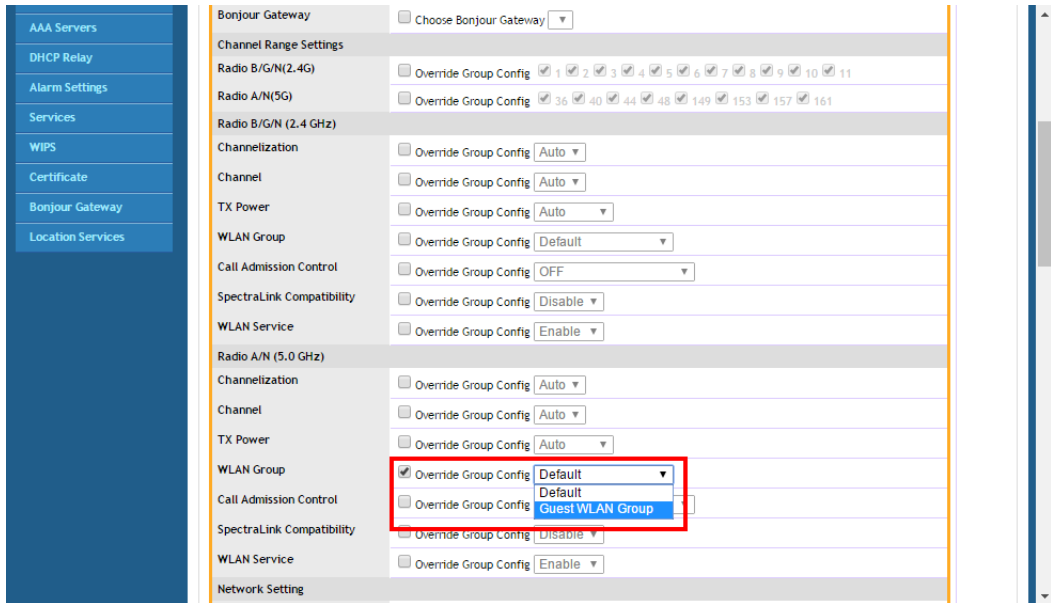
- 1 Go to **Configure > Access Points**.

## Working with WLAN Groups

Viewing a List of APs That Belong to a WLAN Group

- 2 In the list of access points, find the MAC address of the AP that you want to assign to a WLAN group, and then click **Edit**.
- 3 In **WLAN Group**, click **Override Group Config** and select the WLAN group to which you want to assign the AP. Each AP (or radio, on dual radio APs) can only be a member of a single WLAN group.
- 4 Click **OK** to save your changes.

Figure 137. Assign a WLAN group to an AP



## Viewing a List of APs That Belong to a WLAN Group

- 1 Go to **Monitor > WLANs**.
- 2 Under Currently Active WLAN Groups, click the WLAN group name for which you want to view the member AP list.
- 3 On the page that loads, look for the Member APs section. All APs that belong to this WLAN group are listed.

# Deploying ZoneDirector WLANs in a VLAN Environment

---

**NOTE:** 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.

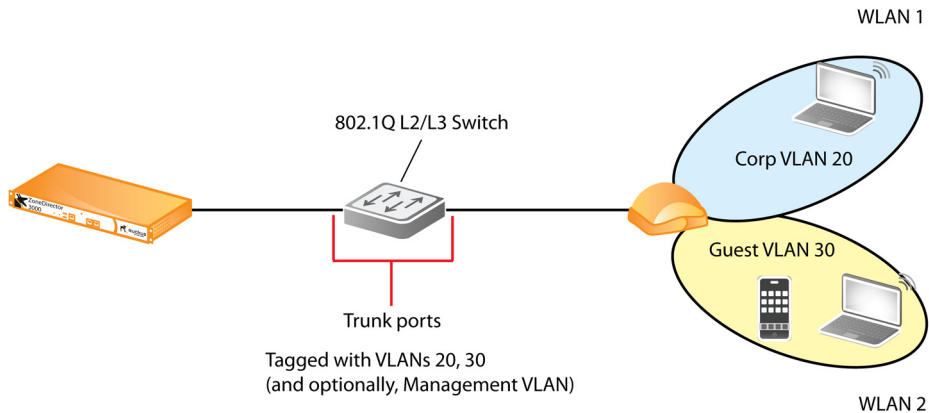
---

You can set up a ZoneDirector wireless LAN as an extension of a VLAN network environment by tagging wireless client traffic to specific VLANs. 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 ([Figure 138](#)): VLAN 20 is used for internal clients, VLAN 30 is used for guest clients, and Management VLAN configuration is optional.

Figure 138. 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 a 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.

---

**NOTE:** Assigning management traffic to a VLAN makes automatic AP provisioning more complicated, and should not be undertaken without a thorough understanding of your own network configuration as well as the ZoneFlex 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 **Configure > Access Points**.
- 2 In *Access Point 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 **Configure > System**.
- 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 Configure > Access Points > Access Point Policies > Management VLAN page, if APs exist on the same VLAN as ZoneDirector.

Figure 139. Configuring management VLAN for ZoneDirector

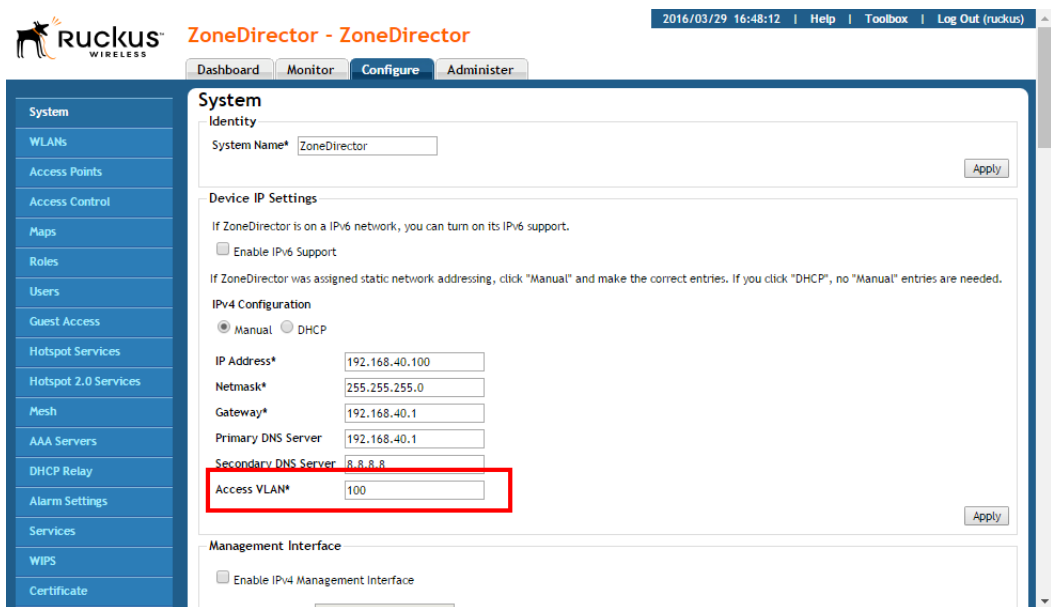




Figure 140. Configuring management VLAN for APs

The screenshot shows the ZoneDirector configuration interface. On the left is a navigation menu with items like 'Hotspot 2.0 Services', 'Mesh', 'AAA Servers', 'DHCP Relay', 'Alarm Settings', 'Services', 'WIPS', 'Certificate', 'Bonjour Gateway', and 'Location Services'. The main content area is titled 'Access Point Policies' and contains several sections:

- Access Point Groups:** A table with columns for Name, Description, # of Members, and Actions. It shows a 'System Default' group with 3 members. Below the table are buttons for 'Create New', 'Delete', and '1-1 (1)'. A search terms section is also present.
- Access Point Policies:**
  - Approval:** A checked checkbox 'Automatically approve all join requests from APs. (To enhance wireless security, deactivate this option. This means you must manually "allow" each newly discovered AP.)'
  - Limited ZD Discovery:** An unchecked checkbox 'Only connect to the following ZoneDirector:'. Below it are radio buttons for 'Configure Primary and Secondary ZD Settings to AP (IP or domain name is acceptable):'. This section includes input fields for 'Primary ZoneDirector Addr\*' and 'Secondary ZoneDirector Addr', and a 'Prefer Primary ZD' checkbox.
  - Management VLAN:** A section with a red box around it. It has a radio button for 'Keep AP's setting' (unchecked) and a radio button for 'VLAN ID' (checked) with an input field containing '100'.
  - Tunnel MTU:** An input field with '1500' and a note '(To limit the maximum transmission unit size between ZoneDirector and AP, range: 850 - 1500)'
  - Auto Recovery:** A checked checkbox 'AP reboots if disconnected from ZoneDirector for more than 30 Minutes.'
- Access Point USB Software Packages:** A section with a note 'No USB Software Package has been imported.'

An 'Apply' button is located at the bottom right of the 'Access Point Policies' section.

## How Dynamic VLAN Works

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

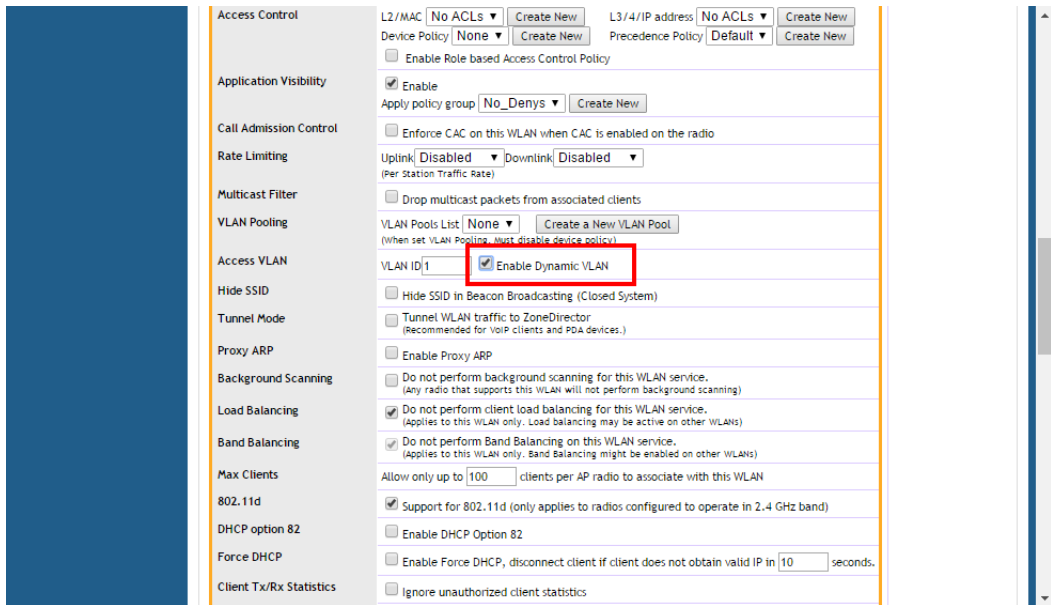
Dynamic VLAN Requirements:

- A RADIUS server must have already been added to ZoneDirector
- 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 **Configure > WLANs**. Click **Edit** next to the WLAN you want to configure.
- 2 In **Authentication Server**, select the RADIUS server that you configured on the AAA Servers page.
- 3 Expand the **Advanced Settings** section and click the **Enable Dynamic VLAN** box next to **Access VLAN**.
- 4 Click **OK** to save your changes.

Figure 141. 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:

- 1 Dynamic VLAN (top priority)
- 2 VLAN
- 3 Tunnel Mode

## How It Works

- 1 User associates with a WLAN on which Dynamic VLAN has been enabled.
- 2 The AP requires the user to authenticate with the RADIUS server via ZoneDirector.
- 3 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.

- 4 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. [Table 21](#) lists the RADIUS user attributes related to dynamic VLAN.

Table 21. 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 WiFi 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](#)), 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 **Configure > WLANs**, and locate the *VLAN Pooling* section.
- 2 Click **Create New** to create a new VLAN pool.
- 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 142. Creating a VLAN pool

The screenshot shows the ZoneDirector web interface with a sidebar on the left containing navigation options like Users, Guest Access, Hotspot Services, etc. The main content area is divided into sections: WLAN Groups, VLAN Pooling, and Zero-IT Activation. The 'VLAN Pooling' section is active, displaying a table of existing pools and a 'Create New' dialog box. The dialog box has the following fields:

- Name\***: VLAN Pool 1
- Description**: Student VLAN Pool
- VLANs\***: 7-10,13,17,20-28

Below the dialog box, there are 'OK' and 'Cancel' buttons. The 'Create New' button is also visible in the table below the dialog.

To assign a pool of VLANs to an SSID:

- 1 Go to **Configure > WLANs**.
- 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 143. Assign a VLAN Pool to a WLAN

The screenshot displays the configuration page for a WLAN in ZoneDirector. The left sidebar contains a navigation menu with categories like Zero-IT Activation, Priority, Advanced Options, Accounting Server, Access Control, Application Visibility, Call Admission Control, Rate Limiting, Multicast Filter, VLAN Pooling, Access VLAN, Hide SSID, Tunnel Mode, Proxy ARP, Background Scanning, Load Balancing, and Band Balancing. The main content area is under the 'Advanced Options' tab. Key settings include:

- Zero-IT Activation™:**  Enable Zero-IT Activation (WLAN users are provided with wireless configuration installer after they log in.)
- Priority:**  High  Low
- Accounting Server:** Disabled | Send Interim-Update every 10 minutes
- Access Control:** L2/MAC: No ACLs | L3/4/IP address: No ACLs | Device Policy: None | Precedence Policy: Default
- Application Visibility:**  Enable
- Call Admission Control:**  Enforce CAC on this WLAN when CAC is enabled on the radio
- Rate Limiting:** Uplink: Disabled | Downlink: Disabled (Per Station Traffic Rate)
- Multicast Filter:**  Drop multicast packets from associated clients
- VLAN Pooling:** VLAN Pools List: **vlan pool 1** | (When set VLAN Pooling is disabled, the device policy is None) |  Enable Dynamic VLAN
- Access VLAN:** VLAN ID: 1
- Hide SSID:**  Hide SSID in Beacon Broadcasting (Closed System)
- Tunnel Mode:**  Tunnel WLAN traffic to ZoneDirector (Recommended for VoIP clients and PDA devices.)
- Proxy ARP:**  Enable Proxy ARP
- Background Scanning:**  Do not perform background scanning for this WLAN service. (Any radio that supports this WLAN will not perform background scanning)
- Load Balancing:**  Do not perform client load balancing for this WLAN service. (Applies to this WLAN only. Load balancing may be active on other WLANs.)
- Band Balancing:**  Do not perform Band Balancing on this WLAN service. (Applies to this WLAN only. Band Balancing might be enabled on other WLANs.)

---

**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](#).

## 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 smartphones. 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](#)
- [Creating a Hotspot 2.0 Service](#)

### Creating a Hotspot Service

ZoneDirector's *Configure > Hotspot Services* page can be used to configure a traditional (WISPr 1.0) hotspot service to provide public access to users via its WLANs. 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](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 **Configure > 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 (**Configure > WLANs > Edit > Type > Hotspot Service (WISPr) > Hotspot Services > Create New.**)

---

- 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 Configure optional settings as preferred:
    - In **Start Page**, configure where users will be redirected after successful login. You could redirect them to the page that they want to visit, or you could set a different page where users will be redirected (for example, your company website).
    - In **User Session**, configure session timeout and grace period, both disabled by default.
      - **Session Timeout:** Specify a time limit after which users will be disconnected and required to log in again.
      - **Grace Period:** Allow disconnected users a grace period after disconnection, during which clients will not need to re-authenticate. Enter a number in minutes, between 1 and 144,000.



- 7 In **Authentication Server**, select the AAA server that you want to use to authenticate users.
    - Options include Local Database and any AAA servers that you configured on the Configure > AAA Servers page. If a RADIUS server is selected, an additional option appears: **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](#).
- 

**NOTE:** Alternatively, you can create an Authentication or Accounting server from the Hotspot configuration page while creating a new WLAN or modifying an existing WLAN (**Configure > WLANs > Edit > Type > Hotspot Service (WISPr) > Hotspot Services > Create New > Authentication/Accounting Servers > Create New.**)

---

- 8 In **Accounting Server** (if you have an accounting server set up), select the server from the list and configure the frequency (in minutes) at which accounting data will be retrieved.
- 9 In **Wireless Client Isolation**, choose whether clients connected to this Hotspot WLAN should be allowed to communicate with one another locally. See [Advanced Options](#) in the Creating a WLAN section for a description of the same feature for non-Hotspot WLANs.
- 10 Configure optional settings as preferred:
  - In **Location Information**, enter *Location ID* and *Location Name* WISPr attributes, as specified by the WiFi Alliance.
  - In **Walled Garden**, enter network destinations (URL or IP address) that users can access without going through authentication. A Walled Garden is a limited environment to which an unauthenticated user is given access for the purpose of setting up an account. After the account is established, the user is allowed out of the Walled Garden.
  - In **Restricted Subnet**, define L3/4 IP address access control rules for the hotspot service to allow or deny wireless devices based on their IP addresses.
  - Under **Advanced Options**, enable **Intrusion Prevention** to temporarily block hotspot clients that fail repeated authentication attempts. 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.

**11** Click **OK** to save the hotspot settings.

The page refreshes and the hotspot service you created appears in the list. You may now assign this hotspot service to the WLANs that you want to provide hotspot Internet access, as described in [Assigning a WLAN to Provide Hotspot Service](#).

Figure 144. Creating a Hotspot service

The screenshot shows the 'Create New' configuration page for a hotspot service. The left sidebar contains a navigation menu with the following items: Access Points, Access Control, Maps, Roles, Users, Guest Access, Hotspot Services (highlighted), Hotspot 2.0 Services, Mesh, AAA Servers, DHCP Relay, Alarm Settings, Services, WIPS, Certificate, Bonjour Gateway, and Location Services. The main configuration area is titled 'Create New' and includes the following sections:

- Name:** Hotspot 1
- Redirection:** (Empty field)
- WISPr Smart Client Support:** Radio buttons for None (selected), Enabled, and Only WISPr Smart Client allowed.
- Login Page\*:** Redirect unauthenticated user to  for authentication.
- Start Page:** After user is authenticated, radio buttons for redirect to the URL that the user intends to visit (selected) and redirect to the following URL: .
- User Session:**
  - Session Timeout:**  Terminate user session after  minutes
  - Grace Period:**  Allow users to reconnect with out re-authentication for  minutes
- Authentication/Accounting Servers:**
  - Authentication Server:** Local Database
  - Accounting Server:** Disabled
- Wireless Client Isolation:**
  - Isolate wireless client traffic from other clients on the same AP.
  - Isolate wireless client traffic from all hosts on the same VLAN/subnet.
  - 
  - (Requires whitelist for gateway and other allowed hosts.)
- Location Information:** (Collapsible section)

---

**NOTE:** If ZoneDirector is located behind a NAT device and signed certificates are used with 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 **Configure > WLANs**.
- 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 145. Assigning a Hotspot service to a Hotspot WLAN

The screenshot shows the 'Create New' configuration page for a WLAN. The left sidebar contains a navigation menu with items: Maps, Roles, Users, Guest Access, Hotspot Services, Hotspot 2.0 Services, Mesh, AAA Servers, DHCP Relay, Alarm Settings, Services, WIPS, Certificate, Bonjour Gateway, and Location Services. The main content area is titled 'Create New' and is divided into several sections:

- General Options:** Name/ESSID\* is 'Hotspot 1', ESSID is 'Hotspot 1', and Description is empty.
- WLAN Usages:** Type is set to 'Hotspot Service (WISPr)' (highlighted with a red box). Other options include Standard Usage, Guest Access, Hotspot 2.0, Autonomous, and Social Media.
- Authentication Options:** Method is 'Open'. Other options include 802.1x EAP, MAC Address, and 802.1x EAP + MAC Address.
- Encryption Options:** Method is 'None'. Other options include WPA2, WPA-Mixed, and WEP-64 (40 bit).
- Options:** Hotspot Services is set to 'Hotspot1' (highlighted with a red box). Other options include 'Create New', 'High', and 'Low'.
- Advanced Options:** Access Control includes L2/MAC (No ACLs), Device Policy (None), and Precedence Policy (Default). Other options include 'Create New', 'Enable Role based Access Control Policy', 'Application Visibility' (Enable), and 'Call Admission Control' (Enforce CAC on this WLAN when CAC is enabled on the radio).

## Common WISPr Attribute Abbreviations

[Table 22](#) 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 22. 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.
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](#).

---

## Creating a Hotspot 2.0 Service

“Hotspot 2.0” is a newer WiFi 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 WiFi Alliance certification) aims to improve the experience of mobile users when selecting and joining a WiFi 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 WiFi Alliance Hotspot 2.0 Technical Specification.

Enabling Hotspot 2.0 service on ZoneDirector requires the following three steps:

- [Create a Service Provider Profile](#)
- [Create an Operator Profile](#)
- [Create a Hotspot 2.0 WLAN](#)

### Create a Service Provider Profile

To create a Service Provider Profile:

- 1 Go to **Configure > Hotspot 2.0 Services**.
- 2 Click **Create New** under *Service Provider Profiles*.

**NOTE:** 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 (**Configure > WLANs > Edit > Type > Hotspot 2.0 > Hotspot 2.0 Operator > Create New > Service Provider Profiles > Create New.**)

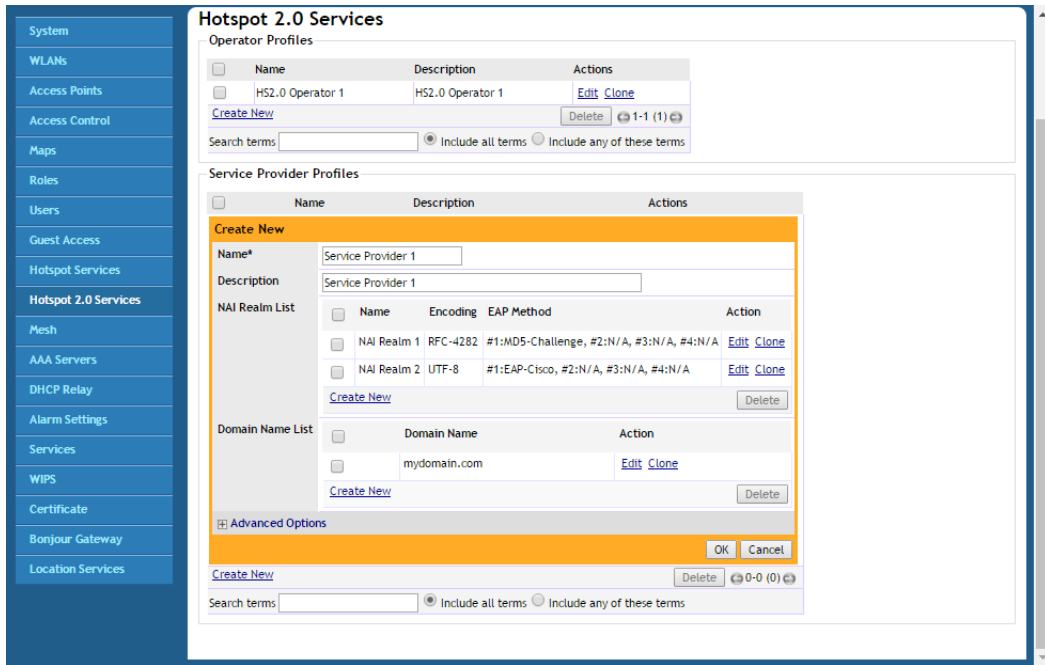
3 Configure the settings in [Table 23](#) to create a Service Provider profile.

Table 23. Hotspot 2.0 Service Provider profile configuration

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](#).

Figure 146. Creating a Service Provider Profile



## Create an Operator Profile

To create an Operator Profile:

- 1 Go to **Configure > Hotspot 2.0 Services**.
- 2 Click **Create New** under *Operator Profiles*.

**NOTE:** 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 (**Configure > WLANs > Edit > Type > Hotspot 2.0 > Hotspot 2.0 Operator > Create New.**)

- 3 Configure the settings in [Table 147](#) to create a Hotspot 2.0 Operator profile.

Figure 147. Hotspot 2.0 Operator profile configuration options

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.

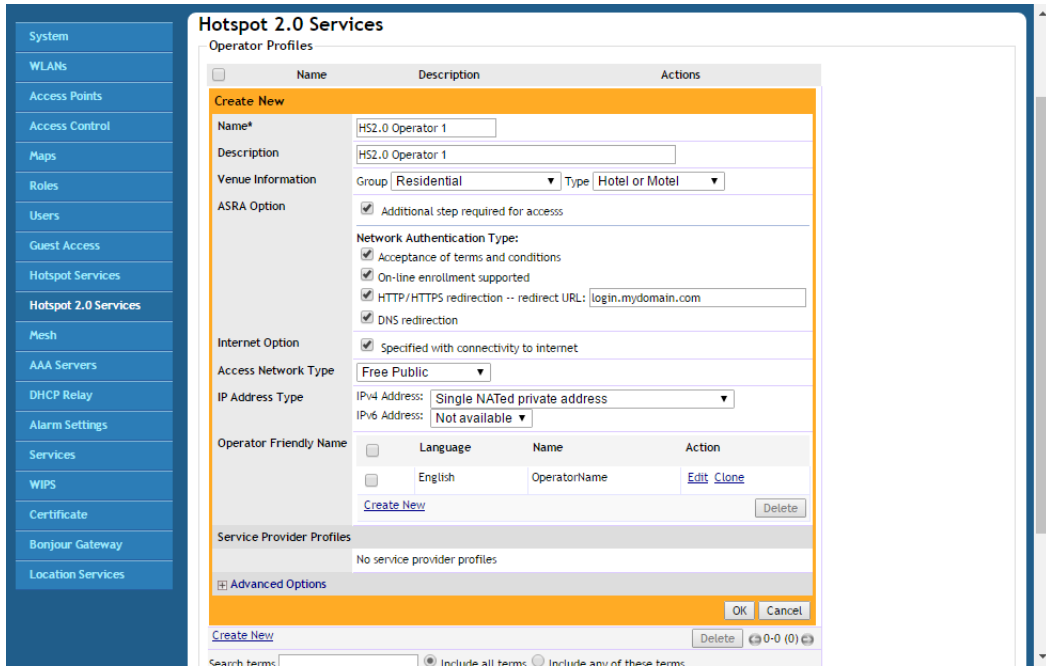


Figure 147. Hotspot 2.0 Operator profile configuration options

Option	Description
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](#).

Figure 148. Creating a Hotspot 2.0 Operator Profile



### 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 **Configure > WLANs**.
- 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**.

---

**NOTE:** 802.1X EAP is the only authentication method and WPA2/AES is the only encryption method available when you select Hotspot 2.0 for 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 Options](#) 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 149. Creating a Hotspot 2.0 WLAN

The screenshot shows the 'Create New' configuration page for a Hotspot 2.0 WLAN. The page is divided into several sections:

- General Options:** Name/ESSID\* is 'Hotspot 2.0 WLAN', ESSID is 'Hotspot 2.0 WLAN'.
- WLAN Usages:** Type is 'Hotspot 2.0' (selected and highlighted with a red box).
- Authentication Options:** Method is '802.1x EAP', Algorithm is 'AES'.
- Encryption Options:** Method is 'WPA2', Algorithm is 'AES'.
- Options:** Hotspot 2.0 Operator is 'HS2.0 Operator 1' (highlighted with a red box), Authentication Server is 'Local Database'.
- Wireless Client Isolation:** 'Isolate wireless client traffic from all hosts on the same VLAN/subnet.' is checked.
- Zero-IT Activation™:** 'Enable Zero-IT Activation' is unchecked.
- Priority:** 'High' is selected.

## Setting the Venue Name for a Hotspot 2.0 AP

See [Configuring Hotspot 2.0 Venue Settings for an AP](#) for instructions on setting AP venue names for individual APs.

## Working with Dynamic Pre-Shared Keys

Dynamic PSK is a unique Ruckus Wireless 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.
- 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 DPSK.

DPSKs can be created in bulk and manually distributed to users and devices, or ZoneDirector can auto-configure devices with a DPSK when they connect to the network for the first time using Zero-IT Activation (see [Enabling Automatic User Activation with Zero-IT](#)).

## 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).

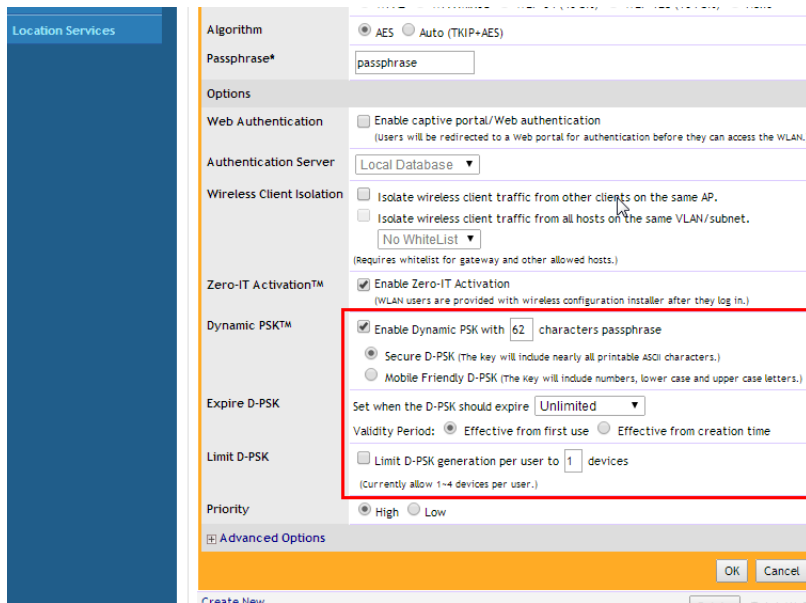
To enable DPSK for a WLAN:

- 1 Go to **Configure > WLANs**.
- 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, as selecting WPA-Mixed will disable the Zero-IT activation option).
- 6 Under *Encryption Options: Algorithm*, select **AES** (not Auto, as selecting Auto will disable the Zero-IT activation option).
- 7 If using MAC Address authentication, choose an *Authentication Server* to authenticate clients against--either **Local Database** or **RADIUS Server**.
- 8 Ensure that the **Zero-IT Activation** check box is enabled.
- 9 Next to *Dynamic PSK*, enable the check box next to **Enable Dynamic PSK**. Select a DPSK passphrase length (between 8 and 62 characters).
- 10 Choose whether to use **Secure DPSK** or **Mobile Friendly DPSK**.

- **Secure DPSK:** Includes almost all printable ASCII characters, including periods, hyphens, dashes, etc. This option is more secure, however it is difficult to input for mobile clients whose keyboards may not contain the entire set of printable ASCII characters.
  - **Mobile Friendly DPSK:** Choose this option if this WLAN will be used for mobile clients. This option limits the range of characters to lower case and upper case letters and numbers, which makes it easier for users to input the DPSK when activating a mobile client to a Zero-IT WLAN. (You may also want to limit the DPSK length to 8 characters for the convenience of your mobile client users.)
- 11** *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.
  - 12** *Limit DPSK:* By default each authenticated user can generate multiple DPSKs. Select this option to limit the number of DPSKs each user can generate (1-4).
  - 13** Click **OK** to save your settings.

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.

Figure 150. Enabling Dynamic PSK for a WLAN



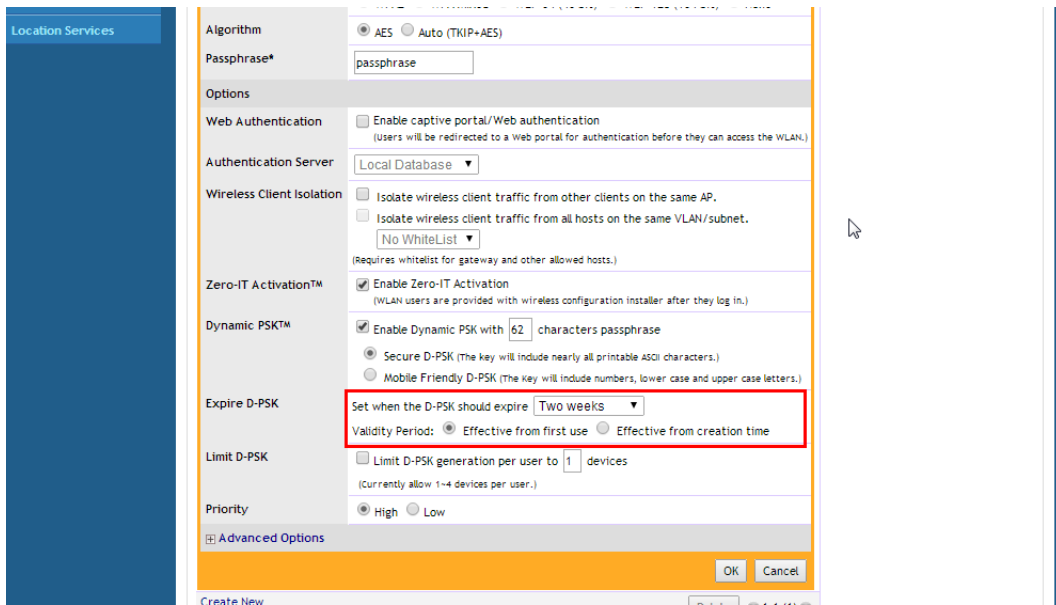
## Setting Dynamic Pre-Shared Key Expiration

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 **Configure > WLANs**, 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 the **Apply** button that is in the same section. The new setting goes into effect immediately.

Figure 151. Dynamic PSK expiration options



**NOTE:** If you change the dynamic PSK expiration period, the new expiration period will only be applied to new PSKs. Existing PSKs will retain the expiration period that was in effect when the PSKs were generated. To force expiration, go to **Monitor > 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 **Configure > WLANs**.
- 2 Scroll down to the Dynamic PSK Batch Generation section.
- 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](#) below for more information.
- 8 Click **Generate**. ZoneDirector generates the dynamic PSKs, and then the following message appears:
- 9 To download the new DPSK record, [click here](#)
- 10 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.

Alternatively, you can allow users to automatically self-provision their clients using Zero-IT, as described in [Enabling Automatic User Activation with Zero-IT](#).

## 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 In the Dynamic PSK Batch Generation section, look for the following message:

To download an example of profile, **click here**.

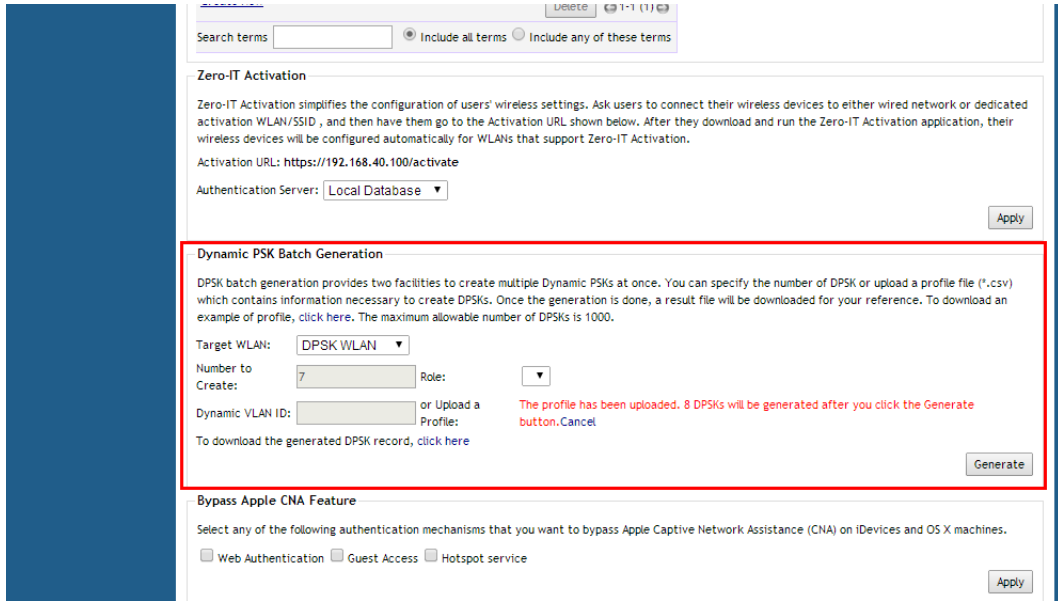
- 2 Click the **click here** link to download a sample profile.
- 3 Save the sample batch DPSK profile (in CSV format) to your computer.
- 4 Using a spreadsheet application, open the CSV file and edit the batch dynamic PSK profile by filling out the following columns:
  - **User Name**: (Required) Type 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 152. Editing the batch\_dpsk\_sample.csv file to create a custom batch DPSK profile

	A	B	C	D	E	F	G
1	#User Name	Mac Address	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							

- Go back to the Dynamic PSK Batch Generation section, and click the **Choose File** button to upload the CSV file you edited.
- Click **Generate** to generate the custom DPSKs that you modified.

Figure 153. DPSK batch generation



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 154. Downloading a generated batch DPSK profile

	A	B	C	D	E	F	G	H	
1	User Name	Passphrase	Role	WLAN	Mac Addr	Configured	Expires		
2	Tom	Y0ggpXeQROQ9GpI	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	XYzBHfTXsGCYNXID	DPSK	WL 00:00:00:0		0	Unlimited		
6	Sue	2DXfaQMfT5MR8OI	DPSK	WL 00:00:00:0		0	Unlimited		
7	Mary	2PTrb98ncUIgyrpuK	DPSK	WL 00:00:00:0		0	Unlimited		
8	Rumplestil	2KrcacBb3qubSM7UI	DPSK	WL 00:00:00:0		0	Unlimited		
9									
10									
11									
12									
13									

## 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 **Configure > WLANs**.
- 2 Locate the *Bypass Apple CNA Feature* section at the bottom of the page.
- 3 Select any or all of the following WLAN types for which you want to bypass the Apple CNA feature:
  - Web Authentication
  - Guest Access
  - Hotspot service
- 4 Click **Apply** to save your changes.

Figure 155. Enabling the Bypass Apple CNA Feature

**Dynamic PSK Batch Generation**

DPSK batch generation provides two facilities to create multiple Dynamic PSKs at once. You can specify the number of DPSK or upload a profile file (\*.csv) which contains information necessary to create DPSKs. Once the generation is done, a result file will be downloaded for your reference. To download an example of profile, [click here](#). The maximum allowable number of DPSKs is 1000.

Target WLAN:  Role:

Number to Create:  or Upload a Profile:  No file chosen

To download the new DPSK record, [click here](#)



**Bypass Apple CNA Feature**

Select any of the following authentication mechanisms that you want to bypass Apple Captive Network Assistance (CNA) on iOS devices and OS X machines.

Web Authentication  Guest Access  Hotspot service  Social Media

**Web Portal Logo**

Upload your logo to show it on the Web portal pages. The recommended image size is 138 x 40 pixels and the maximum file size is 20KB.

 Logo  No file chosen 

# Managing Access Points

# 5

In this chapter:

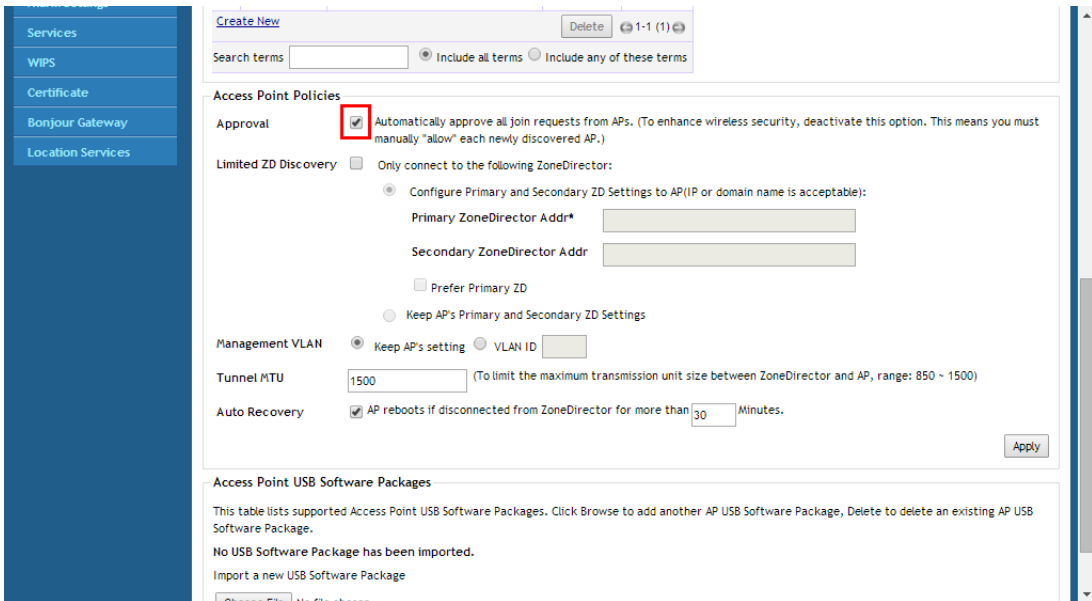
- [Adding New Access Points to the Network](#)
- [Working with Access Point Groups](#)
- [Configuring AP Ethernet Ports](#)
- [Reviewing Current Access Point Policies](#)
- [Importing a USB Software Package](#)
- [Managing Access Points Individually](#)
- [Optimizing Access Point Performance](#)

# 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, the 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—as detailed in this guide.

Figure 156. Automatic AP approval is enabled by default. Deselect this option to manually approve each AP join request.



The screenshot shows the ZoneDirector configuration interface. On the left is a navigation menu with options: Services, WIPS, Certificate, Bonjour Gateway, and Location Services. The main content area is titled 'Access Point Policies' and includes the following settings:

- Create New** (button) and **Delete** (button) with a count of 1-1 (1).
- Search terms** (input field) and radio buttons for **Include all terms** (selected) and **Include any of these terms**.
- Access Point Policies** section:
  - Approval**:  Automatically approve all join requests from APs. (To enhance wireless security, deactivate this option. This means you must manually "allow" each newly discovered AP.)
  - Limited ZD Discovery**:  Only connect to the following ZoneDirector:
    - Configure Primary and Secondary ZD Settings to AP(IP or domain name is acceptable):
      - Primary ZoneDirector Addr\*** (input field)
      - Secondary ZoneDirector Addr** (input field)
      - Prefer Primary ZD
      - Keep AP's Primary and Secondary ZD Settings
    - Keep AP's setting
  - Management VLAN**:  Keep AP's setting  VLAN ID (input field)
  - Tunnel MTU**: 1500 (To limit the maximum transmission unit size between ZoneDirector and AP, range: 850 ~ 1500)
  - Auto Recovery**:  AP reboots if disconnected from ZoneDirector for more than 30 Minutes.
- Apply** (button)

Below the 'Access Point Policies' section is the 'Access Point USB Software Packages' section, which includes a table listing supported packages, a message stating 'No USB Software Package has been imported.', and an 'Import a new USB Software Package' button with a file selection field.

## 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 Gigabit Ethernet, ensure that you use Cat5e or better Ethernet cables.

---

**NOTE:** By default, Ruckus Wireless 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:** If the Ruckus Wireless APs that you are using are PoE-capable and power sources are not convenient, they will draw power through the Ethernet cabling if connected to a PoE-ready hub or switch.

---

## Verifying/Approving New APs

- 1 Go to **Monitor > Access Points**. The Access Points page appears, showing the first 15 access points that have been approved or are awaiting approval. If ZoneDirector is managing more than 15 access points, the Show More button at the bottom of the list will be active. To display more access points in the list, click **Show More**. When all access points are displayed on the page, the Show More button disappears.
- 2 Review the *Currently Managed APs* table. See [Figure 157](#).
  - If the **Configure > Access Points > Access Points Policies > Approval** check box is checked, all new APs should be listed in the table, and their *Status* should be “Connected.”
  - If the Automatic AP Approval option is disabled, all new APs will be listed, but their status will be “Approval Pending.”
- 3 Under the *Action* column, click **Allow** . After the status is changed from “Disconnected” to “Connected,” the new AP is activated and ready for use.

---

**NOTE:** Use “Map View” (on the Monitoring tab) to place the marker icons of any newly approved APs. See [Evaluating and Optimizing Network Coverage](#) for more information.

---

# Adding New Access Points to the Network

Verifying/Approving New APs

Figure 157. The Monitor > Access Points page

**Access Points**

This table lists all currently active access points, and highlights basic details, such as number of clients per AP. Below are a table of currently managed AP groups and an AP-specific table of events and activities.

Currently Managed APs						
MAC Address	Device Name	Status	Mesh Mode	IP Address	Clients	Action
00:13:92:04:25:00	AP-7942 RAP - Wilson	Connected (Root AP)	Auto	172.17.16.53	1	[Icons]
00:22:7f:18:bc:00	AP-7942 MAP - Pantry	Connected (eMesh AP, 2 hops)	Auto	172.17.16.37	0	[Icons]
00:24:82:2c:d9:40		Approval Pending	Auto	172.17.16.82		[Icons]
00:1d:2e:2d:37:40		Approval Pending	Auto	172.17.16.208		[Icons]
00:13:92:18:78:e0		Approval Pending	Auto	192.168.200.168		[Icons]
04:4f:aa:32:2b:40		Approval Pending	Auto	192.168.200.156		[Icons]
00:25:c4:00:36:e0	AP-7962 MAP - David	Connected (Root AP)	Auto	172.17.16.93	8	[Icons]
00:25:c4:10:8c:10	AP-7962 RAP - 9F	Connected (Root AP)	Auto	172.17.16.62	8	[Icons]
00:25:c4:00:31:30	AP-7962 RAP - Formosa	Connected (Root AP)	Auto	172.17.16.126	3	[Icons]
00:25:c4:19:82:e0		Approval Pending	Auto	172.17.16.79		[Icons]
00:25:c4:19:e2:c0		Approval Pending	Auto	172.17.16.207		[Icons]
00:1f:41:26:4c:c0	AP-7942 NMAP - Pantry	Connected (Mesh AP, 1 hop)	Auto	172.17.16.89	0	[Icons]
00:25:c4:19:e1:90	AP-7962 RAP - Chow Chow	Connected (Mesh AP, 1 hop)	Auto	172.17.16.51	2	[Icons]
74:91:1a:20:42:40		Approval Pending	Auto	172.17.16.193		[Icons]
00:25:c4:2a:c5:d0	AP - 7762 - SDC	Disconnected (2011/04/06 13:45:35)	Auto	172.18.110.186		[Icons]

Search terms   Include all terms  Include any of these terms   1-15 (22)

Currently Managed AP Groups					
Member	Device Name/Description	APs	Clients	Status	Action
[Icon]	System Default - System default group for Access Points	77	77	[Icon]	[Icon]



# 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](#) for more information). 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](#): 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](#): 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](#): 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 (Configure > Access Points > Edit [AP MAC address]) and set the Tx Power setting to a lower setting.

Table 24. Maximum number of AP groups by ZoneDirector model

ZoneDirector Model	Max AP Groups
ZoneDirector 1200	64
ZoneDirector 3000	256
ZoneDirector 5000	512

## 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 settings:

- 1 Go to **Configure > Access Points**.
- 2 In the *Access Point Groups* section, locate the *System Default* access point group, and click the **Edit** button on the same line. The *Editing (System Default)* form appears.
- 3 Modify any of the settings in [Table 25](#) that you want to apply to the System Default AP group, and click **OK** to save your changes.

Table 25. Access Point group settings

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, 20MHz or 40MHz channel width for the 2.4 GHz radio, or Auto, 20, 40, or 80 MHz channel width for the 5 GHz radio.
Channel	Select <i>Auto</i> 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).
11n/ac Only Mode	Force all 802.11n and 11ac APs to accept only 802.11n/ac compliant devices on the 2.4 GHz or 5 GHz radio. If <i>11n/ac Only Mode</i> is enabled, all older 802.11b/g devices will be denied access to the radio.
WLAN Group	Specify which WLAN group this AP group belongs to.

Setting	Description
Call Admission Control	(Disabled by default). Enable Wi-Fi Multimedia Admission Control (WMM-AC) to support Polycom/Spectralink VIEW certification. See <a href="#">Advanced Options</a> under <a href="#">Creating a WLAN</a> for more information.
Spectralink Compatibility	(Disabled by default). Enable this option if this AP radio will be used as a voice WLAN for Polycom/Spectralink phones. This option changes several AP radio settings such as DTIM, BSS minrate and RTS-CTS to improve voice quality with Spectralink phones.  For optimal VoWLAN voice quality, also disable Self-Healing and Background Scanning from the <i>Configure &gt; Services</i> page).
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.
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 <i>Configure &gt; Location Services</i> page. See <a href="#">Configuring SPoT Location Services</a> .  For information on configuration and administration of Ruckus SmartPositioning Technology (SPoT) service, please refer to the <i>SPoT User Guide</i> , available from the Ruckus support site: <a href="https://support.ruckuswireless.com">https://support.ruckuswireless.com</a> .
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 <a href="#">Modifying Model Specific Controls</a> .
Group Settings	The Group Settings section is used to move access points between groups. See <a href="#">Modifying Access Point Group Membership</a> .

Figure 158. Editing the System Default access point group settings

The screenshot displays the configuration interface for the 'System Default' access point group. The settings are organized into several sections:

- Name:** System Default
- Description:** System default group for Access Points
- Channel Range Settings:**
  - Radio B/G/N(2.4G): Channels 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11 (all checked)
  - Radio A/N/AC(5G) Indoor: Channels 36, 40, 44, 48, 149, 153, 157, 161 (all checked)
  - Radio A/N/AC(5G) Outdoor: Channels 149, 153, 157, 161 (all checked)
- Radio Settings:**
  - Radio B/G/N (2.4 GHz):** Channelization: Auto; Channel: Auto; TX Power: Auto; 11n/ac only Mode: Auto; WLAN Group: Default; Call Admission Control: OFF; SpectraLink Compatibility: Disable; WLAN Service: Enable.
  - Radio A/N/AC (5.0 GHz):** Channelization: Auto; Indoor: Auto, Outdoor: Auto; TX Power: Auto; 11n/ac only Mode: Auto; WLAN Group: Default; Call Admission Control: OFF; SpectraLink Compatibility: Disable; WLAN Service: Enable.
- Network Setting:** IP Mode: IPv4 and IPv6
- Location Services:**
  - Enable/Disable:  Enable
  - Venue Name: (empty)
  - Model Specific Control: zf7055
  - Max Clients: Allow Max 100 clients to associate with this AP

## Creating a New Access Point Group

To create a new AP group with custom settings:

- 1 Go to **Configure > Access Points**.
- 2 In the *Access Point Groups* section, click the **Create New** button. The *Create New* form appears.
- 3 Enter a **Name** and optionally a **Description** for the new AP group.
- 4 Modify any of the settings in [Table 25](#) that you want to apply to the new AP group, and click **OK** to save your changes.

## 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 *Editing [AP Group]* form. The Group Settings section is divided into two subsections:

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

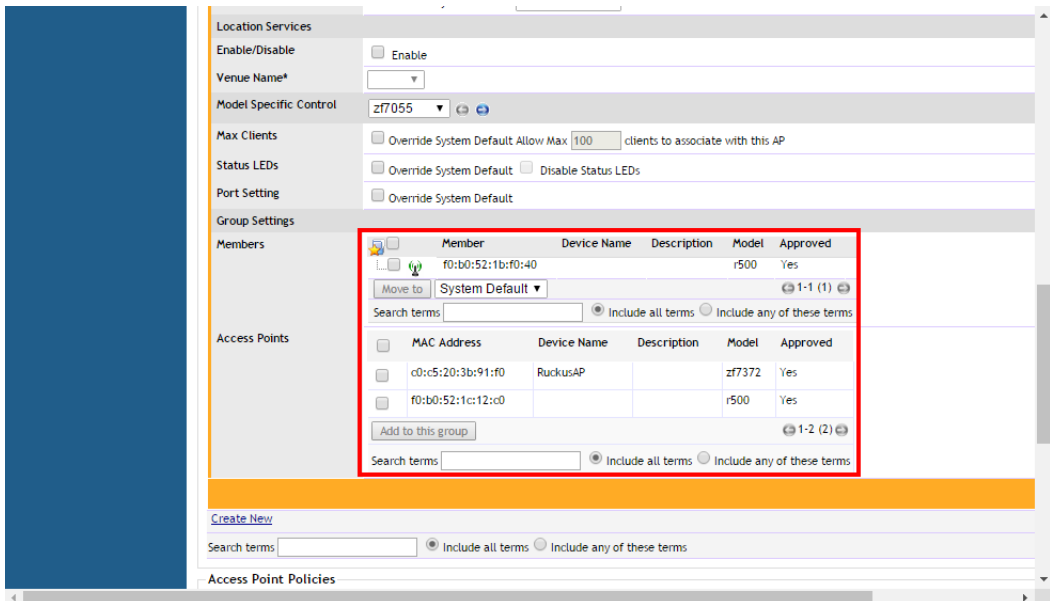
To move an AP from the current AP group to another group:

- 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** button. (To select all APs in the group, click the check box at the top of the column)
- 2 Click **OK** to save your changes.

To move an AP from another AP group into the AP group you are currently editing:

- 1 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.
- 2 Click **OK** to save your changes.

Figure 159. 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 for outdoor 11n/11ac APs. Enabling this 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.

---

- *PoE Operating Mode*: Select PoE operating mode, **Auto** or **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 *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](#).
- *Status LEDs*: When managed by ZoneDirector, you can disable the external LEDs on certain ZoneFlex models. This can be useful if your APs are installed in a public location and you don’t want to draw attention to them.
- *External Antenna*: On APs with external antenna options, select 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.
- *Port Settings*: See [Configuring AP Ethernet Ports](#).

---

**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.

---

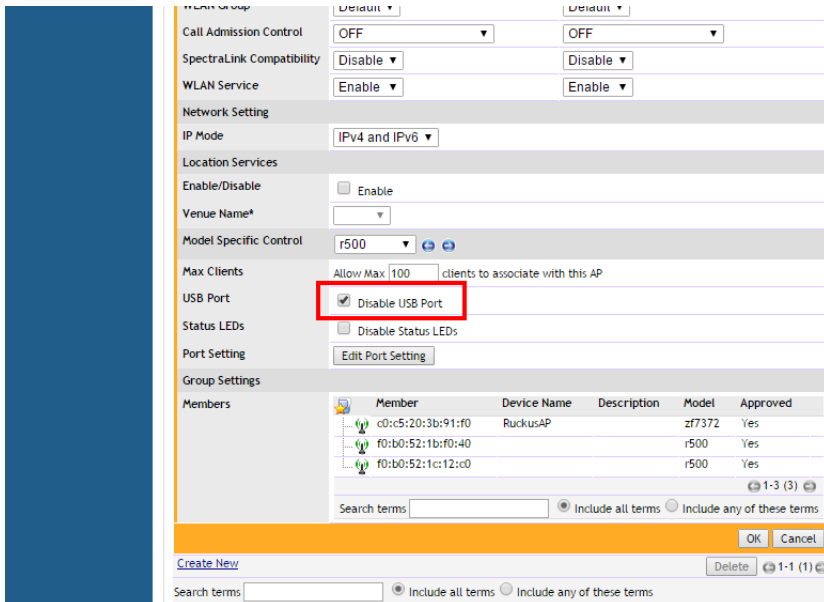
## Configuring AP USB Ports

Some Ruckus Wireless APs, such as the H500, support customer-supplied, low power (1W or less), Bluetooth Low Energy (BLE) devices, such as BLE beacons. The BLE 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. Ruckus Wireless APs with USB ports

supporting BLE devices can provide power to the BLE device. The BLE devices perform whatever tasks they are designed to do without interference from or control (other than supplying USB power) by the Ruckus Wireless network equipment. AP 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 **Configure > Access Points**.
- 2 In *Access Point Groups*, click **Edit** next to 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 160. Disabling AP USB ports



## 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 **Configure > Access Points**.
- 2 In *Access Point Groups*, click **Edit** next to 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*, select **Override System Default**. 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 fairness, rate limiting, client count limits, ACLs, prioritization of Ethernet vs. wireless traffic, client fingerprinting, application visibility, 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](#)).
- 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., ZoneFlex R300), the single LAN port must be a trunk port and is therefore not configurable.
  - For ZoneFlex 7055, the LAN5/Uplink port on the rear of the AP is defined as a Trunk Port and is not configurable. The four front-facing LAN ports are configurable.
  - For all other APs, you can configure each port individually as either a Trunk Port, Access Port or General Port. (See [Designating Ethernet Port Type](#) for more information.)



- 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](#) for more information.)
- 10 Click **Apply** to save your changes.

Figure 161. The ZoneFlex 7982 has two Ethernet ports, LAN1 and LAN2

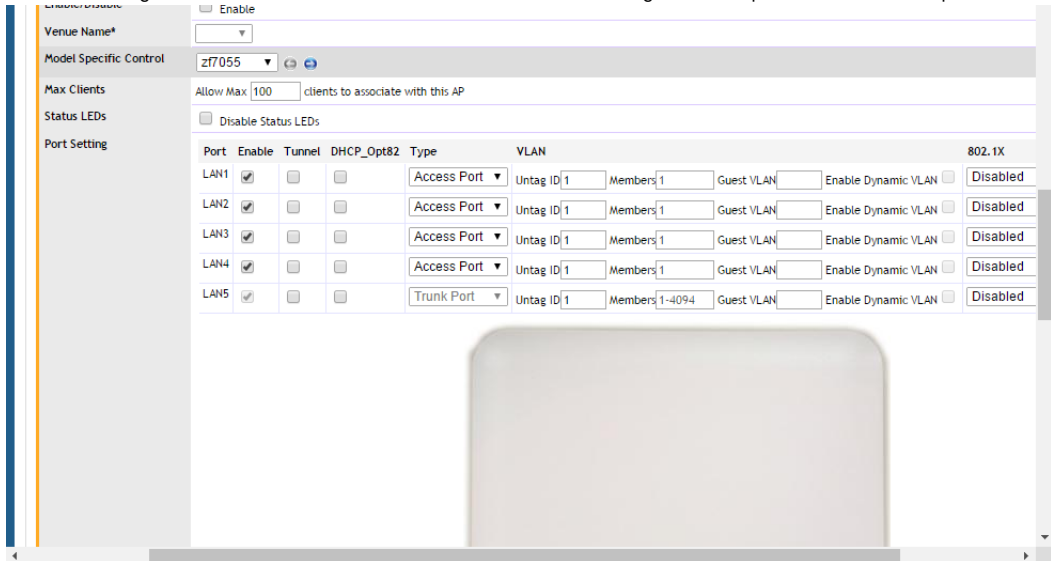
The screenshot displays the configuration page for a Ruckus AP. The 'Port Setting' section contains the following table:

Port	Enable	Tunnel	DHCP_Opt82	Type	VLAN			802.1X	
LAN1	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Trunk Port	Untag ID: 1	Members: 1-4094	Guest VLAN:	Enable Dynamic VLAN: <input type="checkbox"/>	Disabled
LAN2	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Trunk Port	Untag ID: 1	Members: 1-4094	Guest VLAN:	Enable Dynamic VLAN: <input type="checkbox"/>	Disabled

Below the table is a photograph of the AP's rear panel, highlighting the LAN1 and LAN2 ports. At the bottom, the 'Members' table shows:

Member	Device Name	Description	Model	Approved
c0:c5:20:3b:91:f0	RuckusAP		z7372	Yes

Figure 162. The ZoneFlex 7055 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.

Figure 163. Enabling DHCP Option 82 sub-options for a WLAN

The screenshot displays the configuration page for a WLAN, with a sidebar on the left listing various settings. The main content area is titled '(Per Station Traffic Rate)'. The 'DHCP Relay' section is highlighted with a red box, showing the 'Enable DHCP relay agent with relay-agent-1 DHCP server' checkbox checked. Below this, the 'DHCP option 82' section is also highlighted with a red box, showing four sub-options checked: 'Enable DHCP Option 82', 'Subopt-1 with format AP-MAC-hex', 'Subopt-2 with format Client-MAC-hex', and 'Subopt-151 with format Area-Name'. Other sections like 'Multicast Filter', 'VLAN Pooling', and 'Access VLAN' are visible but not highlighted.

## Designating Ethernet Port Type

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

- [Trunk Ports](#)
- [Access Ports](#)
- [General Ports](#)

All three port types are used to define how to manage the following two aspects of VLAN processing:

- Which VLANs are processed vs. dropped
- What to do with untagged packets (in other words, Native VLAN)

For most ZoneFlex 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 ZoneFlex 7055 and H500, 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 26. 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.

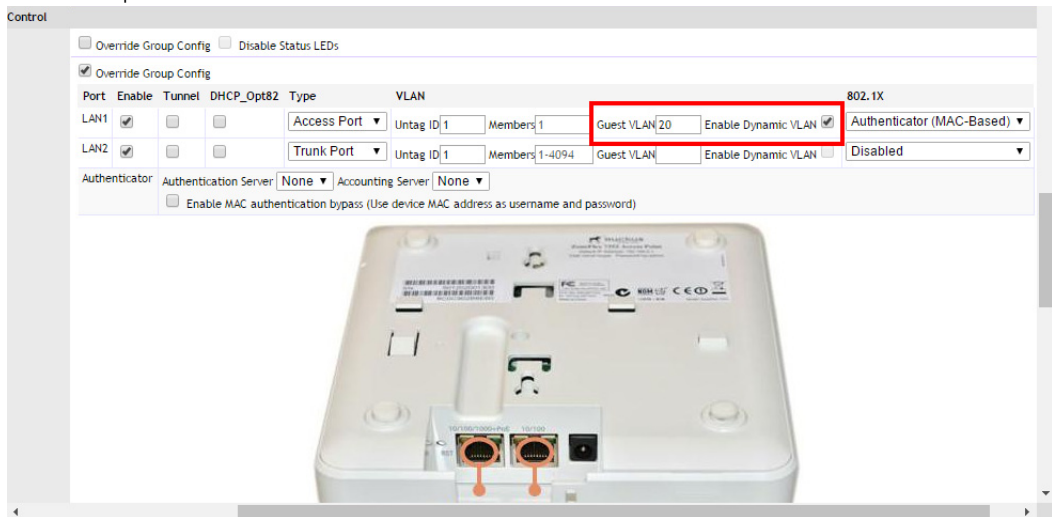
Table 27. Authenticator support vs. Port Type

	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 **Configure > Access Points** and click the **Edit** link next to 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 164. 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 165. 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 **Monitor > Access Points** and clicking on the MAC address of the AP.

# Configuring AP Ethernet Ports

## Viewing AP Ethernet Port Status

Figure 166. Viewing an AP's Ethernet port configuration

2016/03/30 11:25:03 | Help | Toolbox | Log Out (ruckus)

such as the clients and events associated with it.

Info		WLANs									
RuckusAP	Status	Connected	Name/ESSID	BSSID	Radio	State					
	Certificate Status	Non Ruckus PKI Certificate	Ruckus-Wireless-1	c0:c5:20:3b:91:f8	802.11a/g/n	Up					
	Uptime	12d 21h 52m	Ruckus-Wireless-1	c0:c5:20:3b:91:fc	802.11a/n	Up					
	Connection Mode	L3 (IPv4)									
c5:20:3b:91:f0	VLAN	1									
192.168.40.10	Associated Clients	1									
88.40.10:12223	Bonjour Gateway	Disabled									
	DHCP										
	z7372										
	Not Present										
	Not Support										
	Actions										
981202006357											
9.13.0.0.87											
	Radio 802.11a/n										
11	Current Channel	6	LAN	State	Tunnel Mode	Type	Access VLAN	GUEST VLAN	Dynamic VLAN	DHCP opt82	
Auto	Config Channel	Auto	LAN1	Enabled	Disabled	Trunk	1		Disabled	Disabled	
20	Channelization	0	LAN2	Enabled	Disabled	Trunk	1		Disabled	Disabled	
	Default WLAN Group	Default	<b>LAN Port Configuration</b>								
	Disabled SpectraLink Compatibility	Disabled	<b>LAN Port Status</b>								
	Enabled WLAN Service	Enabled	Port	Interface	Dot1x	Logical Link	Physical Link	Label			
	1/27/11 Deployed/Maximum/WLAN-Group	1/27/11	0	eth0	None	Down	Down	10/100 LAN1			
	Enabled Background Scanning	Enabled	1	eth1	None	Up	Up 1000Mbps full	10/100/1000 PoE LAN2			
	Full TX Power	Full									
	# of Authorized Client Devices	0									
1.24 / 0.00	% Retries/% Drops	0.261 / 0.00									
0.00243	% Non-unicast	0.0324									
9.0M/1.8G	Packets/Bytes Received	113K/21M									
4.9M/1.4G	Packets/Bytes Transmitted	250K/73M									
1.3M/168M	Wlans Data Packets/Bytes Received	34K/9.6M									

# Reviewing Current 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 client distribution 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 *Configure > WLANs* page.

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

- 1 Go to **Configure > Access Points**.
- 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 ZoneFlex 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 ZD 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 Wireless 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](#). For information on N+1 redundancy using Limited ZD Discovery, see [Using Limited ZD Discovery for N+1 Redundancy](#).

---

- **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 **Configure > 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](#)).
  - **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 167. Setting global AP policies on the Configure > Access Points page

The screenshot shows the 'Configure > Access Points' page. On the left is a navigation menu with items: Mesh, AAA Servers, DHCP Relay, Alarm Settings, Services, WIPS, Certificate, Bonjour Gateway, and Location Services. The main content area is divided into three sections:

- Table of AP Groups:** A table with columns: Name, Description, # of Members, and Actions. It lists one group: 'System Default' with 3 members. Below the table are 'Create New' and 'Delete' buttons, and a search filter with radio buttons for 'Include all terms' (selected) and 'Include any of these terms'.
- Access Point Policies:** A section with several settings:
  - Approval:** Checked. Text: 'Automatically approve all join requests from APs. (To enhance wireless security, deactivate this option. This means you must manually "allow" each newly discovered AP.)'
  - Limited ZD Discovery:** Unchecked. Text: 'Only connect to the following ZoneDirector:'. Below are radio buttons for 'Configure Primary and Secondary ZD Settings to AP (IP or domain name is acceptable):'. Two text boxes are present: 'Primary ZoneDirector Addr\*' and 'Secondary ZoneDirector Addr'. Below these are radio buttons for 'Prefer Primary ZD' and 'Keep AP's Primary and Secondary ZD Settings'.
  - Management VLAN:** Radio buttons for 'Keep AP's setting' (selected) and 'VLAN ID' with a text box.
  - Tunnel MTU:** Text box containing '1500'. Text: '(To limit the maximum transmission unit size between ZoneDirector and AP, range: 850 - 1500)'
  - Auto Recovery:** Checked. Text: 'AP reboots if disconnected from ZoneDirector for more than 30 minutes.'
- Access Point USB Software Packages:** Text: 'This table lists supported Access Point USB Software Packages. Click Browse to add another AP USB Software Package, Delete to delete an existing AP USB Software Package. No USB Software Package has been imported. Import a new USB Software Package'. Below is a 'Choose File' button and the text 'No file chosen'.

## Using Limited ZD Discovery for N+1 Redundancy

ZoneDirector's Smart Redundancy feature (see [Enabling Smart Redundancy](#)) can only be used with two ZoneDirectors of the same model (e.g., two ZoneDirector 1200s). If you want to deploy one ZoneDirector as a backup controller for multiple primary controllers (for example, using a ZD3000 as a backup for several ZD1200s in remote locations), 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 **Configure > 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*.

---

**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.

---

- 8 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 **Configure > 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 28. Max APs by ZoneDirector model

Model	Max APs per controller
ZoneDirector 1200	75
ZoneDirector 3000	500
ZoneDirector 5000	1000

## Importing a USB Software Package

Ruckus ZoneFlex 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-WiFi 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 **Configure > Access Points**.
- 2 Scroll down to *Access Point USB Software Packages*.
- 3 Click **Choose File**, and select the file to upload.
- 4 Click **OK** to upload the file to ZoneDirector.

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.

## Importing a USB Software Package

Using Limited ZD Discovery for N+1 Redundancy

- 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.

Figure 168. Importing a USB software package

The screenshot shows the ZoneDirector configuration interface. On the left is a navigation menu with items: AAA Servers, DHCP Relay, Alarm Settings, Services, WIPS, Certificate, Bonjour Gateway, and Location Services. The main content area is titled 'Access Point Policies' and contains several sections:

- System Default Group:** A table with columns 'Name', 'Description', '# of Members', and 'Actions'. It lists 'System Default' with 3 members. Buttons for 'Create New', 'Delete', and '1-1 (1)' are present.
- Search terms:** A search box with radio buttons for 'Include all terms' (selected) and 'Include any of these terms'.
- Access Point Policies:**
  - Approval:**  Automatically approve all join requests from APs. (To enhance wireless security, deactivate this option. This means you must manually "allow" each newly discovered AP.)
  - Limited ZD Discovery:**  Only connect to the following ZoneDirector:
    - Configure Primary and Secondary ZD Settings to AP (IP or domain name is acceptable):
      - Primary ZoneDirector Addr\* [text input]
      - Secondary ZoneDirector Addr [text input]
      - Prefer Primary ZD
      - Keep AP's Primary and Secondary ZD Settings
    - Keep AP's setting  VLAN ID [text input]
  - Management VLAN:**  Keep AP's setting  VLAN ID [text input]
  - Tunnel MTU:** [text input: 1500] (To limit the maximum transmission unit size between ZoneDirector and AP, range: 850 - 1500)
  - Auto Recovery:**  AP reboots if disconnected from ZoneDirector for more than [text input: 30] Minutes.
- Apply** button.

**Access Point USB Software Packages**

This table lists supported Access Point USB Software Packages. Click Browse to add another AP USB Software Package, Delete to delete an existing AP USB Software Package.

No USB Software Package has been imported.

Import a new USB Software Package

No file chosen



## 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 settings configured in AP Groups.

To edit the parameters of an access point:

- 1 Go to **Configure > Access Points**.
- 2 Find the AP to edit in the *Access Points* table, and then click **Edit** under the *Actions* column.
- 3 Edit any of the following:
  - **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 location on Google Maps, if using FlexMaster.
  - **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](#).
- 4 By clicking "Override Group Config" and changing the default values, the following parameters can be configured independently for each AP radio:
- 5 **Channel Range Settings:** Deselect any channels that you do not want the AP to use in channel selection.
- 6 **Channelization:** Sets the channel width (20 or 40 MHz) of each channel in the spectrum used during transmission.
- 7 **Channel:** Manually set the channel used by the AP radio.
- 8 **Tx Power:** Manually set the maximum transmit power level relative to the calibrated power.

- 9 WLAN Group:** Specify a WLAN group for this radio.
- 10 Call Admission Control:** (Disabled by default). Enable Wi-Fi Multimedia Admission Control (WMM-AC) to support Polycom/Spectralink VIEW certification. See [Advanced Options](#) under [Creating a WLAN](#) for more information.
- 11 Spectralink Compatibility:** (Disabled by default). Enable this option if this AP radio will be used as a voice WLAN for Polycom/Spectralink phones. This option changes several AP radio settings such as DTIM, BSS minrate and RTS-CTS to improve voice quality with Spectralink phones.

---

**NOTE:** For optimal VoWLAN voice quality, also disable Self-Healing and Background Scanning from the *Configure > Services* page).

---

- 12 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 Options](#) for creating a WLAN.
- 13 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.
- 14 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

15 If Smart Mesh is enabled (see [Deploying a Wireless Mesh via ZoneDirector](#)), the **Advanced Options** 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 Wireless 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.

16 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.

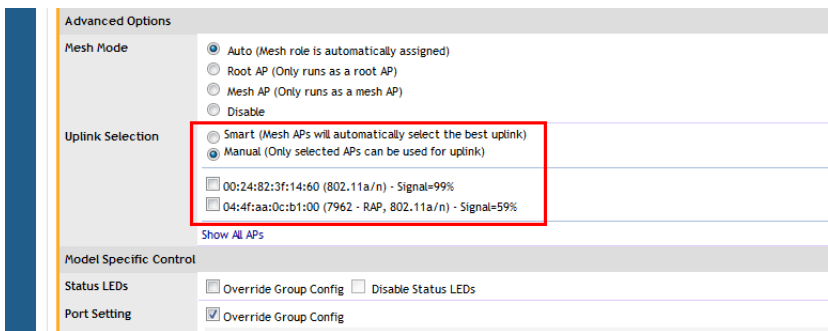
17 Select the check box next to each AP that you want to allow the current AP to use as an uplink.

---

**NOTE:** 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 Monitor > Access Points page will appear as *Isolated Mesh AP*. See [Troubleshooting Isolated Mesh APs](#) for more information.

---

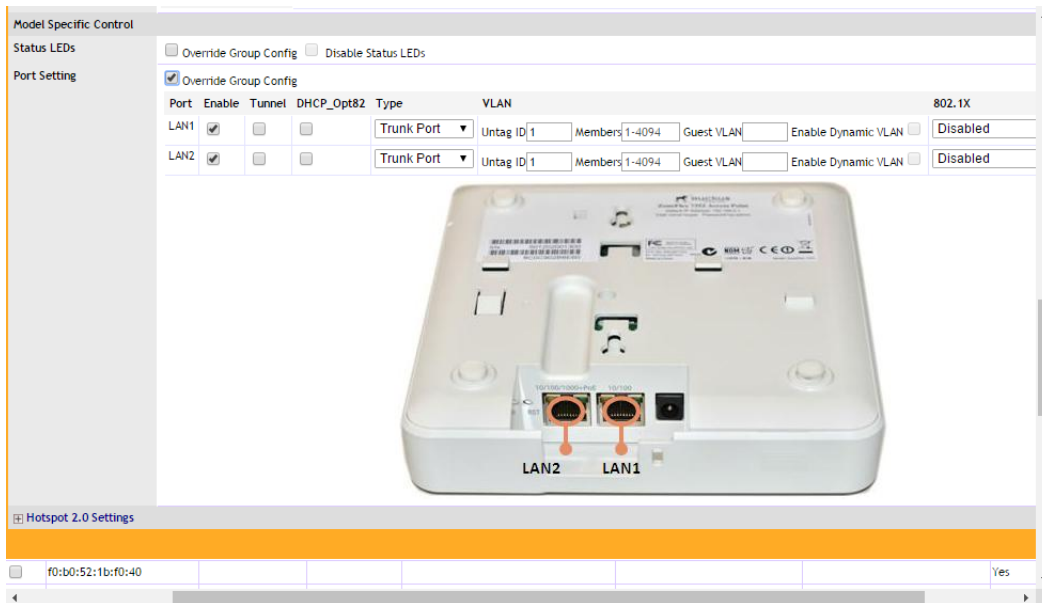
Figure 169. Manual uplink selection for APs in a mesh



18 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](#).

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

Figure 170. Ethernet port configuration - Override Group Config



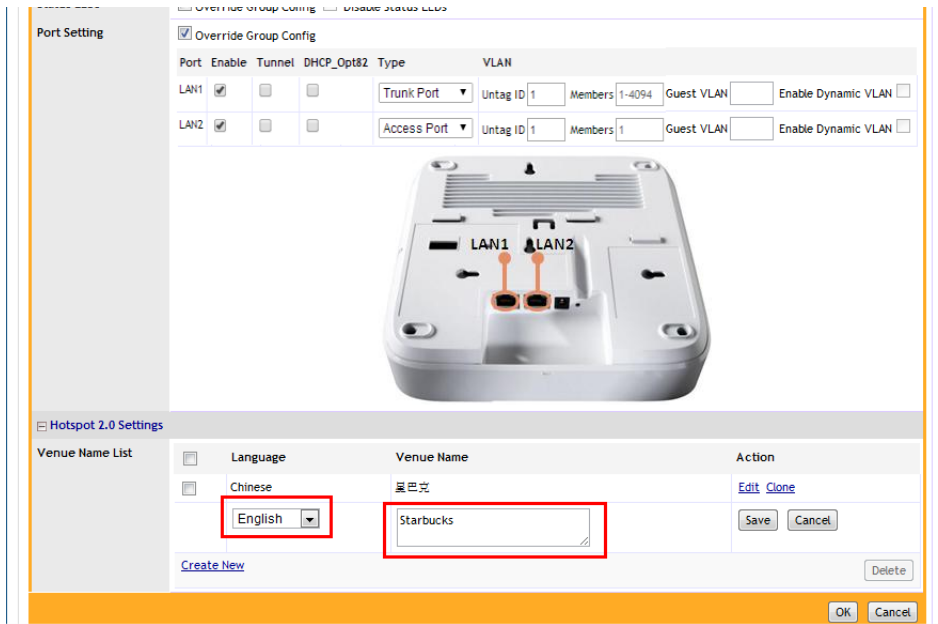
## Configuring Hotspot 2.0 Venue Settings for an AP

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 **Configure > Access Points**.
- 2 Click the **Edit** link next to the AP you want to configure.
- 3 Scroll down to the bottom and expand the **Hotspot 2.0 Settings** section.
- 4 Click **Create New** 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 171. Setting the Venue Name for a Hotspot 2.0 service AP



## Optimizing Access Point Performance

ZoneDirector, through its 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 network 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 Map View

**REQUIREMENT:** The importing of a floorplan and placement of APs are detailed in [Importing a Map View Floorplan Image](#) and [Placing the Access Point Markers](#).

- 1 Go to **Monitor > Map View**. If *Map View* displays a floorplan with active device symbols, you can assess the performance of individual APs, in terms of coverage. (For detailed information on the Map View, see [Using the Map View Tools](#).)
- 2 In the *Coverage* options, select **2.4 GHz** or **5 GHz** to view coverage for the radio band.

- 3 When the “heat map” appears, look for the Signal (%) scale in the upper right corner of the map.
- 4 Note the overall color range, especially colors that indicate low coverage.
- 5 Look at the floorplan and evaluate the current coverage. You can make adjustments as detailed in the following procedure.

## Improving AP RF Coverage

- 1 Click and drag individual AP markers to new positions on the Map View floorplan until your RF coverage coloration is optimized. There may be a need for additional APs to fill in large coverage gaps.
- 2 When your adjustments are complete, note the new locations of relocated AP markers.
- 3 After physically relocating the actual APs according to the Map View placements, reconnect the APs to a power source.
- 4 To refresh the ZoneDirector Map View, run a full-system RF Scan, as detailed in [Starting a Radio Frequency Scan](#).
- 5 When the RF scan is complete and ZoneDirector has recalibrated the Map View, you can assess your changes and make further adjustments as needed.

## Assessing Current Performance Using the Access Point Table

- 1 Go to **Monitor > Access Points**.
- 2 When the *Access Points* page appears, review the *Currently Managed APs* 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

- 1 Go to **Configure > 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 **Configure > WLANs**.
- 2 Click the **Edit** link next to the WLAN for which a lower priority will be set.
- 3 Select **Low** next to *Priority*, and click **OK**.

## Optimizing Access Point Performance

Prioritizing WLAN Traffic



In this chapter:

- [Reviewing the ZoneDirector Monitoring Options](#)
- [Importing a Map View Floorplan Image](#)
- [Using the Map View Tools](#)
- [Evaluating and Optimizing Network Coverage](#)
- [Reviewing Current Alarms](#)
- [Reviewing Recent Network Events](#)
- [Monitoring WLAN Status](#)
- [Reviewing Current User Activity](#)
- [Monitoring Individual Clients](#)
- [Monitoring Access Point Status](#)
- [Monitoring Individual APs](#)
- [Monitoring Mesh Status](#)
- [Detecting Rogue Access Points](#)
- [Monitoring System Ethernet Port Status](#)
- [Monitoring AAA Server Statistics](#)
- [Monitoring Location Services](#)

## Reviewing the ZoneDirector Monitoring Options

The following highlights key ZoneDirector tab options and what you can do with them.

- *Dashboard*: Every time you log into ZoneDirector via the web interface, this collection of status indicators appears. Use it as your regular network-monitoring starting point. Data are blue-colored links that you can use to further drill down to focus on particular activities or devices.
- *Real Time Monitoring*: To view network traffic, resource utilization and usage statistics in real time, use the Real Time Monitoring tool accessible via the Toolbox at the top of any page of the web interface (see [Real Time Monitoring](#)).
- *Monitor > Map View* provides a fast scan of key network factors: APs (legitimate, neighboring and rogue), client devices, and RF coverage. You can see what devices are where in your floorplan, and visually evaluate network coverage.

---

**NOTE:** For Map View to work, your computer must have Java version 7 installed. If it is not installed, ZoneDirector will notify you that you need to download it. The latest version can be downloaded from [www.java.com](http://www.java.com).

---

- Other *Monitor* tab options incorporated in the left column's buttons provide numeric data on WLAN performance and individual device activity. As with the Dashboard, some data entries are links that take you to more detailed information. And, finally, the All Events/Activities log displays the most recent actions by users, devices and network, in chronological order.
- *Configure*: Use the options in this tab to assess the current state of WLAN users, any restricted WLANs, along with the settings for guest access, user roles, etc. You can also combine this tab's options with those in the Administer tab to perform system diagnostics and other preventive tasks.

## Importing a Map View Floorplan Image

If your Ruckus ZoneDirector does not display a floorplan for your worksite when you open the Monitor tab Map View, you can import a floorplan and place AP markers in relevant locations by following the steps outlined in this section. The sample floorplan image cannot be deleted, but it can be replaced with an actual floorplan image file and relabeled. Then you can add additional floorplan maps for additional locations or floors.

You can import an unlimited number of floorplan images to ZoneDirector. However, the total file size of all imported floor maps is limited to 2MB on ZoneDirector 1200, and 10MB on ZoneDirector 3000/5000. An error message appears when these file size limits are reached.

Additionally, the maximum file size per floorplan image is 512kb. (200kb or smaller is recommended).

### Requirements

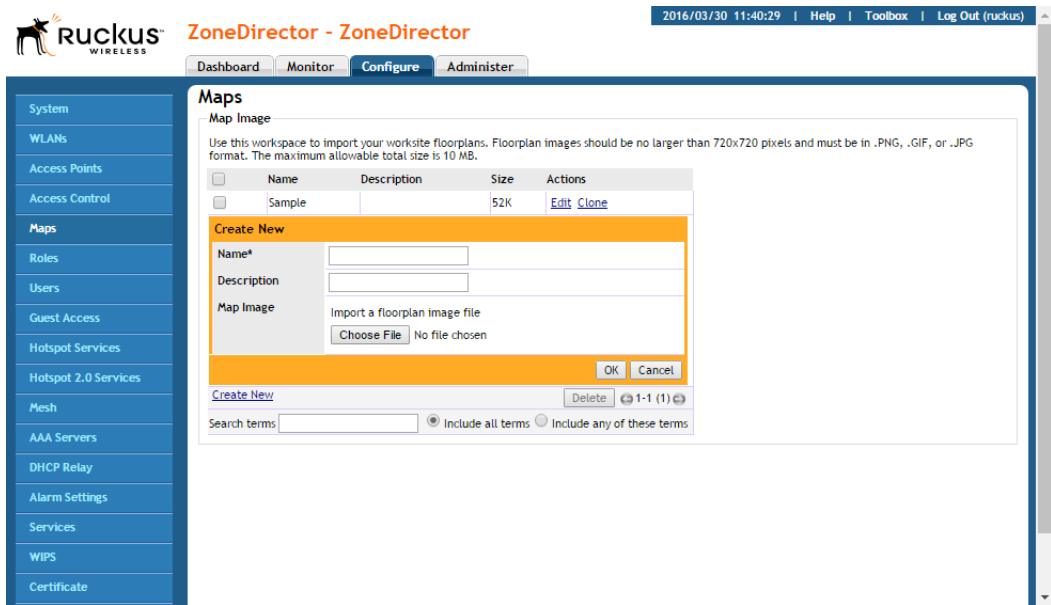
- A floorplan image in .GIF, .JPG or .PNG format
- The image should be monochrome or grayscale.
- The file size should be no larger than 200kb in size.
- The floorplan image should be (ideally) no larger than 10 inches (720 pixels) per side.

### Importing the Floorplan Image

- 1 Go to **Configure > Maps**.
- 2 Click **Create New**. The *Create New* form appears.
- 3 In **Name**, type a name to assign to the floorplan image that you will be importing. Type a description as well, if preferred.
- 4 Click **Browse**. The Choose File dialog box appears.
- 5 Browse to the location of the floorplan image file, select the file, and then click **Open** to import it. If the import is successful, a thumbnail version of the floorplan will appear in the *Map Image* area.
- 6 Go to **Monitor > Map View** to see this image.

You can now use the Map View to place the Access Point markers.

Figure 172. The Create New form for importing a floorplan image



## Placing the Access Point Markers

After using the **Configure > Maps** options to import your floorplan image, you can use the Monitor tab's Map View to distribute markers that represent the APs to the correct locations. This will give you a powerful monitoring tool.

**NOTE:** If you have imported multiple floor plans representing multiple floors in your building(s), make sure you place the access point markers on the correct floorplan.

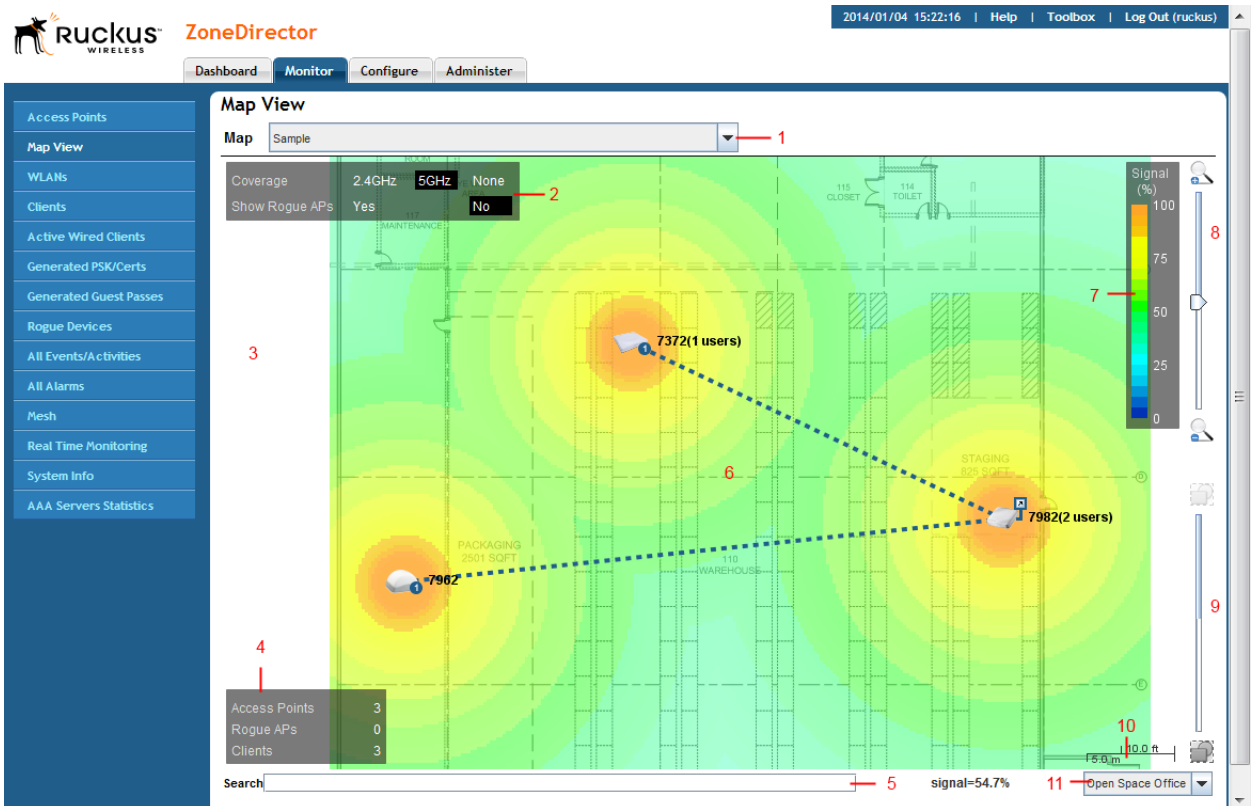
- 1 Have the list of APs handy, with MAC addresses and locations.
- 2 Go to **Monitor > Map View** (if it is not already in view).
- 3 Look in the upper left corner for AP marker icons. There should be one for each AP, with a tiny red question mark at the top.
- 4 Look at the MAC address notation under the marker icon, to identify a marker.
- 5 Drag each marker icon from the upper left corner into its correct location on the floorplan.

When you finish, you can make immediate use of the Map View to optimize your wireless coverage, as detailed in [Optimizing Access Point Performance](#).

# Using the Map View Tools

If your worksite floorplan has been scanned in and mapped with APs, the *Map View* will display a graphical image of your physical Ruckus network AP distribution.




Figure 173. Elements on the Map View



There are a number of helpful features built into the Map View, as noted here and marked in the above illustration:

- 1 *Map drop-down list*: Select the floorplan to view from the Map drop-down list.
- 2 *Coverage and Show Rogue APs box*: For Coverage, selecting 2.4 GHz enables a signal strength view of your placed 2.4 GHz APs. Selecting 5 GHz displays the signal coverage of 5 GHz radios. Selecting either 2.4 or 5 GHz opens the Signal (%) legend on the right side of the Map View. See item number 8 below for the description of the Signal%. For Show Rogue APs, selecting Yes displays the detected rogue APs in the floorplan.

- 3 *Unplaced APs area*: As noted in Importing a Map View Floorplan Image, when you first open the Map View, newly placed APs appear in this area. If they are approved for use (see [Adding New Access Points to the Network](#)), you can drag them into the correct location in the floorplan. Unplaced APs are available across all of the floor plans you upload. Thus, you can toggle between maps (see number 1) and place each AP on the appropriate map. For the various AP icon types, see [AP Icons](#).
- 4 *Access Points, Rogue APs, and Clients box*: This lower left corner box displays the number of active APs, any rogue (unapproved or illegitimate) APs, and all associated clients.
- 5 *Search text box*: Enter a string, such as part of an AP's name or MAC address, and the map is filtered to show only the matching results. Clearing the search value returns the map to its unfiltered view.
- 6 *Floorplan area*: The floorplan displays in this main area. You can manipulate the size and angle of the floorplan by using the tools on this screen. Note the following icons:

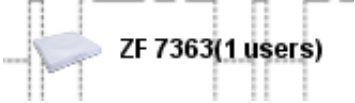







	Click this icon, and then click an AP from the floorplan to remove that AP.
	Click this icon to rotate the floorplan. When clicked, rotation crosshairs appear in the center of the map; click and hold these crosshairs and move your cursor to rotate the view.
	Refresh the floorplan.

- 7 *Signal (%)*: This colored legend displays the signal strength coverage when you selected either 2.4 GHz or 5 GHz for Coverage (see #2 above). See [Evaluating and Optimizing Network Coverage](#) for more information.
- 8 *Upper slider*: The upper slider is a zoom slider, allowing you to zoom in and out of the floorplan. This is helpful in exact AP marker placement, and in assessing whether physical obstructions that affect RF coverage are in place.
- 9 *Lower slider*: The bottom slider is the image contrast slider, allowing you to dim or enhance the presence of the floorplan. If you have trouble seeing the floorplan, move the slider until you achieve a satisfactory balance between markers and floorplan details.
- 10 *Scale legend*: To properly assess the distances in a floorplan, a scaler has been provided so that you can place APs in the most precise location.

- 11** *Open Space Office drop-down list:* Open Office Space refers to the methodology used to compute RF coverage/signal% (i.e., heat map) based on the current environment.

## AP Icons

Each AP marker has variable features that help indicate identity and status:

	<p>A normal AP marker displays the description of the AP and the number of users that are currently associated with the AP.</p>
	<p>An unplaced AP marker displays a “?” (question mark) above the icon.</p>
	<p>A rogue AP displays a smaller red icon imprinted with a “bug.”</p>
	<p>A “bug” icon with a lock on it indicates a rogue AP with security enabled.</p>
	<p>In a Smart Mesh network, an isolated AP displays a red “X” above the icon.</p>
	<p>When Smart Mesh is enabled, a circled number appears next to the AP icon to indicate that it is a Mesh AP. The number indicates the number of hops from this Mesh AP to the Root AP.</p>
	<p>When Smart Mesh is enabled, a blue square with an arrow indicates that it is a Root AP with active downlinks. Dotted lines that connect this AP to other APs indicate the active downlinks.</p>
	<p>When Smart Mesh is enabled, a gray square (dimmed) with an arrow indicates that it is a Root AP without any active downlinks.</p>



An AP with a red square with an arrow indicates this is an eMAP. An eMAP uses its wired Ethernet interface as its uplink, and can mesh with other Mesh APs through its wireless interface.

## Evaluating and Optimizing Network Coverage

If there are gaps or dead spots in your worksite WLAN coverage, you can use ZoneDirector to assess network RF coverage and then reposition APs to enhance coverage.

- 1 Go to **Monitor > Map View**.
- 2 If Map View displays a floorplan with active device symbols, you can assess the performance of individual APs, in terms of coverage. (See [Importing a Map View Floorplan Image](#) for information on setting up the Map View.)
- 3 For the *Coverage* option, click **2.4 GHz** or **5 GHz**.
- 4 When the “heat map” appears, look for a Signal% scale in the upper right corner of the map.
- 5 Note the color range, especially colors that indicate low coverage.
- 6 Look at the floorplan and evaluate the current coverage.

## Moving the APs into More Efficient Positions

You can now move the APs into more efficient positions.

- 1 To do so, click and drag individual AP markers on the Map View floorplan until your RF coverage coloration is optimized. (You may need to acquire additional APs to fill in large coverage gaps.)
- 2 Note the new physical locations of relocated AP markers.
- 3 After physically relocating the actual APs in accordance with Map View repositioning, reconnect each AP to a power source.

When ZoneDirector has recalibrated the Map View after each AP restart, you can assess your changes and make further adjustments as needed.

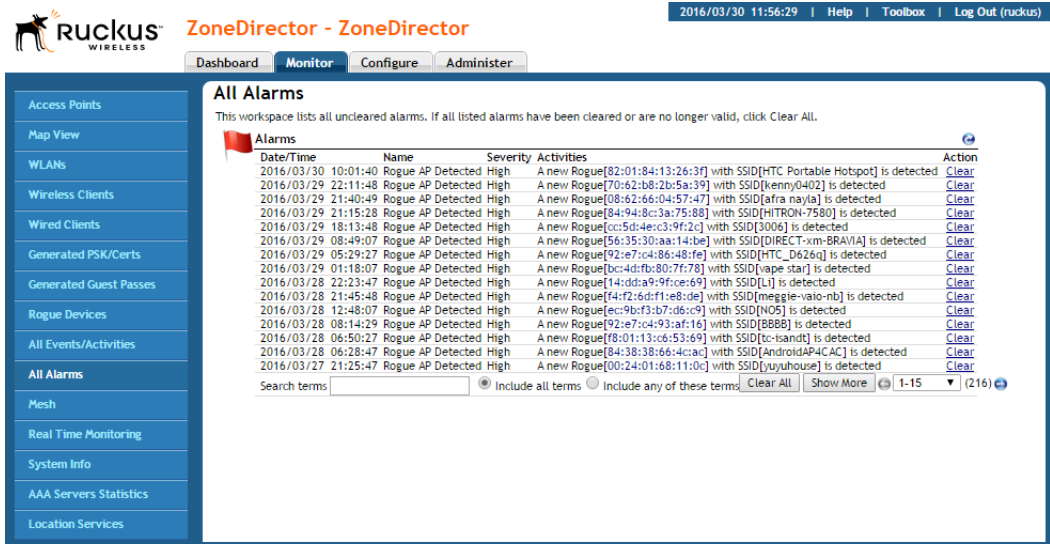


# Reviewing Current Alarms

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 **Monitor > All Alarms**.
- 2 When the *All Alarms* page appears, the *Alarms* table lists the unresolved alarms, the most recent at the top.

Figure 174. The All Alarms page



- 3 Review the contents of this table. The *Activities* column is especially informative.
- 4 If a listed alarm condition has been resolved, click the now-active **Clear** link to the right. You also have the option of clicking **Clear All** to resolve all alarms at one time.

# Reviewing Recent Network Events

You have two options for reviewing events in your network: [1] open a complete list of all events, or [2] look at specific lists of events in each Monitor tab workspace, such as the WLANs workspace “Events/Activities” table.

- 1 Open the ZoneDirector Dashboard and look at the *Most Recent User Activities* table and *Most Recent System Activities* table for summaries of activity in the network.
- 2 Go to the **Monitor** tab.
- 3 Click any of the specific options, such as WLANs, Access Points, or Clients.
- 4 Look for an *All Events* table that specifically focuses on the selected category.
- 5 Under the Monitor tab, click either the **All Alarms** button or the **All Events/Activities** button to see a complete list, with all categories represented in chronological order.

AP events display the first 17 characters of an AP name, if AP names are used. 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.

## Clearing Recent Events/Activities

To review the current events and, if appropriate, clear all resolved events, follow these steps:

- 1 Go to **Monitor > All Events/Activities**.
- 2 When the *All Events/Activities* page appears, the *Events/Activities* table lists the unresolved events, the most recent at the top.
- 3 Review the contents of this table. You can sort the list by severity level, date/time, user name and activity type. Click the column header to sort, and click again to reverse the order displayed.
- 4 You can click **Clear All** at the bottom of the table to resolve and clear all events in the view.

## Monitoring WLAN Status

The Monitor > WLANs page lists the currently deployed WLANs, WLAN Groups, VLAN Pools, Events/Activities and RADIUS statistics for any WLANs that use RADIUS authentication.

Figure 175. The Monitor > WLANs page

**ZoneDirector - ZoneDirector**

2016/03/30 11:57:43 | Help | Toolbox | Log Out (ruckus)

Dashboard Monitor Configure Administer

### WLANs

These tables list [1] currently active WLANs, [2] currently active WLAN Groups, and [3] an up-to-date record of WLAN events/activities. Click on a WLAN-name name link or MAC-address link for more details.

#### Currently Active WLANs

Name	ESSID	Authentication	Encryption	VLAN	Clients
<a href="#">Ruckus-Wireless-1</a>	Ruckus-Wireless-1	open	wpa2	1	1

Search terms:  Include all terms Include any of these terms 1-1 (1)

#### Currently Active WLAN Groups

Name	Description	WLANs
Default	Default WLANs for Access Points	Ruckus-Wireless-1

Search terms:  Include all terms Include any of these terms 1-1 (1)

#### Currently Active VLAN Pools

Name	Description	VLANs	VLAN:Users	WLANs

Search terms:  Include all terms Include any of these terms 0-0 (0)

#### RADIUS Statistics

Name	Access Requests	Access Rejects	Access Retries	Access Timeouts	Accounting Requests	Accounting ACKs	Accounting Retries	Accounting
------	-----------------	----------------	----------------	-----------------	---------------------	-----------------	--------------------	------------

Search terms:  Include all terms Include any of these terms Select Display Span for the latest 1 day Reset

#### Events/Activities

Date/Time	Severity	User	Activities
2016/03/11 09:28:19	Medium	User[1c:b7:2c:30:12:d3]	repeatedly fails authentication when joining WLAN[Ruckus-Wireless-1] at AP[0:c0:c5:20:20:00:00:00]
2016/02/01 23:39:36	High	User[1c:b7:2c:30:12:d3]	fails authentication too many times in a row when joining WLAN[Ruckus-Wireless-1] at AP[0:c0:c5:20:20:00:00:00]. User[1c:b7:2c:30:12:d3] is temporarily blocked from the system for [30 seconds].
2016/02/01 23:35:10	Medium	User[1c:b7:2c:30:12:d3]	repeatedly fails authentication when joining WLAN[Ruckus-Wireless-1] at AP[0:c0:c5:20:20:00:00:00]
2016/02/01 23:29:27	Medium	User[1c:b7:2c:30:12:d3]	repeatedly fails authentication when joining WLAN[Ruckus-Wireless-1] at AP[0:c0:c5:20:20:00:00:00]
2016/02/01 23:17:10	Medium	User[1c:b7:2c:30:12:d3]	repeatedly fails authentication when joining WLAN[Ruckus-Wireless-1] at AP[0:c0:c5:20:20:00:00:00]
2016/02/01 23:09:25	Medium	User[1c:b7:2c:30:12:d3]	repeatedly fails authentication when joining WLAN[Ruckus-Wireless-1] at AP[0:c0:c5:20:20:00:00:00]
2016/02/01 22:30:18	Medium	User[1c:b7:2c:30:12:d3]	repeatedly fails authentication when joining WLAN[Ruckus-Wireless-1] at AP[0:c0:c5:20:20:00:00:00]

# Reviewing Current User Activity

You can monitor current wireless users by viewing a general overview and on a per-client basis by doing the following:

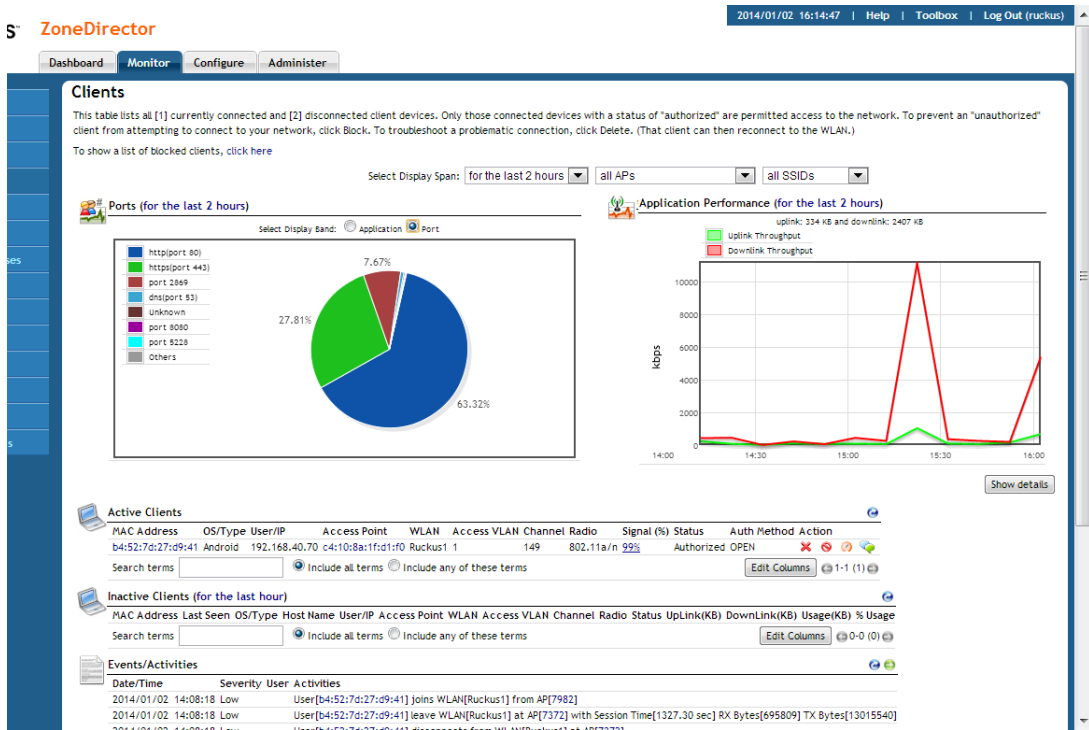
- 1 Go to **Monitor > Wireless Clients**.
- 2 When the *Clients* page appears, review the table for a general survey.
- 3 Click any client device MAC address link to monitor that client in more detail.

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.

## 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 the values displayed in the charts.

Figure 176. Monitoring client activity



Click the **Show Details** button to display detailed application or port usage percentages.

Figure 177. Click Show Details to view application usage statistics

The screenshot shows the Ruckus ZoneDirector interface. The top navigation bar includes the Ruckus logo, the title 'ZoneDirector - ZoneDirector', and the date/time '2016/03/30 14:16:13'. Below the navigation bar are tabs for 'Dashboard', 'Monitor', 'Configure', and 'Administrator'. The left sidebar contains a menu with items like 'Access Points', 'Map View', 'WLANs', 'Wireless Clients', 'Wired Clients', 'Generated PSK/Certs', 'Generated Guest Passes', 'Rogue Devices', 'All Events/Activities', 'All Alarms', 'Mesh', 'Real Time Monitoring', 'System Info', 'AAA Servers Statistics', and 'Location Services'. The main content area is titled 'Wireless Clients' and contains a summary of connected and disconnected devices, a pie chart for application usage, and a table of active clients. A red box highlights the 'Show details' button in the 'Applications (for the last 1 hour)' section.

**Wireless Clients**  
This table lists all [1] currently connected and [2] disconnected client devices. Only those connected devices with a status of "authorized" are permitted access attempting to connect to your network, click Block. To troubleshoot a problematic connection, click Delete. (That client can then reconnect to the WLAN.) To show a list of blocked clients, click here

Select Display Span: for the last 1 hour | all APs | all S

**Applications (for the last 1 hour)**  
Select Display: Application Port

Application	Percentage
skype	36.45%
Miscellaneous	12.13%
google-plus	10.97%
trouter.io	10.90%
microsoft authentication via ssl	8.06%
dns	4.90%
hotmail.com	4.00%
ssl/rts	3.97%
facebook	3.46%
skype.net	3.20%
Others	12.13%

**Application Performance**  
Uplink Thru (Mbps) | Downlink Thru (Mbps)

**Show details** | Top 10 Clients

**Active Clients**

MAC Address	OS/Type	Host Name	User/IP	Role	Access Point	WLAN	Access VLAN	Channel	Radio
4c:21:d0:16:a42:24	Android	android-216ef6f02a5a3df9	192.168.40.11		cd:c5:20:3b:91:f0	Ruckus-Wireless-1	1	11	802.

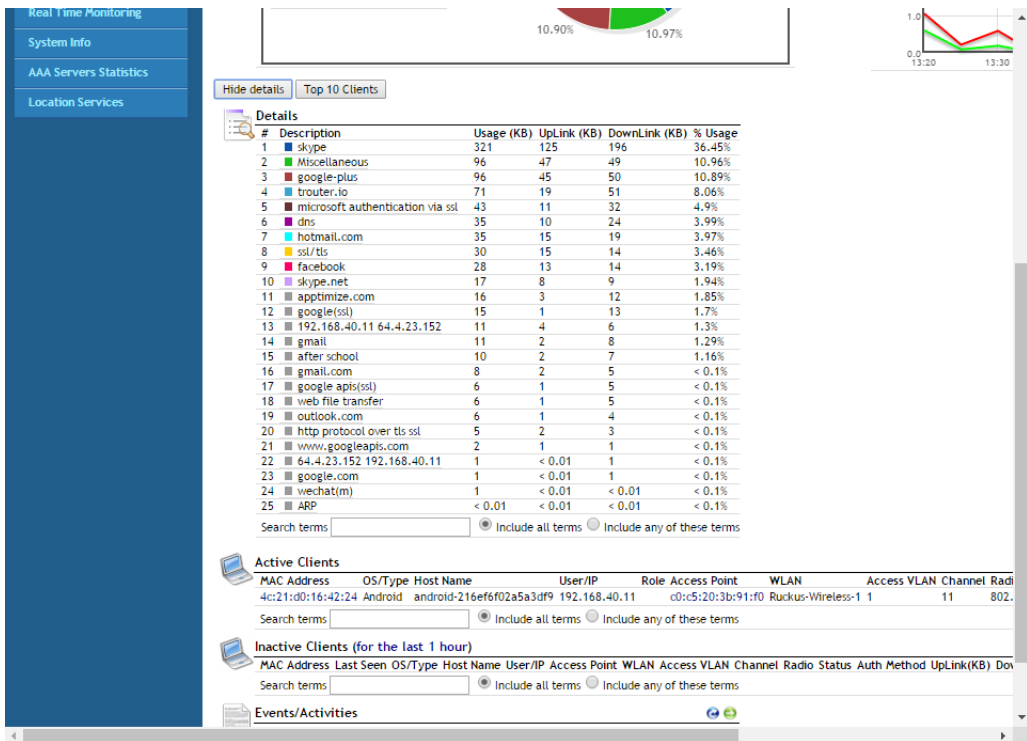
**Inactive Clients (for the last 1 hour)**

MAC Address	Last Seen	OS/Type	Host Name	User/IP	Access Point	WLAN	Access VLAN	Channel	Radio	Status	Auth Method	UpLink(KB)	DownLink(KB)
-------------	-----------	---------	-----------	---------	--------------	------	-------------	---------	-------	--------	-------------	------------	--------------

**Events/Activities**

Date/Time	Severity	User	Activities
-----------	----------	------	------------

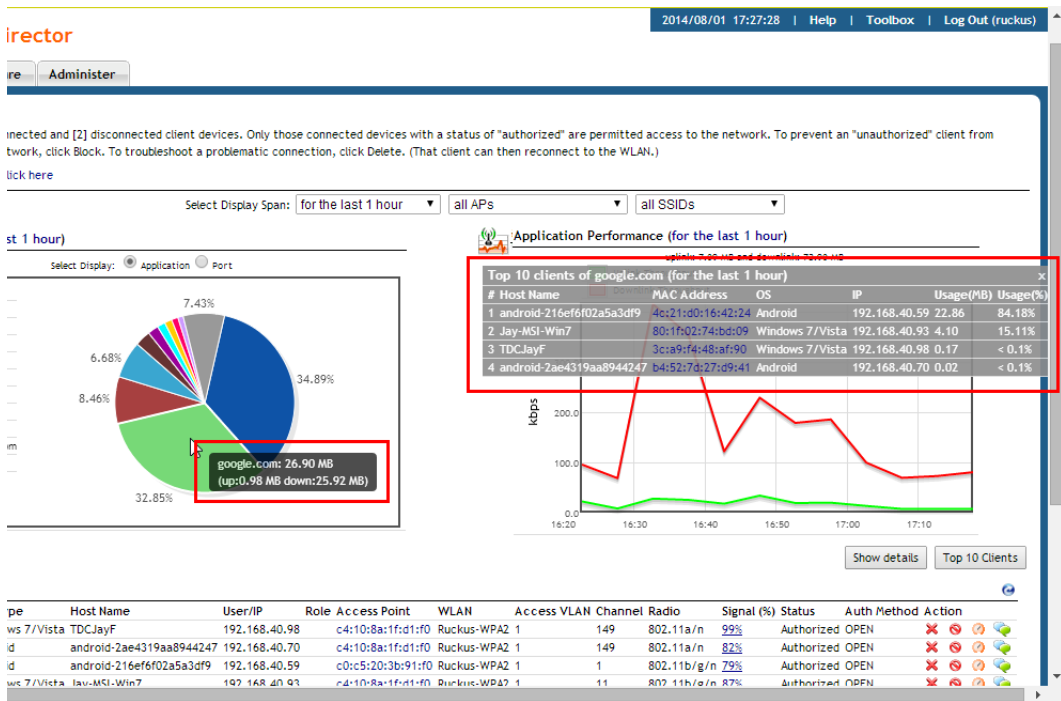
Figure 178. Client application usage details table



## 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 10 clients responsible for this traffic.

Figure 179. Viewing the top 10 clients of an application

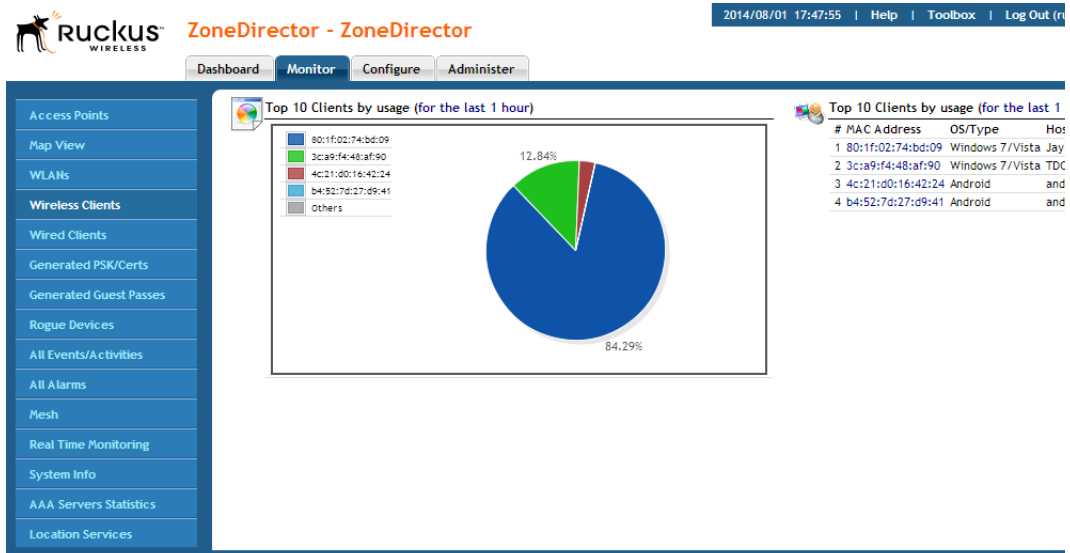


## Viewing the Top 10 Clients by Usage

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 180. Click the “Top 10 Clients” button to view details on the top clients by traffic volume



## Active Clients

The Active Clients table displays a list of active wireless clients. You can customize the columns displayed by clicking the **Edit Columns** button. You can also delete, block, run SpeedFlex and test connectivity using the action icons in this table.

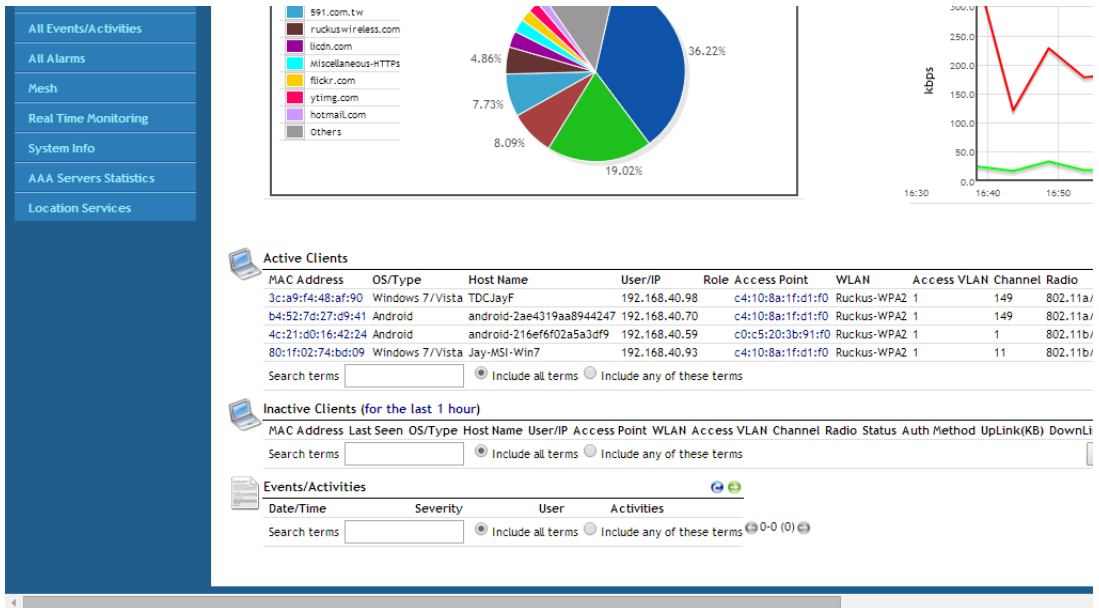
## Inactive Clients

The Inactive Clients table displays a list of inactive clients and can be used to view usage statistics of recently disconnected clients.

## Events/Activities

The Events/Activities table displays a client-specific subset of the events listed on the All Events/Activities page.

Figure 181. Monitoring Clients



## 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:

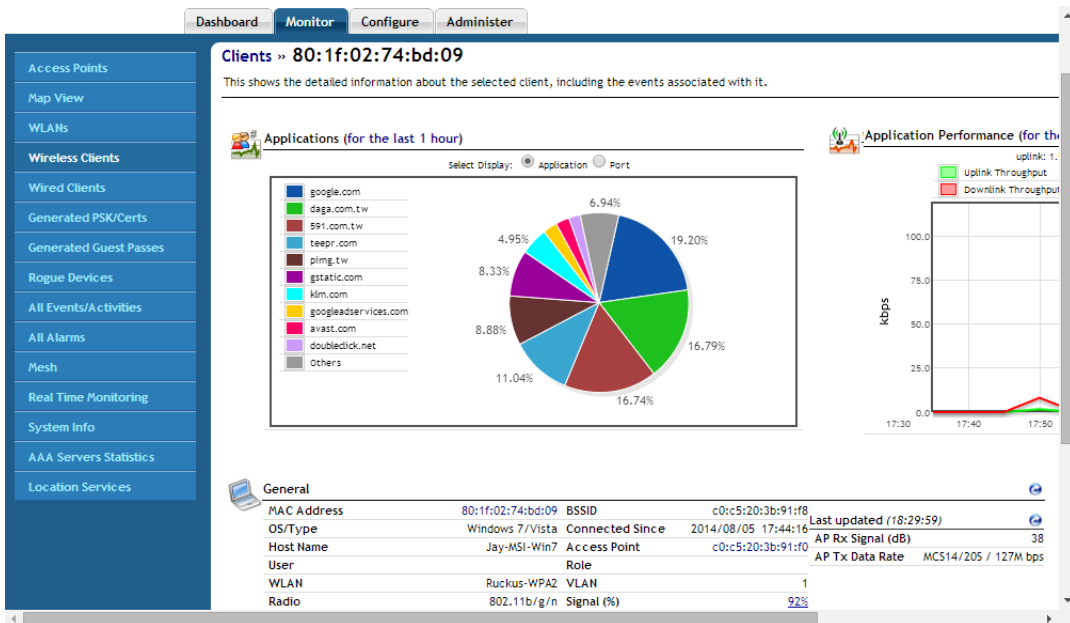
- 1 Go to **Monitor > Wireless Clients**.
- 2 Click the link for the MAC address of the client you want to monitor. The page refreshes to display a page of client specific information and statistics.

The *Monitoring > Clients > [client MAC address]* page displays the following information about the connected client.

Table 29. Client information details

Heading	Description
Applications/Ports and Application Performance Charts	Displays client application usage and throughput in pie chart and time graph formats. Click <b>Show Details</b> to view application usage statistics for this client.
General	<ul style="list-style-type: none"> <li>• Displays general information on the client, including Host Name, OS, AP, WLAN, channel, and signal strength indication.</li> <li>• The <i>Last Updated</i> column 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 <a href="http://en.wikipedia.org/wiki/IEEE_802.11n-2009">http://en.wikipedia.org/wiki/IEEE_802.11n-2009</a>), the channel width (20S or 40S), and the data rate in Mbps.</li> <li>• Contains a Client Performance icon (see <a href="#">Monitoring Client Performance</a>).</li> </ul>
Events	Displays a client-specific subset of the events in the All Events/Activities table.

Figure 182. Viewing individual client information and performance statistics



## 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 **Monitor > Wireless Clients** and locate the client MAC address in the *Active Clients* list.
- 2 Click the client's MAC address link to view the client details page.
- 3 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 183. The Client Performance icon

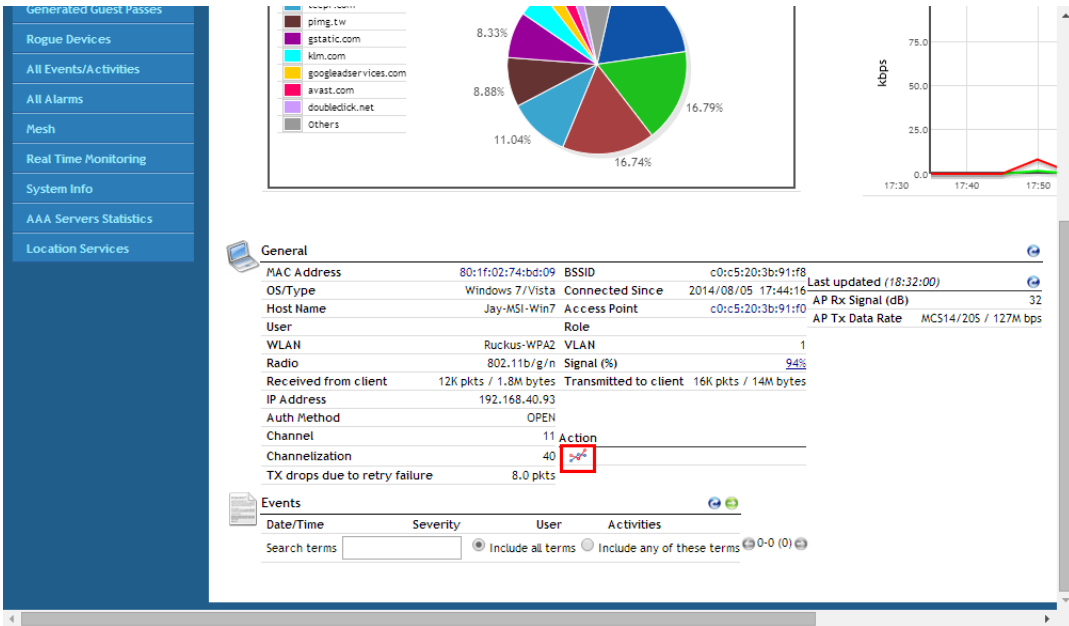
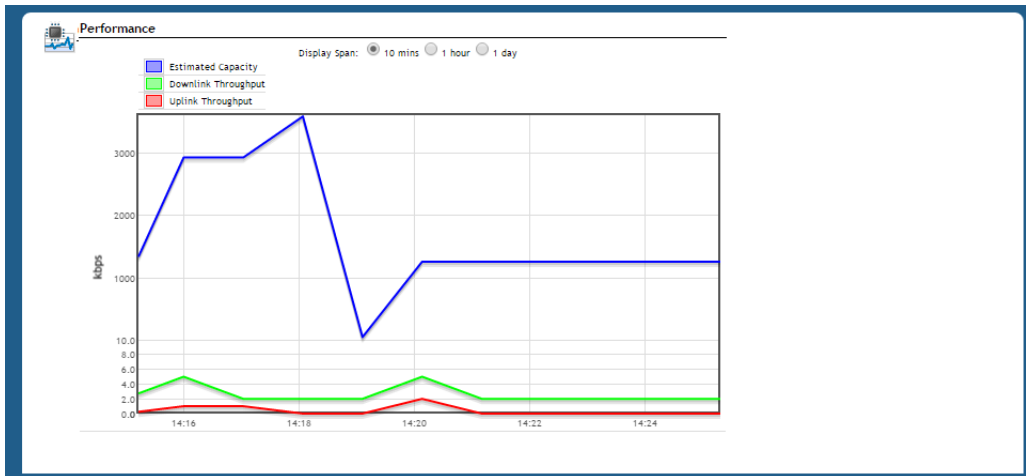


Figure 184. Client Performance chart



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 also monitor currently connected wired clients using the **Monitor > 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 port number, VLAN and authorization status. Click the delete button to remove the entry of the wired client. The *Events / Activities* table displays recent connection and authentication events related to wired clients only.

## Monitoring Access Point Status

ZoneDirector provides several different features for monitoring the status and performance of your APs. The following are three ways you can quickly locate information on the APs that ZoneDirector is managing:

- Open the **Dashboard** for a snapshot of the most active APs. Click the MAC address link of any AP record to see more details.
- Go to **Monitor > Map View** and click a radio frequency to see a heat-map rendering of the current RF coverage.
- Go to **Monitor > Access Points** and review the usage and coverage of your APs. Click the MAC address link of any listed APs to see more details.

## Using the AP Status Overview Page

The **Monitor > Access Points** page provides an overview of currently managed APs and consists of three tables: *Currently Managed APs*, *Currently Managed AP Groups* and *Events/Activities*. These tables list the first 15 entries by default and can be expanded using the **Show More** button. Click on the MAC address, AP name or user name for more detailed information on the specific AP or client.

### Currently Managed APs

The *Currently Managed APs* table includes the following information:

Table 30. Currently managed APs

Heading	Description
MAC Address	The AP's MAC address. Click this link to view details specific to this AP.
Device Name	The AP's "name." This can be modified on the <b>Configure &gt; Access Points</b> page by clicking the <b>Edit</b> link next to the AP's MAC address.
Description	The AP's "description." This can be modified on the <b>Configure &gt; Access Points</b> page by clicking the <b>Edit</b> link next to the AP's MAC address.
Location	The AP's "location." This can be modified on the <b>Configure &gt; Access Points</b> page by clicking the <b>Edit</b> link next to the AP's MAC address.
Model	The ZoneFlex model number.
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
Mesh Mode	Displays whether the AP is manually set as a Root or Mesh AP, or set to automatically choose Mesh mode.
IP Address	The IP address of the AP.

## Monitoring Access Point Status

Using the AP Status Overview Page

External IP: Port	This column displays the public IP and port number for APs connected via Layer 3 behind a NAT device.
VLAN	The VLAN ID, if configured.
Channel	Displays the channel number and channel width. On dual band APs, details for each radio are shown.
Clients	The number of clients currently connected to this AP.
Bonjour Gateway	Indicates whether Bonjour Gateway service is enabled, disabled or not supported on this AP.
Application Capability	Indicates whether Application Visibility is enabled, disabled or not supported on this AP.
Action	These icons allow you to configure and troubleshoot APs individually. See <a href="#">Using Action Icons to Configure and Troubleshoot APs in a Mesh</a> .

### ***Export to CSV***

The Currently Managed APs table can be exported as a CSV file, which can be opened in a spreadsheet program such as Microsoft Excel. Once you have finished editing which columns you want to display, the option to **Export to CSV** appears. 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.



Figure 185. Saving a managed AP list as a CSV file

The screenshot shows the Ruckus ZoneDirector interface. The top navigation bar includes the Ruckus logo, the text 'ZoneDirector - ZoneDirector', and a status bar with the date '2016/03/30 14:31:47' and links for 'Help', 'Toolbox', and 'Log Out (ruckus)'. Below this is a secondary navigation bar with 'Dashboard', 'Monitor', 'Configure', and 'Administer' tabs. The main content area is titled 'Access Points' and contains three sections: 'Currently Managed APs', 'Currently Managed AP Groups', and 'Events/Activities'. The 'Currently Managed APs' section features a table with columns for MAC Address, Device Name, Model, Status, Mesh Mode, IP Address, Channel, Clients, Application Capability, and Action. A search bar is located below the table, and an 'Export to CSV' button is highlighted with a red box. The 'Currently Managed AP Groups' section shows a table with columns for Member, Device Name/Description, APs, Clients, Status, and Action. The 'Events/Activities' section displays a list of events with columns for Date/Time, Severity, User, and Activities. A search bar and a 'Show More' button are also present in this section.

## Currently Managed AP Groups

Click the + icon to expand the AP group to display all members of the group.

Figure 186. Viewing AP group members

The screenshot shows the Ruckus ZoneDirector interface. The 'Monitor' tab is active. The 'Access Points' section is expanded, showing 'Currently Managed AP Groups'. A red box highlights this section. Below it, the 'Events/Activities' table is visible, listing various rogue device detections.

Member	Device Name/Description	APs	Clients	Status	Action
System Default	System default group for Access Points	3	1	Disconnected	[Action icons]
f0:b0:52:1b:f0:40		0	0	Disconnected	[Action icons]
c0:c5:20:3b:91:f0	RuckusAP	1	1	Connected	[Action icons]
f0:b0:52:1c:12:c0		0	0	Disconnected	[Action icons]

Date/Time	Severity	User	Activities
2016/03/30 10:01:40	High		A new Rogue[82:01:84:13:26:3f] with SSID[HTC Portable Hotspot] is detected
2016/03/29 22:11:48	High		A new Rogue[70:62:b8:2b:5a:39] with SSID[Kenny0402] is detected
2016/03/29 21:40:49	High		A new Rogue[08:62:66:04:57:47] with SSID[afra naya] is detected
2016/03/29 21:15:28	High		A new Rogue[84:94:8c:3a:75:88] with SSID[HiTRON-7580] is detected
2016/03/29 18:13:48	High		A new Rogue[cc:5d:4e:c3:9f:2c] with SSID[3006] is detected
2016/03/29 08:49:07	High		A new Rogue[56:35:30:aa:14:be] with SSID[DIRECT-xm-BRAVIA] is detected
2016/03/29 05:29:27	High		A new Rogue[92:e7:4:86:48:fe] with SSID[HTC_D626a] is detected
2016/03/29 01:18:07	High		A new Rogue[b3:4d:fb:80:7f:78] with SSID[vape-star] is detected
2016/03/28 22:23:47	High		A new Rogue[14:dda9:9f:ce:69] with SSID[L] is detected
2016/03/28 21:45:48	High		A new Rogue[f4:f2:6d:f1:e8:de] with SSID[meggie-vato-nb] is detected
2016/03/28 17:05:07	High		A new Rogue[84:94:8c:3a:75:88] with SSID[HiTRON-7580] is detected
2016/03/28 12:48:07	High		A new Rogue[ec:9b:f3:b7:d6:c9] with SSID[NO5] is detected
2016/03/28 08:14:29	High		A new Rogue[92:e7:c4:93:af:16] with SSID[B88B] is detected
2016/03/28 06:50:27	High		A new Rogue[f8:01:13:c6:53:69] with SSID[tc-isandt] is detected
2016/03/28 06:28:47	High		A new Rogue[84:38:38:66:4c:ac] with SSID[AndroidAPAC] is detected

## Events/Activities

This table displays an AP-related subset of the information on the **Monitor > All Events/Activities** page.

## Monitoring Individual APs

When you click on the MAC address of any AP, the **Monitor > Access Points** page changes to a detailed view of information related to that specific AP.

You can also click the AP name or MAC address in any of the tables or dashboard widgets in which it appears as a link to go directly to the AP detail page.

The **Monitor > Access Points > [MAC Address]** page provides the following details on the specific AP:

Table 31. AP Information details

Heading	Description
General	Displays general information on the AP, including software version, IP address and model number.
Info	Displays uptime, clients and mesh status.
Actions	Action icons provide tools for managing the AP (see <a href="#">Using Action Icons to Manage and Troubleshoot APs</a> ). On supported APs, an additional <a href="#">Spectrum Analysis</a> icon launches the spectrum analysis tool.
WLANs	Displays the WLANs that this AP is supporting.
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.

## Monitoring Individual APs











### Using Action Icons to Manage and Troubleshoot APs

Performance	<p>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 the maximum potential throughput of a particular client or the current mix of clients. 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 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.</p> <p>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 <a href="#">RF Pollution FAQ</a> for more information.)</p>
Neighbor APs	Displays nearby APs, their channel and signal strength.
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 " <a href="#">Orientation</a> " below 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	Displays an AP-related subset of the <i>All Events / Activities</i> table.

## Using Action Icons to Manage and Troubleshoot APs

The following action icons are used to perform configuration and troubleshooting tasks on the respective AP.

Table 32. Action icons

Icon	Icon Name	Action
	System Info	Generate a log file (support.txt) containing system information on this AP.
	Configure	Go to the Configure > 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 <i>Configure &gt; Access Points</i> page.
	RF Info	Generates a log file called <i>info.txt</i> , containing radio frequency data that can be used for troubleshooting the RF environment.
	Join Another Controller	Click this button to migrate an AP to another controller. For more information, see <a href="#">Migrating an AP from ZoneDirector to Another Controller</a> .

## 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.

- 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 *Smart-Zone Admin Guide*.

If you have blocked an AP this way and want to allow it to join ZoneDirector again, go to **Configure > Access Points** and click **Allow**.

Figure 187. Click Allow to allow the AP to re-join ZoneDirector

The screenshot shows the Ruckus Wireless configuration interface. The 'Configure' tab is selected, and the 'Access Points' menu item is highlighted. The 'Access Points' page displays a table of access points that have already been approved to join the network, or are pending approval. A red arrow points to the 'Allow' link in the 'Approved Action' column for the first row.

MAC Address	Device Name	Description	Channel	TX Power	WLAN Group	Approved Action
<input type="checkbox"/> 2c:5d:93:09:44:b0	RuckusAP			*(11a/n-), *(11b/g/n-*)	*(11a/n), *(11b/g/n)	No <a href="#">Edit</a> <a href="#">Allow</a>
<input type="checkbox"/> 58:b6:33:15:c5:10	RuckusAP			*(11a/n/ac-), *(11b/g/n-*)	*(11a/n/ac), *(11b/g/n)	Yes <a href="#">Edit</a>
<input type="checkbox"/> f8:e7:1e:13:4f:90						Yes <a href="#">Edit</a>
<input type="checkbox"/> e0:10:7f:28:26:30	RuckusAP			*(11a/n/ac-), *(11b/g/n-*)	*(11a/n/ac), *(11b/g/n)	Yes <a href="#">Edit</a>
<input type="checkbox"/> 74:3e:2b:10:33:c0						Yes <a href="#">Edit</a>
<input type="checkbox"/> 84:18:3a:34:1e:50						Yes <a href="#">Edit</a>
<input type="checkbox"/> ec:8ca2:26:53:30						Yes <a href="#">Edit</a>
<input type="checkbox"/> 2c:5d:93:15:db:d0	RuckusAP			*(11a/n-), *(11b/g/n-*)	*(11a/n), *(11b/g/n)	Yes <a href="#">Edit</a>

\* = Use Group Configuration  1-8 (8)

Search terms:   Include all terms  Include any of these terms

If you need to import the APs configuration, click Browse, and then select the backup file that contains the settings that you want to import.

No file chosen

## 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 are indicative of 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.

Figure 188. Viewing an individual AP's information

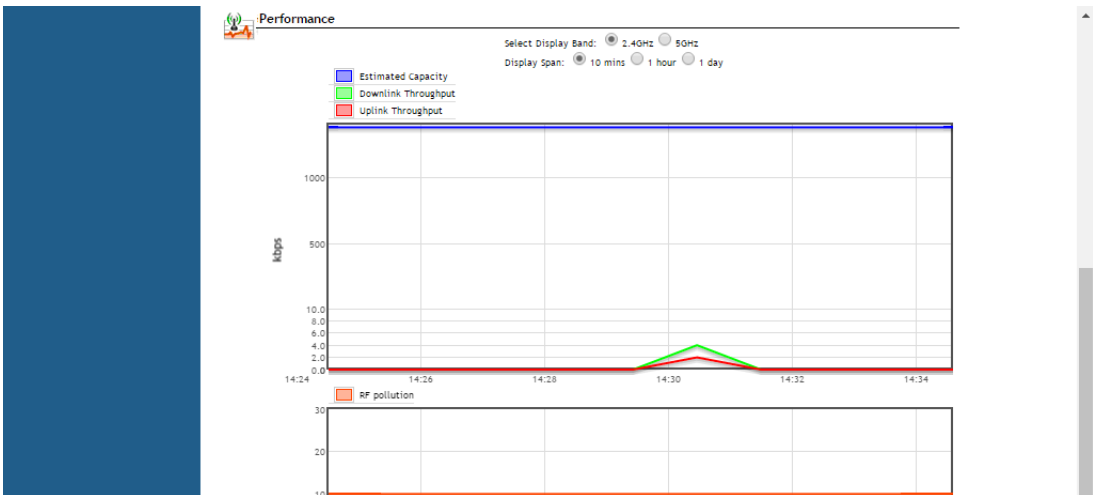
The screenshot shows the Ruckus ZoneDirector interface. The top navigation bar includes 'Dashboard', 'Monitor', 'Configure', and 'Administer'. The left sidebar lists various monitoring categories like 'Access Points', 'WLANs', and 'Wireless Clients'. The main content area displays 'Access Points >> c0:c5:20:3b:91:f0'. Below this, a table lists detailed information about the selected AP, categorized into 'General' and 'Info'.

General		Info	
Device Name	RuckusAP	Status	Connected
Description		Certificate Status	Non Ruckus PKI Certificate
Location		Uptime	13d 1h 2m
GPS Coordinates		Connection Mode	L3 (IPv4)
MAC Address	c0:c5:20:3b:91:f0	VLAN	1
IP Address	192.168.40.10	Associated Clients	1
External IP:Port	192.168.40.10:12223	Bonjour Gateway	Disabled
IP Type	DHCP		
Model	z7372		
USB Port	Not Present		
Power Consumption Mode	Not Support		
S/N	981202006357	Actions	
Version	9.13.0.0.87		

Radio 802.11b/g/n		Radio 802.11a/n	
Current Channel	11	Current Channel	36
Config Channel	Auto	Config Channel	Auto
Channelization	20	Channelization	40
WLAN Group	Default	WLAN Group	Default
SpectralLink Compatibility	Disabled	SpectralLink Compatibility	Disabled
WLAN Service	Enabled	WLAN Service	Enabled
Deployed/Maximum/WLAN-Group WLAN Number	1/27/1	Deployed/Maximum/WLAN-Group WLAN Number	1/27/1
Background Scanning	Enabled	Background Scanning	Enabled
TX Power	Full	TX Power	Full
# of Authorized Client Devices	1	# of Authorized Client Devices	0
% Retries/% Drops	1.27 / 0.00	% Retries/% Drops	0.259 / 0.00
% Non-unicast	0.00247	% Non-unicast	0.0322
Packets/Bytes Received	9.1M/1.8G	Packets/Bytes Received	114K/21M
Packets/Bytes Transmitted	5.1M/1.4G	Packets/Bytes Transmitted	262K/78M
Wlans Data Packets/Bytes Received	1.3M/169M	Wlans Data Packets/Bytes Received	34K/9.6M
Wlans Data Packets/Bytes Transmitted	2.0M/717M	Wlans Data Packets/Bytes Transmitted	65K/49M
Noise Floor	-90	Noise Floor	-113
PHY Errors	88	PHY Errors	88
% AirTime (total/busy/RX/TX)	4.3/2.1/1.5/1.0	% AirTime (total/busy/RX/TX)	0.0/0.0/0.0/0.0
Available Channel	1,2,3,4,5,6,7,8,9,10,11	Available Channel	36,40,44,48,149,153,157,161
Block Channel		Block Channel	165

Figure 189. Monitoring an AP's performance





## 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 **Monitor > Access Points** and click the MAC address of the AP to view the AP detailed information page.
- 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 190. APs that support spectrum analysis display an extra icon in the Actions table

**Ruckus WIRELESS ZoneDirector - ZoneDirector** 2016/03/30 14:37:15 | Help | Toolbox | Log Out (ruckus)

Dashboard Monitor **Configure** Administer

Access Points >> c0:c5:20:3b:91:f0

This table lists detailed information about the selected access point, such as the clients and events associated with it.

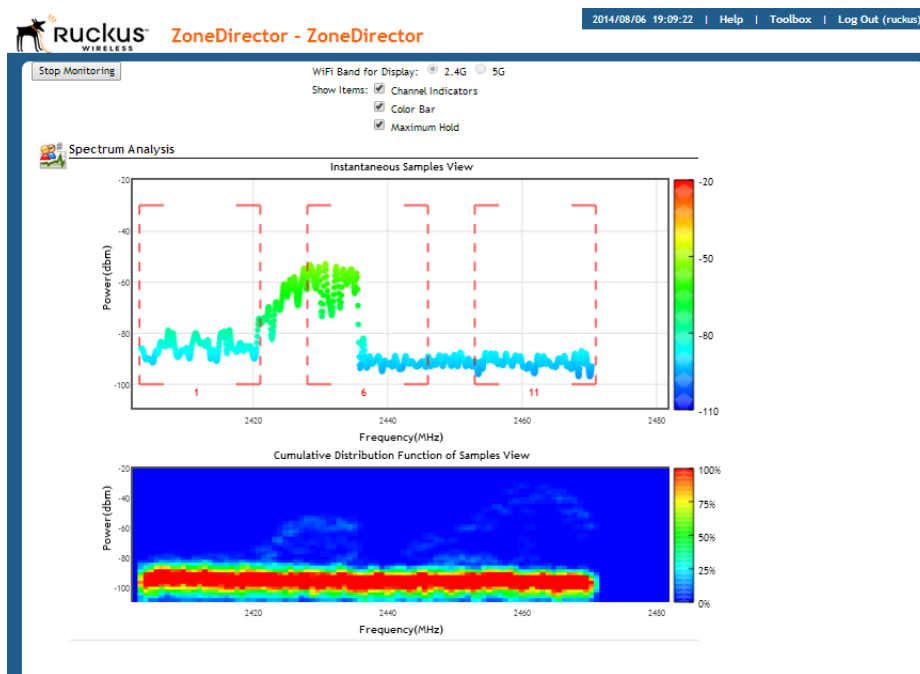
**Access Point Information**

General		Info	
Device Name	RuckusAP	Status	Connected
Description		Certificate Status	Non Ruckus PKI Certificate
Location		Uptime	13d 1h 4m
GPS Coordinates		Connection Mode	L3 (IPv4)
MAC Address	c0:c5:20:3b:91:f0	VLAN	1
IP Address	192.168.40.10	Associated Clients	1
External IP:Port	192.168.40.10:12223	Bonjour Gateway	Disabled
IP Type	DHCP		
Model	z7372		
USB Port	Not Present		
Power Consumption Mode	Not Support		
S/N	981202006357		
Version	9.13.0.0.87		

**Actions**

Radio 802.11b/g/n		Radio 802.11a/n	
Current Channel	11	Current Channel	36
Config Channel	Auto	Config Channel	Auto
Channelization	20	Channelization	40
WLAN Group	Default	WLAN Group	Default
SpectralLink Compatibility	Disabled	SpectralLink Compatibility	Disabled
WLAN Service	Enabled	WLAN Service	Enabled
Deployed/Maximum/WLAN-Group WLAN Number	1/27/1	Deployed/Maximum/WLAN-Group WLAN Number	1/27/1
Background Scanning	Enabled	Background Scanning	Enabled
TX Power	Full	TX Power	Full
# of Authorized Client Devices	1	# of Authorized Client Devices	0
% Retries/% Drops	1.27 / 0.00	% Retries/% Drops	0.259 / 0.00
% Non-unicast	0.00247	% Non-unicast	0.0322
Packets/Bytes Received	9.1M/1.8G	Packets/Bytes Received	11.4K/21M

Figure 191. The Spectrum Analysis page



## 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.
- Signal (dB): Signal strength.
- Path Score (status): A higher score indicates better performance over the link between this AP and its neighbor. *Note that only ZoneFlex APs of the same radio type can mesh with one another. If the AP is of a different radio type than the one you are currently viewing, this field will display "N/A (Unknown)."*

## 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 Wireless outdoor APs.

### Orientation

This sensor displays the mounting orientation of the AP. Three orientations are possible:

- Desktop/Horizontal Mount
- Ceiling/Horizontal Mount
- Wall/Vertical Mount


Figure 192. AP orientation sensor information

Packets/Bytes Transmitted 7.3M pkts / 2.8G bytes  
Retries 0 pkts

**Access Point Sensor Information**

**Orientation**

Mounting Direction Desktop/Horizontal Mount

Illustration 

**Clients**

MAC Address	User/IP	Access Point	WLAN	VLAN	Channel	R
00:18:de:82:a5:52	twruckus@lee	7962.MAP - Formos	TNet-Radius	None	149	81

### Temperature

This sensor displays the temperature statistics as reported by the AP.

Figure 193. AP temperature sensor information

Access Point	Description	Type	Connected Since	Signal (dB)
00:1d:2e:05:42:c0	2942.MAP - John - L3	Wireless	2010/10/20	15:48:46 54

**Access Point Sensor Information**

**Internal Temperature**

Current 47°C/116.6°F (2010/10/20 16:10:52)

Lifetime Maximum 58°C/136.4°F (2008/11/13 22:26:02)

Lifetime Minimum 0°C/32°F (2008/11/21 20:15:02)

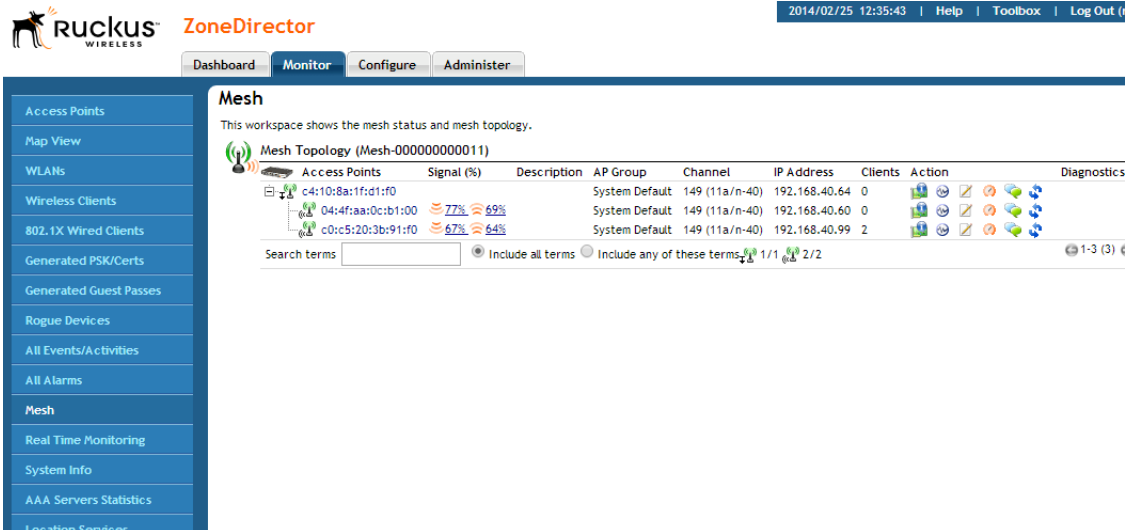
**Clients**

MAC Address	User/IP	Access Point	WLAN	VLAN	Channel	Radio	Signal (dB)	Stat
Search terms: <input type="radio"/> Include all terms <input type="radio"/> Include any of these te								

## Monitoring Mesh Status

The *Monitor > Mesh* page can be used to view Smart Mesh topologies of any mesh trees present on your network. Similar to the Mesh widget on the Dashboard, this page also displays non-meshing APs controlled by ZoneDirector and provides a number of action icons to troubleshoot and diagnose mesh-related problems.

Figure 194. Reviewing Mesh status of APs using the Monitor > Mesh page



## Detecting Rogue Access Points

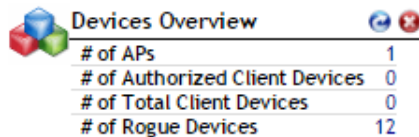
“Rogue” (unauthorized) APs pose problems for a wireless network in terms of airtime contention as well as security. Usually, a rogue AP appears in the following way: an employee obtains another manufacturer's AP and connects it to the LAN, to gain wireless access to other LAN resources. This would potentially allow even more unauthorized users to access your corporate LAN - posing a security risk. Rogue APs also interfere with nearby Ruckus Wireless APs, thus degrading overall wireless network coverage and performance.

ZoneDirector's rogue AP detection options include 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 **Monitor > Rogue Devices**. (You can also click the “#of Rogue Devices” link from the **Devices Overview** widget on the Dashboard.)

Figure 195. Rogue devices indicator



Devices Overview	
# of APs	1
# of Authorized Client Devices	0
# of Total Client Devices	0
# of Rogue Devices	12

- 2 When the **Monitor > Rogue Devices** page appears, three tables are listed:
  - *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 from the *Configure > Alarms* page):
  - *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 (MAC-spoof)*: A malicious rogue AP that has the same BSSID (MAC) as one of the virtual APs managed by ZoneDirector.
  - *malicious AP (Same-Network)*: A malicious rogue AP that is connected to the same wired network.
  - *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 mechanism (enabled from the *Configure > WIPS > Intrusion Detection and Prevention* page) is 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.
- 6 To locate rogue APs that do pose a threat to your internal WLAN, click the Map View  icon for a device to open the Map View.


7 Open the Map View, and look for rogue AP icons . This provides a clue to their location.

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 need to do a bit more research to determine where the AP is located and if it should be marked 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 ZoneFlex APs have detected this rogue, sorted according to signal strength.

Figure 196. Monitoring Rogue Access Points



**Ruckus WIRELESS ZoneDirector - ZoneDirector** 2016/03/30 14:57:20 | Help | Toolbox | Log Out (ruckus)

Dashboard Monitor **Configure** Administer

**Rogue Devices**

This table lists unknown access points that might pose a security threat to your network if connected to the LAN. If a rogue device neither poses a threat nor interferes with neutralizes that AP's effect on ZoneDirector and on Web interface monitoring, if a rogue device is detected by radio, the 5 strongest signal detector AP will be listed as a Strength Indication) number.

**Currently Active Rogue Devices**

MAC Address	Device Name	Location	Channel	Radio	Type	Encryption	SSID	Last Detected
1c:7e:e5:d4:60:f4			1	802.11g/n	AP	Encrypted	emily	2016/03/30 14
fe:f5:28:cb:fd:86		149		802.11a/n	AP	Open	ZyXEL	2016/03/30 14
fc:f5:28:cb:fd:85		6		802.11g/n	AP	Open	ZyXEL	2016/03/30 14
64:09:80:43:ed:0d		2		802.11g/n	AP	Encrypted	Xiaomi_wifi	2016/03/30 14
82:01:84:13:26:3f		7		802.11g/n	AP	Encrypted	HTC Portable Hotspot	2016/03/30 14
70:62:b8:2b:5a:39		6		802.11g/n	AP	Encrypted	kenny0402	2016/03/30 14
84:94:8c:de:bb:48		7		802.11g/n	malicious AP (Same-Network)	Encrypted	Backup WiFi	2016/03/30 14

Search terms   Include all terms  Include any of these terms 7/11

**Known/Recognized Rogue Devices**

MAC Address Channel Radio Type Encryption SSID Last Detected

Search terms   Include all terms  Include any of these terms Remove 0-0 (0)

**User Blocked Rogue Devices**

MAC Address Channel Radio Type Encryption SSID Last Detected

Search terms   Include all terms  Include any of these terms Remove 0-0 (0)

# Monitoring System Ethernet Port Status

To view the status of ZoneDirector's Ethernet ports, go to **Monitor > 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 197. Monitoring system Ethernet port information

**Ruckus WIRELESS** ZoneDirector - ZoneDirector

2016/03/30 14:58:12 | Help | Toolbox | Log Out (ruckus)

Dashboard Monitor Configure Administer

### System Ethernet Info

This table lists system ethernet information.

Port	MAC Address	Interface	Physical Link	Speed	Input pkts	Input bytes	Output pkts	Output bytes
0	6c:aa:b3:00:00:a0	eth0	down	100Mbps	0	0	0	0
1	6c:aa:b3:00:00:a1	eth1	up	1000Mbps	2.4M	392M	201K	76M

## Monitoring AAA Server Statistics

To monitor AAA servers that you have configured on the *Configure > AAA Servers* page, go to **Monitor > AAA Servers Statistics**.



Figure 198. Monitoring AAA servers

The screenshot shows the Ruckus ZoneDirector web interface. The top header displays the Ruckus logo and 'ZoneDirector - ZoneDirector'. Below the header are navigation tabs: Dashboard, Monitor (selected), Configure, and Administer. A date and time stamp '2014/08/06 19:14:27' along with 'Help' and 'Toolbox' links are visible in the top right corner.

The left sidebar contains a navigation menu with the following items: Access Points, Map View, WLANs, Wireless Clients, Wired Clients, Generated PSK/Certs, Generated Guest Passes, Rogue Devices, All Events/Activities, All Alarms, Mesh, Real Time Monitoring, System Info, AAA Servers Statistics (highlighted), and Location Services.

The main content area is titled 'AAA Servers Statistics' and includes a sub-section for 'RADIUS Servers Statistics'. Below this is a table with the following data:

AAA Server Name	Server IP	Access Requests	Access Rejects	Access Retries	Access Timeouts	Accounting Requets	Accounting ACKs	Accounting Retries	Accounting Ti
Ruckus RADIUS	192.168.3.14	0	0	0	0	0	0	0	0
RADIUS Acct	192.168.3.11	0	0	0	0	0	0	0	0

Below the table, there is a search bar with the text 'Search terms', two radio buttons for 'Include all terms' (selected) and 'Include any of these terms', a 'Select Display Span' dropdown menu set to 'from power on', and a 'Reset All' button.

## Monitoring Location Services

To monitor SmartPositioning location servers that you have configured on the *Configure > Access Points > AP Groups* page, go to **Monitor > 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: <https://support.ruckuswireless.com>.

Figure 199. Monitoring Location Services

The screenshot shows the Ruckus ZoneDirector web interface. The left sidebar contains navigation options: Access Points, Map View, WLANs, Clients, Active Wired Clients, Generated PSK/Certs, Generated Guest Passes, Rogue Devices, All Events/Activities, All Alarms, Mesh, Real Time Monitoring, System Info, AAA Servers Statistics, and Location Services. The main content area is titled "Location Services" and includes a sub-header "Location Server Status". Below this is a table with columns: Venue Name, Server FQDN or IP Address, Port, Status, and AP Groups. A red box highlights a row for the venue "hq-test-east". To the right of the table, a red-bordered box contains a detailed view of the AP status for the highlighted venue.

Venue Name	Server FQDN or IP Address	Port	Status	AP Groups
hq-test-east	hq-test-east.venue.ruckuslbs.com	8883	Connected	System Default

AP MAC Address	ZD-AP Status	AP-LS Status
00:11:22:33:44:55	Connected	Connected
00:11:22:33:44:56	Connected	Connected
00:11:22:33:44:57	Connected	Not Connected

You can also view the status of location services venues by dragging the Location Services widget onto the Dashboard.

Figure 200. SPoT dashboard widget

The screenshot shows the "LBS Venue Info" dashboard widget. It features a title bar with a location pin icon and a refresh button. Below the title is a table with columns "Venue Name" and "AP State".

Venue Name	AP State
qa-sdc	■
hq-test-west	■

# Managing User Access

# 7

In this chapter:

- [Enabling Automatic User Activation with Zero-IT](#)
- [Adding New User Accounts to ZoneDirector](#)
- [Managing Current User Accounts](#)
- [Creating New User Roles](#)
- [Managing Automatically Generated User Certificates and Keys](#)
- [Using an External Server for User Authentication](#)
- [Activating Web Authentication](#)

# Enabling Automatic User Activation with Zero-IT

Ruckus Wireless 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 ZoneFlex 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 (**Configure > WLANs**)
- A user *Role* with access to this *WLAN* (**Configure > Roles**)
- A *User* with this role assigned that exists in either the internal database or an external RADIUS, Active Directory or LDAP server (**Configure > Users**)

To enable Zero-IT activation, do the following:

- 1 Go to **Configure > WLANs**.
- 2 Click **Edit** on the *WLAN* where you want to enable Zero-IT Activation.
- 3 Enable **WPA2** (*not WPA-Mixed; selecting WPA-Mixed 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](#) 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 201. Enabling Zero-IT for a WLAN

The screenshot shows the configuration page for a WLAN. The left sidebar contains navigation links: Hotspot Services, Hotspot 2.0 Services, Mesh, AAA Servers, DHCP Relay, Alarm Settings, Services, WIPS, Certificate, Bonjour Gateway, and Location Services. The main configuration area is divided into several sections:

- Type:** Standard Usage (selected), Guest Access, Hotspot Service (WISPr), Hotspot 2.0, Autonomous, Social Media.
- Authentication Options:**
  - Method:** Open (selected), 802.1x EAP, MAC Address, 802.1x EAP + MAC Address.
  - Fast BSS Transition:** Enable 802.11r FT Roaming (Recommended to enable 802.11k Neighbor-list Report for assistant.)
- Encryption Options:**
  - Method:** WPA2 (selected), WPA-Mixed, WEP-64 (40 bit), WEP-128 (104 bit), None.
  - Algorithm:** AES (selected), Auto (TKIP+AES).
  - Passphrase\*:** 12345678
- Options:**
  - Web Authentication:** Enable captive portal/Web authentication (Users will be redirected to a Web portal for authentication before they can access the WLAN.)
  - Authentication Server:** Local Database (selected), Create New.
  - Wireless Client Isolation:**
    - Isolate wireless client traffic from other clients on the same AP.
    - Isolate wireless client traffic from all hosts on the same VLAN/subnet. (Checked)
    - No WhiteList (selected), Create New.
  - Zero-IT Activation™:** Enable Zero-IT Activation (Checked). (WLAN users are provided with wireless configuration installer after they log in.)
  - Dynamic PSK™:** Enable Dynamic PSK with 62 character passphrase (Checked).
    - Secure D-PSK (The key will include nearly all printable ASCII characters.)
    - Mobile Friendly D-PSK (The key will include numbers, lower case and upper case letters.)
  - Expire D-PSK:** Set when the D-PSK should expire: Unlimited (selected).
  - Validity Period:** Effective from first use (selected), Effective from creation time.
  - Limit D-PSK:** Limit D-PSK generation per user to 1 devices (Currently allow 1-4 devices per user.)

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

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

Zero-IT Activation can be used with most modern operating systems including 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.

## 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 web 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 202. 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](#)).

Figure 203. 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 such as iOS, Windows Phone and Android smartphones can also use Zero-IT Activation. This is done using the Onboarding Portal which is described in [Using the BYOD Onboarding Portal](#).

## 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 204. Manual configuration information



## 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 Server for User Authentication](#).

### 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 **Configure > 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.

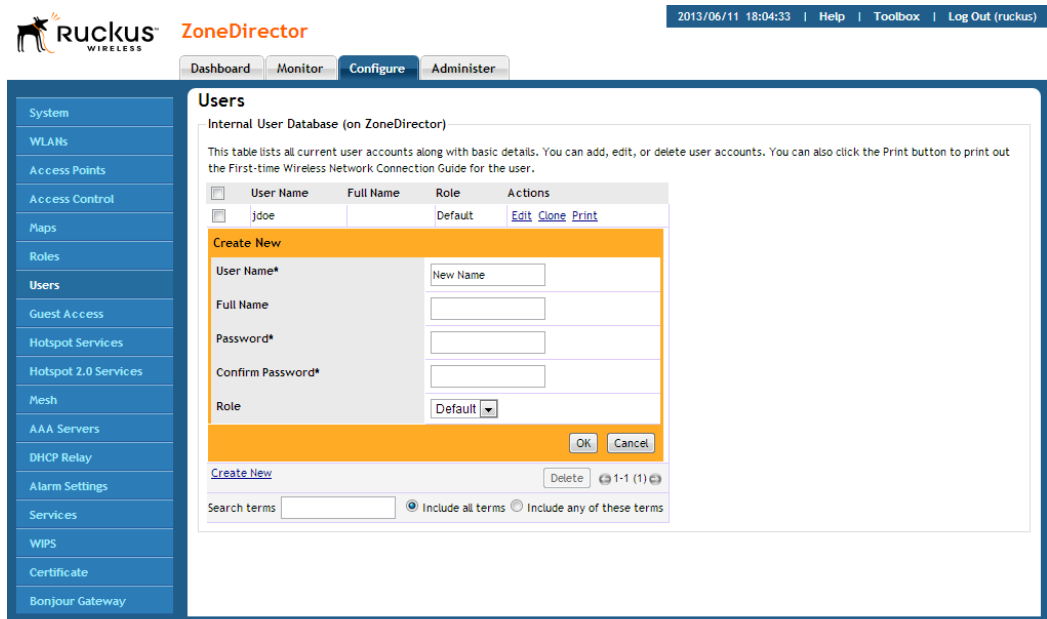
---

**NOTE:** ZoneDirector 1200 can support up to 2,000 DPSK users and guest passes, and up to 2,000 concurrently connected clients. ZoneDirector 3000 can support up to 10,000 total DPSK users and guest passes, and up to 10,000 concurrently connected clients. ZoneDirector 5000 can support up to 20,000 guest passes and 10,000 DPSKs, and up to 20,000 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](#).
- 5 Click **OK** to save your settings. Be sure to communicate the user name and password to the appropriate end user.

Figure 205. 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.

### Changing an Existing User Account

- 1 Go to **Configure > Users**.
- 2 When the *Users* features appear, locate 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](#).)
- 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 **Configure > Users**.
- 2 When the *Users* screen appears, review the “Internal User Database.”
- 3 To delete one or more records, click the check boxes next to 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.

## 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 **Configure > 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](#)).* 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](#).

---

- **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 WLAN](#).
- **Guest Pass:** If you want users with this role to have the permission to generate guest passes, enable this option.

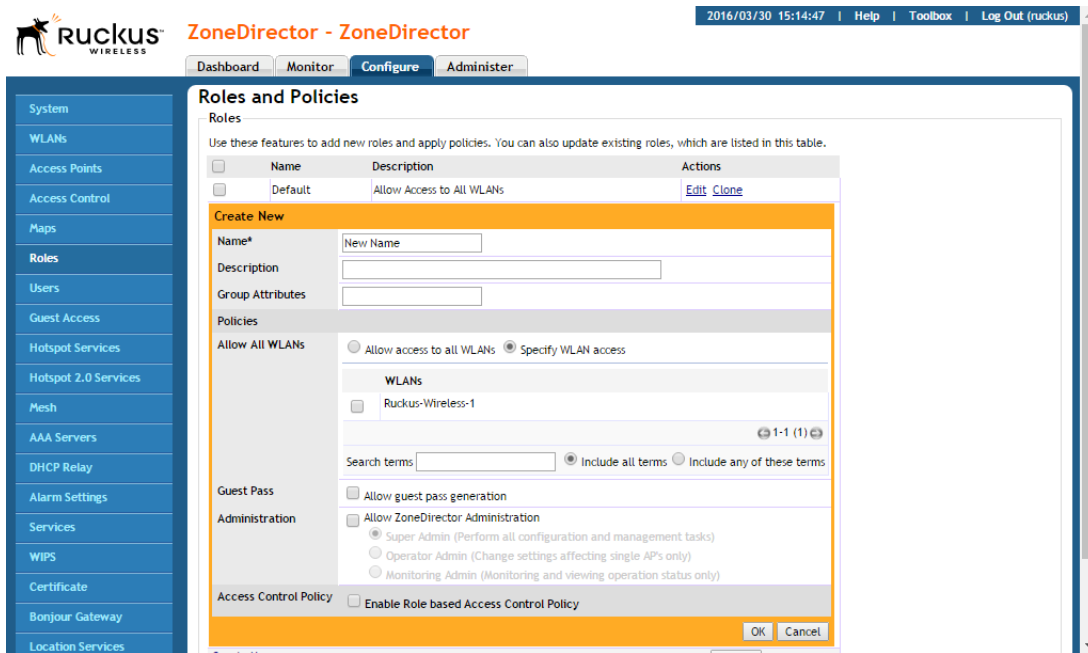
---

**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.
- 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 206. The Create New form for adding a role



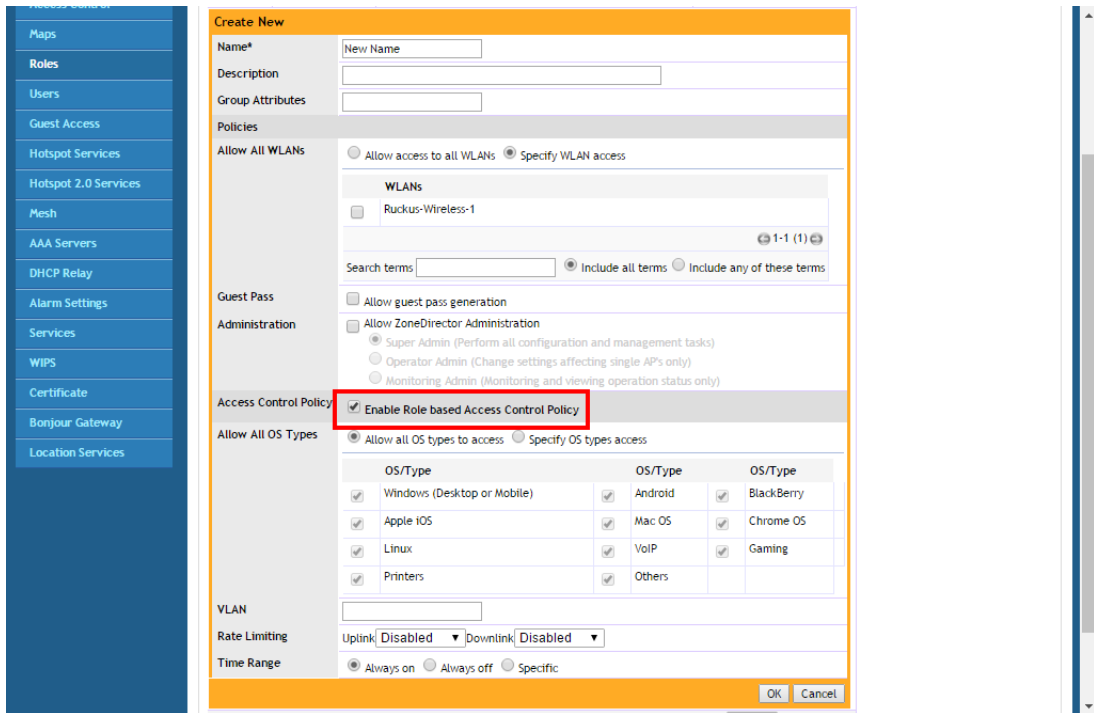
## Role Based Access Control Policy

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 connects to the network they would be given access rights based on their roles 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.

When RBAC is enabled on a WLAN, Client Fingerprinting must be enabled and Dynamic VLAN should also be enabled.

Figure 207. Configuring RBAC policy for a role



## Managing Automatically Generated User Certificates and Keys

With Ruckus Zero-IT wireless activation, a unique key or certificate is automatically generated for a user during the activation process. More precisely, for a WLAN configured with WPA or WPA2 and Dynamic PSK enabled, a unique and random key phrase is generated for each wireless user. Similarly, for a WLAN configured with 802.1X/EAP authentication, a unique certificate for each wireless user is created.

When using the internal user database, automatically generated user certificates and keys are deleted whenever the associated user account is deleted from the user database. In the case of using Windows Active Directory, LDAP or RADIUS as an authentication server, you can delete the generated user keys and certificates by following these steps:

- 1 Go to **Monitor > Generated PSK/Certs**. The Generated PSK/Certs page appears.
- 2 Select the check boxes for the PSKs and Certificates that you want to delete.
- 3 Click **Delete** to delete the selected items.

The selected PSKs and Certificates are deleted from the system.

A user with a deleted PSK or a deleted certificate will not be able to connect to the wireless network without obtaining a new key or a new certificate.

## 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 **Configure > 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.

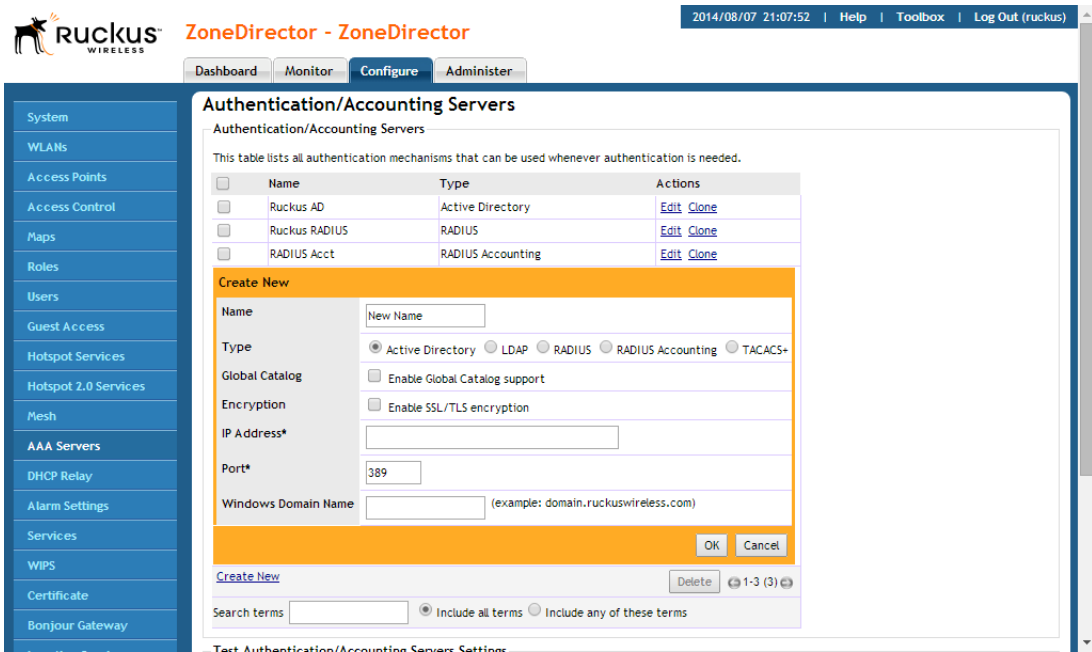
---

**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 208. The Create New form for adding an authentication server



For more information on configuring an external authentication server, see [Using an External AAA Server](#).

## Activating Web Authentication

Web authentication (also known as a “captive portal”) redirects users to a login web page the first time they connect to this 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 **Configure > WLANs**. The WLAN page appears.
- 2 Look for the WLAN that you want to edit, and then click the **Edit** link that is on the same row.
- 3 When the *Editing (WLAN\_Name)* form appears, locate the *Web Authentication* option. See [Figure 209](#).

## Activating Web Authentication

Captive Portal Redirect on Initial Browser HTTPS Request

- 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.

Repeat this “enabling” process for each WLAN to which you want to apply web authentication.

Figure 209. Activating captive portal/web authentication

The screenshot shows the 'Create New' configuration page for a WLAN. The left sidebar contains a navigation menu with items: Maps, Roles, Users, Guest Access, Hotspot Services, Hotspot 2.0 Services, Mesh, AAA Servers, DHCP Relay, Alarm Settings, Services, WIPS, Certificate, Bonjour Gateway, and Location Services. The main content area is titled 'Create New' and contains several sections:

- General Options:** Name/SSID\* (New Name, ESSID/New Name), Description.
- WLAN Usages:** Type (Standard Usage (selected), Guest Access, Hotspot Service (WISPr), Hotspot 2.0, Autonomous, Social Media).
- Authentication Options:** Method (Open (selected), 802.1x EAP, MAC Address, 802.1x EAP + MAC Address), Fast BSS Transition (Enable 802.11r FT Roaming).
- Encryption Options:** Method (WPA2, WPA-Mixed, WEP-64 (40 bit), WEP-128 (104 bit), None).
- Options:** Web Authentication (checked), Authentication Server (Local Database (highlighted), Create New), Wireless Client Isolation (Isolate wireless client traffic from other clients on the same AP, Isolate wireless client traffic from all hosts on the same VLAN/subnet), Zero-IT Activation™ (Enable Zero-IT Activation), Priority (High (selected), Low).
- Advanced Options:** Accounting Server (Disabled, Create New, Send Interim-Update every 10 minutes), Access Control (L2/MAC: No ACLs, Create New; L3/4/IP address: No ACLs, Create New; Device Policy: None, Create New; Precedence Policy: Default, Create New; Enable Role based Access Control Policy).

## 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 may be 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 2 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](#) for more information.

## Activating Web Authentication

Captive Portal Redirect on Initial Browser HTTPS Request

# Managing Guest Access

# 8

In this chapter:

- [Configuring Guest Access](#)
- [Creating a Guest Access Service](#)
- [Creating a Guest WLAN](#)
- [Using the BYOD Onboarding Portal](#)
- [Working with Guest Passes](#)

# 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. The following sections describe how to configure guest WLANs and access policies that control guest use of your network:

- [Creating a Guest Access Service](#)
- [Creating a Guest WLAN](#)
- [Using the BYOD Onboarding Portal](#)
- [Working with Guest Passes](#)

## 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 **Configure > Guest Access**.
- 2 Click **Create New** to configure a guest access service.

---

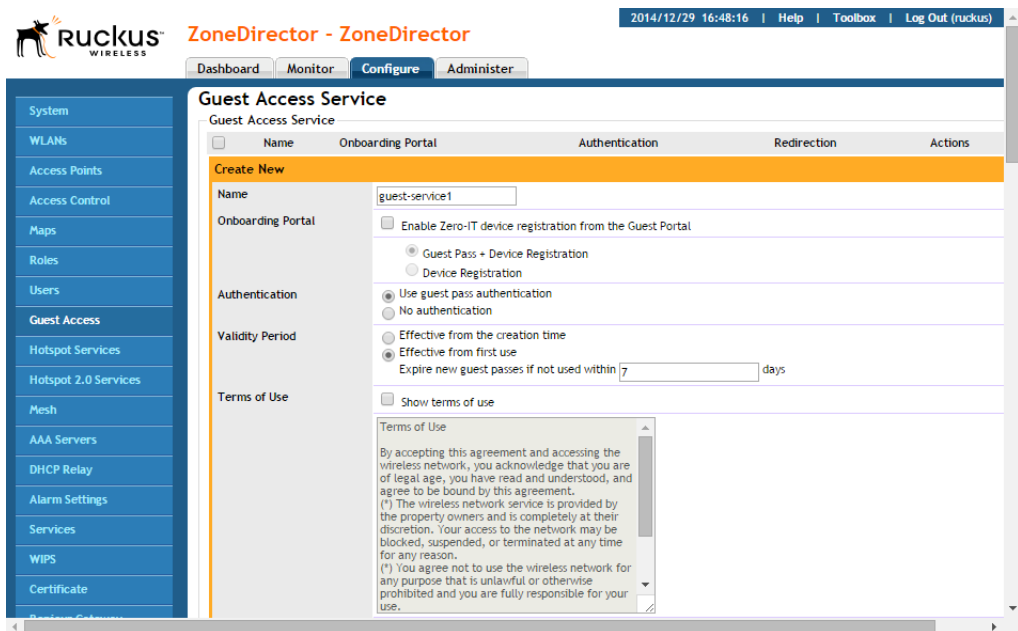
**NOTE:** Alternatively, you can create a Guest Access Service from the WLAN creation page while creating a new WLAN or modifying an existing WLAN (**Configure > WLANs > Edit > Type > Guest Access > Guest Access Service > Create New.**)

---

- 3 In **Onboarding Portal**, choose which options to display in the BYOD Onboarding Portal. See [Using the BYOD Onboarding Portal](#).
- 4 In **Authentication**, choose whether to use guest pass authentication or no authentication:
  - *Use guest pass 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](#).
  - *No authentication:* Do not require redirection and guest pass validation.
- 5 Under *Validity Period*, choose whether the guest pass will be **effective from creation time** or **effective from first use**, and enter an expiration period after which the guest pass will expire if unused.

- 6 Under *Terms of Use*, select 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.
- 7 Under *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) prior to forwarding them to their destination. When guest users land on this page, they are shown the expiration time for their guest pass.
- 8 Customize any of the following optional configuration settings:
  - Web Portal Logo: Upload a logo to replace the Ruckus logo.
  - Guest Access Customization: Enter text to display on the welcome page.
  - Guest Pass Self-Service: Enable this option to allow users to self-activate guest passes. See [Using Guest Pass Self-Service](#).
  - Restricted Subnet Access: See [Configuring Guest Subnet Restrictions](#).
- 9 Click **Apply** to save your settings.

Figure 210. Configuring Guest Access



## 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 *Configure > 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 Authentication**.
- 4 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.
- 5 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.
- 6 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**.
- 7 Select **Enable Guest Pass Self-Service** (enabled by default). 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 one device.)
  - **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](#).)
  - **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.
  - **Terms and Conditions:** Enable this option to display a message to the user before proceeding to registration/authentication.
- 8 Click **OK** to save your changes.
- 9 Go to **Configure > WLANs**, and apply this Guest Access Policy to a Guest Access WLAN, as described in [Creating a Guest WLAN](#).

Figure 211. Creating a Self-Service Guest Access service

The screenshot shows the configuration page for a GuestPass Self-Service. A red box highlights the following settings:

- Enable guestpass self service
- Default guestpass lifetime: 1 Days
- Each guest re-logs in after: (empty) Mins
- Max Device: 1 devices share one single guestpass
- Enable guestpass registration approval
- Allow max sponsor number (Sponsor number is limited 1 to 5): 3
- Sponsor Authentication Server: Local Database
- Notification Method: Email
- Show terms and conditions

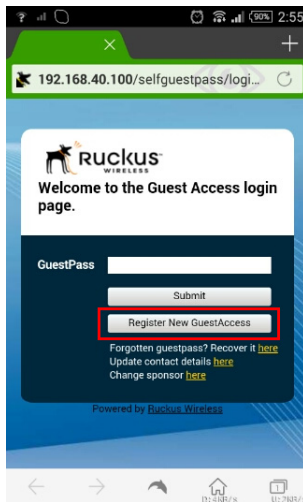
At the bottom of the configuration area, there is a status bar that reads "Restricted Subnet Access" and buttons for "OK" and "Cancel".

## 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:

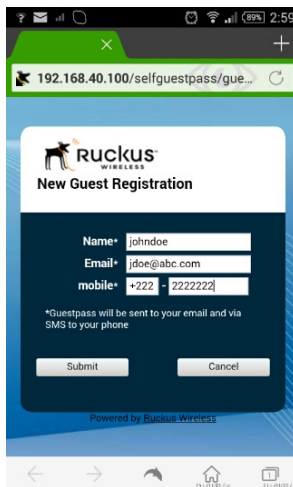
- 1 Connect to the guest WLAN, launch a web browser and attempt to browse to any site.
- 2 The browser redirects to the *Guest Access Login* page.
- 3 Click **Register New Guest Access**.

Figure 212. Guest Access login page



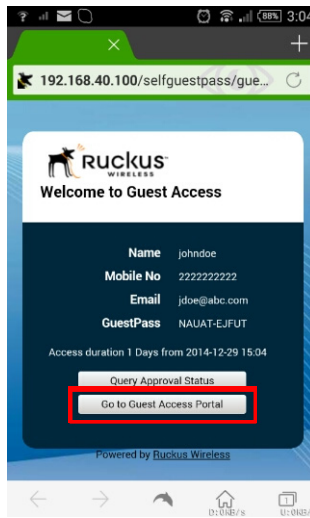
- 4 The *New Guest Registration* page appears.
- 5 Enter a **Name**, **Email** address and **mobile** phone number.
- 6 Click **Submit**.

Figure 213. New Guest Registration page



- 7 The *Welcome to Guest Access* page appears, displaying the information you entered along with your new Guest Pass code.

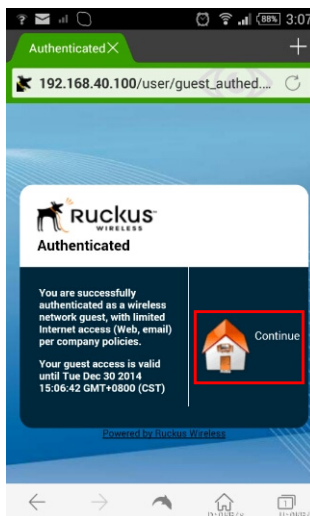
Figure 214. Your Guest Pass code along with your registration information are displayed



8 Click **Go to Guest Access Portal**.

9 The *Authenticated* page appears. Your guest pass is now activated and you can begin using the wireless network. Click **Continue** to be redirected to the URL you originally intended to visit.

Figure 215. Click the Continue icon to begin using the wireless network



## 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 or Clickatell account to deliver guest passes via SMS. See [Setting Up Email Alarm Notifications](#) and [Configuring SMS Settings for Guest Pass Delivery via SMS](#) for more information.

---

Configure the following options if Sponsor Approval is enabled:

- **Sponsor number:** Set how many sponsors the user can specify to approve the guest pass request. Valid values are 1-5.
- **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.

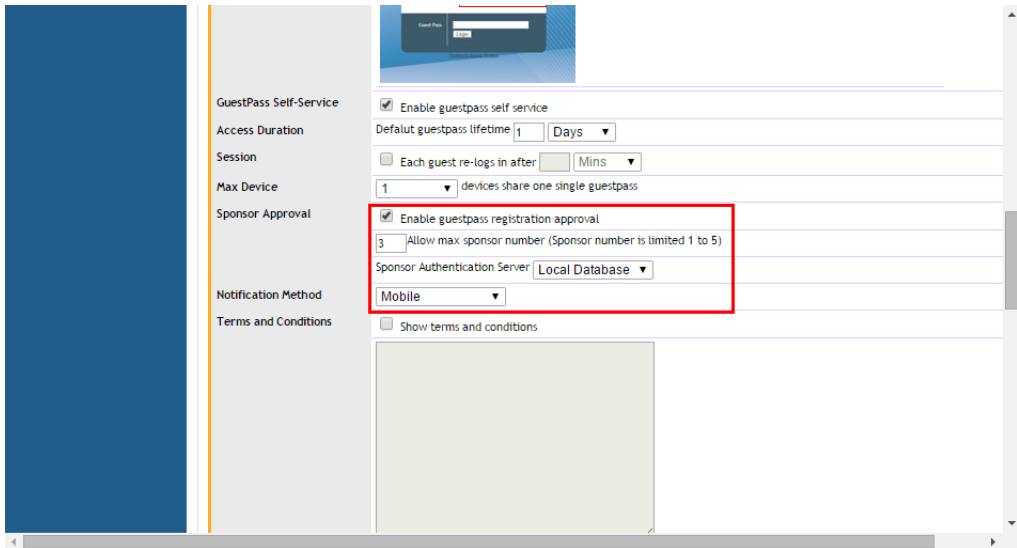
---

**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.

---

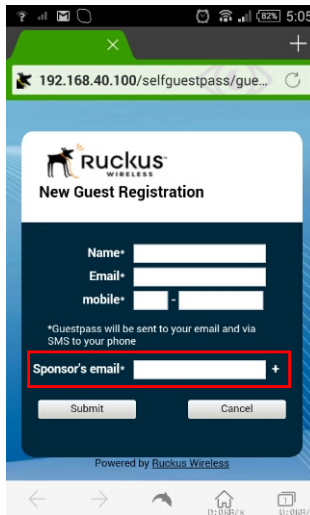
- **Notification Method:** Select whether the guest pass will be delivered via email, mobile (SMS), or both. When Sponsor Approval is selected, delivering the guest pass directly to the client Device Screen is not allowed.

Figure 216. Configuring Sponsor Approval for Self Service Guest Passes



When a user connects to a guest WLAN with Sponsor Approval enabled, the *New Guest Registration* page displays an additional mandatory field, **Sponsor's email**.

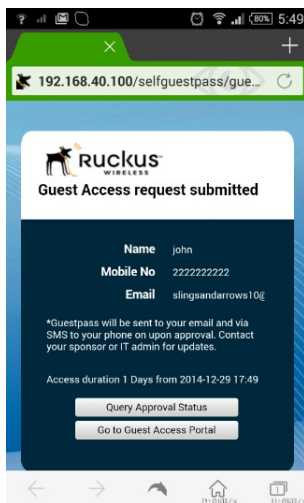
Figure 217. New Guest Registration page - with Sponsor Approval enabled



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

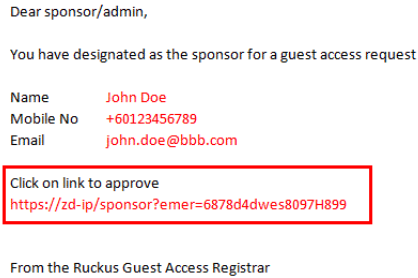
- 1 On the *New Guest Registration* screen, enter your **Name**, **Mobile** number and **Email** address.
- 2 Enter the sponsor's email address and click **Submit**. A guest pass request email is sent to the sponsor's address, and the *Guest Access request submitted* screen is displayed.

Figure 218. Guest Access Request Submitted page



- 3 The sponsor will then receive an email requesting approval for guest pass activation.
- 4 Open the email and click the link to open the *Sponsor/Approver Authentication* page.

Figure 219. Sponsor approval email



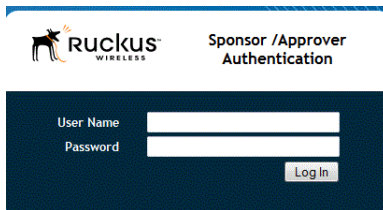
- 5 On the *Sponsor/Approver Authentication* page, enter a valid **User Name** and **Password** and click **Log in** to continue.

---

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

---

Figure 220. Sponsor Login



- 6 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 221. Guest Pass Approval

Guest access registration pending approval :

<input type="checkbox"/>	Name	Mobile	E-mail	Duration	
<input type="checkbox"/>	John	+6012347990	john@bbb.com	4	hour
<input type="checkbox"/>	Jack	+6013547123	john@aaa.com	3	days
<input type="checkbox"/>	Bobe	+6012847789	john@bbb.com	1	month

Approve Reject

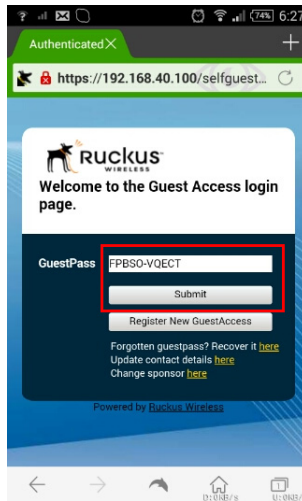
- 7 Approving a guest pass triggers delivery of an email (and/or SMS message) containing the guest pass code to the guest.
- 8 As a guest user, open this email and copy the **Guest Pass** code to the clipboard.

Figure 222. Guest pass activation email

Dear Alice,  
 You request for guest access has been approved  
 Name: Alice  
 Mobile No: +8618066900071  
 Email: [zhaoyuhu@pactera.com](mailto:zhaoyuhu@pactera.com)  
 Guestpass: NSCZH-XSXAD  
 Access is valid till 1 day

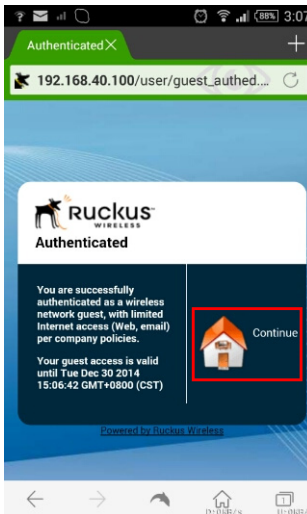
- 9 Launch a web browser and browse to any URL. You will be redirected to the *Welcome* login page.
- 10 Enter the **Guest Pass** code received in the activation email and click **Submit**.

Figure 223. Enter Guest Pass code and click Submit



- 11 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.

Figure 224. Click Continue to begin using the wireless network



## 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.

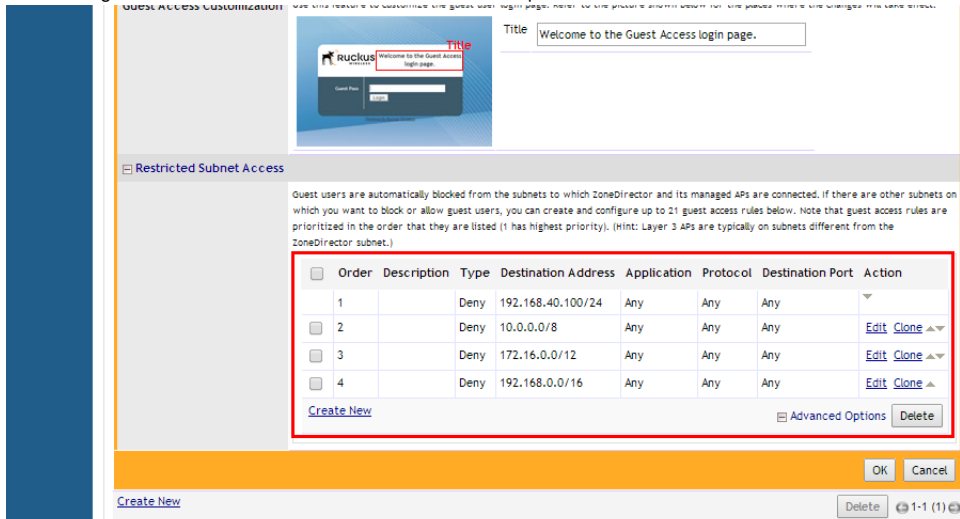
You can create up to 22 subnet access rules, which will be enforced both on the ZoneDirector side (for tunneled/redirect traffic) and the AP side (for local-bridging traffic).

To create a guest access rule for a subnet:

- 1 Go to **Configure > 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 225. The Restricted Subnet Access options



## Creating a Guest WLAN

After 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 the secure internal WLANs.

To create a Guest WLAN:

- 1 Go to **Configure > WLANs**.
- 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 Since this is a Guest network, the only *Authentication Option* available is **Open**.
- 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 Select a **Guest Access Service** from the list of services created on the *Configure > 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](#).

- 8 If you want your internal wireless traffic to have priority over guest traffic, set the *Priority* to **Low**.
- 9 Under *Advanced Options*, select the options to enable for this WLAN. For more information on WLAN advanced options, see [Advanced Options](#).
  - 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.
- 10 Click **OK** to save your changes.

Figure 226. Create a Guest Access WLAN

The screenshot shows the configuration interface for a Guest Access WLAN. On the left is a navigation menu with items like Roles, Users, Guest Access, Hotspot Services, etc. The main content area is titled 'General options' and includes fields for Name/SSID, Description, and WLAN Usages. Under 'WLAN Usages', the 'Guest Access' radio button is selected and highlighted with a red box. Below this, the 'Authentication Options' section shows 'Open' as the selected method. The 'Encryption Options' section shows 'None' as the selected method. In the 'Options' section, the 'Guest Access Service' dropdown is set to 'guest-service-1' and is also highlighted with a red box, with a 'Create New' button next to it. The 'Advanced Options' section includes 'Accounting Server' (Disabled), 'Access Control' (No ACLs, None, Default), and 'Application Visibility' (Enabled).

## Using the BYOD Onboarding Portal

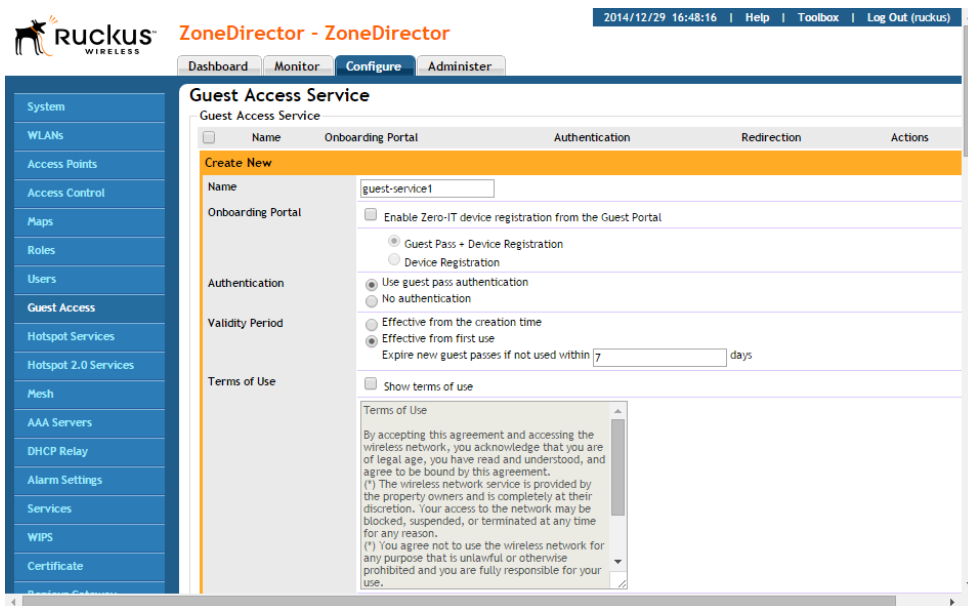
The Onboarding Portal feature provides a series of intuitive option screens allowing mobile users to choose whether to connect to a Guest WLAN or to self-configure their mobile devices to authenticate to an internal WLAN using Zero-IT activation.

To enable the Onboarding Portal for mobile devices:

- 1 Go to **Configure > 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**.

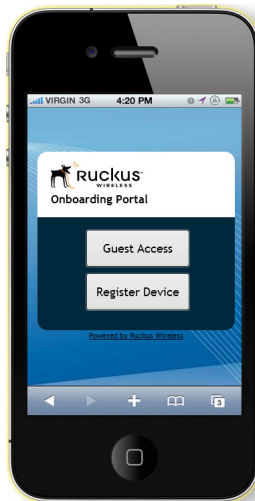
Figure 227. Enable Onboarding Portal



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:

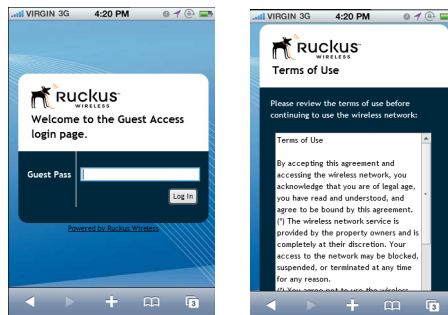
- Guest Access
- Register Device (download Zero-IT activation file)
- Both

Figure 228. The Onboarding Portal for mobile devices



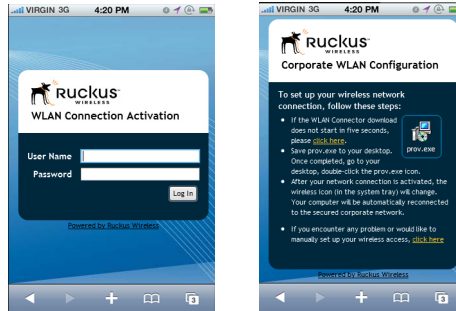
If the user clicks the **Guest Access** button, the process is the same as when connecting to a Guest WLAN and all settings on the Guest Access configuration page will be put into effect.

Figure 229. 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 230. 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:

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

---

**NOTE:** To enable guest pass delivery via email or SMS, you must first configure an email server or an SMS delivery account (Twilio or Clickatell) from the Configure > System page.

---

**NOTE:** ZoneDirector 1200 can support up to 2,000 DPSK users and guest passes, and up to 2,000 concurrently connected clients. ZoneDirector 3000 can support up to 10,000 total DPSK users and guest passes, and up to 10,000 concurrently connected clients. ZoneDirector 5000 can support up to 20,000 guest passes and 10,000 DPSKs, and up to 20,000 concurrently connected clients. When the maximum number of users that ZoneDirector supports has been reached, additional clients attempting to connect will be refused.

---

## Configuring Guest Pass Generation

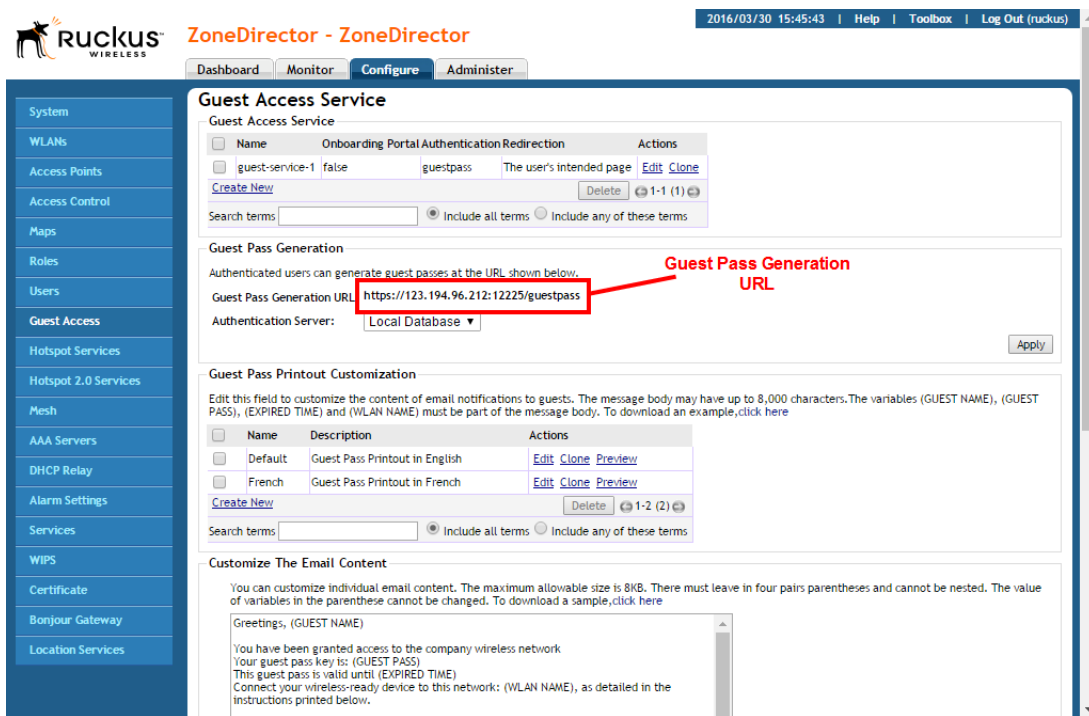
By default, all authenticated users in the internal database with the Default role are allowed to generate guest passes. To authenticate guest pass generators using an external authentication server, do the following:

- 1 Go to **Configure > Guest Access**. The *Guest Access* 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 *Configure > 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 Server for User Authentication](#).)
  - 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 [Figure 231](#), the Guest Pass Generation URL is `https://192.168.40.100/guestpass`.

Figure 231. The Guest Pass Generation section on the Guest Pass page



## 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 **Configure > 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 *Policies* options, clear the **Allow Guest Pass Generation** check box.
- 4 Click **OK** to save your settings. Users with “default” roles no longer have guest pass generation privileges.

## 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 **Configure > Roles**.
- 2 In the *Roles* table, click **Create New**.
- 3 When the *Create New* features appear, make these entries:
  - **Name:** Enter a name for this role (e.g., “Guest Pass Generator”).
  - **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.

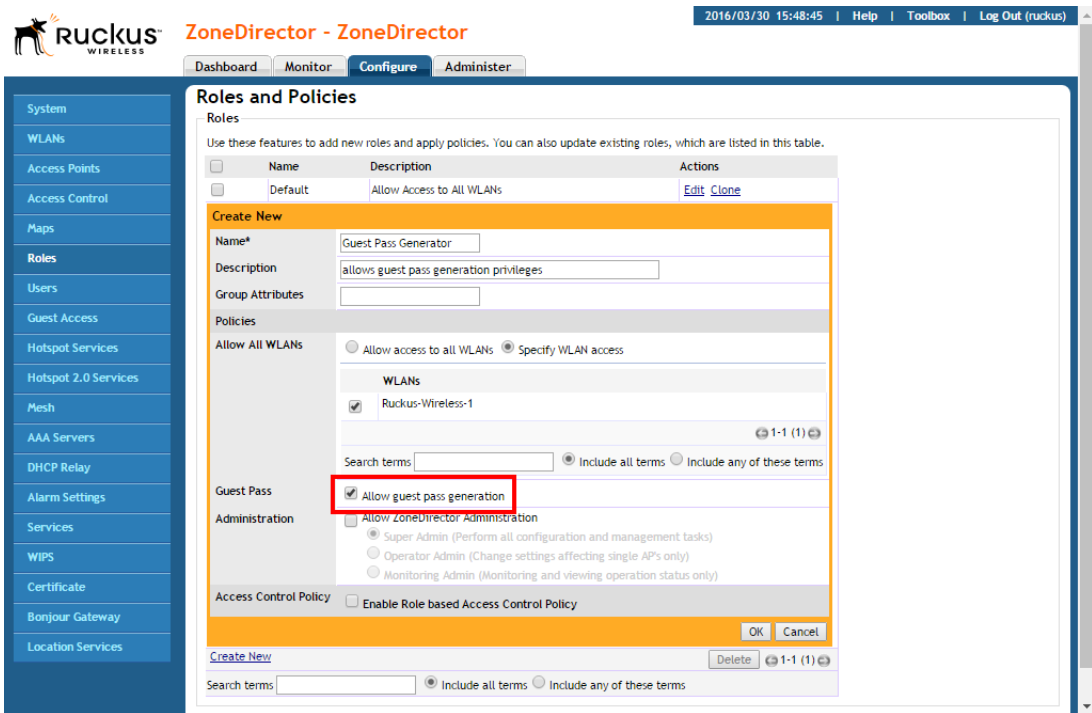
---

**NOTE:** When creating a guest pass generator Role, you must ensure that this Role is given access to the Guest WLAN. 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.

---

- **Guest Pass:** If you want users with this role to have permission to generate guest passes, check this option.
- 4 Click **OK** to save your settings. This new role is ready for application to authorized users.

Figure 232. Create a guest pass generator Role



## Assigning a Pass Generator Role to a User Account

This procedure details the procedure for assigning a guest pass generator role to a user account.

- 1 Go to **Configure > 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 Open the **Role** menu and choose the assigned role for this user.

**NOTE:** You can edit an existing user account and reassign the guest pass generator role, if you prefer.

- 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](#).

---

---

**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-hostname-or-ipaddress}/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 user to enable ZoneDirector to generate the guest pass.

Figure 233. Creating a Guest Pass



The screenshot shows the 'Guest Information' form in the Ruckus Wireless interface. The form is titled 'Guest Information' and features the Ruckus logo. It includes the following fields and options:

- Creation Type:** Radio buttons for 'Single' (selected) and 'Multiple'.
- Full Name \*:** A text input field.
- Valid for \*:** A numeric input field with '1' entered, followed by a 'Days' dropdown menu.
- WLAN \*:** A dropdown menu with 'Ruckus-Guest' selected.
- Email:** A text input field.
- Phone Number:** A text input field with '+1' and '4081234567' entered.
- Key \*:** A text input field with 'WZMES-WOBVQ' entered.
- Remarks (Max length is 64):** A large text area.
- Sharable:** A dropdown menu with '1' selected, followed by the text 'guests share a single guest pass'.
- Session:** A checkbox for 'Each guest re-logs in after' followed by a numeric input field and a 'Mins' dropdown menu.
- Navigation:** A 'Next >' button and a link for 'Show existing guest passes'.

At the bottom of the form, it says 'Powered by Ruckus Wireless'.

- 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](#).
  - **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-RZKKE`, you can 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. Therefore, you cannot create the same guest pass for use on multiple WLANs.

---

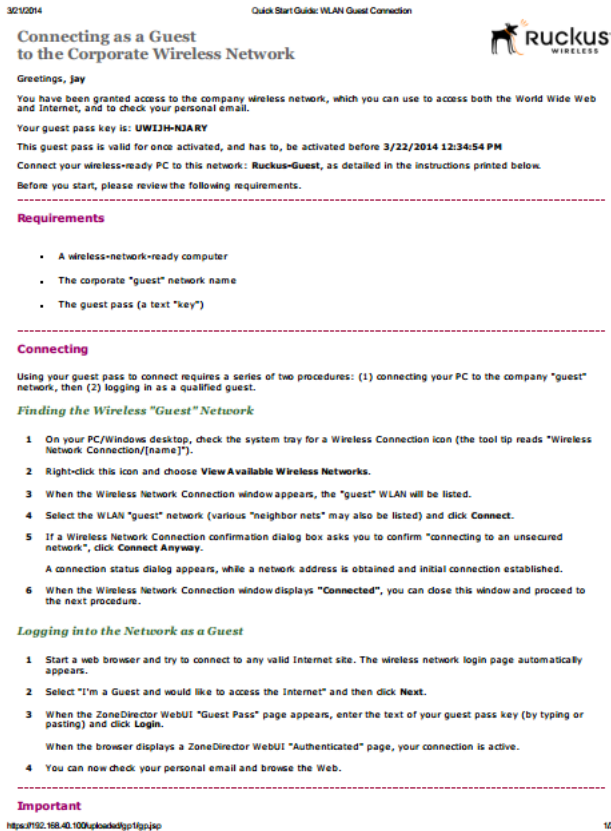
- **Remarks** (optional): Type any notes or comments. For example, if the guest user is a visitor from a partner organization, you can type the name of the organization.
  - **Sharable:** Use this option to allow multiple users to share a single guest pass.
  - **Session:** Enable this check box and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



Figure 235. Sample guest pass printout





## 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](#).

---

**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://{zonedirector-hostname-or-ipaddress}/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:** Click **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.
  - **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.

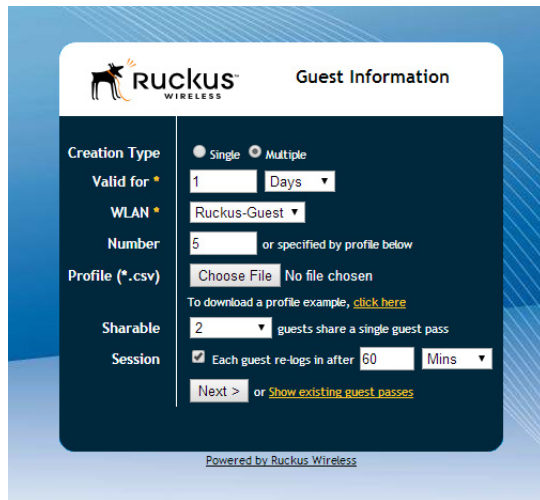
---

**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](#)), 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 236. Generating multiple guest passes at once



The screenshot shows the 'Guest Information' form in the Ruckus Wireless interface. The form is titled 'Guest Information' and features the Ruckus logo. It includes the following fields and options:

- Creation Type:** Radio buttons for 'Single' and 'Multiple' (selected).
- Valid for \*:** A text input field containing '1' and a dropdown menu set to 'Days'.
- WLAN \*:** A dropdown menu set to 'Ruckus-Guest'.
- Number:** A text input field containing '5' and the text 'or specified by profile below'.
- Profile (\*.csv):** A 'Choose File' button and the text 'No file chosen'. Below this is a link: 'To download a profile example, [click here](#)'.
- Sharable:** A dropdown menu set to '2' and the text 'guests share a single guest pass'.
- Session:** A checked checkbox and the text 'Each guest re-logs in after' followed by a text input field containing '60' and a dropdown menu set to 'Mins'.
- Next >** button and a link: 'or [show existing guest passes](#)'.

At the bottom of the form, it says 'Powered by Ruckus Wireless'.

**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”](#) below 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 guest passes, click **Print All Instructions**.

- To print instructions for a single guest pass, click the **Print** link 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

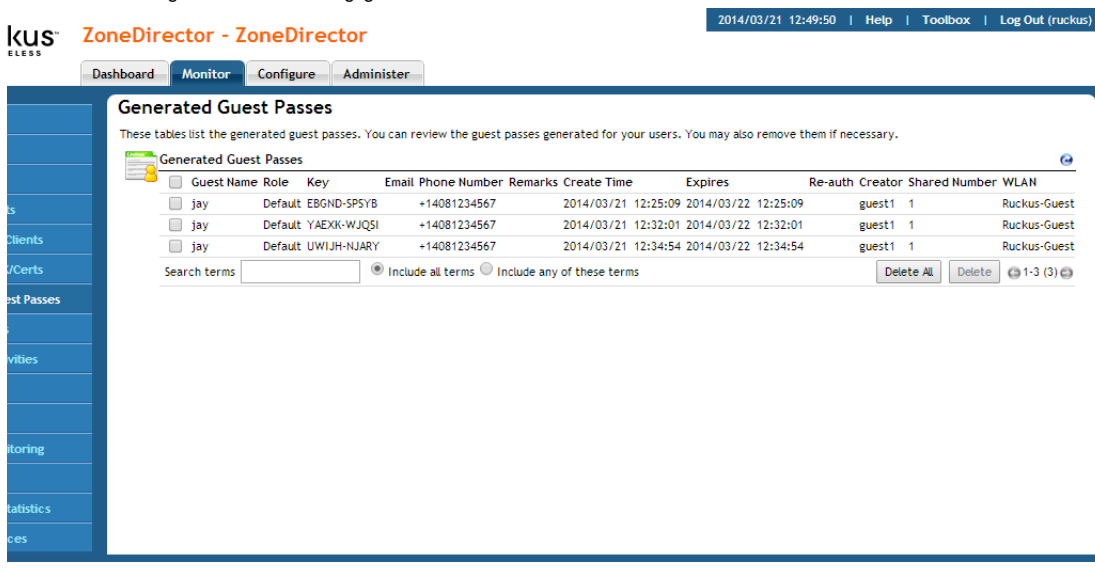
- 1 Log in to the guest pass generation page. Refer to steps 2 to 5 in “[Generating and Printing Multiple Guest Passes at Once](#)” above for instructions.
- 2 In *Creation Type*, click **Multiple**.
- 3 Click the **click here** link in *To download a profile sample*, [click here](#).
- 4 Save the sample 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 Information* page, and then complete steps 6 to 10 in “[Generating and Printing Multiple Guest Passes at Once](#)” above to upload the guest pass profile and generate multiple guest passes.

## Monitoring Generated Guest Passes

Once you have generated a pass for a guest, you can monitor and, if necessary, remove it.

- 1 Go to **Monitor > 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.

Figure 237. Viewing generated Guest Passes



## Customizing the Guest Login Page

You can customize the guest user login page, to display your corporate logo and to note helpful instructions, along with a “Welcome” title.

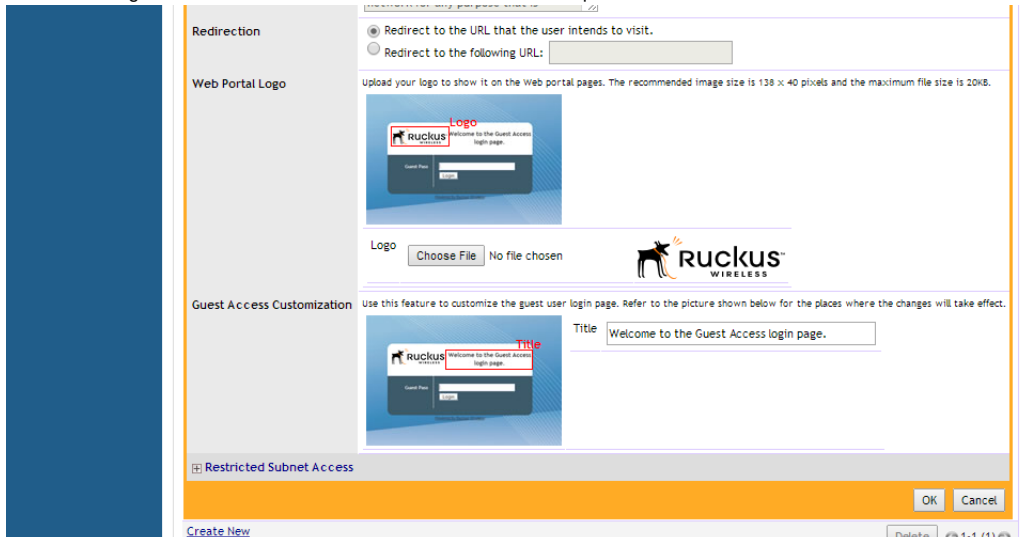
If you want to include a logo, you will need to prepare a web-ready graphic file, in one of three acceptable formats (.JPG, .GIF or .PNG). Make sure that the logo file *does not exceed* the following:

- Length: Two inches on any side
- File size: 20kB

To customize the guest login page

- 1 Go to **Configure > Guest Access**. Edit or create a new Guest Access Policy.
- 2 Scroll down to the *Web Portal Logo* section.
- 3 If your logo is ready for use, click **Browse** to open a dialog box that you can use to import the logo file. (ZoneDirector will notify you if the file is too large.)
- 4 Scroll down to the *Guest Access Customization* section.
- 5 (Optional) Delete the text in the Title field and type a short descriptive title or “welcome” message.
- 6 Click **OK** to save your settings.

Figure 238. The Guest Access Customization options



## 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 **Configure > 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

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](#).

- 5 Go back to the Guest Pass Printout Customization section, and then click **Create New**. The Create New form appears.
- 6 In **Name**, type a name for the guest pass printout that you are creating. For example, if this guest pass printout is in Spanish, you can type *Spanish*.
- 7 In **Description** (optional), add a brief description of the guest pass printout.
- 8 Click **Browse**, select the HTML file that you customized earlier, and then click **Open**. ZoneDirector copies the HTML file to its database.
- 9 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 (see [Figure 234](#)).

## Guest Pass Printout Tokens

[Table 33](#) 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 33. Tokens that you can use in the guest pass printout

Token	Description
{GP_GUEST_NAME}	Guest pass user name.
{GP_GUEST_KEY}	Guest pass key.
{GP_IF_EFFECTIVE_FROM_CREATION_TIME}	If you set the validity period of guest passes to <b>Effective from the creation time</b> (in the Guest Pass Generation section), this token shows when the guest pass was created and when it will expire.

Token	Description
{GP_ELSEIF_EFFECTIVE_FROM_FIRST_USE}	If you set the validity period of guest passes to <b>Effective from first use</b> (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.

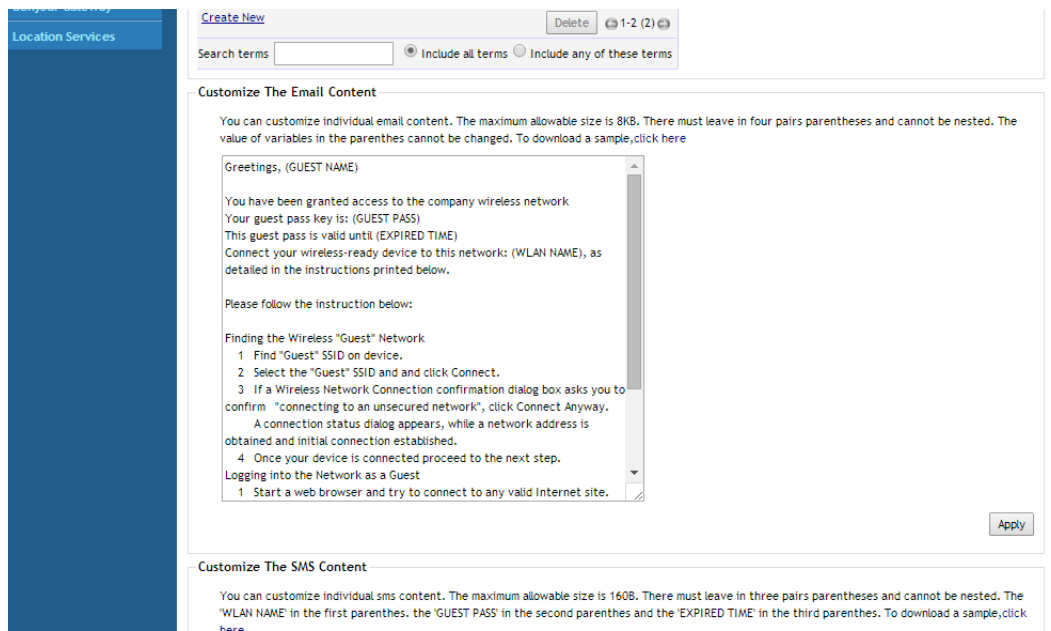
## Delivering Guest Passes via Email

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

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

- 1 On the **Configure > 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 239. Customize the email content



## Delivering Guest Passes via SMS

**NOTE:** SMS delivery requires that the SMS settings on the **Configure > System** page are first configured to allow ZoneDirector to use the configured Twilio or Clickatell account to deliver guest passes.

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

- 1 On the **Configure > 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 240. Customize the SMS content

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.

Apply

**Customize The SMS Content.**

You can customize individual sms content. The maximum allowable size is 1608. There must leave in three pairs parentheses and cannot be nested. The 'WLAN NAME' in the first parentheses, the 'GUEST PASS' in the second parentheses and the 'EXPIRED TIME' in the third parentheses. To download a sample,click [here](#)

SSID: (WLAN NAME)  
Passcode: (GUEST PASS)  
Expires on (EXPIRED TIME)

Apply

---

**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”](#).

---

## Working with Guest Passes

Delivering Guest Passes via SMS

# Deploying a Smart Mesh Network

# 9

In this chapter:

- [Overview of Smart Mesh Networking](#)
- [Smart Mesh Networking Terms](#)
- [Supported Mesh Topologies](#)
- [Deploying a Wireless Mesh via ZoneDirector](#)
- [Understanding Mesh-related AP Statuses](#)
- [Using the ZoneFlex LEDs to Determine the Mesh Status](#)
- [Using Action Icons to Configure and Troubleshoot APs in a Mesh](#)
- [Setting Mesh Uplinks Manually](#)
- [Troubleshooting Isolated Mesh APs](#)
- [Best Practices and Recommendations](#)

## 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 wireless mesh network, the routing nodes (that is, the Ruckus Wireless APs forming the network), or “mesh nodes,” form the network's backbone. Clients (for example, 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. The mesh network enables clients to reach other systems by creating a path that 'hops' between nodes.

Smart Mesh networking offers many advantages:

- Smart Mesh networks are self-healing: If any one of the nodes fails, the nodes note the blockage and re-route data.
- Smart Mesh networks are self-organizing: When a new node appears, it becomes assimilated into the mesh network.

In the Ruckus Wireless 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 Wireless APs communicate with ZoneDirector through a wired LAN connection or through wireless LAN connection with other Ruckus Wireless access points.

---

**NOTE:** For best practices and recommendations on planning and deploying a Ruckus Wireless Smart Mesh network, refer to [Choosing the Right AP Model for Your Mesh Network](#).

---

## Smart Mesh Networking Terms

Before you begin deploying your Smart Mesh network, Ruckus Wireless recommends getting familiar with the following terms that are used in this document to describe wireless mesh networks.

Table 34. Mesh networking terms

Term	Definition
Mesh Node	A Ruckus Wireless ZoneFlex AP with mesh capability enabled.
Root AP (RAP)	A mesh node that communicates with ZoneDirector through its Ethernet (that is, wired) interface.

Term	Definition
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 1106 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 <i>one</i> 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 <i>two</i> hops away from the Root AP. A maximum of 8 hops is supported.

## Supported Mesh Topologies

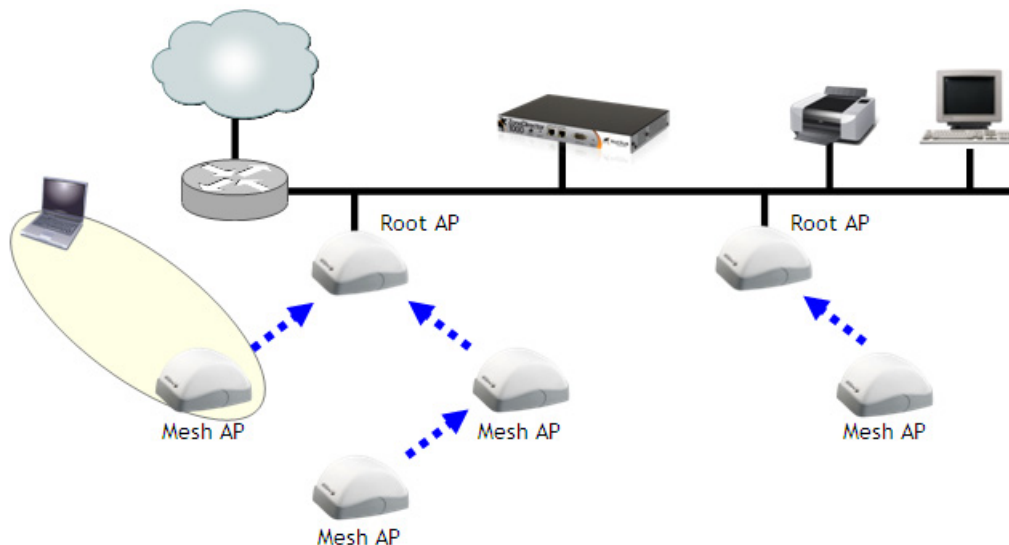
Smart Mesh networks can be deployed in three types of topologies:

- [Standard Topology](#)
- [Wireless Bridge Topology](#)
- [Hybrid Mesh Topology](#)

### 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 (see [Figure 241](#)) 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.”

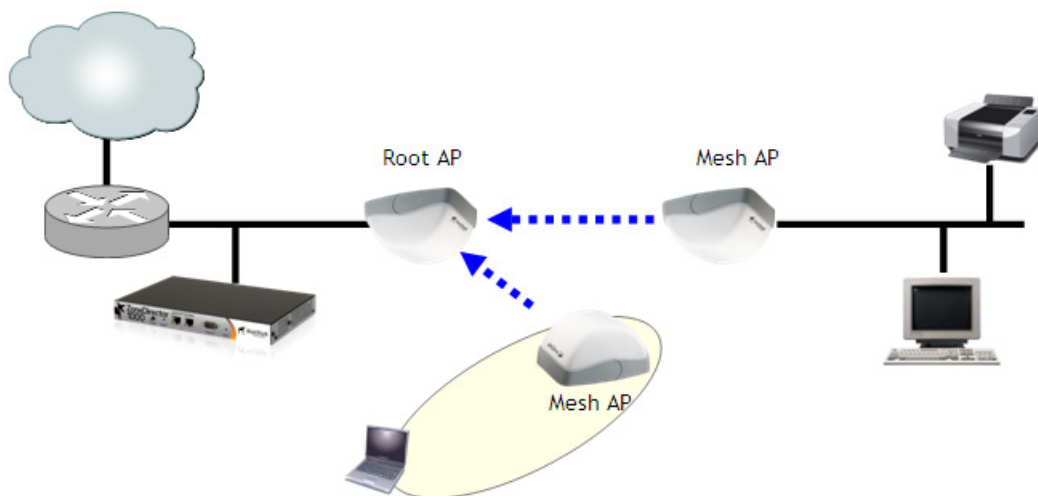
Figure 241. Mesh - standard topology



## 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 [Figure 242](#) below.

Figure 242. Mesh - wireless bridge topology



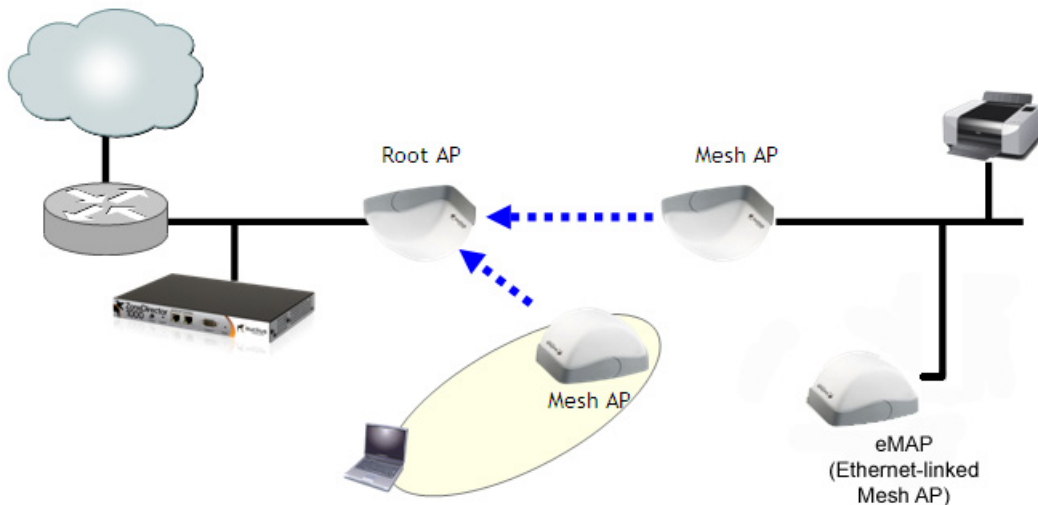
## Hybrid Mesh Topology

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 can be set on a different channel to take advantage of spectrum reuse.

Figure 243. eMAP - Hybrid Mesh topology



Use the **Monitor > Mesh** page to see a tree diagram of your Smart Mesh network.

Icon	Meaning
	Root AP (RAP)
	Mesh AP (MAP)
	eMesh AP (eMAP)

You can also view the role of any AP in your mesh network from the **Monitor > Access Points** page or from the **Mesh Topology** widget on the Dashboard.

## 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

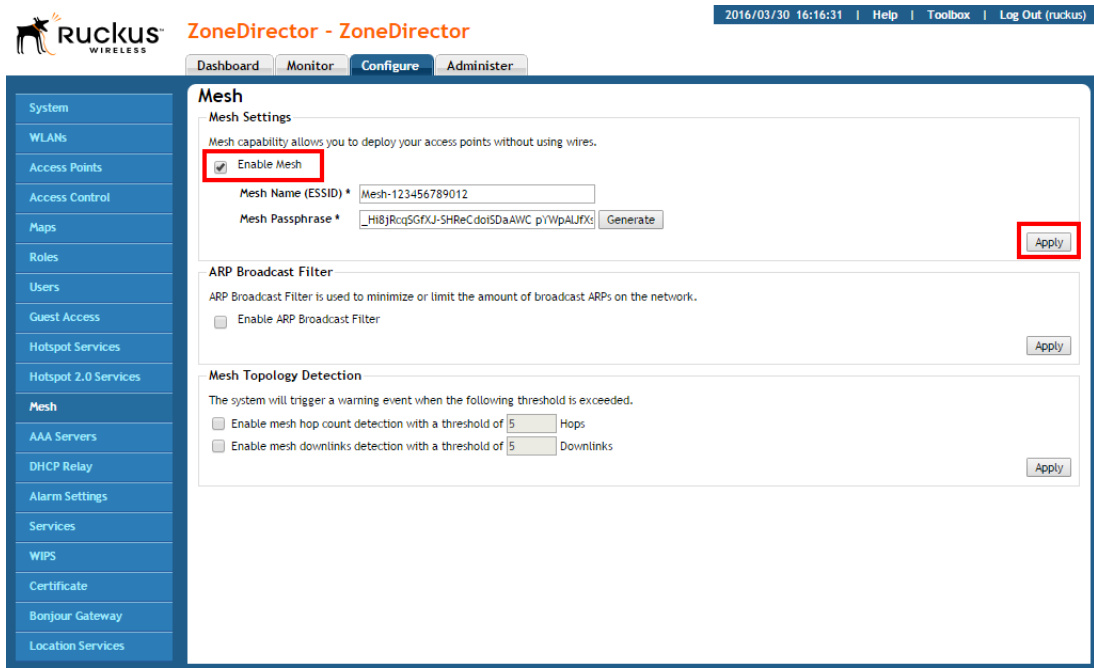
Before starting with your wireless mesh deployment, Ruckus Wireless recommends performing a number of tasks that can help ensure a smooth deployment.

- 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 11n/11ac APs.
- Plan Your Wireless Mesh Network - Survey 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 simple 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.
- Make Sure That Your Access Points Support Mesh Networking - Verify that the access points that you are planning to include in your wireless mesh network all provide mesh capability.
- 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](#).

## 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 Configure > Mesh screen.

Figure 244. Enable Mesh in Configure > Mesh



To enable mesh capability:

- 1 Log into the ZoneDirector web interface.
- 2 Click the **Configure** 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 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.

## 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.

## 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.

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. For detailed procedures on approving join requests, see [Verifying/Approving New APs](#).
- 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 other Root APs or Mesh 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 **Configure > System > 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.

## 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 Map View on the ZoneDirector web interface to verify that mesh associations have been established and mesh trees formed.



- 1 On the ZoneDirector web interface, click the **Monitor** tab, and then click **Map View** on the menu. The Map View appears and shows the mesh nodes that are currently active. (See [Importing a Map View Floorplan Image](#) for instructions on importing a map.)
- 2 Check if all the mesh nodes that you have provisioned and deployed appear on the Map View.
- 3 Verify that a mesh network has been formed by checking if dotted lines appear between the mesh nodes. These dotted lines identify the neighbor relationships that have been established in the current mesh network.

**NOTE:** If your mesh spans multiple ZoneDirectors, it is possible for a node to be associated to a different ZoneDirector than its parent or children.

Figure 245. Dotted lines indicate that these APs are part of the wireless mesh network






The symbols next to the AP icons indicate whether the AP is a Root AP, Mesh AP or eMAP. Refer to the following table:

	An AP with the upward pointing arrow is a Root AP.
	An AP with a number in a circle is a Mesh AP. The number indicates the number of hops from the mesh AP to the Root AP.

## Understanding Mesh-related AP Statuses

Step 4: Verify That the Wireless Mesh Network Is Up

	An AP with a dimmed blue square indicates that it is a Root AP without any active downlinks.
	An AP with a red square is an Ethernet-Linked Mesh AP (eMAP).
	An AP with an X icon is disconnected.

## Understanding Mesh-related AP Statuses

In addition to using the Map View to monitor the status of the mesh network, you can also check the Access Points page on the Monitor tab for mesh-related AP statuses. The table below lists all possible AP statuses that are related to mesh networking, 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.	

Status	Description	Recommended Action
Isolated Mesh AP	AP is disconnected from the ZoneDirector mesh	<ul style="list-style-type: none"> <li>The AP may be configured incorrectly. Verify that the mesh SSID and passphrase configured on the AP are correct.</li> <li>If Uplink Selection is set to Manual, the uplink AP specified for this AP may be off or unavailable.</li> </ul>

## Using the ZoneFlex LEDs to Determine the Mesh Status

In addition to checking the mesh status of ZoneFlex APs from the ZoneDirector web interface, you can also check the LEDs on the APs. The LED behaviors that indicate the AP's mesh status vary depending whether the AP is a single-band or a dual-band model.

### On Single-band ZoneFlex APs

On single-band ZoneFlex APs (for example, ZoneFlex 7352), the two LEDs that indicate the mesh status are:

- WLAN (Wireless Device Association) LED - Indicates downlink status and client association status
- AIR (Signal/Air Quality) LED - Indicates uplink status and the quality of the wireless signal to the uplink AP

### WLAN LED

When Smart Mesh is enabled, the behavior of the WLAN LED indicates downlink status. Refer to the table below for a complete list of possible LED colors and behaviors for Root APs and Mesh APs, and the mesh status that they indicate.

LED Color/Behavior	Root AP / Mesh AP / eMAP
Solid green	No mesh downlink, and; At least one client is associated with the AP

LED Color/Behavior	Root AP / Mesh AP / eMAP
Solid amber (not available on some models)	No mesh downlink, and; No client is associated with the AP
Fast blinking green	At least one mesh downlink exists, and; At least one client is associated with the AP
Slow blinking green	At least one mesh downlink exists, and; No client is associated with the AP

## Signal/Air Quality LED

LED Color/Behavior	Root AP / eMAP	Mesh AP
Solid green	N/A	<ul style="list-style-type: none"> <li>Connected to a Root AP or another Mesh AP</li> <li>Signal quality is good</li> </ul>
Fast blinking green	N/A	<ul style="list-style-type: none"> <li>Connected to a Root AP or another Mesh AP</li> <li>Signal quality is fair or poor</li> </ul>
Slow blinking green	N/A	The AP is searching for an uplink
Off	This is a Root AP or eMAP	N/A

## On Dual-band ZoneFlex APs

**NOTE:** On dual-band ZoneFlex APs, mesh networking is enabled only on the 5 GHz radio.

Refer to the following sections for information on how to check these dual-band APs for their mesh status.

## Outdoor ZoneFlex APs

On outdoor ZoneFlex APs, the **STATUS** LED indicates the AP's mesh status. See the table below for more information.

LED Color/Behavior	Description
Solid green	<ul style="list-style-type: none"> <li>This is a Root AP or eMAP, or;</li> <li>This is a Mesh AP and is connected to a Root AP with good signal</li> </ul>



LED Color/Behavior	Description
Fast blinking green	<ul style="list-style-type: none"><li>• This is a Mesh AP, and;</li><li>• The Root AP signal is fair</li></ul>
Slow blinking green	<ul style="list-style-type: none"><li>• This is a Mesh AP that is currently searching for a Root AP, or;</li><li>• This AP is currently searching for ZoneDirector</li></ul>

## Indoor Dual Band APs

On dual band ZoneFlex indoor APs, the **5G LED** indicates the Root AP's mesh status, and the **5G LED** and the **AIR LED** indicate the mesh status of a Mesh AP. See the table below for more information.






LED	Root AP / eMAP	Mesh AP
5G LED	Solid Green: <ul style="list-style-type: none"> <li>• 5G radio is up</li> <li>• No Mesh APs are connected</li> <li>• At least one client is connected</li> </ul>	Mesh AP 5G LED is consistent with Root AP behavior.
	Amber: <ul style="list-style-type: none"> <li>• 5G radio is up</li> <li>• No Mesh APs/clients connected</li> </ul>	
	Slow Flashing Green (one flash every two seconds): <ul style="list-style-type: none"> <li>• 5G radio is up</li> <li>• At least one MAP is connected</li> <li>• No clients are associated</li> </ul>	
	Fast Flashing Green (two flashes every second) <ul style="list-style-type: none"> <li>• 5G radio is up</li> <li>• At least one MAP is connected</li> <li>• At least one client is connected</li> </ul>	

LED	Root AP / eMAP	Mesh AP
AIR LED	Off	Solid Green: <ul style="list-style-type: none"> <li>• Connected to an uplink AP</li> <li>• Signal quality is good</li> </ul> Fast flashing green (two flashes every second): <ul style="list-style-type: none"> <li>• Connected to a uplink AP</li> <li>• Signal quality is fair</li> </ul> Slow flashing green (one flash every two seconds): <ul style="list-style-type: none"> <li>• Mesh network is enabled</li> <li>• Not connected to a uplink AP, searching for a mesh uplink</li> </ul>

## 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 in the *Currently Managed APs* table on the *Dashboard*. Some of the same action icons are also available on other pages including *Monitor > Access Points* and *Monitor > Mesh*.

Table 35. Action icons

Icon	Icon Name	Action
	System Info	Generate a log file (support.txt) containing system information on this AP.
	Configure	Go to the Configure > 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.

## Setting Mesh Uplinks Manually

On Dual-band ZoneFlex APs

Icon	Icon Name	Action
	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 <i>Configure &gt; Access Points</i> page.
	RF Info	Generates a log file called <i>info.txt</i> , containing radio frequency data that can be used for troubleshooting the RF environment.
	Join Another Controller	Click this button to migrate an AP to another controller. For more information, see <a href="#">Migrating an AP from ZoneDirector to Another Controller</a> .

## 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 that in most situations, Ruckus Wireless recommends against manually changing the roles of APs in a mesh, because it can result in isolated Mesh APs.

Figure 246. Setting Uplink Selection to Manual

The screenshot shows the 'Advanced Options' section of the ZoneDirector web interface. Under 'Mesh Mode', 'Auto (Mesh role is automatically assigned)' is selected. Under 'Uplink Selection', 'Manual (Only selected APs can be used for uplink)' is selected. Below this, two APs are listed with their MAC addresses and signal strengths. A red box highlights the 'Manual' radio button and the two AP entries. Below the AP list is a 'Show All APs' link. The 'Model Specific Control' section shows 'Status LEDs' with 'Override Group Config' and 'Disable Status LEDs' checkboxes, and 'Port Setting' with 'Override Group Config' checked.

**CAUTION!** 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 **Configure** tab.
- 2 On the menu, click **Access Points**.
- 3 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.
- 4 Under *Advanced Options > Uplink Selection*, select the **Manual** radio button. The other APs in the mesh appear below the selection.
- 5 Select the check box for each AP that the current AP can use as uplink.

**NOTE:** 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 Monitor > Access Points page will appear as *Isolated Mesh AP*.

- 6 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 Monitor > 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 five possible reasons for a mesh AP to become isolated. The table below lists all possible Isolated Mesh AP statuses that may appear on the Monitor > 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 Configure > Access Points page on the ZoneDirector web interface, and then click SmartSelection.
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 this.

Status	Possible Reason
Config error	<p>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).</p> <p>To resolve this, follow the instructions in <a href="#">Recovering an Isolated Mesh AP</a>.</p>
No APs with matching radio type	<p>The AP is unable to find an uplink AP with the same radio type. Ruckus Wireless 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 Mesh AP will only connect to another 802.11n AP, and an 802.11b/g Mesh AP will only connect to another 802.11b/g AP.</p> <p>To resolve this, place additional wired APs or Mesh APs that use the same radio type near this AP.</p>

## Recovering an Isolated Mesh AP

When a Mesh AP becomes isolated, it begins broadcasting a recovery SSID (named *“island- <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:

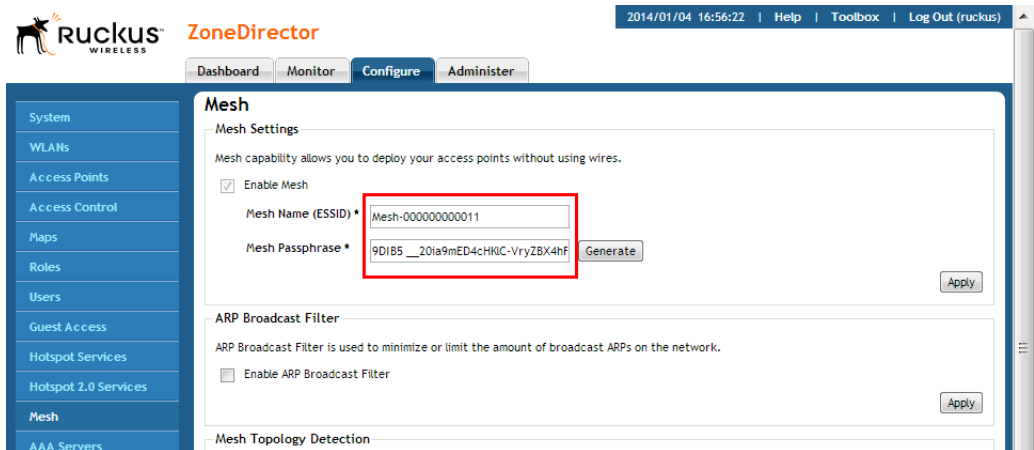
- A notebook computer with wireless capability.
- The current ZoneDirector mesh configuration (steps for obtaining this information are provided below).
- An SSH client, such as PuTTY or OpenSSH.
- A text editor such as Notepad.

### Step 1: Obtain the Mesh SSID and Passphrase

- 1 On the ZoneDirector web interface, click the **Configure** 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 247. 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 **Configure > 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 "island-xxxxxxx" (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.)
- 3 You can now access the AP's web interface by entering the AP's recovery IP address `169.254.1.1` in the browser.

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 `169.254.1.1`.



- 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.

---

**NOTE:** 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 Wireless Smart Mesh network, refer to [Smart Mesh Networking Best Practices](#).

## Best Practices and Recommendations

Recovering an Isolated Mesh AP

# Setting Administrator Preferences

# 10

In this chapter:

- [Changing the ZoneDirector Administrator User Name and Password](#)
- [Changing the Web Interface Display Language](#)
- [Upgrading ZoneDirector and ZoneFlex APs](#)
- [Working with Backup Files](#)
- [Restoring ZoneDirector to Default Factory Settings](#)
- [Working with SSL Certificates](#)
- [Using an External Server for Administrator Authentication](#)
- [Upgrading the License](#)

## 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 the user name and password:

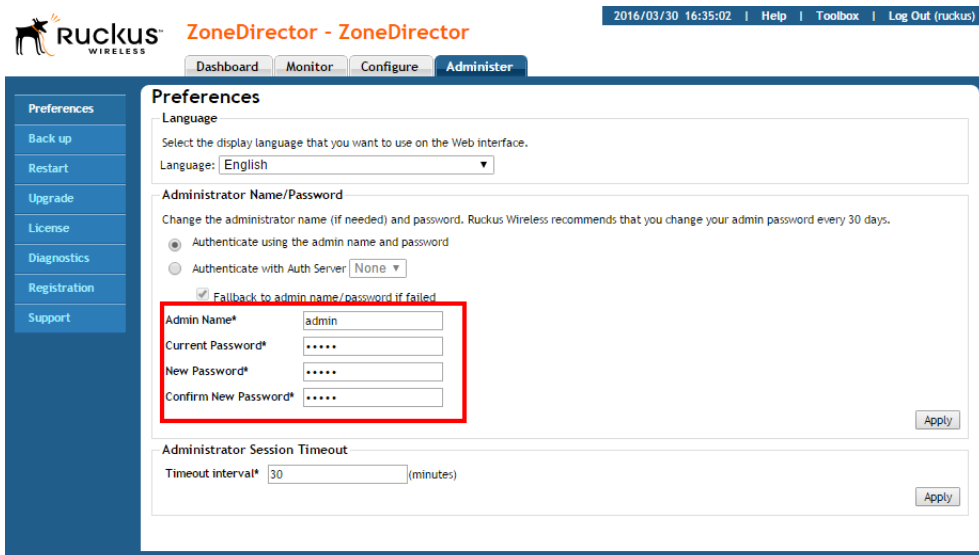
1. Select the **Fallback to admin name/password if failed** check box to enable the user name and password boxes.
2. Change the user name and password.
3. Clear the **Fallback to admin name/password if failed** check box.
4. Click **Apply** to save your changes.

---

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 *Configure > 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).
  - **Password/Confirm Password:** Delete the text in both fields and type the same text for a new password.
- 3 Click **Apply** to save your settings. The changes go into effect immediately.

Figure 248. The Preferences page



## 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**.

## 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 When the *Preferences* page appears, choose your preferred language from the Language drop-down menu.

---

**NOTE:** This only affects how the ZoneDirector web interface appears, and does not modify either the operating system or web browser settings.

---

3 Click **Apply** to save your settings. The changes go into effect immediately.

## Upgrading ZoneDirector and ZoneFlex APs

Check the Ruckus Wireless Support web site on a regular basis for updates that can be applied to your Ruckus Wireless network devices — to ZoneDirector and all your ZoneFlex APs. After downloading any update package to a convenient folder on your administrative PC, you can complete the network upgrade (of both ZoneDirector and APs) by following the steps detailed below.

---

**NOTE:** Upgrading ZoneDirector and the APs will temporarily disconnect them (and any associated clients) from the network. To minimize network disruption, Ruckus Wireless recommends performing the upgrade procedure at an off-peak time.

---

---

**NOTE:** If ZoneDirector is running a software version earlier than version 9.12 and you want to upgrade to version 9.13, you will need to upgrade to version 9.12 first, and then upgrade to version 9.13. If you try to upgrade directly to 9.13 from a version earlier than 9.12, the upgrade will fail (see *ZoneDirector Release 9.13 Release Notes* for more information).

---

- 1 Go to **Administer > Upgrade**.
- 2 Under the *Software Upgrade* section, click **Browse**. The Browse dialog box appears.
- 3 Browse to the location where you saved the upgrade package, and then click **Open**.
- 4 When the upgrade file name appears in the text field, the **Browse** button becomes the **Upgrade** button.
- 5 Click **Upgrade**.

ZoneDirector will automatically log you out of the web interface, run the upgrade, and then restart itself. When the upgrade process is complete, the Status LED on ZoneDirector is steadily lit. You may now log back into the web interface as Administrator.

---

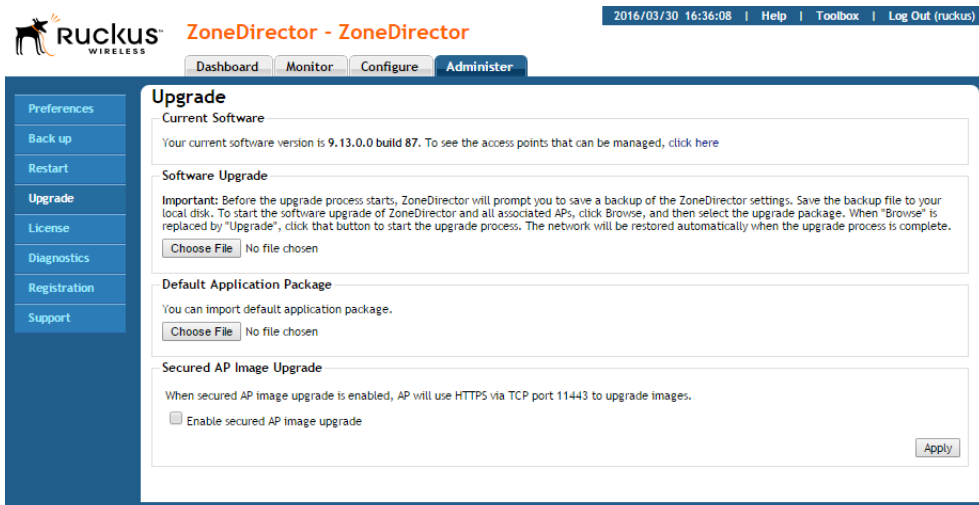
**NOTE:** The full network upgrade is successive in sequence. After ZoneDirector is upgraded, it will contact each active AP, upgrade it, and then restore it to service.

---

**NOTE:** The AP uses FTP to download firmware updates from ZoneDirector. If you have an access control list (ACL) or firewall between ZoneDirector and the AP, make sure that FTP traffic is allowed to ensure that the AP can successfully download the firmware update.

---

Figure 249. The Upgrade page



## Importing a Default Application Package

If an updated application signature package is available for Application Visibility, you can import the new signature package by clicking **Choose File** and selecting the new package.

## Enabling Secure 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 unsupported, AP image upgrades will fall back to FTP.

## Performing an Upgrade with Smart Redundancy

If you have two ZoneDirectors in a Smart Redundancy configuration, the procedure is similar. Note however, that the active and standby ZoneDirectors will reverse roles during an upgrade.

To upgrade both ZoneDirectors in a Smart Redundancy configuration:

- 1 Log in to the *active* ZoneDirector or the shared Management Interface.

---

**NOTE:** Do not attempt to manually upgrade the standby ZoneDirector first, followed by the active unit. If you do this, some configuration options may get lost during the upgrade process. Be sure to begin the upgrade process from either the active ZoneDirector's web interface or the shared Management interface.

---

- 2 Go to **Administer > Upgrade**.
- 3 Under the *Software Upgrade* section, click **Browse**. The Browse dialog box appears.
- 4 Browse to the location where you saved the upgrade package, and then click **Open**.
- 5 When the upgrade file name appears in the text field, the **Browse** button becomes the **Upgrade** button.
- 6 Click **Upgrade**. The backup ZoneDirector is upgraded first.
- 7 When the backup ZoneDirector upgrade is complete, the backup ZoneDirector reboots and becomes active (begins accepting AP requests), while the original active ZoneDirector enters backup state and begins its own upgrade process.
- 8 All APs are now associated to the original backup ZoneDirector (which is now the active ZoneDirector), and begin upgrading AP firmware to the new version.
- 9 Each AP reboots after upgrading.

## Working with Backup Files

After you have set up and configured your Ruckus wireless network, you may want to back up the full configuration. The resulting archive can be used to restore your ZoneDirector and network. And, whenever you make additions or changes to the setup, you can create new backup files at that time, too.



## Backing Up a Network Configuration

- 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**.

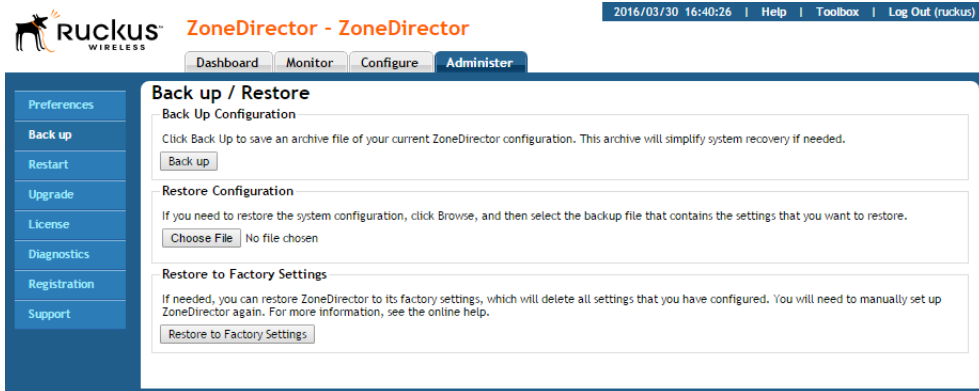
---

**NOTE:** Ruckus Wireless 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 250. The Back Up Configuration option



## Restoring Archived Settings to ZoneDirector

---

**NOTE:** 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.

---

- 1 Go to **Administer > Backup**.
- 2 Under *Restore Configuration*, click **Browse**.

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.

---

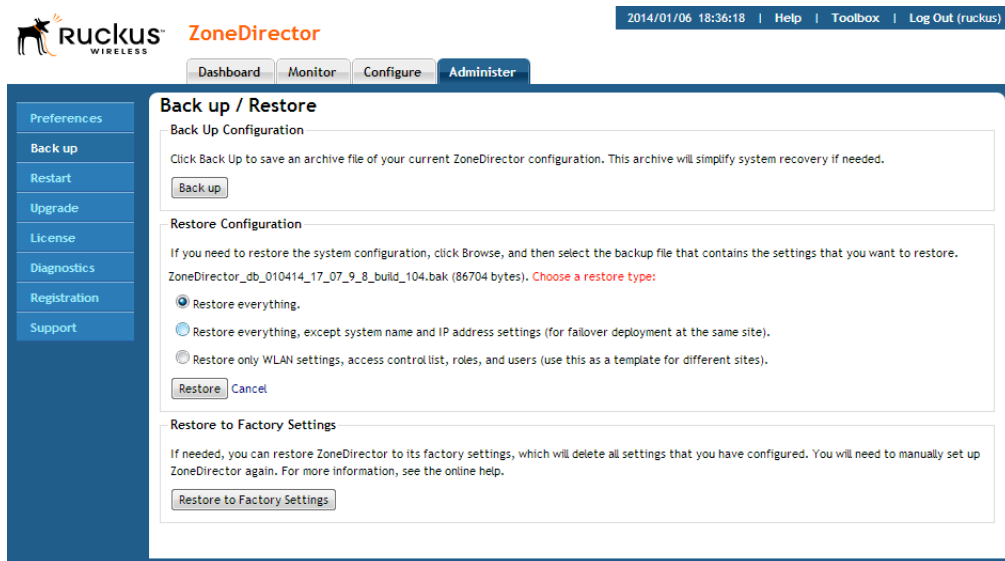
**NOTE:** In addition to system name and IP address, this option restores everything except for the following configuration settings: 1.) VLAN settings. 2.) Management IP address and VLAN settings. 3.) Smart Redundancy settings. 4.) DHCP server settings. 5.) Session timeout. 6.) Limited ZD Discovery 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 251. 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 1200 controllers are deployed in different locations and with one ZoneDirector 3000 serving as a backup, you can use this feature to export AP lists from the three ZD1200s and import them one by one into the ZD3000. For more information on N+1 redundancy deployment, see [Using Limited ZD Discovery for N+1 Redundancy](#).

To restore an AP list from a backup file without altering ZoneDirector settings:

- 1 Go to **Configure > Access Points**.
- 2 Under the *Access Points* table, click the **Browse** button near the line that begins “*If you need to import the APs configuration...*”.
- 3 Browse to a previously saved backup file, select the file and 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.

## Working with Backup Files

### Restoring Archived Settings to ZoneDirector

- 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 252. Importing AP lists only from a backup file

The screenshot shows the Ruckus ZoneDirector web interface. The top navigation bar includes the Ruckus logo, the title 'ZoneDirector - ZoneDirector', and the date/time '2014/08/07 21:26:56'. Below the navigation bar are tabs for 'Dashboard', 'Monitor', 'Configure', and 'Administer'. The left sidebar contains a menu with items like 'System', 'WLANS', 'Access Points', 'Access Control', 'Maps', 'Roles', 'Users', 'Guest Access', 'Hotspot Services', 'Hotspot 2.0 Services', 'Mesh', 'AAA Servers', 'DHCP Relay', 'Alarm Settings', 'Services', 'WIPS', 'Certificate', and 'Bonjour Gateway'. The main content area is titled 'Access Points' and contains a table of access points. Below the table is a search bar and a message box highlighted in red: 'If you need to import the APs configuration, click Browse, and then select the backup file that contains the settings that you want to import.' Below the message box is a 'Choose File' button and the text 'No file chosen'. Below this is a section for 'Access Point Groups' with a table of groups and a 'Create New' button. At the bottom is a section for 'Access Point Policies' with a checkbox for 'Approval'.

MAC Address	Device Name	Description	Channel	TX Power	WLAN Group	Approved Actions
<input type="checkbox"/> c0:c5:20:3b:91:f0	RuckusAP		*(11a/n-*)	*(11b/g/n-*)	*(11a/n), *(11b/g/n)	*(11a/n), *(11b/g/n) Yes <a href="#">Edit</a>
<input type="checkbox"/> c4:10:8a:1f:d1:f0	RuckusAP		*(11a/n-*)	*(11b/g/n-*)	*(11a/n), *(11b/g/n)	*(11a/n), *(11b/g/n) Yes <a href="#">Edit</a>

\* = Use Group Configuration [Delete](#) ↻ 1-2 (2) ↻

Search terms   Include all terms  Include any of these terms

If you need to import the APs configuration, click Browse, and then select the backup file that contains the settings that you want to import.

[Choose File](#) No file chosen

**Access Point Groups**

This table lists your current AP groups and provides basic details about them. Click Create New to add another AP group, or click Edit to make changes to an existing AP group.

<input type="checkbox"/>	Name	Description	# of Members	Actions
<input type="checkbox"/>	System Default	System default group for Access Points	2	<a href="#">Edit</a> <a href="#">Clone</a>

[Create New](#) [Delete](#) ↻ 1-1 (1) ↻

Search terms   Include all terms  Include any of these terms

**Access Point Policies**

Approval  Automatically approve all join requests from APs. (To enhance wireless security, deactivate this option. This means you must manually "allow" each newly discovered AP.)

## 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.

**CAUTION!** 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.

---

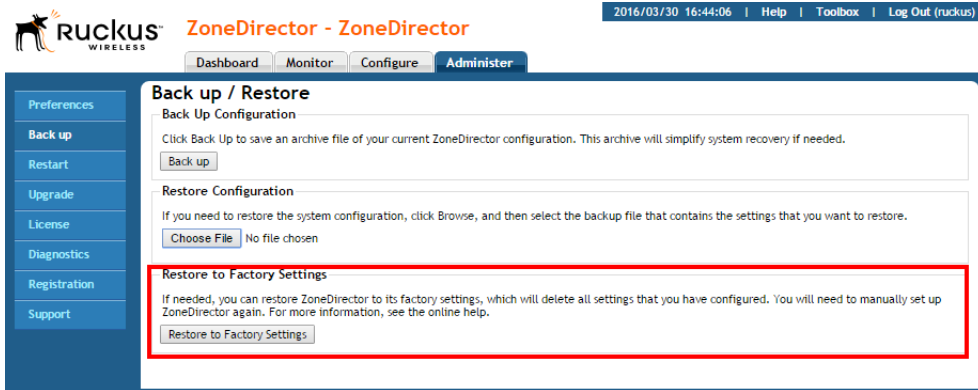
**NOTE:** A complete set of instructions is available in the *ZoneDirector Quick Start Guide* (QSG). Before restoring ZoneDirector to factory default settings, you should open and print out the QSG pages. You can follow those instructions to set up ZoneDirector after restoring factory defaults.

---

To reset your ZoneDirector to factory default settings:

- 1 Go to **Administer > Backup**.
- 2 When the *Backup/Restore* page appears, look for **Restore Factory Settings**, and click the button.
- 3 Owing to the drastic effect of this operation, one or more confirmation dialog boxes will appear. Click **OK** to confirm this operation.
- 4 When this process begins, you will be logged out of the web interface.
- 5 When the reset is complete, the Status LED is 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 253. 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.

## 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 web 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:

- Generate a Certificate Signing Request (CSR) with the required requester information.
- Submit the CSR to a public CA for signing.
- Receive a signed certificate from the CA.
- 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 *Configure > 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 **Configure > 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 "ZoneDirector").

---

**NOTE:** Ruckus Wireless 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 (for example, Ruckus Wireless, Inc.). 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 254. Generating a CSR file

The screenshot shows the Ruckus ZoneDirector web interface. The top navigation bar includes the Ruckus logo, the title 'ZoneDirector - ZoneDirector', and a status bar with the date '2016/03/30 16:46:15', 'Help', 'Toolbox', and 'Log Out (ruckus)'. Below the navigation bar are tabs for 'Dashboard', 'Monitor', 'Configure', and 'Administer'. The left sidebar contains a menu with items like System, WLANs, Access Points, Access Control, Maps, Roles, Users, Guest Access, Hotspot Services, Hotspot 2.0 Services, Mesh, AAA Servers, DHCP Relay, Alarm Settings, Services, WIPS, and Certificate. The main content area is titled 'SSL Certificate' and has a sub-header 'Generate a request'. Below this is a text box with the instruction 'Create a new certificate request. For more information, click here.' followed by several input fields: 'Common Name\*' (zd.example.com), 'Subject Alternative Name' (IP), 'Organization\*' (Ruckus Wireless), 'Organization Unit' (Engineering), 'Locality/ City\*' (Sunnyvale), 'State/ Province\*' (CA), and 'Country\*' (United States). An 'Apply' button is located to the right of the 'Country\*' field. Below the 'Generate a request' section is the 'Import Signed Certificate' section, which includes a text box with instructions and a 'Choose File' button. The 'Advanced Options' section is partially visible at the bottom.

- 5 Go to a certificate authority's web site and follow the instructions for purchasing an SSL certificate.
- 6 When you are prompted for the certificate signing request, copy and paste the content of the text file that you saved to your local computer, and then complete the certificate purchase.

After the certificate authority approves your CSR, you will receive the SSL certificate via email. The following is an example of a signed certificate that you will receive from a certificate authority:

```
-----BEGIN CERTIFICATE-----
MIIFVjCCBD6gAwIBAgIQLfagUqKukMumWhbVf5v4vDANBgkqhkiG9w0B
AQUFADCBsDELMAkGA1UEBhMCVVMxZjZAVBgNVBAoTDlZlcmlTaWduLCBJ
bmMuMR8wHQYDVQQLBgEgEFBQcBAQRtMGswJAYIKwYBBQUHMAGGGGh0dHA6
Ly9vY3NwLnZlcmlzaWduLmNvbTBDBGgrBgEgEFBQcWAwY3aHR0cDovL1NW
U1NlY3VyZS1haWEudmVyaXNpZ24uY29tL1NWU1NlY3VyZTIwMDUuYWlh
LmNlclJBUjBGRGRBgEgEFBQcBDARiMGChXqBcMFowWDBWFglpbWFfnZS9naWYw
ITAFMacGBSsOAwIaBBRLa7kolgYMu9BSOJsprEsHiyEFGDAmFiRodHRw
Oi8vbG9nby52ZXJpc2lnbi5jb20vdnNsb2dvMS5naWYwdQYJKoZIhvcN
AQEFBQADggEBAl/S2dmm/kgPeVALsIHmx-
751o4oq8+fwehRDBmQDaKiBvVXGZ5ZMnoc3DMYDjx0SrI9lkPsn223CV
3UVBZo385g1T4iKwXgcQ7WF6QcUYOE6HK+4ZGcHermFf3fv3C1-
FoCjq+zEu8ZboUf3fWbGprGRA+MR/dDI1dTPtSUG7/zWjXO5jC//
0pykSldW/q8hgO8kq30S8JzCwkqrXJfQ050N4TJtgb/
YC4gwh3BuB9wqpRjUahTiK1V1-
ju9bHB+bFkMWIIMIXc1Js62JClWzWfGaGUS2DLE8xICQ3wU1ez8RUPGn
wSxAYtz2N7zDxYDP2tEiO5j2cXY7O8mR3ni0C30=
-----END CERTIFICATE-----
```

- 7 Copy the content of the signed certificate, and then paste it into a text file. Save the file.

You may now import the signed certificate into ZoneDirector. Refer to the following section for instructions.

## 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:

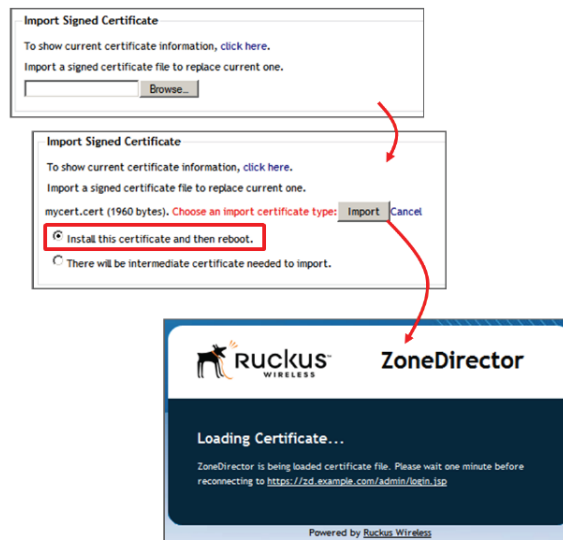
- 1 Click on the Browse button and select the file that contains the certificate (in PEM format) to upload it.
- 2 If there are no intermediate CA certificates, then click on the Import button to install the uploaded certificate.

---

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

---

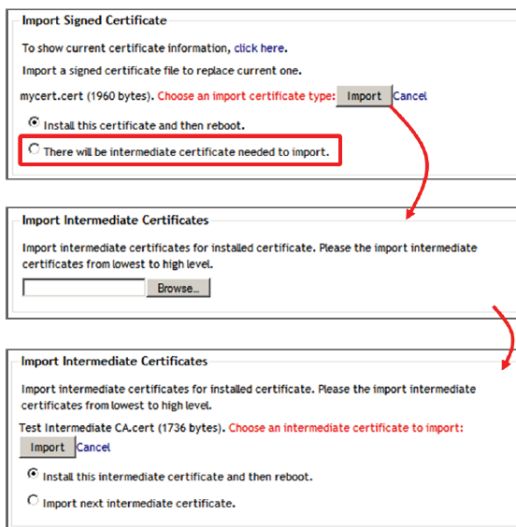
Figure 255. Importing a signed SSL Certificate



- 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 intermediate CA certificate download instructions from the certificate vendor. To import an intermediate certificate:

  - After selecting the end certificate, click on the intermediate certificate import option.
  - Click on the **Import** button to reveal the *Import Intermediate Certificates* form.
  - Click on **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.
- 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 256. 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 on both devices. In this way, you can access the shared virtual

management interface advertised in DNS for the same FQDN without seeing the security warning. 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](#).

- **Back Up Trusted CA Information:** Use this option to apply the same trusted CA from this ZoneDirector to peer ZoneDirectors. The file is output as a .tar.gz file containing all trusted Certificate Authority 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](#).

Figure 257. SSL Certificate Advanced Options

**Advanced Options**

**Restore to Default Certificate/Private Key**

If needed, you can discard the imported certificate and private key. ZoneDirector will use factory default certificate/key after restore and reboot.

**Back Up Private Key**

If you want to apply the same certificate from this ZoneDirector to other ZoneDirectors, please back up the private key from this ZoneDirector and then apply it to other ZoneDirectors for certificate key pairing.

**Back Up Certificates for Smart Redundancy**

If you want to apply the same certificate and private key from this ZoneDirector to peer ZoneDirectors, please back up the certificate from this ZoneDirector and then apply it to peer ZoneDirectors.

**Back Up trusted CA information**

If you want to apply the same trusted CA from this ZoneDirector to peer ZoneDirectors, please back up the trusted CA from this ZoneDirector and then apply it to peer ZoneDirectors.

**Re-generate private key of a specific key length**

Re-generate a new private key of a specific key length. This function is only needed when your certificate vendor only accepts 2048 key length instead of 1024 key length. Warning: The ZoneDirector will be rebooted after re-generating a new private key.

Private key length  1024  2048

**Add a trusted CA**

To show all trusted CA [click here](#).

Import a trusted CA to ZoneDirector. When ZoneDirector received a server's certificate, ZoneDirector will match the server's CA against the ZoneDirector's list of trusted CA. If there is not match, ZoneDirector will send an error.

Add a new trusted CA  
 Cover all trusted CA

No file chosen

**Import Ruckus PKI Certificate Package**

To generate Ruckus PKI certificate request, [click here](#).

Import Ruckus PKI certificate package generated by Ruckus certs server. Click the link above to generate Ruckus PKI certificate request and Submit the file to <https://certrenewal.ruckuswireless.com>. You will receive an email containing the Ruckus PKI certificate package.

No file chosen

## Importing Ruckus PKI Certificate Packages

To generate a Ruckus PKI certificate request:

- 1 Go to **Configure > Certificate**, and expand the **Advanced Options** section.
- 2 Locate the **Import Ruckus PKI Certificate Package** section, and click the **click here** link. A file named *ZoneDirector\_rpki\_cert\_request.req* will be generated.

Figure 258. Import Ruckus PKI Certificate Package

The screenshot shows a web interface with several sections:

- Back Up Certificate**: A button labeled "Back Up Certificate".
- Back Up trusted CA information**: A text block explaining that trusted CA information should be backed up from the ZoneDirector to peer ZoneDirectors. Below it is a button labeled "Back Up trusted CA".
- Re-generate private key of a specific key length**: A text block explaining the function and warning that the ZoneDirector will be rebooted. Below it are radio buttons for "Private key length" with options "1024" (selected) and "2048", and a button labeled "Create New".
- Add a trusted CA**: A text block explaining how to show all trusted CA and import a trusted CA. Below it are radio buttons for "Add a new trusted CA" (selected) and "Cover all trusted CA", and a button labeled "Choose File" with the text "No file chosen".
- Import Ruckus PKI Certificate Package**: A text block explaining that to generate a Ruckus PKI certificate request, the user should "click here." (this link is highlighted with a red box in the image). Below it is a button labeled "Choose File" with the text "No file chosen".

- 3 Save the *ZoneDirector\_rpk\_i\_cert\_request.req* file to your local computer.
- 4 Launch a web browser, and go to the following URL: [https://certrenewal.ruckuswireless.com/certificate\\_renewal\\_requests/new](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 259. AP Certificate Replacement page

UPLOAD FILES | REPLACEMENT REQUESTS | LOGOUT Logged in as: [ ]

**RUCKUS**  
Simply Better Wireless.

## AP Certificate Replacement

[Hide Instructions](#)

1. In the "Upload File(s)" section above, select a request file with '.req' extension from appropriate location.
2. You can also use the '.req' file archived as '.tar.gz' for uploading.
3. Click "+" button to add multiple files (10 files max).
4. Click "-" button if you want to remove any chosen file.
5. Optionally, you can provide alternate email address in the email text box. The email address will be notified about the status of Certificate Replacement.
6. After selecting the required files and optional email address, click "Upload" button to upload the files.
7. The submitted requests can be viewed by clicking the "Replacement requests" menu option. Expand the request to view the details of '.req' files. Expand the '.req' file row to view the details of Status and response file.

Upload File(s)

Choose File | ZoneDirector\_rpki\_cert\_request.req

+

email@example.com

Upload

- 6 In the **Upload Files** section, click **Choose File**, and locate the .req 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* page, 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 appears. Wait for the progress screen to complete importing the new package (this process should take approximately one minute).

Figure 260. Loading Ruckus PKI Certificate Package



- 13 Once complete, log back into ZoneDirector, and in the **Most Recent System Activities** widget, you should see the following event message: “ZD/AP Ruckus PKI certificates successfully installed on ZoneDirector.”

Figure 261. Ruckus PKI Certificate successfully installed

The screenshot displays the Ruckus ZoneDirector web interface. The top navigation bar includes the Ruckus logo, the title "ZoneDirector - ZoneDirector", and a status bar with the date "2016/04/05 16:25:52" and links for "Help", "Toolbox", and "Log Out (ruckus)". Below the navigation bar are tabs for "Dashboard", "Monitor", "Configure", and "Administer".

The main content area is divided into several sections:

- System Overview:** Displays system details such as System Name (ZoneDirector), IP Address (192.168.40.100), MAC Address (6C:AA:B3:00:00:A0), Uptime (4d 5h 33m), Model (ZD1200), Licensed APs (5), S/N (123456789012), and Version (9.13.0.0 build 107).
- Currently Managed APs:** A table listing APs with columns for MAC Address, Device Name, Model, Status, Mesh Mode, IP Address, Channel, Clients, and Application Capability. Two APs are shown: one disconnected and one connected.
- Most Recent User Activities:** A section for monitoring user actions.
- Most Active Client Devices (since the last connection):** A table showing client device usage.
- Currently Active WLANs:** A table listing active WLANs with columns for Name, ESSID, Authentication, Encryption, VLAN, and Clients.
- Mesh Topology (Mesh-123456789012):** A section for monitoring mesh network status.
- Most Recent System Activities:** A log of system events. A red box highlights the entry: "ZD/AP Ruckus PKI certificates successfully installed on ZoneDirector".
- Most Frequently Used Access Points:** A table showing the most used APs.
- Support:** A section with links for Ruckus Wireless, Inc., Warranty Info, Product Registration, Activate Your Account, Ruckus Support Web, Support Documentation, Discussion Forums, and Open a Support Case.

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 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 configuration with Guest Access, Web Portal and Hotspot captive portals, use the 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.

---

## **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](#).

To authenticate ZoneDirector administrators using an AAA server:

**1** Set up Group Attributes on the AAA server.

- RADIUS:
  - Ruckus Wireless 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+](#) for more information.

**2** Set up ZoneDirector to use an AAA server (**Configure > AAA Servers**).

**3** Create an Administrator Role in ZoneDirector (**Configure > 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.

---

**CAUTION!** 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 (**Configure > 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}).
```

## Upgrading the License

Depending on the number of Ruckus Wireless APs you need to manage with your ZoneDirector, you may need to upgrade your license as your network expands. Contact your authorized Ruckus Wireless 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.

---

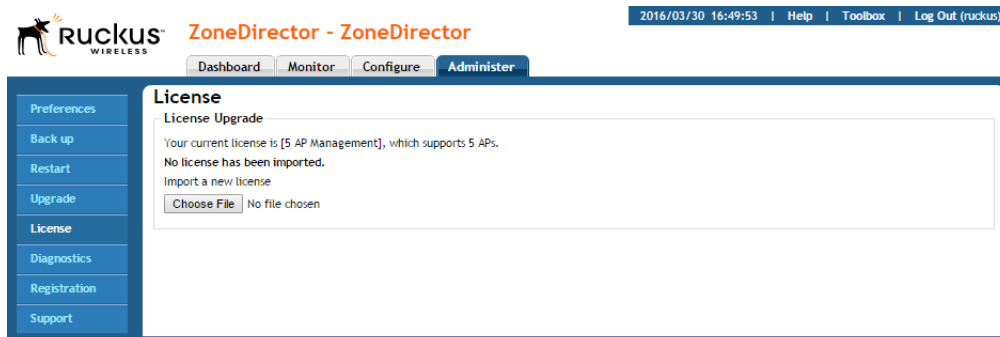
**NOTE:** The system does not reboot or reset after a license is imported.

---

To import a new license file

- 1 Go to **Administer > License**.
- 2 Click **Choose File** and select your license file.
- 3 Once you select your license file and close the *Browse* window, ZoneDirector immediately attempts to validate and install the license.

Figure 262. The License page



## Support Entitlement

The 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 a new support entitlement. After you have purchased a support package and registered your purchase on the Support website, you can click **Check Entitlement** to download the entitlement file and automatically import into your ZoneDirector or manually upload it to ZoneDirector.

To import a new Support entitlement file:

- 1 Go to **Administer > Support**.
- 2 In the *Support Service* section, click **Browse...** to import a new support entitlement file.

Figure 263. Uploading a Support entitlement file

The screenshot shows the Ruckus ZoneDirector Administer page. The top navigation bar includes the Ruckus logo, the text "ZoneDirector - ZoneDirector", and a status bar with "2016/03/30 16:56:34 | Help | Toolbox | Log Out (ruckus)". Below the navigation bar are tabs for "Dashboard", "Monitor", "Configure", and "Administer". A left sidebar contains menu items: "Preferences", "Back up", "Restart", "Upgrade", "License", "Diagnostics", "Registration", and "Support". The main content area is titled "Support" and contains two sections: "Support services" and "Support renew".

**Support services**

The Support Service on this ZoneDirector will expire in [88] days. An active Support service entitles you to future firmware upgrades. Please contact Ruckus Support for further assistance.

Serial number	Services purchased	Date to start	Date to end	Number of AP	Status
123456789012	904	2016/03/27 09:00:00	2016/06/26 08:59:00	licensed	Active <a href="#">Detail</a>

Import a new entitlement file.

No file chosen

**Support renew**

Click on this button to command ZD to get new entitlement from Ruckus support server.

**Support Entitlement**

SSL Certificate Advanced Options



In this chapter:

- [Troubleshooting Failed User Logins](#)
- [Fixing User Connections](#)
- [Measuring Wireless Network Throughput with SpeedFlex](#)
- [Diagnosing Poor Network Performance](#)
- [Starting a Radio Frequency Scan](#)
- [Using the Ping and Traceroute Tools](#)
- [Viewing Current System and AP Logs](#)
- [Packet Capture and Analysis](#)
- [Importing a Script](#)
- [Enabling Remote Troubleshooting](#)
- [Restarting an Access Point](#)
- [Restarting ZoneDirector](#)

## Troubleshooting Failed User Logins

**SUMMARY:** This troubleshooting topic addresses the problems that network users might have with configuring their client devices and logging into your ZoneFlex WLAN.

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 configuration, which enables 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 WPA encryption.

If you and your WLAN users run into initial connection failures when using the Zero-IT configuration and login, almost all 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, and if needed, acquire a wireless network adapter with WPA 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 WPA passphrase in their network configuration (see [Provisioning Clients that Do Not Support Zero-IT](#)).
- 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 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.

# 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 user's client from the Active Clients table in the Ruckus ZoneDirector, and when their client connection automatically renews itself, any previous problems will hopefully be resolved.

To fix the connection of an active client:


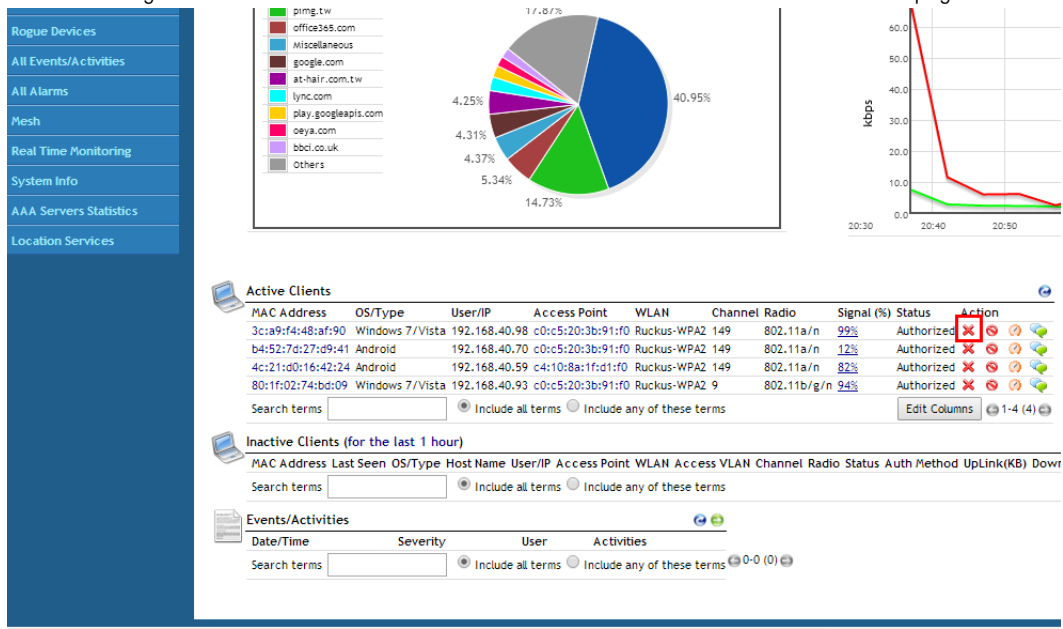
- 1 Go to **Monitor > Wireless Clients**.
- 2 In the *Clients* table, locate the problematic client., and click the **Delete** button  on the same row.
- 3 The client will be immediately disconnected from the WLAN. (Be sure not to block the client. If you do accidentally block a client, go to Configure > Access Control to unblock.)
- 4 From the client computer, refresh the list of wireless networks and attempt to log in again.
- 5 After one to two minutes, the *Clients* table will refresh and display the client again.

Figure 264. Click the X icon to delete a client record from the Wireless Clients page



## 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 reactivate their device with ZoneDirector.

- 1 Have the user log out of the WLAN.
- 2 Go to **Configure > 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 Windows 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 the downlink throughput between ZoneDirector and a wireless client, ZoneDirector and an AP, and 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 **Configure > WLANs > Editing {WLAN Name}** 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 **Monitor > Access Points**. If you want to test client throughput, click **Monitor > 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 the SpeedFlex link on the same row. 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 perfor-

mance 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](#).) 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 265. The SpeedFlex interface

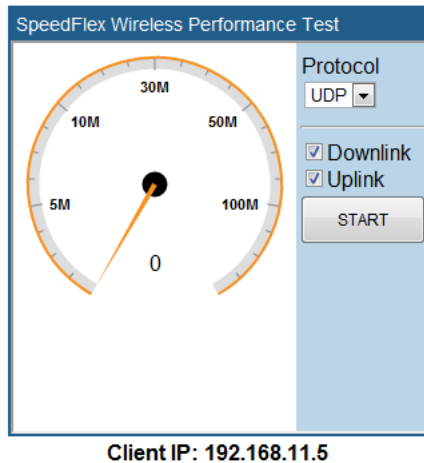


Figure 266. Click the download link for the target client's operating system

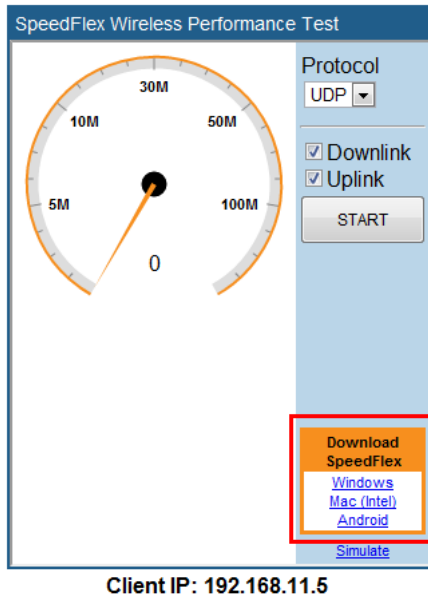


Figure 267. A progress bar appears as SpeedFlex measures the wireless throughput

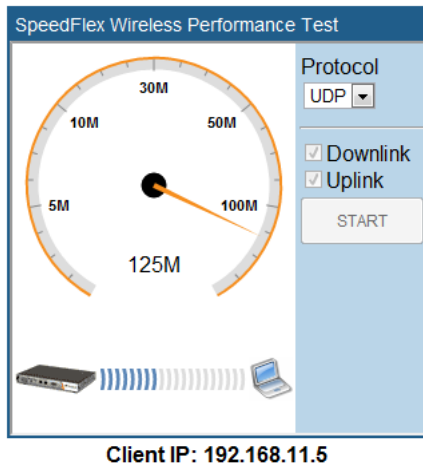
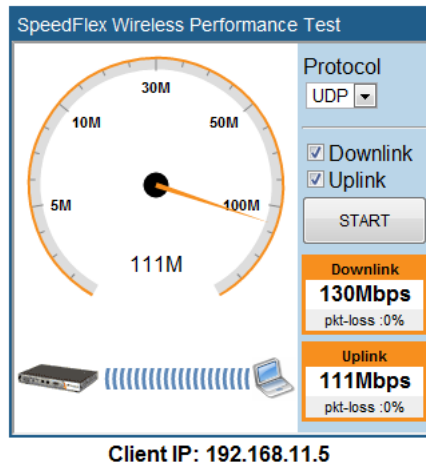


Figure 268. When the test is complete, the tool shows the uplink and downlink throughput and packet loss percentage



## 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 **Monitor > Mesh**, or open the **Mesh Topology** widget on the Dashboard.
- 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.
- 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 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 269. Running Multi-Hop SpeedFlex in a mesh tree

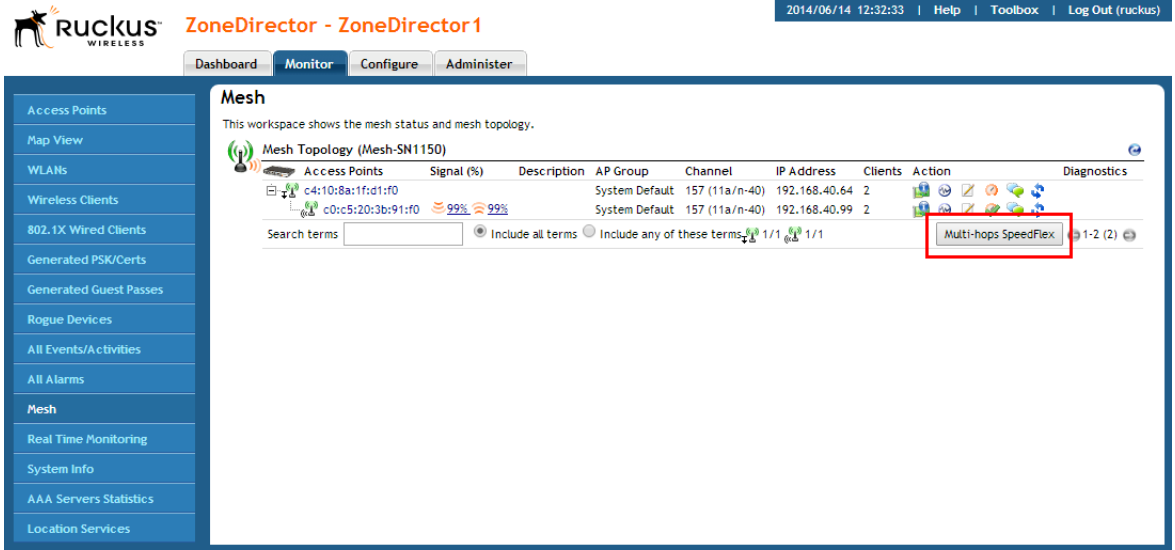
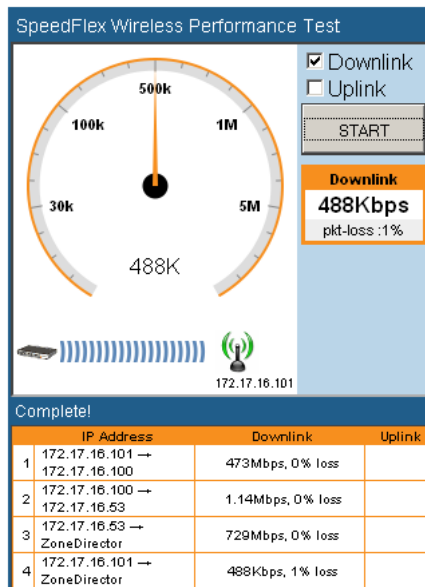


Figure 270. Multi-Hop SpeedFlex test results



## 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, remember to replace the `{zonedirector-ip-address}` variable with the actual ZoneDirector IP address.

### How to Measure the Speed of Your Wireless Connection

The following instructions describe how you can use SpeedFlex, a wireless performance test tool from Ruckus Wireless, 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:

```
http://{zonedirector-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 and Mac (Intel) 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. Alternatively, contact your network administrator for assistance.

## Diagnosing Poor Network Performance

You can try the following diagnostic and troubleshooting techniques to resolve poor network performance.

- 1 Go to **Monitor > Map View**.
- 2 Look on the map for rogue APs. If there is a large number, and they belong to neighboring networks, proceed to the next task.
- 3 Go to **Configure > Access Points**.
- 4 Edit each AP record to assign each device a channel that will not interfere with other nearby APs.

For example, if you have three APs operating in the 2.4 GHz band, you can manually set each one to a different non-overlapping channel by selecting channel “1”, “6” and “11” from the Channel drop-down list.

## Starting a Radio Frequency Scan

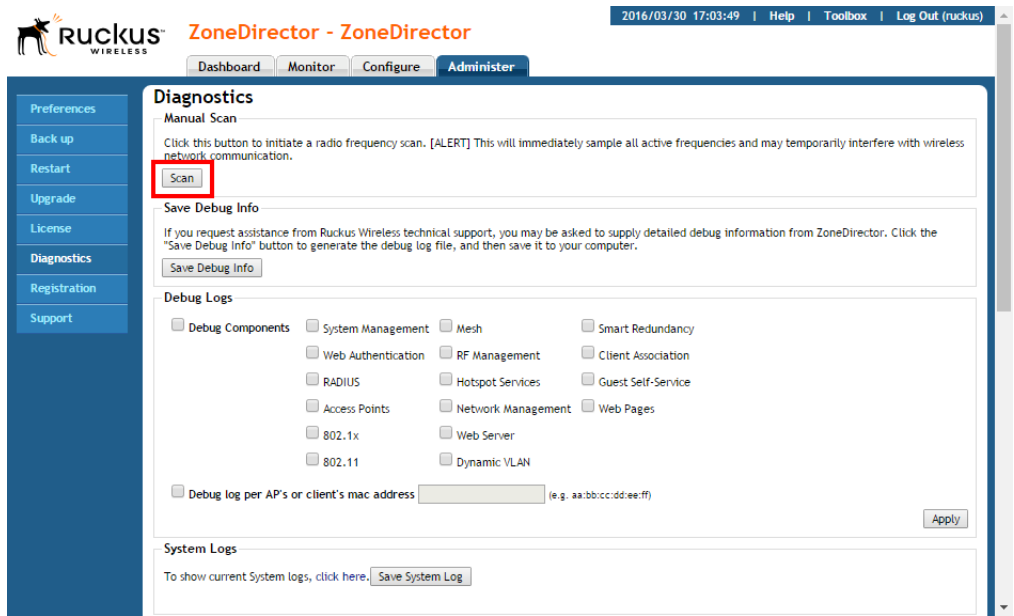
This task complements the automatic RF scanning feature that is built into the Ruckus ZoneDirector. That automatic scan assesses one radio frequency at a time, every 20 seconds or so. To manually start a complete radio frequency scan that assesses all possible frequencies in all devices at one time, follow these steps:

- 1 Go to **Administer > Diagnostics**.
- 2 When the *Diagnostics* page appears, look for the *Manual Scan* options, and then click **Scan**.


**CAUTION!** This operation will interrupt active network connections for all current users.

- 3 Open the Dashboard or go to **Monitor > Map View** to review the scan results. This will include rogue device detection, and an updated coverage evaluation.

Figure 271. The Diagnostics page

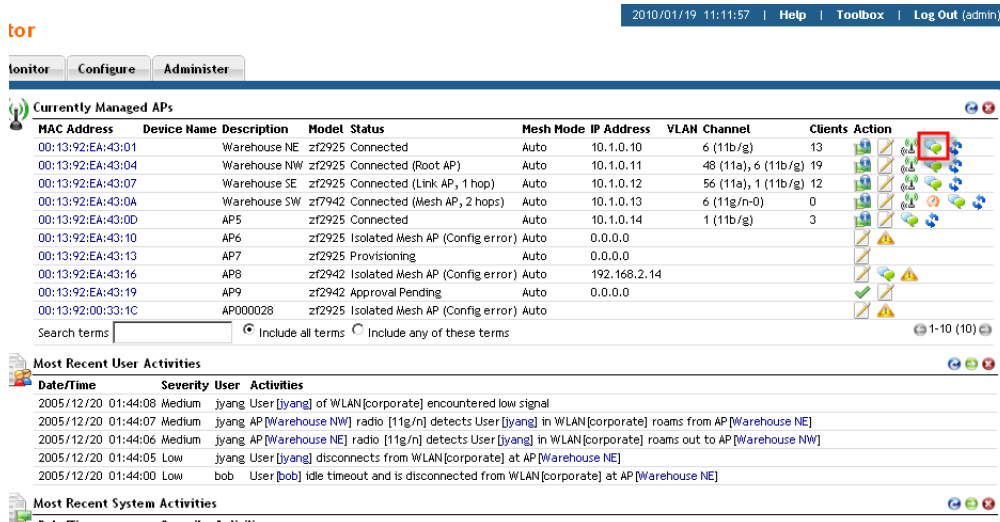


## Using the Ping and Traceroute Tools

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 anywhere in the UI that you see the  icon.

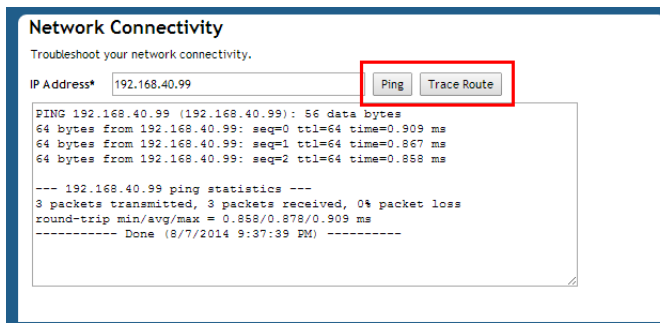
For example, from the Dashboard, if the “Currently Managed APs” widget is open, click the icon next to an AP to launch the troubleshooting window.


Figure 272. Launching the Ping/Traceroute Troubleshooting window from the Dashboard



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 273. Network Connectivity dialog



You can also access the Ping and Traceroute tools by clicking the troubleshooting icon  for an AP or client on the *Monitor > Access Points* and *Monitor > Wireless Clients* pages, or via the **Toolbox** drop-down menu available from any page in the web interface.

## Generating a Debug File

---

**CAUTION!** 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 **Administer > 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 When the *File Download* dialog box appears, select **Save File**, and click **OK**.
- 7 When the *Save As* dialog box appears, pick a convenient destination folder, type a name for the file, and click **Save**.
- 8 When the *Download Complete* dialog box appears, click **Close**.

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 Wireless support representatives have the proper tools to decrypt this file.

---

## Viewing Current System and AP Logs

You can display a list of recent ZoneDirector or AP activity logs from the ZoneDirector web interface.

To view ZoneDirector system logs:

- 1 Go to **Administer > Diagnostics**, and locate the *System Logs* section.
- 2 Click the **“Click Here”** link next to *“To show current System logs...”*. The log data is displayed in the text box beneath the link.
- 3 Click the **Save System Log** button to save the log as a compressed .tar file.

To view AP logs:

- 1 Go to **Administer > Diagnostics**, and locate the *AP Logs* section.
- 2 Click the **“Click Here”** link next to *“To show current AP logs...”*. The log data is displayed in the text box beneath the link.

Figure 274. Viewing System and AP logs

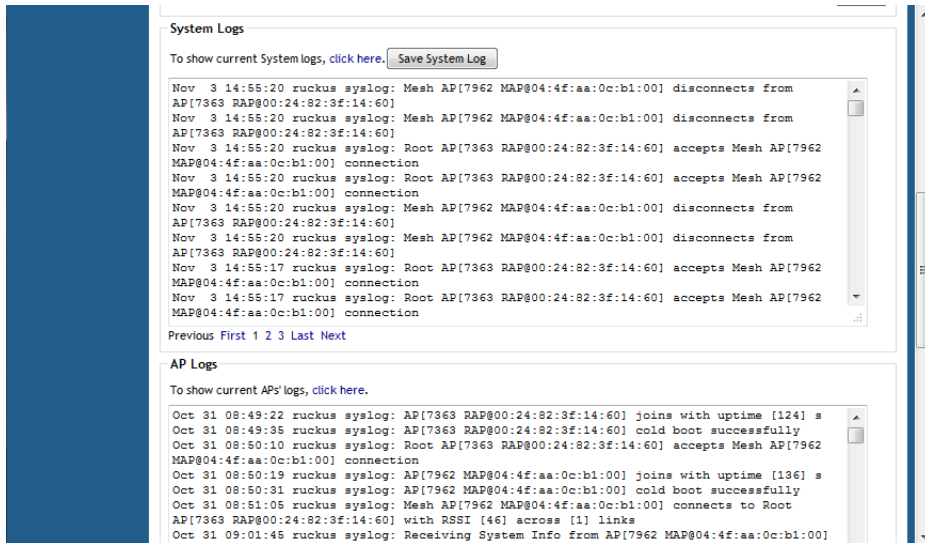
The screenshot shows the 'Diagnostics' configuration page. At the top, there are several checked checkboxes for 'Debug Components': System Management, Mesh, Smart Redundancy, Web Authentication, RF Management, Web Pages, RADIUS, Hotspot Services, Access Points, Network Management, 802.1x, Web Server, and 802.11, Dynamic VLAN. There is also an unchecked checkbox for 'Debug log per AP's or client's mac address' with a text input field and an 'Apply' button.

The 'System Logs' section is highlighted with a red box. It contains the text 'To show current System logs, click here.' followed by a 'Save System Log' button.

The 'AP Logs' section is also highlighted with a red box. It contains the text 'To show current APs' logs, click here.'

The 'Packet Capture' section is visible below. It has a 'Radio' section with '2.4GHz' and '5GHz' options, where '5GHz' is selected. Below that is a table for 'Current Managed APs' with columns for 'MAC Address', 'Device Name', 'Description', and 'Model'. The table contains one entry: '00:24:82:3f:14:60', '7363 RAP', '7363 RAP', and 'zF7363'. To the right of the table is a 'Capture APs' section with the text: '---> There are no APs selected to capture packets. Please select APs from the left table.'

Figure 275. UI display of current system and 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 <http://www.manpagez.com/man/7/pcap-filter/>.

## Local Capture

To capture packets to a local file for external analysis:

- 1 Choose **2.4 GHz** or **5 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 and click **OK**.

- 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.
- Click **Start**. Wireshark displays the packet stream in a new window.

Figure 276. Add APs from Currently Managed APs list to Capture APs list

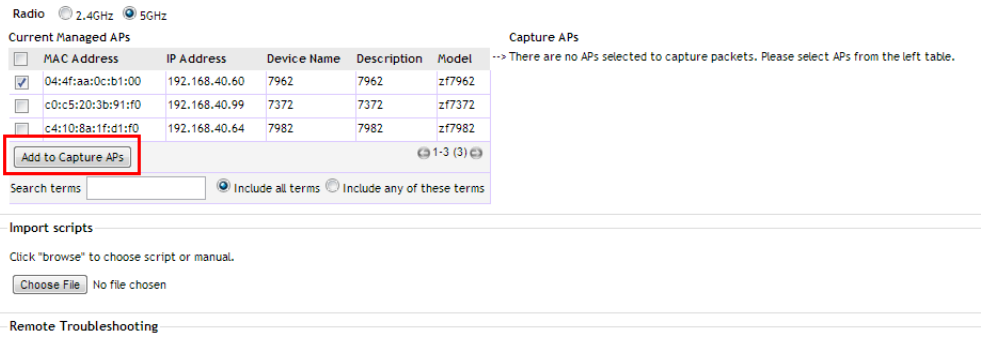
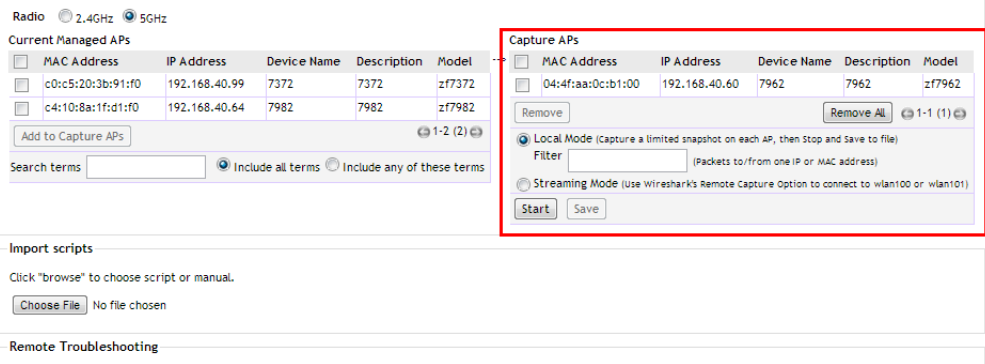


Figure 277. Click Start to begin packet capture; click Remove to remove APs from the list

Use this feature to capture wireless packets during normal operation and save them in local files or stream them to Wireshark.



## 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.

- 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 36. 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 278. AP diagnostic information

To show current System logs, click here.

**AP Logs**  
To show current APs' logs, click here.

**Packet Capture**  
Use this feature to capture wireless packets during normal operation and save them in local files or stream them to Wireshark.

Radio  2.4GHz  5GHz

Current Managed APs

MAC Address	IP Address	Device Name	Description	Model
<input type="checkbox"/> c0:c5:20:3b:91:f0	192.168.40.10	RuckusAP		zF7372

Add to Capture APs  1-1 (1)

Search terms   Include all terms  Include any of these terms

**AP diagnostic information**  
This AP list is the diagnostic AP list.

MAC Address	IP Address	Device Name	Description	Model	Action
					<input type="button" value="Delete All APs"/> 0-0 (0)

Search terms   Include all terms  Include any of these terms

**Import scripts**  
Click "browse" to choose script or manual.  
 No file chosen

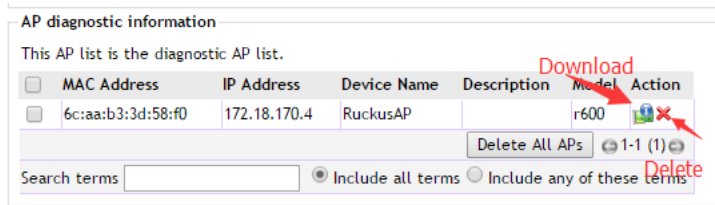
**Remote Troubleshooting**  
Start/stop remote troubleshooting and clicking on the "refresh" will display status information when this function is enabled in real time.

Start remote troubleshooting

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 279. AP Diagnostic Information buttons



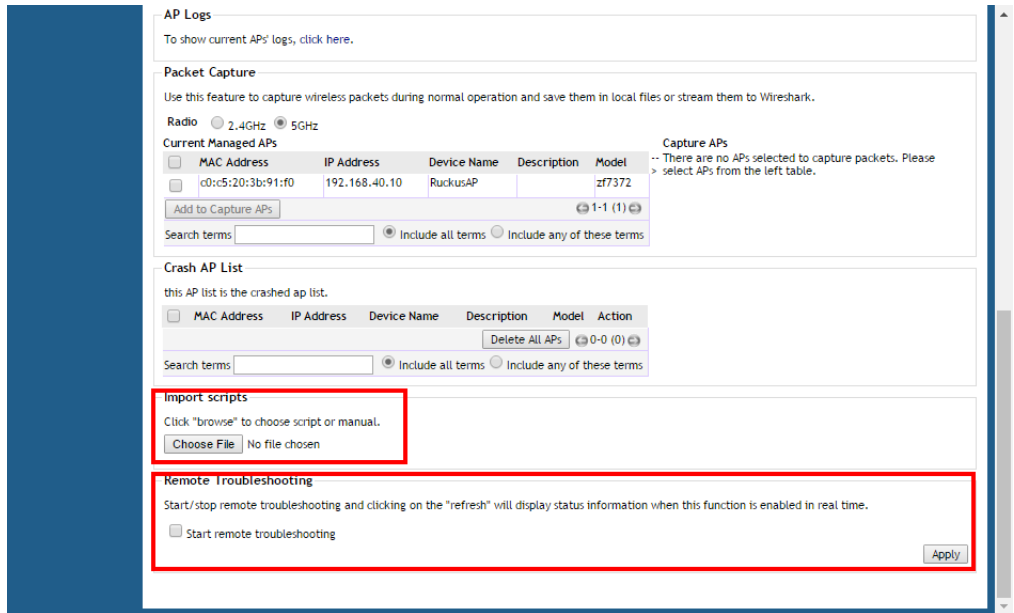
## Importing a Script

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 **Administer > 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 280. The Upload Scripts and Remote Troubleshooting features are used by Ruckus Support in diagnosing customer network issues remotely



## 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 **Monitor > Access Points**.
- 2 When the *Access Points* page appears, look in the *Currently Managed APs* table for the particular Access Point record.  
The *Status* column should display “Connected.”
- 3 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 Ruckus 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](#)”).

---

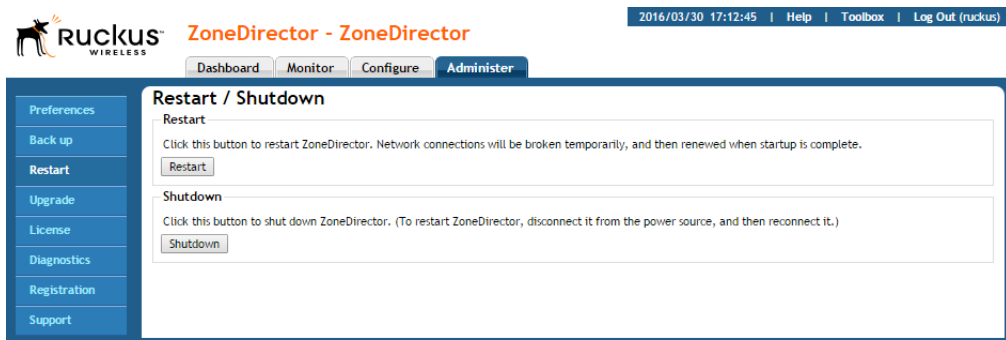
**NOTE:** If you have made any configuration changes, Ruckus Wireless recommends shutting down ZoneDirector to ensure that all configuration changes are saved and remain after reboot. Performing a Restart may cause ZoneDirector to lose configuration changes if you forgot to click Apply after making changes and navigate away from a configuration page, for example.

---

To restart ZoneDirector (and all currently active APs):

- 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 281. The Restart/Shutdown page



## Restarting ZoneDirector

Streaming Mode



# Smart Mesh Networking Best Practices

# 12

In this chapter:

- [Choosing the Right AP Model for Your Mesh Network](#)
- [Calculating the Number of APs Required](#)
- [Placement and Layout Considerations](#)
- [Signal Quality Verification](#)
- [Mounting and Orientation of APs](#)
- [Best Practice Checklist](#)

## Choosing the Right AP Model for Your Mesh Network

Ruckus Smart Mesh networks support both 802.11n and the newer, faster 802.11ac APs with which to form a mesh network. 802.11ac APs will mesh with 802.11n APs, and vice versa.

The most important point to note, however, is that dual band APs can only mesh with other dual band APs, while single band APs can only mesh with other single band APs.

In summary, build your mesh network as follows:

- Ensure that all APs are dual band (H500, R300, R310, R500, R510, R600, R700, R710, T300, 7055, 7372, 7782, 7982, etc.)
- Ensure that all APs are single band (ZoneFlex 7352, etc.)

## Calculating the Number of APs Required

This is an important step in planning your mesh network. You will need 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.

WiFi 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, 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.

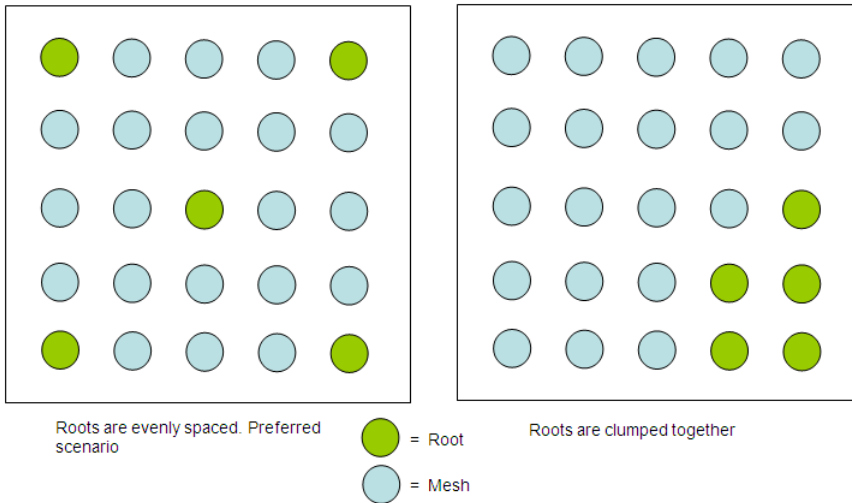
In a Smart Mesh network, the Root AP (RAP) has all its wireless bandwidth available for downlink, because the uplink is wired. For Mesh APs (MAPs), the available wireless bandwidth has to be shared between the uplink and the downlink. This

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  $\geq$  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 [Figure 282](#) 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 282. 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 Ruckus Wireless AP. A distance of 10 feet or more would be desirable.

## Signal Quality Verification

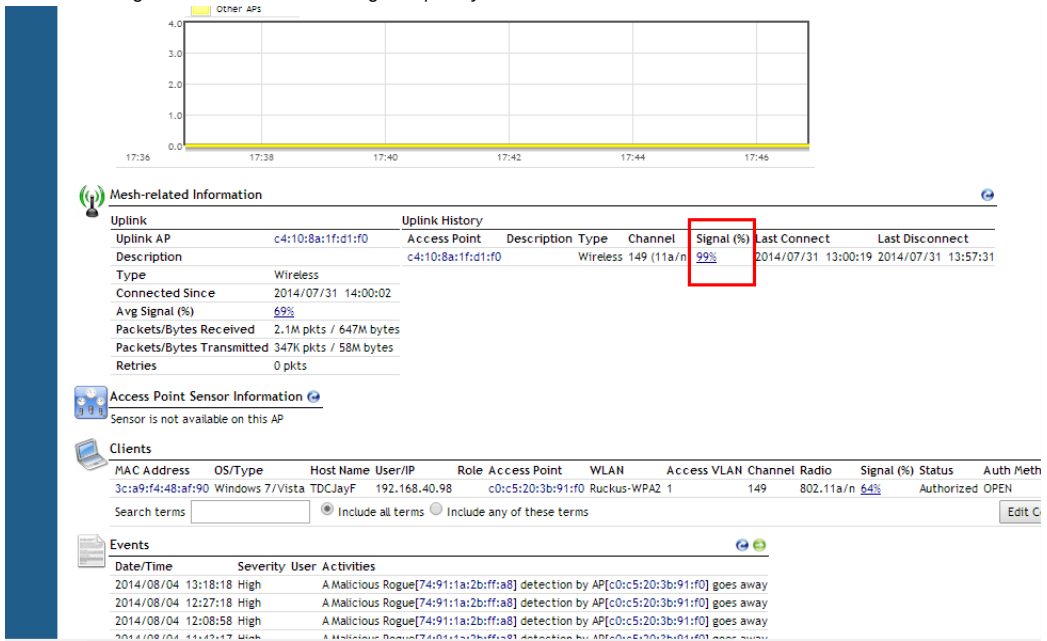
The above guidelines for planning will result in a well-designed mesh. However, it is advisable to place the APs in the planned locations temporarily using a tripod stand or other means, and actually checking the Signal Quality throughout the mesh network. In addition, once the mesh is deployed, the Signal Quality should be periodically monitored to make sure the mesh is operating optimally. Signal Quality is a measurement of the link quality of the MAP's uplink, and is available on the ZoneDirector web interface.

To view the Signal parameter in the ZoneDirector web interface, go to **Monitor > Access Points**, and click on the Mesh AP being tested (click the MAC address) to see the Access Point detail screen, as shown in [Figure 283](#) below.

There are two best practice observations that should be met:

- Ensure Signal  $\geq$  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.

Figure 283. Check the signal quality from the ZoneDirector web interface



## Mounting and Orientation of APs

ZoneFlex APs are very tolerant to a variety of mounting and orientation options due to Ruckus Wireless' use of its unique BeamFlex technology, in which the RF signal is dynamically concentrated and focused towards the other end of the RF link.

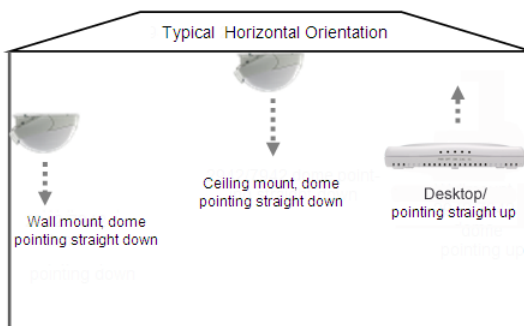
The bottom line regarding orientation and placement is that during the planning phase, it is advisable to use the Signal Quality as your benchmark, as explained in the Signal Quality Verification section. Ensure that the Signal is better than 25% for trouble-free operation.

For additional mounting details, please also consult the Quick Setup Guide and the Wall and Ceiling Mounting Instructions that came in the AP box.

### Indoor APs - Typical Case: Horizontal Orientation

ZoneFlex indoor APs are typically oriented such that the top of the AP is pointing either straight up or straight down.

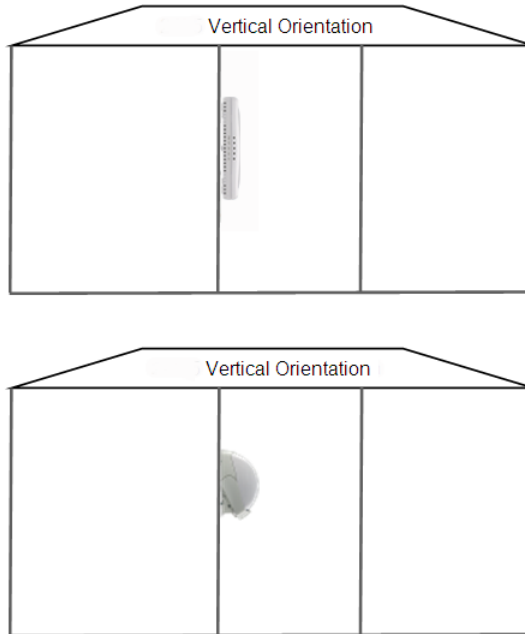
Figure 284. ZoneFlex indoor AP horizontal orientation



## Indoor APs - Vertical Orientation

A less typical vertical orientation may be used in certain cases where it is not possible for mechanical or aesthetic reasons to use the typical horizontal orientation. In such cases, indoor APs may also be wall mounted vertically. Examples of vertical mounting are shown in Figure 285.

Figure 285. ZoneFlex indoor AP vertical orientation



## Outdoor APs - Typical Horizontal Orientation

Outdoor APs are typically mounted in a horizontal orientation, as shown in [Figure 286](#). A less typical orientation would be vertically mounted.

Figure 286. 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.



## 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** Do not mix single band with dual band APs in your mesh. They will NOT mesh. To ensure your APs will mesh with each other, ensure they are all of the same radio type: either all single band or all dual band APs.
- 2** Avoid an excessive number of hops. Ideally keep hop count to 3 or less.
- 3** Having more RAPs is better for performance.
- 4** 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.
- 5** Where possible, ensure that the RAPs are distributed evenly throughout the coverage area rather than clumped together.
- 6** 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.
- 7** 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.



# Appendix: Zone 2 APs

Some Ruckus Wireless access points can be purchased with the country code factory configured and locked to a regulatory region referred to as “Zone 2”. AP ordering numbers with a “Z2” in the suffix, for example 901-R700-Z200, have been factory locked to the Zone 2 country code setting. End users of these access points are not able to change the country code setting, operate the AP on non-Z2 channels, or use non-Z2 transmit power limits.

APs discover and join Ruckus Wireless controllers with matching “Zone 2” or “Z2” country code settings.

APs with locked Z2 country code settings comply with the Zone 2 regulatory limits outlined in [Table 37](#).

Table 37. Zone 2 Regulatory Information

SKU suffix	Locked	Country	Country Code	2.4 GHz CH (1-13) and RF Power Limit	5.150 GHz-5.250 GHz (W52) RF Power Limit	5.250 GHz-5.350 GHz CH (W53) and RF Power Limit
-WWxx	Unlocked	Algeria	DZ	1-13/100mW (outdoor limited to 28mW)	200mW	Indoor: 200mW Outdoor: 1000mW
-WWxx	Unlocked	Morocco	MA	1-13/100mW	200mW	200mW
-WWxx	Unlocked	Tunisia	TN	1-13/100mW	200mW	200mW
-WWxx	Unlocked	Vietnam	VN	1-13/100mW	200mW	200mW
-WWxx	Unlocked	Israel	IL	1-13/100mW	200mW	200mW
-ILxx ( <b>Note</b> )	Locked	Israel	IL	1-13/100mW	200mW	200mW
-Z2xx	Locked	Zone 2	Z2	1-13/100mW	200mW	200mW

**Note:** -ILxx is not used for new designs

# Index

## Numerics

- 11n/ac Only Mode 282
- 802.11d 231
- 802.11k 234
- 802.11r 224
- 802.11u 261
- 802.1X
  - authenticator 294
  - supplicant 296
  - user requirements 241
  - WLAN security 241
- 802.1X EAP
  - option values 224
  - Windows OS requirements 241
- 802.1X EAP + MAC Address Authentication 224

## A

- AAA servers 367
- Access Controls 229
- Access Permissions 150
- Access Point Policy approval 279
- Access Point Policy options 299
- Access Points
  - managing individually 305
  - monitoring 334
  - monitoring individually 339
  - sensor information 348
  - working with AP Groups 281
- Accounting Server 229
- ACL 229
- ACLs
  - Layer 2/MAC 150
  - Layer 3/Layer 4/IP Address 151
  - Management ACL 78
- Action Icons 329, 336
- Actions
  - individual APs 339
- Active Client Detection 138
- Active Clients 329
- Active Directory 171, 367
- Active Directory over TLS 173

- Adding a Widget 52
- Adjusting AP Settings
  - Map View 310
- Administrator Login Session Timeout 437
- Advanced LDAP Filtering 176
- AeroScout 136
- AES
  - option values 225
- airtime % 339
- Alarms
  - activating email notification 90
- Algorithm
  - New WLAN creation 225
- All Events/Activities (Logs) 84
- AP
  - Zone 2/Z2 499
- AP Activities 52
- AP Groups 281
- AP License Pools 74
- AP markers
  - overview 319
- AP Power 126
- AP Site Bonjour Policy 117
- Application Capability 336
- Application Denial Policies 167, 232
- Application Performance 324
- Application Port Mapping 165
- Application Recognition 324
- Application Recognition and Filtering 164
- Application Usage 324
- Application Usage by Client 327
- Application Usage Statistics 331
- Application Visibility 166, 232, 324
  - Client Usage 327
- Applications 52
- Applying an Application Denial Policy to a WLAN 169
- APs
  - detecting rogue devices 349
  - placing markers on a floorplan map 316
  - restarting 486
  - verifying new APs 279
- Archived ZoneDirector settings
  - restoring 441
- ARP Broadcast Filter 419
- Assigning a Pass Generator role to a user 396
- Authentication Method 224
- Authentication Server 226
- Authentication Servers

- external 367
- internal user database 360
- Authentication settings
  - testing 196
- Authentication, Authorization and Accounting (AAA) 171
- Authenticator 294, 295
- Authenticator (MAC-based) 295
- Authenticator (Port-based) 295
- Auto encryption algorithm 225
- Auto Recovery 300
- Auto Refresh 57
- Automatic AP Approval 278, 279, 299, 341, 428
- Automatic Channel Selection 126
- Automatically Adjust AP Power 126
- Automatically Generated User Certificates and Keys
  - managing 366
- Autonomous WLAN 205
- Auto-Proxy 233
- Auto-Refresh
  - stopping and starting 57
- AVP 166, 184, 232, 324, 327

## B

- Background Scanning 126, 129, 231
- Backup RADIUS / RADIUS Accounting 179
- Backup/Restore ZoneDirector 441
- Band Balancing 134, 231
- Blocked Clients 144, 157
- Blocked clients
  - reviewing a list 160
- Blocking Client Devices 159
  - Temporary 158
- Blocking client devices 157
- Blocking specific client devices 159
- Bonjour
  - Example 118
- Bonjour Gateway 111, 336
- Buttons (Web interface)
  - explained 49
- Bypass Apple CNA Feature
  - Apple CNA Bypass 275

## C

- Call Admission Control 229, 283, 306

- Captive Portal 255, 370
- Changing an Existing User Account 362
- Changing the event log level 85
- Changing the System Name 62
- Channel 282, 305
- Channel Mode 84
- Channel optimization 82
- Channel Range Settings 282, 305
- Channel Selection 126
- ChannelFly 127
- Channelization 282, 305, 311
- Client Application Usage Statistics 331
- Client Device Type 52
- Client devices
  - monitoring 158
  - permanently blocking WLAN access 159
  - reviewing a list of blocked clients 160
  - temporarily disconnecting 158
- Client Events 331
- Client Events/Activities 329
- Client Fingerprinting 233
- Client Isolation 228
- Client Isolation White Lists 161
- Client Tx Data Rate 331
- Client Tx/Rx Statistics 232
- Clients
  - monitoring 331
- Cloning a WLAN 236
- Common WISPr Attribute Abbreviations 260
- Configuring Access Controls 150
- Controller migration 341, 428
- Controlling Guest Pass Generation Privileges 395
- Controlling Network Access Permissions 150
- Copying a WLAN 236
- Country Code 81
- Create New options
  - Authentication Servers 367
- Create New User
  - internal database 361
- create user 360
- Creating a Guest Pass Generation User role 395
- Creating a new WLAN
  - Access VLAN 230
  - Algorithm 225
  - Description 204

- Hide SSID 230
- Method 224
- Name/ESSID 203
- Passphrase 226
- WEP key 226
- Zero IT Activation 229
- Creating a WLAN 202
- Creating Additional WLANs 236
- Current Alarms
  - reviewing 321
- Current User accounts
  - managing 362
- Current User Activity
  - Reviewing 324
- Currently Active WLAN Groups 51
- Currently Active WLANs 51
- Currently Managed AP Groups 51
- Currently Managed APs 51
- Customizing Guest Login page 404
- Customizing network security 200

## D

- Dashboard 50
  - overview 314
- Dashboard (Web interface)
  - explained 49
- Dashboard Widgets 51
- Data Rate 331
- Deleting a User Record 363
- Delivering Guest Passes via Email 407
- Delivering Guest Passes via SMS 408
- Denial of Service (DoS) Protection 144
- Description
  - New WLAN creation 204
  - option values 204
- Detecting rogue Access Points 349
- Device Access Policies 153
- Device Name 305
- Device Policy 254
- Devices Overview 51
- DGAF 266
- DHCP 76
  - network address option 64
  - server customization 35
- DHCP clients
  - viewing 78
- DHCP Option 82 232, 290
- DHCP Relay 108, 231
- DHCP server

- configuring 76
- Diagnostics
  - tools 476
- disabling status LEDs 286
- Disconnecting specific client devices 158
- Disconnecting users from the WLAN 466
- DNS Server
  - Registering ZoneDirector 40
- DoS (Denial of Service) Protection 144
- Downlink Throughput 334, 340
- Downlink Traffic 334
- downstream group-addressed frame forwarding 266
- DPSK 267, 268
- Dynamic Pre-Shared Keys 267, 268
- Dynamic PSK 229, 356
  - expiration 270
- Dynamic VLAN 230, 295

## E

- EAP
  - using the built-in server 240
- EAP-MD5 183
- Ekahau 137
- Email
  - Guest Passes 407
- Email alarm notification
  - activation 90
- Email Guest Passes 407
- Encryption Options 225
- ESSID 203
- Estimated Capacity 334, 340
- Ethernet Port Redundancy 142
- Ethernet port status 297
- Event Log Level 85
- Events 331
  - monitoring 340
- Events and alarms 84
- Events/Activities
  - Clients 329
- Example Bonjour Gateway Network Setup 118
- External Antenna 306
- external antenna 286
- External IP 336

## F

- Facebook 206

- Factory default state
  - restoring ZoneDirector 445
- Fail Over 70
- Failed user connections 466
- Failover
  - force 74
- Fast BSS Transition 224
- Firewall
  - open ports 43
- Firewall Integration 86
- Firmware upgrade 438
- FlexMaster
  - enabling 108
  - Performance Monitoring 98
- Floorplan
  - adding to Map View 309
- Force DHCP 232

## G

- Google/Google+ 206
- Graphic file formats
  - guest user login page 404
- Graphic file specifications
  - guest user login page 404
- Group Extraction 177
- Group Settings 283
- Guest Access Customization 404
- Guest Access WLAN 204
- Guest Pass 408
  - custom 405
  - SMS Delivery 93
  - Sponsor Approval 381
- Guest Pass Access
  - managing 374
- Guest Pass Self-Service 376
- Guest Passes
  - Email Delivery 407
- Guest user login page
  - adding a graphic 404
  - editing the welcome text 404
- Guest users
  - login page customization 404
- Guest VLAN 295

## H

- Help and Log Out 49
- Hide SSID
  - New WLAN creation 230

- Hotspot 255
  - configuration 255
  - WISPr Smart Client 256
- Hotspot 2.0 261
  - AP Venue Settings 308
  - Operator Profile 263
  - Service Provider Profile 261
  - WLAN 266
- Hotspot 2.0 WLAN 205
- Hotspot Service (WISPr) WLAN 204
- Hotspot2.0 261

## I

- Import Scripts 485
- Importing the floorplan image 315
- Improving AP RF coverage 310
- Inactive Clients 329
- Inactivity timeout 234
- Indicator Widgets 51
- installation 46
- Internal user database
  - using for authentication 360
- Intrusion Detection and Prevention 145
- Intrusion Prevention 144
- IP Address 335
- IP Mode 283

## J

- Join another controller 341, 428

## L

- L2/MAC Access Control 150
- L3/L4 Access Control 151
- LAN Port Configuration
  - monitoring 339
- Language
  - changing the Web interface language 437
- Layer 2/MAC Address Access Control Lists 150
- Layer 3/Layer 4/IP Address Access Control Lists 151
- LBS 119, 283
- LBS Venue Info Widget 354
- LDAP 174, 184, 367
- LDAP Filtering 176
- LDAP Group Extraction 177

- LDAP over TLS 174
- LEDs 22, 25
- License Pools 74
- License Upgrade 461
- Limited ZD Discovery 299
- Link Layer Discovery Protocol 286
- LinkedIn 206
- LLDP 286
- Load Balancing 131, 231, 300
- Location Service 283
- Location Services
  - Monitoring 353
- Location Services Widget 354
- Log
  - All Events/Activities 84
- Log settings
  - changing 84
  - overview 84
- Login failures 466
- Login page
  - guest use 404
- Logout Button 49
- Logs
  - sorting contents 84
  - viewing 478

## M

- MAC Authentication 181, 224
  - RADIUS 181
- MAC authentication bypass 257, 295
- MAC-spoofing Rogue AP 146
- malicious AP 350
- Malicious Rogue AP 146
- Management ACL 78
- Management VLAN 300
- management VLAN 247
- Managing current user accounts 362
- Map View
  - adding a floorplan 309
  - adjusting AP positions and settings 310
  - importing a floorplan 315
  - placing AP markers on a floorplan 316
  - requirements (graphics) 315
  - tools 317
- Maps
  - importing a floorplan image 315
- Mark as Malicious 146
- Max Clients 231, 285, 300
- max clients per AP 285

- MCS 331
- Mesh Mode 311, 335
- Mesh recovery SSID 431
- Mesh Topology 51
- Mesh Topology Detection 419
- Mesh-related Information 340
- Microsoft IAS 191
- Microsoft Windows
  - EAP requirements 241
- Microsoft Windows Live 206
- Migrate button 341, 428
- Mobile Friendly DPSK 269
- Model Specific Control 283
- Modulation and Coding Scheme 331
- Monitor
  - overview 314
- Monitoring
  - individual clients 331
  - Real Time 55
- Monitoring Active Clients 329
- Monitoring AP status 334
- Monitoring Client Devices 158
- Monitoring Client Events 331
- Monitoring individual APs 339
- Monitoring Location Services 353
- Monitoring wired clients 334
- Monitoring Wireless Clients 324
- Monitoring ZoneDirector
  - overview 314
- Most Active Client Devices 51
- Most Frequently Used Access Points 51
- Most Recent System Activities 51
- Most Recent User Activities 51
- Multicast Filter 230
- Multi-Domain Active Directory Authentication 172
- Multi-Hop SpeedFlex 472

## N

- Name/ESSID
  - New WLAN creation 203
  - option values 203
- Navigating the Dashboard 50
- Neighbor APs 340, 347
- Network addressing
  - changing 63
- Network Connectivity 477
- Network Diagnostics 476
- New User Accounts



- adding new accounts 360
- New User Roles
  - creating 363
- NIC Bonding 142

## O

- OKC 235
- Online Help 49
- Opportunistic Key Caching 235
- Optimizing network coverage 320
- Option 82 290
- orientation 348
- Overview
  - Map view 314

## P

- Packet capture and analysis 480
- Packet Inspection Filter 141
- Passphrase
  - New WLAN creation 226
- Passpoint 261
- Performance Analysis
  - monitoring APs 340
- Performance test 468
- Permanently Blocking Client Devices 159
- Ping 476
- PKC 234
- Placing the Access Point markers 316
- PMK Caching 234
- PoE Operating Mode 286
- PoE Out Ports
  - enabling 286
- PoE Out ports 286
- Policies
  - Access Point-specific 299
- Poor network performance
  - diagnosis 475
- Port Redundancy 142
- Port Settings 286
- Port-based 802.1X
  - Authenticator 295
    - authenticator 294
    - Dynamic VLAN 295
      - guest VLAN 295
    - MAC-based Authenticator 295
    - Port-based Authenticator 295
      - supplicant 296
- Potential Throughput 334

- Precedence Policies 156
- Prefer Primary ZD 300
- Preference tab
  - use 436
- Priority 229, 311
- Product Registration 58
- Proxy ARP 140, 231, 266
- PSK
  - Setting key expiration 270
- PSK lifetime settings 270

## R

- Radar Avoidance Pre-Scanning 135
- Radio frequency scans
  - starting a scan 475
- Radio Resource Management 234
- radio statistics 339
- RADIUS 177, 178, 367
  - using an external server 240
  - using for authentication 367
- RADIUS / RADIUS Accounting 178
- RADIUS Accounting Attributes 187
- RADIUS Attribute Value Pairs 184
- RADIUS attributes 184
- RADIUS Authentication 185
- RADIUS over TLS 179
- RAPS 135
- Rate Limiting 229, 230
- RBAC 229
- Real Time Monitoring 55, 314
- Recent events
  - overview 321
- Recently Disconnected Clients 329
- Recovery SSID 431
- Redundancy 70
- Registration 58
- remote syslog advanced settings 89
- Remote Troubleshooting 485
- Removing a Widget 54
- Report Rogue Devices 146
- restarting a ZoneDirector 486
- Restarting an Access Point 486
- Restoring AP configuration settings only 443
- Restoring archived settings 441
- Reviewing AP policies 299
- Reviewing current alarms 321
- RF
  - see also 'Radio frequencies'

- RF Pollution 340, 342
- RFID tags 136
- Rogue Access Points 145
- Rogue APs
  - detecting 349
- Rogue DHCP Server Detection 147
- Role Based Access Control Policy 229, 365
- Roles
  - creating 363
- Roles options
  - Allow all WLANs 363
  - Description 363
  - Group attributes 363
  - Guest Pass 363
  - Name 363

## S

- Same-Network Rogue AP 146
- Scanning radio frequencies 475
- Search Filter 177
- Secure Active Directory 173
- Secure DPSK 269
- Secure LDAP 174
- Secure RADIUS 179
- Security 201
  - overview 200, 201
- Security configuration
  - reviewing 237
- Self Healing 126
- Self-Service Guest Pass 376
- Sensor information 340, 348
- Service Schedule 233
- Session Timeout
  - admin 437
- Setting Dynamic Pre-Shared Key expiration 270
- Single Domain Active Directory Authentication 171
- Smart Redundancy 52, 70
  - Configuration 71
- Smart Redundancy AP License Pools 74
- SMS 408
  - Guest Passes 93
- SMS Guest Passes 408
- SNMP
  - enabling SNMP agent 100
  - enabling SNMP trap notifications 103
  - trap notifications 105

- SNMPv2 101
- SNMPv3 102
- Social Media 205
- Social Media WLANs 205
- Spectralink Compatibility 283, 306
- Spectralink VIEW certification 283
- Spectrum Analysis 345
- SpeedFlex 468
- SpeedFlex in a Multi-Hop Smart Mesh Network 472
- Sponsor Approval 381
- SPoT 283, 353
  - Location Services 119
  - Monitoring 353
- SPoT Dashboard Widget 354
- SSID-Spoofing Rogue AP 146
- SSL Certificate
  - importing 450
- Standard Usage WLAN 204
- Status LEDs
  - disabling 286
- status LEDs 286
- Stopping and Starting Auto Refresh 57
- Supplicant 296
- Support 51
- Support Entitlement 462
- Syslog Firewall Integration 86
- System log 84
- System Logs 84
- System Name 62
- System Overview 51
- SZ migration 341, 428

## T

- Tabs (Web interface)
  - explained 49
- TACACS+ 194
- Telnet 108
- Temperature 348
- Temporarily Block Wireless Clients 144
- Temporarily Disconnecting Client Devices 158
- Testing authentication settings 196
- Throughput Capacity 334
- Timeout interval 437
- TKIP
  - option values 225
- TLS encryption 173, 174
- Toolbox 49, 55, 477

- Tools
  - Map View 317
- Top 10 Applications by Usage 52
- Top 10 APs by Usage 52
- Top 10 Clients by Usage 52, 328
- Top 10 SSIDs by Usage 52
- Traceroute 476
- transmission statistics 339
- Troubleshooting
  - diagnosing poor network performance 475
  - manually Scanning radio frequencies 475
  - problems with user connections 466
  - restarting the ZoneDirector 486
  - Reviewing Current Activity 324
  - reviewing current alarms 321
  - reviewing recent events 321
  - users cannot connect to WLAN 466
- Tunnel configuration 139
- Tunnel Mode 230
  - configuration 139
- Tunnel MTU 300
- Tx Power 282, 305, 311

## U

- Upgrading
  - with Smart Redundancy 440
  - ZoneDirector software 438
  - ZoneFlex APs 438
- Upgrading the license 461
- Uplink Selection 311
- Uplink Throughput 334, 340
- Usage Summary 51
- USB Port 286
- User authentication options
  - Active Directory 367
  - RADIUS 367
- User Defined Applications 164
- User Marked Rogue AP 146
- Users
  - adding new accounts 360
  - creating new roles 363
  - disconnecting a user from the WLAN 466
  - failed WLAN logins 466
  - managing accounts 362
  - Reviewing Current User Activity 324
  - switching to 802.1X-based security 241

- switching to WEP-based security 241
- troubleshooting connection problems 466
- Using Active Directory 367
- Using an external RADIUS server 240
- Using Indicator Widgets 51
- Using Map View to assess network performance 309
- Using the built-in EAP server 240
- Using the Map View 317

## V

- Verifying/Approving New APs 279
- Viewing Application Usage by Client 327
- VLAN
  - New WLAN creation 230
- VLAN Pools 252
- VLANs 245

## W

- Walled Garden 257
- Web Authentication 226
  - activating 369
- Web interface
  - changing the language 437
  - Generated PSK/Certs page 367
  - Roles and Policies 363
- Web interface buttons
  - explained 49
- Web interface Dashboard
  - explained 49
- Web interface tabs
  - explained 49
- Web interface workspaces
  - explained 49
- Web Portal
  - customizing 404
- Well-Known Service and Destination Port Mappings 166
- WEP
  - WLAN Security 241
- WEP Key
  - New WLAN creation 226
- WEP-128
  - option values 225
- WEP-64
  - option values 225
- WEP-based security

- user requirements 241
- Whitelist 161
- Widgets 49, 51
- Windows Live 206
- WIPS 144
- Wireless Client Isolation 228, 257
- Wireless Clients
  - Monitoring 324
- Wireless Intrusion Prevention 144
- Wireless networks
  - overview 32, 200
- Wireless performance test tool 468
- WISPr Attributes 260
- WLAN
  - Autonomous 205
  - creation 202
  - Hotspot 255
  - Hotspot 2.0 261
  - optimizing coverage 320
  - recent events (reviewing) 321
  - Social Media 205
- WLAN Description 204
- WLAN Group 241, 282, 306
- WLAN network security
  - customizing 200
- WLAN performance
  - using Map View 309
- WLAN priority 229, 311
- WLAN security
  - overview 201
- WLAN Service 283
  - disabling 306
- WLAN Usages 204
- WLANs
  - blocking client devices 159
  - Creating Additional Wireless Networks 236
  - failed user logins 466
- WMM-AC 229, 283, 306
- Workspaces (Web interface)
  - explained 49
- WPA2 225
- WPA-Mixed 225
- New WLAN creation 229
- Zero-IT
  - for clients without Ethernet ports 359
- Zone 2 APs 499
- ZoneDirector
  - changing network addressing 63
  - Installation 46
  - Monitoring options overview 314
  - overview 20
  - Physical features 21
  - restarting the device 486
  - restoring backup file contents 441
  - restoring to a factory default state 445
  - upgrading software 438
  - WLAN security explained 201
- ZoneDirector 1200 21
- ZoneDirector 3000 24
- ZoneDirector 5000 27
- ZoneDirector management access 78
- ZoneDirector VLAN Deployment
  - Deploying in a VLAN Environment 245
- ZoneFlex APs
  - upgrading software 438

## Z

- Z2 APs 499
- Zero IT 32, 200, 240, 366, 442
  - enabling 356
- Zero IT Activation







Copyright © 2006-2016. Ruckus Wireless, Inc.  
350 West Java Dr. Sunnyvale, CA 94089. USA  
[www.ruckuswireless.com](http://www.ruckuswireless.com)