Ruckus®

Simply Better Wireless.

Ruckus Wireless™ ZoneDirector™ 9.5

User Guide

Part Number 800-70401-001 Rev C
Published October 2013

www.ruckuswireless.com

About This Guide

This guide describes how to install, configure, and manage the Ruckus Wireless™ ZoneDirector™ version 9.5. This guide is written for those responsible for installing and managing network equipment. Consequently, it assumes that the reader has 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 Web site at:

http://support.ruckuswireless.com/

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]>`
`monospace bold`	Represents information that you enter	`[Device name]>` **`set ipaddr 10.0.0.12`**
default font bold	Keyboard keys, software buttons, and field names	On the **Start** menu, click **All Programs**.
italics	Screen or page names	Click **Advanced Settings**. The *Advanced Settings* page appears.

Table 2. Notice Conventions

Icon	Notice Type	Description
i	Information	Information that describes important features or instructions
!	Caution	Information that alerts you to potential loss of data or potential damage to an application, system, or device
⚡	Warning	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

When contacting us, please include the following information:

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

For example:

- Ruckus Wireless ZoneDirector 9.5 User Guide
- Part number: 800-70401-001 Rev C
- Page 88

Contents

About This Guide

1 Introducing Ruckus Wireless ZoneDirector

2 Configuring System Settings

3 Configuring Security and Other Services

4 Managing a Wireless Local Area Network

5 Managing Access Points

6 Monitoring Your Wireless Network

7 Managing User Access

8 Managing Guest Access

9 Deploying a Smart Mesh Network

10 Setting Administrator Preferences

11 Troubleshooting

12 Smart Mesh Networking Best Practices

Index

1

Introducing Ruckus Wireless ZoneDirector

In This Chapter

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, radio frequency (RF), and location management within a single system. User authentication is accomplished with an internal user database, or forwarded to existing Authentication, Authorization and Accounting (AAA) servers, 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 802.11n are used.

In addition, ZoneDirector supports rogue AP detection and the ability to blacklist client devices from the network — all of which are easily configured and enabled system-wide. When multiple APs are in close proximity, ZoneDirector automatically controls the power and the channel settings on each AP to provide the best possible total coverage and resilience.

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

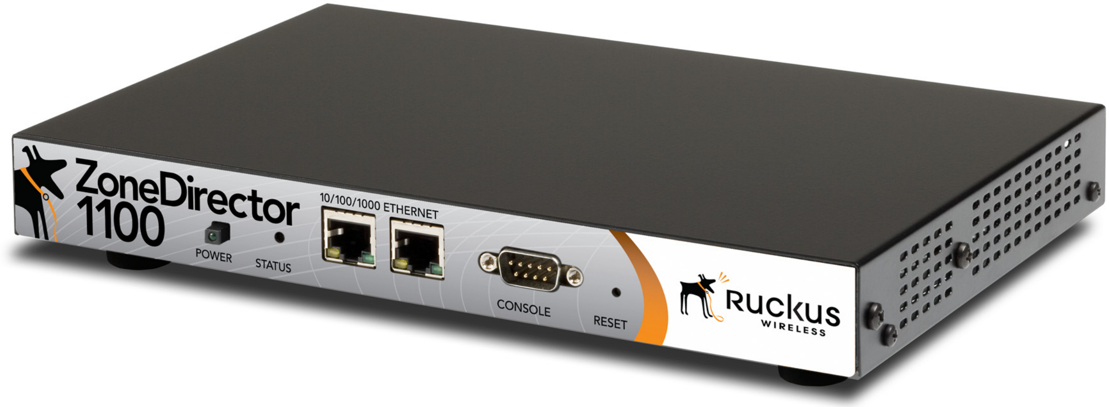
Three models of ZoneDirector are currently available: ZoneDirector 1100, ZoneDirector 3000 and ZoneDirector 5000. This section describes the physical features of these ZoneDirector models.

ZoneDirector 1100

This section describes the following physical features of ZoneDirector 1100:

- Buttons, Ports, and Connectors
- Front Panel LEDs

Figure 1. ZoneDirector 1100



Buttons, Ports, and Connectors

Table 1 describes the buttons, ports, connectors on ZoneDirector 1100.

Table 1. Buttons, ports, and connectors on ZoneDirector 1100

Label	Description
Power	Press this button to power on ZoneDirector.
10/100/1000 Ethernet	Two auto negotiating 10/100/1000Mbps Ethernet ports. For information on what the two Ethernet LEDs indicate, refer to Table 2.
Console	DB-9 port for accessing the ZoneDirector command line interface

Table 1. Buttons, ports, and connectors on ZoneDirector 1100

Label	Description
Reset	Use the Reset button to restart ZoneDirector or to reset it to factory default settings. • To restart ZoneDirector, press the Reset button once for less than two seconds. • To reset ZoneDirector to factory default settings, press and hold the Reset button for at least five (5) seconds. For more information, refer to "Alternate Factory Default Reset Method" on page 261. *WARNING: Resetting ZoneDirector to factory default settings will erase all configuration changes that you made.*

Front Panel LEDs

Table 2 describes the LEDs on the front panel of ZoneDirector 1100.

Table 2. ZoneDirector 1100 front panel LEDs

LED Label	State	Meaning
Power (embedded on the Power button)	Solid Green	ZoneDirector is receiving power.
	Off	ZoneDirector is NOT receiving power. If the power cable or adapter is connected to a power source, verify that the power cable is connected properly to the power jack on the rear panel of ZoneDirector.
Status	Solid Green	Normal state.
	Flashing Green	ZoneDirector has not yet been configured. Log into the Web interface, and then configure ZoneDirector using the setup wizard.
	Red	ZoneDirector has shut down (but is still connected to a power source).
	Flashing Red	ZoneDirector is starting up or shutting down.

Table 2. ZoneDirector 1100 front panel LEDs

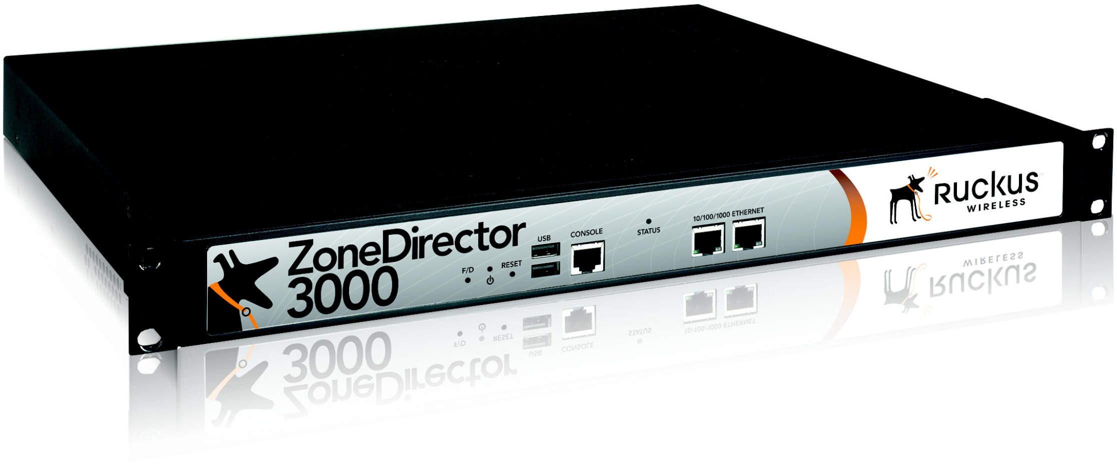
LED Label	State	Meaning
Ethernet Link	Solid Green or Amber	The port is connected to a device.
	Flashing Green or Amber	The port is transmitting or receiving traffic.
	Off	The port has no network cable connected or is not receiving a link signal.
Ethernet Rate	Green	The port is connected to a 1000Mbps device.
	Amber	The port is connected to a 100Mbps or 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. Buttons, ports, and connectors on ZoneDirector 3000

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 "Alternate Factory Default Reset Method" on page 261. *WARNING: Resetting ZoneDirector to factory default settings will erase all configuration changes that you have made.*
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 Table 4.

Front Panel LEDs

Table 4 describes the LEDs on the front panel of ZoneDirector 3000.

Table 4. ZoneDirector 3000 front panel LEDs

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.

Table 4. ZoneDirector 3000 front panel LEDs

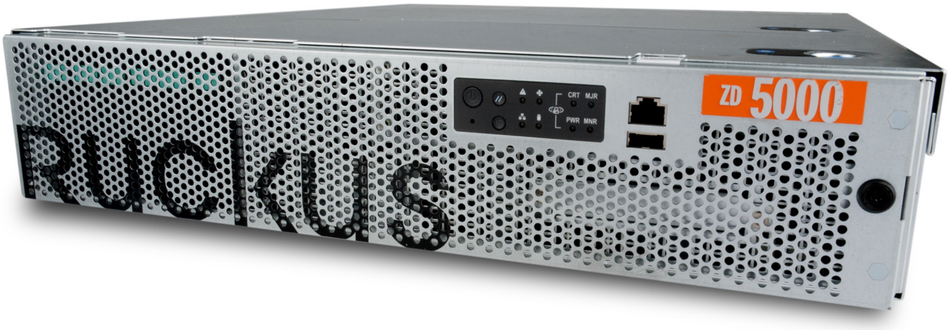
LED Label	State	Meaning
Status	Solid Green	Normal state.
	Flashing Green	ZoneDirector has not yet been configured. Log into the Web interface, and then configure ZoneDirector using the setup wizard.
	Solid Red	ZoneDirector has shut down (but is still connected to a power source).
	Flashing Red	ZoneDirector is starting up or shutting down.
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 10Mbps or 100Mbps 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 Control Panel 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)

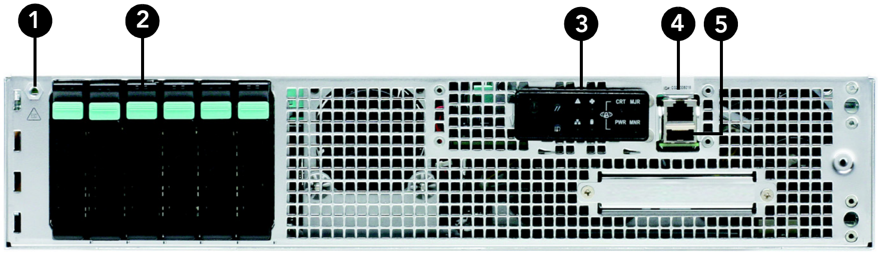


Table 6. ZoneDirector 5000 front panel (bezel removed)

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

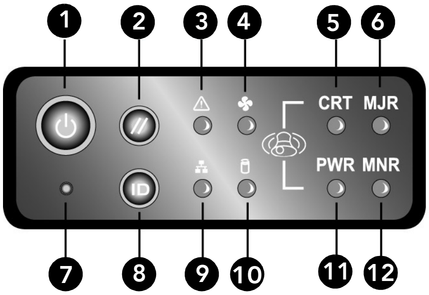


Table 7. ZoneDirector 5000 control panel

Number	Feature
1	Power button
2	System reset button
3	System status LED
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	Minor alarm (Amber: system unavailable; OFF: system available)

Rear Panel Features

Figure 6. ZoneDirector 5000 rear panel features

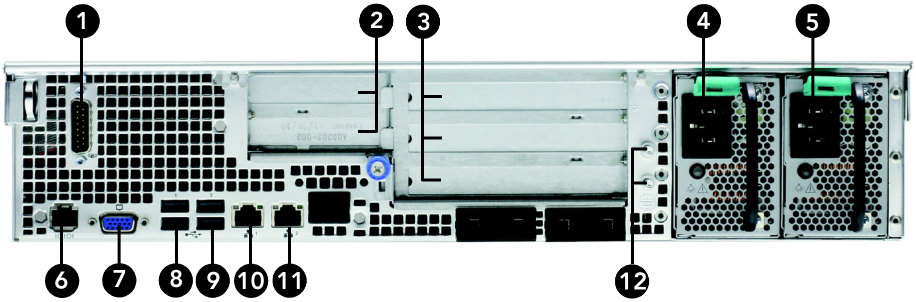


Table 8. Rear panel features

Number	Feature
1	Alarms cable connector (not used)
2	Two low-profile PCIe add-in cards (not used)

Number	Feature
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 9.   NIC status LEDs

LED Color	LED State	NIC State
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 (see "Option 2: Customize Your DHCP Server" on page 14), 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

If the AP and ZoneDirector Are on the Same Subnet

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

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

If you are deploying the AP and ZoneDirector on different subnets, let the AP perform auto discovery on the same subnet as ZoneDirector before moving the AP to another subnet. To do this, connect the AP to the same network as ZoneDirector. When the AP starts up, it will discover and attempt to register with ZoneDirector. Approve the registration request if auto approval is disabled.

After the AP registers with ZoneDirector successfully, transfer it to its intended subnet. It will be able to find and communicate with ZoneDirector once you reconnect it to the other subnet.

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

Option 2: Customize Your DHCP Server

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

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

For 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 Web site, 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.

Table 10. URL, IP address and Sub-option values that are used as examples in this procedure

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

Most commonly used DHCP servers such as Microsoft DHCP and ISC DHCP 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.

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

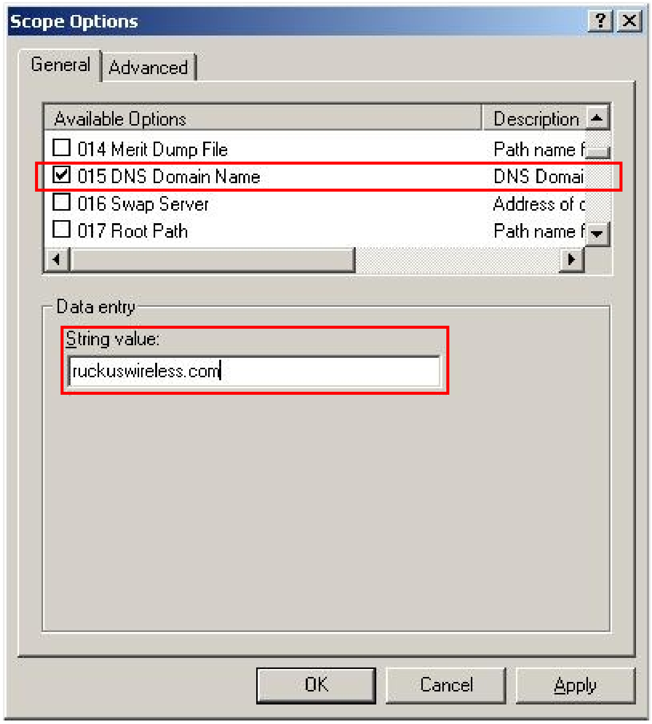
- Step 1: Set the DNS Domain Name on the DHCP Server
- Step 2: Set the DNS Server IP Address on the DHCP Server
- Step 3: Register the ZoneDirector IP Addresses with a DNS Server

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



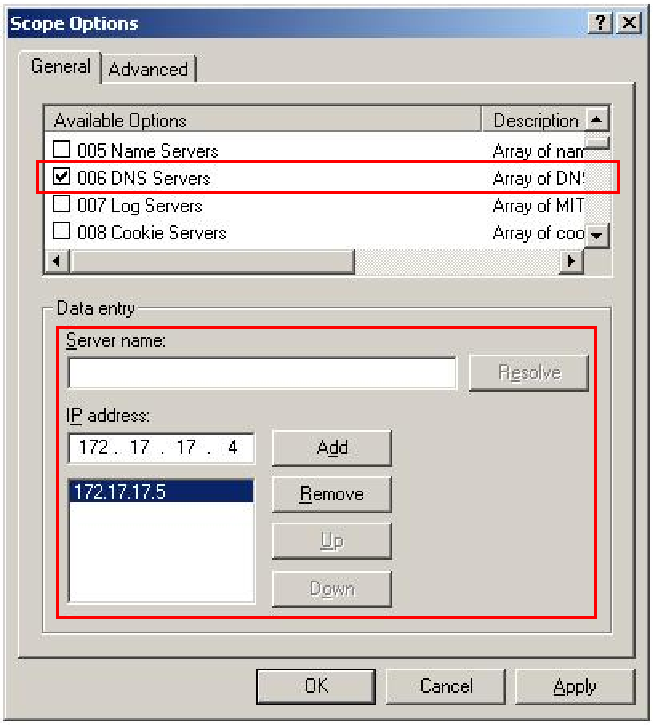
Available Options	Description
□ 014 Merit Dump File	Path name f
☑ 015 DNS Domain Name	DNS Domai
□ 016 Swap Server	Address of c
□ 017 Root Path	Path name f

String value: ruckuswireless.com

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



Available Options	Description
☐ 005 Name Servers	Array of nan
☑ 006 DNS Servers	Array of DN!
☐ 007 Log Servers	Array of MIT
☐ 008 Cookie Servers	Array of coo

Data entry

Server name:

IP address: 172 . 17 . 17 . 4

172.17.17.5

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: When 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 firewall 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

Communication	Ports
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)
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)

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 will not work (NAT equipment limits mapping each port to a single ZoneDirector IP address).

- 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, 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 9. Discover ZoneDirector using UPnP

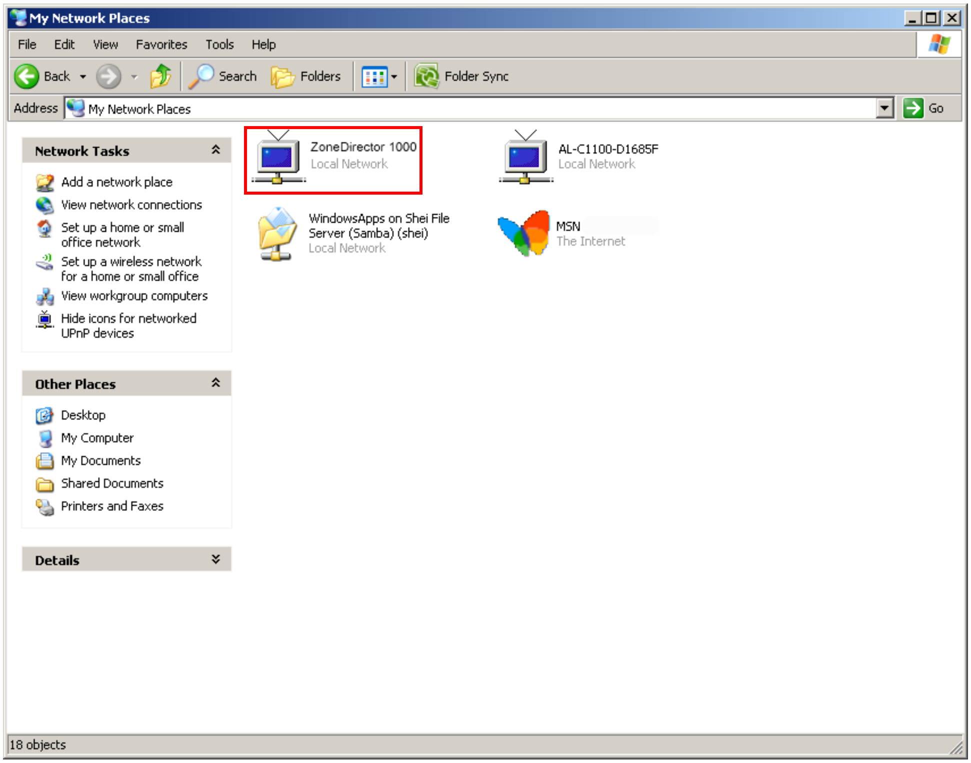
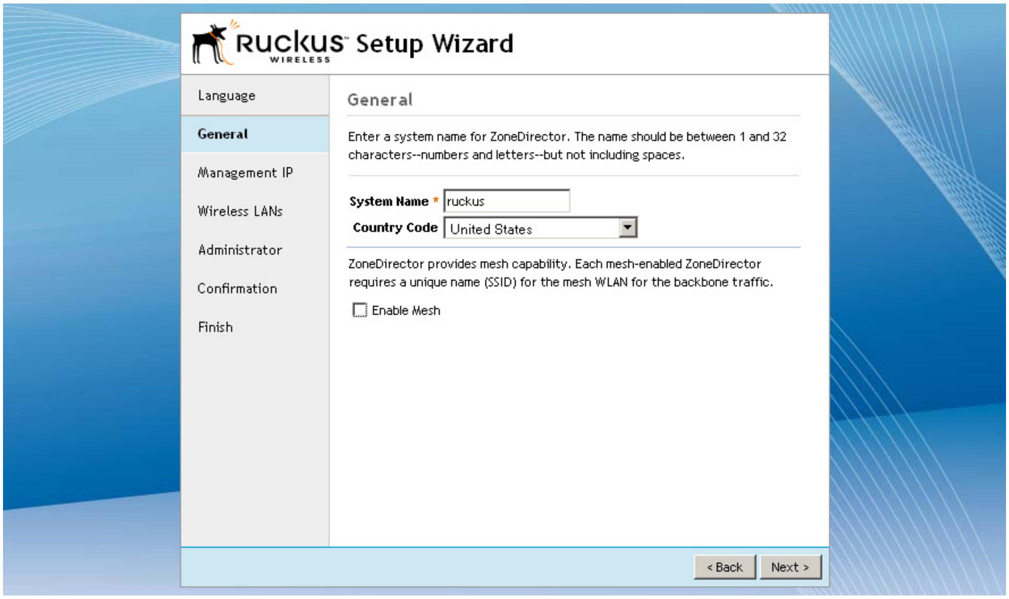


Figure 10. ZoneDirector Setup Wizard



General

Enter a system name for ZoneDirector. The name should be between 1 and 32 characters--numbers and letters--but not including spaces.

System Name * ruckus
Country Code United States

ZoneDirector provides mesh capability. Each mesh-enabled ZoneDirector requires a unique name (SSID) for the mesh WLAN for the backbone traffic.

□ Enable Mesh

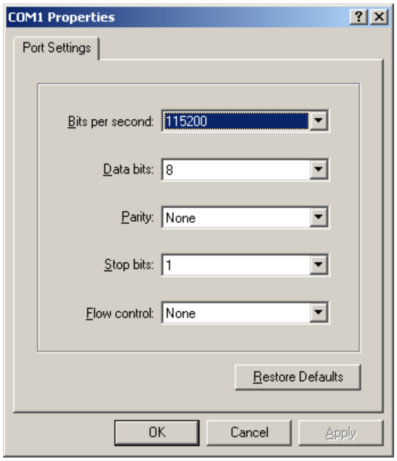
Accessing ZoneDirector's Command Line Interface

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 11. Configure a terminal client



COM1 Properties

Port Settings

Bits per second: 115200

Data bits: 8

Parity: None

Stop bits: 1

Flow control: None

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).

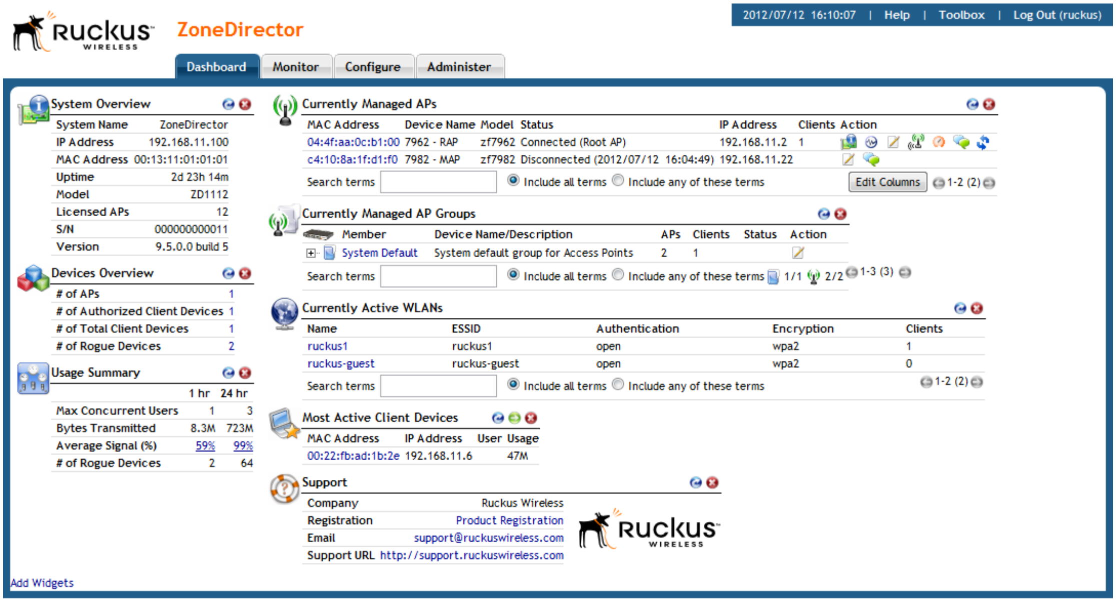
Table 12. Components of the ZoneDirector Web interface

Dashboard	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. 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.
Widgets	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.
Tabs	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.
Buttons	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.
Workspace	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.
Toolbox	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.
Help and Log Out	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.

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 12. The Dashboard



System Overview

System Name	ZoneDirector
IP Address	192.168.11.100
MAC Address	00:13:11:01:01:01
Uptime	2d 23h 14m
Model	ZD1112
Licensed APs	12
S/N	000000000011
Version	9.5.0.0 build 5

Devices Overview

# of APs	1
# of Authorized Client Devices	1
# of Total Client Devices	1
# of Rogue Devices	2

Usage Summary

	1 hr	24 hr
Max Concurrent Users	1	3
Bytes Transmitted	8.3M	723M
Average Signal (%)	59%	99%
# of Rogue Devices	2	64

Currently Managed APs

MAC Address	Device Name	Model	Status	IP Address	Clients	Action
04:4f:aa:0c:b1:00	7962 - RAP	zf7962	Connected (Root AP)	192.168.11.2	1	
c4:10:8a:1f:d1:f0	7982 - MAP	zf7982	Disconnected (2012/07/12 16:04:49)	192.168.11.22		

Search terms ● Include all terms ○ Include any of these terms 1-2 (2)

Currently Managed AP Groups

Member	Device Name/Description	APs	Clients	Status	Action
System Default	System default group for Access Points	2	1		

Search terms ● Include all terms ○ Include any of these terms 1/1 2/2 1-3 (3)

Currently Active WLANs

Name	ESSID	Authentication	Encryption	Clients
ruckus1	ruckus1	open	wpa2	1
ruckus-guest	ruckus-guest	open	wpa2	0

Search terms ● Include all terms ○ Include any of these terms 1-2 (2)

Most Active Client Devices

MAC Address	IP Address	User	Usage
00:22:fb:ad:1b:2e	192.168.11.6		47M

Support

Company	Ruckus Wireless
Registration	Product Registration
Email	support@ruckuswireless.com
Support URL	http://support.ruckuswireless.com

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" on page 26.

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:

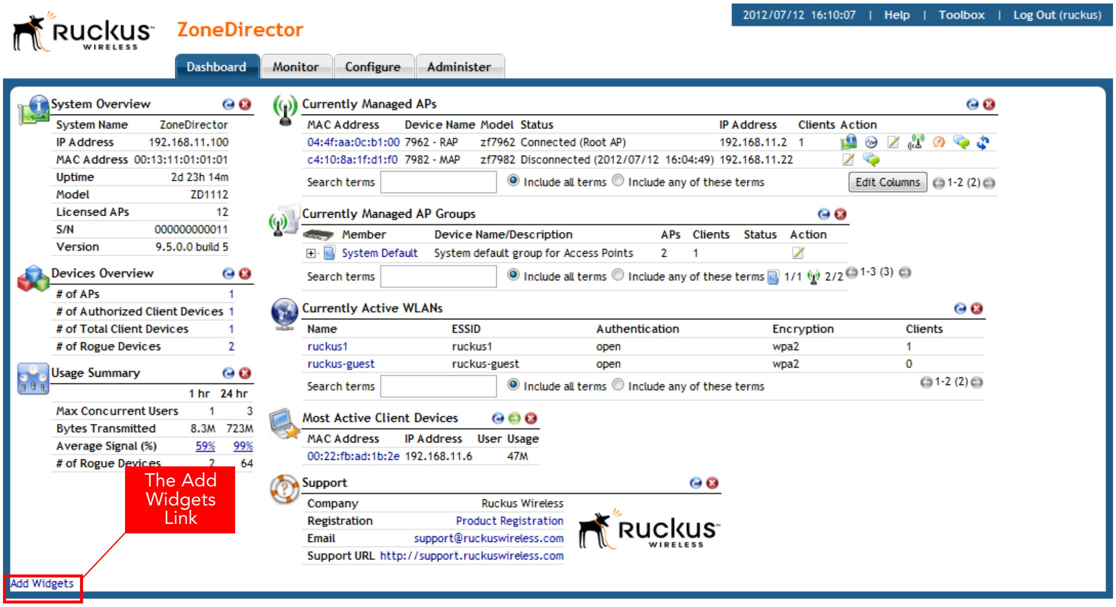
- *System Overview*: Shows ZoneDirector system information including its IP address, MAC address, model number, maximum number of licensed APs, serial number, software version number, and others.
- *Devices Overview*: Shows the number of APs being managed by ZoneDirector, the number of authorized clients, 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 ZoneDirector 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.
- *Most Active Client Devices*: Shows the top five clients in terms of usage, their IP addresses and MAC addresses, and the user name.
- *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.

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



System Overview

System Name	ZoneDirector
IP Address	192.168.11.100
MAC Address	00:13:11:01:01:01
Uptime	2d 23h 14m
Model	ZD1112
Licensed APs	12
S/N	000000000011
Version	9.5.0.0 build 5

Devices Overview

# of APs	1
# of Authorized Client Devices	1
# of Total Client Devices	1
# of Rogue Devices	2

Usage Summary

	1 hr	24 hr
Max Concurrent Users	1	3
Bytes Transmitted	8.3M	723M
Average Signal (%)	59%	99%
# of Rogue Devices	2	64

Currently Managed APs

MAC Address	Device Name	Model	Status	IP Address	Clients	Action
04:4f:aa:0c:b1:00	7962 - RAP	zf7962	Connected (Root AP)	192.168.11.2	1	
c4:10:8a:1f:d1:f0	7982 - MAP	zf7982	Disconnected (2012/07/12 16:04:49)	192.168.11.22		

Search terms ● Include all terms ○ Include any of these terms 1-2 (2)

Currently Managed AP Groups

Member	Device Name/Description	APs	Clients	Status	Action
System Default	System default group for Access Points	2	1		

Search terms ● Include all terms ○ Include any of these terms 1/1 2/2 1-3 (3)

Currently Active WLANs

Name	ESSID	Authentication	Encryption	Clients
ruckus1	ruckus1	open	wpa2	1
ruckus-guest	ruckus-guest	open	wpa2	0

Search terms ● Include all terms ○ Include any of these terms 1-2 (2)

Most Active Client Devices

MAC Address	IP Address	User	Usage
00:22:fb:ad:1b:2e	192.168.11.6		47M

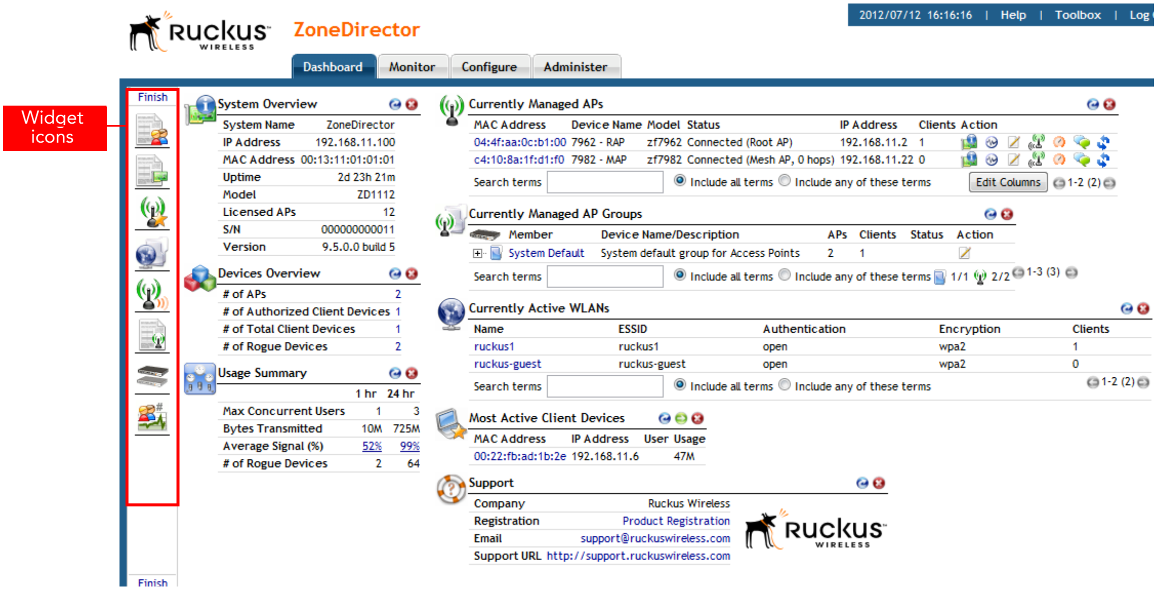
Support

Company	Ruckus Wireless
Registration	Product Registration
Email	support@ruckuswireless.com
Support URL	http://support.ruckuswireless.com

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



System Overview

System Name	ZoneDirector
IP Address	192.168.11.100
MAC Address	00:13:11:01:01:01
Uptime	2d 23h 21m
Model	ZD1112
Licensed APs	12
S/N	000000000011
Version	9.5.0.0 build 5

Devices Overview

# of APs	2
# of Authorized Client Devices	1
# of Total Client Devices	1
# of Rogue Devices	2

Usage Summary

	1 hr	24 hr
Max Concurrent Users	1	3
Bytes Transmitted	10M	725M
Average Signal (%)	52%	99%
# of Rogue Devices	2	64

Currently Managed APs

MAC Address	Device Name	Model	Status	IP Address	Clients	Action
04:4f:aa:0c:b1:00	7962 - RAP	zf7962	Connected (Root AP)	192.168.11.2	1	
c4:10:8a:1f:d1:f0	7982 - MAP	zf7982	Connected (Mesh AP, 0 hops)	192.168.11.22	0	

Search terms ● Include all terms ○ Include any of these terms Edit Columns 1-2 (2)

Currently Managed AP Groups

Member	Device Name/Description	APs	Clients	Status	Action
System Default	System default group for Access Points	2	1		

Search terms ● Include all terms ○ Include any of these terms 1/1 2/2 1-3 (3)

Currently Active WLANs

Name	ESSID	Authentication	Encryption	Clients
ruckus1	ruckus1	open	wpa2	1
ruckus-guest	ruckus-guest	open	wpa2	0

Search terms ● Include all terms ○ Include any of these terms 1-2 (2)

Most Active Client Devices

MAC Address	IP Address	User	Usage
00:22:fb:ad:1b:2e	192.168.11.6		47M

Support

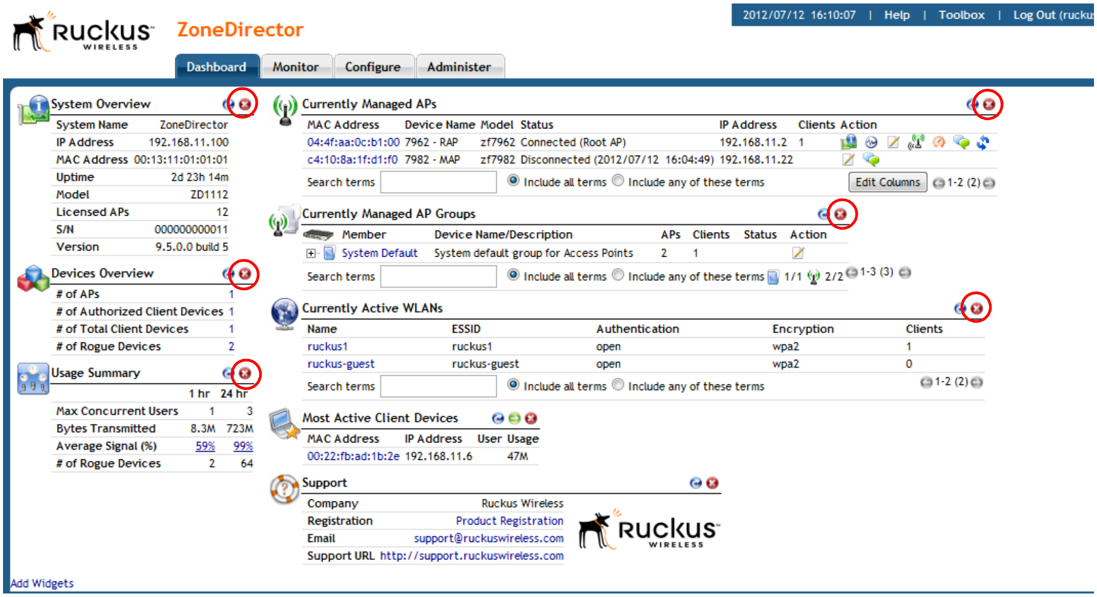
Company	Ruckus Wireless
Registration	Product Registration
Email	support@ruckuswireless.com
Support URL	http://support.ruckuswireless.com

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



System Overview

System Name	ZoneDirector
IP Address	192.168.11.100
MAC Address	00:13:11:01:01:01
Uptime	2d 23h 14m
Model	ZD1112
Licensed APs	12
S/N	000000000011
Version	9.5.0.0 build 5

Devices Overview

# of APs	1
# of Authorized Client Devices	1
# of Total Client Devices	1
# of Rogue Devices	2

Usage Summary

	1 hr	24 hr
Max Concurrent Users	1	3
Bytes Transmitted	8.3M	723M
Average Signal (%)	59%	99%
# of Rogue Devices	2	64

Currently Managed APs

MAC Address	Device Name	Model	Status	IP Address	Clients	Action
04:4f:aa:0c:b1:00	7962 - RAP	zf7962	Connected (Root AP)	192.168.11.2	1	
c4:10:8a:1f:d1:f0	7982 - MAP	zf7982	Disconnected (2012/07/12 16:04:49)	192.168.11.22		

Search terms ● Include all terms ○ Include any of these terms Edit Columns 1-2 (2)

Currently Managed AP Groups

Member	Device Name/Description	APs	Clients	Status	Action
System Default	System default group for Access Points	2	1		

Search terms ● Include all terms ○ Include any of these terms 1/1 2/2 1-3 (3)

Currently Active WLANs

Name	ESSID	Authentication	Encryption	Clients
ruckus1	ruckus1	open	wpa2	1
ruckus-guest	ruckus-guest	open	wpa2	0

Search terms ● Include all terms ○ Include any of these terms 1-2 (2)

Most Active Client Devices

MAC Address	IP Address	User	Usage
00:22:fb:ad:1b:2e	192.168.11.6		47M

Support

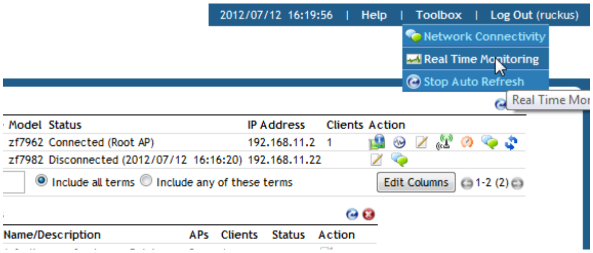
Company	Ruckus Wireless
Registration	Product Registration
Email	support@ruckuswireless.com
Support URL	http://support.ruckuswireless.com

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 16. Select Real Time Monitoring from the Toolbox



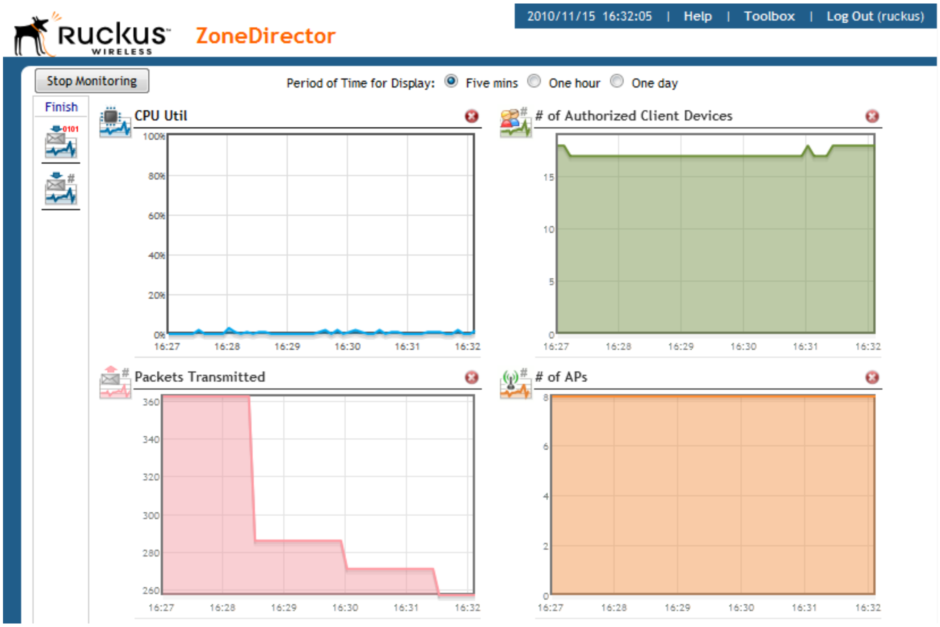
Model	Status	IP Address	Clients	Action
zf7962	Connected (Root AP)	192.168.11.2	1	
zf7982	Disconnected (2012/07/12 16:16:20)	192.168.11.22		

● Include all terms ○ Include any of these terms Edit Columns 1-2 (2)

Name/Description APs Clients Status Action

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

Figure 17. The Real Time Monitoring screen



2010/11/15 16:32:05 | Help | Toolbox | Log Out (ruckus)

Stop Monitoring

Period of Time for Display: ● Five mins ○ One hour ○ One day

Select a time increment to monitor statistics by (5 minutes, 1 hour or 1 day) and click **Start Monitoring** to begin. Note that because the Real Time Monitoring process itself consumes a small amount of system resources, it should be used as a general overview tool rather than a precise measurement. Actual resources used (CPU and memory utilization) will be lower when Real Time Monitoring is not running.

Real Time Monitoring Widgets

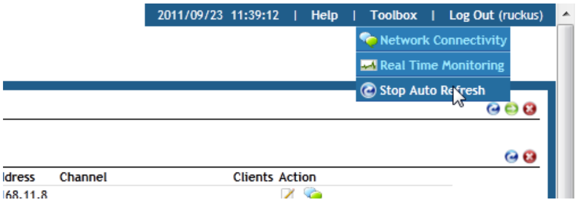
- *CPU Util*: Displays the % utilization of ZoneDirector's CPU.
- *Memory Util*: Displays the % utilization of ZoneDirector's memory.
- *# of AP's*: Displays the number of APs being managed by ZoneDirector.
- *# of Client Devices*: Displays the number of client devices associated to APs being managed 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 ZoneDirector.
- *Packets Transmitted*: Total packets transmitted by all APs being managed by ZoneDirector.

NOTE: Real Time Monitoring should be closed when not in use, as it can impact ZoneDirector performance.

Stopping and Starting Auto Refresh

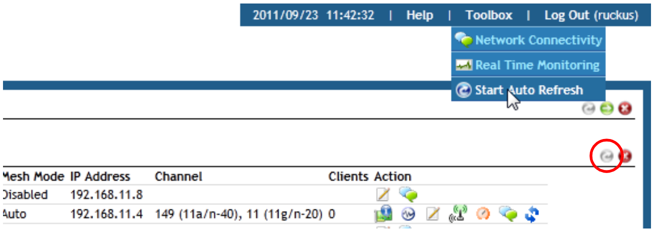
By default, ZoneDirector Web interface pages automatically refresh themselves periodically depending on activity. You can pause auto-refresh on any page in the Web interface from the Toolbox. After clicking **Stop Auto Refresh**, ZoneDirector pauses automatic updating of all widgets on the current page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

Figure 18. Stopping and starting automatic page refreshing



ldress	Channel	Clients	Action
168.11.8			

Figure 19. The Refresh icon on all widgets is disabled when auto refresh is stopped



Mesh Mode	IP Address	Channel	Clients	Action
Disabled	192.168.11.8			
Auto	192.168.11.4	149 (11a/n-40), 11 (11g/n-20)	0	

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.

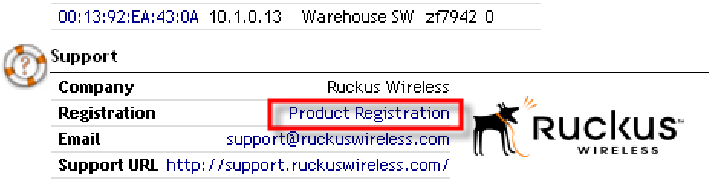
NOTE: To ensure that all registration information for all of your APs is included, be sure to register *after* all APs have been installed. If you register ZoneDirector before installing the APs, the registration will not include AP information.

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 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).
5. Email the CSV file (which includes the serial numbers and MAC addresses of your ZoneDirector and all known APs, and your contact information) to register@ruckuswireless.com.

Figure 20. Support Widget on the Dashboard

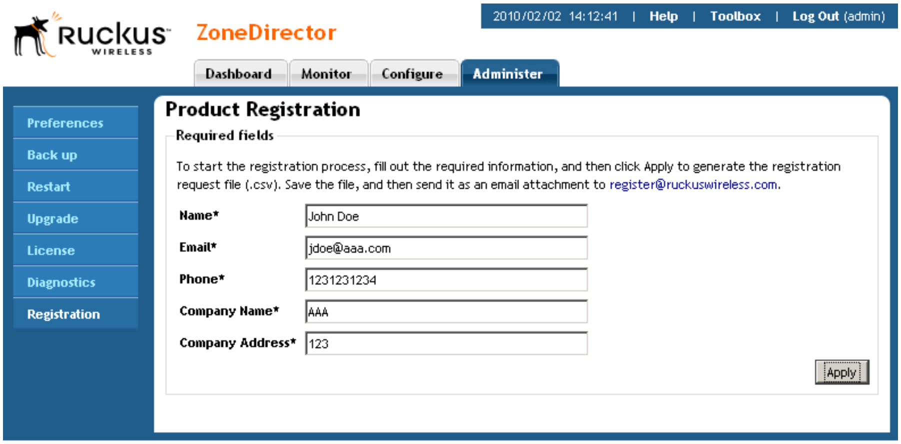


00:13:92:EA:43:0A 10.1.0.13 Warehouse SW zf7942 0

Support

Company	Ruckus Wireless
Registration	Product Registration
Email	support@ruckuswireless.com
Support URL	http://support.ruckuswireless.com/

Figure 21. The Product Registration page



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 send it as an email attachment to register@ruckuswireless.com.

Name*	John Doe
Email*	jdoe@aaa.com
Phone*	1231231234
Company Name*	AAA
Company Address*	123

Your ZoneDirector is now registered with Ruckus Wireless.

2

Configuring System Settings

In This Chapter

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.

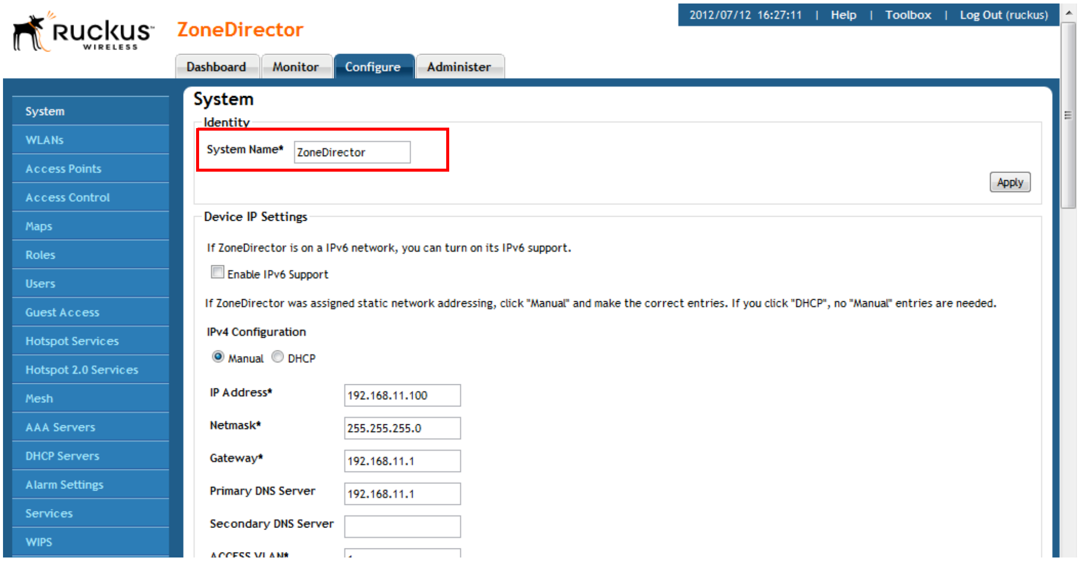
Changing the System Name

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 6 and 32 characters in length, using letters, numbers, underscores (_) and hyphens (-). Do not use spaces or other special characters. The first character must be a letter. System names are case sensitive.
3. Click **Apply** to save your settings. The change goes into effect immediately.

Figure 22. The Identity section on the Configure > System page



System

Identity

System Name* ZoneDirector

Device IP Settings

If ZoneDirector is on a IPv6 network, you can turn on its IPv6 support.

□ Enable IPv6 Support

If ZoneDirector was assigned static network addressing, click "Manual" and make the correct entries. If you click "DHCP", no "Manual" entries are needed.

IPv4 Configuration

● Manual ○ DHCP

IP Address* 192.168.11.100
Netmask* 255.255.255.0
Gateway* 192.168.11.1
Primary DNS Server 192.168.11.1
Secondary DNS Server
ACCESS VLAN* 1

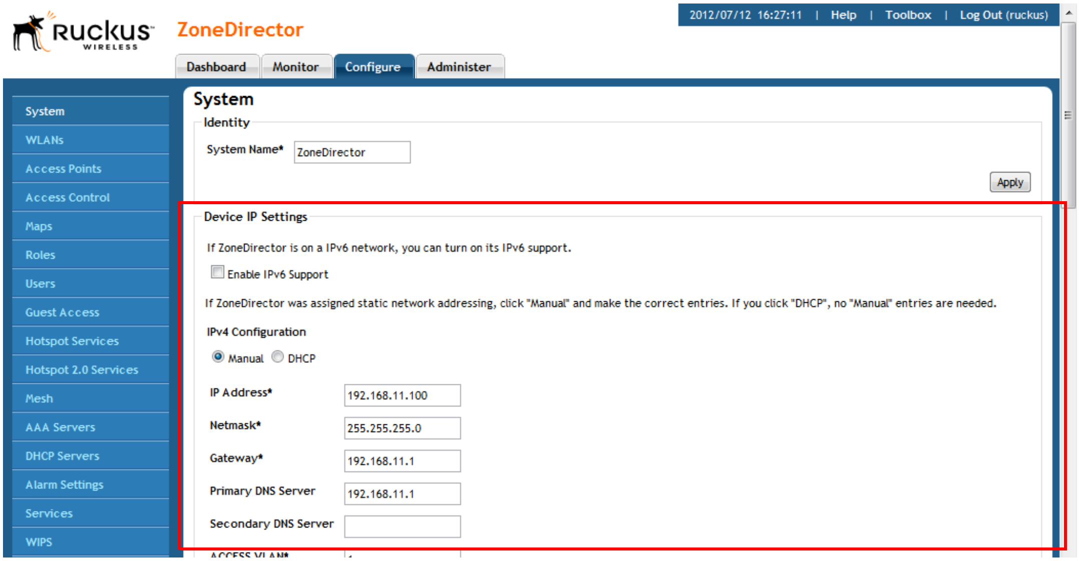
Changing the Network Addressing

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 23. The Device IP options



System

Identity

System Name* ZoneDirector

Device IP Settings

If ZoneDirector is on a IPv6 network, you can turn on its IPv6 support.

□ Enable IPv6 Support

If ZoneDirector was assigned static network addressing, click "Manual" and make the correct entries. If you click "DHCP", no "Manual" entries are needed.

IPv4 Configuration

● Manual ○ DHCP

IP Address* 192.168.11.100

Netmask* 255.255.255.0

Gateway* 192.168.11.1

Primary DNS Server 192.168.11.1

Secondary DNS Server

ACCESS VLAN*

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 13. Default static IPv4 and IPv6 addresses

	AP default IP address	ZoneDirector default IP address
IPv4	192.168.0.1	192.168.0.2
IPv6	fc00::1	fc00::2

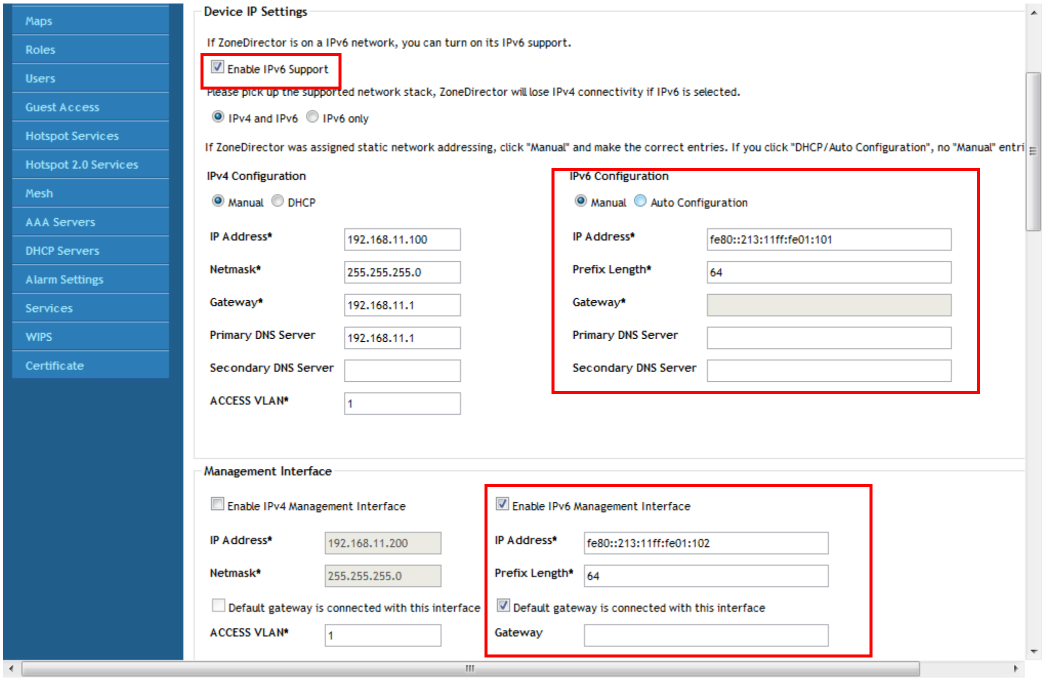
DNS Address can be configured manually or obtained automatically by the DHCPv6 client.

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

When IPv6 is enabled, the other fields where IP addresses are entered (such as Additional Management Interface) automatically change to allow entry of IPv6 format addresses, as shown in Figure 24.

Note that some features are not supported when in IPv6 mode. Specifically, internal DHCP server, LAN rogue AP detection, DHCPv6 vendor specific options, Aeroscout RFID tag detection, SSL certificate generation, UPnP, remote access to ZD, and L2TP and WISPr in standalone APs are not supported when in IPv6 mode.

Figure 24. Enabling IPv6 automatically changes other fields to allow IPv6 addresses



Device IP Settings

If ZoneDirector is on a IPv6 network, you can turn on its IPv6 support.

☑ Enable IPv6 Support

Please pick up the supported network stack, ZoneDirector will lose IPv4 connectivity if IPv6 is selected.

● IPv4 and IPv6 ○ IPv6 only

If ZoneDirector was assigned static network addressing, click "Manual" and make the correct entries. If you click "DHCP/Auto Configuration", no "Manual" entri

IPv4 Configuration		IPv6 Configuration	
● Manual ○ DHCP		● Manual ○ Auto Configuration	
IP Address*	192.168.11.100	IP Address*	fe80::213:11ff:fe01:101
Netmask*	255.255.255.0	Prefix Length*	64
Gateway*	192.168.11.1	Gateway*	
Primary DNS Server	192.168.11.1	Primary DNS Server	
Secondary DNS Server		Secondary DNS Server	
ACCESS VLAN*	1		

Management Interface

☐ Enable IPv4 Management Interface		☑ Enable IPv6 Management Interface	
IP Address*	192.168.11.200	IP Address*	fe80::213:11ff:fe01:102
Netmask*	255.255.255.0	Prefix Length*	64
☐ Default gateway is connected with this interface		☑ Default gateway is connected with this interface	
ACCESS VLAN*	1	Gateway	

Enabling an Additional Management Interface

The additional management interface is created for receiving or transmitting management traffic only. The management IP address can be configured to allow an administrator to access ZoneDirector remotely from a different subnet and VLAN from the AP network. This interface is only used for accessing the management interface of ZoneDirector; APs still use the main IP interface.

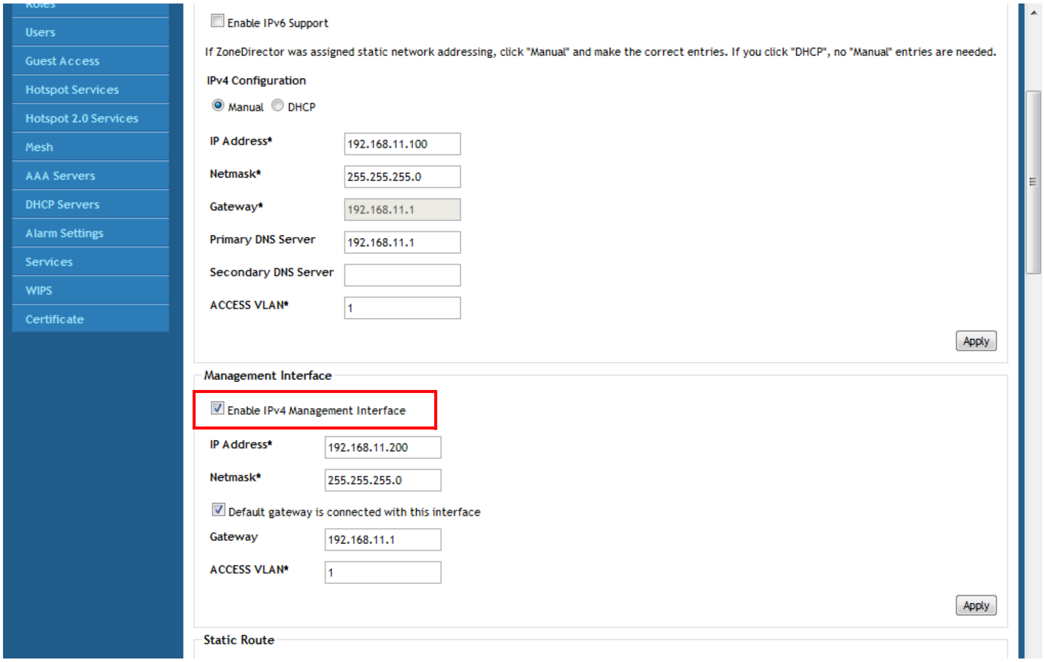
It can also be used for Smart Redundancy -- when redundant ZoneDirectors are deployed, you can create a separate management interface to be shared by both devices. Then, you only have to remember one IP address that you can log into regardless of which ZoneDirector is the active unit. This shared management IP address must be configured identically on both ZoneDirectors (see "Configuring ZoneDirector for Smart Redundancy" on page 40).

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. If ZoneDirector needs to be accessible from a remote network, select **Default gateway is connected with this interface**, and enter the Gateway IP address in the field provided. Enabling this setting is only necessary if you need to access ZoneDirector from a remote network and there are two or more gateways in the network; to ensure that management traffic is able to reach ZoneDirector successfully. Note that you may also need to create a static route for management traffic in this case. See "Creating Static Route Tables" for more information.
5. Click **Apply** to save your settings.
6. If the Management Interface is to be shared by two ZoneDirectors, repeat steps 1-5 for the other ZoneDirector.

Figure 25. Enabling an additional management interface



□ Enable IPv6 Support

If ZoneDirector was assigned static network addressing, click "Manual" and make the correct entries. If you click "DHCP", no "Manual" entries are needed.

IPv4 Configuration

● Manual ○ DHCP

IP Address* 192.168.11.100
Netmask* 255.255.255.0
Gateway* 192.168.11.1
Primary DNS Server 192.168.11.1
Secondary DNS Server
ACCESS VLAN* 1

Apply

Management Interface

☑ Enable IPv4 Management Interface

IP Address* 192.168.11.200
Netmask* 255.255.255.0

☑ Default gateway is connected with this interface

Gateway 192.168.11.1
ACCESS VLAN* 1

Apply

Static Route

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.

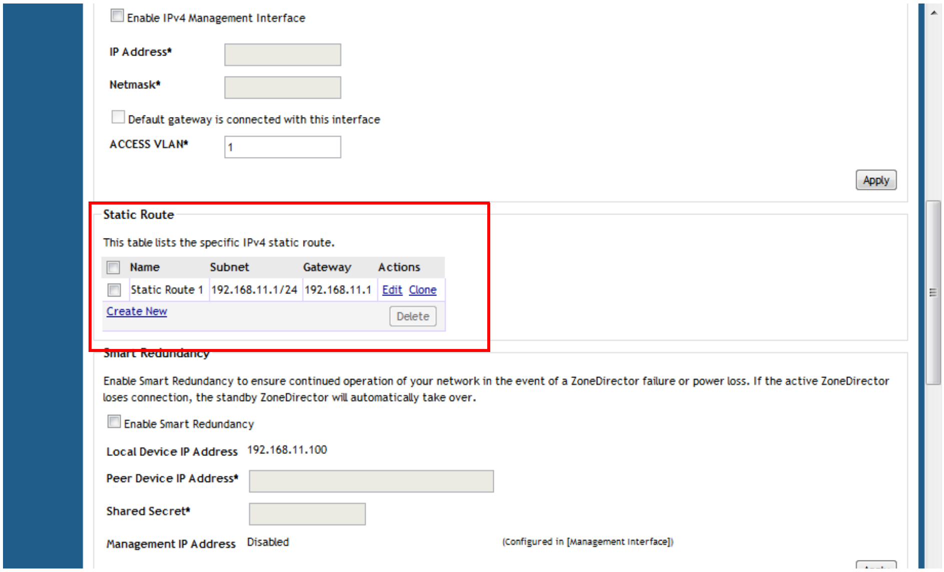
Creating Static Route Tables

Customizing static route tables may be necessary in cases where ZoneDirector needs to be managed from a remote network. By default, ZoneDirector management traffic is restricted to stations on the same VLAN and IP subnet as ZoneDirector to prevent unauthorized access. However, if you need to manage ZoneDirector from a remote network, you can create custom static routes to ensure management traffic will be able to reach ZoneDirector successfully.

To create a static route from ZoneDirector to an external IP address/range

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 through which you want to route management traffic (note: this default Gateway must also be configured under the *Management Interface* section).
6. Click **OK** to save your changes.

Figure 26. Creating static routes



□ Enable IPv4 Management Interface

IP Address*

Netmask*

□ 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
□	Static Route 1	192.168.11.1/24	192.168.11.1	Edit Clone

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 192.168.11.100

Peer Device IP Address*

Shared Secret*

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

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.

NOTE: This feature is only available using two ZoneDirectors of the same model and number of licensed APs. You can not enable Smart Redundancy using a ZoneDirector 3000 as the primary and a ZoneDirector 1100 as the backup unit, for example.

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

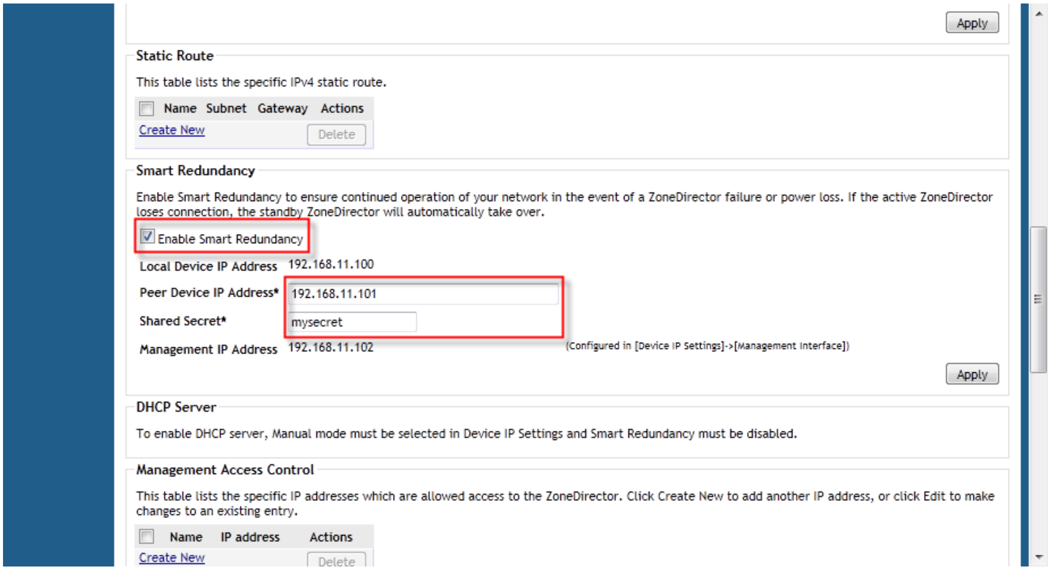
All configuration changes are made to the active ZoneDirector and synchronized to the standby unit. The user can access the Web interface from any of the three IP addresses, however not all configuration options are available from the standby device.

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 27. Enable Smart Redundancy



Static Route

This table lists the specific IPv4 static route.

□	Name	Subnet	Gateway	Actions

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 192.168.11.100

Peer Device IP Address* 192.168.11.101

Shared Secret* mysecret

Management IP Address 192.168.11.102 (Configured in [Device IP Settings]->[Management Interface])

DHCP Server

To enable DHCP server, Manual mode must be selected in Device IP Settings and Smart Redundancy must be disabled.

Management Access Control

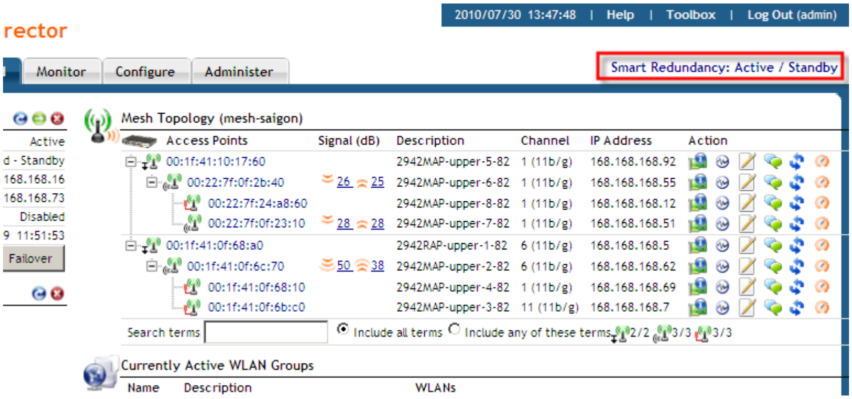
This table lists the specific IP addresses which are allowed access to the ZoneDirector. Click Create New to add another IP address, or click Edit to make changes to an existing entry.

□	Name	IP address	Actions

5. Enable the check box next to **Enable Smart Redundancy**.
6. Enter the IP address of the backup unit under **Peer IP Address** (if known). 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 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 28. Smart Redundancy status link



2010/07/30 13:47:48 | Help | Toolbox | Log Out (admin)
rector
Monitor
Configure
Administer
Smart Redundancy: Active / Standby
Active
d - Standby
168.168.16
168.168.73
Disabled
9 11:51:53
Failover
Mesh Topology (mesh-saigon)
Currently Active WLAN Groups

Access Points	Signal (dB)	Description	Channel	IP Address	Action
00:1f:41:10:17:60		2942MAP-upper-5-82	1 (11b/g)	168.168.168.92	
00:22:7f:0f:2b:40	26 25	2942MAP-upper-6-82	1 (11b/g)	168.168.168.55	
00:22:7f:24:a8:60		2942MAP-upper-8-82	1 (11b/g)	168.168.168.12	
00:22:7f:0f:23:10	28 28	2942MAP-upper-7-82	1 (11b/g)	168.168.168.51	
00:1f:41:0f:68:a0		2942RAP-upper-1-82	6 (11b/g)	168.168.168.5	
00:1f:41:0f:6c:70	50 38	2942MAP-upper-2-82	6 (11b/g)	168.168.168.62	
00:1f:41:0f:68:10		2942MAP-upper-4-82	1 (11b/g)	168.168.168.69	
00:1f:41:0f:6b:c0		2942MAP-upper-3-82	11 (11b/g)	168.168.168.7	

Search terms ● Include all terms ○ Include any of these terms 2/2 3/3 3/3

Name	Description	WLANs

NOTE: If you have two ZoneDirectors of the same model and license level, Ruckus Wireless recommends using the Smart Redundancy feature. If you have two ZoneDirectors of different models or different license levels, you can use Limited ZD Discovery to provide limited redundancy; however, this method does not provide synchronization of the user database.

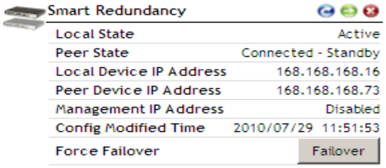
NOTE: If you disable Smart Redundancy after it has been enabled, both ZoneDirectors will revert to active state, which could result in unpredictable network topologies. Therefore, Ruckus Wireless recommends first factory resetting the standby ZoneDirector before disabling Smart Redundancy.

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 that 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" on page 14).

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 29. The Smart Redundancy widget



Smart Redundancy

Local State	Active
Peer State	Connected - Standby
Local Device IP Address	168.168.168.16
Peer Device IP Address	168.168.168.73
Management IP Address	Disabled
Config Modified Time	2010/07/29 11:51:53
Force Failover	Failover

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.

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 (if VLANs are assigned).

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

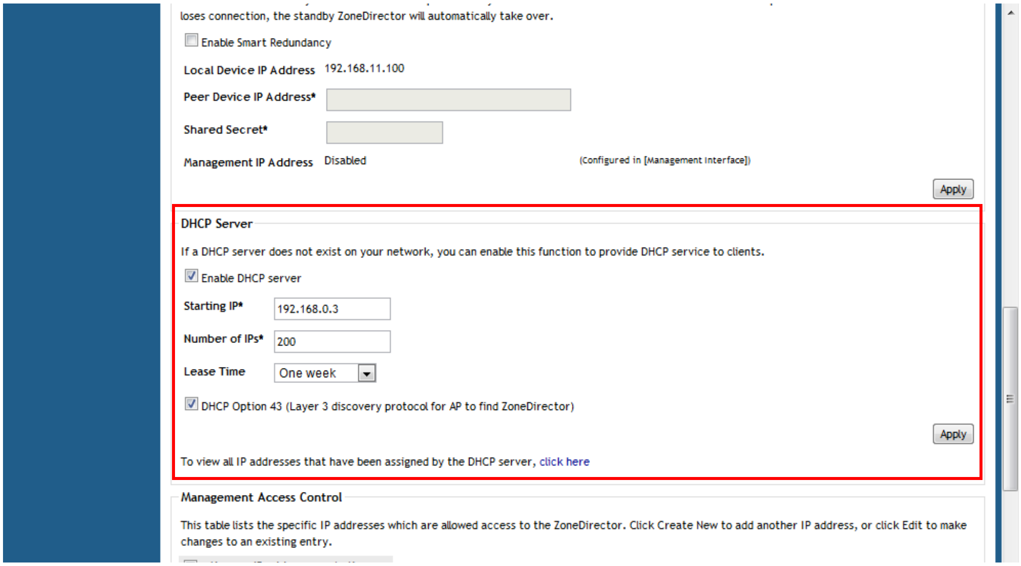
NOTE: Ruckus Wireless recommends that you only enable the built-in DHCP server if there are no other DHCP servers on the network. The DHCP server in ZoneDirector can support only a single subnet. If you enable the built-in DHCP server, Ruckus Wireless also recommends enabling the rogue DHCP server detector. For more information, refer to “Rogue DHCP Server Detection” on page 75.

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 30. The DHCP Server options



loses connection, the standby ZoneDirector will automatically take over.

□ Enable Smart Redundancy

Local Device IP Address 192.168.11.100

Peer Device IP Address*

Shared 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

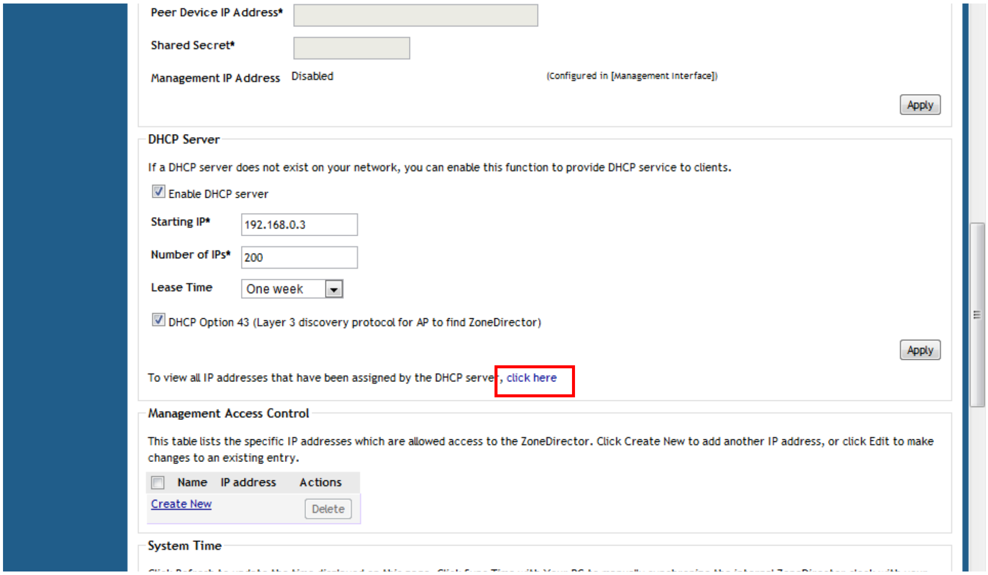
Management Access Control

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.

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.

Figure 31. To view current DHCP clients, click the "click here" link



Peer Device IP Address*

Shared 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

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.

□	Name	IP address	Actions
Create New			Delete

System Time

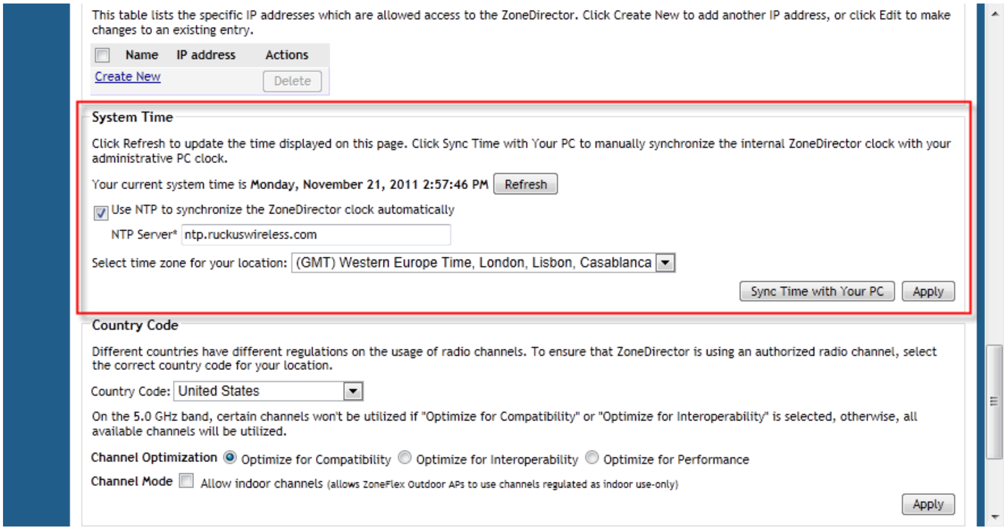
Setting the System Time

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 32. The System Time options



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.

☐	Name	IP address	Actions
Create New			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 **Monday, November 21, 2011 2:57:46 PM** Refresh

☑ Use NTP to synchronize the ZoneDirector clock automatically

NTP Server* ntp.ruckuswireless.com

Select time zone for your location: (GMT) Western Europe Time, London, Lisbon, Casablanca

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: United States

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

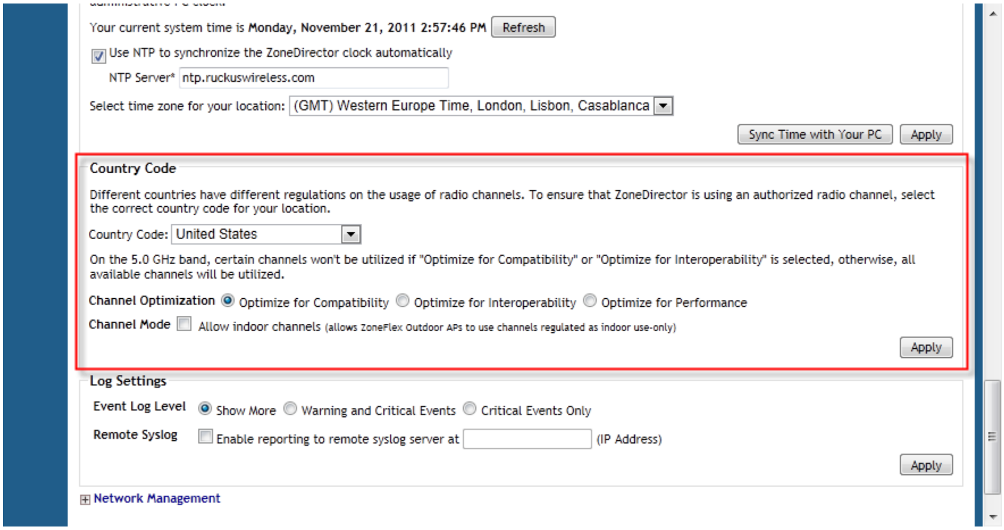
Setting the Country Code

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 33. The Country Code settings



Your current system time is **Monday, November 21, 2011 2:57:46 PM** Refresh

☑ Use NTP to synchronize the ZoneDirector clock automatically

NTP Server* ntp.ruckuswireless.com

Select time zone for your location: (GMT) Western Europe Time, London, Lisbon, Casablanca

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: United States

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)

Apply

⊞ Network Management

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.

Table 14. Channel Optimization settings for US Country Code

Setting	Description	Use this setting when
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.

Specifically, 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.

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 7762, 7761-CM and 7731) 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 channel allowed for outdoor use. 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.

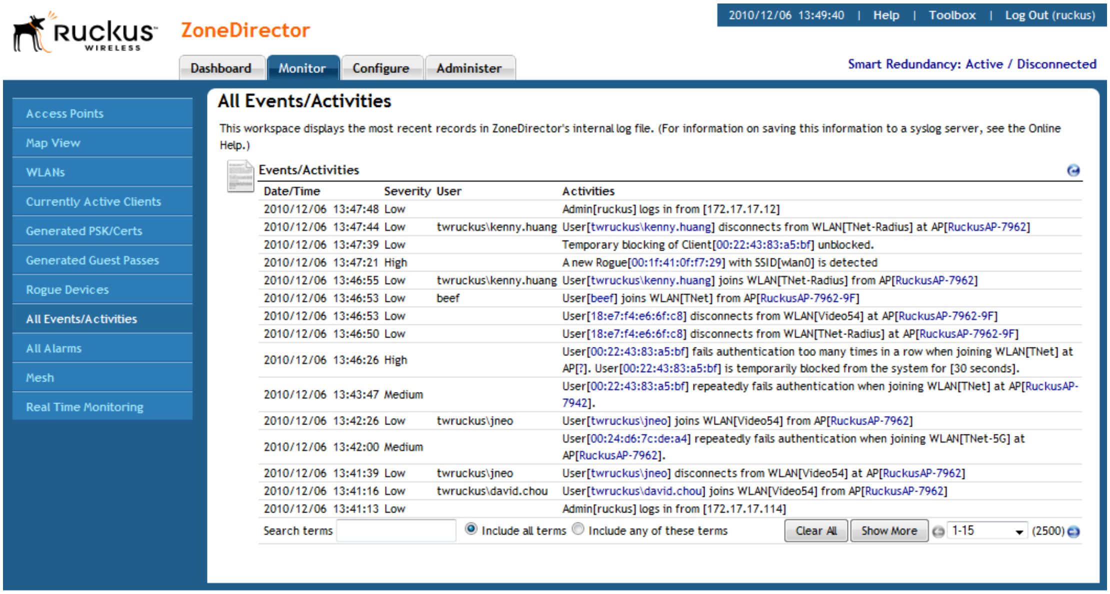
Reviewing the Current Log Contents

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 34. The All Events/Activities page



All Events/Activities

This workspace displays the most recent records in ZoneDirector's internal log file. (For information on saving this information to a syslog server, see the Online Help.)

Events/Activities

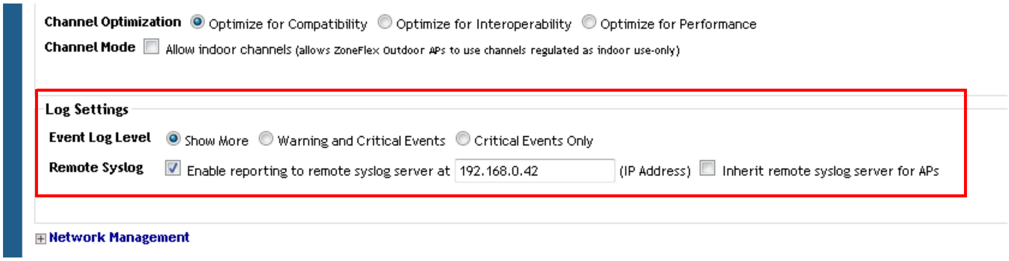
Date/Time	Severity	User	Activities
2010/12/06 13:47:48	Low		Admin[ruckus] logs in from [172.17.17.12]
2010/12/06 13:47:44	Low	twruckus\kenny.huang	User[twruckus\kenny.huang] disconnects from WLAN[TNet-Radius] at AP[RuckusAP-7962]
2010/12/06 13:47:39	Low		Temporary blocking of Client[00:22:43:83:a5:bf] unblocked.
2010/12/06 13:47:21	High		A new Rogue[00:1f:41:0f:f7:29] with SSID[wlan0] is detected
2010/12/06 13:46:55	Low	twruckus\kenny.huang	User[twruckus\kenny.huang] joins WLAN[TNet-Radius] from AP[RuckusAP-7962]
2010/12/06 13:46:53	Low	beef	User[beef] joins WLAN[TNet] from AP[RuckusAP-7962-9F]
2010/12/06 13:46:53	Low		User[18:e7:f4:e6:6f:c8] disconnects from WLAN[Video54] at AP[RuckusAP-7962-9F]
2010/12/06 13:46:50	Low		User[18:e7:f4:e6:6f:c8] disconnects from WLAN[TNet-Radius] at AP[RuckusAP-7962-9F]
2010/12/06 13:46:26	High		User[00:22:43:83:a5:bf] fails authentication too many times in a row when joining WLAN[TNet] at AP[?]. User[00:22:43:83:a5:bf] is temporarily blocked from the system for [30 seconds].
2010/12/06 13:43:47	Medium		User[00:22:43:83:a5:bf] repeatedly fails authentication when joining WLAN[TNet] at AP[RuckusAP-7942].
2010/12/06 13:42:26	Low	twruckus\jneo	User[twruckus\jneo] joins WLAN[Video54] from AP[RuckusAP-7962]
2010/12/06 13:42:00	Medium		User[00:24:d6:7c:de:a4] repeatedly fails authentication when joining WLAN[TNet-5G] at AP[RuckusAP-7962].
2010/12/06 13:41:39	Low	twruckus\jneo	User[twruckus\jneo] disconnects from WLAN[Video54] at AP[RuckusAP-7962]
2010/12/06 13:41:16	Low	twruckus\david.chou	User[twruckus\david.chou] joins WLAN[Video54] from AP[RuckusAP-7962]
2010/12/06 13:41:13	Low		Admin[ruckus] logs in from [172.17.17.114]

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.
     – Optional: If you want to disable AP syslog message delivery (receive ZD messages only), deselect the **Inherit remote syslog server for APs** check box.
4. Click **Apply** to save your settings. The changes go into effect immediately.

Figure 35. The Log Settings options



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 192.168.0.42 (IP Address) □ Inherit remote syslog server for APs

⊞ Network Management

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**. The *Email Notification* form appears.
2. To enable email notification, select the **Send an email message when an alarm is triggered** check box.
3. Configure the settings listed in Table 15.

Table 15. SMTP settings for email notification

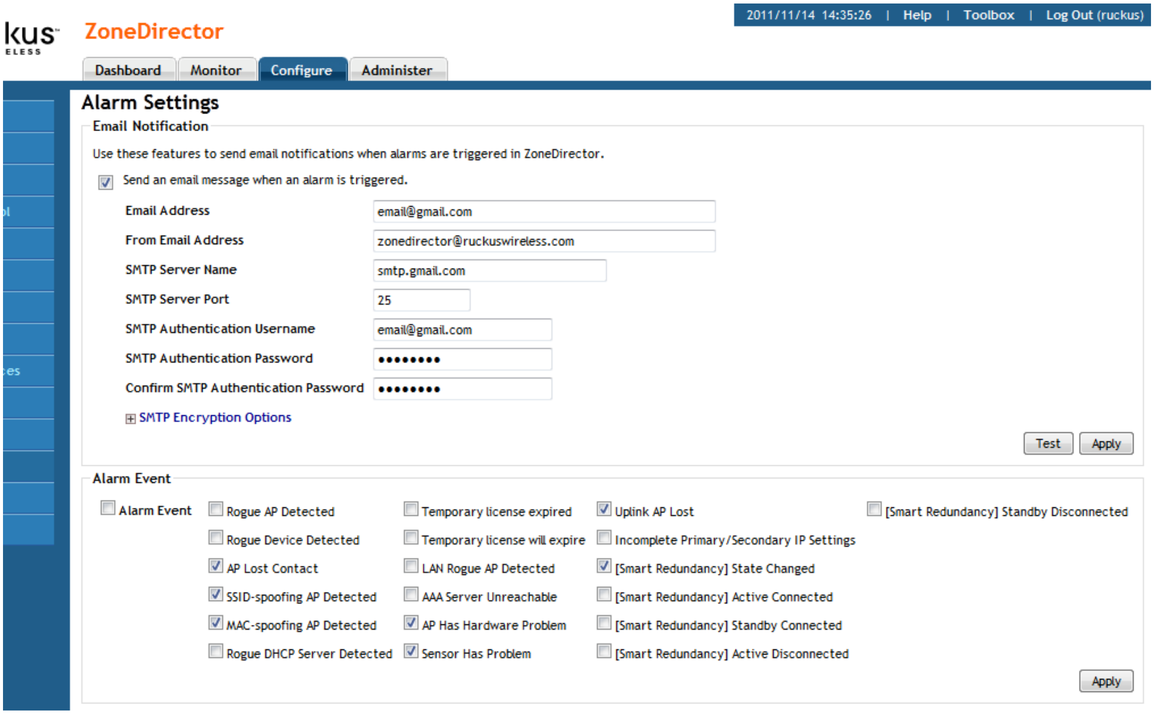
SMTP Setting	Description
Email address	Type the email address to which ZoneDirector will send alarm messages. You can send alarm messages to a single email address.
From email address	Type the email address from which ZoneDirector will send alarm messages.

Table 15. SMTP settings for email notification

SMTP Setting	Description
SMTP Server Name	Type the full name of the server provided by your ISP or mail administrator. Often, the SMTP server name is in the format **`smtp.company.com`**.. • For Hotmail addresses, the SMTP server name is *smtp.live.com*.
SMTP Server Port	Type the SMTP port number provided by your ISP or mail administrator. Often, the SMTP port number is **`25`** or **`587`**. The default SMTP port value is **`587`**.
SMTP Authentication Username	Type the user name provided by your ISP or mail administrator. This might be just the part of your email address before the @ symbol, or it might be your complete email address. If you are using a free email service (such as Hotmail or Gmail), you typically have to type your complete email address.
SMTP Authentication Password	Type the password that is associated with the user name above.
Confirm SMTP Authentication Password	Retype the password you typed above to confirm.
SMTP Encryption Options	If your mail server uses TLS encryption, click the **SMTP Encryption Options** link, and then select the **TLS** check box. Additionally, select the **STARTTLS** check box that appears after you select the **TLS** check box. Check with your ISP or mail administrator for the correct encryption settings that you need to set. • If using a Yahoo! email account, STARTTLS must be disabled. • If using a Hotmail account, both TLS and STARTTLS must be enabled.

4. 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 5.
   - 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 3., and then verify that the SMTP settings are correct.
5. Click **Apply**. The email notification settings you configured become active immediately.

Figure 36. The Alarm Settings page



Alarm Settings

Email Notification

Use these features to send email notifications when alarms are triggered in ZoneDirector.

☑ Send an email message when an alarm is triggered.

Email Address	email@gmail.com
From Email Address	zonedirector@ruckuswireless.com
SMTP Server Name	smtp.gmail.com
SMTP Server Port	25
SMTP Authentication Username	email@gmail.com
SMTP Authentication Password	••••••••
Confirm SMTP Authentication Password	••••••••

⊞ SMTP Encryption Options

Alarm Event

□ Alarm Event	□ Rogue AP Detected	□ Temporary license expired	☑ Uplink AP Lost	□ [Smart Redundancy] Standby Disconnected
	□ Rogue Device Detected	□ Temporary license will expire	□ Incomplete Primary/Secondary IP Settings	
	☑ AP Lost Contact	□ LAN Rogue AP Detected	☑ [Smart Redundancy] State Changed	
	☑ SSID-spoofing AP Detected	□ AAA Server Unreachable	□ [Smart Redundancy] Active Connected	
	☑ MAC-spoofing AP Detected	☑ AP Has Hardware Problem	□ [Smart Redundancy] Standby Connected	
	□ Rogue DHCP Server Detected	☑ Sensor Has Problem	□ [Smart Redundancy] Active Disconnected	

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: After ZoneDirector is upgraded to software version 9.2 or later, the alarm email notification settings must be reconfigured to include the mail server name and port number. This will help ensure that ZoneDirector alarm recipients will continue to receive email notifications.

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.

Enabling Network Management Systems

ZoneDirector supports several external network management systems including Ruckus Wireless 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 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.

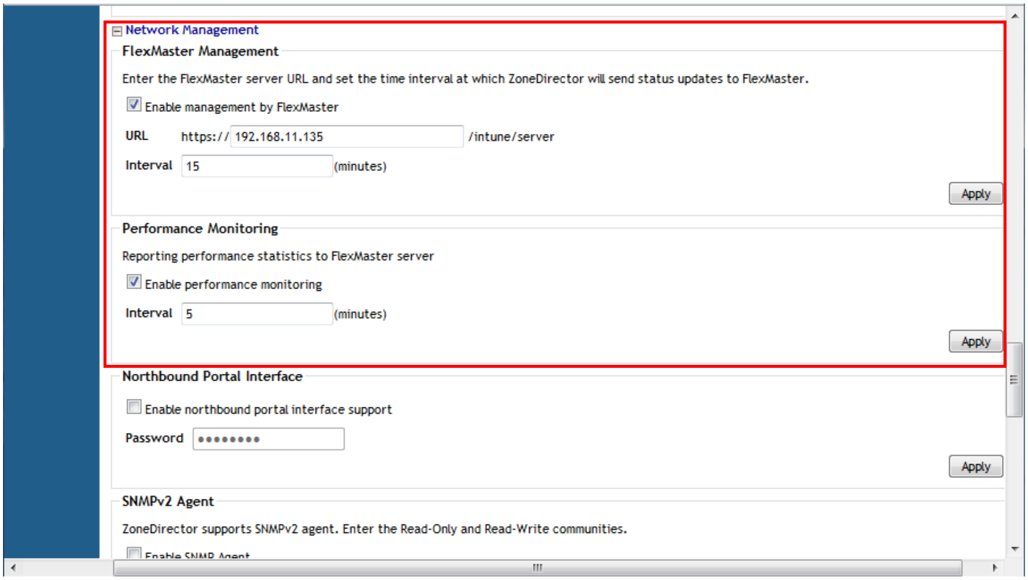
To enable FlexMaster management

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 37. The FlexMaster Management options



⊟ Network Management

FlexMaster Management

Enter the FlexMaster server URL and set the time interval at which ZoneDirector will send status updates to FlexMaster.

☑ Enable management by FlexMaster

URL https:// 192.168.11.135 /intune/server

Interval 15 (minutes)

Performance Monitoring

Reporting performance statistics to FlexMaster server

☑ Enable performance monitoring

Interval 5 (minutes)

Northbound Portal Interface

□ Enable northbound portal interface support

Password ●●●●●●●●

SNMPv2 Agent

ZoneDirector supports SNMPv2 agent. Enter the Read-Only and Read-Write communities.

□ Enable SNMP Agent

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

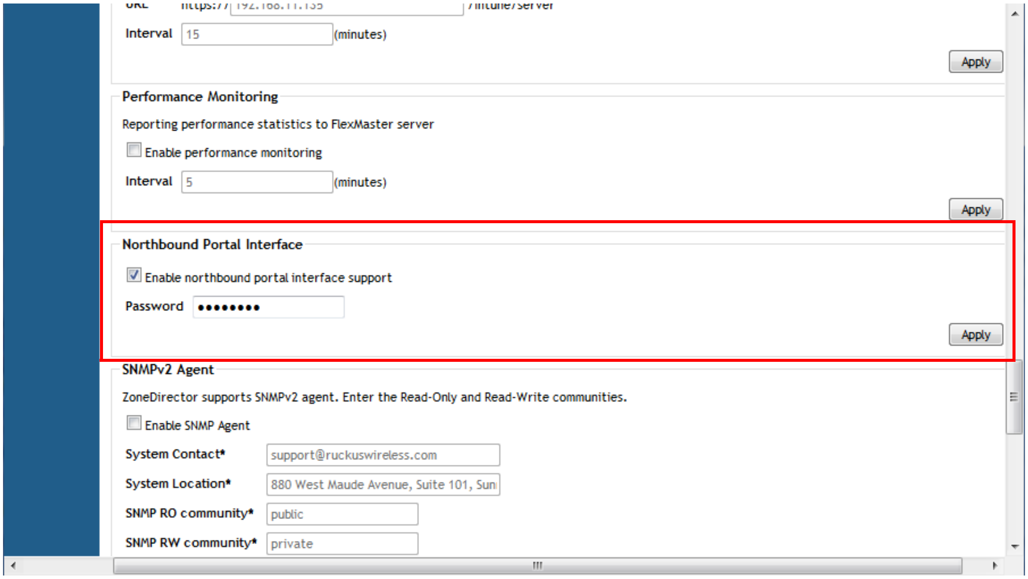
The Northbound Portal interface allows the use of DPSKs on open authentication WLANs meant for public access.

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 38. Enabling Northbound Portal interface



URL https:// 192.168.11.135 /intune/server

Interval 15 (minutes)

Apply

Performance Monitoring

Reporting performance statistics to FlexMaster server

☐ Enable performance monitoring

Interval 5 (minutes)

Apply

Northbound Portal Interface

☑ Enable northbound portal interface support

Password ••••••••

Apply

SNMPv2 Agent

ZoneDirector supports SNMPv2 agent. Enter the Read-Only and Read-Write communities.

☐ Enable SNMP Agent

System Contact* support@ruckuswireless.com

System Location* 880 West Maude Avenue, Suite 101, Sun

SNMP RO community* public

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.

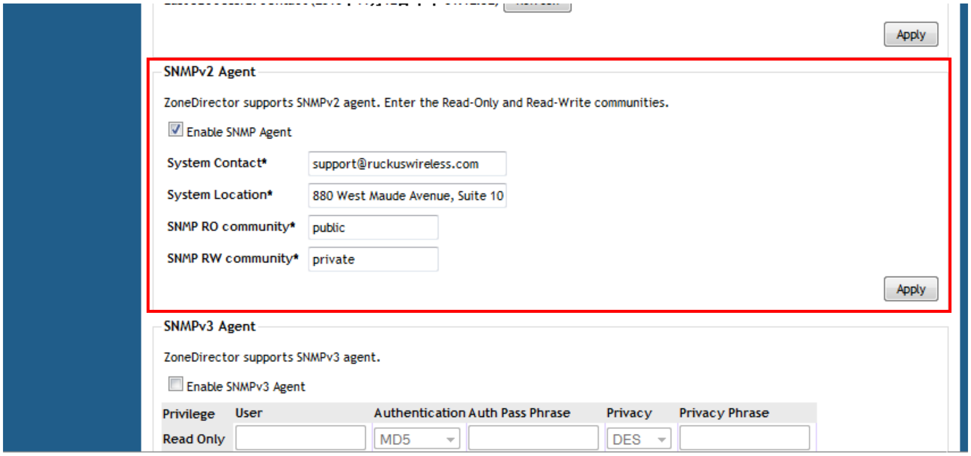
NOTE: For a list of the MIB variables that you can get and set using SNMP, check the related SNMP documentation on the Ruckus Wireless Support Web site at `http://support.ruckuswireless.com/documents`.

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

Figure 39. Enabling the SNMPv2 agent



Apply

SNMPv2 Agent

ZoneDirector supports SNMPv2 agent. Enter the Read-Only and Read-Write communities.

☑ Enable SNMP Agent

System Contact*	support@ruckuswireless.com
System Location*	880 West Maude Avenue, Suite 10
SNMP RO community*	public
SNMP RW community*	private

Apply

SNMPv3 Agent

ZoneDirector supports SNMPv3 agent.

☐ Enable SNMPv3 Agent

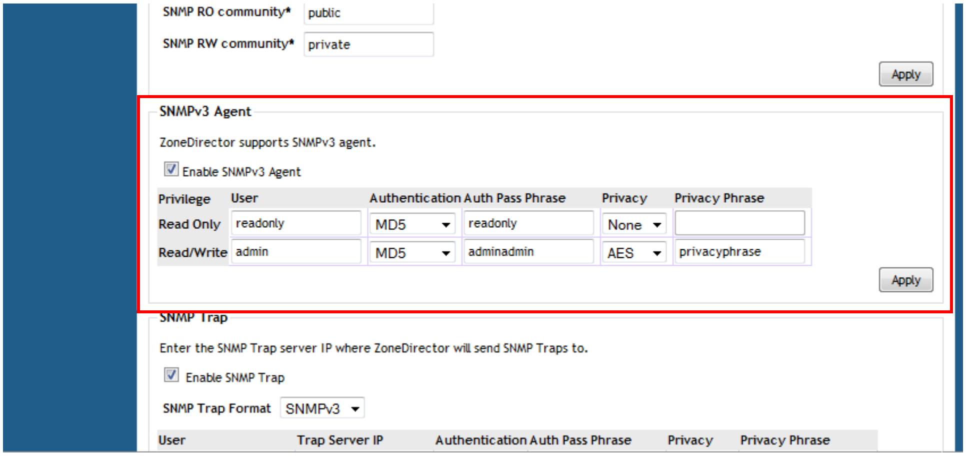
Privilege	User	Authentication	Auth Pass Phrase	Privacy	Privacy Phrase
Read Only		MD5		DES	

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 40. Enabling the SNMPv3 agent



SNMP RO community* public

SNMP RW community* private

SNMPv3 Agent

ZoneDirector supports SNMPv3 agent.

☑ Enable SNMPv3 Agent

Privilege	User	Authentication	Auth Pass Phrase	Privacy	Privacy Phrase
Read Only	readonly	MD5	readonly	None	
Read/Write	admin	MD5	adminadmin	AES	privacyphrase

SNMP Trap

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

☑ Enable SNMP Trap

SNMP Trap Format SNMPv3

User	Trap Server IP	Authentication	Auth Pass Phrase	Privacy	Privacy Phrase

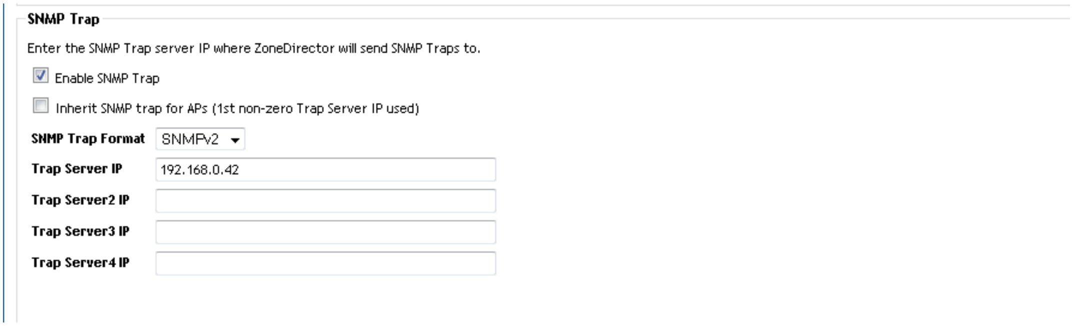
Enabling SNMP Trap Notifications

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" on page 60).

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.
   - Optional: If you want to disable AP SNMP trap delivery (receive ZD traps only), deselect the **Inherit SNMP trap for APs (1st Trap Server IP used)** 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 41. Enabling SNMPv2 trap notifications



SNMP Trap

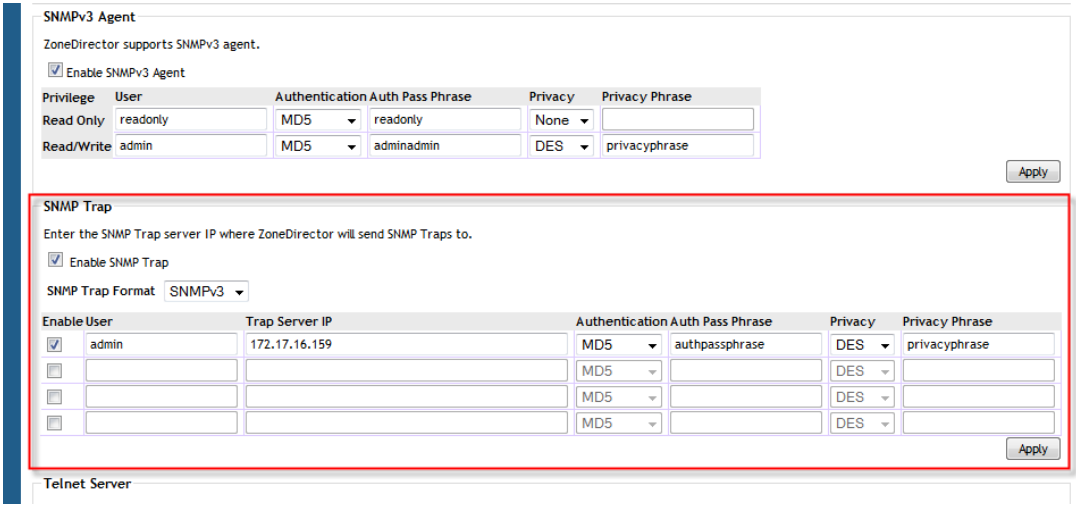
Enter the SNMP Trap server IP where ZoneDirector will send SNMP Traps to.

☑ Enable SNMP Trap

□ Inherit SNMP trap for APs (1st non-zero Trap Server IP used)

SNMP Trap Format	SNMPv2
Trap Server IP	192.168.0.42
Trap Server2 IP	
Trap Server3 IP	
Trap Server4 IP	

Figure 42. 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	None	
Read/Write	admin	MD5	adminadmin	DES	privacyphrase

Apply

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
☑	admin	172.17.16.159	MD5	authpassphrase	DES	privacyphrase
□			MD5		DES	
□			MD5		DES	
□			MD5		DES	

Apply

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.

Table 16. Trap notifications

Trap Name	Description
`ruckusZDEventSSIDSpoofTrap`	An SSID-spoofing rogue AP has been detected on the network. The rogue AP's MAC address and SSID are included in the trap notification.
`ruckusZDEventMACSpoofTrap`	A MAC-spoofing rogue AP has been detected on the network. The rogue AP's MAC address and SSID are included in the trap notification.
`ruckusZDEventRogueAPTrap`	A rogue AP has been detected on the network. The rogue AP's MAC address and SSID are included in the trap notification.
`ruckusZDEventAPLostTrap`	An AP has lost contact with ZoneDirector. The AP's MAC address is included in the trap notification.
`ruckusZDEventAPLostHeartbeatTrap`	An AP's heartbeat has been lost. The AP's MAC address is included in the trap notification.
`ruckusZDEventClientAuthFailBlockTrap`	A wireless client repeatedly failed to authenticate with an AP. The client's MAC address, AP's MAC address and SSID are included in the trap notification.
`ruckusZDEventClientJoin`	A client has successfully joined an AP. The client's MAC address, the AP's MAC address and SSID are included in the trap notification.
`ruckusZDEventClientJoinFailed`	A client has attempted and failed to join an AP. The client's MAC address, the AP's MAC address and SSID are included in the trap notification.
`ruckusZDEventClientJoinFailedAPBusy`	A client attempt to join an AP failed because the AP was busy. The client's MAC address, AP's MAC address and SSID are included.
`ruckusZDEventClientDisconnect`	A client has disconnected from the AP. The client's MAC address, AP's MAC address and SSID are included.
`ruckusZDEventClientRoamOut`	A client has roamed away from an AP. The client's MAC address, AP's MAC address and SSID are included.

Table 16. Trap notifications

Trap Name	Description
`ruckusZDEventClientRoamIn`	A client has roamed in to an AP. The client's MAC address, AP's MAC address and SSID are included.
`ruckusZDEventClientAuthFailed`	A client authentication attempt has failed. The client's MAC address, AP's MAC address, SSID and failure reason are included.
`ruckusZDEventClientAuthorizationFailed`	A client authorization attempt to join an AP has failed. The client's MAC address, AP's MAC address and SSID are included.
`ruckusZDEventAPcoldstart`	An AP has been cold started.
`ruckusZDEventAPwarmstart`	An AP has been warm started.
`ruckusZDEventAPclientValve`	Triggered when an AP's online client limit has been exceeded.
`ruckusZDEventAPCPUvalve`	An AP's CPU utilization has exceeded the set value.
`ruckusZDEventAPMEMvalve`	An AP's memory utilization has exceeded the set value.
`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.

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 acknowledgement 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 client's AP tunnel and radio.

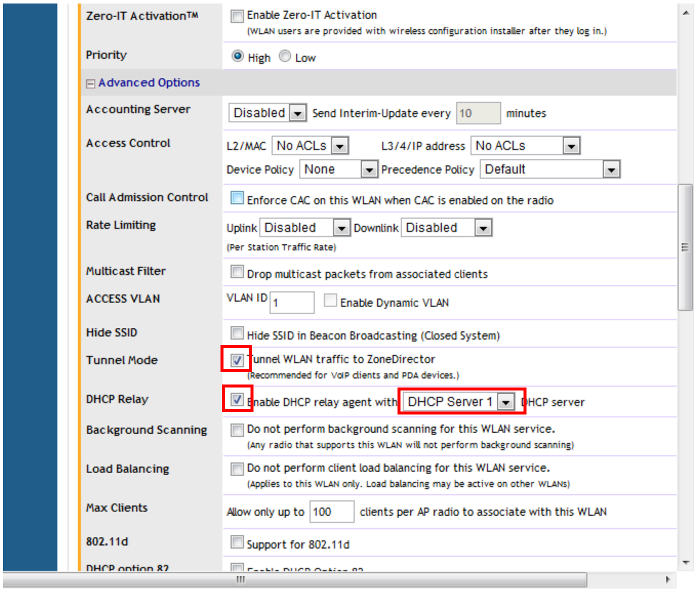
To configure DHCP Relay for tunneled WLANs

1. Go to **Configure > DHCP Servers**.
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.

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 43. Enabling DHCP Relay agent for a Tunnel Mode WLAN



Zero-IT Activation™	□ Enable Zero-IT Activation (WLAN users are provided with wireless configuration installer after they log in.)
Priority	● High ○ Low
⊟ Advanced Options	
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 ▾
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
ACCESS VLAN	VLAN ID 1 □ 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.)
DHCP Relay	☑ Enable DHCP relay agent with DHCP Server 1 ▾ DHCP server
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)
Max Clients	Allow only up to 100 clients per AP radio to associate with this WLAN
802.11d	□ Support for 802.11d
DHCP option 82	□ Enable DHCP Option 82

3

Configuring Security and Other Services

In This Chapter

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."

ZoneDirector offers two methods of automatically adjusting AP channels for self healing 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 can not 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

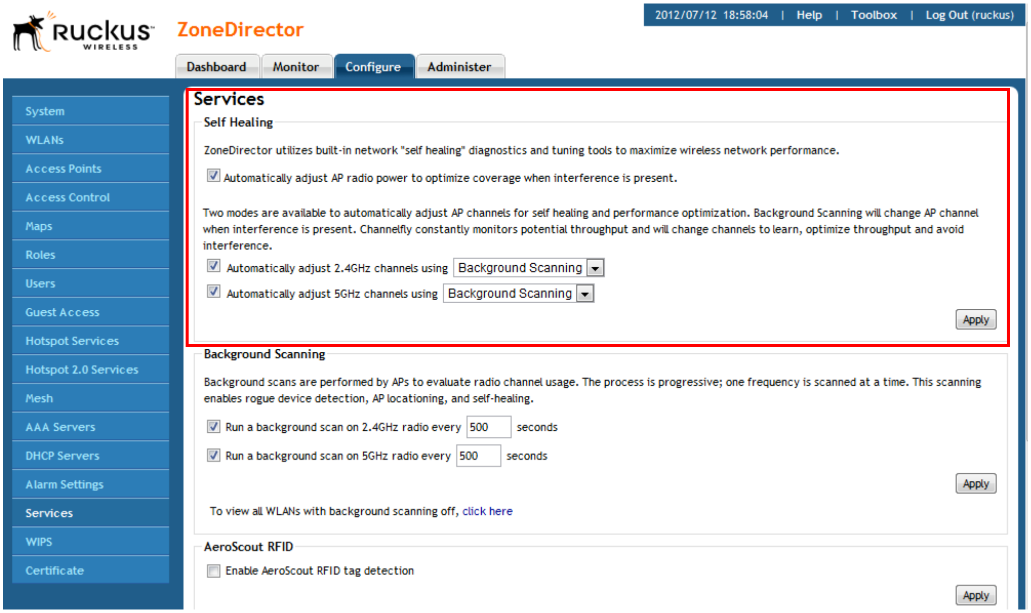
Compared to Background Scanning, ChannelFly takes considerably longer for the network to settle down. If you will be adding and removing APs to your network frequently, Background Scanning may be preferable. Additionally, if you have clients that do not support the 802.11h standard, ChannelFly may cause 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 44. Self Healing options



Services

Self Healing

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

☑ Automatically adjust AP radio power to optimize coverage when interference is present.

Two modes are available to automatically adjust AP channels for self healing and performance optimization. Background Scanning will change AP channel when interference is present. Channelfly constantly monitors potential throughput and will change channels to learn, optimize throughput and avoid interference.

☑ Automatically adjust 2.4GHz channels using Background Scanning

☑ Automatically adjust 5GHz channels using Background Scanning

Background Scanning

Background scans are performed by APs to evaluate radio channel usage. The process is progressive; one frequency is scanned at a time. This scanning enables rogue device detection, AP locationing, and self-healing.

☑ Run a background scan on 2.4GHz radio every 500 seconds

☑ Run a background scan on 5GHz radio every 500 seconds

To view all WLANs with background scanning off, click here

AeroScout RFID

☐ Enable AeroScout RFID tag detection

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.

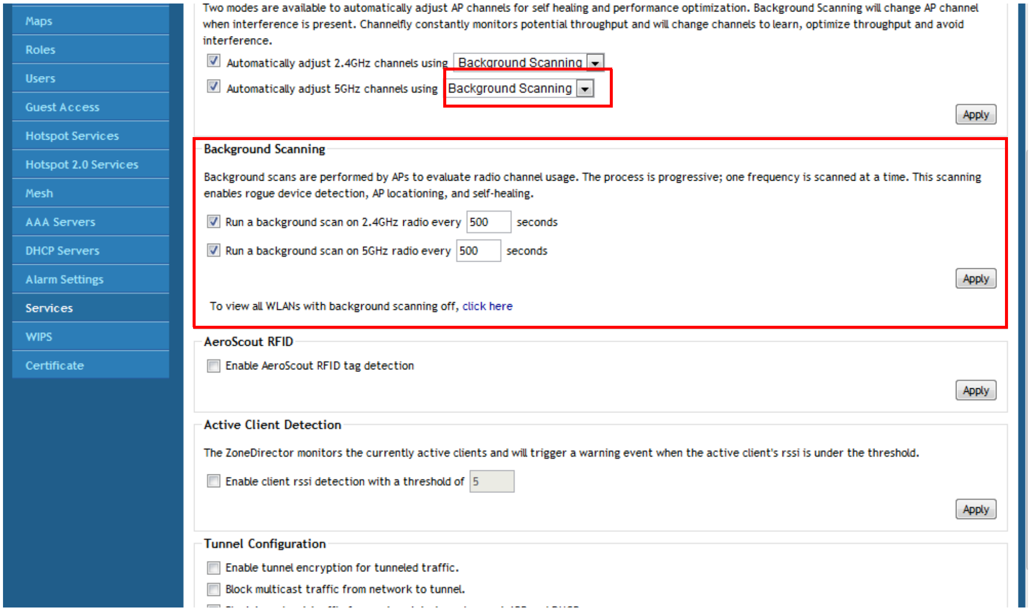
To configure Background Scanning

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 45. Background scanning options



Two modes are available to automatically adjust AP channels for self healing and performance optimization. Background Scanning will change AP channel when interference is present. Channelfly constantly monitors potential throughput and will change channels to learn, optimize throughput and avoid interference.

☑ Automatically adjust 2.4GHz channels using Background Scanning

☑ Automatically adjust 5GHz channels using Background Scanning

Apply

Background Scanning

Background scans are performed by APs to evaluate radio channel usage. The process is progressive; one frequency is scanned at a time. This scanning enables rogue device detection, AP locationing, and self-healing.

☑ Run a background scan on 2.4GHz radio every 500 seconds

☑ Run a background scan on 5GHz radio every 500 seconds

Apply

To view all WLANs with background scanning off, click here

AeroScout RFID

☐ Enable AeroScout RFID tag detection

Apply

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

Apply

Tunnel Configuration

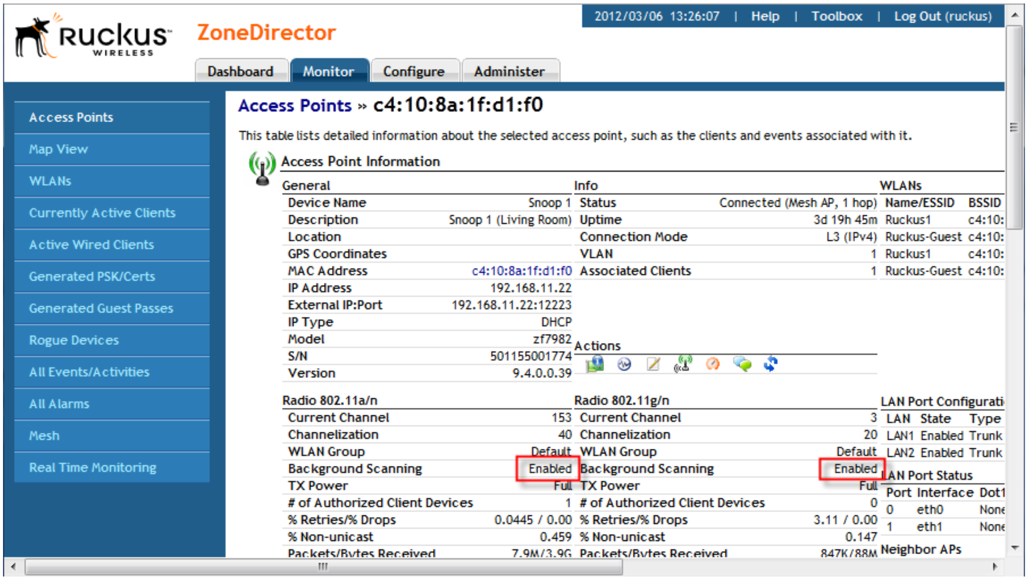
☐ Enable tunnel encryption for tunneled traffic.

☐ Block multicast traffic from network to tunnel.

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 46. Viewing whether Background Scanning is enabled for an AP



Access Points » c4:10:8a:1f:d1: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	Snoop 1	Status	Connected (Mesh AP, 1 hop)
Description	Snoop 1 (Living Room)	Uptime	3d 19h 45m
Location		Connection Mode	L3 (IPv4)
GPS Coordinates		VLAN	1
MAC Address	c4:10:8a:1f:d1:f0	Associated Clients	1
IP Address	192.168.11.22		
External IP:Port	192.168.11.22:12223		
IP Type	DHCP		
Model	zf7982		
S/N	501155001774		
Version	9.4.0.0.39		

WLANs

Name/ESSID	BSSID
Ruckus1	c4:10:
Ruckus-Guest	c4:10:
Ruckus1	c4:10:
Ruckus-Guest	c4:10:

Radio 802.11a/n		Radio 802.11g/n	
Current Channel	153	Current Channel	3
Channelization	40	Channelization	20
WLAN Group	Default	WLAN Group	Default
Background Scanning	Enabled	Background Scanning	Enabled
TX Power	Full	TX Power	Full
# of Authorized Client Devices	1	# of Authorized Client Devices	0
% Retries/% Drops	0.0445 / 0.00	% Retries/% Drops	3.11 / 0.00
% Non-unicast	0.459	% Non-unicast	0.147
Packets/Bytes Received	7.9M/3.9G	Packets/Bytes Received	847K/88M

LAN Port Configurati

LAN	State	Type
LAN1	Enabled	Trunk
LAN2	Enabled	Trunk

LAN Port Status

Port	Interface	Dot1
0	eth0	None
1	eth1	None

Neighbor APs

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.

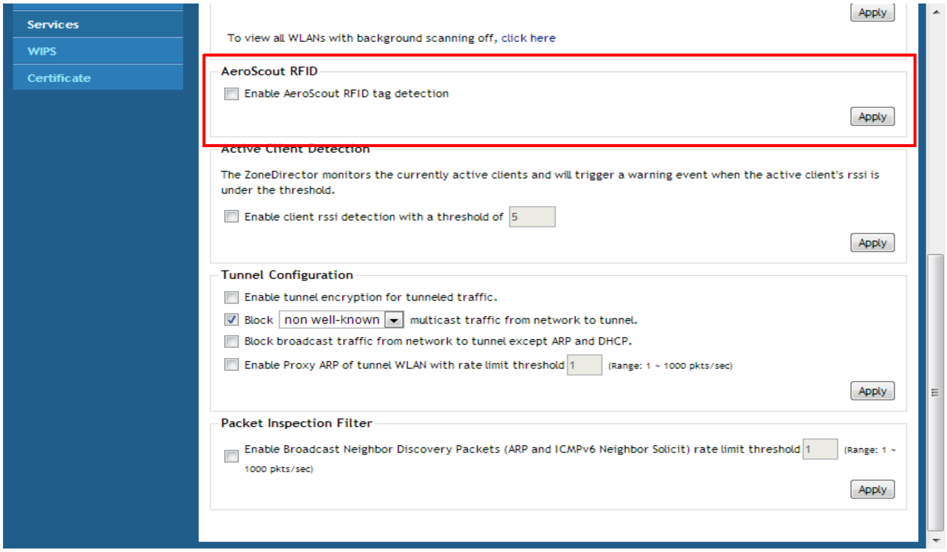
If you are using AeroScout Tags in your organization, you can use the APs that are being managed by ZoneDirector to relay data from the AeroScout Tags to the AeroScout Engine. You only need to enable AeroScout tag detection on ZoneDirector to enable APs to relay data to the AeroScout engine.

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 47. AeroScout Tag detection option



To view all WLANs with background scanning off, click here

AeroScout RFID

□ Enable AeroScout RFID tag detection

Apply

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

Apply

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 with rate limit threshold 1 (Range: 1 ~ 1000 pkts/sec)

Apply

Packet Inspection Filter

□ Enable Broadcast Neighbor Discovery Packets (ARP and ICMPv6 Neighbor Solicit) rate limit threshold 1 (Range: 1 ~ 1000 pkts/sec)

Apply

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.

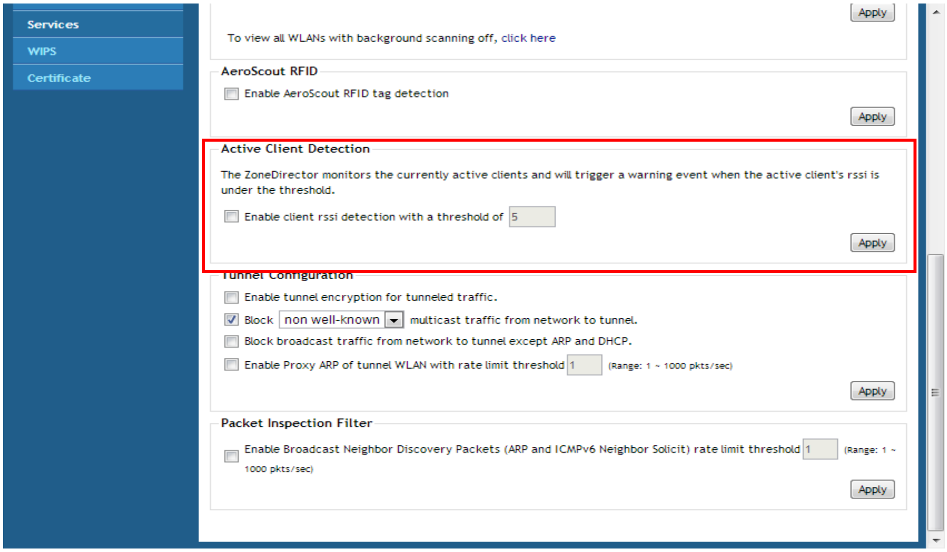
Active Client Detection

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 48. Enabling active client detection



Apply

To view all WLANs with background scanning off, click here

AeroScout RFID

□ Enable AeroScout RFID tag detection

Apply

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

Apply

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 with rate limit threshold 1 (Range: 1 ~ 1000 pkts/sec)

Apply

Packet Inspection Filter

□ Enable Broadcast Neighbor Discovery Packets (ARP and ICMPv6 Neighbor Solicit) rate limit threshold 1 (Range: 1 ~ 1000 pkts/sec)

Apply

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 "Managing a Wireless Local Area Network" chapter for information on enabling Tunnel Mode for a WLAN.

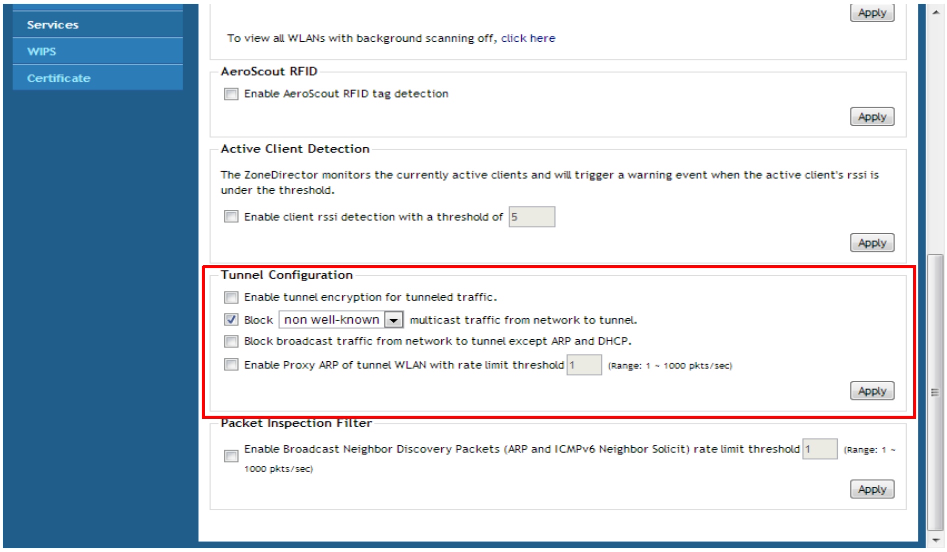
To configure data encryption and filtering for tunneled WLANs:

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] multi-cast 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" on page 73).

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

Figure 49. Set tunnel configuration parameters for all WLANs with tunnel mode enabled.



To view all WLANs with background scanning off, click here

AeroScout RFID

□ Enable AeroScout RFID tag detection

Apply

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

Apply

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 with rate limit threshold 1 (Range: 1 ~ 1000 pkts/sec)

Apply

Packet Inspection Filter

□ Enable Broadcast Neighbor Discovery Packets (ARP and ICMPv6 Neighbor Solicit) rate limit threshold 1 (Range: 1 ~ 1000 pkts/sec)

Apply

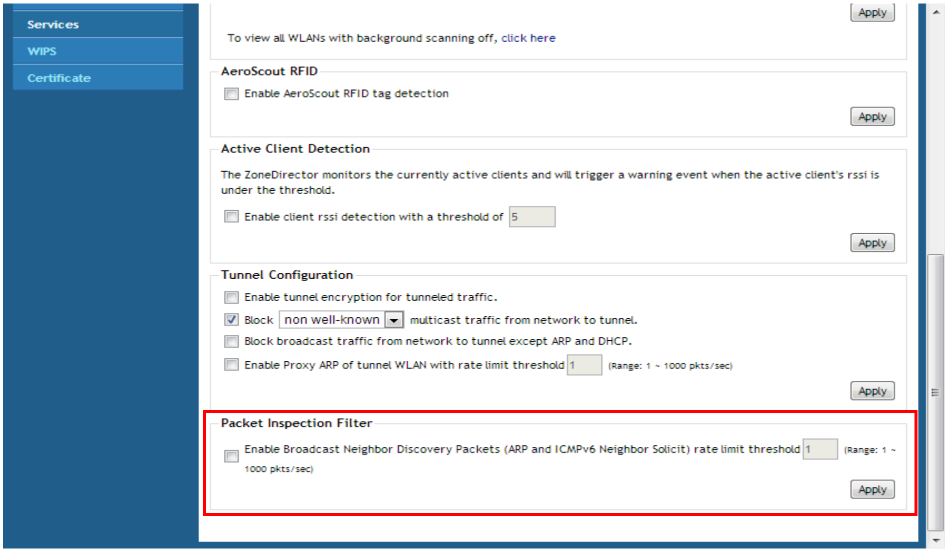
Packet Inspection Filter

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 50. Packet Inspection Filter



To view all WLANs with background scanning off, click here

AeroScout RFID

□ Enable AeroScout RFID tag detection

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 with rate limit threshold 1 (Range: 1 ~ 1000 pkts/sec)

Packet Inspection Filter

□ Enable Broadcast Neighbor Discovery Packets (ARP and ICMPv6 Neighbor Solicit) rate limit threshold 1 (Range: 1 ~ 1000 pkts/sec)

Configuring Wireless Intrusion Prevention

ZoneDirector has built-in intrusion prevention features called WIPS (Wireless Intrusion Prevention System) to protect the wireless network from security threats such as DoS attacks and intrusion attempts.

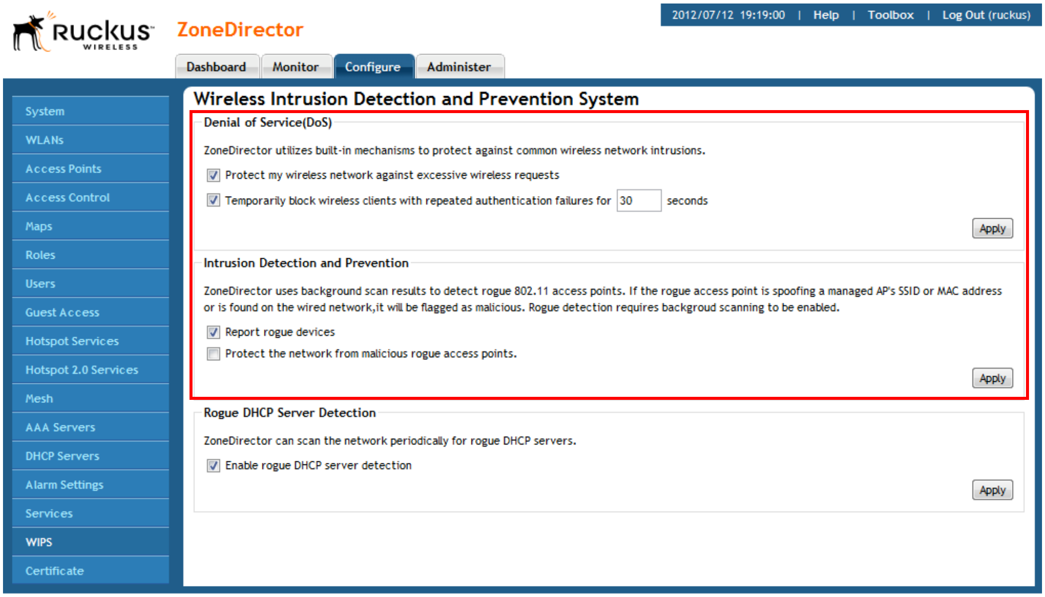
To configure the intrusion prevention options

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 under Monitor > Access Control.
3. In the *Intrusion Detection and Prevention* section, configure the following settings:
   - **Report rogue devices**: Enabling this check box allows ZoneDirector to include rogue device detection in logs and email alarm event notifications.
   - **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.

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

Figure 51. Intrusion Prevention options



Wireless Intrusion Detection and Prevention System

Denial of Service(DoS)

ZoneDirector utilizes built-in mechanisms to protect against common wireless network intrusions.

☑ Protect my wireless network against excessive wireless requests

☑ Temporarily block wireless clients with repeated authentication failures for 30 seconds

Apply

Intrusion Detection and Prevention

ZoneDirector uses background scan results to detect rogue 802.11 access points. If the rogue access point is spoofing a managed AP's SSID or MAC address or is found on the wired network,it will be flagged as malicious. Rogue detection requires backgroud scanning to be enabled.

☑ Report rogue devices

☐ Protect the network from malicious rogue access points.

Apply

Rogue DHCP Server Detection

ZoneDirector can scan the network periodically for rogue DHCP servers.

☑ Enable rogue DHCP server detection

Apply

See "Detecting Rogue Access Points" on page 197 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.

To enable rogue DHCP server detection on ZoneDirector

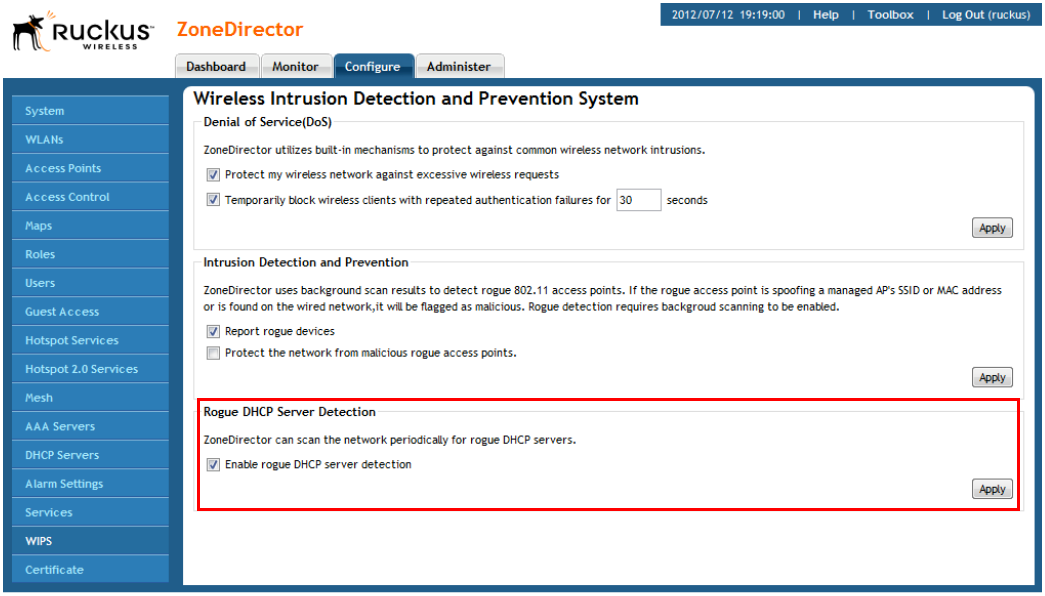
1. Go to **Configure** > **WIPS**.
2. In the Rogue DHCP Server Detection section, select the **Enable rogue DHCP server detection** check box.
3. Click the **Apply** button that is in the same section.

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. If ZoneDirector detected any rogue DHCP server, you will see the following event 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.

Figure 52. Enabling Rogue DHCP server detection



Wireless Intrusion Detection and Prevention System

Denial of Service(DoS)

ZoneDirector utilizes built-in mechanisms to protect against common wireless network intrusions.

☑ Protect my wireless network against excessive wireless requests

☑ Temporarily block wireless clients with repeated authentication failures for 30 seconds

Apply

Intrusion Detection and Prevention

ZoneDirector uses background scan results to detect rogue 802.11 access points. If the rogue access point is spoofing a managed AP's SSID or MAC address or is found on the wired network,it will be flagged as malicious. Rogue detection requires backgroud scanning to be enabled.

☑ Report rogue devices

☐ Protect the network from malicious rogue access points.

Apply

Rogue DHCP Server Detection

ZoneDirector can scan the network periodically for rogue DHCP servers.

☑ Enable rogue DHCP server detection

Apply

Controlling Device Permissions: Blocking and ACLs

Access controls can be configured to control access to both your wireless network and to the ZoneDirector interface itself. For network access, ZoneDirector features a block list as well as access control lists (ACL) to control access to the network.

WLAN ACLs and Block Lists

ZoneDirector provides two methods of controlling access to your wireless LANs:

- *Block List*: When users log into a ZoneDirector network, their client devices (for example, notebook computers and smart phones) are recorded and tracked. If, for any reason, you need to block a client device from network use, you can do so via the ZoneDirector Web interface. For more on configuring the block list, see "Blocking Client Devices" on page 81.
- *Access Control Lists*: Access control lists (ACLs) establish which devices are allowed to associate to a ZoneDirector-managed AP. By using the **Configure** > **Access Control** options, you can define Layer 2 ACLs (MAC address ACLs), which can then be applied to one or more ZoneDirector WLANs. You can also create L3/L4 ACLs (to restrict access by IP address). 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.

Take note of the following ZoneDirector rules:

- The block list is system-wide and is applied to all WLANs in addition to the per-WLAN ACL. 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.

Configuring Access Control Lists

You can build L2/MAC and L3/L4 access control lists to establish which devices are allowed to associate to the APs. You can configure these options on the **Configure** > **Access Control** page.

NOTE There is a system-wide block list that is applied to all WLANs in addition to the per-WLAN ACLs. The entries of the system-wide block list are added when the Admin chooses to block clients from the Monitor/Currently Active Clients panel. The Admin can remove entries from the system-wide block list via **Configure** > **Access Control** > **Block Clients** list. If a MAC address is listed in the system-wide block list, it will be blocked even if it is an allowed entry in another ACL list.

L2/MAC Access Control

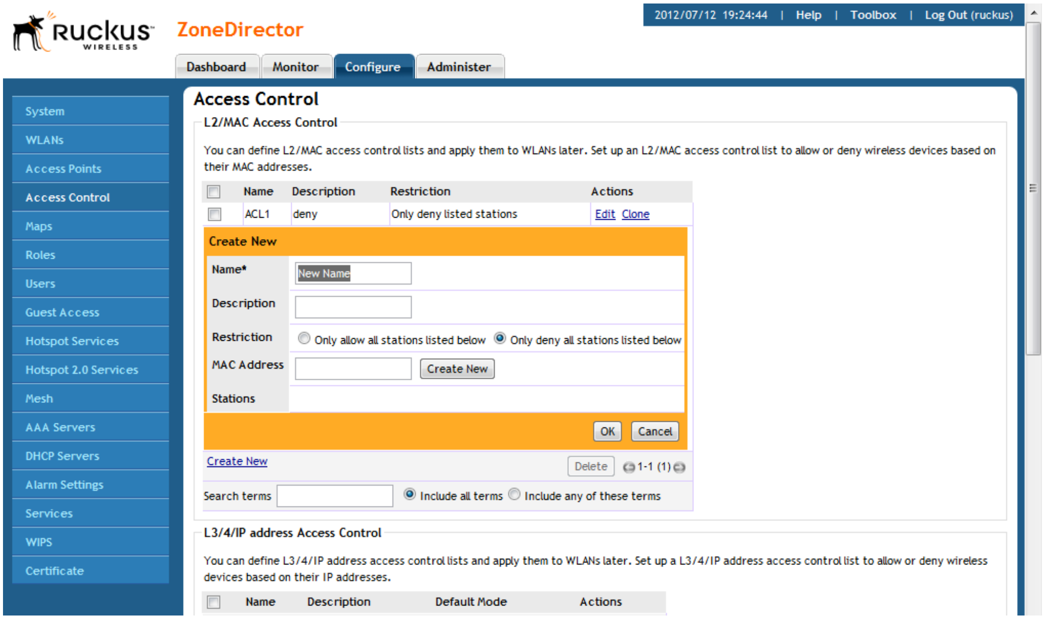
Using the Access Controls configuration options, you define Layer 2/MAC address ACLs, which can then be applied to one or more WLANs (upon WLAN creation or edit). ACLs are either allow-only or deny-only; that is, an ACL can be set up to allow only specified clients or to deny only specified clients. 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. In L2/MAC Access Control, click **Create New**.
3. Type a **Name** for the ACL.
4. Type a **Description** of the ACL.
5. Select the **Restriction** mode as either allow or deny.
6. 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.
7. 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.

Figure 53. Configuring an L2/MAC access control list



Access Control

L2/MAC Access Control

You can define L2/MAC access control lists and apply them to WLANs later. Set up an L2/MAC access control list to allow or deny wireless devices based on their MAC addresses.

□	Name	Description	Restriction	Actions
□	ACL1	deny	Only deny listed stations	Edit Clone

Create New

Name*	New Name
Description	
Restriction	○ Only allow all stations listed below ● Only deny all stations listed below
MAC Address	Create New
Stations	

OK Cancel

Create New Delete 1-1 (1)

Search terms ● Include all terms ○ Include any of these terms

L3/4/IP address Access Control

You can define L3/4/IP address access control lists and apply them to WLANs later. Set up a L3/4/IP address access control list to allow or deny wireless devices based on their IP addresses.

□	Name	Description	Default Mode	Actions

L3/L4 Access Control

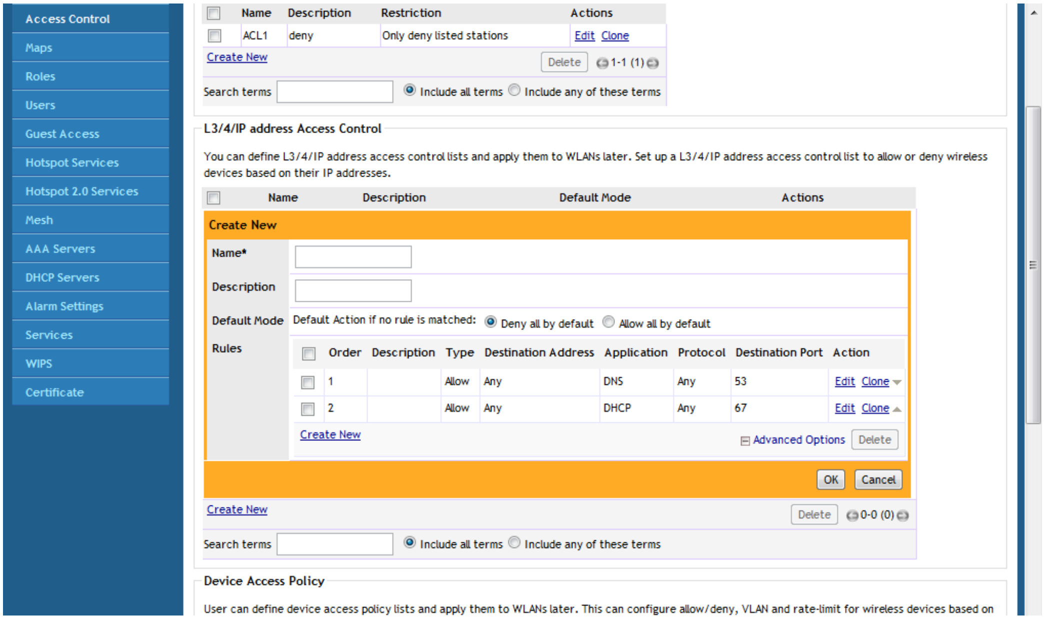
In addition to L2/MAC based ACLs, ZoneDirector also provides access control options at Layer 3 and Layer 4. This means that you can configure the access control options based on a set of criteria, including:

- Destination Address
- Application
- Protocol
- Destination Port

To create an L3/L4/IP address based ACL

1. Go to **Configure** > **Access Control**.
2. In L3/4/IP address Access Control, click **Create New**.
3. Type a **Name** for the ACL.
4. Type a **Description** for the ACL.
5. In **Default Mode**, set the default access privilege (allow all or deny all) that you want to grant all users by default.
6. In **Rules**, click **Create New** or click **Edit** to edit an existing rule.
7. 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 the IP subnet and netmask, or host IP address and 32-bit netmask, of the network or hostname URL target to which you want to allow or deny access. (IP addresses must be in the format `A.B.C.D/M`, where `M` is the bitmask.) Otherwise, select Any.
   - *Application*: If you have a specific application to which you want to allow or deny access, select it from the menu. Otherwise, select Any. If you select an option here besides Any, the Protocol and Destination Port options are disabled.
   - *Protocol*: If you have a network protocol that you want to allow or deny, select it from the menu. Otherwise, select Any.
   - *Destination Port*: If you have a specific destination port to which you want to allow or deny access, select it from the menu. Otherwise, select Any.
8. Click **OK** to save the ACL.
9. Repeat these steps to create up to 32 L3/L4/IP address-based access control rules.

Figure 54. Configuring L3/L4 access control list



□	Name	Description	Restriction	Actions
□	ACL1	deny	Only deny listed stations	Edit Clone

Create New — Delete 1-1 (1)

Search terms ________ ● Include all terms ○ Include any of these terms

L3/4/IP address Access Control

You can define L3/4/IP address access control lists and apply them to WLANs later. Set up a L3/4/IP address access control list to allow or deny wireless devices based on their IP addresses.

□	Name	Description	Default Mode	Actions

Create New

Name* ________

Description ________

Default Mode: Default Action if no rule is matched: ● Deny all by default ○ Allow all by default

Rules

□	Order	Description	Type	Destination Address	Application	Protocol	Destination Port	Action
□	1		Allow	Any	DNS	Any	53	Edit Clone
□	2		Allow	Any	DHCP	Any	67	Edit Clone

Create New — Advanced Options — Delete

OK Cancel

Create New — Delete 0-0 (0)

Search terms ________ ● Include all terms ○ Include any of these terms

Device Access Policy

User can define device access policy lists and apply them to WLANs later. This can configure allow/deny, VLAN and rate-limit for wireless devices based on

ZoneDirector Management ACL

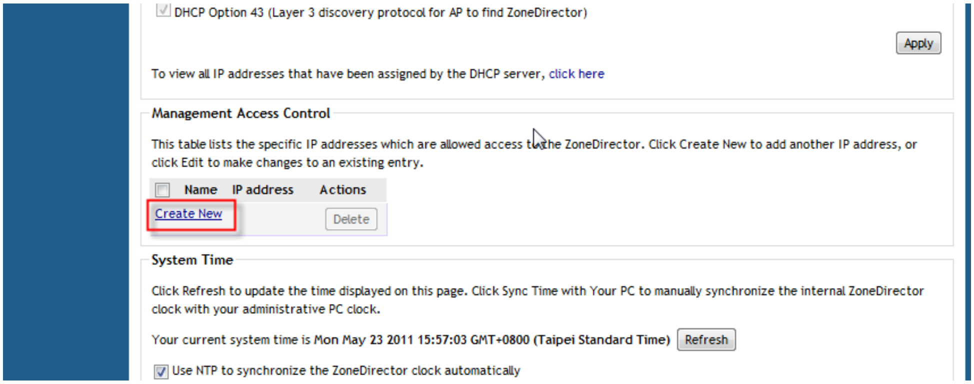
Additionally, ZoneDirector also includes an access control feature for controlling access to ZoneDirector's management interface. The **Management Access Control** interface is located on the *Configure > System* screen. Options include limiting access by subnet, single IP address and IP address range.

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 55. Management Access Control



☑ 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.

□	Name	IP address	Actions

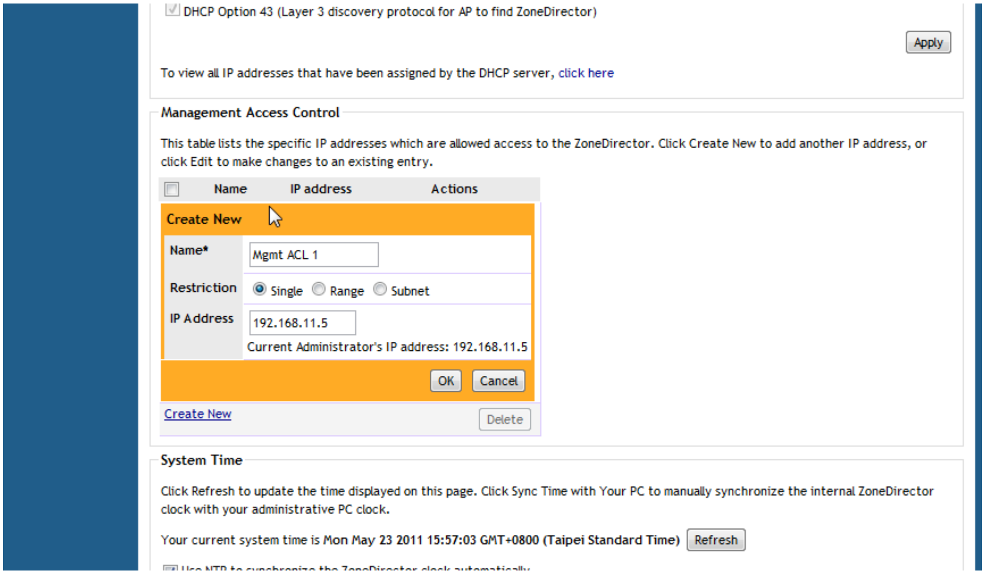
System Time

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

Figure 56. Creating a new ZoneDirector management ACL



☑ 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.

□	Name	IP address	Actions

Create New

Name* Mgmt ACL 1

Restriction ● Single ○ Range ○ Subnet

IP Address 192.168.11.5

Current Administrator's IP address: 192.168.11.5

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

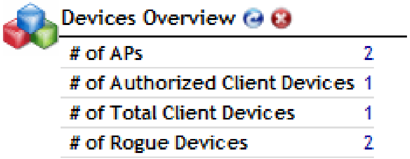
Blocking Client Devices

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 track client devices.

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 57. The Device Overview widget



Devices Overview

# of APs	2
# of Authorized Client Devices	1
# of Total Client Devices	1
# of Rogue Devices	2

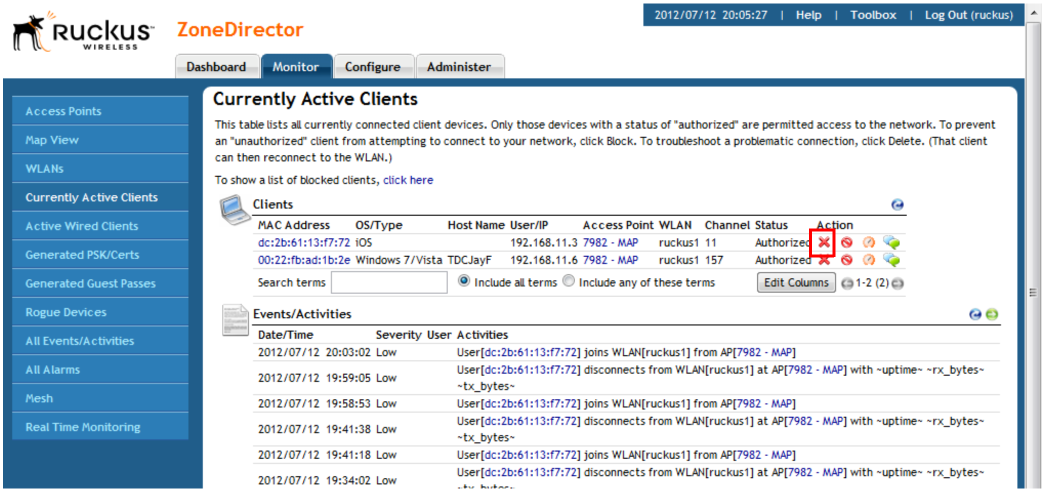
3. Click the current number, which is also a link. The Currently Active Clients page (on the Monitor tab) appears, showing the first 15 clients that are currently connected to ZoneDirector. If there are more than 15 currently active clients, the Show More button at the bottom of the page will be active. 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 58. Click the Delete button to temporarily delete a client. The client will be able to reconnect.



Currently Active Clients

This table lists all currently connected client devices. Only those devices with a status of "authorized" are permitted access to the network. To prevent an "unauthorized" client from 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

Clients

MAC Address	OS/Type	Host Name	User/IP	Access Point	WLAN	Channel	Status	Action
dc:2b:61:13:f7:72	iOS		192.168.11.3	7982 - MAP	ruckus1	11	Authorized	
00:22:fb:ad:1b:2e	Windows 7/Vista	TDCJayF	192.168.11.6	7982 - MAP	ruckus1	157	Authorized	

Search terms ● Include all terms ○ Include any of these terms Edit Columns 1-2 (2)

Events/Activities

Date/Time	Severity	User	Activities
2012/07/12 20:03:02	Low		User[dc:2b:61:13:f7:72] joins WLAN[ruckus1] from AP[7982 - MAP]
2012/07/12 19:59:05	Low		User[dc:2b:61:13:f7:72] disconnects from WLAN[ruckus1] at AP[7982 - MAP] with ~uptime~ ~rx_bytes~ ~tx_bytes~
2012/07/12 19:58:53	Low		User[dc:2b:61:13:f7:72] joins WLAN[ruckus1] from AP[7982 - MAP]
2012/07/12 19:41:38	Low		User[dc:2b:61:13:f7:72] disconnects from WLAN[ruckus1] at AP[7982 - MAP] with ~uptime~ ~rx_bytes~ ~tx_bytes~
2012/07/12 19:41:18	Low		User[dc:2b:61:13:f7:72] joins WLAN[ruckus1] from AP[7982 - MAP]
2012/07/12 19:34:02	Low		User[dc:2b:61:13:f7:72] disconnects from WLAN[ruckus1] at AP[7982 - MAP] with ~uptime~ ~rx_bytes~ ~tx_bytes~

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.

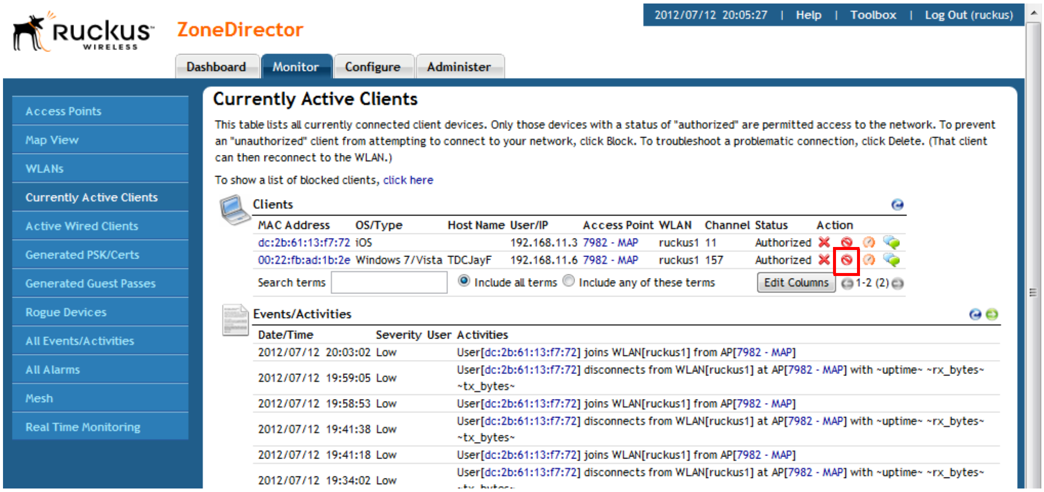
Permanently Blocking Specific Client Devices

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 59. Click the Block button to permanently delete a client



Currently Active Clients

This table lists all currently connected client devices. Only those devices with a status of "authorized" are permitted access to the network. To prevent an "unauthorized" client from 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

Clients

MAC Address	OS/Type	Host Name	User/IP	Access Point	WLAN	Channel	Status	Action
dc:2b:61:13:f7:72	iOS		192.168.11.3	7982 - MAP	ruckus1	11	Authorized	
00:22:fb:ad:1b:2e	Windows 7/Vista	TDCJayF	192.168.11.6	7982 - MAP	ruckus1	157	Authorized	

Search terms ● Include all terms ○ Include any of these terms

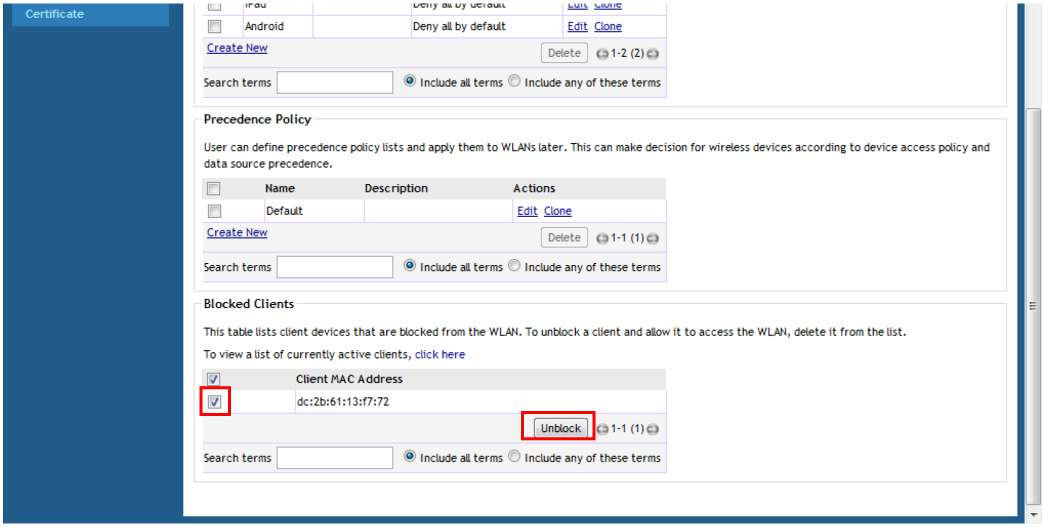
Events/Activities

Date/Time	Severity	User	Activities
2012/07/12 20:03:02	Low		User[dc:2b:61:13:f7:72] joins WLAN[ruckus1] from AP[7982 - MAP]
2012/07/12 19:59:05	Low		User[dc:2b:61:13:f7:72] disconnects from WLAN[ruckus1] at AP[7982 - MAP] with ~uptime~ ~rx_bytes~ ~tx_bytes~
2012/07/12 19:58:53	Low		User[dc:2b:61:13:f7:72] joins WLAN[ruckus1] from AP[7982 - MAP]
2012/07/12 19:41:38	Low		User[dc:2b:61:13:f7:72] disconnects from WLAN[ruckus1] at AP[7982 - MAP] with ~uptime~ ~rx_bytes~ ~tx_bytes~
2012/07/12 19:41:18	Low		User[dc:2b:61:13:f7:72] joins WLAN[ruckus1] from AP[7982 - MAP]
2012/07/12 19:34:02	Low		User[dc:2b:61:13:f7:72] disconnects from WLAN[ruckus1] at AP[7982 - MAP] with ~uptime~ ~rx_bytes~

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 60. Unblocking a previously blocked client



□	iPad	Deny all by default	Edit Clone
□	Android	Deny all by default	Edit Clone

Search terms ● Include all terms ○ Include any of these terms

Precedence Policy

User can define precedence policy lists and apply them to WLANs later. This can make decision for wireless devices according to device access policy and data source precedence.

□	Name	Description	Actions
□	Default		Edit Clone

Search terms ● Include all terms ○ 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 MAC Address
☑	dc:2b:61:13:f7:72

Search terms ● Include all terms ○ Include any of these terms

Configuring Device Access Policies

In response to the growing trend of employees and students bringing their personally owned devices 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.

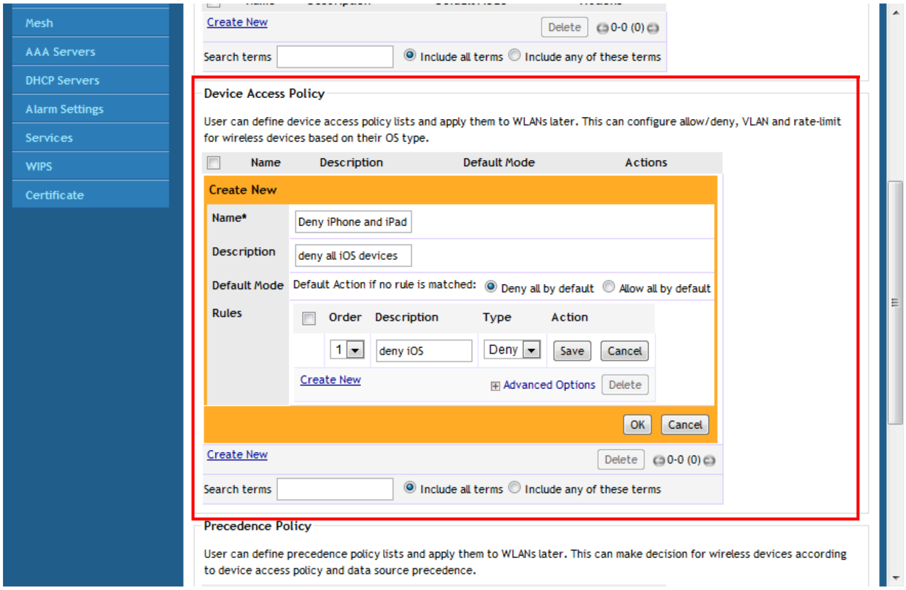
Using the Device Access Policy settings, ZoneDirector can identify the type of client device attempting to connect and perform control actions such as permit/deny, rate limiting and VLAN tagging based on client type.

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.

To create a Device Access Policy

1. Go to **Configure > Access Control**.
2. In the *Device Access Policy* section, click **Create New**.
3. Enter a **Name** and optionally a description for the access policy.
4. In *Default Mode*, select **Deny all by default** or **Allow all by default**.
5. In *Rules*, you can create multiple OS-specific rules for each access policy.
   - Description: Description of the rule.
   - OS/Type: Select from any of the supported client types.
   - Type: Select rule type (allow or deny)
   - Uplink/Downlink: Set rate limiting for this client type.
   - 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 nine rules per access policy (one for each OS/Type).
7. To change the order in which rules are implemented, click the up or down arrows in the *Action* column. You can also **Edit** or **Clone** rules from the *Action* column. 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 61. Creating a Device Access Policy



Create New   Delete   0-0 (0)

Search terms   ● Include all terms ○ Include any of these terms

Device Access Policy

User can define device access policy lists and apply them to WLANs later. This can configure allow/deny, VLAN and rate-limit for wireless devices based on their OS type.

□	Name	Description	Default Mode	Actions

Create New

Name*	Deny iPhone and iPad
Description	deny all iOS devices
Default Mode	Default Action if no rule is matched: ● Deny all by default ○ Allow all by default

Rules

□	Order	Description	Type	Action
	1	deny iOS	Deny	Save Cancel

Create New   ⊞ Advanced Options   Delete

OK   Cancel

Create New   Delete   0-0 (0)

Search terms   ● Include all terms ○ Include any of these terms

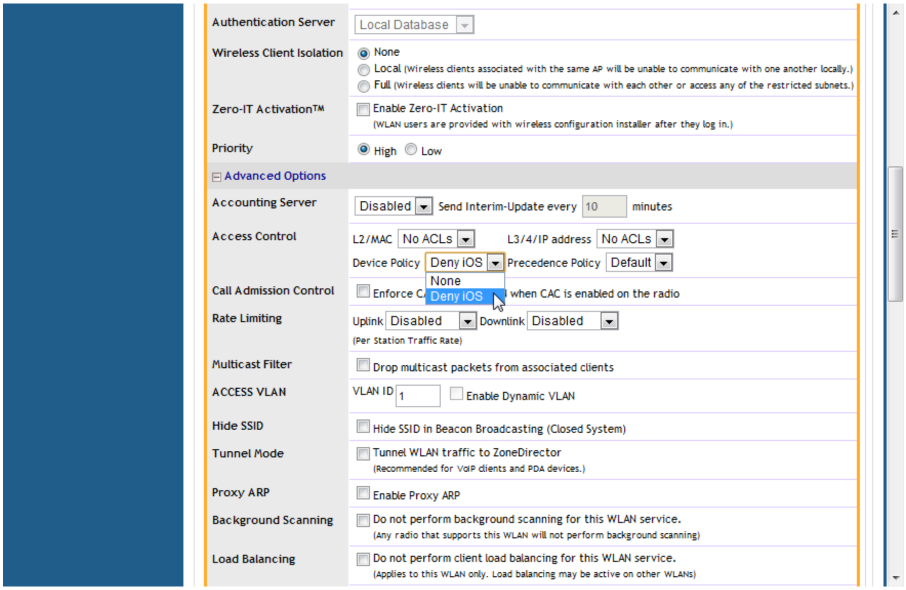
Precedence Policy

User can define precedence policy lists and apply them to WLANs later. This can make decision for wireless devices according to device access policy and data source precedence.

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 62. Selecting a device policy for a WLAN



Authentication Server	Local Database
Wireless Client Isolation	● None ○ Local (Wireless clients associated with the same AP will be unable to communicate with one another locally.) ○ Full (Wireless clients will be unable to communicate with each other or access any of the restricted subnets.)
Zero-IT Activation™	□ Enable Zero-IT Activation (WLAN users are provided with wireless configuration installer after they log in.)
Priority	● High ○ Low
⊟ Advanced Options	
Accounting Server	Disabled Send Interim-Update every 10 minutes
Access Control	L2/MAC No ACLs L3/4/IP address No ACLs Device Policy Deny iOS Precedence Policy Default
Call Admission Control	□ Enforce C[A] 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
ACCESS VLAN	VLAN ID 1 □ 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 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)

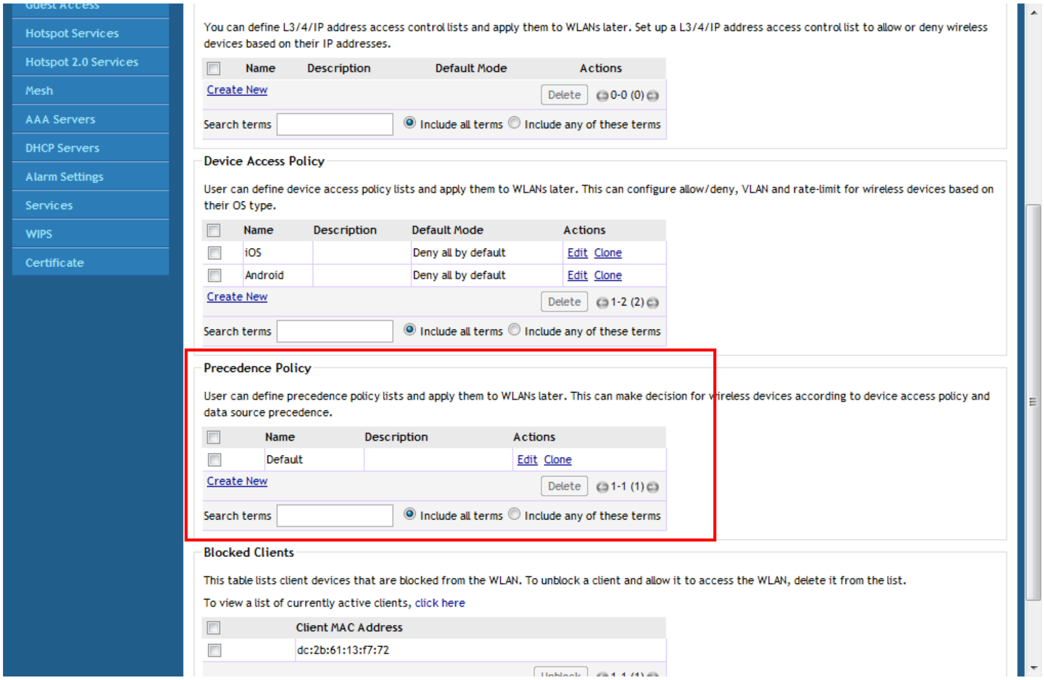
Configuring Precedence Policies

Use the Precedence Policy settings to define rate limiting and VLAN precedence of AAA server, device and WLAN policies.

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.
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 63. Precedence Policy settings



You can define L3/4/IP address access control lists and apply them to WLANs later. Set up a L3/4/IP address access control list to allow or deny wireless devices based on their IP addresses.

□	Name	Description	Default Mode	Actions
Create New				Delete 0-0 (0)

Search terms ● Include all terms ○ Include any of these terms

Device Access Policy

User can define device access policy lists and apply them to WLANs later. This can configure allow/deny, VLAN and rate-limit for wireless devices based on their OS type.

□	Name	Description	Default Mode	Actions
□	iOS		Deny all by default	Edit Clone
□	Android		Deny all by default	Edit Clone
Create New				Delete 1-2 (2)

Search terms ● Include all terms ○ Include any of these terms

Precedence Policy

User can define precedence policy lists and apply them to WLANs later. This can make decision for wireless devices according to device access policy and data source precedence.

□	Name	Description	Actions
□	Default		Edit Clone
Create New			Delete 1-1 (1)

Search terms ● Include all terms ○ 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 MAC Address
□	dc:2b:61:13:f7:72

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

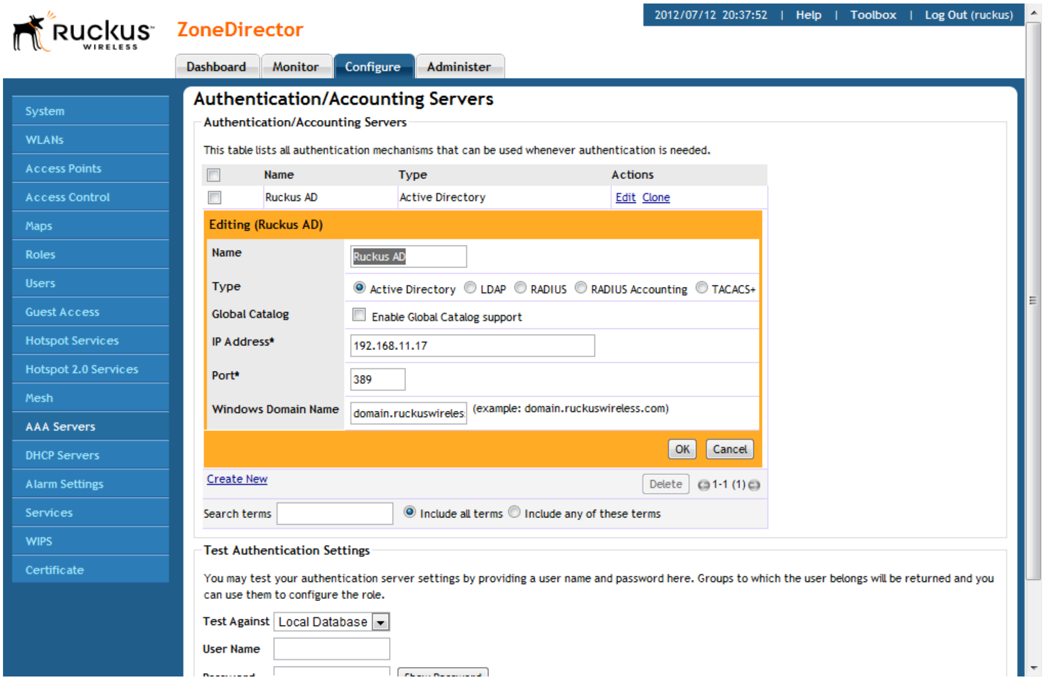
Single Domain Active Directory Authentication

To enable Active Directory authentication for a single domain:

1. Go to **Configure > AAA Servers**.
2. Click the **Edit** link next to Active Directory.
3. Do *not* enable Global Catalog support.
4. Enter the **IP address** and **Port** of the AD server. The default Port number (389) 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 64. Enable Active Directory for a single domain



Authentication/Accounting Servers

Authentication/Accounting Servers

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

□	Name	Type	Actions
□	Ruckus AD	Active Directory	Edit Clone

Editing (Ruckus AD)

Name	Ruckus AD
Type	● Active Directory ○ LDAP ○ RADIUS ○ RADIUS Accounting ○ TACACS+
Global Catalog	□ Enable Global Catalog support
IP Address*	192.168.11.17
Port*	389
Windows Domain Name	domain.ruckuswireles (example: domain.ruckuswireless.com)

Search terms ● Include all terms ○ Include any of these terms

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: Local Database

User Name

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. On the **Configure > AAA Servers** page, in the *Editing (Active Directory)* form, select the **Global Catalog** check box next to *Enable Global Catalog support*.
2. The default port changes to 3268, and the fields for Admin DN and password appear. The default port number (3268) should not be changed unless you have configured your AD server to use a different port.
   - Global Catalog queries are directed to port 3268, while ordinary searches are received through port 389. If the port binds to 389, even with Global Catalog server, the search includes only a single domain directory partition. If the port binds to port 3268, the search includes all directory partitions in the forest. If the server attempting to bind over port 3268 is not a Global Catalog server, the server refuses the bind.
3. Leave the **Windows Domain Name** field empty to search all domains in the forest.

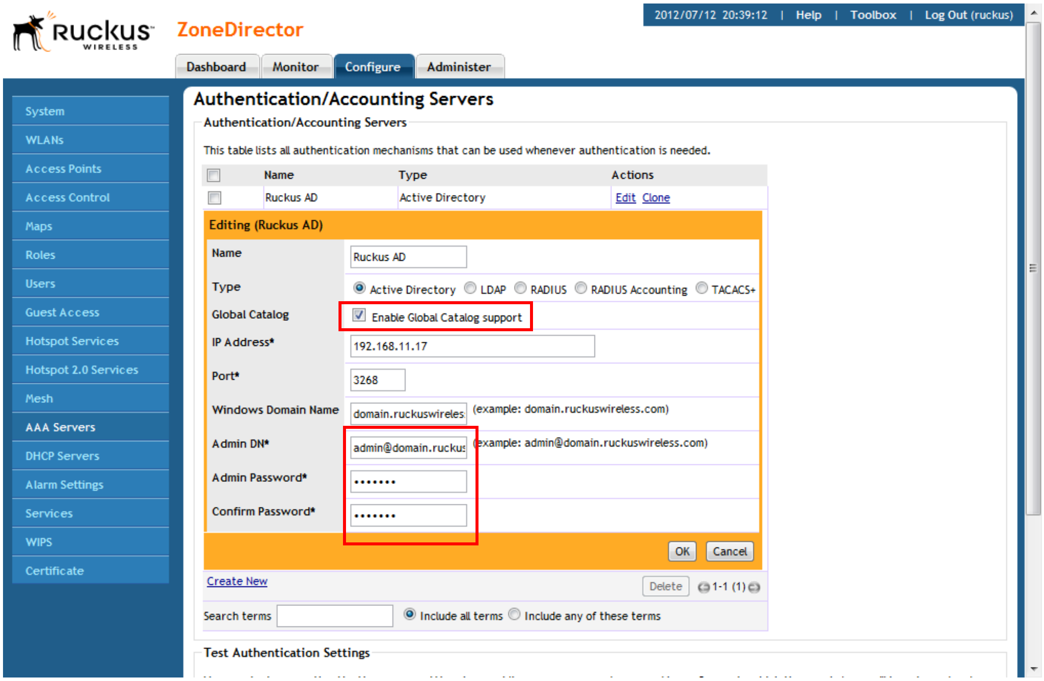
NOTE: Do NOT enter anything in the Windows Domain Name field. If you enter a Windows Domain Name, the search will be limited to that domain, rather than the whole forest.

4. Enter an **Admin DN** (distinguished name) in Active Directory format (`name@xxx.yyy`).
5. Enter the admin **Password**, and re-enter the same password for confirmation.

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

6. Click **OK** to save changes.
7. To test your authentication settings, see "Testing Authentication Settings" on page 109.

Figure 65. Active Directory with Global Catalog enabled



Authentication/Accounting Servers

Authentication/Accounting Servers

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

□	Name	Type	Actions
□	Ruckus AD	Active Directory	Edit Clone

Editing (Ruckus AD)

Name	Ruckus AD
Type	● Active Directory ○ LDAP ○ RADIUS ○ RADIUS Accounting ○ TACACS+
Global Catalog	☑ Enable Global Catalog support
IP Address*	192.168.11.17
Port*	3268
Windows Domain Name	domain.ruckuswireles (example: domain.ruckuswireless.com)
Admin DN*	admin@domain.ruckus (example: admin@domain.ruckuswireless.com)
Admin Password*	•••••••
Confirm Password*	•••••••

Search terms ● Include all terms ○ Include any of these terms

Test Authentication Settings

LDAP

ZoneDirector supports several of the most commonly used LDAP servers, including:

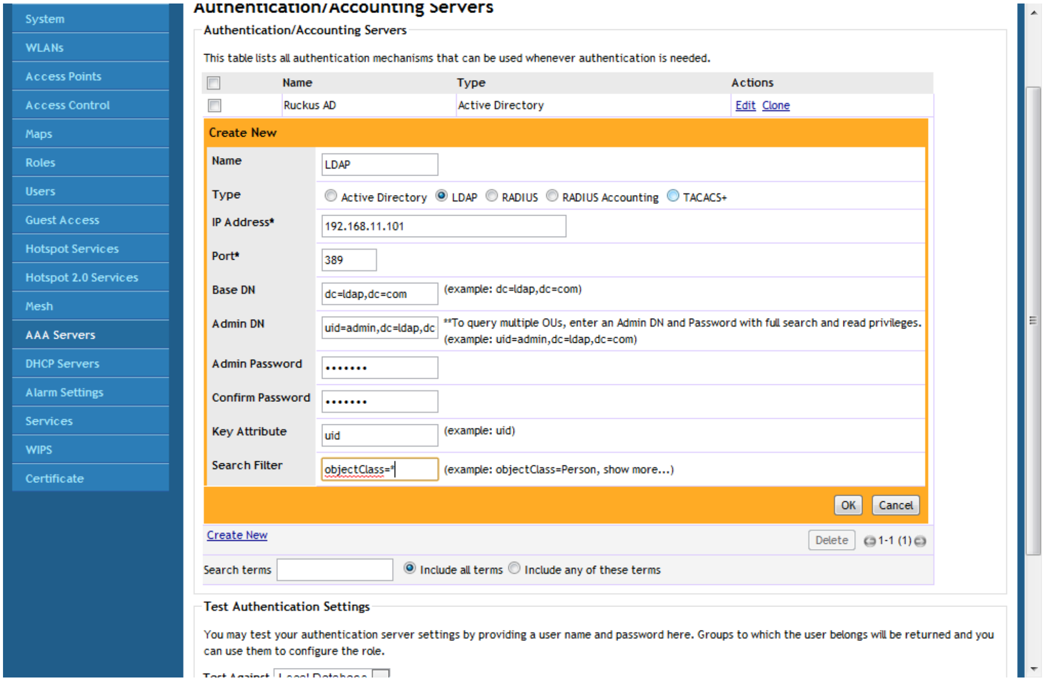
- OpenLDAP
- Apple Open Directory
- Novell eDirectory
- Sun JES (limited support)

To enable LDAP user authentication for all users

1. Click the **Edit** link next to *LDAP* on the **Configure > AAA Servers** page. The *Editing LDAP* form appears.
2. Enter the **IP address** and **Port** of your LDAP server. The default port (389) should not be changed unless you have configured your LDAP server to use a different port.
3. Enter a **Base DN** in LDAP format for all user accounts.
   - Format: `cn=Users;dc=<Your Domain>,dc=com`
4. Enter an **Admin DN** in LDAP format.
   - Format: `cn=Admin;dc=<Your Domain>,dc=com`
5. Enter the **Admin Password**, and reenter to confirm.
6. Enter a **Key Attribute** to denote users (default: uid).
7. Click **OK** to save your changes.
8. If you want to filter more specific settings, see "Advanced LDAP Filtering".

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

Figure 66. Creating a new LDAP server object in ZoneDirector



Authentication/Accounting Servers

Authentication/Accounting Servers

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

□	Name	Type	Actions
□	Ruckus AD	Active Directory	Edit Clone

Create New

Name	LDAP	
Type	○ Active Directory ● LDAP ○ RADIUS ○ RADIUS Accounting ○ TACACS+	
IP Address*	192.168.11.101	
Port*	389	
Base DN	dc=ldap,dc=com	(example: dc=ldap,dc=com)
Admin DN	uid=admin,dc=ldap,dc	**To query multiple OUs, enter an Admin DN and Password with full search and read privileges. (example: uid=admin,dc=ldap,dc=com)
Admin Password	•••••••	
Confirm Password	•••••••	
Key Attribute	uid	(example: uid)
Search Filter	objectClass=*	(example: objectClass=Person, show more...)

OK Cancel

Create New Delete 1-1 (1)

Search terms ● Include all terms ○ Include any of these terms

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.

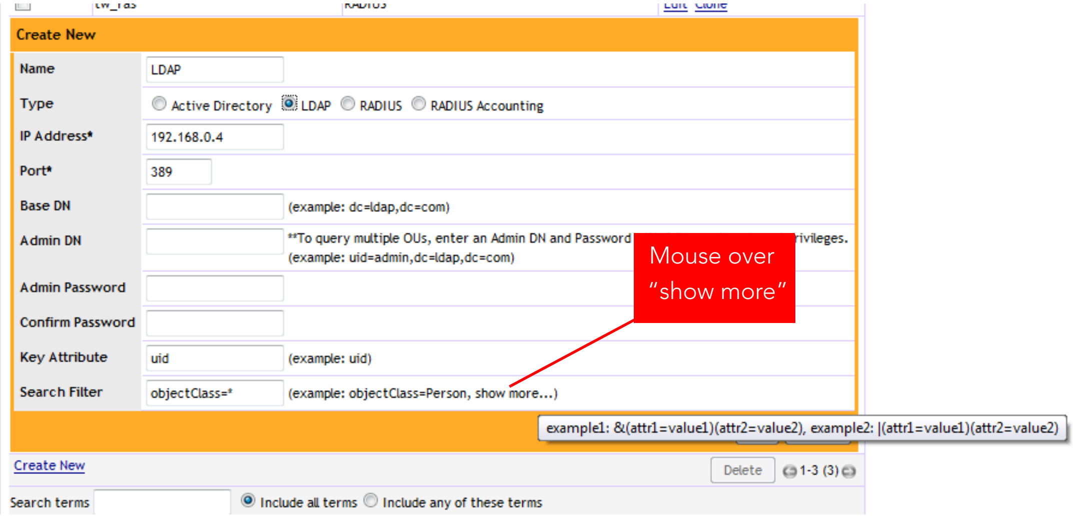
Test Against Local Database

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 67 below.

Figure 67.   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=ldap,dc=com)
Admin DN	**To query multiple OUs, enter an Admin DN and Password rivileges. (example: uid=admin,dc=ldap,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)

Mouse over "show more"

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.

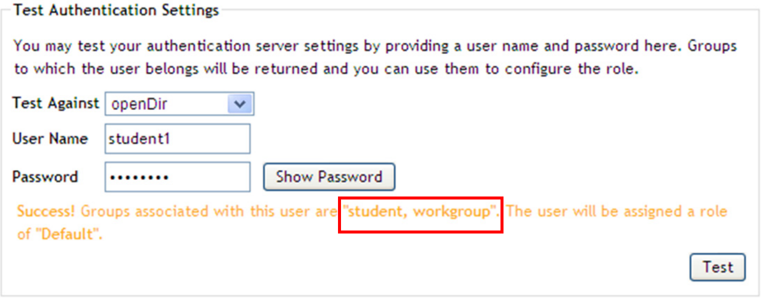
To configure user roles based on LDAP group

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 68. 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: ••••••••

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

7. Go to **Configure > Roles**, and create a Role based on this User Group (see "Creating New User Roles" on page 210).
   - 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.
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.

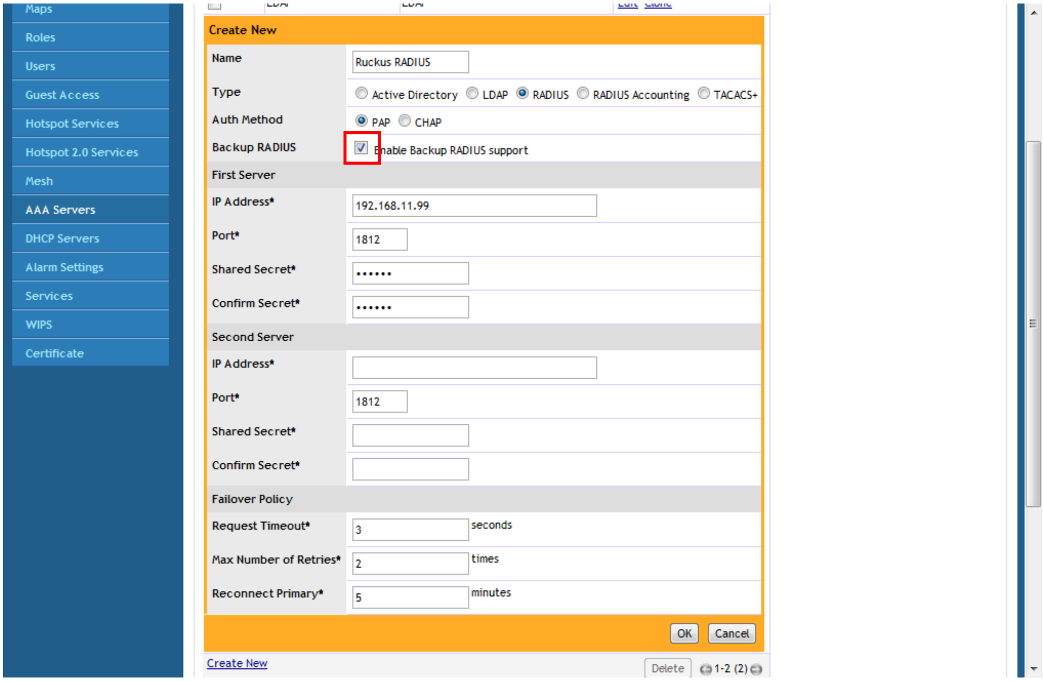
Configuring a Backup RADIUS / RADIUS Accounting Server

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 **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.

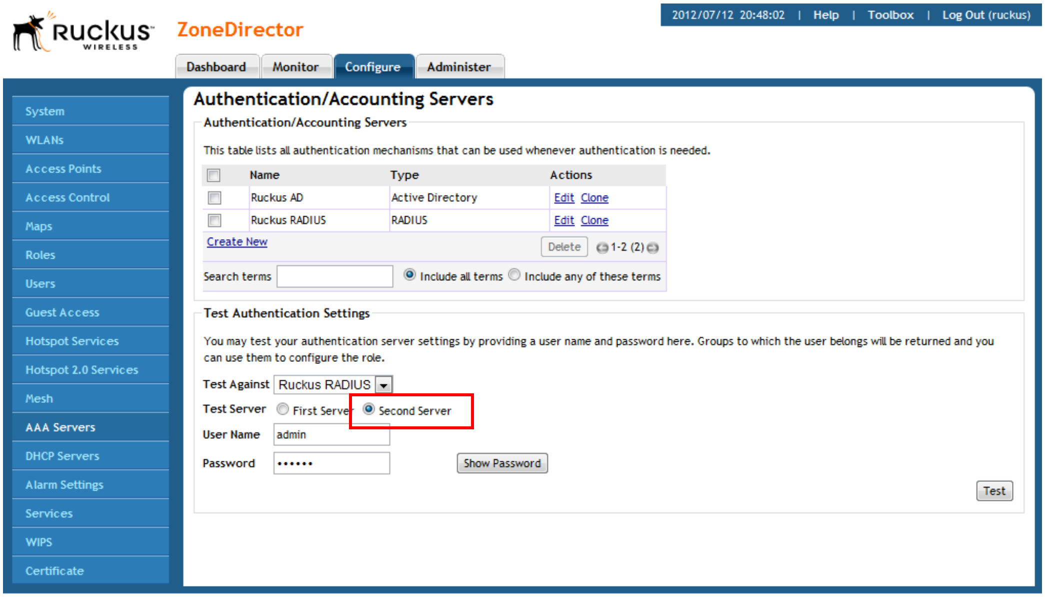
Figure 69. Enable backup RADIUS server



Create New

Name	Ruckus RADIUS
Type	○ Active Directory ○ LDAP ● RADIUS ○ RADIUS Accounting ○ TACACS+
Auth Method	● PAP ○ CHAP
Backup RADIUS	☑ Enable Backup RADIUS support
First Server	
IP Address*	192.168.11.99
Port*	1812
Shared Secret*	••••••
Confirm Secret*	••••••
Second Server	
IP Address*	
Port*	1812
Shared Secret*	
Confirm Secret*	
Failover Policy	
Request Timeout*	3 seconds
Max Number of Retries*	2 times
Reconnect Primary*	5 minutes

Figure 70. Test authentication settings against backup RADIUS server



Authentication/Accounting Servers

Authentication/Accounting Servers

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

□	Name	Type	Actions
□	Ruckus AD	Active Directory	Edit Clone
□	Ruckus RADIUS	RADIUS	Edit Clone

Search terms ● Include all terms ○ Include any of these terms

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.

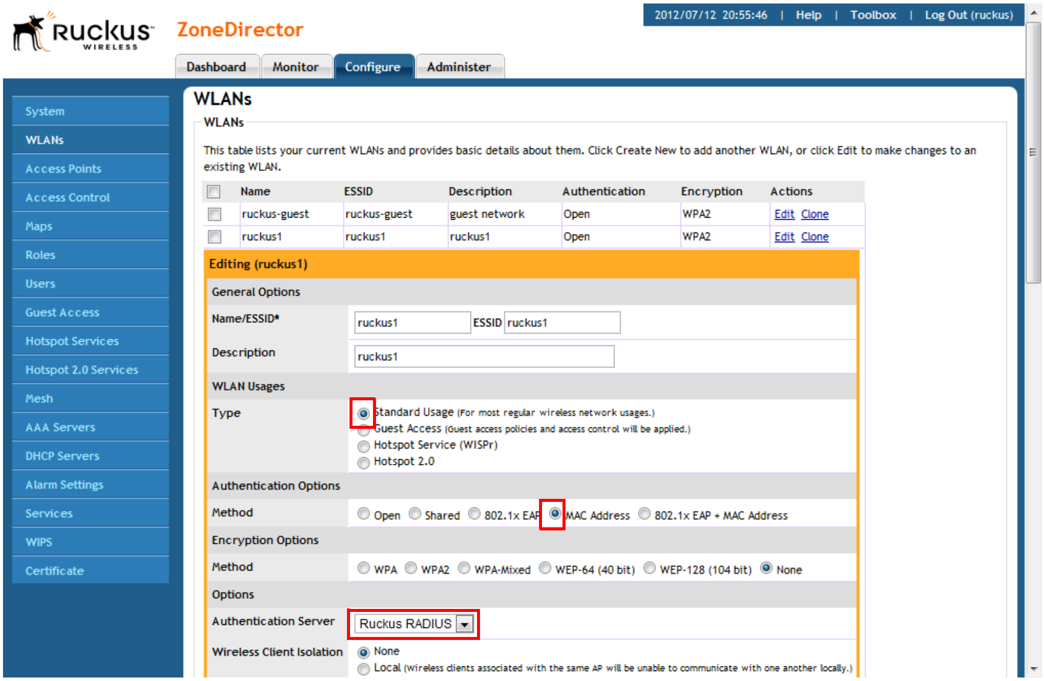
Test Against	Ruckus RADIUS
Test Server	○ First Server ● Second Server
User Name	admin
Password	••••••

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" on page 89.
2. Create a user on the RADIUS server using the MAC address of the client as both the username and password. The MAC address format is a single string of characters without punctuation. (Format: "xxxxxxxxxxxx"; not "xx:xx:xx:xx:xx" or "xx_xx_xx_xx_xx_xx".)
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 (e.g., "internal," "corporate," etc.).
5. Under *Authentication Options: Method*, select **MAC Address**.
6. Under *Authentication Server*, select your **RADIUS Server**.
7. Click **OK** to save your changes.

Figure 71. RADIUS authentication using MAC address



WLANs

WLANs

This table lists your current WLANs and provides basic details about them. Click Create New to add another WLAN, or click Edit to make changes to an existing WLAN.

□	Name	ESSID	Description	Authentication	Encryption	Actions
□	ruckus-guest	ruckus-guest	guest network	Open	WPA2	Edit Clone
□	ruckus1	ruckus1	ruckus1	Open	WPA2	Edit Clone

Editing (ruckus1)

General Options

Name/ESSID* ruckus1 ESSID ruckus1

Description ruckus1

WLAN Usages

Type ● Standard Usage (For most regular wireless network usages.)
○ Guest Access (Guest access policies and access control will be applied.)
○ Hotspot Service (WISPr)
○ Hotspot 2.0

Authentication Options

Method ○ Open ○ Shared ○ 802.1x EAP ● MAC Address ○ 802.1x EAP + MAC Address

Encryption Options

Method ○ WPA ○ WPA2 ○ WPA-Mixed ○ WEP-64 (40 bit) ○ WEP-128 (104 bit) ● None

Options

Authentication Server Ruckus RADIUS

Wireless Client Isolation ● None
○ Local (Wireless clients associated with the same AP will be unable to communicate with one another locally.)

You have completed configuring the WLAN to authenticate users by MAC address from a RADIUS server.

Using 802.1X EAP + MAC Address Authentication

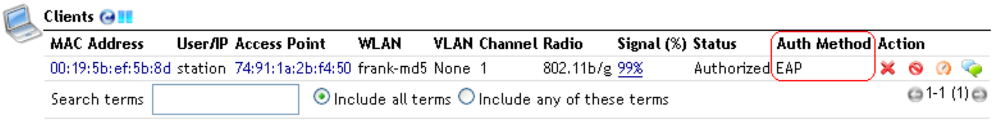
With the 802.1X EAP + MAC Address authentication method, clients configured with either "open" or EAP-MD5 authentication methods are both supported on the same WLAN. The encryption method is limited to "none," and an external RADIUS server is required.

When ZoneDirector authenticates a client, MAC authentication is checked first, followed by the EAP process. When the client tries to associate, if MAC authentication succeeds, the client is authorized directly and allowed to pass traffic without any further EAP authentication required.

If MAC authentication fails, the EAP authentication process begins and the client must provide a valid EAP account before access is granted.

You can view the actual authentication method used (MAC address or EAP) from the **Monitor > Currently Active Clients** page.

Figure 72. The Monitor > Currently Active Clients page shows the actual authentication method used for clients in an 802.1X EAP + MAC Address authentication WLAN



Clients

MAC Address	User/IP	Access Point	WLAN	VLAN	Channel	Radio	Signal (%)	Status	Auth Method	Action
00:19:5b:ef:5b:8d	station	74:91:1a:2b:f4:50	frank-md5	None	1	802.11b/g	99%	Authorized	EAP	

Search terms ● Include all terms ○ Include any of these terms

1-1 (1)

Using 802.1X with EAP-MD5

EAP-MD5 differs from other EAP methods in that it only provides authentication of the EAP peer to the EAP server but not mutual authentication. ZoneDirector supports 802.1X authentication with EAP-MD5 using either ZoneDirector's internal database or an external RADIUS server.

To configure a WLAN for EAP-MD5 authentication

1. Go to **Configure > WLANs** and click the **Edit** link next to the WLAN you would like to configure.
2. Under *Authentication Options: Method*, select **802.1X EAP**.
3. Under *Encryption Options: Method*, select **None**.
4. Under *Authentication Server*, select either **Local Database** or a previously configured RADIUS server from the list.
5. Click **OK** to save your changes.

RADIUS Attributes

Ruckus products communicate with an external RADIUS server as a RADIUS client. Packets from Ruckus products are called "access-request" or "accounting-request" messages. The RADIUS server, in turn, sends an "access-challenge", "access-accept" or "access-reject" message in response to an access-request, and an "accounting-response" message in response to an accounting-request.

RADIUS Attribute Value Pairs (AVP) carry data in both the request and the response messages. The RADIUS protocol also allows vendor specific attributes (VSA) to extend the functionality of the protocol. The following tables list the RADIUS attributes used in these messages between ZoneDirector and the RADIUS/RADIUS Accounting server based on which type of authentication is used for the WLAN. Table 17 lists the attributes used in authentication, and Table 18 lists those used in accounting.

Notation "==>" below indicates this value is generated external to AP/ZoneDirector.

- In the case of EAP payload, this is generated by a wireless client and encapsulated in the radius access-request packet.
- In the case of a "state" attribute, it indicates that an access-request packet is a response to the last received access-challenge packet by copying the "state" AVP unmodified.
- As for the "class" attribute, it is parsed and stored from an access-accept packet and then subsequently used in accounting-request packets.

RADIUS Authentication attributes

Table 17. RADIUS attributes used in authentication

WLAN Type	Attributes
802.1X / MAC Auth	*Sent from ZoneDirector in Access Request messages:* • (1) User name • (4) NAS IP Address (optional; prefer sending NAS ID) • (5) NAS Port • (6) Service Type: hard-coded to be Framed-User(2) • (12) Framed MTU: hard-coded to be 1400 • (30) Called Station ID: user configurable • (31) Calling Station ID: format is sta's mac • (32) NAS Identifier: user configurable • (61) NAS Port Type: hard-coded to be 802.11 port (19) • (77) Connection Info: indicates client radio type • ==> (79) EAP payload • ==> (24) State: if radius access-challenge in last received radius msg from AAA • (80) Message Authenticator • (95) NAS IPv6 address (if using/talking to an IPv6 RADIUS server) • Ruckus private attribute: • Vendor ID: 25053 • Vendor Type / Attribute Number: 3 (Ruckus-SSID)

Table 17. RADIUS attributes used in authentication

WLAN Type	Attributes
802.1X / MAC Auth	*Sent from RADIUS server in Access Accept messages:* • (1) User name • (25) Class • (27) Session-timeout & (29) Termination-action: Session-timeout event becomes a disconnect event or re-authentication event if termination-action indicates "(1) radius-request" • (85) Acct-interim-interval *For Dynamic VLAN application:* • (64) Tunnel-Type: value only relevant if it is (13) VLAN • (65) Tunnel-Medium-Type: value only relevant if it is (6) 802 (as in all 802 media plus ethernet) • (81) Tunnel-Private-Group-ID: this is the VLAN ID assignment (per RFC, this is bettween 1 and 4094) *Administrator Authentication:* • Ruckus private attribute: • Vendor ID: 25053 • Vendor Type / Attribute Number: 1 (Ruckus-User-Groups) • Value Format: group_attr1, group_attr2, group_attr3, ... • Cisco private attribute: • Vendor ID: 9 • Vendor Type/ Attribute Number: 1 (Cisco-AVPair) • Value Format: shell:roles="group_attr1 group_attr2 group_attr3 ..."

Table 17. RADIUS attributes used in authentication

WLAN Type	Attributes
WISPr / Web Auth / Guest Access	*Additional attributes supported in WISPr WLANs (**generic attributes NOT the same as non-WISPr/802.1X)* • (1) User name • (2) Password or (3) CHAP-Password • (4) NAS IP Address • (6) Service Type: hardcoded to be Framed-User(2) • (8) Framed IP address • (30) Called Station ID: user configurable • (31) Calling Station ID: format is sta's mac • (32) NAS Identifier: user configurable • (44) Account session ID • Ruckus private attribute: • Vendor ID: 25053 • Vendor Type / Attribute Number: 3 (Ruckus-SSID) • WISPr vendor specific attribute (vendor id = 14122) • (1) WISPr location id • (2) WISPr location name • (4) WISPr redirection URL • (7) WISPr Bandwidth-Max-Up: Maximum transmit rate (bits/second) • (8) WISPr Bandwidth-Max-Down: Maximum receive rate (bits/second) • (80) Message Authenticator

RADIUS Accounting attributes

The following table lists attributes used in RADIUS accounting messages.

Table 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
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

Table 18. RADIUS attributes used in Accounting

WLAN Type	Attribute
802.1X / MAC Auth	*Sent from RADIUS server in Accept messages:* • (1) User name • (25) Class • (85) Acct-interim-interval • (27) Session-timeout & (29) Termination-action: Session-timeout event becomes a disconnect event or re-authentication event if termination-action indicates "(1) radius-request" *For Dynamic VLAN application:* • (64) Tunnel-Type: value only relevant if it is (13) VLAN • (65) Tunnel-Medium-Type: value only relevant if it is (6) 802 (as in all 802 media plus Ethernet) • (81) Tunnel-Private-Group-ID: this is the VLAN ID assignment (per RFC, this is between 1 and 4094)
WISPr / Web Auth / Guest Access	*Common to Start, Interim Update, and Stop messages:* • (1) User name • (2) Password • (4) NAS IP address • (5) NAS port • (8) Framed-IP • (30) Called station ID: user configurable • (31) Calling station ID • (32) NAS Identifier: user configurable • (45) Acct authentic • (50) Acct-Multi-Session-Id • (61) NAS port type • (77) Connection Info: indicates client radio type • Ruckus private attribute: • Vendor ID: 25053 • Vendor Type / Attribute Number: 3 (Ruckus-SSID) *Additional attributes supported in WISPr WLANs:* • WISPr vendor specific attributes (vendor id = 14122) • (1) WISPr location id • (2) WISPr location name • (4) WISPr redirection URL • (7) WISPr Bandwidth-Max-Up: Maximum transmit rate (bits/second) • (8) WISPr Bandwidth-Max-Down: Maximum receive rate (bits/second)

Table 18. RADIUS attributes used in Accounting

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

Configuring Microsoft IAS for PAP Authentication

If you are using Microsoft Internet Authentication Service (IAS) as your RADIUS server and PAP authentication, you will need to configure your user/group profiles to use only PAP authentication rather than the default (MS-CHAP). If you selected CHAP under "RADIUS / RADIUS Accounting", you do not need to configure IAS for PAP authentication.

To configure user/group profiles for PAP authentication

1. From the Internet Authentication Service main page, select the user or group for which you want to configure PAP authentication.
2. Right-click the user or group and select **Properties** to open the [user/group name] Properties dialog box.
3. 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 73. On the Microsoft IAS page, right-click the user/group and select Properties.

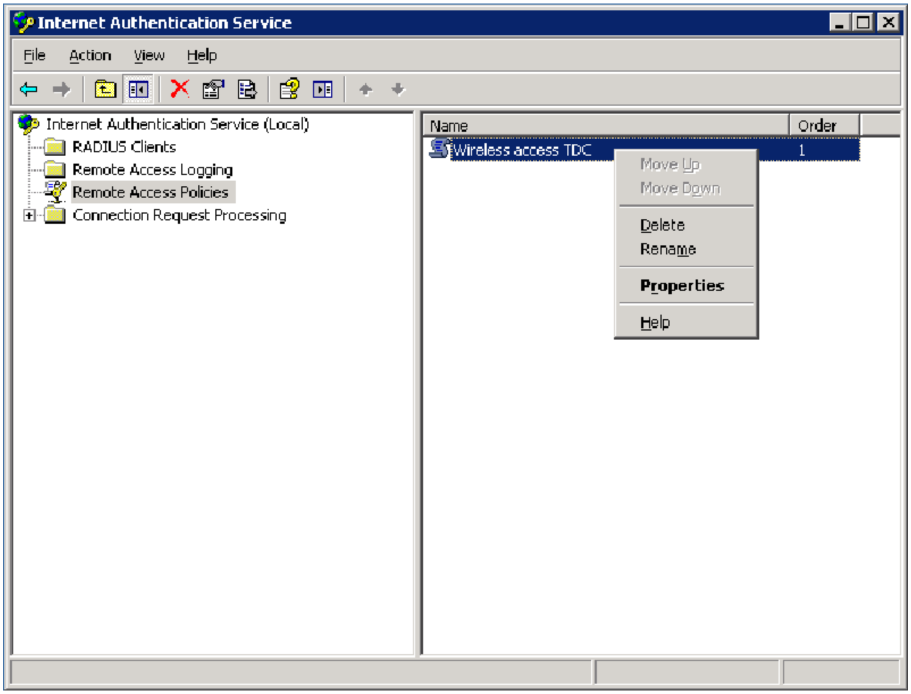
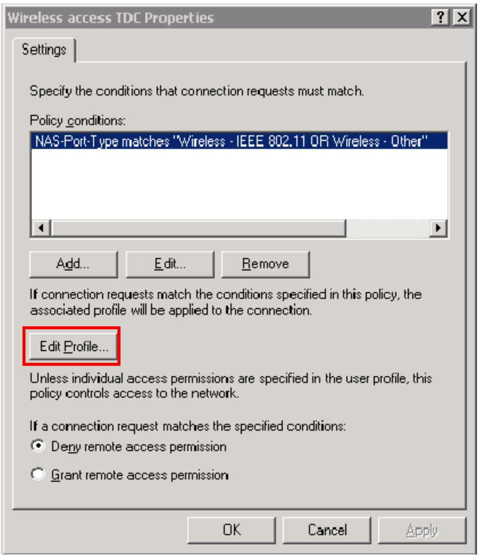


Figure 74. On the Properties page, click Edit Profile...



Specify the conditions that connection requests must match.

Policy conditions:

NAS-Port-Type matches "Wireless - IEEE 802.11 OR Wireless - Other"

If connection requests match the conditions specified in this policy, the associated profile will be applied to the connection.

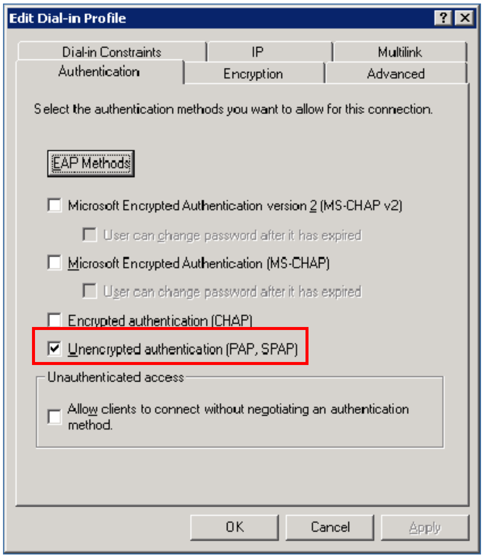
Unless individual access permissions are specified in the user profile, this policy controls access to the network.

If a connection request matches the specified conditions:

● Deny remote access permission

○ Grant remote access permission

Figure 75. On the Authentication tab of the Edit Dial-in Profile dialog, select Unencrypted authentication (PAP, SPAP)



Edit Dial-in Profile

Select the authentication methods you want to allow for this connection.

□ Microsoft Encrypted Authentication version 2 (MS-CHAP v2)

□ User can change password after it has expired

□ Microsoft Encrypted Authentication (MS-CHAP)

□ User can change password after it has expired

□ Encrypted authentication (CHAP)

☑ Unencrypted authentication (PAP, SPAP)

Unauthenticated access

□ Allow clients to connect without negotiating an authentication method.

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)

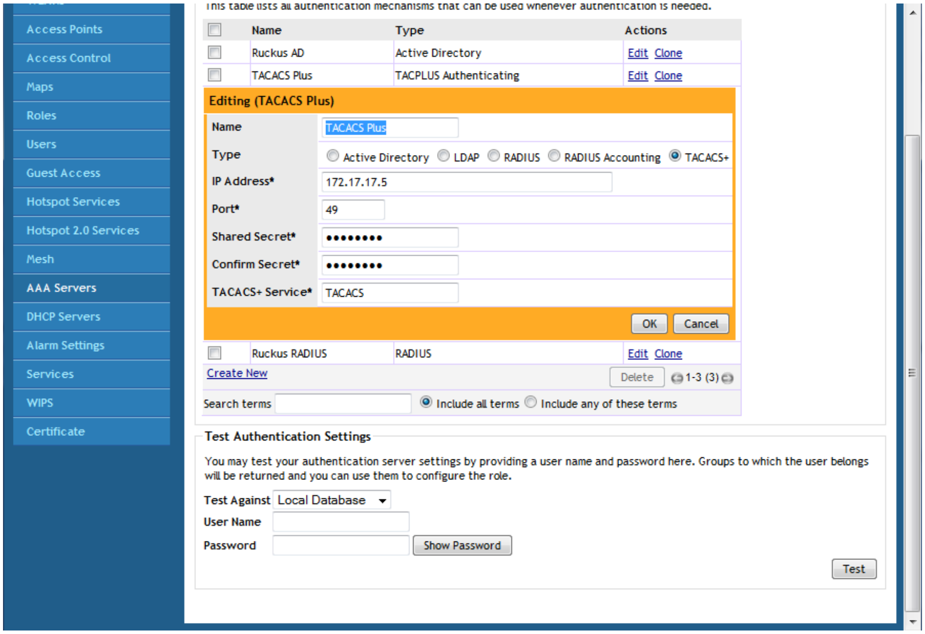
TACACS+ is an extensible AAA protocol that provides customization and future development features, and uses TCP to ensure reliable delivery. The daemon should listen at port 49 which is the "login" port assigned for the TACACS protocol.

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 76. Configuring a TACACS+ AAA server



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

□	Name	Type	Actions
□	Ruckus AD	Active Directory	Edit Clone
□	TACACS Plus	TACPLUS Authenticating	Edit Clone

Editing (TACACS Plus)

Name	TACACS Plus
Type	○ Active Directory ○ LDAP ○ RADIUS ○ RADIUS Accounting ● TACACS+
IP Address*	172.17.17.5
Port*	49
Shared Secret*	••••••••
Confirm Secret*	••••••••
TACACS+ Service*	TACACS

OK Cancel

□	Ruckus RADIUS	RADIUS	Edit Clone

Create New   Delete   1-3 (3)

Search terms ● Include all terms ○ Include any of these terms

Test Authentication Settings

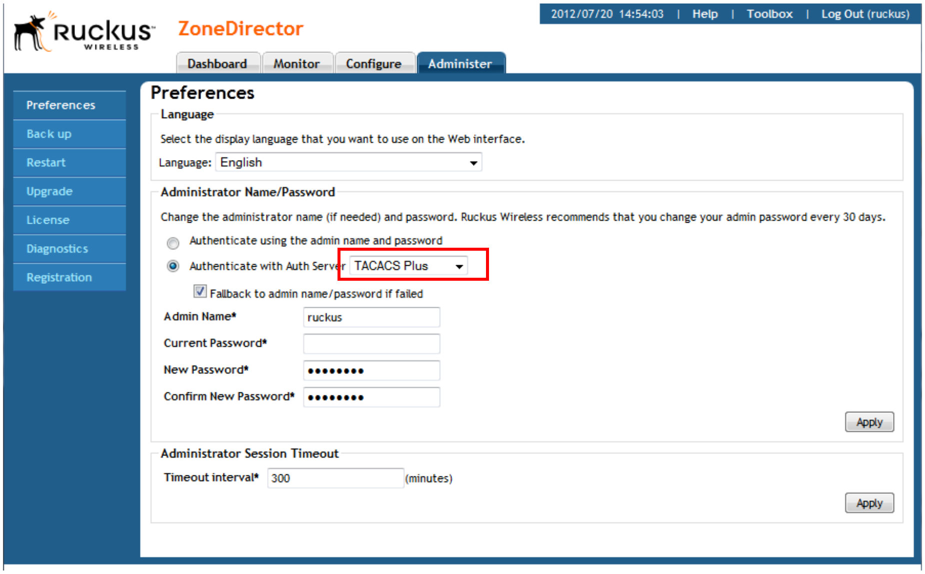
You may test your authentication server settings by providing a user name and password here. Groups to which the user belongs will be returned and you can use them to configure the role.

Test Against: Local Database
User Name
Password   Show Password

Test

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 77. Select TACACS+ for ZoneDirector administrator authentication



Preferences

Language

Select the display language that you want to use on the Web interface.

Language: English

Administrator Name/Password

Change the administrator name (if needed) and password. Ruckus Wireless recommends that you change your admin password every 30 days.

○ Authenticate using the admin name and password

● Authenticate with Auth Server TACACS Plus

☑ Fallback to admin name/password if failed

Admin Name*	ruckus
Current Password*	
New Password*	••••••••
Confirm New Password*	••••••••

Administrator Session Timeout

Timeout interval* 300 (minutes)

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.

4

Managing a Wireless Local Area Network

In This Chapter

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 for "standard" client devices, those clients running Windows XP SP2 (or later), Windows Vista, Windows 7 or Mac OS X, and utilizing WPA-ready NICs.

There are several scenarios in which you will want to create additional WLANs, in addition to the default 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 are as follows:

Table 19. Max WLANs by ZoneDirector model

Model	Max WLANs
ZoneDirector 1100	128
ZoneDirector 3000	1024
ZoneDirector 5000	2048

The maximum number of WLANs deployable per AP radio is eight. If an AP is in mesh mode, the maximum number of WLANs deployable per radio is six, since the mesh uses two SSIDs (this applies to both radios on dual-band APs).

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 (no authentication)
- Shared (a single key shared among all users)
- 802.1X EAP
- MAC Address
- 802.1X EAP + MAC Address

Encryption options depend on which type of authentication is chosen. Even with Open authentication, you can still encrypt WLAN traffic using WPA, WPA2 or WEP encryption. If you choose Shared authentication, you will only be able to use WEP encryption, because WPA and WPA2 use unique dynamically generated keys. WPA/WPA2 provides increased security, but limits flexibility because some older client devices do not support the newer standards.

802.1X EAP is a very secure authentication/encryption method that requires a backend authentication server such as a RADIUS server. Your choice mostly depends on what kinds of authentication your users' client devices support and your local network authentication environment.

One drawback to 802.1X is the more labor-intensive setup, which can require (among other tasks) the transfer of root certificate copies to your users, who must then import the certificates into their client devices. This task can be automated by using the Ruckus Wireless Zero-IT Activation, which significantly reduces the amount of setup required.

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.

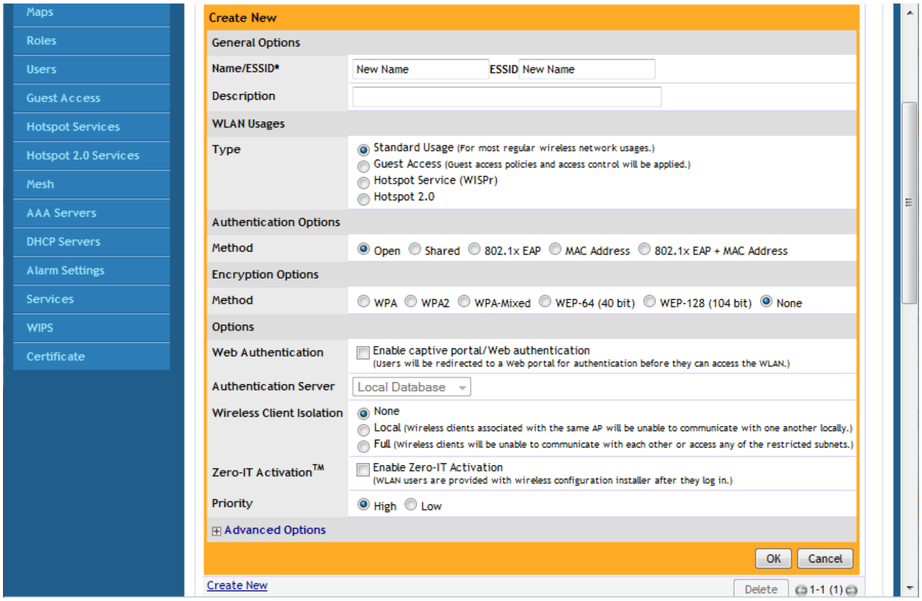
The 802.1X EAP + MAC Address authentication option allows clients to authenticate to the same WLAN using either MAC address or 802.1X authentication.

All client authentication options (Open, Shared, 802.1X and MAC Address) are detailed in "Creating a WLAN" on page 114, and you can learn how to apply them to your WLANs in the same section.

Creating a 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 78. Creating a new WLAN



Create New

General Options

Name/ESSID* New Name ESSID New Name

Description

WLAN Usages

Type
- ● Standard Usage (For most regular wireless network usages.)
- ○ Guest Access (Guest access policies and access control will be applied.)
- ○ Hotspot Service (WISPr)
- ○ Hotspot 2.0

Authentication Options

Method ● Open ○ Shared ○ 802.1x EAP ○ MAC Address ○ 802.1x EAP + MAC Address

Encryption Options

Method ○ WPA ○ WPA2 ○ WPA-Mixed ○ WEP-64 (40 bit) ○ WEP-128 (104 bit) ● None

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

Wireless Client Isolation
- ● None
- ○ Local (Wireless clients associated with the same AP will be unable to communicate with one another locally.)
- ○ Full (Wireless clients will be unable to communicate with each other or access any of the restricted subnets.)

Zero-IT Activation™ □ Enable Zero-IT Activation
(WLAN users are provided with wireless configuration installer after they log in.)

Priority ● High ○ Low

⊞ Advanced Options

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" on page 115.

Table 20. Create new WLAN options

Option	Description
General Options	Enter WLAN name and description.
WLAN Usages	Select usage type (standard, guest access, hotspot).
Authentication Options	Select an authentication method for this WLAN (open, shared key, 802.1X EAP, MAC address).
Encryption Options	Select encryption method (WPA, WPA2, WPA-Mixed, WEP), encryption algorithm (AES or TKIP) and enter a WPA passphrase/WEP key.

Table 20. Create new WLAN options

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

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" on page 210.

General Options

- *Name/ESSID*: Type a short name for this WLAN. The maximum SSID length can contain between 2 and 32 characters, including characters from ! (char 33) to ~ (char 126).
  - 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

To create a WLAN with specific options, choose "Standard Usage." If you have configured Hotspot services (see "Creating a Hotspot Service" on page 138), you can enable Hotspot service on this new WLAN. Additionally, you can select a default "Guest Access" WLAN with open access and customizable encryption (see "Configuring Guest Access" on page 216). Guest WLANs are subject to guest access policies, such as redirection and subnet access restrictions.

CAUTION: When Guest Usage 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 Usage and Wireless Client Isolation options are disabled. For more information on SpeedFlex, refer to "Measuring Wireless Network Throughput with SpeedFlex" on page 276.

Authentication Method

Authentication Method defines the method by which users are authenticated prior to gaining access to the WLAN. The level of security should be determined by the purpose of the WLAN you are creating.

- *Open* [Default]: No authentication mechanism is applied to connections. If WPA or WPA2 encryption is used, this implies WPA-PSK authentication.
- *Shared*: If you click **Shared**, only WEP encryption will be available, and the WEP Key option appears. The Shared authentication type requires creation of a WEP key that is shared by all users. ***Note that because WEP encryption is easily circumvented, Shared authentication provides little security and should not 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" on page 98.

Encryption Options

Encryption choices include WPA, WPA2, WPA-Mixed, WEP and none. WPA and WPA2 are both encryption methods certified by the WiFi Alliance and are the recommended encryption methods. The Wi-Fi Alliance will be mandating the removal of WEP due to its security vulnerabilities, and Ruckus Wireless recommends against using WEP if possible.

Method

- *WPA*: Standard Wi-Fi Protected Access with either TKIP or AES encryption.
- *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 40-bit WEP encryption.
- *WEP-128*: Provides a higher level of encryption than WEP-64, using a 104-bit key for WEP encryption. However, WEP is inherently less secure than WPA.

- *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 AP for the WLAN, the WLAN will operate in 802.11g mode.

Algorithm (Only for WPA or WPA2 encryption methods)

- *TKIP*: This algorithm provides greater compatibility with older client devices, but retains many of the security weaknesses of WEP. Therefore, if you select TKIP encryption, 11n devices will be limited to 11g transfer rates. Furthermore, the Wi-Fi Alliance will be mandating the removal of TKIP, so it should not be used.
- *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 APs will be at lower 11g rates).

CAUTION: If you set the encryption algorithm to TKIP and you are using an 802.11n 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 be up to 10 characters in length. If it is for WEP 128 encryption, enter a key up to 26 characters in length.
- *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" or "Shared" 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" on page 213).
- *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" on page 212).

- *Wireless Client Isolation*: Wireless client isolation enables subnet restrictions for connected clients. Options are:
  - *None*: Clients associated with this WLAN are not isolated and have full access to communicate with each other and any other nodes on the local network.
  - *Local*: Clients can not communicate with each other on the same WLAN, but can access other resources on the local network. When you configure *Local* client isolation, isolation is made using Layer 2 but applies only to clients connected to the same radio and SSID on the same AP.
  - *Full*: When full wireless client isolation is enabled, stations associated to this WLAN will not be able to communicate with each other or access the local LAN; rather, they can only access the Internet. Access controls will be exactly the same as for those that associate to a guest WLAN -- the same guest policy will be applied to a guest WLAN as to a WLAN with wireless client isolation enabled. When you configure *Full* client isolation, isolation is made using a Layer 3 ACL. This L3 ACL is defined in the Guest Access tab, which blocks all traffic to private (10.x, 192.x, etc.) IP addresses by default.The only difference between a WLAN with wireless client isolation enabled and a guest WLAN is that a guest WLAN requires users to enter a guest pass before they can access the network. To restrict access to certain subnets, see "Configuring Guest Subnet Access" on page 227.

CAUTION: The SpeedFlex wireless performance tool may not work properly if wireless client isolation is enabled on the WLAN. 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.

- *Zero-IT Activation*: Enable this option to activate ZoneDirector's share in the automatic "new user" process, in which the new user's PC is easily and quickly configured for WLAN use. For more information, see "Enabling Automatic User Activation with Zero-IT" on page 202.
- *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" on page 146.
- *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 the ACL to apply to this WLAN. An ACL must be created before being available here. For more information, see "Configuring Access Control Lists" on page 77.
- *Call Admission Control*: (Disabled by default). Enable Wi-Fi Multimedia Admission Control (WMM-AC) to support Polycom/Spectralink VIEW certification. When enabled, the AP announces in beacons if admission control is mandatory or not for various access categories and admits only the traffic streams it can support based on available network resources. When network resources are not sufficient to provide this level of performance, the new traffic stream is not admitted. Call Admission Control is effective only when both AP and the client support WMM-AC. Ruckus APs are capable of handling hundreds of simultaneous clients, but when it comes to VoIP traffic, the number of VoIP calls needs to be policed to ensure adequate voice/video quality. Ruckus recommends limiting bandwidth allocation to six calls (four active calls and two reserved for roaming) on the 2.4 GHz radio and 10 calls on the 5 GHz radio (seven active and three reserved for roaming). Enable this feature if you want this WLAN to serve as a VoIP WLAN to support Spectralink phones. (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" on page 135 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: Note that Wireless Distribution System (WDS) clients, for example, MediaFlex 7211/ 2111 adapters, do not work when the ZoneDirector WLAN is in 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" *on page 63*.
- *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" on page 68).
- *Load Balancing*: Client load balancing between APs is disabled by default on all WLANs. To disable load balancing for this WLAN, check this box. Ruckus Wireless recommends disabling load balancing on WLANs used for voice. For more information, see "Load Balancing" on page 178.
- *Max Clients*: Limit the number of clients that can associate with this WLAN per AP (default is 100). You can also limit the total number of clients that a specific AP (or radio, on dual radio APs) will manage. See "Reviewing Current Access Point Policies" on page 169 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.

- *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" on page 162 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.
- *Grace Period*: Allows disconnected users a grace period after disconnection, during which clients will not need to re-authenticate, on any WLAN that requires authentication.
- *Client Tx/Rx Statistics*: Enable this option to ignore unauthorized client statistics and report only statistics from authorized clients in device view and other reports. This can be useful for service providers who are more interested in accounting statistics (after authorization) than in all wireless client statistics. For example, a Hotspot WLAN can be configured to allow unauthorized clients to connect and traverse any walled garden web pages without adding to transmission statistics (until after authorization).
- *Client Fingerprinting*: When this option is enabled ZoneDirector will attempt to identify client devices by their Operating System, device type and Host Name, if available. This makes identifying client devices easier in the Dashboard, Client Monitor and Client Details screens.
- *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" on page 45.

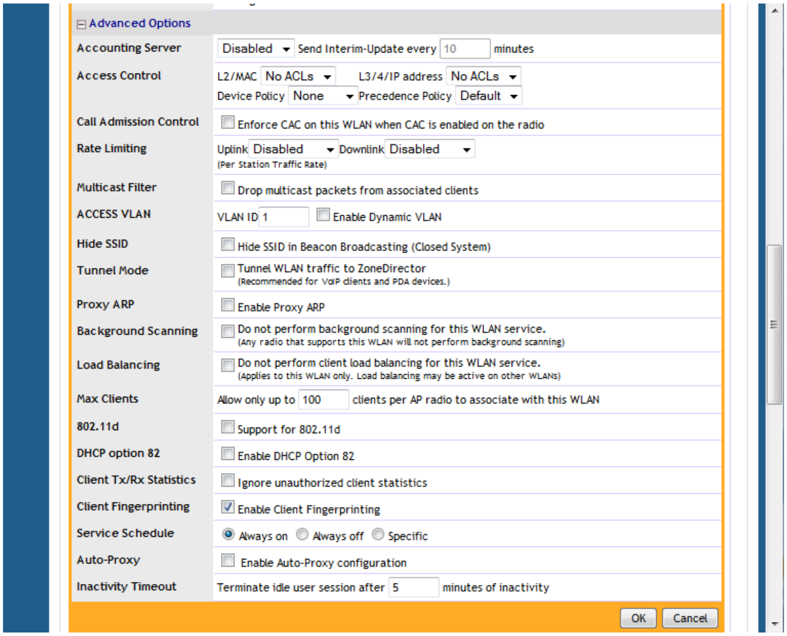
NOTE: WLAN service will be enabled and disabled based on ZoneDirector's system time, and not the time zone where the access point is located. These may be different local times if ZoneDirector and the access points are in different time zones.

- *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, 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.

- *Inactivity Timeout*: Enable the check box and enter a value in minutes after which idle stations will be disconnected (1 to 500 minutes).

Figure 79. Advanced options for creating a new WLAN



⊟ Advanced Options

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 ▾

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

ACCESS VLAN: VLAN ID 1 □ 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 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)

Max Clients: Allow only up to 100 clients per AP radio to associate with this WLAN

802.11d: □ Support for 802.11d

DHCP option 82: □ Enable DHCP Option 82

Client Tx/Rx Statistics: □ Ignore unauthorized client statistics

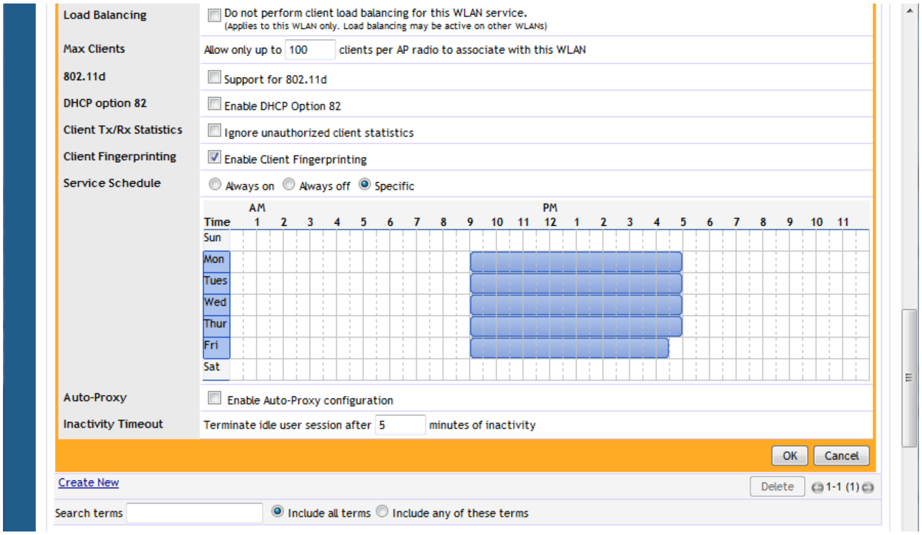
Client Fingerprinting: ☑ Enable Client Fingerprinting

Service Schedule: ● Always on ○ Always off ○ Specific

Auto-Proxy: □ Enable Auto-Proxy configuration

Inactivity Timeout: Terminate idle user session after 5 minutes of inactivity

Figure 80. Configuring WLAN service schedule



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)

Max Clients: Allow only up to 100 clients per AP radio to associate with this WLAN

802.11d: □ Support for 802.11d

DHCP option 82: □ Enable DHCP Option 82

Client Tx/Rx Statistics: □ Ignore unauthorized client statistics

Client Fingerprinting: ☑ Enable Client Fingerprinting

Service Schedule: ○ Always on ○ Always off ● Specific

AM / PM
Time 1 2 3 4 5 6 7 8 9 10 11 12 1 2 3 4 5 6 7 8 9 10 11
Sun
Mon
Tues
Wed
Thur
Fri
Sat

Auto-Proxy: □ Enable Auto-Proxy configuration

Inactivity Timeout: Terminate idle user session after 5 minutes of inactivity

Search terms ● Include all terms ○ Include any of these terms

Creating a New 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**.

   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).
3. If you have no need for custom authentication or encryption methodologies in this new WLAN, locate the default WLAN record and click **Clone**.

   A workspace appears, displaying the default settings of a new WLAN, using the same configuration settings as the default WLAN.
4. Type a descriptive name for this WLAN, and then click **OK**. This new WLAN is ready for use by selected users.
5. You can now assign access to this new WLAN to a limited set of internal users, as detailed in "Creating New User Roles" on page 210.

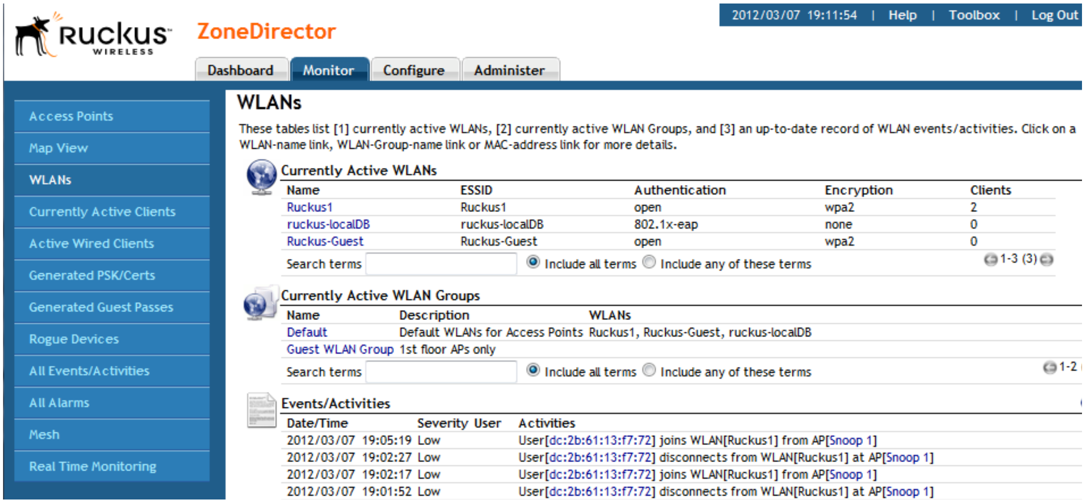
Customizing WLAN Security

The default security method for your internal WLAN incorporates a WPA2-based authentication passphrase and the AES encryption algorithm, and utilizes dynamic pre-shared keys. To review the default WLAN configurations 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 when you worked through the ZoneDirector Setup Wizard. You can review the details of a WLAN's configuration by clicking the WLAN name. See Figure 81.
3. You have three options with the internal WLAN: [1] continue using the current configuration, [2] fine-tune the existing security mode, or [3] replace this mode entirely with either an 802.1X mode or a WEP-based mode. The two WLAN-editing processes are described separately, below.

Figure 81. The Monitor > WLANs page



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 link, WLAN-Group-name link or MAC-address link for more details.

Currently Active WLANs

Name	ESSID	Authentication	Encryption	Clients
Ruckus1	Ruckus1	open	wpa2	2
ruckus-localDB	ruckus-localDB	802.1x-eap	none	0
Ruckus-Guest	Ruckus-Guest	open	wpa2	0

Search terms ● Include all terms ○ Include any of these terms 1-3 (3)

Currently Active WLAN Groups

Name	Description	WLANs
Default	Default WLANs for Access Points	Ruckus1, Ruckus-Guest, ruckus-localDB
Guest WLAN Group	1st floor APs only	

Search terms ● Include all terms ○ Include any of these terms 1-2

Events/Activities

Date/Time	Severity	User	Activities
2012/03/07 19:05:19	Low		User[dc:2b:61:13:f7:72] joins WLAN[Ruckus1] from AP[Snoop 1]
2012/03/07 19:02:27	Low		User[dc:2b:61:13:f7:72] disconnects from WLAN[Ruckus1] at AP[Snoop 1]
2012/03/07 19:02:17	Low		User[dc:2b:61:13:f7:72] joins WLAN[Ruckus1] from AP[Snoop 1]
2012/03/07 19:01:52	Low		User[dc:2b:61:13:f7:72] disconnects from WLAN[Ruckus1] at AP[Snoop 1]

Fine-Tuning the Current Security Mode

To keep the original WPA 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 WPA encryption with no authentication (Open Auth).
   - *WPA2*: Switch to this encryption method if you prefer the IEEE 802.11i standard, which provides the highest level of security, but is limited to devices with newer wireless NICs.
   - *WPA-Mixed*: Allows both WPA and WPA2 compliant devices to access the network.
   - *AES*: Switch to this algorithm for stronger encryption.
   - *Passphrase*: Replace the current passphrase with a new one, to help lower the risk of unauthorized access.
4. Click **OK** to apply any changes.

Switching to a Different Security Mode

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

- Open Auth/WEP encryption: Least security, only use if necessary to support older WEP-only client devices.
- Open Auth/WPA encryption: Less security than WPA2, but better than WEP.

- Open Auth/WPA-Mixed encryption: Allows both WPA and WPA2 devices on the same WLAN.
- Shared Auth/WEP encryption: Same as Open Auth.
- 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, Shared, 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.
   - **Shared** limits you to WEP-key encryption.
   - **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.

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" on page 204). Once this is done, users can connect to the internal WLAN using 802.1X/EAP authentication.

Authenticating with an External RADIUS Server

You can also use an external RADIUS server for your wireless client 802.1X/EAP authentication. An EAP-aware RADIUS server is required for this application. Also, you might need to deploy your own certificates for wireless client devices and for the RADIUS server you are using. In this case, ZoneDirector works as a bridge between your wireless clients and the RADIUS server during the wireless authentication process.

ZoneDirector allows wireless clients to access the networks only after successful authentication of the wireless clients by the RADIUS server. For information on configuring a RADIUS server for client authentication, see "RADIUS / RADIUS Accounting" on page 94.

⚠ **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 WPA 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 eight WLANs that you create are automatically assigned to this Default WLAN group.

NOTE: A WLAN Group can include a maximum of eight member WLANs. If Smart Mesh is enabled, the maximum number of WLANs in a WLAN group is six. 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.

Figure 82. Maximum number of WLAN groups by ZoneDirector model

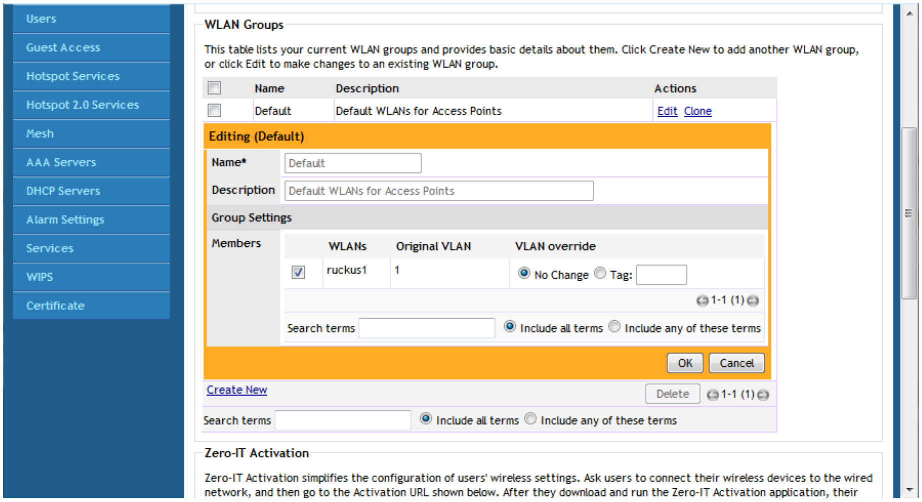
ZoneDirector Model	Max WLAN Groups
ZoneDirector 1100	128
ZoneDirector 3000	1024
ZoneDirector 5000	2048

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 83. WLAN group



WLAN Groups

This table lists your current WLAN groups and provides basic details about them. Click Create New to add another WLAN group, or click Edit to make changes to an existing WLAN group.

□	Name	Description	Actions
□	Default	Default WLANs for Access Points	Edit Clone

Editing (Default)

Name*: Default

Description: Default WLANs for Access Points

Group Settings

Members

	WLANs	Original VLAN	VLAN override
☑	ruckus1	1	● No Change ○ Tag:

1-1 (1)

Search terms ● Include all terms ○ Include any of these terms

OK Cancel

Create New · Delete · 1-1 (1)

Search terms ● Include all terms ○ Include any of these terms

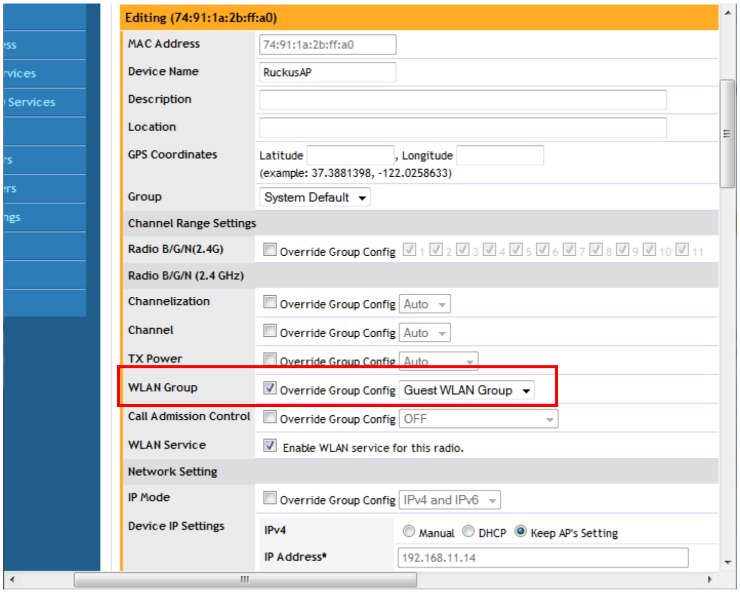
Zero-IT Activation

Zero-IT Activation simplifies the configuration of users' wireless settings. Ask users to connect their wireless devices to the wired network, and then go to the Activation URL shown below. After they download and run the Zero-IT Activation application, their

Assigning a WLAN Group to an AP

1. Go to **Configure** > **Access Points**.
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 84. *Assign a WLAN group to an AP*



Editing (74:91:1a:2b:ff:a0)

MAC Address: 74:91:1a:2b:ff:a0
Device Name: RuckusAP
Description:
Location:
GPS Coordinates: Latitude , Longitude
(example: 37.3881398, -122.0258633)
Group: System Default

Channel Range Settings
Radio B/G/N(2.4G): □ Override Group Config ☑ 1 ☑ 2 ☑ 3 ☑ 4 ☑ 5 ☑ 6 ☑ 7 ☑ 8 ☑ 9 ☑ 10 ☑ 11

Radio B/G/N (2.4 GHz)
Channelization: □ Override Group Config Auto
Channel: □ Override Group Config Auto
TX Power: □ Override Group Config Auto
WLAN Group: ☑ Override Group Config Guest WLAN Group
Call Admission Control: □ Override Group Config OFF
WLAN Service: ☑ Enable WLAN service for this radio.

Network Setting
IP Mode: □ Override Group Config IPv4 and IPv6
Device IP Settings: IPv4 ○ Manual ○ DHCP ● Keep AP's Setting
IP Address*: 192.168.11.14

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:

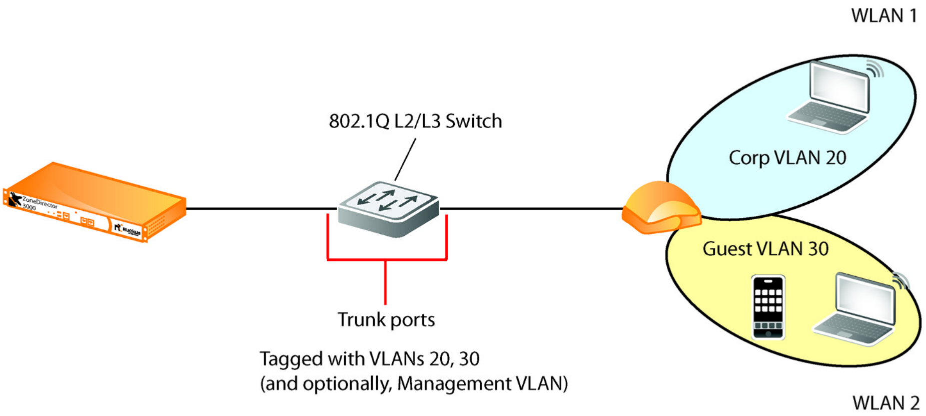
- Verifying that the VLAN switch supports native VLANs. A *native VLAN* is a VLAN that allows the user to designate untagged frames going in/out of a port to a specific VLAN.

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 85): VLAN 20 is used for internal clients, VLAN 30 is used for guest clients, and Management VLAN configuration is optional.

Figure 85. 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.

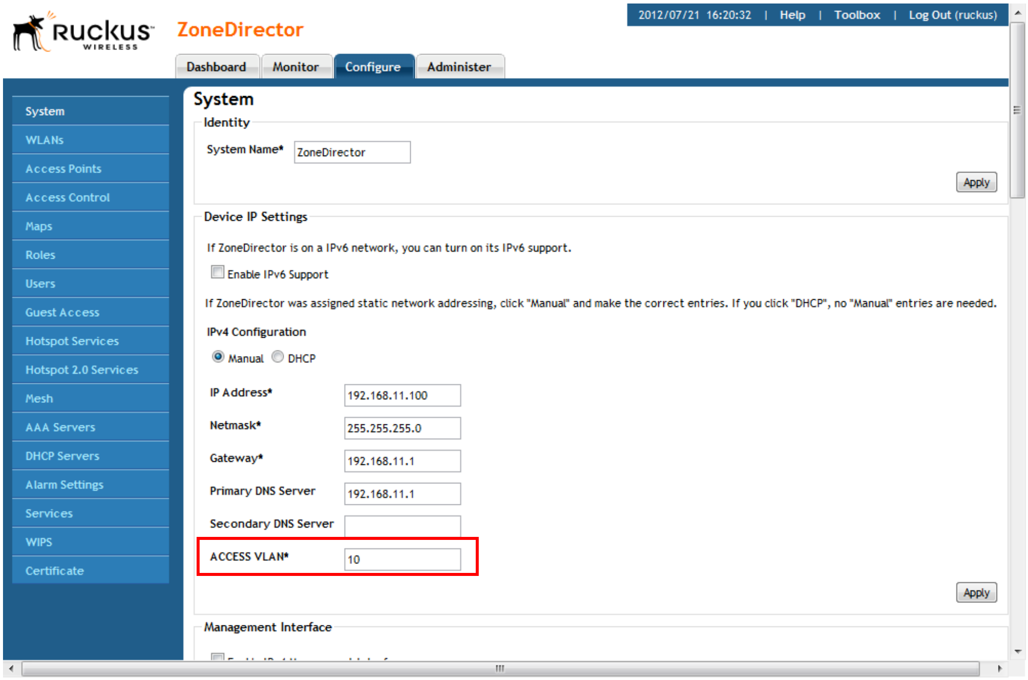
1. Click **Apply** to save your settings.
2. Go to **Configure > System**.
3. In *Device IP Settings*, enter the VLAN ID in the **Access VLAN** field.
4. If you are using an additional management interface for ZoneDirector, enter the same ID in the **Access VLAN** field for the additional management interface.
5. Click **Apply** to save your settings.

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

6. 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 86. Configuring management VLAN for ZoneDirector



System

Identity

System Name* ZoneDirector

Device IP Settings

If ZoneDirector is on a IPv6 network, you can turn on its IPv6 support.

□ Enable IPv6 Support

If ZoneDirector was assigned static network addressing, click "Manual" and make the correct entries. If you click "DHCP", no "Manual" entries are needed.

IPv4 Configuration

● Manual ○ DHCP

IP Address* 192.168.11.100

Netmask* 255.255.255.0

Gateway* 192.168.11.1

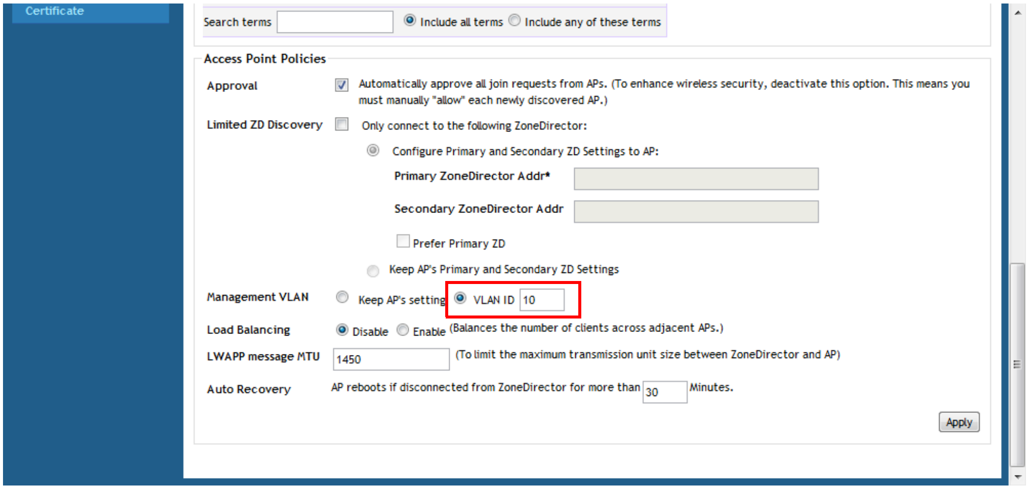
Primary DNS Server 192.168.11.1

Secondary DNS Server

ACCESS VLAN* 10

Management Interface

Figure 87. Configuring management VLAN for APs



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.)

Limited ZD Discovery □ Only connect to the following ZoneDirector:

○ Configure Primary and Secondary ZD Settings to AP:

Primary ZoneDirector Addr*

Secondary ZoneDirector Addr

□ Prefer Primary ZD

○ Keep AP's Primary and Secondary ZD Settings

Management VLAN ○ Keep AP's setting ● VLAN ID 10

Load Balancing ● Disable ○ Enable (Balances the number of clients across adjacent APs.)

LWAPP message MTU 1450 (To limit the maximum transmission unit size between ZoneDirector and AP)

Auto Recovery AP reboots if disconnected from ZoneDirector for more than 30 Minutes.

How Dynamic VLAN Works

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

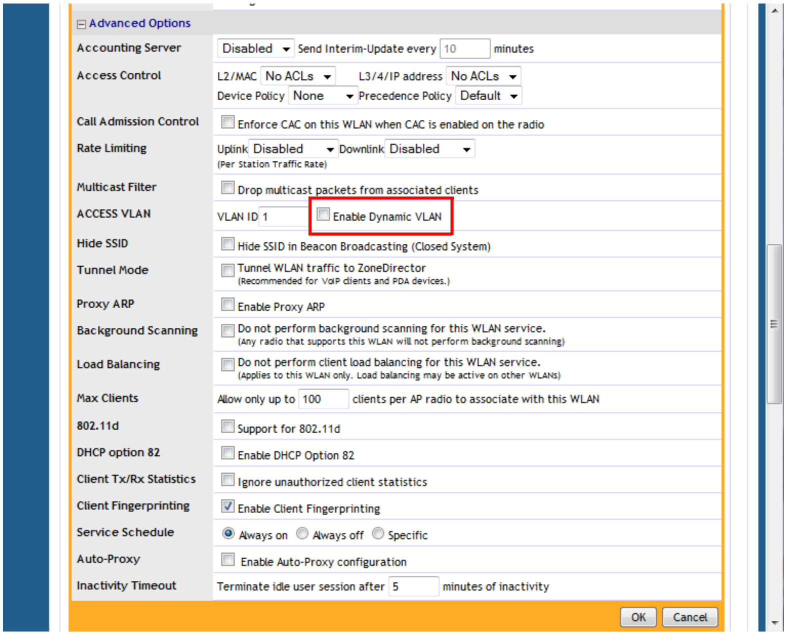
Dynamic VLAN Requirements

- 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 88. Enabling Dynamic VLAN



⊟ Advanced Options

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 ▾
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
ACCESS VLAN	VLAN ID 1 □ 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 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)
Max Clients	Allow only up to 100 clients per AP radio to associate with this WLAN
802.11d	□ Support for 802.11d
DHCP option 82	□ Enable DHCP Option 82
Client Tx/Rx Statistics	□ Ignore unauthorized client statistics
Client Fingerprinting	☑ Enable Client Fingerprinting
Service Schedule	● Always on ○ Always off ○ Specific
Auto-Proxy	□ Enable Auto-Proxy configuration
Inactivity Timeout	Terminate idle user session after 5 minutes of inactivity

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-Media-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 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 logon page, to which users that have associated with your hotspot will be redirected for authentication purposes. Users will need to enter a valid user name and password before they are allowed access to the Internet through the hotspot. Open source captive portal packages, such as Chillispot, are available on the Internet. For a list of open source and commercial captive portal software, visit http://en.wikipedia.org/wiki/Captive_portal#Software_Captive_Portals, and
- *RADIUS Server*: A Remote Authentication Dial-In User Service (RADIUS) server through which users can authenticate.

For installation and configuration instructions for the captive portal and RADIUS server software, refer to the documentation that was provided with them. After completing the steps below, you will need to edit the WLAN(s) for which you want to enable Hotspot service.

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

To create a Hotspot service

1. Go to **Configure** > **Hotspot Services**.
2. Click **Create New**. The Create New form appears.
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.

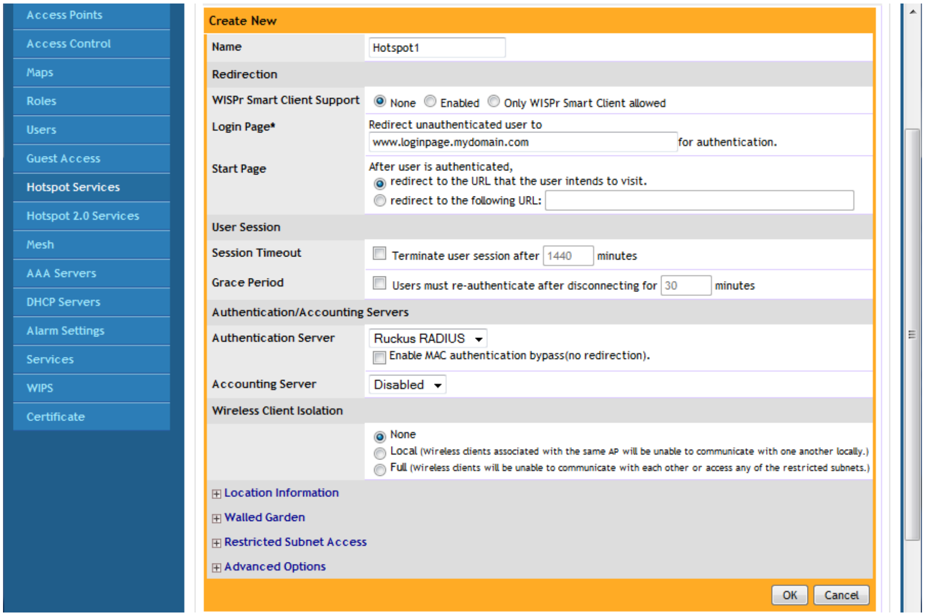
5. In **Login Page** (under Redirection), type the URL of the captive portal (the page where hotspot users can log in to access the service).
6. Configure optional settings as preferred:
   - In **Start Page**, configure where users will be redirected after successful login. You could redirect them to 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.
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 username and password. The MAC address format is a single string of characters without punctuation.
   - 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.
   - In **Wireless Client Isolation**, choose whether clients connected to this Hotspot WLAN should be allowed to communicate with one another locally. See "Options" in the Creating a WLAN section for a description of the same feature for non-Hotspot WLANs.
8. Configure optional settings as preferred:
   - In **Location Information**, enter *Location ID* and *Location Name* WISPr attributes, as specified by the Wi-Fi Alliance.
   - In **Walled Garden**, enter network destinations (URL or IP address) that users can access without going through authentication. A Walled Garden is a limited environment to which an unauthenticated user is given access for the purpose of setting up an account. After the account is established, the user is allowed out of the Walled Garden. URLs will be resolved to an IP address (up to 35). Users will not be able to click through to other URLs that may be presented on a page if that page is hosted on a server with a different IP address. Avoid using common URLs that are translated into many IP addresses (such as www.yahoo.com), as users may be redirected to reauthenticate when they navigate through the page.
   - 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.

9. 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 89. Creating a Hotspot service



Create New

Name: Hotspot1

Redirection

WISPr Smart Client Support: ● None ○ Enabled ○ Only WISPr Smart Client allowed

Login Page*: Redirect unauthenticated user to www.loginpage.mydomain.com for authentication.

Start Page: After user is authenticated,
● redirect to the URL that the user intends to visit.
○ redirect to the following URL:

User Session

Session Timeout: □ Terminate user session after 1440 minutes

Grace Period: □ Users must re-authenticate after disconnecting for 30 minutes

Authentication/Accounting Servers

Authentication Server: Ruckus RADIUS
□ Enable MAC authentication bypass(no redirection).

Accounting Server: Disabled

Wireless Client Isolation

● None
○ Local (wireless clients associated with the same AP will be unable to communicate with one another locally.)
○ Full (wireless clients will be unable to communicate with each other or access any of the restricted subnets.)

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.

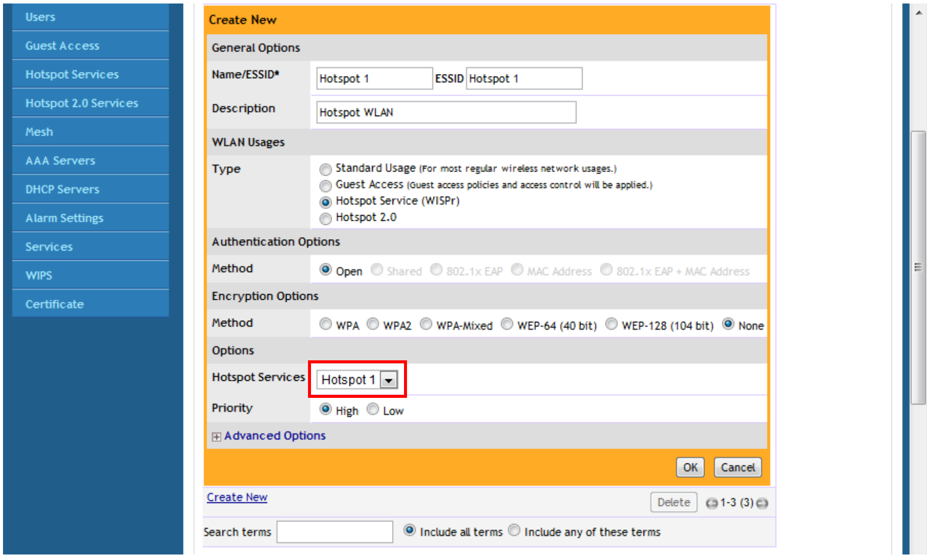
Assigning a WLAN to Provide Hotspot Service

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 90. Assigning a Hotspot service to a Hotspot WLAN



Create New

General Options

Name/ESSID* Hotspot 1 ESSID Hotspot 1

Description Hotspot WLAN

WLAN Usages

Type
○ Standard Usage (For most regular wireless network usages.)
○ Guest Access (Guest access policies and access control will be applied.)
● Hotspot Service (WISPr)
○ Hotspot 2.0

Authentication Options

Method ● Open ○ Shared ○ 802.1x EAP ○ MAC Address ○ 802.1x EAP + MAC Address

Encryption Options

Method ○ WPA ○ WPA2 ○ WPA-Mixed ○ WEP-64 (40 bit) ○ WEP-128 (104 bit) ● None

Options

Hotspot Services Hotspot 1

Priority ● High ○ Low

⊞ Advanced Options

OK Cancel

Create New Delete 1-3 (3)

Search terms ● Include all terms ○ Include any of these terms

Creating a Hotspot 2.0 Service

"Hotspot 2.0" is a newer Wi-Fi Alliance specification that allows for automated roaming between service provider access points when both the client and access gateway support the newer protocol.

Hotspot 2.0 aims to improve the experience of mobile users when selecting and joining a Wi-Fi hotspot by providing information to the station prior to association. This information can then be used by the client to automatically select an appropriate network based on the services provided and the conditions under which the user can access them. In this way, rather than being presented with a list of largely meaningless SSIDs to choose from, the Hotspot 2.0 client can automatically select and authenticate to an SSID based on the client's configuration and services offered, or allow the user to manually select an SSID for which the user has login credentials.

ZoneDirector's Hotspot 2.0 implementation complies with the IEEE 802.11u standard and the Wi-Fi Alliance Hotspot 2.0 Technical Specification.

Enabling Hotspot 2.0 service on ZoneDirector requires the following 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

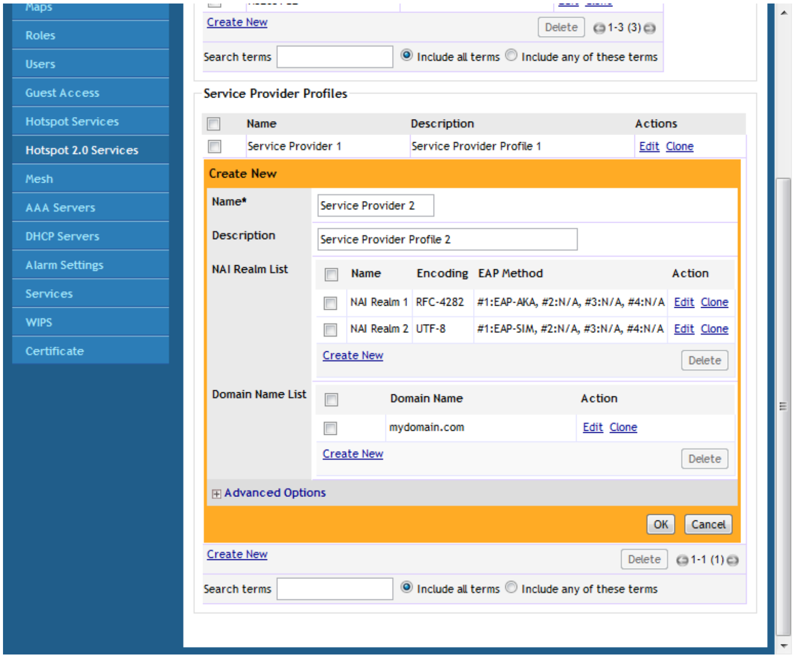
1. Go to **Configure > Hotspot 2.0 Services**.
2. Click **Create New** under *Service Provider Profiles.*
3. Configure the settings in Table 22 to create a Service Provider profile.

Table 22. 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 91. Creating a Service Provider Profile



Service Provider Profiles

□	Name	Description	Actions
□	Service Provider 1	Service Provider Profile 1	Edit Clone

Create New

Name*: Service Provider 2

Description: Service Provider Profile 2

NAI Realm List

□	Name	Encoding	EAP Method	Action
□	NAI Realm 1	RFC-4282	#1:EAP-AKA, #2:N/A, #3:N/A, #4:N/A	Edit Clone
□	NAI Realm 2	UTF-8	#1:EAP-SIM, #2:N/A, #3:N/A, #4:N/A	Edit Clone

Domain Name List

□	Domain Name	Action
□	mydomain.com	Edit Clone

Create an Operator Profile

To create an Operator Profile

1. Go to **Configure > Hotspot 2.0 Services**.
2. Click **Create New** under *Operator Profiles*.
3. Configure the settings in Table 23 to create a Hotspot 2.0 Operator profile.

Table 23. Hotspot 2.0 Operator profile configuration options

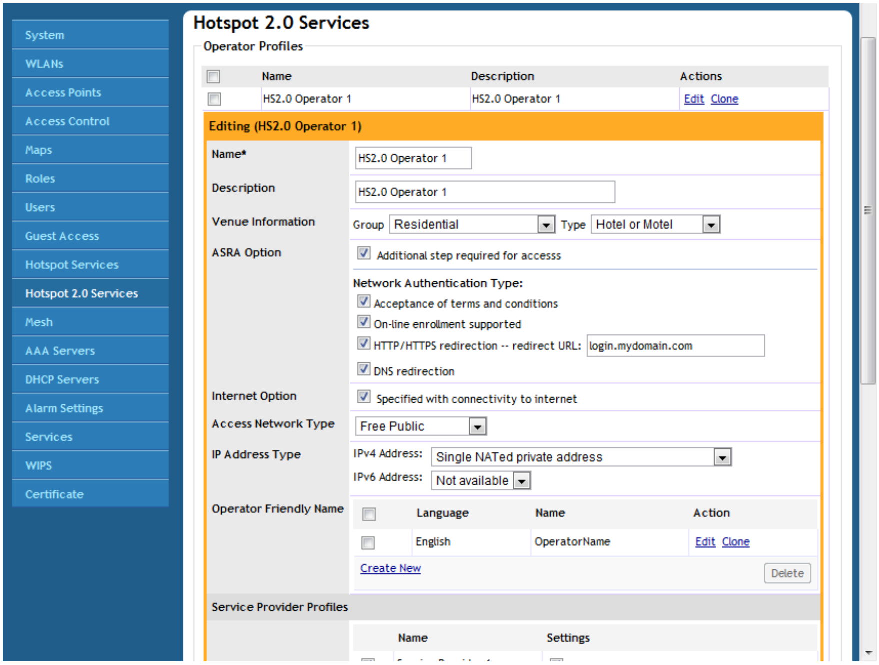
Option	Description
Name	Enter a name for this Operator profile. This name identifies the service operator when assigning an HS2.0 service to a HS2.0 WLAN.
Description	(Optional) Enter a description for the service.
Venue Information	Select venue group and venue type as defined in IEEE802.11u, Table 7.25m/n.
ASRA Option	Additional steps required for access. Select to indicate that the network requires a further step for access.

Table 23. Hotspot 2.0 Operator profile configuration options

Option	Description
Internet Option	Specify if this HS2.0 network provides connectivity to the Internet.
Access Network Type	Access network type (private, free public, chargeable public, etc.), as defined in IEEE802.11u, Table 7-43b.
IP Address Type	Select IP address type availability information, as defined in IEEE802.11u, 7.3.4.8.
Operator Friendly Name	Network operator names in multiple languages.
Service Provider Profiles	Information for each service provider, including NAI realm, domain name, roaming consortium, 3GPP cellular network info. (A Service Provider profile must first be created before it appears here.) Up to six Service Provider Profiles can be indicated for each Operator Profile.
HESSID	Homogenous extended service set identifier. The HESSID is a 6-octet MAC address that identifies the homogeneous ESS. The HESSID value must be identical to one of the BSSIDs in the homogeneous ESS.
WAN Metrics	Provides information about the WAN link connecting an IEEE 802.11 access network and the Internet; includes link status and backhaul uplink/downlink speed estimates.
Connection Capability	Provides information on the connection status within the hotspot of the most commonly used communications protocols and ports. 11 static rules are available, as defined in WFA Hotspot 2.0 Technical Specification, section 4.5.
Additional Connection Capability	Allows addition of custom connection capability rules. Up to 21 custom rules can be created.

4. Click **OK** to save this Operator Profile.
5. Continue to Create a Hotspot 2.0 WLAN.

Figure 92. Creating a Hotspot 2.0 Operator Profile



Hotspot 2.0 Services

Operator Profiles

□	Name	Description	Actions
□	HS2.0 Operator 1	HS2.0 Operator 1	Edit Clone

Editing (HS2.0 Operator 1)

Name*	HS2.0 Operator 1
Description	HS2.0 Operator 1
Venue Information	Group Residential Type Hotel or Motel
ASRA Option	☑ Additional step required for accesss Network Authentication Type: ☑ Acceptance of terms and conditions ☑ On-line enrollment supported ☑ HTTP/HTTPS redirection -- redirect URL: login.mydomain.com ☑ DNS redirection
Internet Option	☑ Specified with connectivity to internet
Access Network Type	Free Public
IP Address Type	IPv4 Address: Single NATed private address IPv6 Address: Not available
Operator Friendly Name	see below

□	Language	Name	Action
□	English	OperatorName	Edit Clone

Create New Delete

Service Provider Profiles

Name	Settings

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**.

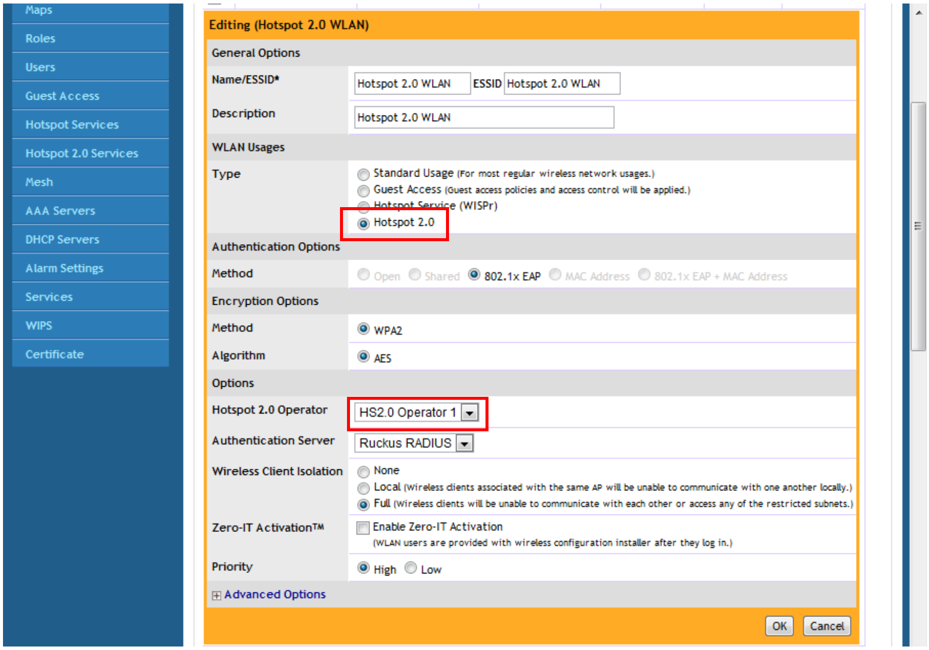
NOTE: 802.1X EAP is the only authentication method and WPA2/AES is the only encryption method available when you select Hotspot 2.0 for WLAN type.

4. In **Hotspot 2.0 Operator**, select the name of the Operator profile that you created previously.
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 93. Creating a Hotspot 2.0 WLAN



Editing (Hotspot 2.0 WLAN)

General Options

Name/ESSID*: Hotspot 2.0 WLAN ESSID: Hotspot 2.0 WLAN

Description: Hotspot 2.0 WLAN

WLAN Usages

Type:
○ Standard Usage (For most regular wireless network usages.)
○ Guest Access (Guest access policies and access control will be applied.)
○ Hotspot Service (WISPr)
● Hotspot 2.0

Authentication Options

Method: ○ Open ○ Shared ● 802.1x EAP ○ MAC Address ○ 802.1x EAP + MAC Address

Encryption Options

Method: ● WPA2

Algorithm: ● AES

Options

Hotspot 2.0 Operator: HS2.0 Operator 1

Authentication Server: Ruckus RADIUS

Wireless Client Isolation:
○ None
○ Local (Wireless clients associated with the same AP will be unable to communicate with one another locally.)
● Full (Wireless clients will be unable to communicate with each other or access any of the restricted subnets.)

Zero-IT Activation™: □ Enable Zero-IT Activation
(WLAN users are provided with wireless configuration installer after they log in.)

Priority: ● High ○ Low

Setting the Venue Name for a Hotspot 2.0 AP

See "Configuring Hotspot 2.0 Venue Settings for an AP" on page 175 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

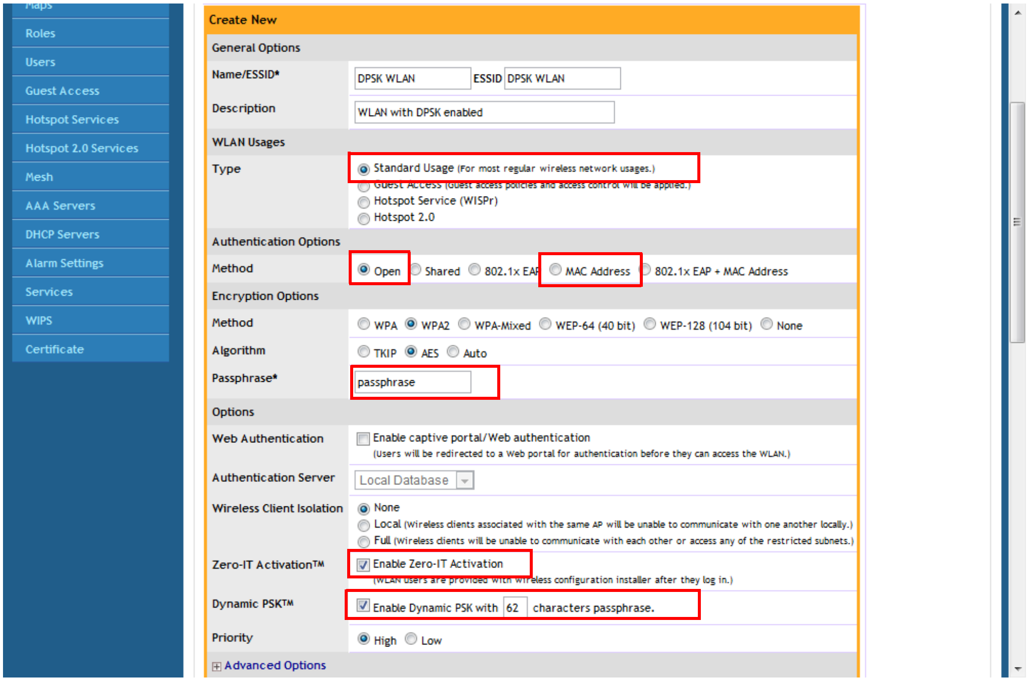
To use DPSK for client authentication, you must enable it for a particular WLAN (if you did not enable it during the initial ZoneDirector Setup Wizard process).

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 **WPA** or **WPA2** (*not* WPA-Mixed, as selecting WPA-Mixed will disable the Zero-IT activation option).
6. Under *Encryption Options: Algorithm*, select **TKIP** or **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. 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 RADIUS server.

Figure 94. Enabling Dynamic PSK for a WLAN



Create New

General Options

Name/ESSID* DPSK WLAN ESSID DPSK WLAN

Description WLAN with DPSK enabled

WLAN Usages

Type
● Standard Usage (For most regular wireless network usages.)
○ Guest Access (Guest access policies and access control will be applied.)
○ Hotspot Service (WISPr)
○ Hotspot 2.0

Authentication Options

Method ● Open ○ Shared ○ 802.1x EAP ○ MAC Address ○ 802.1x EAP + MAC Address

Encryption Options

Method ○ WPA ● WPA2 ○ WPA-Mixed ○ WEP-64 (40 bit) ○ WEP-128 (104 bit) ○ None

Algorithm ○ TKIP ● AES ○ Auto

Passphrase* passphrase

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

Wireless Client Isolation
● None
○ Local (Wireless clients associated with the same AP will be unable to communicate with one another locally.)
○ Full (Wireless clients will be unable to communicate with each other or access any of the restricted subnets.)

Zero-IT Activation™ ☑ Enable Zero-IT Activation
(WLAN users are provided with wireless configuration installer after they log in.)

Dynamic PSK™ ☑ Enable Dynamic PSK with 62 characters passphrase.

Priority ● High ○ Low

⊞ Advanced Options

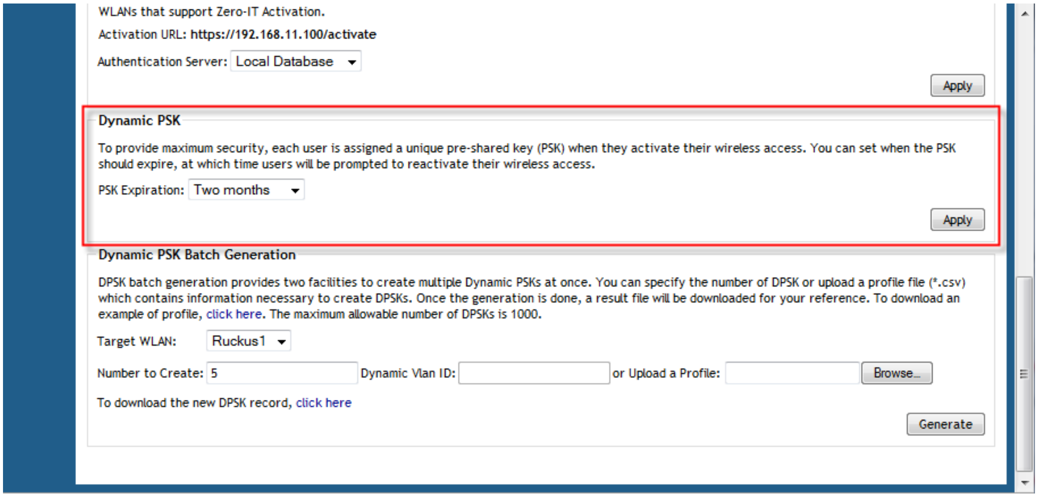
Setting Dynamic Pre-Shared Key Expiration

By default, dynamic pre-shared keys do not expire. 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**.
2. In the Dynamic PSK section, select the PSK expiration time. Range includes one day to unlimited (never expires).
3. Click the **Apply** button that is in the same section. The new setting goes into effect immediately.

Figure 95. The Dynamic PSK option



WLANs that support Zero-IT Activation.

Activation URL: **https://192.168.11.100/activate**

Authentication Server: Local Database

Dynamic PSK

To provide maximum security, each user is assigned a unique pre-shared key (PSK) when they activate their wireless access. You can set when the PSK should expire, at which time users will be prompted to reactivate their wireless access.

PSK Expiration: Two months

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: Ruckus1

Number to Create: 5 Dynamic Vlan ID: or Upload a Profile:

To download the new DPSK record, click here

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. If you want to be able to identify the dynamic PSK users by their names (for monitoring or auditing purposes in a school setting, for example), click Browse, and upload a batch dynamic PSK profile instead. See "Creating a Batch Dynamic PSK Profile" below for more information.
6. Click **Generate**. ZoneDirector generates the dynamic PSKs, and then the following message appears:

```
To download the new DPSK record, click here
```

7. 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
- WLAN Name
- MAC Address
- 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:

- *WLAN Name*: This is the WLAN with which they are authorized to access and use the dynamic PSK that you generated (passphrase).
- *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 passphrase/network key will expire. After this date, the user will no longer be able to access the WLAN using the same passphrase/ network key.

Alternatively, you can allow users to automatically self-provision their clients using Zero-IT, as described in "Enabling Automatic User Activation with Zero-IT" on page 202.

Creating a Batch Dynamic PSK Profile

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 guest pass 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.

5. Go back to the Dynamic PSK Batch Generation section, and then complete steps 4 to 6 in "Generating Multiple Dynamic PSKs" above to upload the batch dynamic PSK profile and generate multiple dynamic PSKs.

5

Managing Access Points

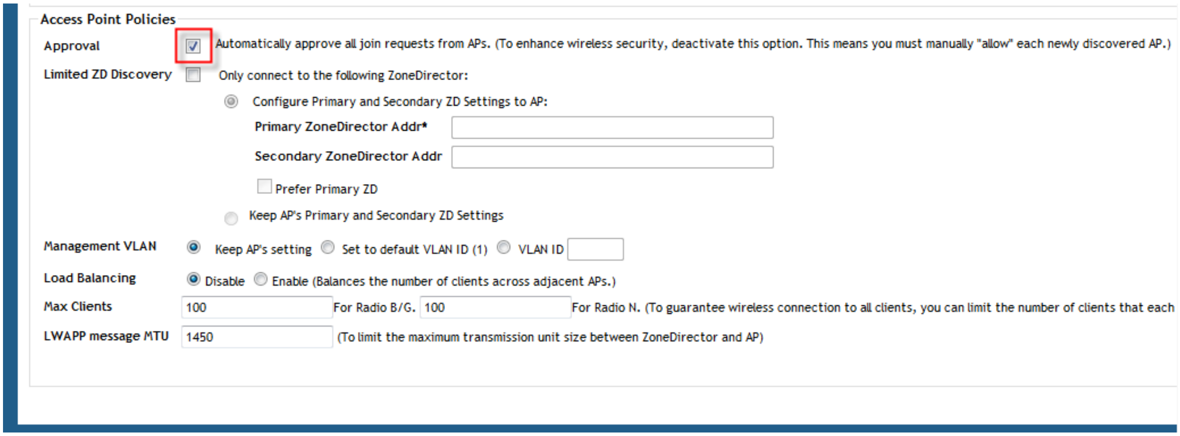
In This Chapter

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



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:

Primary ZoneDirector Addr*

Secondary ZoneDirector Addr

□ Prefer Primary ZD

○ Keep AP's Primary and Secondary ZD Settings

Management VLAN ● Keep AP's setting ○ Set to default VLAN ID (1) ○ VLAN ID

Load Balancing ● Disable ○ Enable (Balances the number of clients across adjacent APs.)

Max Clients 100 For Radio B/G. 100 For Radio N. (To guarantee wireless connection to all clients, you can limit the number of clients that each

LWAPP message MTU 1450 (To limit the maximum transmission unit size between ZoneDirector and AP)

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.

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

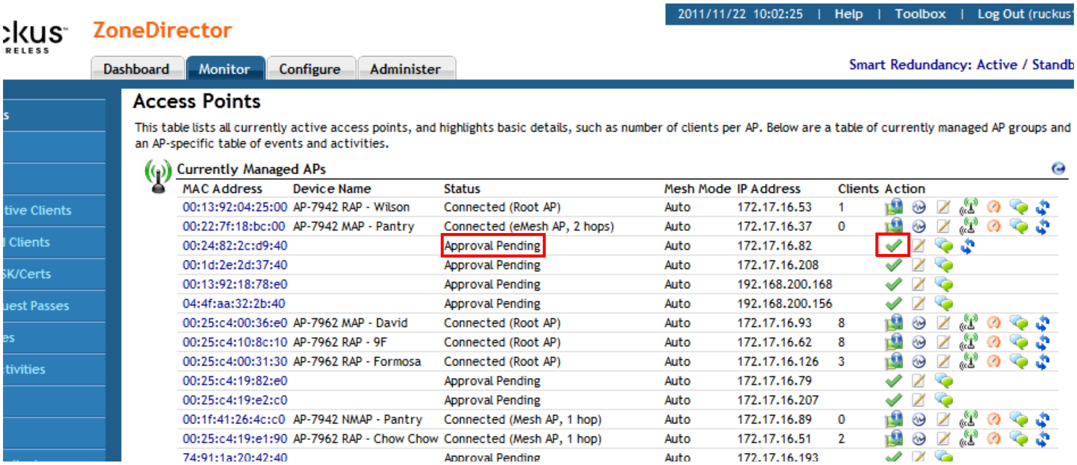
1. Go to **Monitor** > **Access Points**. The Access Points page appears, showing the first 15 access points that have been approved or are awaiting approval. If ZoneDirector is managing more than 15 access points, the Show More button at the bottom of the list will be active. To display more access 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 97.
   - 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" on page 198 for more information.

Figure 97. 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	
00:22:7f:18:bc:00	AP-7942 MAP - Pantry	Connected (eMesh AP, 2 hops)	Auto	172.17.16.37	0	
00:24:82:2c:d9:40		Approval Pending	Auto	172.17.16.82		✓
00:1d:2e:2d:37:40		Approval Pending	Auto	172.17.16.208		✓
00:13:92:18:78:e0		Approval Pending	Auto	192.168.200.168		✓
04:4f:aa:32:2b:40		Approval Pending	Auto	192.168.200.156		✓
00:25:c4:00:36:e0	AP-7962 MAP - David	Connected (Root AP)	Auto	172.17.16.93	8	
00:25:c4:10:8c:10	AP-7962 RAP - 9F	Connected (Root AP)	Auto	172.17.16.62	8	
00:25:c4:00:31:30	AP-7962 RAP - Formosa	Connected (Root AP)	Auto	172.17.16.126	3	
00:25:c4:19:82:e0		Approval Pending	Auto	172.17.16.79		✓
00:25:c4:19:e2:c0		Approval Pending	Auto	172.17.16.207		✓
00:1f:41:26:4c:c0	AP-7942 NMAP - Pantry	Connected (Mesh AP, 1 hop)	Auto	172.17.16.89	0	
00:25:c4:19:e1:90	AP-7962 RAP - Chow Chow	Connected (Mesh AP, 1 hop)	Auto	172.17.16.51	2	
74:91:1a:20:42:40		Approval Pending	Auto	172.17.16.193		✓

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.

Figure 98. Maximum number of AP groups by ZoneDirector model

ZoneDirector Model	Max AP Groups
ZoneDirector 1100	32
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

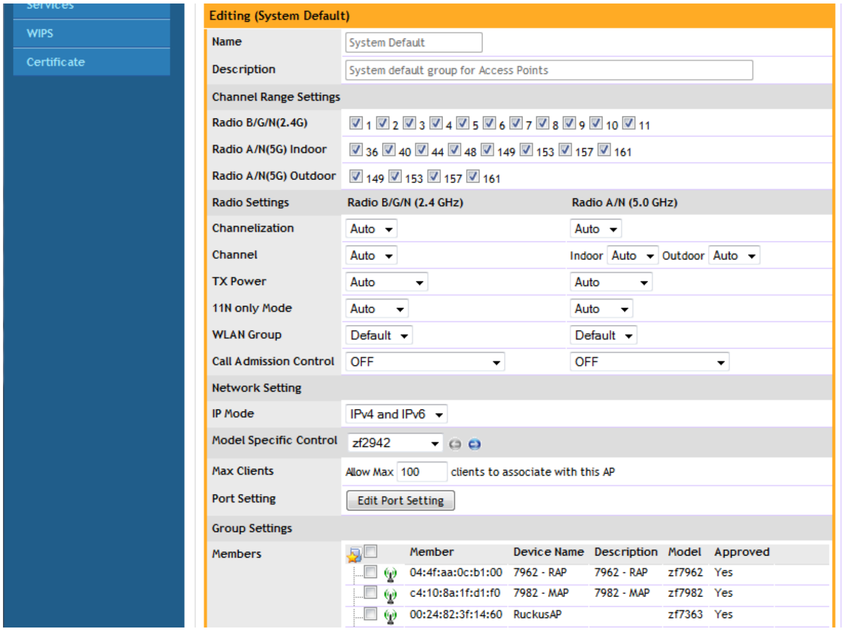
1. Go to **Configure > Access Points**.

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 24 that you want to apply to the System Default AP group, and click **OK** to save your changes.

Table 24. Access Point group settings

Setting	Description
Name	The System Default group name can not be changed (you can edit this field when creating/editing any other AP group).
Description	The System Default description can not 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, select Override System Default and deselect any channels that you do not want the APs to use.
Channelization	Select Auto, 20MHz or 40MHz channel width for either the 2.4 GHz or 5 GHz radio.
Channel	Select *Auto* or manually assign a channel for the 2.4 GHz or 5 GHz radio.
Tx Power	Allows you to manually set the transmit power on all 2.4 GHz or 5 GHz radios (default is Auto).
11n Only Mode	Force all 802.11n APs to accept only 802.11n compliant devices on the 2.4 GHz or 5 GHz radio. If *11n only Mode* 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.
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.
IP Mode	Set IPv4, IPv6 or dual-stack IPv4/IPv6 IP addressing mode.
Model Specific Control	Use this section to configure max clients, LEDs and port settings for all APs of each specific model that are members of the group. See Modifying Model Specific Controls.
Group Settings	The Group Settings section is used to move access points between groups. See Modifying Access Point Group Membership.

Figure 99. Editing the System Default access point group settings



Editing (System Default)

Name	System Default	
Description	System default group for Access Points	
Channel Range Settings		
Radio B/G/N(2.4G)	☑ 1 ☑ 2 ☑ 3 ☑ 4 ☑ 5 ☑ 6 ☑ 7 ☑ 8 ☑ 9 ☑ 10 ☑ 11	
Radio A/N(5G) Indoor	☑ 36 ☑ 40 ☑ 44 ☑ 48 ☑ 149 ☑ 153 ☑ 157 ☑ 161	
Radio A/N(5G) Outdoor	☑ 149 ☑ 153 ☑ 157 ☑ 161	
Radio Settings	**Radio B/G/N (2.4 GHz)**	**Radio A/N (5.0 GHz)**
Channelization	Auto	Auto
Channel	Auto	Indoor Auto Outdoor Auto
TX Power	Auto	Auto
11N only Mode	Auto	Auto
WLAN Group	Default	Default
Call Admission Control	OFF	OFF
Network Setting		
IP Mode	IPv4 and IPv6	
Model Specific Control	zf2942	
Max Clients	Allow Max 100 clients to associate with this AP	
Port Setting	Edit Port Setting	
Group Settings		
Members		

	Member	Device Name	Description	Model	Approved
☐	04:4f:aa:0c:b1:00	7962 - RAP	7962 - RAP	zf7962	Yes
☐	c4:10:8a:1f:d1:f0	7982 - MAP	7982 - MAP	zf7982	Yes
☐	00:24:82:3f:14:60	RuckusAP		zf7363	Yes

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 24 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.

To add more access points to this group

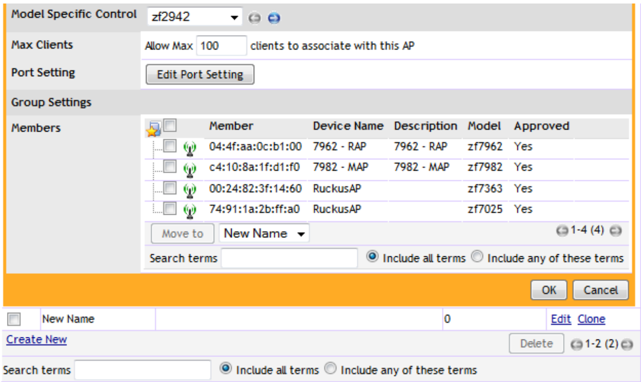
1. In *Group Settings*, click **Add more Access Points to this group** (or **Add more Access Points from System Default group to this group**).
2. Select the APs you want to add, and click **Add to this group**. The AP is added to the *Members* list above.

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

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

1. Click the check box next to any AP you want to move (to select all APs in the group, click the check box at the top of the column).
2. Select the target AP group from the drop-down list, and click **Move To**. The AP disappears from the current group list.
3. Click **OK** to save your changes.

Figure 100. Modify AP group membership



Model Specific Control: zf2942

Max Clients: Allow Max 100 clients to associate with this AP

Port Setting: Edit Port Setting

Group Settings

Members

□	Member	Device Name	Description	Model	Approved
□	04:4f:aa:0c:b1:00	7962 - RAP	7962 - RAP	zf7962	Yes
□	c4:10:8a:1f:d1:f0	7982 - MAP	7982 - MAP	zf7982	Yes
□	00:24:82:3f:14:60	RuckusAP		zf7363	Yes
□	74:91:1a:2b:ff:a0	RuckusAP		zf7025	Yes

Move to | New Name | 1-4 (4)

Search terms ● Include all terms ○ Include any of these terms

OK | Cancel

□	New Name		0	Edit Clone

Create New | Delete | 1-2 (2)

Search terms ● Include all terms ○ Include any of these terms

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 to the AP. Note that different AP models have different maximum client limitations.
- *Internal Heater*: Enable internal heaters (specific AP models only).

NOTE: For the internal heater to be operational, ZoneFlex 7762 APs must be powered by the supplied PoE injector and its associated power adapter or a standard 802.3at PSE. For the PoE Out port to be operational, ZoneFlex 7762 APs must be powered by the supplied PoE injector and its associated power adapter.

- *PoE Out Ports*: Enable PoE out ports (specific ZoneFlex 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 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.

- *Disable Status LEDs*: When managed by ZoneDirector, you can disable the external LEDs on certain ZoneFlex models, such as 73xx (indoor) and 77xx (outdoor) APs. 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*: External antenna configuration is available for the 2.4 GHz radio on the ZoneFlex 2942 and 2741 APs, and for the 5 GHz radio on the ZoneFlex 7762 APs. Once enabled, enter a gain value in the range of 0 to 90dBi.
- *Radio Band*: (ZoneFlex 7321 only) Select 2.4 GHz or 5 GHz radio band for the 7321 APs.
- *Port Settings*: See “Configuring AP Ethernet 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.

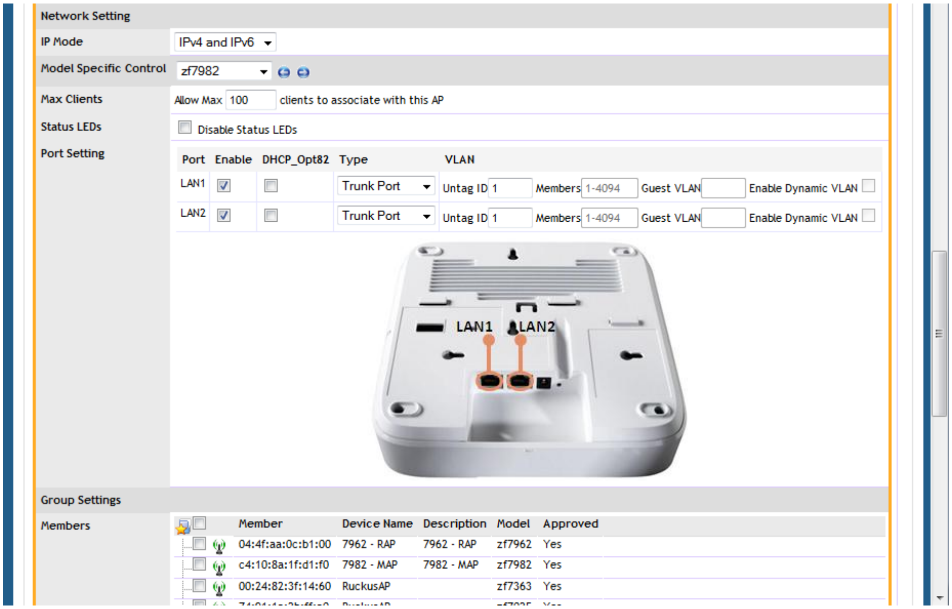
To configure Ethernet ports for all APs of the same model

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 **DHCP_Opt82** if you want to enable this option for this port (see “DHCP Option 82”).
7. For any enabled ports, you can choose whether the port will be used as a **Trunk Port**, an **Access Port** or a **General Port**.

   The following restrictions apply:
   - All APs must be configured with at least one Trunk Port.
   - For single port APs (e.g., ZoneFlex 2741), the single LAN port must be a trunk port and is therefore not configurable.
   - For ZoneFlex 7025, 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” on page 163 for more information.)

8. (If Smart Mesh is not enabled), choose whether this port will serve as an 802.1X Authenticator or Supplicant, or leave 802.1X settings disabled (default). (See "Using Port-Based 802.1X" on page 164 for more information.)
9. Click **Apply** to save your changes.

Figure 101. The ZoneFlex 7982 has two Ethernet ports, LAN1 and LAN2



Network Setting

IP Mode: IPv4 and IPv6

Model Specific Control: zf7982

Max Clients: Allow Max 100 clients to associate with this AP

Status LEDs: □ Disable Status LEDs

Port Setting

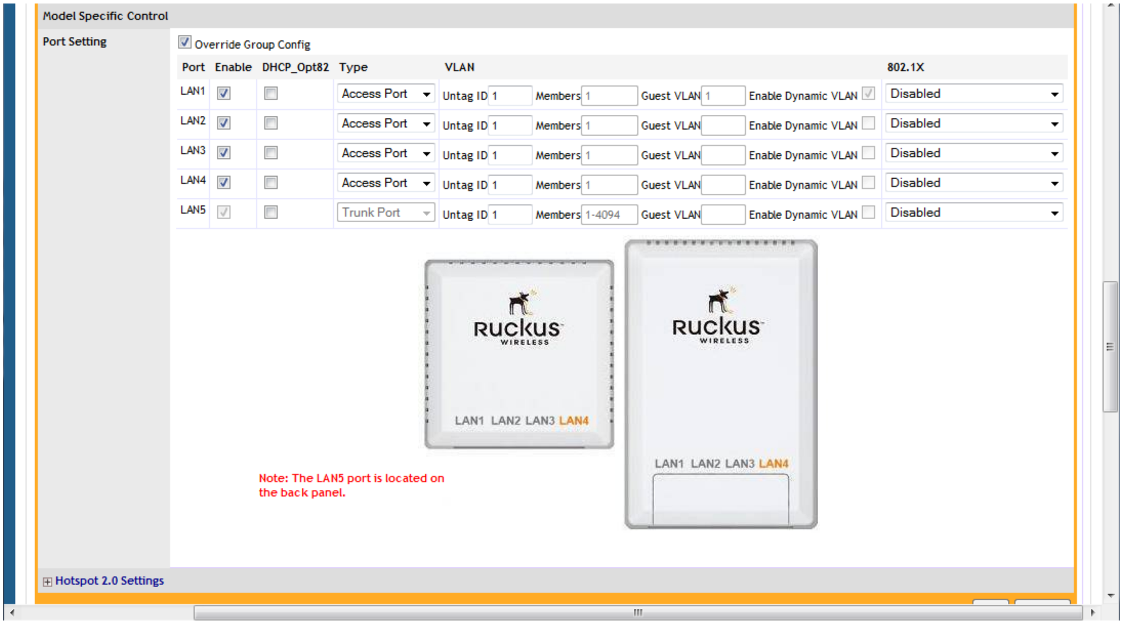
Port	Enable	DHCP_Opt82	Type	VLAN
LAN1	☑	□	Trunk Port	Untag ID 1 Members 1-4094 Guest VLAN Enable Dynamic VLAN □
LAN2	☑	□	Trunk Port	Untag ID 1 Members 1-4094 Guest VLAN Enable Dynamic VLAN □

Group Settings

Members

□	Member	Device Name	Description	Model	Approved
□	04:4f:aa:0c:b1:00	7962 - RAP	7962 - RAP	zf7962	Yes
□	c4:10:8a:1f:d1:f0	7982 - MAP	7982 - MAP	zf7982	Yes
□	00:24:82:3f:14:60	RuckusAP		zf7363	Yes

Figure 102. The ZoneFlex 7025 has four front-facing Ethernet ports and one rear port



Model Specific Control

Port Setting

☑ Override Group Config

Port	Enable	DHCP_Opt82	Type	VLAN	802.1X
LAN1	☑	☐	Access Port	Untag ID 1 Members 1 Guest VLAN 1 Enable Dynamic VLAN ☑	Disabled
LAN2	☑	☐	Access Port	Untag ID 1 Members 1 Guest VLAN Enable Dynamic VLAN ☐	Disabled
LAN3	☑	☐	Access Port	Untag ID 1 Members 1 Guest VLAN Enable Dynamic VLAN ☐	Disabled
LAN4	☑	☐	Access Port	Untag ID 1 Members 1 Guest VLAN Enable Dynamic VLAN ☐	Disabled
LAN5	☑	☐	Trunk Port	Untag ID 1 Members 1-4094 Guest VLAN Enable Dynamic VLAN ☐	Disabled

Note: The LAN5 port is located on the back panel.

⊞ Hotspot 2.0 Settings

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.

Table 25. DHCP Circuit ID sub-option format

Curcuit ID sub-option	Indicator Type: WLAN or Ethernet	Interface Name	VLAN ID	ESSID	AP Model	AP Friendly Name	AP Base MAC Address

WLAN Example:

CIRCUIT ID – WLAN:'wlan0':123:Wi-Fi Services:ZF7762-S:Coffee-Shop-AP:04:4F:AA:34:96:50

Ethernet example:

```
CIRCUIT ID - ETH:'eth0':123:N/A:ZF7762-S:Coffee-Shop-
AP:04:4F:AA:34:96:50
```

Designating Ethernet Port Type

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

- "Trunk Ports"
- "Access Ports"
- "General Ports"

Trunk links are required to pass VLAN information between switches. Access ports provide access to the network and can be configured as members of specific VLANs, thereby separating the traffic on these ports from traffic on other VLANs. General Ports are user-defined ports that can have any combination of up to 20 VLAN IDs assigned.

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.

By default, all ports are enabled as Trunk Ports with Untag VLAN set as 1 (except for ZoneFlex 7025, whose front ports are enabled as Access Ports by default). If configured as an Access Port, all untagged ingress traffic is the configured Untag VLAN, and all egress traffic is 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

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 those VLANs between switches.

Access Ports

All Access Ports are set to Untag VLAN 1 by default. This means that all Access Ports belong to the native VLAN and are all part of a single broadcast domain. 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-specified ports that can have any combination of up to 20 VLAN IDs assigned. Enter multiple valid VLAN IDs separated by commas or a range separated by a hyphen.

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 can not 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. The ZoneFlex 7025 does not support mesh, so 802.1X settings will remain available for those access points even when mesh is enabled. However, the 802.1X settings are only available from the *Editing [Access Point]* dialogue, not from AP Groups. Therefore if you want to use 802.1X on ZoneFlex 7025 ports (when mesh is enabled), you must configure each AP individually.

AP Ethernet port as authenticator

The Access Point is fundamentally 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 can even be 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.

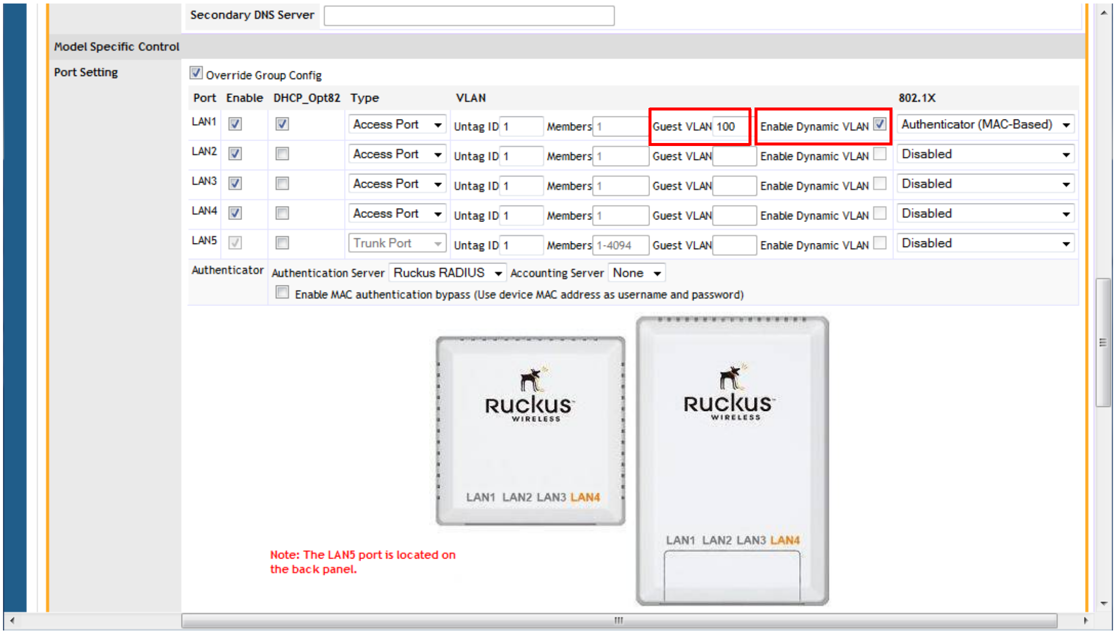
Figure 103. Authenticator support vs. Port Type

	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 104. Enabling Guest VLAN and Dynamic VLAN on a MAC-based 802.1X Authenticator port



Secondary DNS Server

Model Specific Control

Port Setting ☑ Override Group Config

Port	Enable	DHCP_Opt82	Type	VLAN				802.1X
LAN1	☑	☑	Access Port	Untag ID 1	Members 1	Guest VLAN 100	Enable Dynamic VLAN ☑	Authenticator (MAC-Based)
LAN2	☑	□	Access Port	Untag ID 1	Members 1	Guest VLAN	Enable Dynamic VLAN □	Disabled
LAN3	☑	□	Access Port	Untag ID 1	Members 1	Guest VLAN	Enable Dynamic VLAN □	Disabled
LAN4	☑	□	Access Port	Untag ID 1	Members 1	Guest VLAN	Enable Dynamic VLAN □	Disabled
LAN5	☑	□	Trunk Port	Untag ID 1	Members 1-4094	Guest VLAN	Enable Dynamic VLAN □	Disabled

Authenticator Authentication Server Ruckus RADIUS Accounting Server None
□ Enable MAC authentication bypass (Use device MAC address as username and password)

Note: The LAN5 port is located on the back panel.

AP Ethernet port as Supplicant

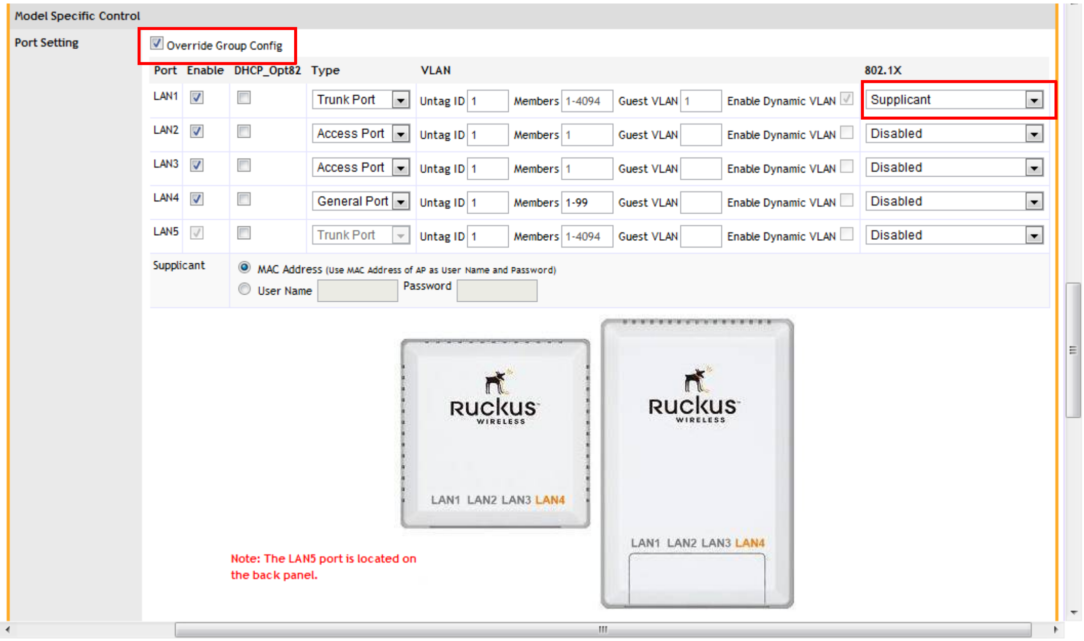
You can also configure a port to act as a supplicant and force it to authenticate itself to an upstream authenticator port. Until the AP has successfully done so, the state of the authenticator port is closed and packets from the AP or stations behind it will be dropped at the authenticator port.

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 105. Configuring an AP Ethernet port as an 802.1X Supplicant



Model Specific Control

Port Setting ☑ Override Group Config

Port	Enable	DHCP_Opt82	Type	VLAN				802.1X
LAN1	☑	□	Trunk Port	Untag ID 1	Members 1-4094	Guest VLAN 1	Enable Dynamic VLAN ☑	Supplicant
LAN2	☑	□	Access Port	Untag ID 1	Members 1	Guest VLAN	Enable Dynamic VLAN □	Disabled
LAN3	☑	□	Access Port	Untag ID 1	Members 1	Guest VLAN	Enable Dynamic VLAN □	Disabled
LAN4	☑	□	General Port	Untag ID 1	Members 1-99	Guest VLAN	Enable Dynamic VLAN □	Disabled
LAN5	☑	□	Trunk Port	Untag ID 1	Members 1-4094	Guest VLAN	Enable Dynamic VLAN □	Disabled

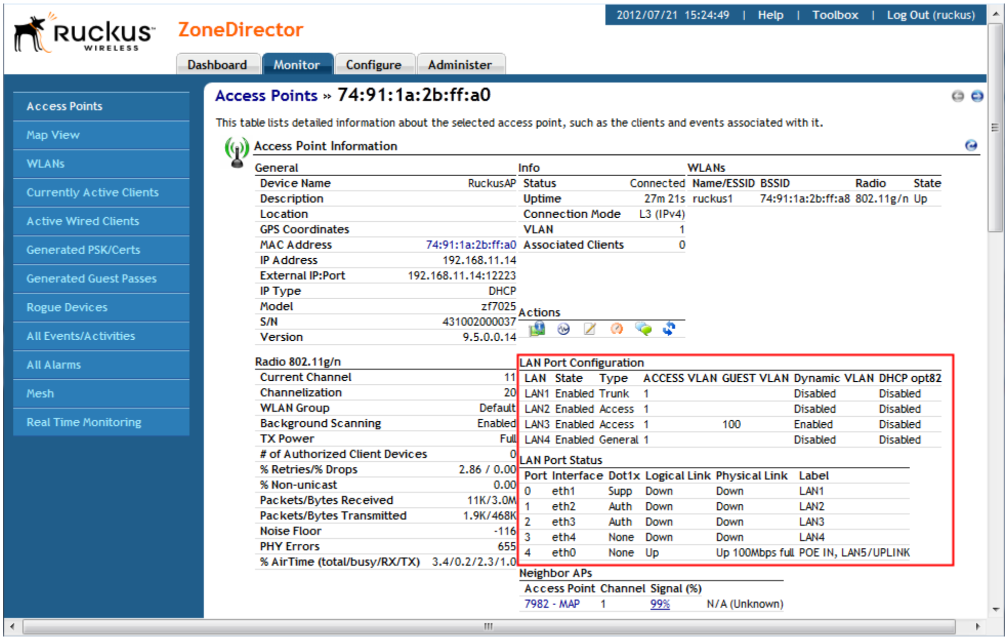
Supplicant ● MAC Address (Use MAC Address of AP as User Name and Password)
○ User Name Password

Note: The LAN5 port is located on the back panel.

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.

Figure 106. Viewing an AP's Ethernet port configuration



Access Points » 74:91:1a:2b:ff:a0

This table lists detailed information about the selected access point, such as the clients and events associated with it.

Access Point Information

General	
Device Name	RuckusAP
Description	
Location	
GPS Coordinates	
MAC Address	74:91:1a:2b:ff:a0
IP Address	192.168.11.14
External IP:Port	192.168.11.14:12223
IP Type	DHCP
Model	zf7025
S/N	431002000037
Version	9.5.0.0.14

Info	
Status	Connected
Uptime	27m 21s
Connection Mode	L3 (IPv4)
VLAN	1
Associated Clients	0

WLANs

Name/ESSID	BSSID	Radio	State
ruckus1	74:91:1a:2b:ff:a8	802.11g/n	Up

Radio 802.11g/n	
Current Channel	11
Channelization	20
WLAN Group	Default
Background Scanning	Enabled
TX Power	Full
# of Authorized Client Devices	0
% Retries/% Drops	2.86 / 0.00
% Non-unicast	0.00
Packets/Bytes Received	11K/3.0M
Packets/Bytes Transmitted	1.9K/468K
Noise Floor	-116
PHY Errors	655
% AirTime (total/busy/RX/TX)	3.4/0.2/2.3/1.0

LAN Port Configuration

LAN	State	Type	ACCESS VLAN	GUEST VLAN	Dynamic VLAN	DHCP opt82
LAN1	Enabled	Trunk	1		Disabled	Disabled
LAN2	Enabled	Access	1		Disabled	Disabled
LAN3	Enabled	Access	1	100	Enabled	Disabled
LAN4	Enabled	General	1		Disabled	Disabled

LAN Port Status

Port	Interface	Dot1x	Logical Link	Physical Link	Label
0	eth1	Supp	Down	Down	LAN1
1	eth2	Auth	Down	Down	LAN2
2	eth3	Auth	Down	Down	LAN3
3	eth4	None	Down	Down	LAN4
4	eth0	None	Up	Up 100Mbps full	POE IN, LAN5/UPLINK

Neighbor APs

Access Point	Channel	Signal (%)	
7982 - MAP	1	99%	N/A (Unknown)

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 and license level, Ruckus Wireless recommends using the Smart Redundancy feature. If you have two ZoneDirectors of different models or different license levels, you can use Limited ZD Discovery to provide limited redundancy; however, this method does not provide synchronization of the user database. For information on Smart Redundancy configuration, see "Enabling Smart Redundancy" on page 39. For information on N+1 redundancy using Limited ZD Discovery, see "Using Limited ZD Discovery for N+1 Redundancy" on page 171.

     - **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.

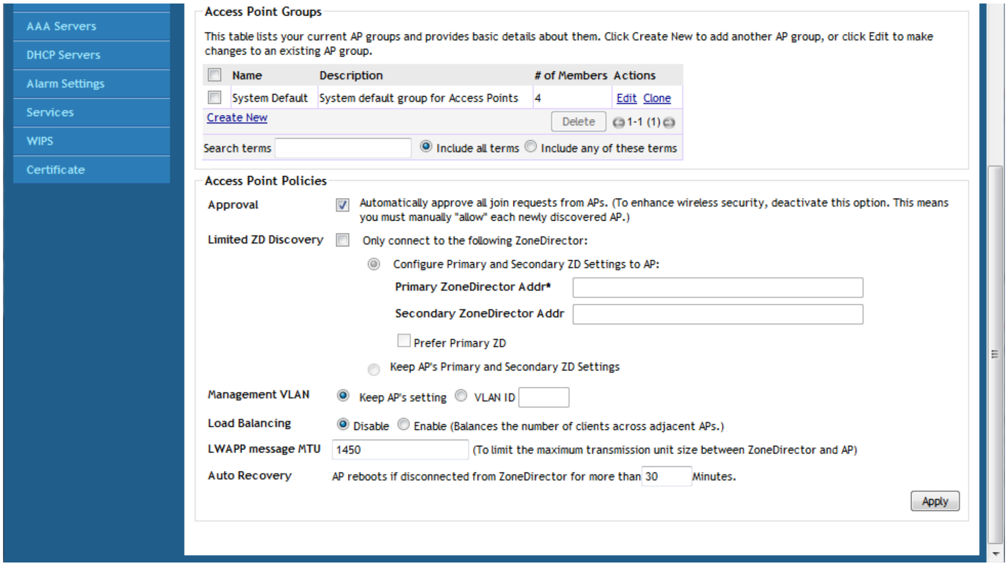
- **Load Balancing**: Balances the number of clients across adjacent APs (see "Load Balancing" **on page 178**).
- **Max Clients**: If you want to guarantee wireless connections to all clients, you can limit the number of wireless clients that each AP (or radio, on dual radio APs) will manage. In the Max Clients box, type the maximum number of clients per radio (default is 100) for the 11b/g radio and for the 11n radio. This is the maximum that any AP radio can accept. Because an AP/radio can provide service to multiple WLANs, you can also limit the number of clients that can associate to a WLAN, on a per AP/per radio basis (see "Advanced Options" on page 119).

NOTE: Note that, for ZoneFlex 802.11g APs (2942 and 2741) and ZoneFlex 7025 Wired/Wireless Wall Switch, the maximum number of clients is 100. For all other ZoneFlex 802.11n APs, the maximum number of clients is 256 for APs with no WLANs using encryption, and 100 if encryption is enabled on any WLAN.

- **LWAPP Message MTU**: Use this field to set the Maximum Transmission Unit for LWAPP protocol messages. The MTU is the size of the largest protocol data unit (in bytes) that can be passed.
- **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 107. Setting global AP policies on the Configure > Access Points page



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.

□	Name	Description	# of Members	Actions
□	System Default	System default group for Access Points	4	Edit Clone

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.)

Limited ZD Discovery □ Only connect to the following ZoneDirector:

● Configure Primary and Secondary ZD Settings to AP:

Primary ZoneDirector Addr*

Secondary ZoneDirector Addr

□ Prefer Primary ZD

○ Keep AP's Primary and Secondary ZD Settings

Management VLAN ● Keep AP's setting ○ VLAN ID

Load Balancing ● Disable ○ Enable (Balances the number of clients across adjacent APs.)

LWAPP message MTU 1450 (To limit the maximum transmission unit size between ZoneDirector and AP)

Auto Recovery AP reboots if disconnected from ZoneDirector for more than 30 Minutes.

Apply

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 and license number. 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 ZD1100s 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 27. Max APs by ZoneDirector model

Model	Max APs per controller
ZoneDirector 1100	150
ZoneDirector 3000	2250
ZoneDirector 5000	2250

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.

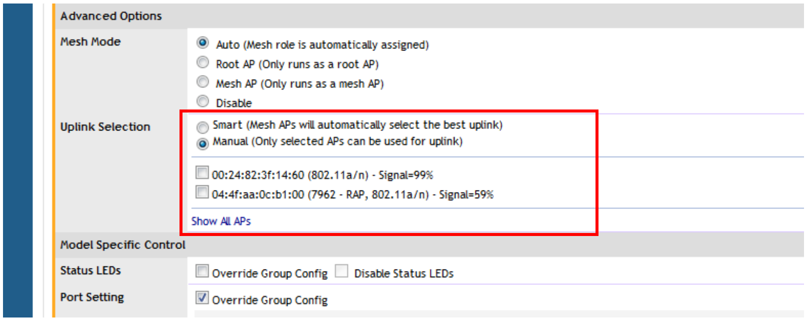
To edit the parameters of an access point

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.
4. By clicking "Override Group Config" and changing the default values, the following parameters can be configured independently for each AP radio:
    - **Channel Range Settings:** Deselect any channels that you do not want the AP to use in channel selection.
    - **Channelization**: Sets the channel width (20 or 40 MHz) of each channel in the spectrum used during transmission.
    - **Channel**: Manually set the channel used by the AP radio.
    - **Tx Power**: Manually set the maximum transmit power level relative to the calibrated power.
    - **WLAN Group**: Specify a WLAN group for this radio.
    - **Call Admission Control**: (Disabled by default). Enable Wi-Fi Multimedia Admission Control (WMM-AC) to support Polycom/Spectralink VIEW certification. See Advanced Options under Creating a WLAN for more information.
    - **WLAN Service**: Uncheck this check box to disable WLAN service entirely for this radio. (This option can be useful if you want dual-band 802.11n 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.
    - **External Antenna**: External antenna configuration is available for the 2.4 GHz radio on the ZoneFlex 2942 and 2741 APs, and for the 5 GHz radio on the ZoneFlex 7762. Once enabled, enter a gain value in the range of 0 to 90dBi.
    - **Radio Band**: (ZoneFlex 7321 only) Select 2.4 GHz or 5 GHz radio band for the 7321 APs.

5. 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
6. If Smart Mesh is enabled (see “Deploying a Smart Mesh Network” on page 233), 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.
7. 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.
8. 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” on page 249 for more information.

Figure 108. Manual uplink selection for APs in a mesh



Advanced Options

Mesh Mode
● Auto (Mesh role is automatically assigned)
○ Root AP (Only runs as a root AP)
○ Mesh AP (Only runs as a mesh AP)
○ Disable

Uplink Selection
○ Smart (Mesh APs will automatically select the best uplink)
● Manual (Only selected APs can be used for uplink)
□ 00:24:82:3f:14:60 (802.11a/n) - Signal=99%
□ 04:4f:aa:0c:b1:00 (7962 - RAP, 802.11a/n) - Signal=59%
Show All APs

Model Specific Control

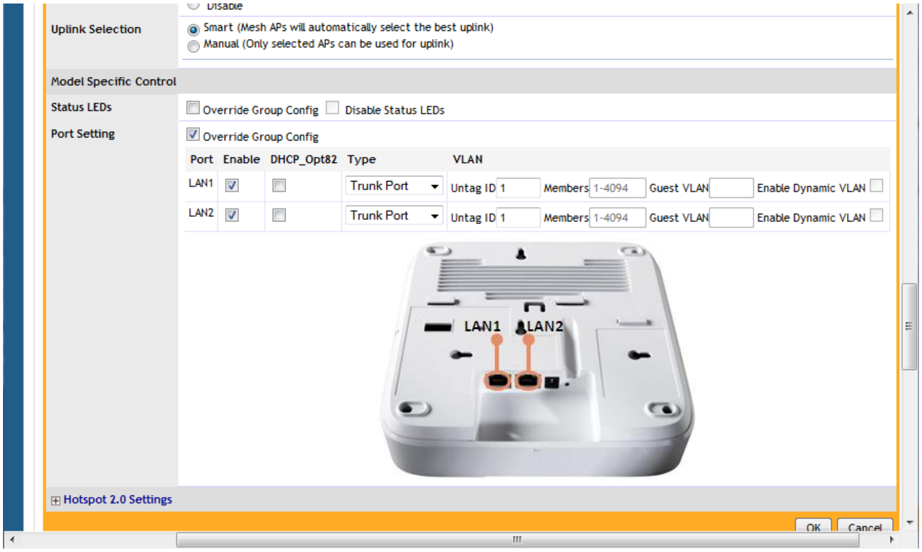
Status LEDs
□ Override Group Config □ Disable Status LEDs

Port Setting
☑ Override Group Config

9. If you select **Override Group Config** in the Port Setting section, a new section opens where you can customize the Ethernet port behavior for this AP. Enabling this will override the AP group settings made on “Configuring AP Ethernet Ports” on page 160.

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

Figure 109. Ethernet port configuration - Override Group Config



○ Disable

Uplink Selection
● Smart (Mesh APs will automatically select the best uplink)
○ Manual (Only selected APs can be used for uplink)

Model Specific Control

Status LEDs: □ Override Group Config □ Disable Status LEDs

Port Setting: ☑ Override Group Config

Port	Enable	DHCP_Opt82	Type	VLAN
LAN1	☑	□	Trunk Port	Untag ID 1 Members 1-4094 Guest VLAN Enable Dynamic VLAN □
LAN2	☑	□	Trunk Port	Untag ID 1 Members 1-4094 Guest VLAN Enable Dynamic VLAN □

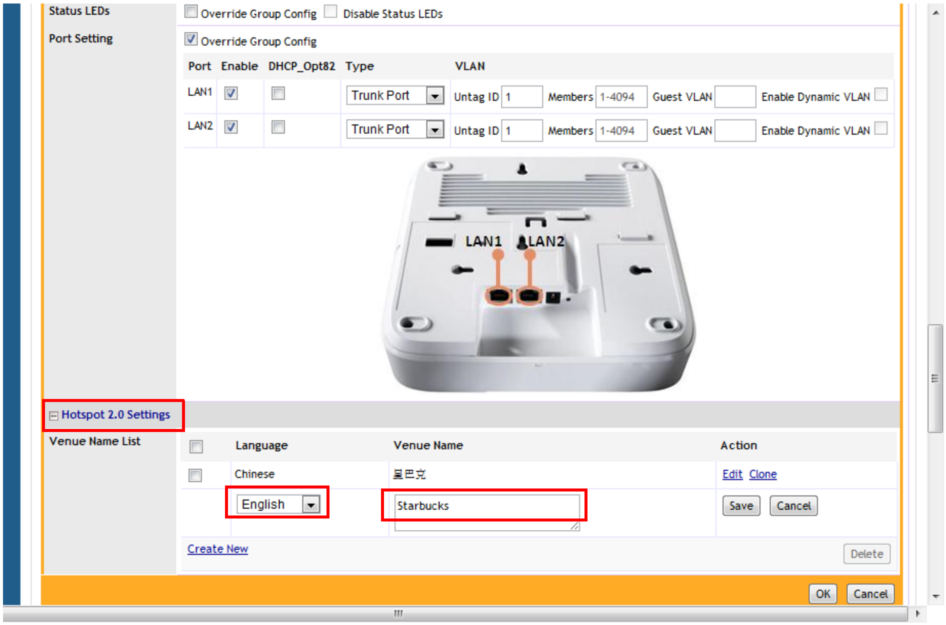
Configuring Hotspot 2.0 Venue Settings for an AP

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 110. Setting the Venue Name for a Hotspot 2.0 service AP



Status LEDs: □ Override Group Config □ Disable Status LEDs

Port Setting: ☑ Override Group Config

Port	Enable	DHCP_Opt82	Type	VLAN
LAN1	☑	□	Trunk Port	Untag ID 1 Members 1-4094 Guest VLAN Enable Dynamic VLAN □
LAN2	☑	□	Trunk Port	Untag ID 1 Members 1-4094 Guest VLAN Enable Dynamic VLAN □

⊟ Hotspot 2.0 Settings

Venue Name List

□	Language	Venue Name	Action
□	Chinese	星巴克	Edit Clone
	English	Starbucks	Save Cancel

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" on page 182 and "Placing the Access Point Markers" on page 184.

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" on page 185.)

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" on page 282.
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 20/40MHz or Auto channel width (11n APs only).
- *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**.

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:

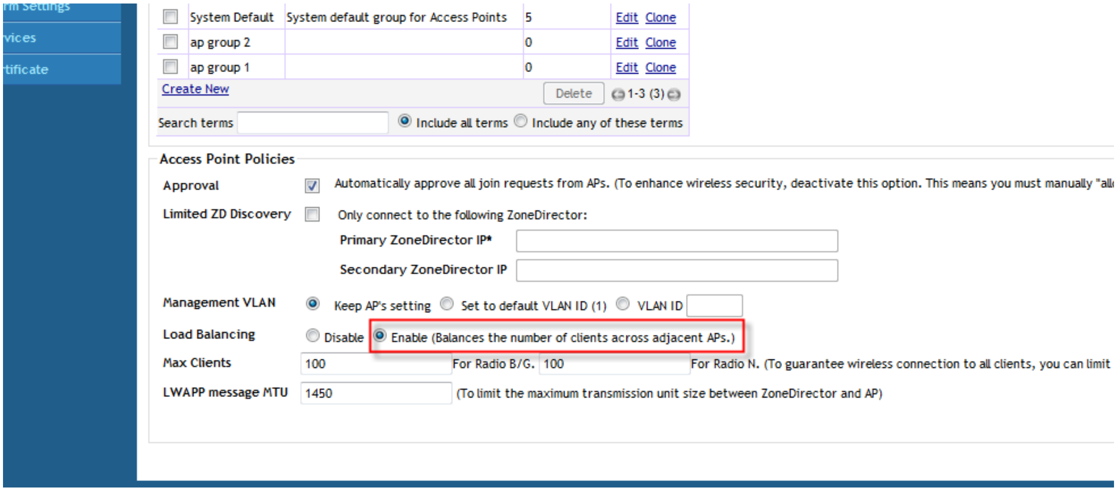
- These rules apply only to client devices; the AP always responds to another AP that is attempting to set up or maintain a mesh network.
- Load balancing does not disassociate clients already connected.
- Load balancing takes action before a client association request, reducing the chance of client 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 > Access Points**.
2. In Access Point Policies, click the **Enable** button next to *Load Balancing*.

Figure 111. Enable Load Balancing globally for all APs and WLANs



□	System Default	System default group for Access Points	5	Edit Clone
□	ap group 2		0	Edit Clone
□	ap group 1		0	Edit Clone

Create New   Delete   1-3 (3)

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 "all

Limited ZD Discovery □ Only connect to the following ZoneDirector:

Primary ZoneDirector IP*

Secondary ZoneDirector IP

Management VLAN ● Keep AP's setting ○ Set to default VLAN ID (1) ○ VLAN ID

Load Balancing ○ Disable ● Enable (Balances the number of clients across adjacent APs.)

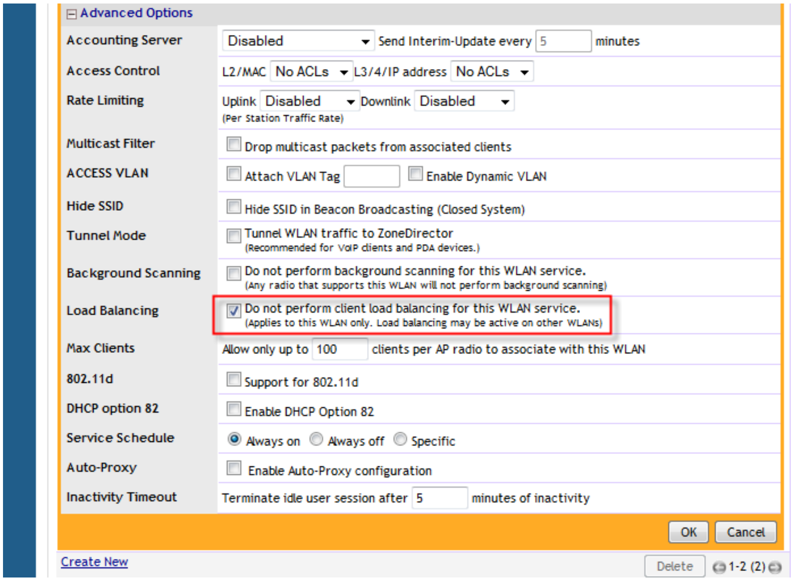
Max Clients 100 For Radio B/G. 100 For Radio N. (To guarantee wireless connection to all clients, you can limit

LWAPP message MTU 1450 (To limit the maximum transmission unit size between ZoneDirector and AP)

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 112. Disable load balancing on a specific WLAN



⊟ Advanced Options

Accounting Server	Disabled ▾ Send Interim-Update every 5 minutes
Access Control	L2/MAC No ACLs ▾ L3/4/IP address No ACLs ▾
Rate Limiting	Uplink Disabled ▾ Downlink Disabled ▾ (Per Station Traffic Rate)
Multicast Filter	□ Drop multicast packets from associated clients
ACCESS VLAN	□ Attach VLAN Tag □ 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.)
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)
Max Clients	Allow only up to 100 clients per AP radio to associate with this WLAN
802.11d	□ Support for 802.11d
DHCP option 82	□ Enable DHCP Option 82
Service Schedule	● Always on ○ Always off ○ Specific
Auto-Proxy	□ Enable Auto-Proxy configuration
Inactivity Timeout	Terminate idle user session after 5 minutes of inactivity

6

Monitoring Your Wireless Network

In This Chapter

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" on page 29).
- *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.

- 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 1100 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

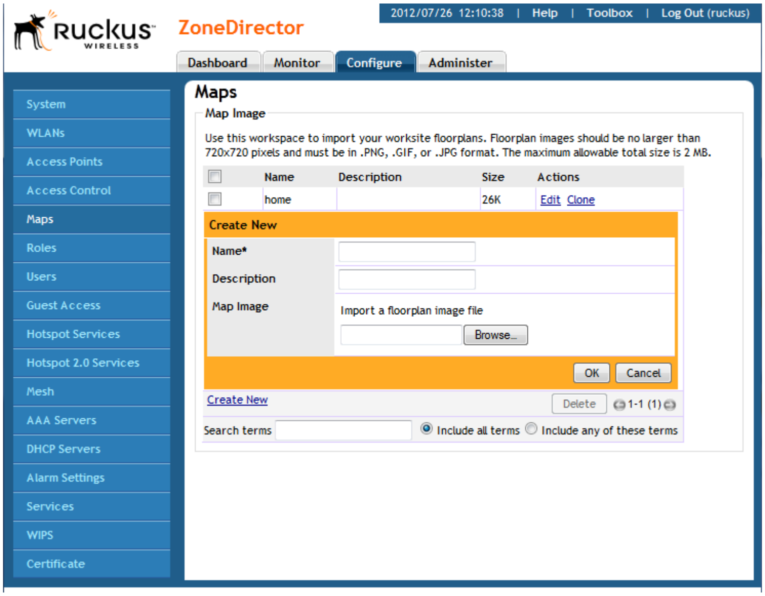
- A floorplan image in .GIF, .JPG or .PNG format
- The image should be monochrome or grayscale.
- The file size should be no larger than 200kb in size.
- The floorplan image should be (ideally) no larger than 10 inches (720 pixels) per side.

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 113. The Create New form for importing a floorplan image



Maps

Map Image

Use this workspace to import your worksite floorplans. Floorplan images should be no larger than 720x720 pixels and must be in .PNG, .GIF, or .JPG format. The maximum allowable total size is 2 MB.

□	Name	Description	Size	Actions
□	home		26K	Edit Clone

Create New

Name*	
Description	
Map Image	Import a floorplan image file Browse...

OK Cancel

Create New   Delete   1-1 (1)

Search terms   ● Include all terms ○ Include any of these terms

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" on page 176.

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.

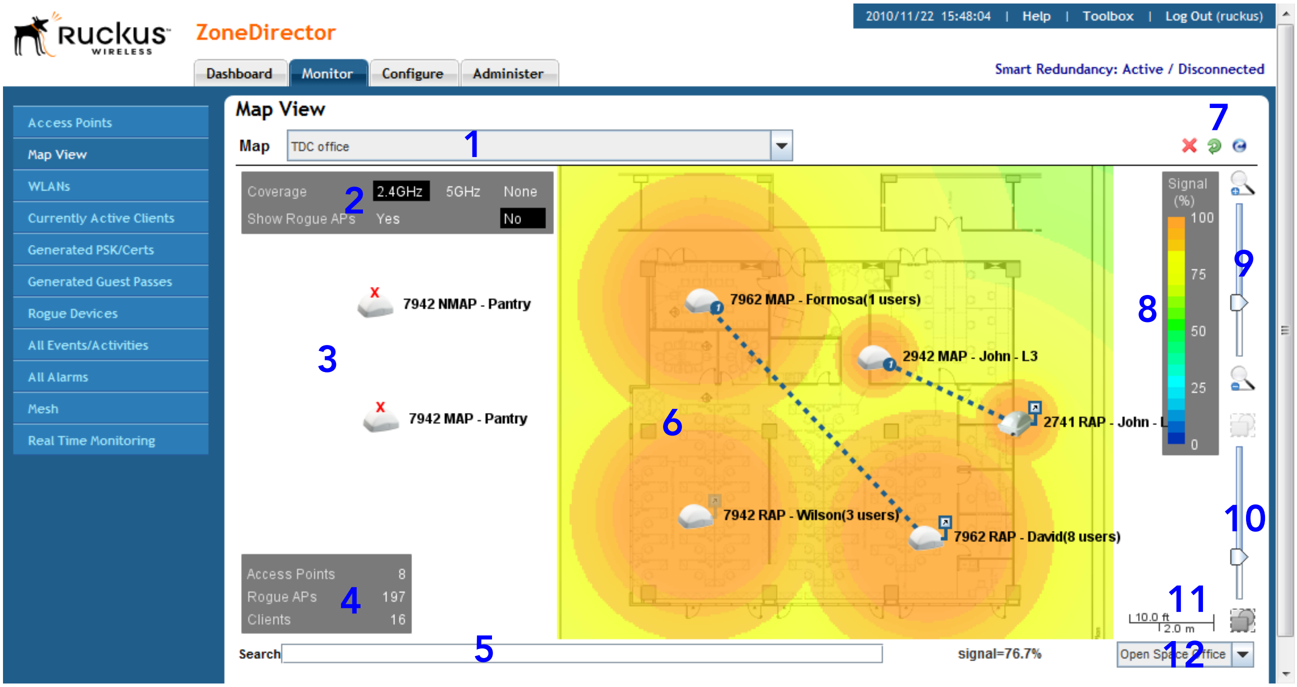


Figure 114. Elements on the Map View

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" on page 154), 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" on page 186.
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.

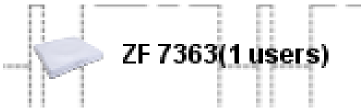
5. *Search text box*: Enter a string, such as part of an AP's name or MAC address, and the map is filtered to show only the matching results. Clearing the search value returns the map to its unfiltered view.
6. *Floorplan area*: The floorplan displays in this main area. You can manipulate the size and angle of the floorplan by using the tools on this screen.
7. 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.

8. *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" on page 198 for more information.
9. *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.
10. *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.
11. *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.
12. *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:

	A normal AP marker displays the description of the AP and the number of users that are currently associated with the AP.
	An unplaced AP marker displays a "?" (question mark) above the icon.
	A rogue AP displays a smaller red icon imprinted with a "bug."

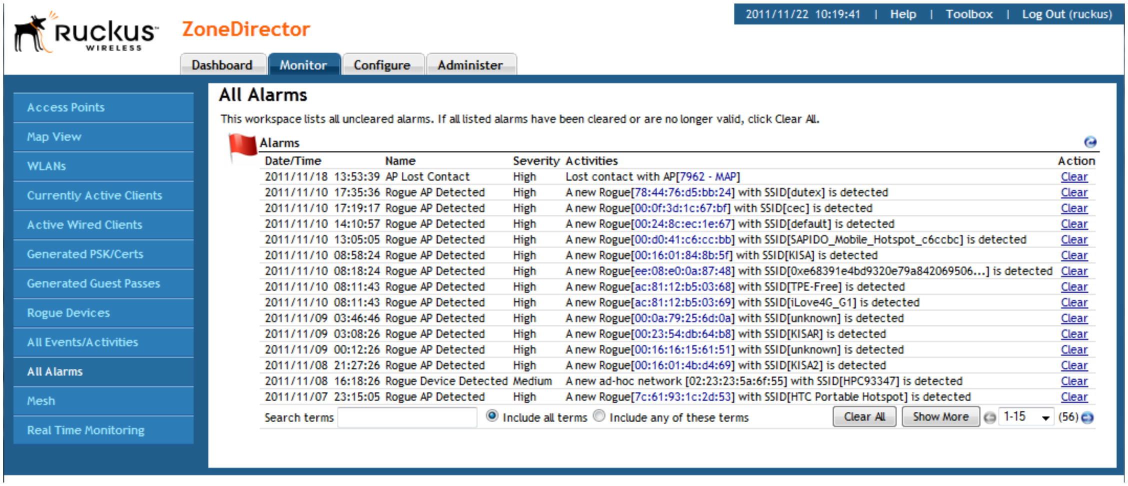
	A "bug" icon with a lock on it indicates a rogue AP with security enabled.
	In a Smart Mesh network, an isolated AP displays a red "X" above the icon.
	When Smart Mesh is enabled, a circled number appears next to the AP icon to indicate that it is a Mesh AP. The number indicates the number of hops from this Mesh AP to the Root AP.
	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.
	When Smart Mesh is enabled, a gray square (dimmed) with an arrow indicates that it is a Root AP without any active downlinks.
	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.

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 115. The All Alarms page



All Alarms

This workspace lists all uncleared alarms. If all listed alarms have been cleared or are no longer valid, click Clear All.

Alarms

Date/Time	Name	Severity	Activities	Action
2011/11/18 13:53:39	AP Lost Contact	High	Lost contact with AP[7962 - MAP]	Clear
2011/11/10 17:35:36	Rogue AP Detected	High	A new Rogue[78:44:76:d5:bb:24] with SSID[dutex] is detected	Clear
2011/11/10 17:19:17	Rogue AP Detected	High	A new Rogue[00:0f:3d:1c:67:bf] with SSID[cec] is detected	Clear
2011/11/10 14:10:57	Rogue AP Detected	High	A new Rogue[00:24:8c:ec:1e:67] with SSID[default] is detected	Clear
2011/11/10 13:05:05	Rogue AP Detected	High	A new Rogue[00:d0:41:c6:cc:bb] with SSID[SAPIDO_Mobile_Hotspot_c6ccbc] is detected	Clear
2011/11/10 08:58:24	Rogue AP Detected	High	A new Rogue[00:16:01:84:8b:5f] with SSID[KISA] is detected	Clear
2011/11/10 08:18:24	Rogue AP Detected	High	A new Rogue[ee:08:e0:0a:87:48] with SSID[0xe68391e4bd9320e79a842069506...] is detected	Clear
2011/11/10 08:11:43	Rogue AP Detected	High	A new Rogue[ac:81:12:b5:03:68] with SSID[TPE-Free] is detected	Clear
2011/11/10 08:11:43	Rogue AP Detected	High	A new Rogue[ac:81:12:b5:03:69] with SSID[iLove4G_G1] is detected	Clear
2011/11/09 03:46:46	Rogue AP Detected	High	A new Rogue[00:0a:79:25:6d:0a] with SSID[unknown] is detected	Clear
2011/11/09 03:08:26	Rogue AP Detected	High	A new Rogue[00:23:54:db:64:b8] with SSID[KISAR] is detected	Clear
2011/11/09 00:12:26	Rogue AP Detected	High	A new Rogue[00:16:16:15:61:51] with SSID[unknown] is detected	Clear
2011/11/08 21:27:26	Rogue AP Detected	High	A new Rogue[00:16:01:4b:d4:69] with SSID[KISA2] is detected	Clear
2011/11/08 16:18:26	Rogue Device Detected	Medium	A new ad-hoc network [02:23:23:5a:6f:55] with SSID[HPC93347] is detected	Clear
2011/11/07 23:15:05	Rogue AP Detected	High	A new Rogue[7c:61:93:1c:2d:53] with SSID[HTC Portable Hotspot] is detected	Clear

Search terms ● Include all terms ○ Include any of these terms

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 Currently Active 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.

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.

Reviewing Current User Activity

You can monitor current wireless users on a per-client basis by doing the following:

1. Go to **Monitor** > **Currently Active Clients**.
2. When the *Currently Active 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.

To review blocked clients, go to **Configure > Access Control > Blocked Clients**.

Monitoring Individual Clients

You can monitor individual wireless clients by clicking on the MAC address of any connected client from the *Currently Active Clients* page, the *All Events/Activities* page and other tables where client information is displayed.

To view detailed information about a specific client

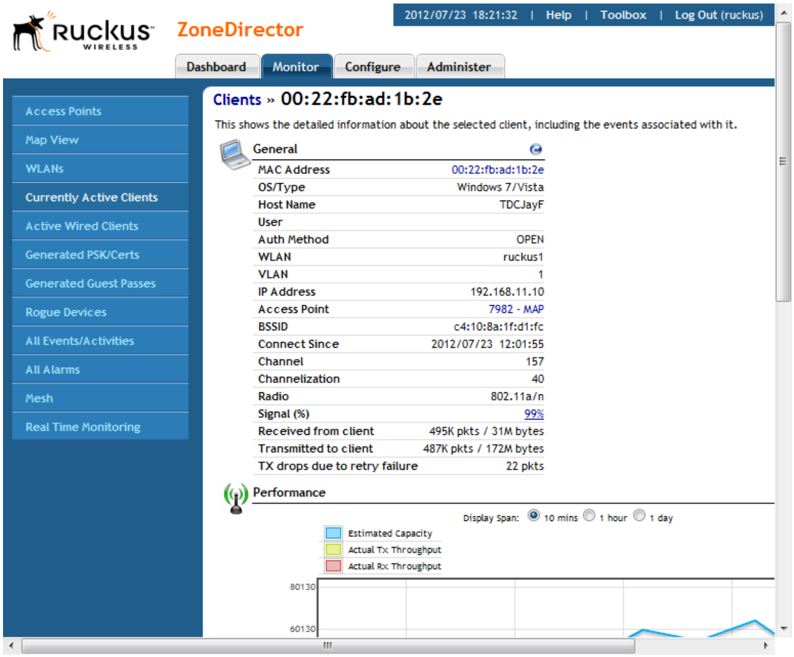
1. Go to **Monitor > Currently Active Clients**.
2. Click the link for the MAC address of the client you want to monitor. The page refreshes to display a page of client specific information and statistics.

The *Monitoring > Currently Active Clients > [client MAC address]* page displays the following information about the connected client.

Table 28. Client information details

Heading	Description
General	Displays general information on the client, including AP and WLAN connected to, channel and signal strength indication.
Performance	Displays a graphical view of client performance.The Performance analysis graph plots the estimated capacity and actual throughput over time. (Limitation: the capacity curve is updated only when the AP transmits packets containing at least 1024 bytes of data.)
Events	Displays a client-specific subset of the events in the All Events/ Activities table.

Figure 116. Viewing individual client information and performance statistics



Clients » 00:22:fb:ad:1b:2e

This shows the detailed information about the selected client, including the events associated with it.

General

MAC Address	00:22:fb:ad:1b:2e
OS/Type	Windows 7/Vista
Host Name	TDCJayF
User	
Auth Method	OPEN
WLAN	ruckus1
VLAN	1
IP Address	192.168.11.10
Access Point	7982 - MAP
BSSID	c4:10:8a:1f:d1:fc
Connect Since	2012/07/23 12:01:55
Channel	157
Channelization	40
Radio	802.11a/n
Signal (%)	99%
Received from client	495K pkts / 31M bytes
Transmitted to client	487K pkts / 172M bytes
TX drops due to retry failure	22 pkts

Performance

Display Span: ● 10 mins ○ 1 hour ○ 1 day

Monitoring Wired Clients

You can also monitor currently connected wired clients using the **Monitor > Active Wired Clients** page. Note that connected devices will only be displayed when 802.1X is enabled on the Ethernet port to which they are connected. 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 two tables: *Currently Managed APs* and *Events/Activities*. Both sections list the first 15 entries by default and can be expanded using the **Show More** button. Click on the MAC address, device 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 29. 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 **Configure > Access Points** page by clicking the **Edit** link next to the AP's MAC address.
Description	The AP's "description." This can be modified on the **Configure > Access Points** page by clicking the **Edit** link next to the AP's MAC address.
Location	The AP's "location." This can be modified on the **Configure > Access Points** page by clicking the **Edit** 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.

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.
Action	These icons allow you to configure and troubleshoot APs individually. See "Using Action Icons to Configure and Troubleshoot APs in a Mesh" on page 247.

Events/Activities

This table displays an AP-related subset of the information on the **Monitor > All Events/ Activities** page.

Monitoring Individual APs

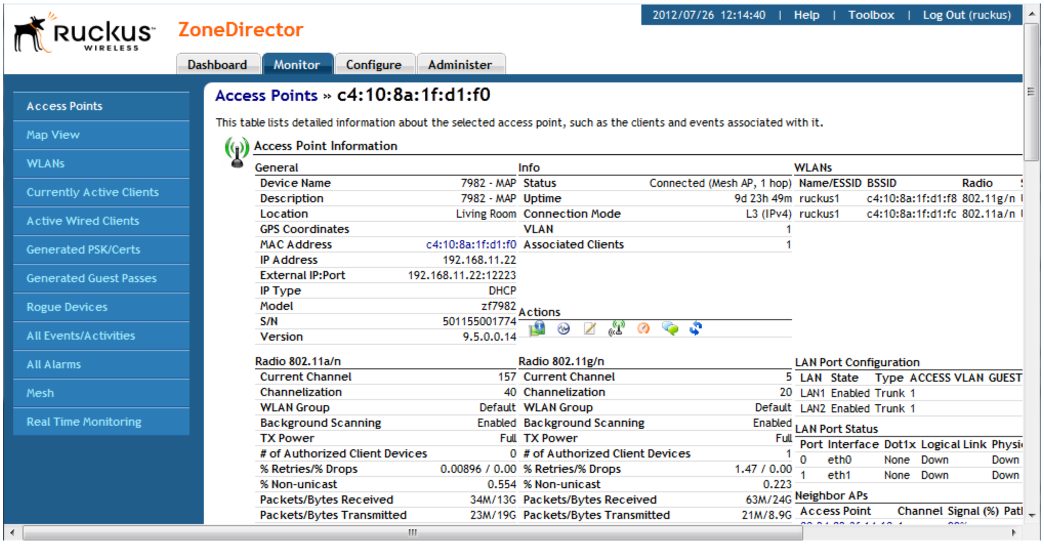
When you click on the MAC address of any AP, the **Monitor > Access Points** page changes to a detailed view of information related to that AP.

The **Monitor > Access Points > [MAC Address]** page provides the following details on the specific AP:

Table 30. 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 "Using Action Icons to Configure and Troubleshoot APs in a Mesh").
WLANs	Displays the WLANs that this AP is supporting.
Radio 802.11(a/n or g/n)	Displays details on the 2.4 GHz (g/n) and 5 GHz (a/n) radios. Transmission statistics are totals since last radio restart.
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.
Performance	Displays a graphical view of AP performance and RF environment statistics.Three Performance analysis graphs plot the capacity, throughput, associated clients and RF contention in the channel as a function of time. Limitations: (1) The capacity curve 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. (2) The Other APs curve counts managed APs plus unmanaged BSSIDs, many of which may emanate from the same unmanaged AP.
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 "Orientation" 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 *All Events / Activities* table.

Figure 117. Viewing an individual AP's information



Access Points » c4:10:8a:1f:d1: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	7982 - MAP	Status	Connected (Mesh AP, 1 hop)
Description	7982 - MAP	Uptime	9d 23h 49m
Location	Living Room	Connection Mode	L3 (IPv4)
GPS Coordinates		VLAN	1
MAC Address	c4:10:8a:1f:d1:f0	Associated Clients	1
IP Address	192.168.11.22		
External IP:Port	192.168.11.22:12223		
IP Type	DHCP		
Model	zf7982		
S/N	501155001774		
Version	9.5.0.0.14		

WLANs

Name/ESSID	BSSID	Radio
ruckus1	c4:10:8a:1f:d1:f8	802.11g/n
ruckus1	c4:10:8a:1f:d1:fc	802.11a/n

Radio 802.11a/n		Radio 802.11g/n	
Current Channel	157	Current Channel	5
Channelization	40	Channelization	20
WLAN Group	Default	WLAN Group	Default
Background Scanning	Enabled	Background Scanning	Enabled
TX Power	Full	TX Power	Full
# of Authorized Client Devices	0	# of Authorized Client Devices	1
% Retries/% Drops	0.00896 / 0.00	% Retries/% Drops	1.47 / 0.00
% Non-unicast	0.554	% Non-unicast	0.223
Packets/Bytes Received	34M/13G	Packets/Bytes Received	63M/24G
Packets/Bytes Transmitted	23M/19G	Packets/Bytes Transmitted	21M/8.9G

LAN Port Configuration

LAN	State	Type	ACCESS VLAN	GUEST
LAN1	Enabled	Trunk	1	
LAN2	Enabled	Trunk	1	

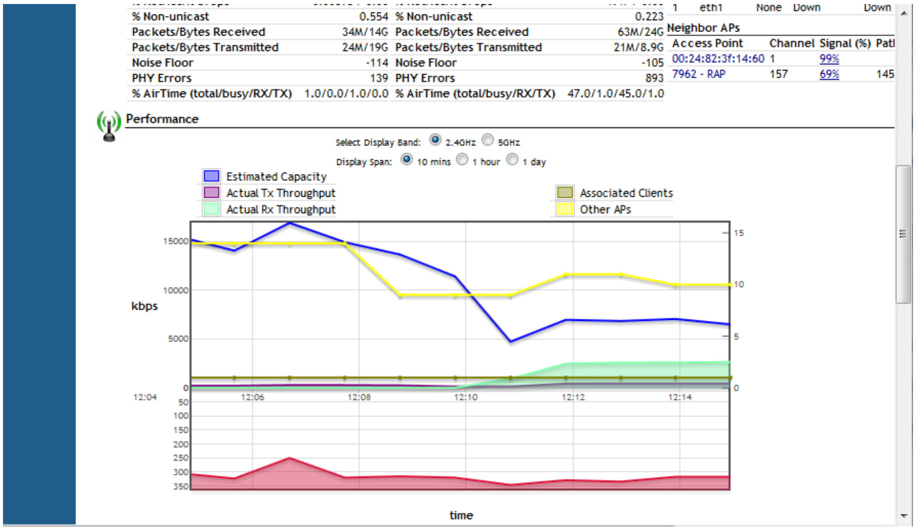
LAN Port Status

Port	Interface	Dot1x	Logical Link	Physi
0	eth0	None	Down	Down
1	eth1	None	Down	Down

Neighbor APs

Access Point	Channel	Signal (%)	Patl

Figure 118. Monitoring an AP's performance



% Non-unicast	0.554	% Non-unicast	0.223
Packets/Bytes Received	34M/14G	Packets/Bytes Received	63M/24G
Packets/Bytes Transmitted	24M/19G	Packets/Bytes Transmitted	21M/8.9G
Noise Floor	-114	Noise Floor	-105
PHY Errors	139	PHY Errors	893
% AirTime (total/busy/RX/TX)	1.0/0.0/1.0/0.0	% AirTime (total/busy/RX/TX)	47.0/1.0/45.0/1.0

1	eth1	None	Down	Down

Neighbor APs

Access Point	Channel	Signal (%)	Patl
00:24:82:3f:14:60	1	99%	
7962 - RAP	157	69%	145

Performance

Select Display Band: ● 2.4GHz ○ 5GHz

Display Span: ● 10 mins ○ 1 hour ○ 1 day

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

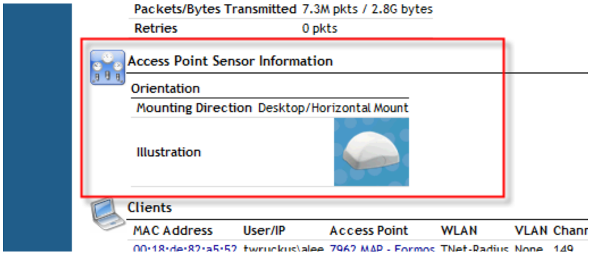
If your APs include internal sensors, ZoneDirector will display the AP's status in this section. Temperature and orientation sensors are available on most Ruckus Wireless outdoor APs, and orientation sensors are available on the ZoneFlex 7962 indoor AP.

Orientation

This sensor displays the mounting orientation of the AP. Three orientations are possible:

- Desktop/Horizontal Mount
- Ceiling/Horizontal Mount
- Wall/Vertical Mount

Figure 119. 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	

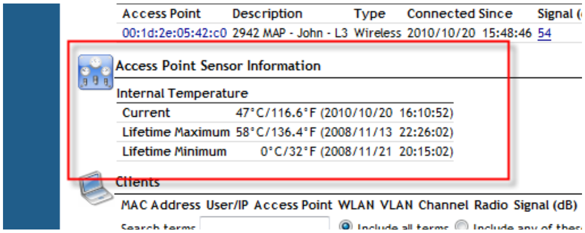
Clients

MAC Address	User/IP	Access Point	WLAN	VLAN	Chanr
00:18:de:82:a5:52	twruckus\alee	7962 MAP - Formos	TNet-Radius	None	149

Temperature

This sensor displays the temperature statistics as reported by the AP.

Figure 120. AP temperature sensor information



Access Point	Description	Type	Connected Since	Signal (
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

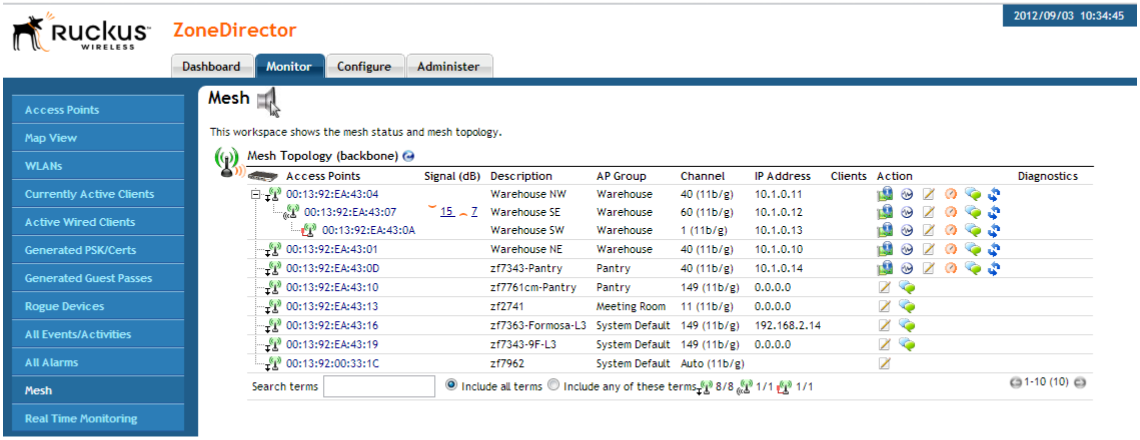
MAC Address	User/IP	Access Point	WLAN	VLAN	Channel	Radio	Signal (dB)

Search terms ● Include all terms ○ Include any of thes

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 121. Reviewing Mesh status of APs using the Monitor > Mesh page



Mesh

This workspace shows the mesh status and mesh topology.

Mesh Topology (backbone)

Access Points	Signal (dB)	Description	AP Group	Channel	IP Address	Clients	Action	Diagnostics
00:13:92:EA:43:04		Warehouse NW	Warehouse	40 (11b/g)	10.1.0.11			
00:13:92:EA:43:07	15 7	Warehouse SE	Warehouse	60 (11b/g)	10.1.0.12			
00:13:92:EA:43:0A		Warehouse SW	Warehouse	1 (11b/g)	10.1.0.13			
00:13:92:EA:43:01		Warehouse NE	Warehouse	40 (11b/g)	10.1.0.10			
00:13:92:EA:43:0D		zf7343-Pantry	Pantry	40 (11b/g)	10.1.0.14			
00:13:92:EA:43:10		zf7761cm-Pantry	Pantry	149 (11b/g)	0.0.0.0			
00:13:92:EA:43:13		zf2741	Meeting Room	11 (11b/g)	0.0.0.0			
00:13:92:EA:43:16		zf7363-Formosa-L3	System Default	149 (11b/g)	192.168.2.14			
00:13:92:EA:43:19		zf7343-9F-L3	System Default	149 (11b/g)	0.0.0.0			
00:13:92:00:33:1C		zf7962	System Default	Auto (11b/g)				

Search terms ● Include all terms ○ Include any of these terms 8/8 1/1 1/1 1-10 (10)

Detecting Rogue Access Points

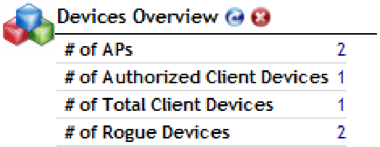
As contrasted with "neighboring" access points that are parts of a neighboring WLAN, "rogue" (unauthorized) APs pose problems for a wireless network. Usually, a rogue AP appears in the following way: an employee obtains another manufacturer's AP and connects it to the LAN, to gain wireless access to 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.

Your ZoneDirector rogue detection options include identifying the presence of a rogue AP, and locating it on your worksite floorplan prior to its removal. You can also mark rogue APs as "Known" if they are located in a neighboring network—outside your worksite—and pose no threat.

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 122. Rogue devices indicator



Devices Overview

# of APs	2
# of Authorized Client Devices	1
# of Total Client Devices	1
# of Rogue Devices	2

2. When the **Monitor** > **Rogue Devices** page appears, two tables are listed:
   - The *Currently Active Rogue Devices* table
   - The *Known/Recognized Rogue Devices* table.
3. Review the *Currently Active Rogue Devices* table. The following types of Rogue APs generate an alarm when ZoneDirector detects them:
   - *SSID-spoof*: A rogue AP that uses the same SSID as ZoneDirector's AP, also known as *Evil-twin AP*.
   - *MAC-spoof*: A rogue AP that has the same BSSID (MAC) as one of the virtual APs managed by ZoneDirector.
   - *Same-Network spoof*: Wired reverse ARPs similar to Rogue AP BSSID.

   The *Encryption* column indicates if a rogue device is encrypted or is open.
4. If a listed AP is part of another, nearby 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.
5. To locate rogue APs that do pose a threat to your internal WLAN, click the MAC Address of a device to open the Map View.
6. If your worksite floorplan is imported into the Map View window and your APs are positioned on the map, rogue APs can be generally identified with relative accuracy.
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."

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" on page 182 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.

7

Managing User Access

In This Chapter

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.

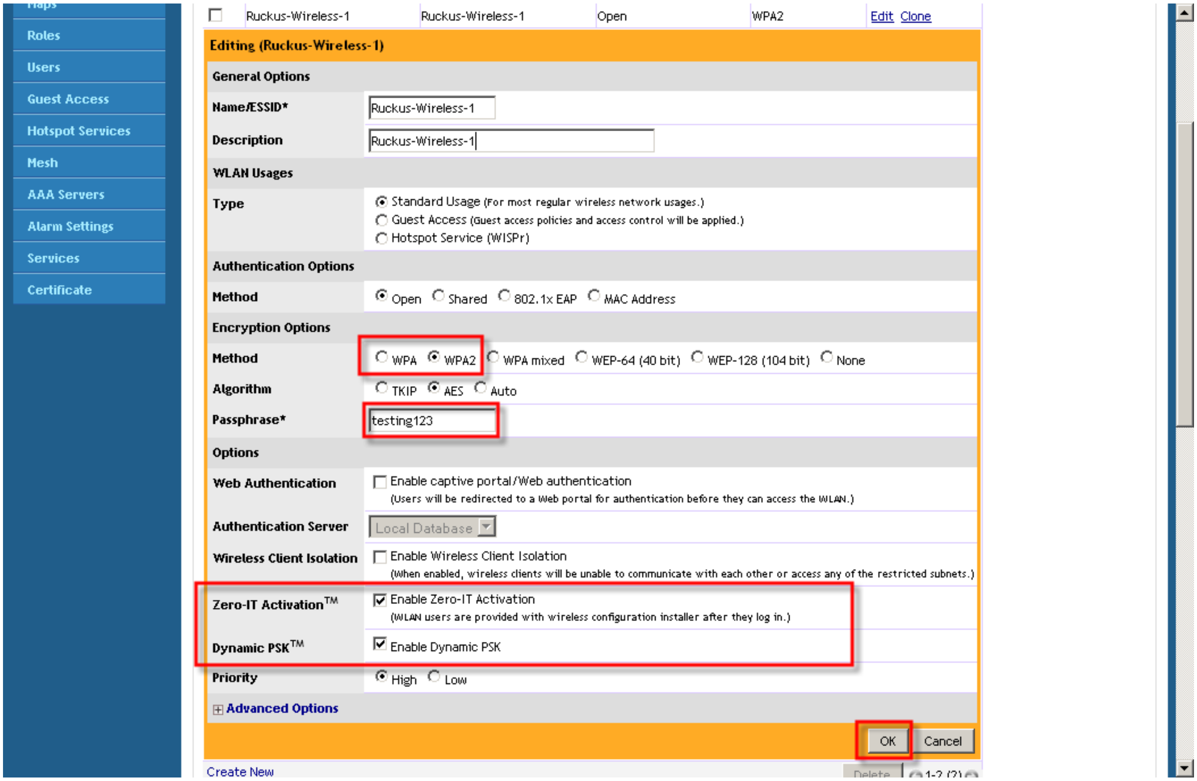
Before enabling Zero-IT, make sure you have at least one of each of the following configured:

- 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 **WPA** or **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 *WPA* or *WPA2* encryption only; see "Working with Dynamic Pre-Shared Keys" on page 146 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 123. Enabling Zero-IT for a WLAN



□	Ruckus-Wireless-1	Ruckus-Wireless-1	Open	WPA2

Editing (Ruckus-Wireless-1)

General Options

Name/ESSID* Ruckus-Wireless-1

Description Ruckus-Wireless-1

WLAN Usages

Type
● Standard Usage (For most regular wireless network usages.)
○ Guest Access (Guest access policies and access control will be applied.)
○ Hotspot Service (WISPr)

Authentication Options

Method ● Open ○ Shared ○ 802.1x EAP ○ MAC Address

Encryption Options

Method ○ WPA ● WPA2 ○ WPA mixed ○ WEP-64 (40 bit) ○ WEP-128 (104 bit) ○ None

Algorithm ○ TKIP ● AES ○ Auto

Passphrase* testing123

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

Wireless Client Isolation □ Enable Wireless Client Isolation
(When enabled, wireless clients will be unable to communicate with each other or access any of the restricted subnets.)

Zero-IT Activation™ ☑ Enable Zero-IT Activation
(WLAN users are provided with wireless configuration installer after they log in.)

Dynamic PSK™ ☑ Enable Dynamic PSK

Priority ● High ○ Low

Advanced Options

OK Cancel

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 computer to securely access your wireless LANs.

Clients that Support Zero-IT

Zero-IT Activation can be used with most modern operating systems including Windows (7/Vista/XP), Apple OS X, Apple iOS, Windows Phone and Android OS.

Note however, that some clients and operating systems may require special procedures for Zero-IT to work. For example, handheld devices without Ethernet ports must use the Self-Provisioning Clients without Ethernet Ports procedure.

For clients with Ethernet ports, the user simply connects to the ZoneDirector activation URL and runs the self-activation script. Any user running Windows 7 or Windows Vista can complete this procedure.

On Windows XP however, the user must generally be logged in as an "Administrator" with registry edit privileges. It is possible to allow WinXP clients to run prov.exe (the Zero-IT application) without being logged in as Administrator. To do this, an administrator must change the following two registry settings for the non-admin users/groups on each WinXP machine:

- `HKLM\SYSTEM\CurrentControlSet\Control\Class\{4D36E972-E325-11CE-BFC1-08002BE10318}` > Allow user to define value and create subkey
- `HKLM\SOFTWARE\Microsoft\WZCSVC\Parameters\Interfaces` > Add total rights permission

Additionally, you must enable permission to modify WZC (Windows Zero Configuration) for the users/groups by creating a new security template and applying the template to the account using MMC (Microsoft Management Console).

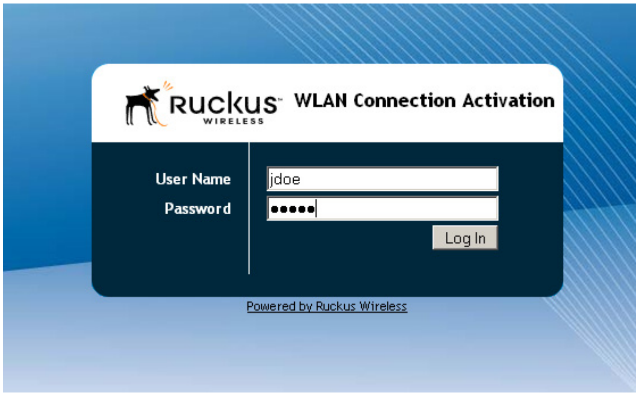
For clients running Mac OS X, the user must be logged in as an administrator for Zero-IT configuration to work.

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 computer is running a supported operating system, an automated script will launch.

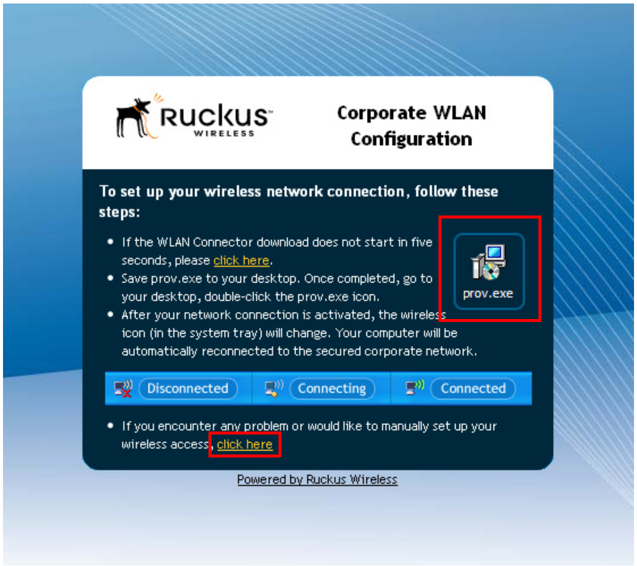
Figure 124. Zero-IT automatic activation



User Name: jdoe
Password: ●●●●●

4. Run the `prov.exe` script to automatically configure this computer's wireless settings for secure access to the WLAN.
5. If you are not running a supported operating system, you can manually configure wireless settings by clicking the link at the bottom of the page (see "Provisioning Clients that Do Not Support Zero-IT" on page 207).

Figure 125. Corporate WLAN configuration



Corporate WLAN Configuration

To set up your wireless network connection, follow these steps:

- If the WLAN Connector download does not start in five seconds, please click here.
- Save prov.exe to your desktop. Once completed, go to your desktop, double-click the prov.exe icon.
- After your network connection is activated, the wireless icon (in the system tray) will change. Your computer will be automatically reconnected to the secured corporate network.

- If you encounter any problem or would like to manually set up your wireless access, click here

Powered by Ruckus Wireless

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 iPhone, iPad, Windows Phone and Android smartphones can also use Zero-IT Activation. However, since these devices do not have Ethernet ports, the setup required is somewhat more complicated.

First, you will need to create a separate provisioning WLAN with Hotspot service so that these devices can be provisioned over the air rather than via Ethernet. Clients without Ethernet ports will need to login to this Hotspot WLAN first before gaining access to the Zero-IT Activation URL. Once logged in, they connect to the Activation URL to download the self-provisioning tool. Running this tool provisions the device for access to any of the "real" WLANs for which the user is authorized.

To enable Zero-IT activation over the air

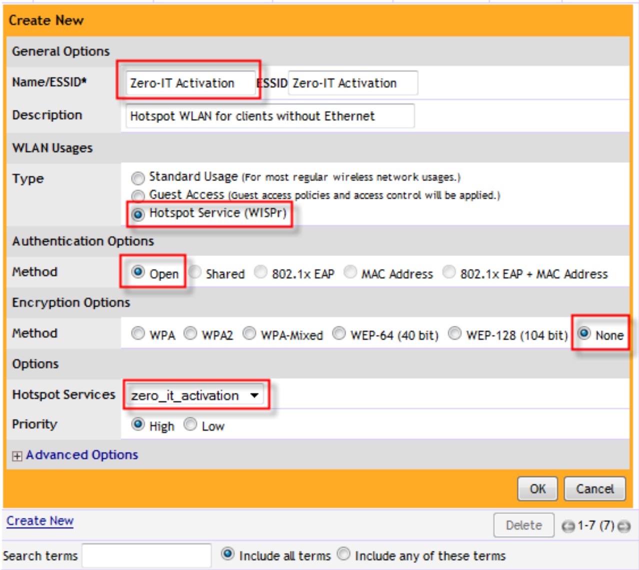
1. Create a Hotspot service (see "Working with Hotspot Services" on page 138). The only details required are:
   - **Name**: For example, "`Zero-IT Activation`")
   - **Login Page** URL: For example, "`https://<zonedirector IP address or host name>/activate`"
2. Go to **Configure > WLANs**. In the *WLANs* section, click **Create New** to create a new WLAN (see Figure 126).

3. Give the WLAN a **Name/ESSID** that is easy for users to recognize. Example: "Zero-IT Activation."
4. Under *WLAN Usages: Type*, select **Hotspot Service (WISPr)**.
5. Select the Hotspot service that you created in step 1 from the *Hotspot Services* drop-down menu. Ensure that *Authentication Method* is left as **Open** and *Encryption Method* as **None**.
6. Click **OK** to save this WLAN.

To self-provision a device over the air:

1. On your wireless client, select and connect to the "Zero-IT Activation" WLAN that you created in the previous procedure.
2. Launch your Web browser and browse to any HTTP Web address (not HTTPS). You will be redirected to the ZoneDirector Zero-IT Activation URL (you may need to click **Continue** at the security certificate warning page before redirection).
3. Enter your **User Name** and **Password** and click **Log In**.
4. Depending on the wireless client device, the auto-provisioning process may start automatically. If it does not start automatically, you will be prompted to run the auto-provisioning application, "prov.exe." Click **OK** to run "prov.exe" and auto-provision this client.
5. Following provisioning, on some devices such as iPhone and iPad, you will need to manually associate to the destination WLAN.

Figure 126. Creating a Hotspot WLAN for Zero-IT Activation of clients without Ethernet ports



Create New

General Options

Name/ESSID* Zero-IT Activation ESSID Zero-IT Activation

Description Hotspot WLAN for clients without Ethernet

WLAN Usages

Type ○ Standard Usage (For most regular wireless network usages.)
○ Guest Access (Guest access policies and access control will be applied.)
● Hotspot Service (WISPr)

Authentication Options

Method ● Open ○ Shared ○ 802.1x EAP ○ MAC Address ○ 802.1x EAP + MAC Address

Encryption Options

Method ○ WPA ○ WPA2 ○ WPA-Mixed ○ WEP-64 (40 bit) ○ WEP-128 (104 bit) ● None

Options

Hotspot Services zero_it_activation

Priority ● High ○ Low

NOTE: There is a known issue with certain versions of the iPhone Safari browser that results in browser crash when redirected by the Hotspot service. If you encounter this problem, disable auto-fill in the Safari browser settings or upgrade your iOS software to the latest version.

Provisioning Clients that Do Not Support Zero-IT

For clients that support Zero-IT, an activation script is generated that will automatically install security settings of WLANs configured on ZoneDirector to the client. If your users are connecting with computers running earlier versions of Windows, Linux, or other operating systems, no activation script will be provided for them. Instead, a detailed page containing all necessary wireless settings is provided. Users must perform manual configuration based on these settings. The following table describes the configurable parameters.

Table 31. Client authentication and wireless encryption options

Authentication Options	Encryption Options	Client Configurables
Open	WEP-64 WEP-128 WPA/WPA2/WPA-Mixed	Users must (1) manually enter the text of the same WEP key stored in ZoneDirector in their wireless configuration software, or (2) must manually enter the WPA passphrase.
Shared	WEP-64 WEP-128	Users must manually enter the same WEP key stored in ZoneDirector in their wireless configuration software.
802.1X	WEP-64 WEP-128 WPA/WPA2/WPA-Mixed	Users may need to obtain and install certificates generated on their computers, depending on the Transport Layer Security (TLS) authentication method used.
MAC Address	WEP-64 WEP-128 WPA/WPA2/WPA-Mixed	Users must (1) manually enter the text of the same WEP key stored in ZoneDirector in their wireless configuration software, or (2) must manually enter the WPA passphrase.

Adding New User Accounts to ZoneDirector

Once your wireless network is set up, you can instruct the Ruckus 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" on page 212.

Internal User Database

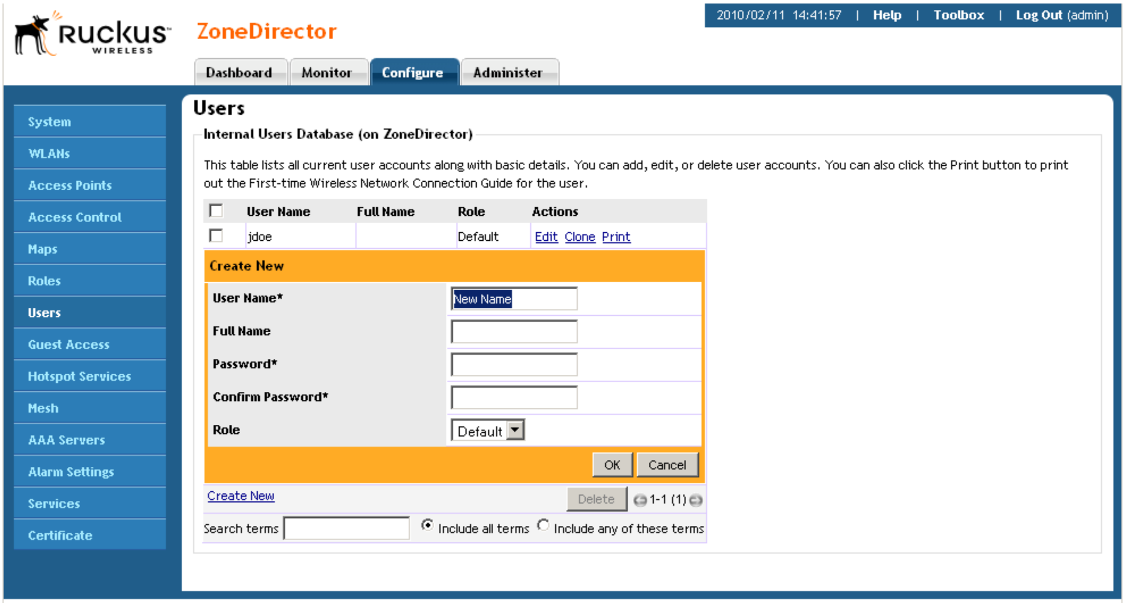
To use the internal user database as the default authentication source and to create new user accounts in the database

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, up to 32 characters in length, using letters, numbers and the period (.) character. User names are case-sensitive.
   - *Full Name*: Enter the assigned user's first and last name.
   - *Password*: Enter a unique password for this user, using a combination of letters and numbers, between 4 and 32 characters in length. Do not incorporate any letter spaces. Passwords are case-sensitive.
   - *Confirm Password*: Re-enter the same password for this user.

NOTE: ZoneDirector 1100 can support up to 1,250 combined total users and guest passes in the internal database. ZoneDirector 3000 licensed up to 250 APs can support up to 5,000 total users and guest passes, while ZoneDirector 3000 licensed from 300 to 500 APs can support up to 10,000. ZoneDirector 5000 can support up to 1,000 APs and 20,000 users. When the maximum number of PSKs that ZoneDirector supports has been reached, the Web interface may be slower in responding to requests.

4. If you have created roles that enable non-standard client logins or that gather staff members into workgroups, open the Role menu, and then choose the appropriate role for this user. For more information on roles and their application, see "Creating New User Roles" on page 210.
5. Click **OK** to save your settings. Be sure to communicate the user name and password to the appropriate end user.

Figure 127. The Create New form for adding users to the internal database



Users

Internal Users Database (on ZoneDirector)

This table lists all current user accounts along with basic details. You can add, edit, or delete user accounts. You can also click the Print button to print out the First-time Wireless Network Connection Guide for the user.

□	User Name	Full Name	Role	Actions
□	jdoe		Default	Edit Clone Print

Create New

User Name*	New Name
Full Name	
Password*	
Confirm Password*	
Role	Default

OK Cancel

Create New Delete 1-1 (1)

Search terms ● Include all terms ○ Include any of these terms

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" on page 210.)
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" on page 93).* Enter the **User Group** name here. Active Directory/LDAP users with the same group attributes are automatically mapped to this user role.

NOTE: For information on how to authenticate administrators using an external authentication server, refer to "Using an External Server for Administrator Authentication" on page 269.

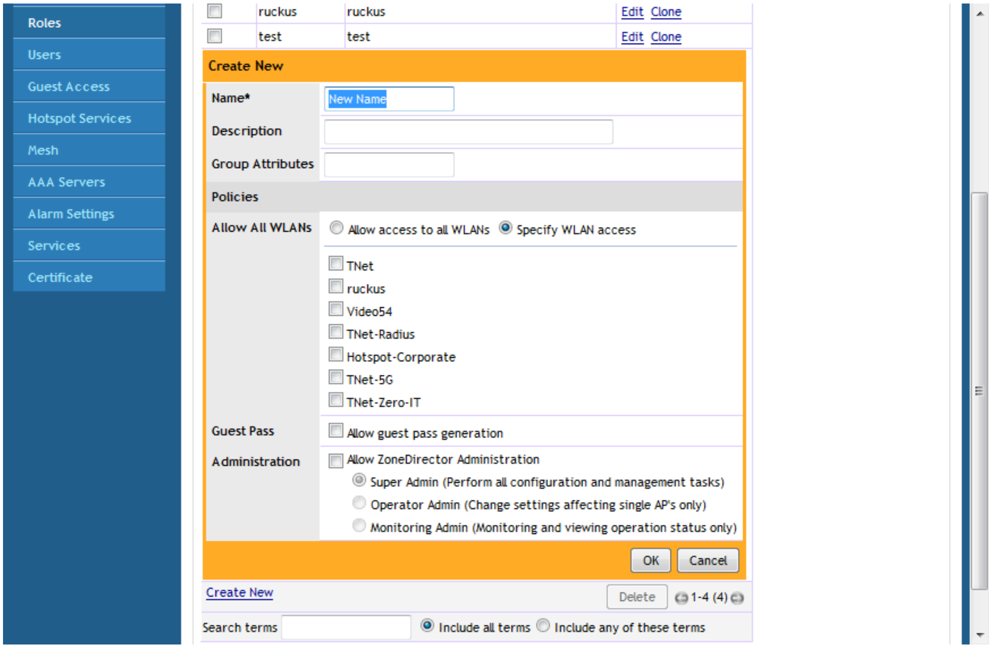
   - **Allow All WLANs**: You have two options: (1) **Allow Access to all WLANs**, or (2) **Specify WLAN Access**. If you select the second option, you must specify the WLANs by clicking the check box next to each one. This option requires that you create WLANs prior to setting this policy. See "Creating a WLAN" on page 114.
   - **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 128. The Create New form for adding a role



□	ruckus	ruckus	Edit Clone
□	test	test	Edit Clone

Create New

Name*	New Name
Description	
Group Attributes	

Policies

Allow All WLANs	○ Allow access to all WLANs ● Specify WLAN access □ TNet □ ruckus □ Video54 □ TNet-Radius □ Hotspot-Corporate □ TNet-5G □ TNet-Zero-IT
Guest Pass	□ Allow guest pass generation
Administration	□ Allow ZoneDirector Administration ● 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)

OK Cancel

Create New Delete 1-4 (4)

Search terms ● Include all terms ○ Include any of these terms

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.

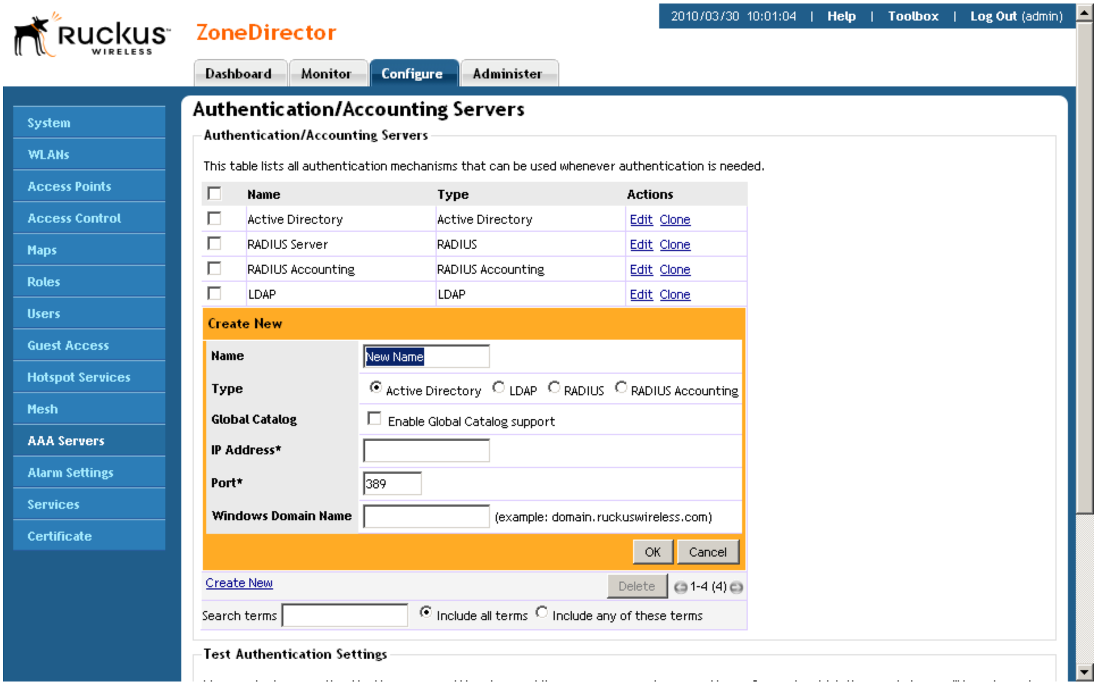
To use an external authentication server

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 129. The Create New form for adding an authentication server



Authentication/Accounting Servers

Authentication/Accounting Servers

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

□	Name	Type	Actions
□	Active Directory	Active Directory	Edit Clone
□	RADIUS Server	RADIUS	Edit Clone
□	RADIUS Accounting	RADIUS Accounting	Edit Clone
□	LDAP	LDAP	Edit Clone

Create New

Name	New Name
Type	● Active Directory ○ LDAP ○ RADIUS ○ RADIUS Accounting
Global Catalog	□ Enable Global Catalog support
IP Address*	
Port*	389
Windows Domain Name	(example: domain.ruckuswireless.com)

Search terms ● Include all terms ○ Include any of these terms

Test Authentication Settings

For more information on configuring an external authentication server, see "Using an External AAA Server" on page 89.

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.

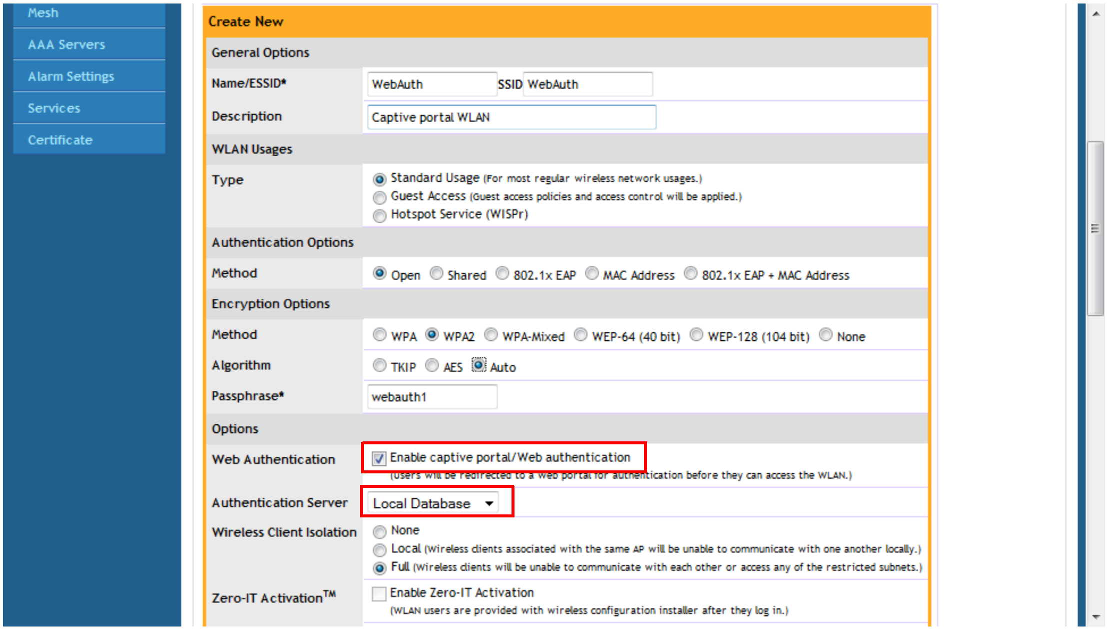
After you activate Web authentication on your WLAN, you must then provide all users with a URL to your login page. After they discover the WLAN on their wireless device or laptop, they open their browser, connect to the Login page and enter the required login information.

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 130.
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 130. Activating captive portal/Web authentication



Create New

General Options

Name/ESSID* WebAuth SSID WebAuth

Description Captive portal WLAN

WLAN Usages

Type
● Standard Usage (For most regular wireless network usages.)
○ Guest Access (Guest access policies and access control will be applied.)
○ Hotspot Service (WISPr)

Authentication Options

Method ● Open ○ Shared ○ 802.1x EAP ○ MAC Address ○ 802.1x EAP + MAC Address

Encryption Options

Method ○ WPA ● WPA2 ○ WPA-Mixed ○ WEP-64 (40 bit) ○ WEP-128 (104 bit) ○ None

Algorithm ○ TKIP ○ AES ● Auto

Passphrase* webauth1

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

Wireless Client Isolation
○ None
○ Local (Wireless clients associated with the same AP will be unable to communicate with one another locally.)
● Full (Wireless clients will be unable to communicate with each other or access any of the restricted subnets.)

Zero-IT Activation™ □ Enable Zero-IT Activation
(WLAN users are provided with wireless configuration installer after they log in.)

8

Managing Guest Access

In This Chapter

Configuring Guest Access

By default, all of your users are allowed to issue temporary "day use" guest passes for visitors and contractors. Such a guest pass allows its user to connect to the WLAN. You must decide whether or not to permit all—or some—users to generate guest passes.

Additionally, you may also want to review the default settings and policies that control guest use of the network. There are options you can fine-tune to fit your work environment.

This section describes how to configure a Guest WLAN and configure global Guest Access Policies in ZoneDirector.

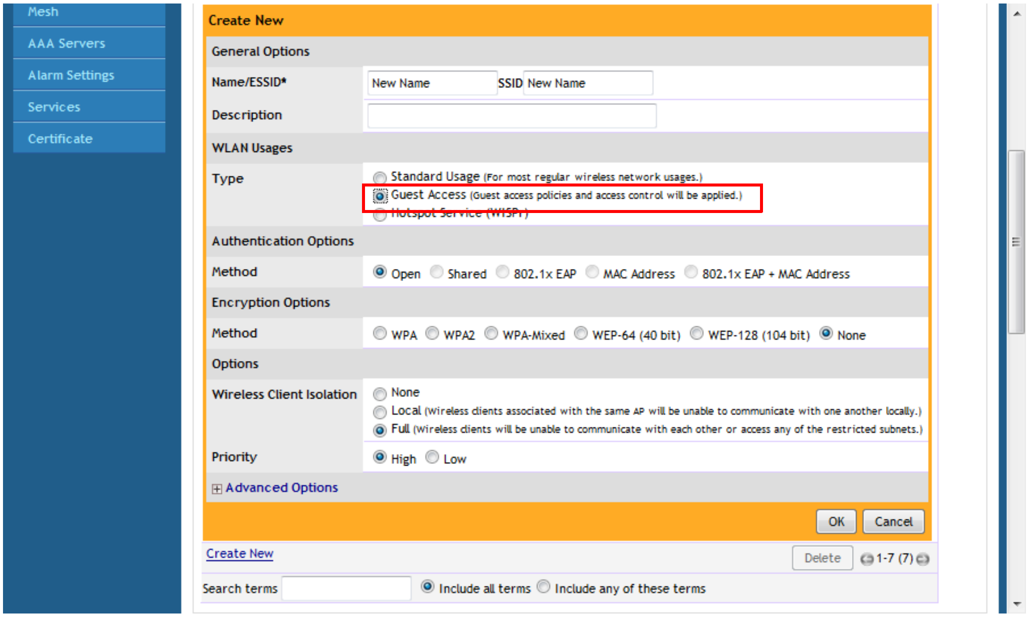
NOTE: ZoneDirector 1100 can support up to 1,250 combined total users and guest passes in the internal database. ZoneDirector 3000 licensed up to 250 APs can support up to 5,000 total users and guest passes, while ZoneDirector 3000 licensed from 300 to 500 APs can support up to 10,000. ZoneDirector 5000 can support up to 1,000 APs and 20,000 users. When the maximum number of PSKs that ZoneDirector supports has been reached, the Web interface may be slower in responding to requests.

Creating a Guest WLAN

If you want to allow guests temporary access to a controlled WLAN (separate from your internal users), the first step is to create a WLAN of the type "Guest Access."

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. If you want your internal wireless traffic to have priority over guest traffic, set the *Priority* to **Low**.
8. Under *Advanced Options*, select the options to enable for this WLAN. For more information on WLAN advanced options, see "Advanced Options" on page 119.
9. Click **OK** to save your changes.

Figure 131. Create a Guest Access WLAN



Create New

General Options

Name/ESSID* New Name SSID New Name

Description

WLAN Usages

Type ○ Standard Usage (For most regular wireless network usages.)
● Guest Access (Guest access policies and access control will be applied.)
○ Hotspot Service (WISPr)

Authentication Options

Method ● Open ○ Shared ○ 802.1x EAP ○ MAC Address ○ 802.1x EAP + MAC Address

Encryption Options

Method ○ WPA ○ WPA2 ○ WPA-Mixed ○ WEP-64 (40 bit) ○ WEP-128 (104 bit) ● None

Options

Wireless Client Isolation ○ None
○ Local (wireless clients associated with the same AP will be unable to communicate with one another locally.)
● Full (wireless clients will be unable to communicate with each other or access any of the restricted subnets.)

Priority ● High ○ Low

⊞ Advanced Options

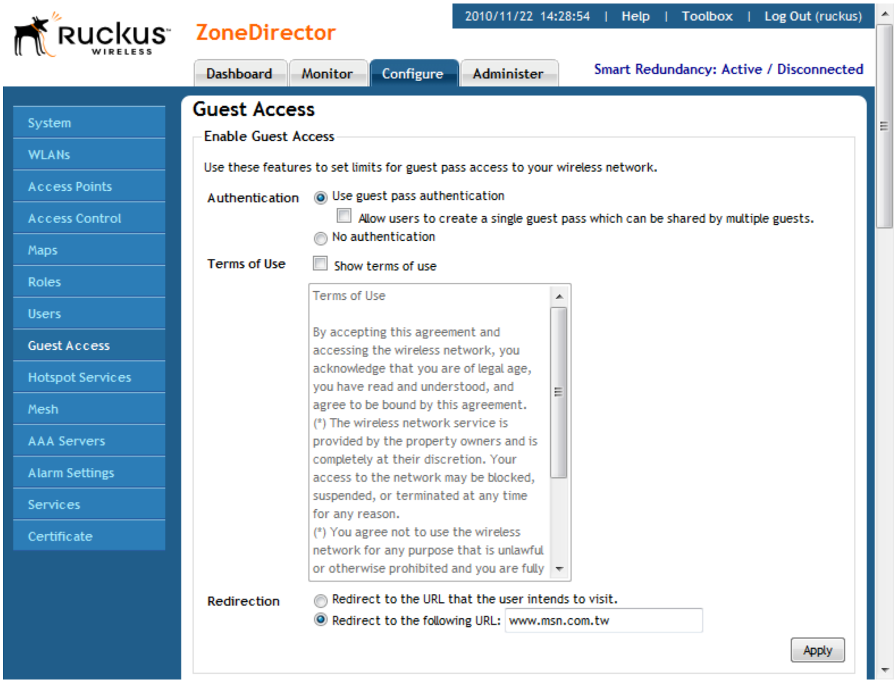
Search terms ● Include all terms ○ Include any of these terms

Configuring System-Wide Guest Access Policy

The *Enable Guest Access* options enable the administrator to define the system-wide guest access policy. You can require guests to validate their guest pass, accept terms of use, and be redirected to a URL you specify.

1. Go to **Configure** > **Guest Access**. The *Guest Access* page appears.
2. Under *Enable Guest Access*, select the *Authentication* type to use:
   - *Use guest pass authentication*: Redirect the user to a page requiring a valid guest pass before allowing the user to use the guest WLAN.
   - If you want multiple guests to be able to use the same guest pass simultaneously, select the **Allow multiple users to share a single guest pass** check box.
   - *No authentication*: Do not require redirection and guest pass validation.
3. 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.
4. 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.
5. Click **Apply** to save your settings.

Figure 132. The Guest Access page



Guest Access

Enable Guest Access

Use these features to set limits for guest pass access to your wireless network.

Authentication ● Use guest pass authentication
□ Allow users to create a single guest pass which can be shared by multiple guests.
○ No authentication

Terms of Use □ Show terms of use

Terms of Use

By accepting this agreement and accessing the wireless network, you acknowledge that you are of legal age, you have read and understood, and agree to be bound by this agreement.
(*) The wireless network service is provided by the property owners and is completely at their discretion. Your access to the network may be blocked, suspended, or terminated at any time for any reason.
(*) You agree not to use the wireless network for any purpose that is unlawful or otherwise prohibited and you are fully

Redirection ○ Redirect to the URL that the user intends to visit.
● Redirect to the following URL: www.msn.com.tw

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.

Activating Guest Pass Generation

You can grant authenticated users the privilege to generate guest passes. Do the following:

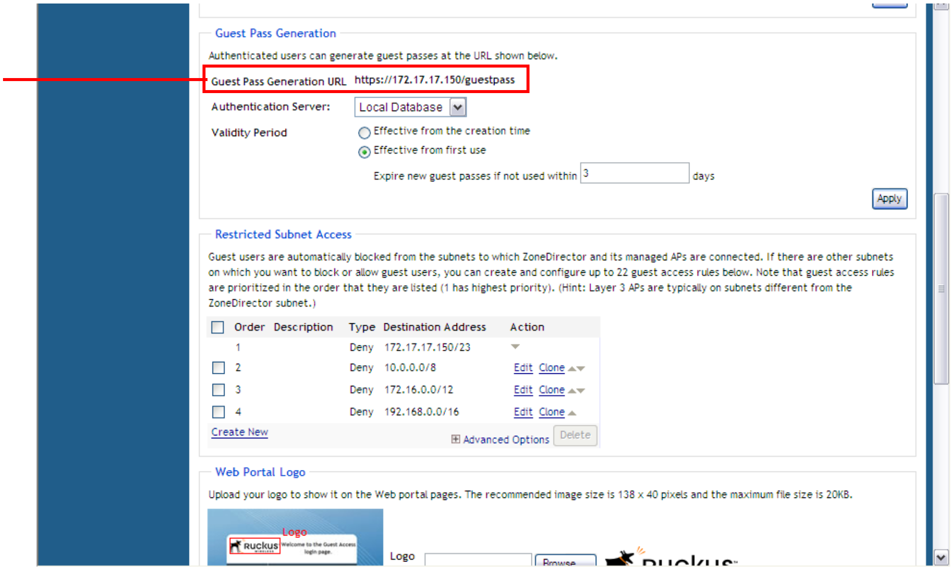
1. Go to **Configure** > **Guest Access**. The *Guest Access* page appears.
2. Scroll down to the *Guest Pass Generation* section.
3. In **Authentication Server**, select the authentication server that you want to use to authenticate users who want to generate guest passes.
   - If you configured an 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" on page 212.)
   - If you want to use ZoneDirector's internal database, select **Local Database**.
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 an unused guest pass will expire regardless of use. The default is 7 days.

5. 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 133, the Guest Pass Generation URL is `https://172.17.17.150/guestpass`.

Figure 133. The Guest Pass Generation section on the Guest Pass page



Guest Pass Generation URL

Guest Pass Generation

Authenticated users can generate guest passes at the URL shown below.

Guest Pass Generation URL https://172.17.17.150/guestpass

Authentication Server: Local Database

Validity Period
○ Effective from the creation time
● Effective from first use
Expire new guest passes if not used within 3 days

Apply

Restricted Subnet Access

Guest users are automatically blocked from the subnets to which ZoneDirector and its managed APs are connected. If there are other subnets on which you want to block or allow guest users, you can create and configure up to 22 guest access rules below. Note that guest access rules are prioritized in the order that they are listed (1 has highest priority). (Hint: Layer 3 APs are typically on subnets different from the ZoneDirector subnet.)

□	Order	Description	Type	Destination Address	Action
	1		Deny	172.17.17.150/23	
□	2		Deny	10.0.0.0/8	Edit Clone
□	3		Deny	172.16.0.0/12	Edit Clone
□	4		Deny	192.168.0.0/16	Edit Clone

Create New
⊞ Advanced Options
Delete

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.

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:

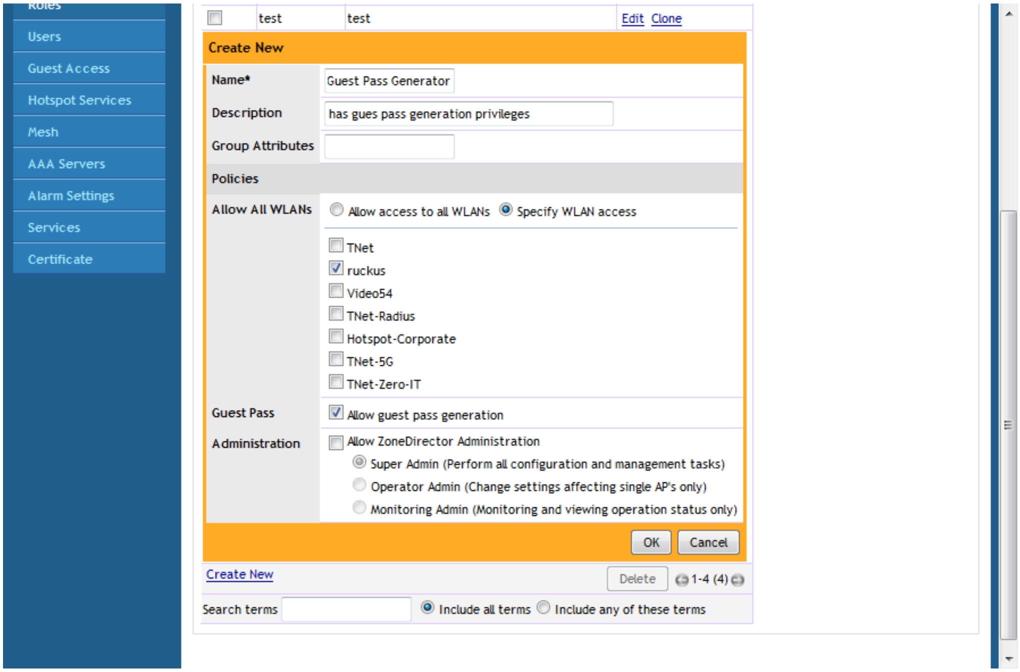
1. Go to **Configure** > **Roles**.
2. In the *Roles* table, click **Create New**.
3. When the *Create New* features appear, make these entries:
   - **Name**: Enter a name for this role (e.g., "Guest Pass Generator").
   - **Description**: Enter a short description of this role's application.
   - **Group 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 134. Create a guest pass generator Role



□ test test

Create New

Name*	Guest Pass Generator
Description	has gues pass generation privileges
Group Attributes	

Policies

Allow All WLANs: ○ Allow access to all WLANs ● Specify WLAN access

□ TNet
☑ ruckus
□ Video54
□ TNet-Radius
□ Hotspot-Corporate
□ TNet-5G
□ TNet-Zero-IT

Guest Pass: ☑ Allow guest pass generation

Administration: □ Allow ZoneDirector Administration
● 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)

Search terms ● Include all terms ○ Include any of these terms

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 Printing 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 printing a guest pass. For instructions on how to generate multiple guest passes, see "Generating and Printing Multiple Guest Passes at Once" on page 225.

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

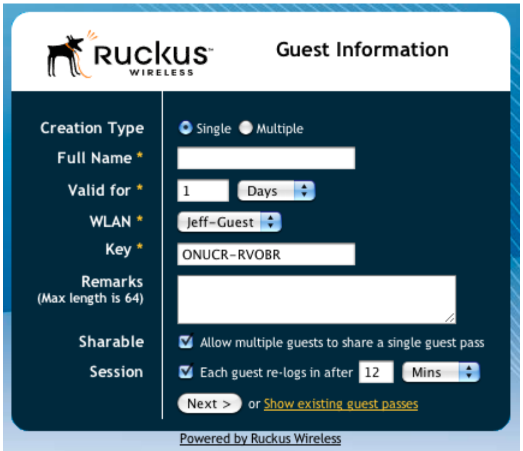
To generate a single guest pass

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 135. Creating a Guest Pass



Guest Information

Creation Type ● Single ○ Multiple
Full Name *
Valid for * 1 Days
WLAN * Jeff-Guest
Key * ONUCR-RVOBR
Remarks (Max length is 64)
Sharable ☑ Allow multiple guests to share a single guest pass
Session ☑ Each guest re-logs in after 12 Mins

6. On the Guest Information page, fill in the following options:
   - **Creation Type**: Choose **Single** to generate a single guest pass.

- **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 (**Minutes**, **Hours**, **Days** or **Weeks**).
- **WLAN**: Select the WLAN for this guest (typically, a “guest” WLAN).
- **Key**: Leave as is if you want to use the random key that ZoneDirector generated. If you want to use a key that is easy to remember, delete the random key, and then type a custom key. For example, if ZoneDirector generated the random key `OVEGS-RZKKF`, you can change it to `joe-guest-key`. Customized keys must be between one and 16 ASCII characters.

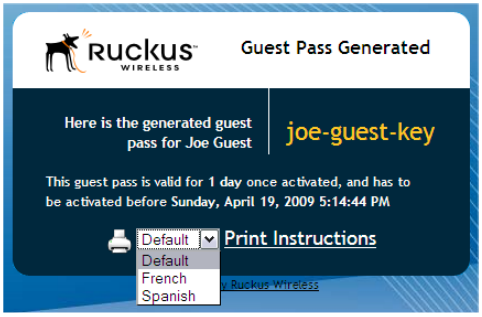
NOTE: Each guest pass key must be unique and is distributed on all guest WLANs. Therefore, you cannot create the same guest pass for use on multiple WLANs.

- **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**: Check this box to allow multiple users to share a single guest pass. (This option will only be available if you allowed multiple users to share a single guest pass on the *Configure > Guest Access* page.)
- **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 Guest Pass Generated page appears.
8. In the drop-down menu, select the guest pass instructions that you want to print out. If you did not create custom guest pass printouts, select **Default**.
9. Click **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 a guest pass for your guest user.

Figure 136. The Guest Pass Generated page (with customized key)



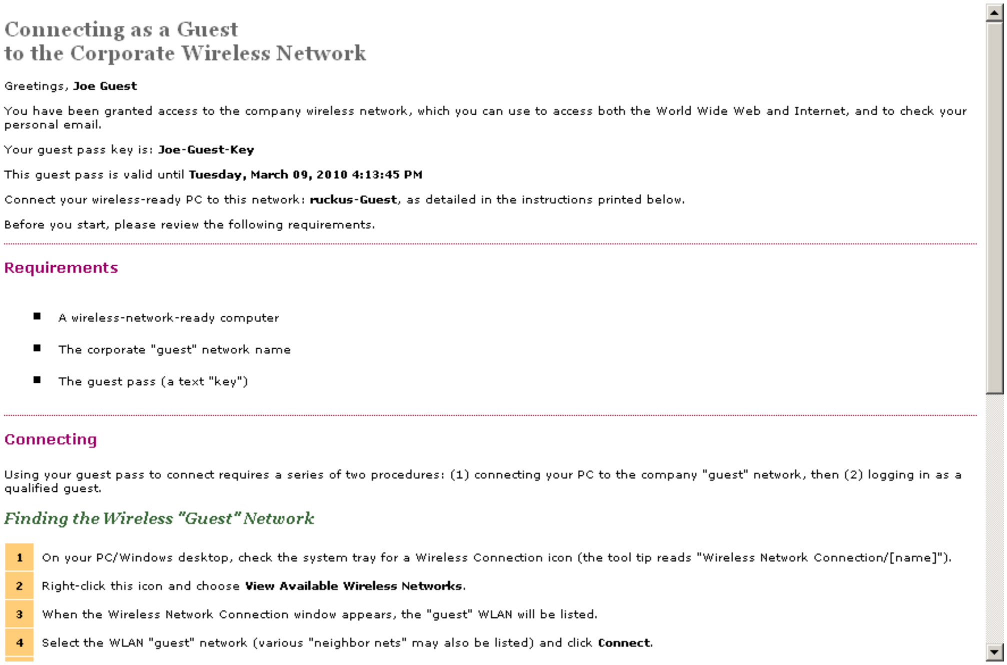
Guest Pass Generated

Here is the generated guest pass for Joe Guest

joe-guest-key

This guest pass is valid for 1 day once activated, and has to be activated before Sunday, April 19, 2009 5:14:44 PM

Figure 137. Sample guest pass printout



Connecting as a Guest to the Corporate Wireless Network

Greetings, **Joe Guest**

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

Your guest pass key is: **Joe-Guest-Key**

This guest pass is valid until **Tuesday, March 09, 2010 4:13:45 PM**

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

Before you start, please review the following requirements.

Requirements

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

Connecting

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

Finding the Wireless "Guest" Network

1 On your PC/Windows desktop, check the system tray for a Wireless Connection icon (the tool tip reads "Wireless Network Connection/[name]").

2 Right-click this icon and choose **View Available Wireless Networks**.

3 When the Wireless Network Connection window appears, the "guest" WLAN will be listed.

4 Select the WLAN "guest" network (various "neighbor nets" may also be listed) and click **Connect**.

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 Printing a Single Guest Pass" on page 222.

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

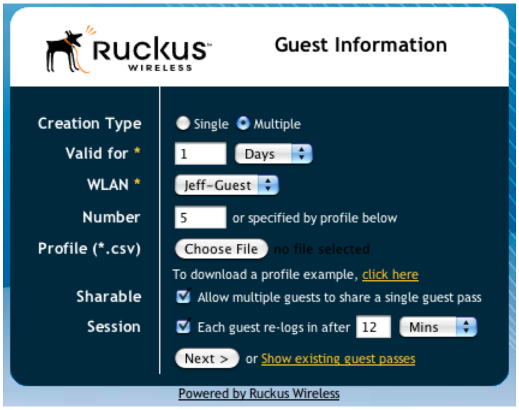
1. On your computer, start your Web browser.
2. In the address or location bar, type the URL of the ZoneDirector Guest Pass Generation page:

   `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 can not create the same guest pass for use on multiple WLANs.

   - **Profile (*.csv)**: If you have created a Guest Pass Profile (see "Creating a Guest Pass Profile" on page 226), use this option to import the file.
   - **Sharable**: Select this option if you want to allow multiple users to share a single guest pass. (This option will only be available if you allowed multiple users to share a single guest pass on the *Configure > Guest Access* page.)
   - **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 138. Generating multiple guest passes at once



Guest Information

Creation Type ○ Single ● Multiple

Valid for * 1 Days

WLAN * Jeff-Guest

Number 5 or specified by profile below

Profile (*.csv) Choose File no file selected

To download a profile example, click here

Sharable ☑ Allow multiple guests to share a single guest pass

Session ☑ Each guest re-logs in after 12 Mins

Next > or Show existing guest passes

Powered by Ruckus Wireless

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.

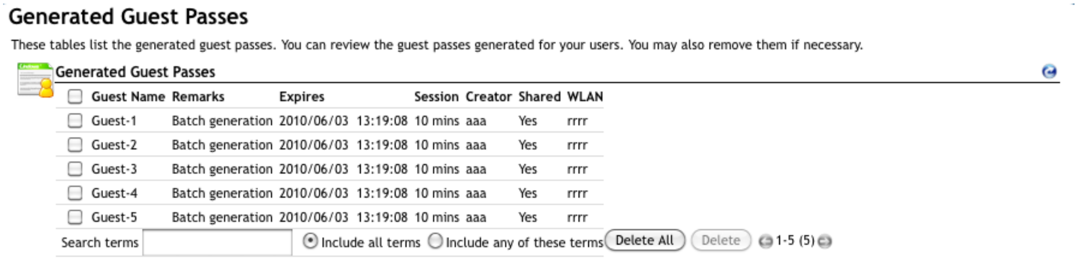
5. Using a spreadsheet application, open the CSV file and edit the guest pass profile by filling out the following columns:
   - *#Guest Name*: Type the name of the guest user (one name per row).
   - *Remarks*: (Optional) Type any note or remarks about the guest pass.
   - *Key*: Type a guest pass key 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.
4. Click the **Delete** button.

Figure 139. Viewing generated Guest Passes



Generated Guest Passes

These tables list the generated guest passes. You can review the guest passes generated for your users. You may also remove them if necessary.

Generated Guest Passes

□	Guest Name	Remarks	Expires	Session	Creator	Shared	WLAN
□	Guest-1	Batch generation	2010/06/03 13:19:08	10 mins	aaa	Yes	rrrr
□	Guest-2	Batch generation	2010/06/03 13:19:08	10 mins	aaa	Yes	rrrr
□	Guest-3	Batch generation	2010/06/03 13:19:08	10 mins	aaa	Yes	rrrr
□	Guest-4	Batch generation	2010/06/03 13:19:08	10 mins	aaa	Yes	rrrr
□	Guest-5	Batch generation	2010/06/03 13:19:08	10 mins	aaa	Yes	rrrr

Search terms ● Include all terms ○ Include any of these terms

Configuring Guest Subnet Access

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 Guest Access > 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).

NOTE: All guests share this same subnet access policy.

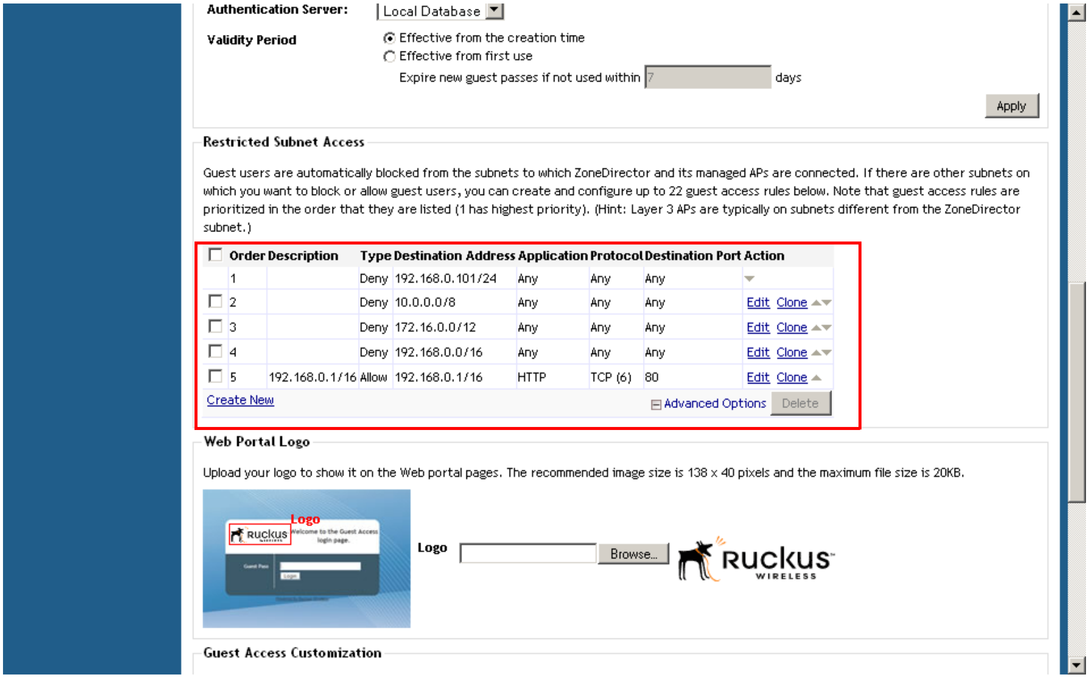
To create a guest access rule for a subnet

1. Go to **Configure** > **Guest Access**.

2. In the Restricted Subnet Access section, click **Create New**. Text boxes appear under the table columns in which you can enter parameters that define the access rule.
3. Under **Description**, type a name or description for the access rule that you are creating.
4. 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.
5. 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.
6. 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.
7. Click **OK** to save the subnet access rule.

Repeat Steps 2 to 7 to create up to 22 subnet access rules.

Figure 140. The Restricted Subnet Access options



Authentication Server: Local Database

Validity Period

● Effective from the creation time
○ Effective from first use
Expire new guest passes if not used within 7 days

Apply

Restricted Subnet Access

Guest users are automatically blocked from the subnets to which ZoneDirector and its managed APs are connected. If there are other subnets on which you want to block or allow guest users, you can create and configure up to 22 guest access rules below. Note that guest access rules are prioritized in the order that they are listed (1 has highest priority). (Hint: Layer 3 APs are typically on subnets different from the ZoneDirector subnet.)

□	Order	Description	Type	Destination Address	Application	Protocol	Destination Port	Action
	1		Deny	192.168.0.101/24	Any	Any	Any	▼
□	2		Deny	10.0.0.0/8	Any	Any	Any	Edit Clone ▲▼
□	3		Deny	172.16.0.0/12	Any	Any	Any	Edit Clone ▲▼
□	4		Deny	192.168.0.0/16	Any	Any	Any	Edit Clone ▲▼
□	5	192.168.0.1/16	Allow	192.168.0.1/16	HTTP	TCP (6)	80	Edit Clone ▲

Create New ⊟ Advanced Options Delete

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 Browse...

Guest Access Customization

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.

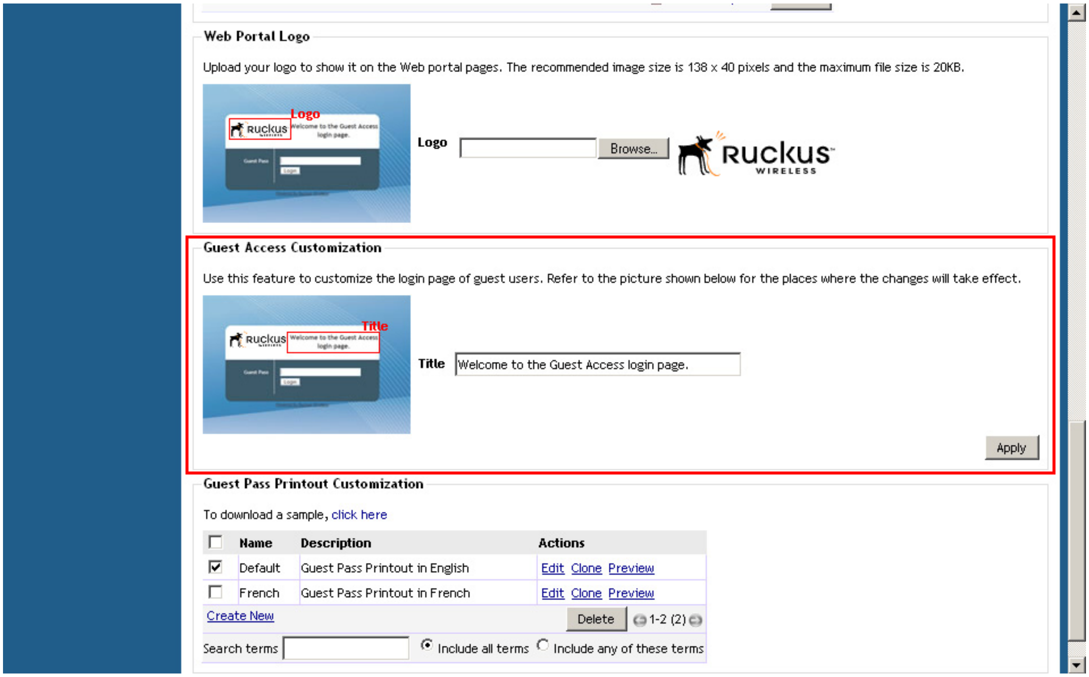
If you want to include a logo, you will need to prepare a Web-ready graphic file, in one of three acceptable formats (.JPG, .GIF or .PNG). Make sure that the logo file *does not exceed* the following:

- Length: Two inches on any side
- File size: 20KB

To customize the guest login page

1. Go to **Configure** > **Guest Access**.
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 **Apply** to save your settings. A `Settings applied!` confirmation message appears.

Figure 141. The Guest Access Customization options



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 [ ] Browse...

Guest Access Customization

Use this feature to customize the login page of guest users. Refer to the picture shown below for the places where the changes will take effect.

Title: Welcome to the Guest Access login page.

Guest Pass Printout Customization

To download a sample, click here

□	Name	Description	Actions
☑	Default	Guest Pass Printout in English	Edit Clone Preview
□	French	Guest Pass Printout in French	Edit Clone Preview

Create New — Delete — 1-2 (2)

Search terms [ ] ● Include all terms ○ Include any of these terms

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 (bottom of the page).
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" on page 230.
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 136).

Guest Pass Printout Tokens

Table 32 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 32. Tokens that you can use in the guest pass printout

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

9

Deploying a Smart Mesh Network

In This Chapter

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 "Smart Mesh Networking Best Practices" on page 293.

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 33. Mesh networking terms

Term	Definition
Mesh Node	A Ruckus Wireless ZoneFlex AP with mesh capability enabled.
Root AP (Root Access Point)	A mesh node that communicates with ZoneDirector through its Ethernet (that is, wired) interface.
Mesh AP (Mesh Access Point)	A mesh node that communicates with ZoneDirector through its wireless interface.
eMAP (Ethernet Mesh AP)	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.

Table 33. Mesh networking terms

Term	Definition
Mesh Tree	Each Mesh AP has exactly one uplink to another Mesh AP or Root AP. Each Mesh AP or Root AP could have multiple Mesh APs connecting to it. Thus, the resulting topology is a tree-like topology. A single ZoneDirector device can manage more than one mesh tree. There is no limit to the number of trees in a mesh. The only limitation on how many mesh trees the ZoneDirector can manage is dependent on the number of APs a ZoneDirector can manage. For example, a ZoneDirector 1006 can manage one mesh tree of 6 APs, two mesh trees of 3 APs each, or three mesh trees of 2 APs each.
Hop	The number of wireless mesh links a data packet takes from one Mesh AP to the Root AP. For example, if the Root AP is the uplink of Mesh AP 1, then Mesh AP 1 is *one* hop away from the Root AP. In the same scenario, if Mesh AP 1 is the uplink of Mesh AP 2, then Mesh AP 2 is *two* hops away from the Root AP. A maximum of 8 hops is supported.

Supported Mesh Topologies

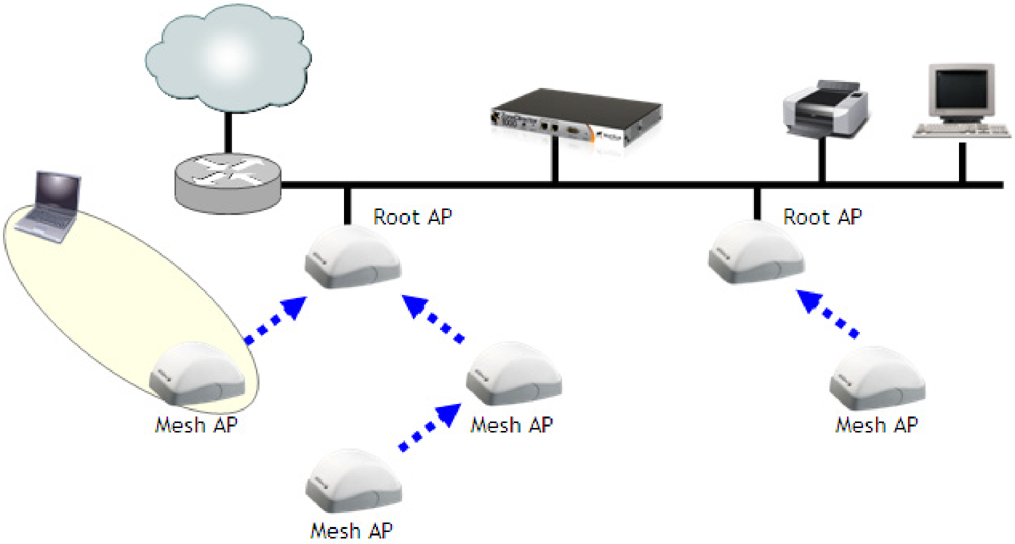
Smart Mesh networks can be deployed in three types of topologies:

- Standard Topology
- 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 142) 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."

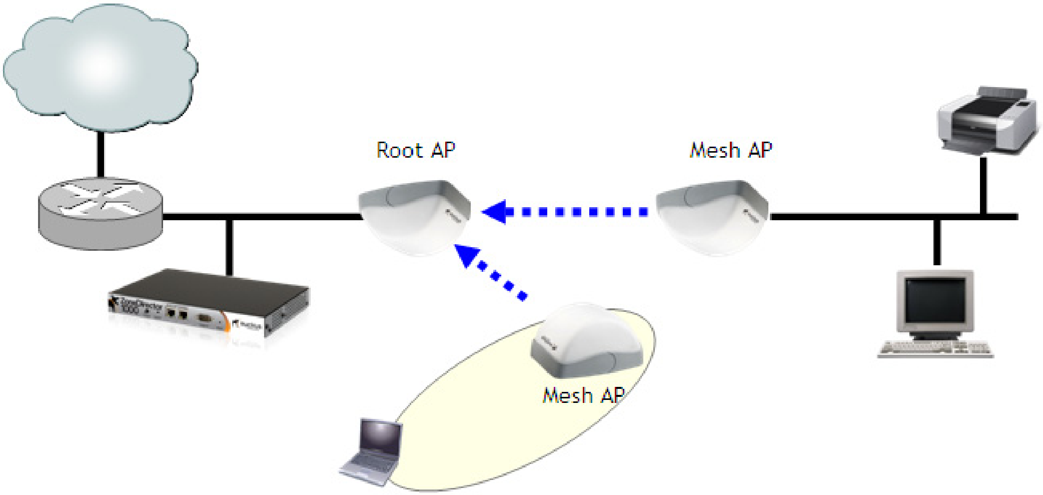
Figure 142. Mesh - standard topology



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 143 below.

Figure 143. Mesh - wireless bridge topology



Hybrid Mesh Topology

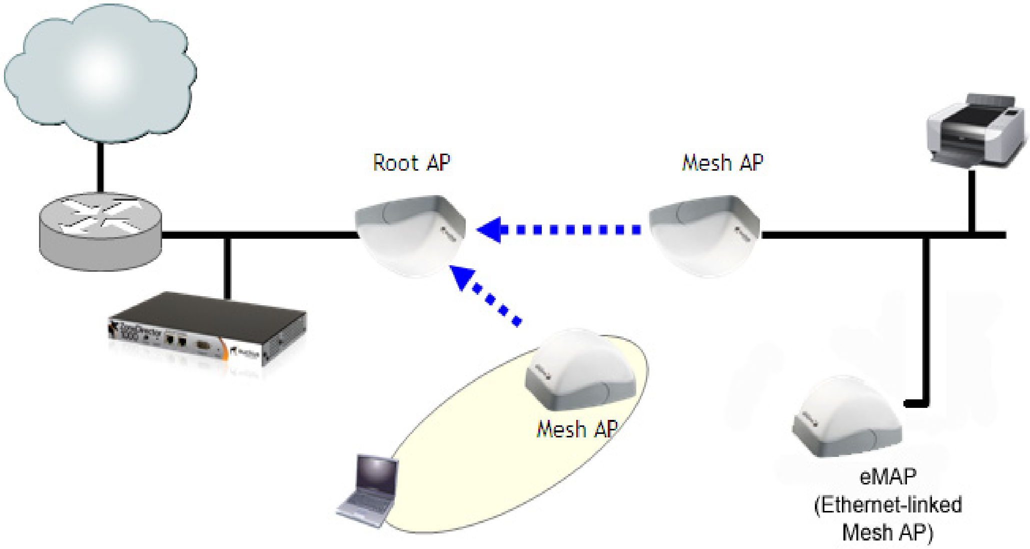
A third type of network topology can be configured using the Hybrid Mesh concept.

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 144. eMAP - Hybrid Mesh topology



Use the **Monitor > Mesh** page to see a tree diagram of your Smart Mesh network.

Table 34. Mesh View icons

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

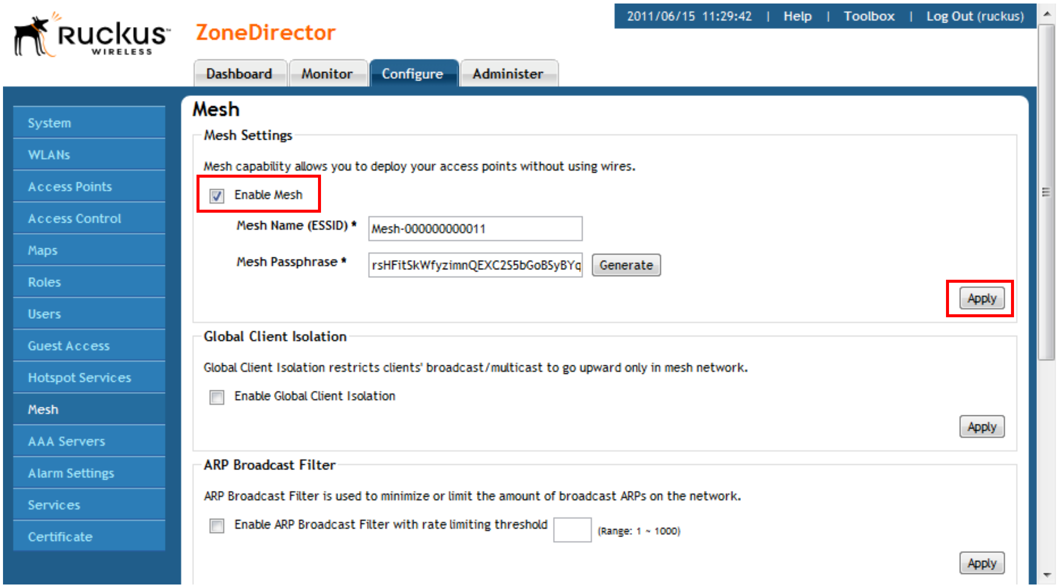
Before starting with your wireless mesh deployment, Ruckus Wireless recommends performing a number of tasks that can help ensure a smooth deployment.

- Ensure that the APs that will form the mesh are of the same radio type.
  - 802.11g APs can only mesh with other 11g APs.
  - Single band 11n APs can only mesh with other single band 11n APs.
  - Dual band 11n APs can only mesh with other dual band 11n 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. Note that only firmware versions 6.0.0.0.* and later (for both ZoneFlex and ZoneDirector) support mesh networking.
- Enable Auto Approval - If you do not want to have to manually approve the join requests from each mesh AP when they start forming the wireless mesh, you can enable Auto Approval. For instructions on how to enable Auto Approval, see "Adding New Access Points to the Network" on page 154.

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 145. Enable Mesh in Configure > Mesh



Mesh

Mesh Settings

Mesh capability allows you to deploy your access points without using wires.

☑ Enable Mesh

Mesh Name (ESSID) * Mesh-000000000011

Mesh Passphrase * rsHFitSkWfyzimnQEXC2S5bGoBSyBYq

Global Client Isolation

Global Client Isolation restricts clients' broadcast/multicast to go upward only in mesh network.

☐ Enable Global Client Isolation

ARP Broadcast Filter

ARP Broadcast Filter is used to minimize or limit the amount of broadcast ARPs on the network.

☐ Enable ARP Broadcast Filter with rate limiting threshold (Range: 1 ~ 1000)

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.

CAUTION: 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" on page 173.

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.

- **Global Client Isolation**: Enable the check box to prevent clients from sending broadcast or multicast frames to ports other than their uplink ports. For example, if a client sends an ARP request, it will be forwarded from the Mesh AP to the Root AP and to the backhaul. It will not be forwarded to other Mesh APs connected to the same Root AP. This feature is disabled by default.
- **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 Packet Forwarding Filter**: When this feature is enabled, packet filtering is applied to the uplink port of an AP. For a Root AP or eMAP, the uplink port is the Ethernet port. For a Mesh AP, the uplink port is the mesh uplink port. Packets received from the uplink port will be dropped if the source MAC address *does not* match one of the MAC addresses specified in the filter. Packets transmitted out via the uplink port will be dropped if the destination MAC address *does* match one of the MAC addresses specified. Enter the colon-separated MAC addresses of the gateway and BRAS servers and click Create New to add them to the list.
- **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" on page 155.
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

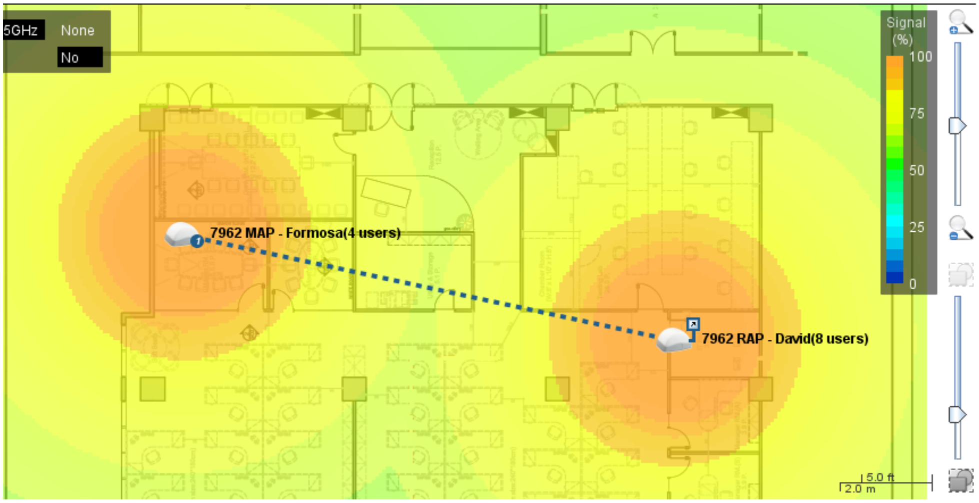
After you complete deploying all mesh nodes to their locations on the network, you can check the Map View on the ZoneDirector Web interface to verify that mesh associations have been established and mesh trees formed.

1. On the Zone Director 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" on page 182 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 146. 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:

Table 35. Map View AP icons

↗	An AP with the upward pointing arrow is a Root AP.
2	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.
↗	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).
X	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.

Figure 147. Mesh-related AP statuses

Status	Description	Recommended Action
Connected	AP is connected to ZoneDirector, but mesh is disabled	If mesh is enabled on the AP, you may need to reboot it to activate the mesh.
Connected (Root AP)	AP is connected to ZoneDirector via its Ethernet port	
Connected (Mesh AP, n hops)	AP is connected to ZoneDirector via its wireless interface and is *n* hops away from the Root AP.	
Connected (eMesh AP, n hops)	AP is connected to ZoneDirector via its Ethernet port, but acts as a Mesh AP using another Mesh AP as its uplink.	
Isolated Mesh AP	AP is disconnected from the ZoneDirector mesh	• The AP may be configured incorrectly. Verify that the mesh SSID and passphrase configured on the AP are correct. • If Uplink Selection is set to Manual, the uplink AP specified for this AP may be off or unavailable.

Using the 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 2741, 2942, 7321, 7341, 7343), 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.

Figure 148. Behavior of the WLAN LED

LED Color/Behavior	Root AP / Mesh AP / eMAP
Solid green	No mesh downlink, and; At least one client is associated with the AP
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

Figure 149. Behavior of the Signal/Air Quality LED

LED Color/Behavior	Root AP / eMAP	Mesh AP
Solid green	N/A	• Connected to a Root AP or another Mesh AP • Signal quality is good
Fast blinking green	N/A	• Connected to a Root AP or another Mesh AP • Signal quality is fair or poor
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.

The following dual-band ZoneFlex AP models currently support mesh networking: ZoneFlex 7363, 7762/S/T, 7761-CM, 7962 and 7982. Refer to the following sections for information on how to check these dual-band APs for their mesh status.

ZoneFlex 7762

On ZoneFlex 7762 APs (including 7762-S and 7762-T), the **STATUS** LED indicates the AP's mesh status. See the table below for more information.

Figure 150. Behavior of the Status LED

LED Color/Behavior	Description
Solid green	• This is a Root AP or eMAP, or; • This is a Mesh AP and is connected to a Root AP with good signal
Fast blinking green	• This is a Mesh AP, and; • The Root AP signal is fair
Slow blinking green	• This is a Mesh AP that is currently searching for a Root AP, or; • This AP is currently searching for ZoneDirector

ZoneFlex 7962, 7982 and 7363 APs

On ZoneFlex 7962, 7982 and 7363 APs, the 5G LED indicates the AP's mesh status. See the table below for more information.

Figure 151. Behavior of the 5G LED

LED Color/Behavior	Root AP / eMAP	Mesh AP
Fast blinking green	No Mesh AP is connected	Disconnected from the Root AP
Solid green	• At least one Mesh AP is connected • Signal quality is good	• Connected to a Root AP • Signal quality is good
Solid amber	• At least one Mesh AP is connected • Signal quality is fair	• Connected to a Root AP • Signal quality is fair

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 36. Action icons

Icon	Icon Name	Action
ℹ	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.

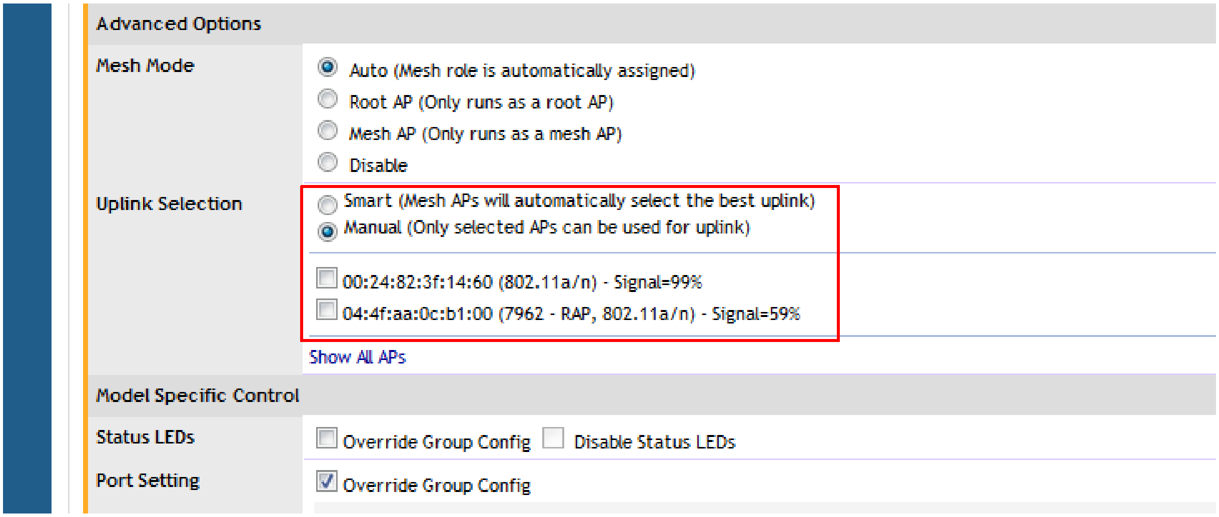
Icon	Icon Name	Action
✓	Allow	Allow this AP to be managed by ZoneDirector. This icon will only appear if you have disabled automatic approval under "Access Point Policies" on the Configure > Access Points page.
◉	RF Info	Generates a log file called *info.txt*, containing radio frequency data that can be used for troubleshooting the RF environment.

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 152. Setting Uplink Selection to Manual



Advanced Options

Mesh Mode
- ● Auto (Mesh role is automatically assigned)
- ○ Root AP (Only runs as a root AP)
- ○ Mesh AP (Only runs as a mesh AP)
- ○ Disable

Uplink Selection
- ○ Smart (Mesh APs will automatically select the best uplink)
- ● Manual (Only selected APs can be used for uplink)
- □ 00:24:82:3f:14:60 (802.11a/n) - Signal=99%
- □ 04:4f:aa:0c:b1:00 (7962 - RAP, 802.11a/n) - Signal=59%

Show All APs

Model Specific Control

Status LEDs □ Override Group Config □ Disable Status LEDs

Port Setting ☑ Override Group Config

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. Misconfiguring 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.

Table 37. Isolated Mesh AP statuses

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.

Table 37. Isolated Mesh AP statuses

Status	**Possible Reason**
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.
Config error	The AP attempted to establish the mesh uplink but was unsuccessful. If you recently updated the mesh SSID and passphrase, it is likely that your changes have not propagated correctly to this AP (for example, the AP was offline when you updated the mesh SSID and passphrase). To resolve this, follow the instructions in "Recovering an Isolated Mesh AP" on page 251.
No APs with matching radio type	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. To resolve this, place additional wired APs or Mesh APs that use the same radio type near this AP.

Recovering an Isolated Mesh AP

When a Mesh AP becomes isolated, it begins broadcasting a recovery SSID (named "*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.

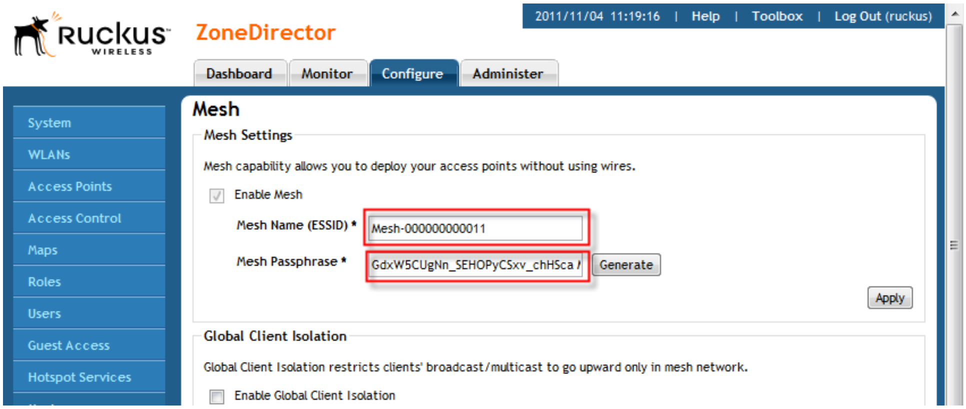
To perform these procedures, you will need:

- A notebook computer with wireless capability. If you are running Windows XP on the computer, make sure that either the WPA2 patch or Service Pack 3 is installed.
- 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 Passhphrase

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 153. The Mesh Name and Mesh Passphrase you will use to configure the AP



Mesh

Mesh Settings

Mesh capability allows you to deploy your access points without using wires.

☑ Enable Mesh

Mesh Name (ESSID) * Mesh-000000000011

Mesh Passphrase * GdxW5CUgNn_SEHOPyCSxv_chHSca /

Global Client Isolation

Global Client Isolation restricts clients' broadcast/multicast to go upward only in mesh network.

□ Enable Global Client Isolation

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-xxxxxx`" (where xxxxxx is the last 6 digits of the AP's MAC address).

2. Connect to this WLAN using WPA and the passphrase `ruckus-<admin password>`. (The admin password is the same as that used to log into ZoneDirector.)
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 can not 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" on page 293.

10

Setting Administrator Preferences

In This Chapter

Changing the ZoneDirector Administrator User Name and Password

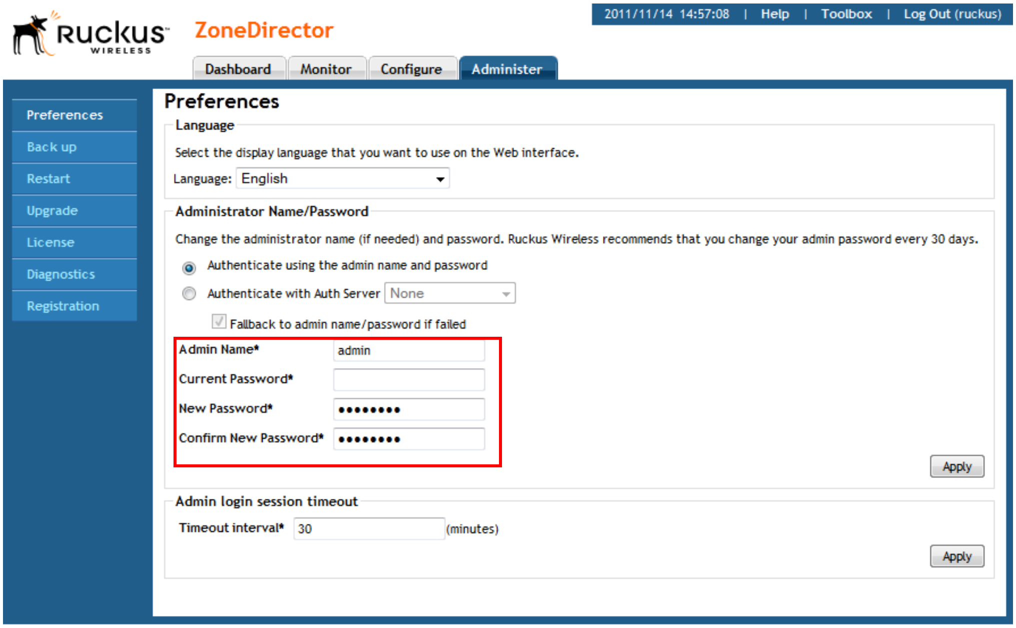
You should change your ZoneDirector administrator login password on a monthly basis, but the administrator user name should be changed only if necessary.

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 154. The Preferences page



Preferences

Language

Select the display language that you want to use on the Web interface.

Language: English

Administrator Name/Password

Change the administrator name (if needed) and password. Ruckus Wireless recommends that you change your admin password every 30 days.

● Authenticate using the admin name and password

○ Authenticate with Auth Server None

☑ Fallback to admin name/password if failed

Admin Name* admin

Current Password*

New Password* ••••••••

Confirm New Password* ••••••••

Admin login session timeout

Timeout interval* 30 (minutes)

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.

CAUTION: If ZoneDirector is running a software version or earlier than version 9.3 and you want to upgrade to version 9.5, you will need to upgrade it to version 9.3 first, and then upgrade it to version 9.5. If you try to upgrade directly to 9.5 from a version earlier than 9.3, the upgrade will fail. (There are some specific exceptions, see 9.5 Release Notes for more information.)

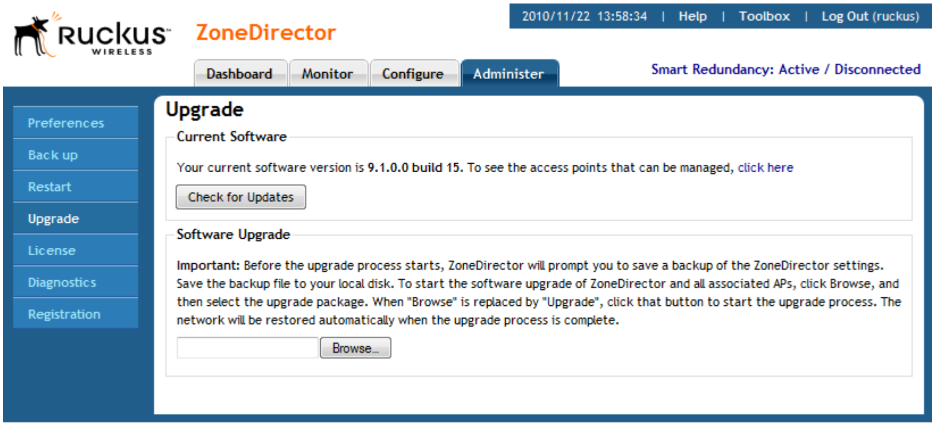
1. Go to **Administer** > **Upgrade**.
2. Under the *Software Upgrade* section, click **Browse**. The Browse dialog box appears.
3. Browse to the location where you saved the upgrade package, and then click **Open**.
4. When the upgrade file name appears in the text field, the **Browse** button becomes 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.

CAUTION: 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 155. The Upgrade page



Upgrade

Current Software

Your current software version is **9.1.0.0 build 15**. To see the access points that can be managed, click here

Software Upgrade

Important: Before the upgrade process starts, ZoneDirector will prompt you to save a backup of the ZoneDirector settings. Save the backup file to your local disk. To start the software upgrade of ZoneDirector and all associated APs, click Browse, and then select the upgrade package. When "Browse" is replaced by "Upgrade", click that button to start the upgrade process. The network will be restored automatically when the upgrade process is complete.

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.

CAUTION: 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.

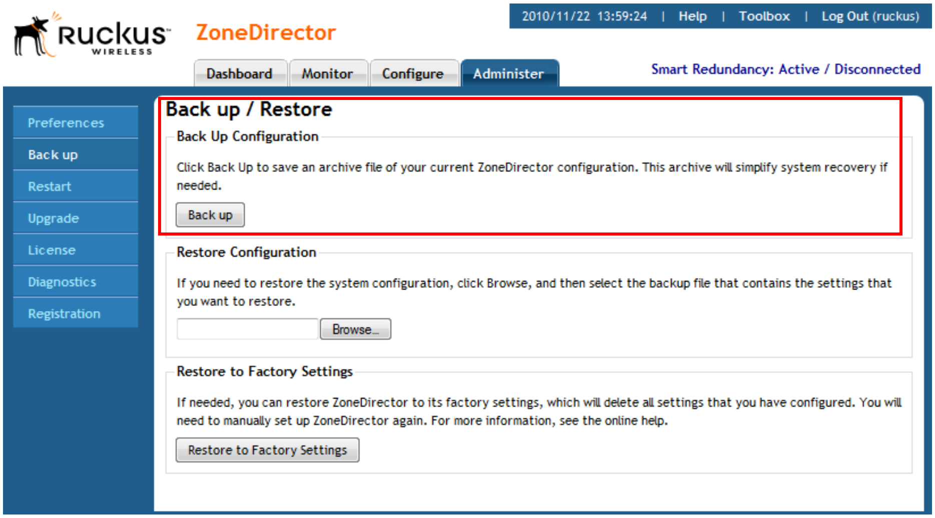
Working with Backup Files

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**.
5. Make sure the filename ends in a ".bak" extension.
6. When the *Download Complete* dialog box appears, click **Close**.

Figure 156. The Back Up Configuration option



Back up / Restore

Back Up Configuration

Click Back Up to save an archive file of your current ZoneDirector configuration. This archive will simplify system recovery if needed.

Restore Configuration

If you need to restore the system configuration, click Browse, and then select the backup file that contains the settings that you want to restore.

Restore to Factory Settings

If needed, you can restore ZoneDirector to its factory settings, which will delete all settings that you have configured. You will need to manually set up ZoneDirector again. For more information, see the online help.

Restoring Archived Settings to ZoneDirector

CAUTION: 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 if you are deploying a second ZoneDirector for failover purposes.
   - *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.

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 1100 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 ZD1100s 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" on page 171.

To restore an AP list from a backup file without altering ZoneDirector settings

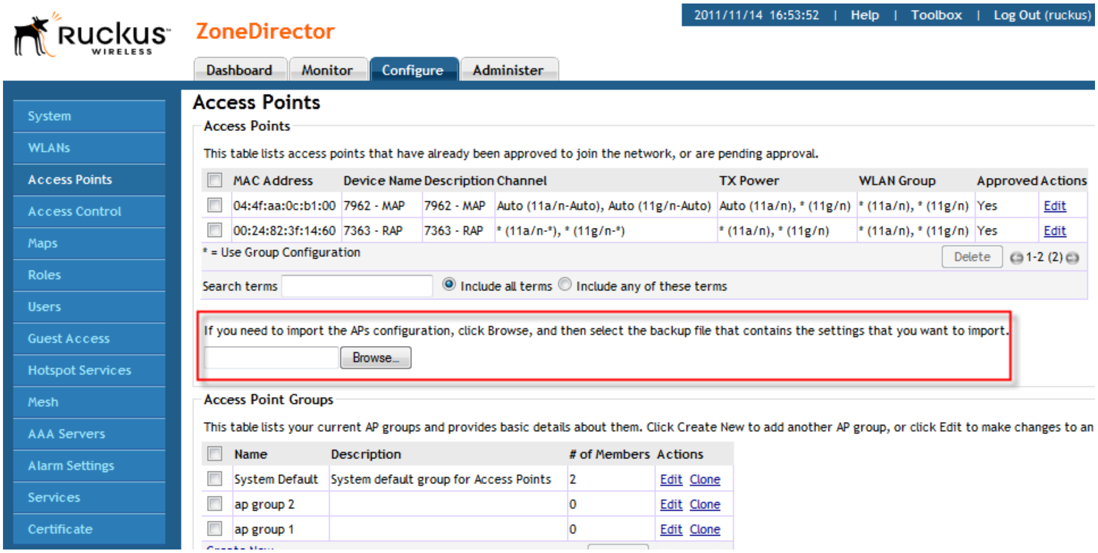
1. Go to **Configure > Access Points**.
2. Under the *Access Points* table, click the **Browse** button near the line that begins "*If you need to import the APs configuration...*".
3. Browse to a previously saved backup file, select the file and click **Open**. The page refreshes and the name of the 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.
   - 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 157. Importing AP lists only from a backup file



Access Points

Access Points

This table lists access points that have already been approved to join the network, or are pending approval.

☐	MAC Address	Device Name	Description	Channel	TX Power	WLAN Group	Approved	Actions
☐	04:4f:aa:0c:b1:00	7962 - MAP	7962 - MAP	Auto (11a/n-Auto), Auto (11g/n-Auto)	Auto (11a/n), * (11g/n)	* (11a/n), * (11g/n)	Yes	Edit
☐	00:24:82:3f:14:60	7363 - RAP	7363 - RAP	* (11a/n-*), * (11g/n-*)	* (11a/n), * (11g/n)	* (11a/n), * (11g/n)	Yes	Edit

* = 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.

Browse...

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

☐	Name	Description	# of Members	Actions
☐	System Default	System default group for Access Points	2	Edit Clone
☐	ap group 2		0	Edit Clone
☐	ap group 1		0	Edit Clone

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.

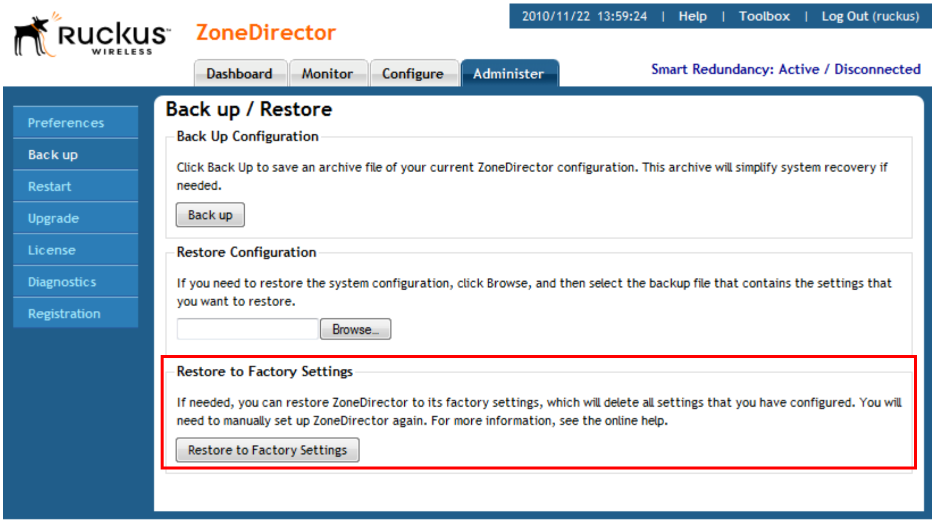
CAUTION: When this procedure is complete, you will need to redo a complete setup. If ZoneDirector is on a live network, a new IP address may be assigned to the system. In this case, the system can be discovered by a UPnP client application, such as Windows "My Network Places." If there is no DHCP server 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 158. The Restore to Factory Settings section



Click Back Up to save an archive file of your current ZoneDirector configuration. This archive will simplify system recovery if needed.

If you need to restore the system configuration, click Browse, and then select the backup file that contains the settings that you want to restore.

If needed, you can restore ZoneDirector to its factory settings, which will delete all settings that you have configured. You will need to manually set up ZoneDirector again. For more information, see the online help.

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

If you use HTTPS to connect to the ZoneDirector Web interface, a security warning appears every time you connect to the Web interface. This is because the default SSL certificate (or security certificate) that ZoneDirector is using for HTTPS communication is signed by Ruckus Wireless and is not recognized by most Web browsers.

If you want to prevent these security warnings from appearing, you will need to import an SSL certificate that was issued by a recognized certificate authority (for example, VeriSign, Thawte, etc). If you do not have an SSL certificate yet, you will need to create a certificate signing request and purchase a certificate from a certificate authority.

Creating 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.

To create a certificate request file

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.
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 in Step 4., 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-----

MIIFVjCCBD6gAwIBAgIQLfaGuqKukMumWhbVf5v4vDANBgkqhkiG9w0BAQUFADCBs
DELMAkGA1UEBhMCVVMxFzAVBgNVBAoTDlZlcmlTaWduLCBJbmMuMR8wHQYDVQQLBg
EFBQcBAQRtMGswJAYIKwYBBQUHMAGGGGh0dHA6Ly9vY3NwLnZlcmlzaWduLmNvbTB
DBggrBgEFBQcwAoY3aHR0cDovL1NWUlNlY3VyZS1haWEudmVyaXNpZ24uY29tL1NW
UlNlY3VyZTIwMDUtYWlhLmNlcjBuBggrBgEFBQcBDARiMGChXqBcMFowWDBWFglpb
WFnZS9naWYwITAfMAcGBSsOAwIaBBRLa7kolgYMu9BSOJsprEsHiyEFGDAmFiRodH
RwOi8vbG9nby52ZXJpc2lnbi5jb20vdnNsb2dvMS5naWYwDQYJKoZIhvcNAQEFBQA
DggEBAI/S2dmm/kgPeVAlsIHmx-
751o4oq8+fwehRDBmQDaKiBvVXGZ5ZMnoc3DMyDjx0SrI9lkPsn223CV3UVBZo385
g1T4iKwXgcQ7WF6QcUYOE6HK+4ZGcHermFf3fv3C1FoCjq+zEu8ZboUf3fWbG-
prGRA+MR/dDI1dTPtSUG7/zWjXO5jC//0pykSldW/q8hgO8kq30S8JzCwkqrX-
JfQ050N4TJtgb/
YC4gwH3BuB9wqpRjUahTiK1V1-
ju9bHB+bFkMWIIMIXc1Js62JClWzwFgaGUS2DLE8xICQ3wU1ez8RUPGnwSxAYtZ2N
7zDxYDP2tEiO5j2cXY7O8mR3ni0C30=
-----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.

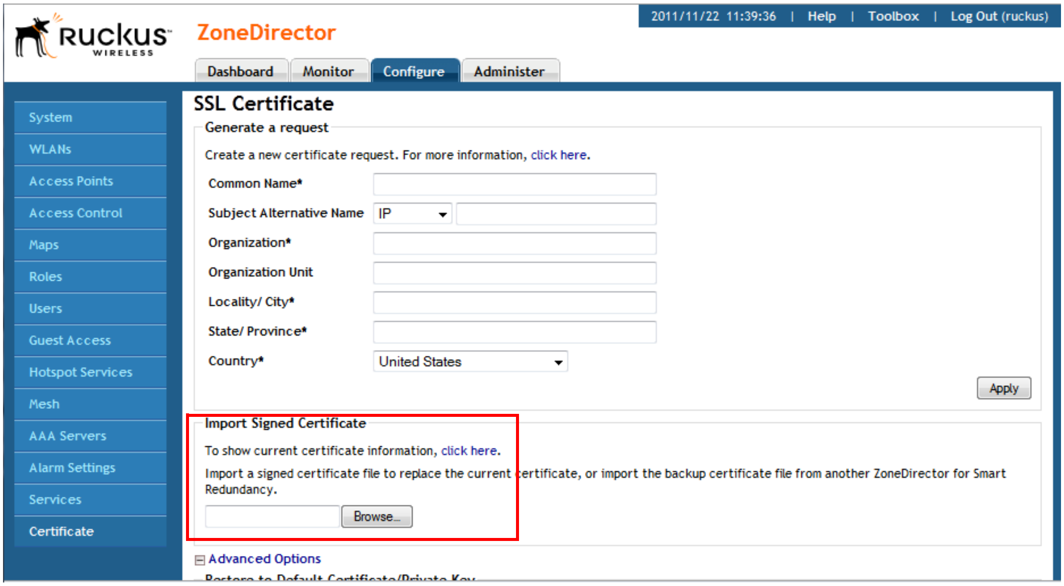
Importing an SSL Certificate

If you already have an SSL certificate, you can import it into ZoneDirector and use it for HTTPS communication. To complete this procedure, you will need the SSL certificate file and the key pair password that you set when you created the certificate signing request (CSR) file.

To import an SSL certificate

1. Copy the certificate file to a location (either on the local drive or a network share) that you can access from the ZoneDirector Web interface.
2. Log in to the ZoneDirector Web interface and go to **Configure** > **Certificate**.
3. Under *Import Certificate*, click **Browse**, and then go to the location where you saved the certificate file.
4. Click **Open**. If the certificate file that you selected is valid, an Import button appears.
5. Click **Import** to import the certificate file to ZoneDirector.

Figure 159. The Import Signed Certificate section



SSL Certificate

Generate a request

Create a new certificate request. For more information, click here.

Common Name*	
Subject Alternative Name	IP
Organization*	
Organization Unit	
Locality/ City*	
State/ Province*	
Country*	United States

Apply

Import Signed Certificate

To show current certificate information, click here.

Import a signed certificate file to replace the current certificate, or import the backup certificate file from another ZoneDirector for Smart Redundancy.

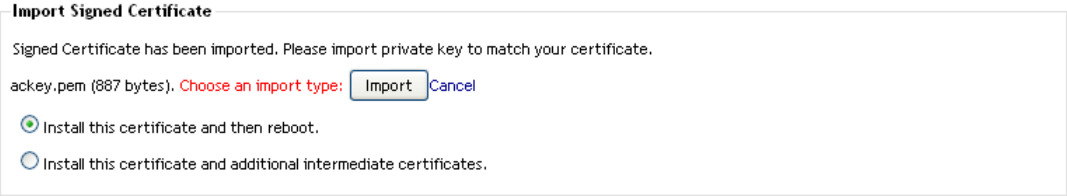
Browse...

⊟ Advanced Options

Restore to Default Certificate/Private Key

6. After importing the certificate, ZoneDirector will check if the imported certificate matches ZoneDirector’s private key. If the certificate matches the private key, ZoneDirector asks whether you want to install the certificate and reboot, or install additional intermediate certificates.

Figure 160. Install certificate and reboot, or install intermediate certificates



Import Signed Certificate

Signed Certificate has been imported. Please import private key to match your certificate.

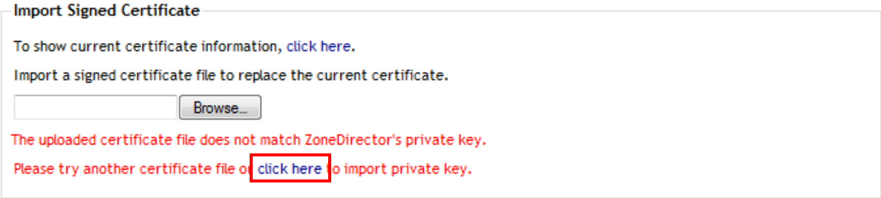
ackey.pem (887 bytes). Choose an import type: Import Cancel

● Install this certificate and then reboot.

○ Install this certificate and additional intermediate certificates.

7. If the SSL certificate you imported does *not* match ZoneDirector's private key, you can try another certificate, or click the **click here** link to import a private key.

Figure 161. Uploaded certificate does not match private key; try another certificate or import private key



Import Signed Certificate

To show current certificate information, click here.

Import a signed certificate file to replace the current certificate.

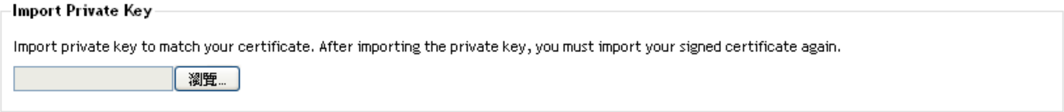
Browse...

The uploaded certificate file does not match ZoneDirector's private key.

Please try another certificate file or click here to import private key.

8. If you click the click here link to import a private key, the following dialog is displayed:

Figure 162. Importing a private key to match your signed certificate



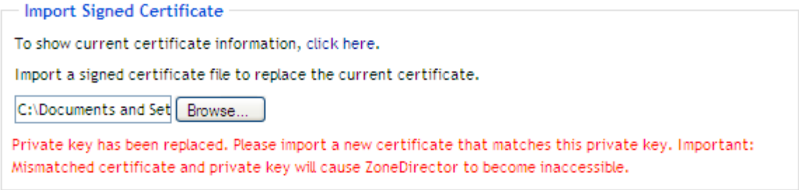
Import Private Key

Import private key to match your certificate. After importing the private key, you must import your signed certificate again.

瀏覽...

9. After you import a private key, you must import the signed certificate again (see Step 3.).

Figure 163. You must import the certificate again after changing ZoneDirector's private key



Import Signed Certificate

To show current certificate information, click here.

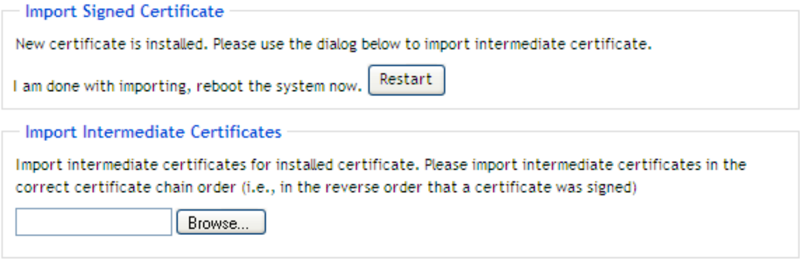
Import a signed certificate file to replace the current certificate.

C:\Documents and Set Browse...

Private key has been replaced. Please import a new certificate that matches this private key. Important: Mismatched certificate and private key will cause ZoneDirector to become inaccessible.

10. If you choose to import additional intermediate certificates, ZoneDirector first installs the new signed certificate, then prompts you to import intermediate certificates.

Figure 164. Importing intermediate certificates



Import Signed Certificate

New certificate is installed. Please use the dialog below to import intermediate certificate.

I am done with importing, reboot the system now. Restart

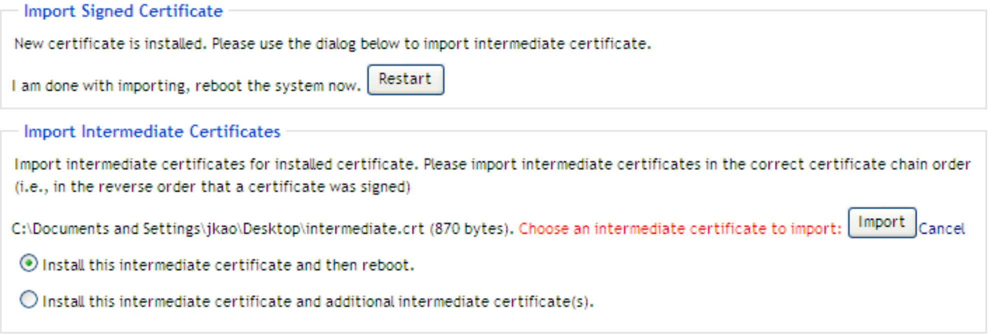
Import Intermediate Certificates

Import intermediate certificates for installed certificate. Please import intermediate certificates in the correct certificate chain order (i.e., in the reverse order that a certificate was signed)

Browse...

11. Once you have finished importing the new signed certificate and any intermediate certificates, click **Import** to complete the installation and reboot ZoneDirector.

Figure 165. Click Import to install all intermediate certificates and reboot



Import Signed Certificate

New certificate is installed. Please use the dialog below to import intermediate certificate.

I am done with importing, reboot the system now. Restart

Import Intermediate Certificates

Import intermediate certificates for installed certificate. Please import intermediate certificates in the correct certificate chain order (i.e., in the reverse order that a certificate was signed)

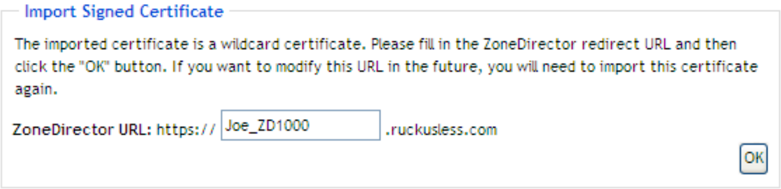
C:\Documents and Settings\jkao\Desktop\intermediate.crt (870 bytes). Choose an intermediate certificate to import: Import Cancel

● Install this intermediate certificate and then reboot.

○ Install this intermediate certificate and additional intermediate certificate(s).

12. Finally, you can also import a wildcard certificate. If you do this, ZoneDirector will prompt you to fill in ZoneDirector's redirect URL before proceeding.

Figure 166. You must enter ZoneDirector's redirect URL if using a wildcard certificate



Import Signed Certificate

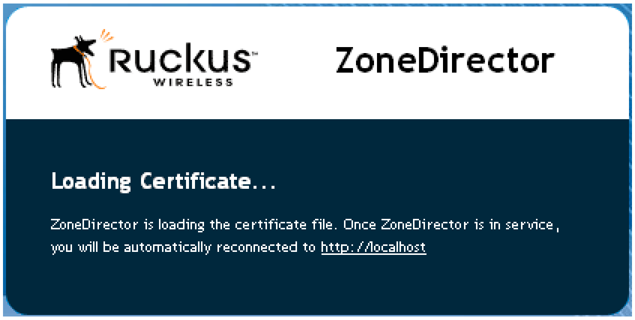
The imported certificate is a wildcard certificate. Please fill in the ZoneDirector redirect URL and then click the "OK" button. If you want to modify this URL in the future, you will need to import this certificate again.

ZoneDirector URL: https:// Joe_ZD1000 .ruckusless.com

OK

13. Once the private key matches and intermediate certificates are imported, clicking the **Import** button will start the *Loading Certificate* process. The following screen is displayed during the install and reboot process:

Figure 167. Loading certificate screen



Loading Certificate...

ZoneDirector is loading the certificate file. Once ZoneDirector is in service, you will be automatically reconnected to http://localhost

You have completed installing a new signed SSL certificate to ZoneDirector. This allows you to connect to ZoneDirector securely using HTTPS without encountering browser security warnings.

SSL Certificate Advanced Options

ZoneDirector also provides four features for managing SSL certificates/private keys easily through the Web interface:

- *Restore to Default Certificate/Private Key*: Allows you to easily restore the factory default certificate/key at any time -- in case you have imported an SSL certificate that causes problems, you can always revert to the factory default and start over.
- *Back Up Private Key*: Allows you to save the key for use in another ZoneDirector or keep a copy in case ZoneDirector needs to be factory reset and loses its current key.
- *Back Up Certificates for Smart Redundancy*: Use this option to apply the same certificate and private key to the Smart Redundancy peer.
- *Re-Generate Private Key*: Only used to generate a new private key of a different length (when required by the Certificate Authority).

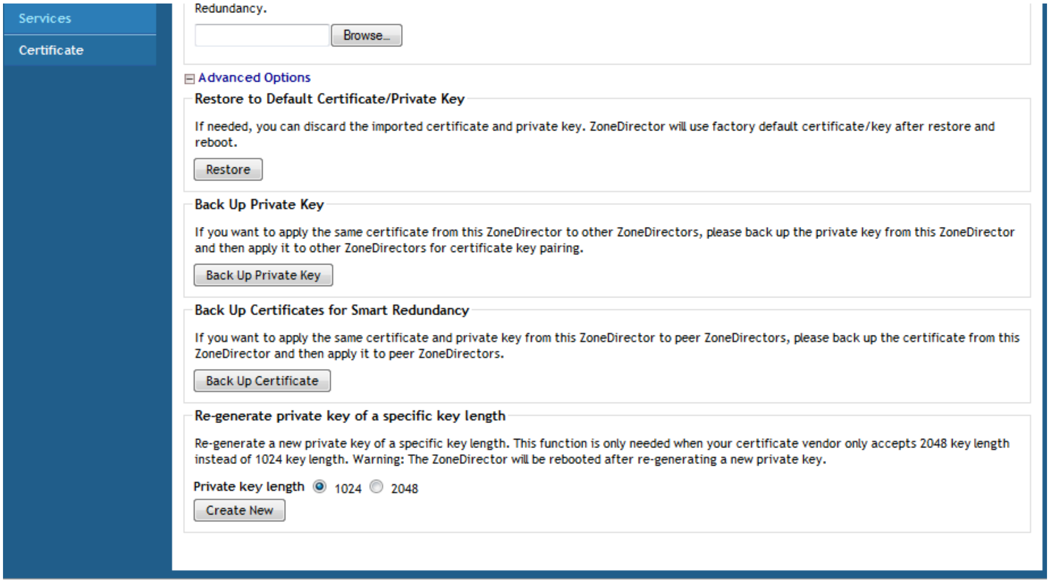
Saving an SSL Certificate or Private Key

Saving an SSL certificate to a local computer can be useful when deploying two ZoneDirectors in a Smart Redundancy configuration. Using the advanced options, you can export an SSL certificate from one device to the other.

To share an SSL certificate and private key between two Zonedirectors

1. On the **Configure > Certificates** page, click **Advanced Options** to expand the options.
2. Click **Back Up Private Key**, and save the file to your local computer.
3. Click **Back Up Certificate**, and save the file to your local computer.

Figure 168. SSL Certificate advanced options



Redundancy.

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.

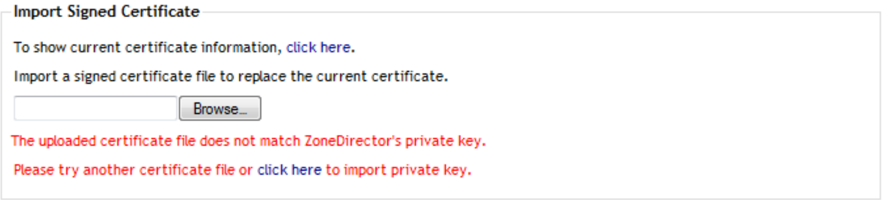
Re-generate private key of a specific key length

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

4. Log in to the peer ZoneDirector, and import the certificate as described in "Importing an SSL Certificate" on page 264.
5. After the certificate has been imported, ZoneDirector checks for private key match.
6. If the imported certificate does not match ZoneDirector's private key, a warning message appears.

Figure 169. The imported certificate does not match ZoneDirector's private key



Import Signed Certificate

To show current certificate information, click here.

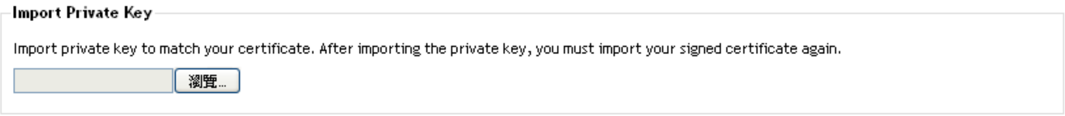
Import a signed certificate file to replace the current certificate.

The uploaded certificate file does not match ZoneDirector's private key.

Please try another certificate file or click here to import private key.

7. Click the **click here** link, and an *Import Private Key* dialog appears.

Figure 170. Importing a private key



Import Private Key

Import private key to match your certificate. After importing the private key, you must import your signed certificate again.

8. Click **Browse** and locate the private key file you saved in step 2.
9. Click **Import** to finish importing the private key to ZoneDirector.

Using an External Server for Administrator Authentication

ZoneDirector supports additional administrator accounts that can be authenticated using an external authentication server such as RADIUS, LDAP, Active Directory or TACACS+. Three types of administrative privileges can be assigned to these administrator accounts:

- Super Admin - Allows all types of configuration and management tasks
- Operator Admin - Allows AP configuration only
- Monitoring Admin – Allows monitoring operations only

This section provides basic instructions for setting up ZoneDirector to authenticate additional administrator accounts with an external authentication server. For more information on AAA server configuration, see "Using an External AAA Server" on page 89.

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+" on page 107 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.

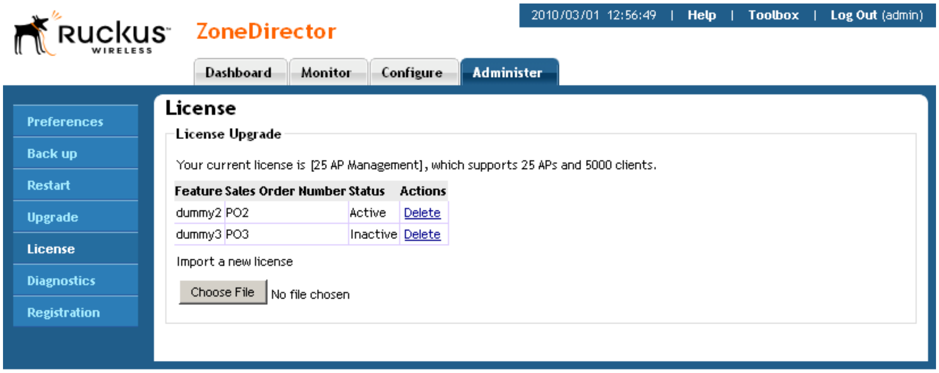
Current license information (description, PO number, status, etc.) is displayed on the Web interface.

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 171. The License page



License Upgrade

Your current license is [25 AP Management], which supports 25 APs and 5000 clients.

Feature	Sales Order Number	Status	Actions
dummy2	PO2	Active	Delete
dummy3	PO3	Inactive	Delete

Import a new license

Choose File No file chosen

Upgrading the License with Smart Redundancy

When two ZoneDirectors are deployed in a Smart Redundancy configuration, upgrading the license on one will cause the Smart Redundancy indicator to display “disconnected” as both devices need to have the same license number.

To upgrade the licenses on two Smart Redundancy ZoneDirectors

1. On the *active* ZoneDirector, go to **Administer > License** and upgrade your license.
2. Repeat for the *standby* ZoneDirector.

3. After both have been upgraded and the license levels match, the Smart Redundancy indicator displays "*Active - Connected*" or "*Standby - Connected*".

11

Troubleshooting

In This Chapter

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 the client be running Windows XP (SP2 or later), Vista (SP1 or later), Windows 7, Mac OS X, iPhone or iTouch and using a wireless network adapter that implements WPA.

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, or running a version of Windows pre-XP/SP2. (This includes XP/SP1.)
- 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 Windows XP SP2/Vista/7 is on the client machine, check the wireless network adapter to verify the implementation of WPA.
- Option 2: Upgrade to Windows XP SP2/Vista/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 Ruckus WPA passphrase in their network configuration (see “Provisioning Clients that Do Not Support Zero-IT” on page 207).
- 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

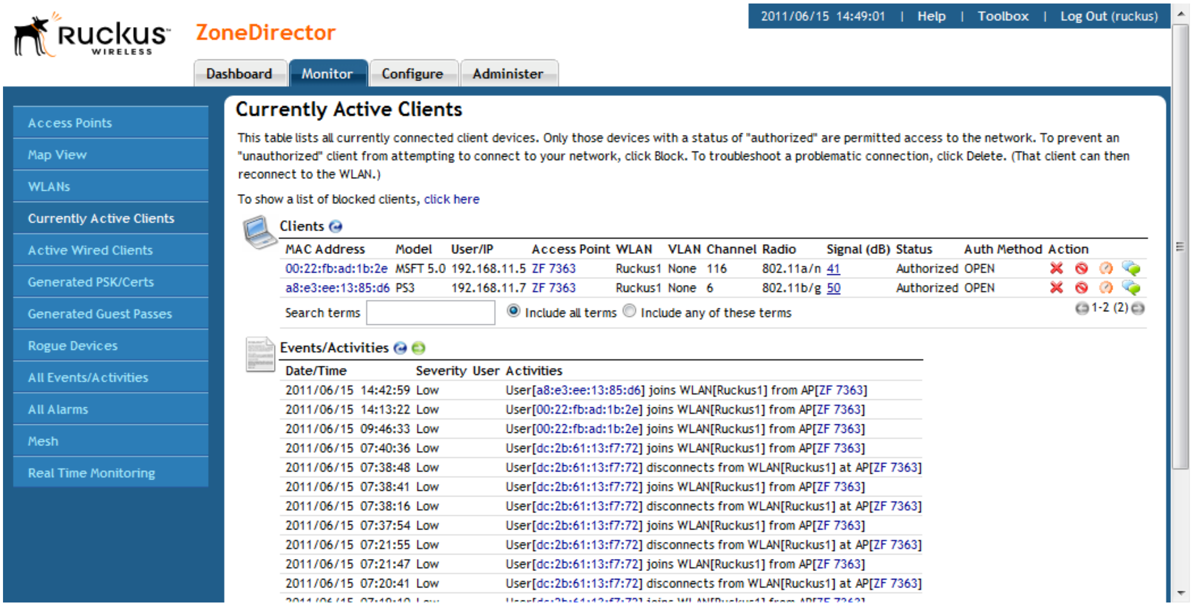
If any of your users report problematic connections to the WLAN, the following debugging technique may prove helpful. Basically, you will be deleting that user's client from the Active Clients table in the Ruckus ZoneDirector, and when their client connection automatically renews itself, any previous problems will hopefully be resolved.

To fix the connection of an active client

1. Go to **Monitor** > **Currently Active 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 172. The Currently Active Clients page



Currently Active Clients

This table lists all currently connected client devices. Only those devices with a status of "authorized" are permitted access to the network. To prevent an "unauthorized" client from 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

Clients

MAC Address	Model	User/IP	Access Point	WLAN	VLAN	Channel	Radio	Signal (dB)	Status	Auth Method	Action
00:22:fb:ad:1b:2e	MSFT 5.0	192.168.11.5	ZF 7363	Ruckus1	None	116	802.11a/n	41	Authorized	OPEN	
a8:e3:ee:13:85:d6	PS3	192.168.11.7	ZF 7363	Ruckus1	None	6	802.11b/g	50	Authorized	OPEN	

Search terms ● Include all terms ○ Include any of these terms 1-2 (2)

Events/Activities

Date/Time	Severity	User	Activities
2011/06/15 14:42:59	Low		User[a8:e3:ee:13:85:d6] joins WLAN[Ruckus1] from AP[ZF 7363]
2011/06/15 14:13:22	Low		User[00:22:fb:ad:1b:2e] joins WLAN[Ruckus1] from AP[ZF 7363]
2011/06/15 09:46:33	Low		User[00:22:fb:ad:1b:2e] joins WLAN[Ruckus1] from AP[ZF 7363]
2011/06/15 07:40:36	Low		User[dc:2b:61:13:f7:72] joins WLAN[Ruckus1] from AP[ZF 7363]
2011/06/15 07:38:48	Low		User[dc:2b:61:13:f7:72] disconnects from WLAN[Ruckus1] at AP[ZF 7363]
2011/06/15 07:38:41	Low		User[dc:2b:61:13:f7:72] joins WLAN[Ruckus1] from AP[ZF 7363]
2011/06/15 07:38:16	Low		User[dc:2b:61:13:f7:72] disconnects from WLAN[Ruckus1] at AP[ZF 7363]
2011/06/15 07:37:54	Low		User[dc:2b:61:13:f7:72] joins WLAN[Ruckus1] from AP[ZF 7363]
2011/06/15 07:21:55	Low		User[dc:2b:61:13:f7:72] disconnects from WLAN[Ruckus1] at AP[ZF 7363]
2011/06/15 07:21:47	Low		User[dc:2b:61:13:f7:72] joins WLAN[Ruckus1] from AP[ZF 7363]
2011/06/15 07:20:41	Low		User[dc:2b:61:13:f7:72] disconnects from WLAN[Ruckus1] at AP[ZF 7363]

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.

CAUTION: 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" on page 280.

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** > **Currently Active 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.

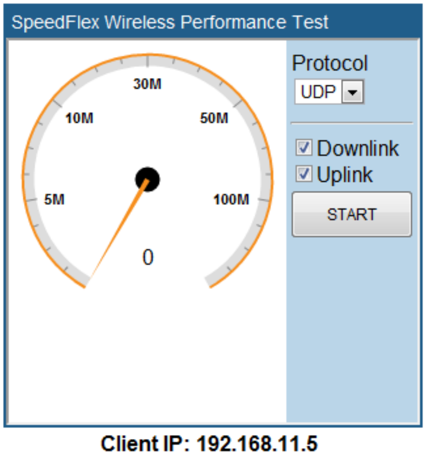
NOTE: If ZoneDirector is unable to determine the IP address of the wireless client that you want to test (for example, if the wireless client is using a static IP address), the SpeedFlex link for that client does not appear on the Currently Active Clients page.

6. Choose **UDP** or **TCP** from the *Protocol* drop-down list. Only one type of traffic can be tested at a time.
7. If you are testing AP throughput, you have the option to test both Downlink and Uplink throughput. Both options are selected by default. If you only want to test one of them, clear the check box for the option that you do not want to test.
8. Click the **Start** button.
   - If the target client does not have SpeedFlex installed, a message appears in the ZoneDirector administrator's browser, informing you that the SpeedFlex tool has to be installed and running on the client before the wireless performance test can continue. Click the OK button on the message, download the appropriate SpeedFlex version (Windows, Mac or Android) from `http://<ZoneDirector-IP-Address>/perf`, and email it to the user, or instruct the user to go to `http://<ZoneDirector-IP-Address>/perf` to download and install it. (See "Allowing Users to Measure Their Own Wireless Throughput" on page 280.) 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 173. The SpeedFlex interface



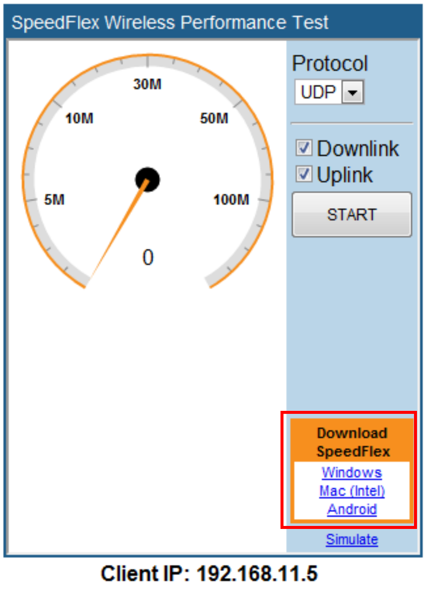
SpeedFlex Wireless Performance Test

Protocol: UDP

☑ Downlink
☑ Uplink

Client IP: 192.168.11.5

Figure 174. Click the download link for the target client’s operating system

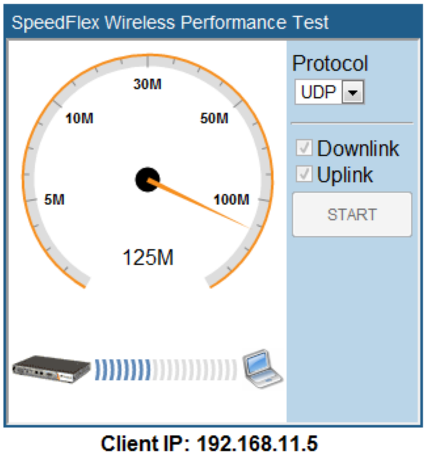

SpeedFlex Wireless Performance Test

Protocol: UDP

☑ Downlink
☑ Uplink

Client IP: 192.168.11.5

Figure 175. A progress bar appears as SpeedFlex measures the wireless throughput

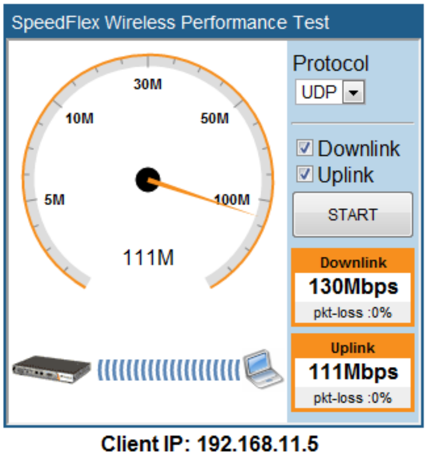

SpeedFlex Wireless Performance Test

Protocol: UDP

☑ Downlink
☑ Uplink

Client IP: 192.168.11.5

Figure 176. When the test is complete, the tool shows the uplink and downlink throughput and packet loss percentage



SpeedFlex Wireless Performance Test

Protocol
UDP ▾

☑ Downlink
☑ Uplink

START

Downlink
130Mbps
pkt-loss :0%

Uplink
111Mbps
pkt-loss :0%

Client IP: 192.168.11.5

Using SpeedFlex in a Multi-Hop Smart Mesh Network

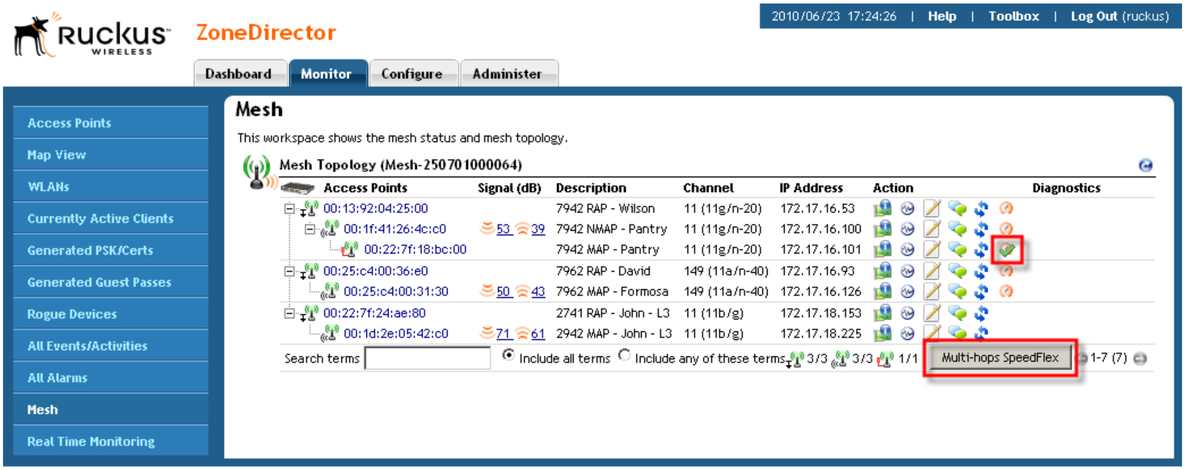
SpeedFlex can also be used to measure multi-hop throughput between APs and ZoneDirector in a mesh tree. For example, if you have a mesh tree that is three hops deep (i.e., ZoneDirector... Root AP... Mesh AP 1... Mesh AP 2), SpeedFlex can measure the total throughput between ZoneDirector and Mesh AP 2. 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

NOTE: Note that SpeedFlex for mesh links is unsupported for 802.11g APs (this feature is available for 11n APs only). SpeedFlex to clients is supported for all ZoneFlex APs.

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 177. Running Multi-Hop SpeedFlex in a mesh tree



Mesh

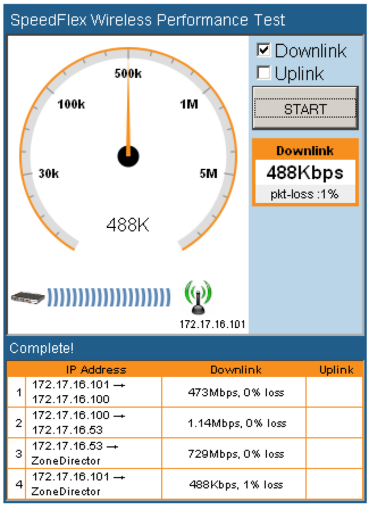
This workspace shows the mesh status and mesh topology.

Mesh Topology (Mesh-250701000064)

Access Points	Signal (dB)	Description	Channel	IP Address	Action	Diagnostics
00:13:92:04:25:00		7942 RAP - Wilson	11 (11g/n-20)	172.17.16.53		
00:1f:41:26:4c:c0	53 39	7942 NMAP - Pantry	11 (11g/n-20)	172.17.16.100		
00:22:7f:18:bc:00		7942 MAP - Pantry	11 (11g/n-20)	172.17.16.101		✓
00:25:c4:00:36:e0		7962 RAP - David	149 (11a/n-40)	172.17.16.93		
00:25:c4:00:31:30	50 43	7962 MAP - Formosa	149 (11a/n-40)	172.17.16.126		
00:22:7f:24:ae:80		2741 RAP - John - L3	11 (11b/g)	172.17.18.153		
00:1d:2e:05:42:c0	71 61	2942 MAP - John - L3	11 (11b/g)	172.17.18.225		

Search terms ● Include all terms ○ Include any of these terms 3/3 3/3 1/1 Multi-hops SpeedFlex 1-7 (7)

Figure 178. Multi-Hop SpeedFlex test results



Complete!

	IP Address	Downlink	Uplink
1	172.17.16.101 → 172.17.16.100	473Mbps, 0% loss	
2	172.17.16.100 → 172.17.16.53	1.14Mbps, 0% loss	
3	172.17.16.53 → ZoneDirector	729Mbps, 0% loss	
4	172.17.16.101 → ZoneDirector	488Kbps, 1% loss	

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

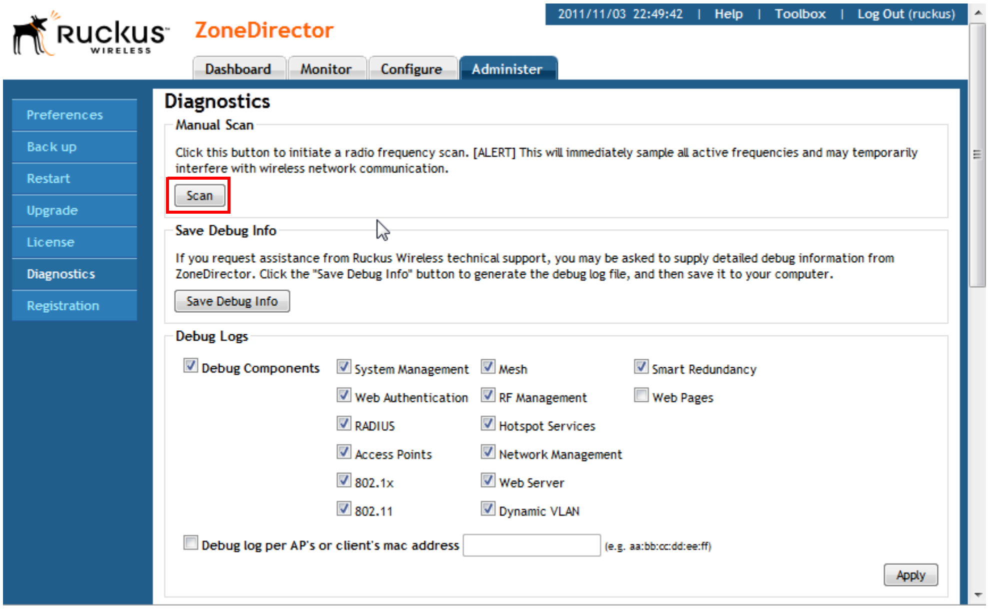
This task complements the automatic RF scanning feature that is built into the Ruckus ZoneDirector. That automatic scan assesses one radio frequency at a time, every 20 seconds or so. To manually start a complete radio frequency scan that assesses all possible frequencies in all devices at one time, 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 179. The Diagnostics page



Diagnostics

Manual Scan

Click this button to initiate a radio frequency scan. [ALERT] This will immediately sample all active frequencies and may temporarily interfere with wireless network communication.

Scan

Save Debug Info

If you request assistance from Ruckus Wireless technical support, you may be asked to supply detailed debug information from ZoneDirector. Click the "Save Debug Info" button to generate the debug log file, and then save it to your computer.

Save Debug Info

Debug Logs

☑ Debug Components

☑ System Management ☑ Mesh ☑ Smart Redundancy
☑ Web Authentication ☑ RF Management □ Web Pages
☑ RADIUS ☑ Hotspot Services
☑ Access Points ☑ Network Management
☑ 802.1x ☑ Web Server
☑ 802.11 ☑ Dynamic VLAN

□ Debug log per AP's or client's mac address (e.g. aa:bb:cc:dd:ee:ff)

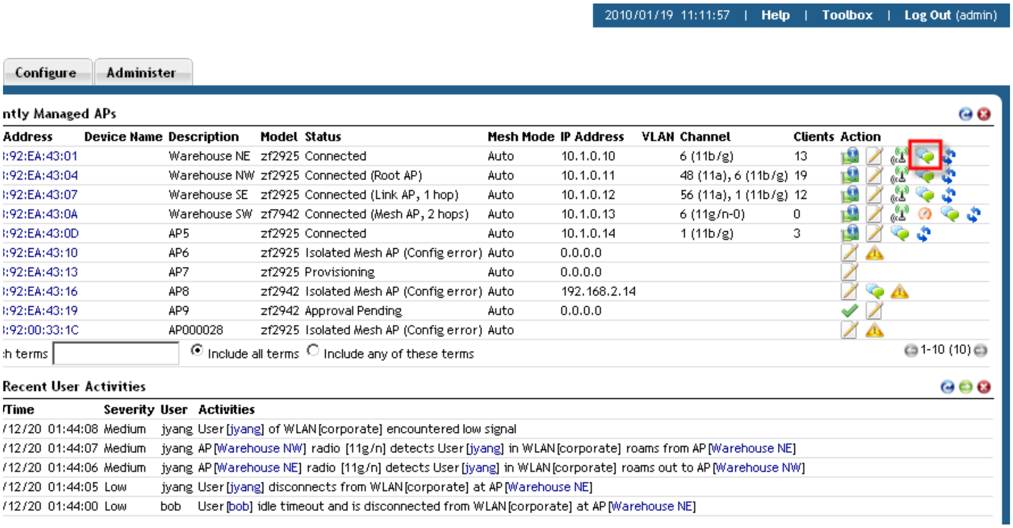
Apply

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 180. Launching the Ping/Traceroute Troubleshooting window from the Dashboard



2010/01/19 11:11:57 | **Help** | **Toolbox** | **Log Out** (admin)

Configure | Administer

ntly Managed APs

Address	Device Name	Description	Model	Status	Mesh Mode	IP Address	VLAN	Channel	Clients	Action
:92:EA:43:01		Warehouse NE	zf2925	Connected	Auto	10.1.0.10		6 (11b/g)	13	
:92:EA:43:04		Warehouse NW	zf2925	Connected (Root AP)	Auto	10.1.0.11		48 (11a), 6 (11b/g)	19	
:92:EA:43:07		Warehouse SE	zf2925	Connected (Link AP, 1 hop)	Auto	10.1.0.12		56 (11a), 1 (11b/g)	12	
:92:EA:43:0A		Warehouse SW	zf7942	Connected (Mesh AP, 2 hops)	Auto	10.1.0.13		6 (11g/n-0)	0	
:92:EA:43:0D		AP5	zf2925	Connected	Auto	10.1.0.14		1 (11b/g)	3	
:92:EA:43:10		AP6	zf2925	Isolated Mesh AP (Config error)	Auto	0.0.0.0				
:92:EA:43:13		AP7	zf2925	Provisioning	Auto	0.0.0.0				
:92:EA:43:16		AP8	zf2942	Isolated Mesh AP (Config error)	Auto	192.168.2.14				
:92:EA:43:19		AP9	zf2942	Approval Pending	Auto	0.0.0.0				
:92:00:33:1C		AP000028	zf2925	Isolated Mesh AP (Config error)	Auto					

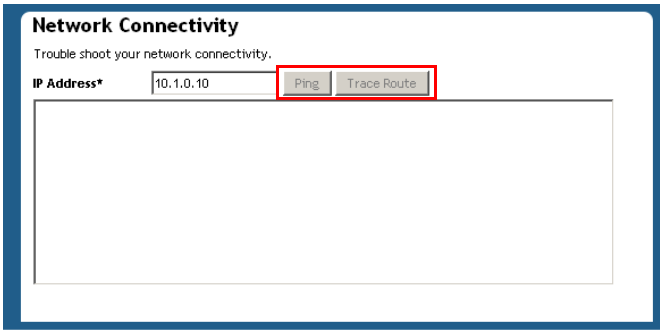
h terms ● Include all terms ○ Include any of these terms 1-10 (10)

Recent User Activities

Time	Severity	User	Activities
/12/20 01:44:08	Medium	jyang	User [jyang] of WLAN [corporate] encountered low signal
/12/20 01:44:07	Medium	jyang	AP [Warehouse NW] radio [11g/n] detects User [jyang] in WLAN [corporate] roams from AP [Warehouse NE]
/12/20 01:44:06	Medium	jyang	AP [Warehouse NE] radio [11g/n] detects User [jyang] in WLAN [corporate] roams out to AP [Warehouse NW]
/12/20 01:44:05	Low	jyang	User [jyang] disconnects from WLAN [corporate] at AP [Warehouse NE]
/12/20 01:44:00	Low	bob	User [bob] idle timeout and is disconnected from WLAN [corporate] at AP [Warehouse NE]

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 181. Network Connectivity dialog



Network Connectivity

Trouble shoot your network connectivity.

IP Address* 10.1.0.10 Ping Trace Route

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 > Currently Active 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.

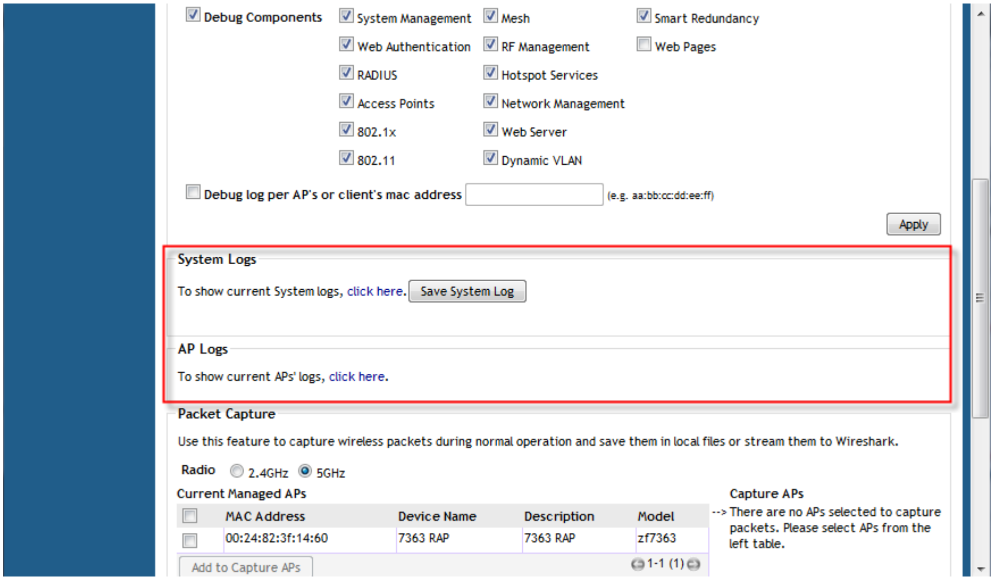
To view ZoneDirector system logs

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 182. Viewing System and AP logs



☑ Debug Components ☑ System Management ☑ Mesh ☑ Smart Redundancy
☑ Web Authentication ☑ RF Management ☐ Web Pages
☑ RADIUS ☑ Hotspot Services
☑ Access Points ☑ Network Management
☑ 802.1x ☑ Web Server
☑ 802.11 ☑ Dynamic VLAN

☐ Debug log per AP's or client's mac address (e.g. aa:bb:cc:dd:ee:ff)

Apply

System Logs

To show current System logs, click here. Save System Log

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

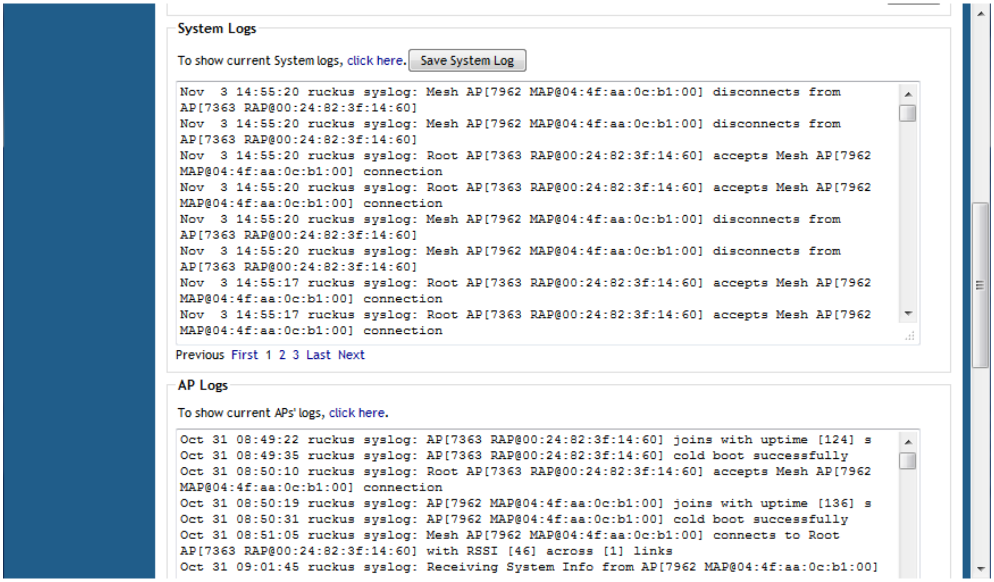
☐	MAC Address	Device Name	Description	Model
☐	00:24:82:3f:14:60	7363 RAP	7363 RAP	zf7363

Add to Capture APs 1-1 (1)

Capture APs

--> There are no APs selected to capture packets. Please select APs from the left table.

Figure 183. UI display of current system and AP logs



System Logs

To show current System logs, click here. Save System Log

```
Nov  3 14:55:20 ruckus syslog: Mesh AP[7962 MAP@04:4f:aa:0c:b1:00] disconnects from
AP[7363 RAP@00:24:82:3f:14:60]
Nov  3 14:55:20 ruckus syslog: Mesh AP[7962 MAP@04:4f:aa:0c:b1:00] disconnects from
AP[7363 RAP@00:24:82:3f:14:60]
Nov  3 14:55:20 ruckus syslog: Root AP[7363 RAP@00:24:82:3f:14:60] accepts Mesh AP[7962
MAP@04:4f:aa:0c:b1:00] connection
Nov  3 14:55:20 ruckus syslog: Root AP[7363 RAP@00:24:82:3f:14:60] accepts Mesh AP[7962
MAP@04:4f:aa:0c:b1:00] connection
Nov  3 14:55:20 ruckus syslog: Mesh AP[7962 MAP@04:4f:aa:0c:b1:00] disconnects from
AP[7363 RAP@00:24:82:3f:14:60]
Nov  3 14:55:20 ruckus syslog: Mesh AP[7962 MAP@04:4f:aa:0c:b1:00] disconnects from
AP[7363 RAP@00:24:82:3f:14:60]
Nov  3 14:55:17 ruckus syslog: Root AP[7363 RAP@00:24:82:3f:14:60] accepts Mesh AP[7962
MAP@04:4f:aa:0c:b1:00] connection
Nov  3 14:55:17 ruckus syslog: Root AP[7363 RAP@00:24:82:3f:14:60] accepts Mesh AP[7962
MAP@04:4f:aa:0c:b1:00] connection
```

Previous First 1 2 3 Last Next

AP Logs

To show current APs' logs, click here.

```
Oct 31 08:49:22 ruckus syslog: AP[7363 RAP@00:24:82:3f:14:60] joins with uptime [124] s
Oct 31 08:49:35 ruckus syslog: AP[7363 RAP@00:24:82:3f:14:60] cold boot successfully
Oct 31 08:50:10 ruckus syslog: Root AP[7363 RAP@00:24:82:3f:14:60] accepts Mesh AP[7962
MAP@04:4f:aa:0c:b1:00] connection
Oct 31 08:50:19 ruckus syslog: AP[7962 MAP@04:4f:aa:0c:b1:00] joins with uptime [136] s
Oct 31 08:50:31 ruckus syslog: AP[7962 MAP@04:4f:aa:0c:b1:00] cold boot successfully
Oct 31 08:51:05 ruckus syslog: Mesh AP[7962 MAP@04:4f:aa:0c:b1:00] connects to Root
AP[7363 RAP@00:24:82:3f:14:60] with RSSI [46] across [1] links
Oct 31 09:01:45 ruckus syslog: Receiving System Info from AP[7962 MAP@04:4f:aa:0c:b1:00]
```

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

The local capture mode stores packet data from a single capture session in two files using a ping-pong method. On 11n APs, each file holds 2 MB of packet data. On 11g APs, each file holds 1 MB. Whenever one file reaches its limit, the other file is cleared and begins filling. 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 wlan50 and wlan51, 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.

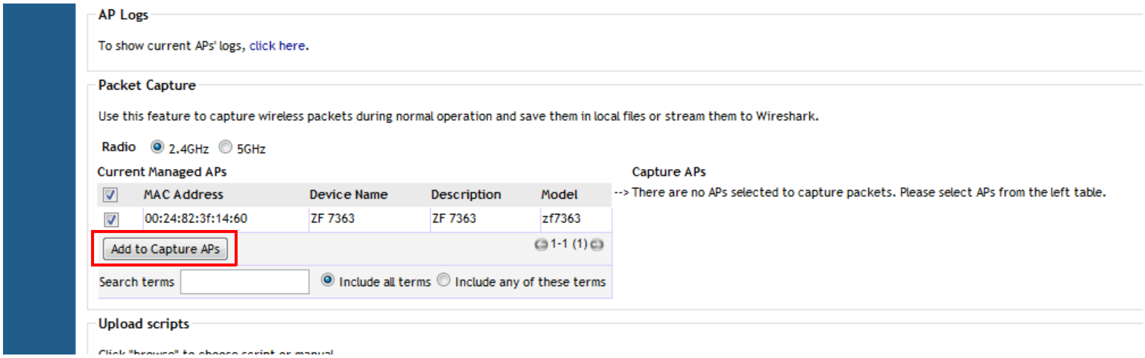
Streaming Mode

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**.
8. The remote host interface list on the right updates. Select **wlan50** from the list if you are streaming on the 2.4 GHz radio, or select **wlan51** if streaming on the 5 GHz radio.
9. Click **Start**. Wireshark displays the packet stream in a new window.

Figure 184. Add APs from Currently Managed APs list to Capture APs list



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	Device Name	Description	Model
☑	00:24:82:3f:14:60	ZF 7363	ZF 7363	zf7363

Add to Capture APs

1-1 (1)

Search terms ● Include all terms ○ Include any of these terms

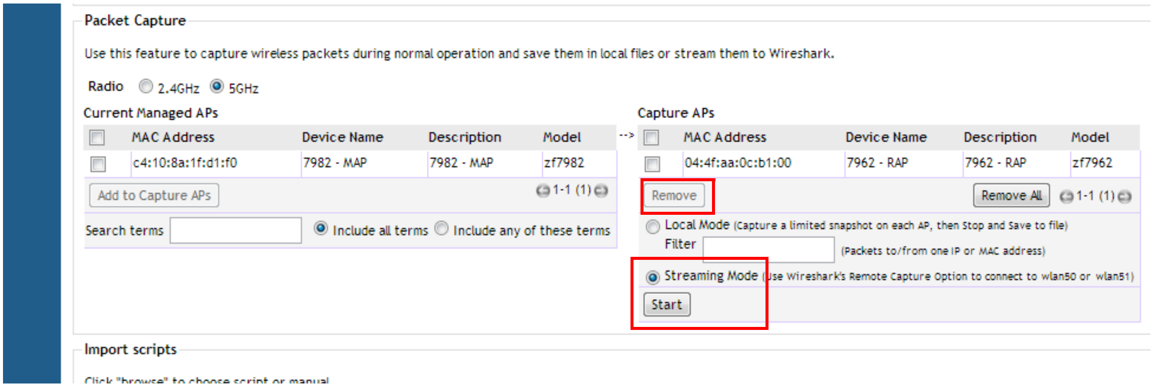
Capture APs

--> There are no APs selected to capture packets. Please select APs from the left table.

Upload scripts

Click "browse" to choose script or manual

Figure 185. Click Start to begin packet capture; click Remove to remove APs from the list



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	Device Name	Description	Model
□	c4:10:8a:1f:d1:f0	7982 - MAP	7982 - MAP	zf7982

Add to Capture APs

1-1 (1)

Search terms ● Include all terms ○ Include any of these terms

Capture APs

□	MAC Address	Device Name	Description	Model
□	04:4f:aa:0c:b1:00	7962 - RAP	7962 - RAP	zf7962

Remove

Remove All

1-1 (1)

○ Local Mode (Capture a limited snapshot on each AP, then Stop and Save to file)

Filter (Packets to/from one IP or MAC address)

● Streaming Mode (Use Wireshark's Remote Capture Option to connect to wlan50 or wlan51)

Start

Import scripts

Click "browse" to choose script or manual

Using Ruckus Custom Indicators

Packets captured on Ruckus APs include some information that is not available when capturing from other WiFi devices. This additional information is stored in the Per-Packet Information (PPI) header that precedes the over-the-air content.

1. The PPI:802.11-Common Header antenna signal and antenna noise fields of packets transmitted by the AP contain the next-to-lowest byte and the lowest byte, respectively, of the antenna pattern used to transmit the packet. On some APs, the pattern value may contain more significant bits, which are not stored in this header. If the packet is 802.11n, it will also contain the full antenna pattern value in the header described below.
2. The PPI:802.11n-MAC+PHY Header EVM-3 field of packets transmitted by the AP contains the full antenna pattern used to transmit the packet (similar to above, except this 32-bit field can accommodate the complete value).
3. The PPI:802.11n-MAC+PHY Header MAC Flags field's upper bits convey additional TX and RX descriptor indicators described in the table below.

Table 38. 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.

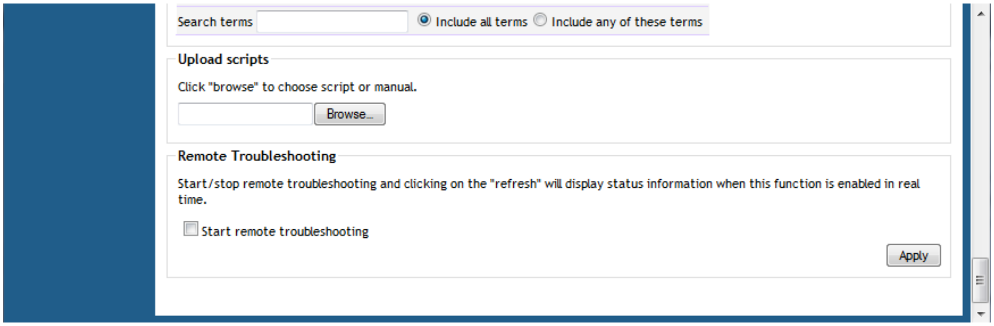
Importing a Script

The Upload 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 186. The Upload Scripts and Remote Troubleshooting features are used by Ruckus Support in diagnosing customer network issues remotely



Search terms ● Include all terms ○ Include any of these terms

Upload scripts

Click "browse" to choose script or manual.

Browse...

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

Apply

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".)

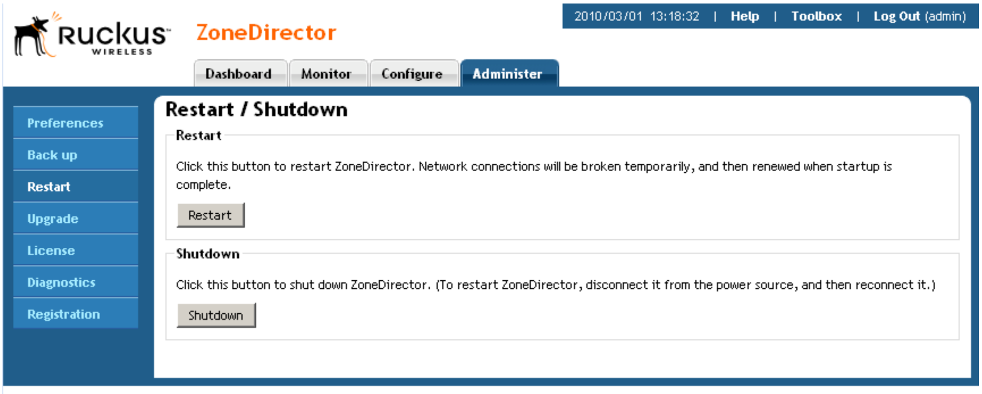
NOTE: If you have made any configuration changes, Ruckus Wireless recommends shutting down ZoneDirector to ensure that all configuration changes are saved and remain after reboot. Performing a Restart may cause ZoneDirector to lose configuration changes if you forgot to click Apply after making changes 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 187. The Restart/Shutdown page



Restart / Shutdown

Restart

Click this button to restart ZoneDirector. Network connections will be broken temporarily, and then renewed when startup is complete.

Restart

Shutdown

Click this button to shut down ZoneDirector. (To restart ZoneDirector, disconnect it from the power source, and then reconnect it.)

Shutdown

12

Smart Mesh Networking Best Practices

In This Appendix

Choosing the Right AP Model for Your Mesh Network

Ruckus Wireless supports both 802.11g and the newer, faster 802.11n APs with which to form a mesh network. Because mesh throughput degrades with the number of hops, the best performance can be achieved using the newer, faster 802.11n APs (ZoneFlex 7962, 7762, 7982, etc.).

However, the 802.11g APs (ZoneFlex 2942 and ZoneFlex 2741) will also form a suitable mesh network if your client devices do not support the newer 11n standard.

The most important point to note, however, is that the two technologies cannot be mixed in a mesh topology. All nodes in a mesh must be 802.11n or 802.11g. You cannot mix 802.11n with 802.11g APs in a mesh. You can mix ZoneFlex 2942 with ZoneFlex 2741 in the same mesh, because they are both 802.11g.

Additionally, dual band 11n APs can only mesh with other dual band 11n APs, and single band 11n APs can only mesh with other single band 11n APs.

In summary, build your mesh network as follows:

- Ensure that all APs are dual band 802.11n - ZoneFlex 7762, 7962, 7363, 7982
- Ensure that all APs are single band 802.11n - ZoneFlex 7341, 7343, 7321
- Ensure that all APs are 802.11g - ZoneFlex 2942 and ZoneFlex 2741

NOTE: The above restrictions apply only to AP-to-AP communication as part of a mesh, not to AP-to-client communication. For example, 802.11g clients can connect to an 802.11n mesh, and vice versa.

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.

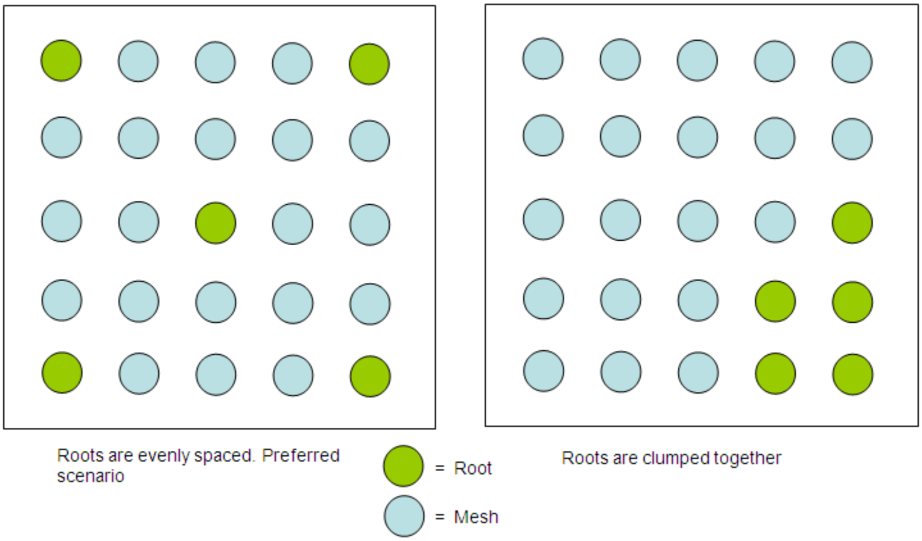
WiFi is a shared medium, of course, so this aggregate bandwidth will be shared amongst the concurrent users at any given time. In other words, if the network is designed to support 10Mbps, it would support 1 user at 10Mbps, or 10 users at 1Mbps each. In reality, due to statistical multiplexing (just 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 >= 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 188 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 188. Root Placement


Roots are evenly spaced. Preferred scenario
= Root
= Mesh
Roots are clumped together

- 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.

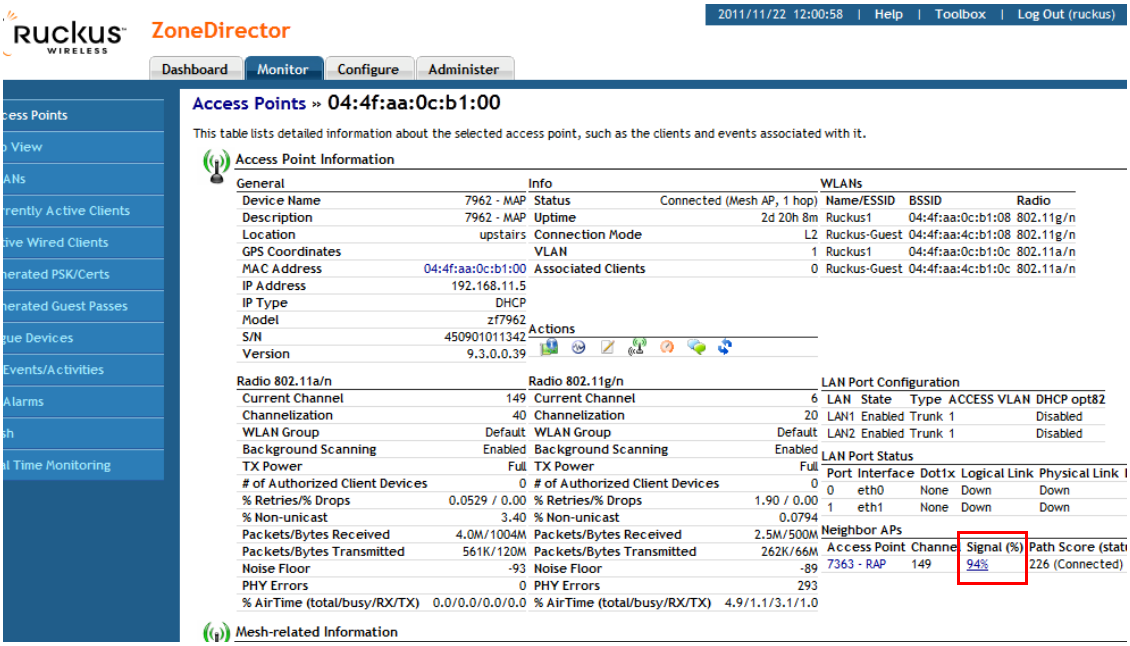
To view the Signal parameter in the Zone Director Web interface, go to **Monitor > Access Points**, and click on the Mesh AP being tested (click the MAC address) to see the Access Point detail screen, as shown in Figure 189 below.

There are two best practice observations that should be met:

- Ensure Signal >= 25%: The Signal value under Neighbor APs that shows “Connected” should be 25% or better. If it is lower, you need to bring the AP closer, or move it to avoid an obstruction, such that the Signal value becomes 25% or better. For a more conservative design, you may use 35% as your Signal benchmark.

- Ensure Minimum 2 Uplink options for every MAP: In addition, under Neighbor APs, it is best practice that there exists an alternate path for this mesh uplink. This alternate path should also have a Signal of 25% or better. Stated differently, there should be at least 2 possible links that the MAP can use for uplink, and both should have a Signal value of 25% or better. For a more conservative design, you may use 35% as your Signal benchmark.

Figure 189. Check the signal quality from the ZoneDirector Web interface



Access Points » 04:4f:aa:0c:b1:00

This table lists detailed information about the selected access point, such as the clients and events associated with it.

Access Point Information

General	
Device Name	7962 - MAP
Description	7962 - MAP
Location	upstairs
GPS Coordinates	
MAC Address	04:4f:aa:0c:b1:00
IP Address	192.168.11.5
IP Type	DHCP
Model	zf7962
S/N	450901011342
Version	9.3.0.0.39

Info	
Status	Connected (Mesh AP, 1 hop)
Uptime	2d 20h 8m
Connection Mode	L2
VLAN	1
Associated Clients	0

Name/ESSID	BSSID	Radio
Ruckus1	04:4f:aa:0c:b1:08	802.11g/n
Ruckus-Guest	04:4f:aa:4c:b1:08	802.11g/n
Ruckus1	04:4f:aa:0c:b1:0c	802.11a/n
Ruckus-Guest	04:4f:aa:4c:b1:0c	802.11a/n

Actions

Radio 802.11a/n	
Current Channel	149
Channelization	40
WLAN Group	Default
Background Scanning	Enabled
TX Power	Full
# of Authorized Client Devices	0
% Retries/% Drops	0.0529 / 0.00
% Non-unicast	3.40
Packets/Bytes Received	4.0M/1004M
Packets/Bytes Transmitted	561K/120M
Noise Floor	-93
PHY Errors	0
% AirTime (total/busy/RX/TX)	0.0/0.0/0.0/0.0

Radio 802.11g/n	
Current Channel	6
Channelization	20
WLAN Group	Default
Background Scanning	Enabled
TX Power	Full
# of Authorized Client Devices	0
% Retries/% Drops	1.90 / 0.00
% Non-unicast	0.0794
Packets/Bytes Received	2.5M/500M
Packets/Bytes Transmitted	262K/66M
Noise Floor	-89
PHY Errors	293
% AirTime (total/busy/RX/TX)	4.9/1.1/3.1/1.0

LAN Port Configuration

LAN	State	Type	ACCESS VLAN	DHCP opt82
LAN1	Enabled	Trunk	1	Disabled
LAN2	Enabled	Trunk	1	Disabled

LAN Port Status

Port	Interface	Dot1x	Logical Link	Physical Link
0	eth0	None	Down	Down
1	eth1	None	Down	Down

Neighbor APs

Access Point	Channe	Signal (%)	Path Score (stat
7363 - RAP	149	94%	226 (Connected)

Mesh-related Information

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.

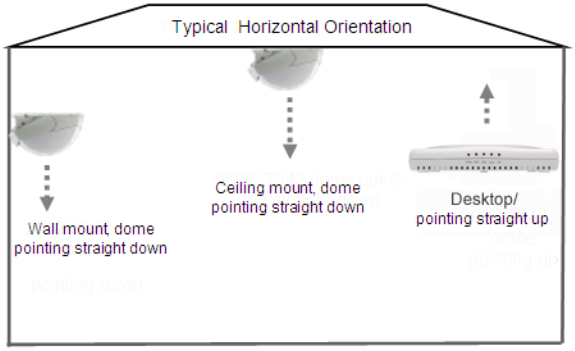
The bottom line regarding orientation and placement is that during the planning phase, it is advisable to use the Signal Quality as your benchmark, as explained in the Signal Quality Verification section. Ensure that the Signal is better than 25% for trouble-free operation.

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.

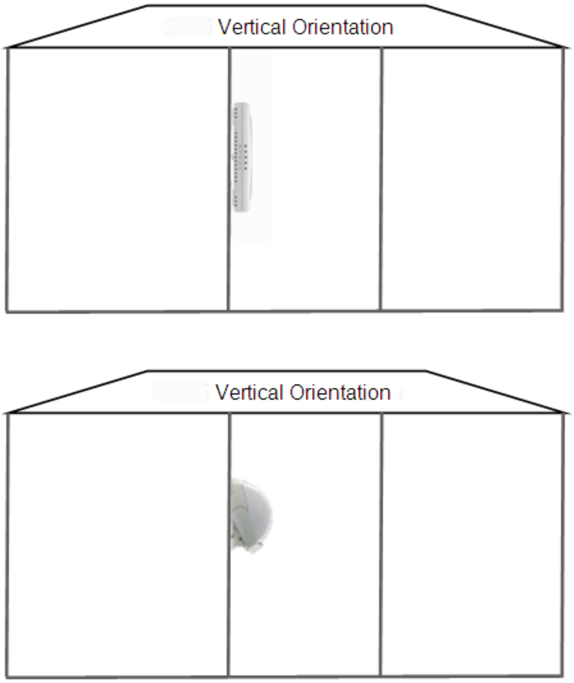
Figure 190. : ZoneFlex indoor AP horizontal orientation


Typical Horizontal Orientation
Wall mount, dome pointing straight down
Ceiling mount, dome pointing straight down
Desktop/ pointing straight up

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 191.

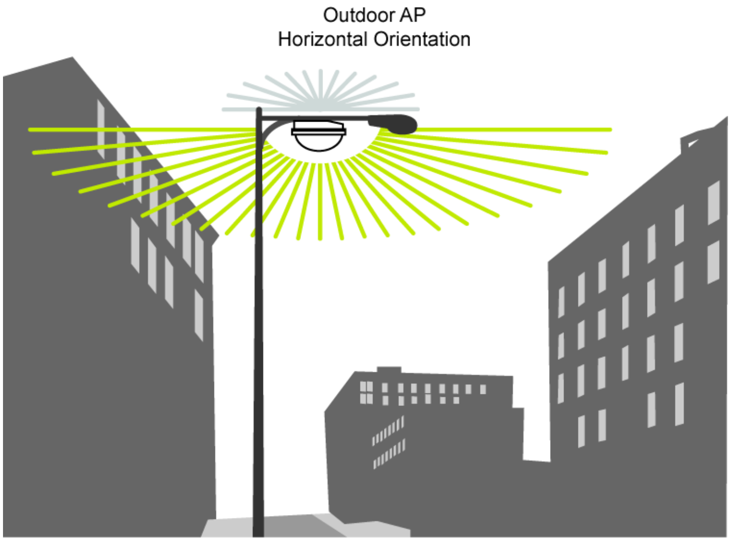
Figure 191. : ZoneFlex indoor AP vertical orientation



Outdoor APs - Typical Horizontal Orientation

Outdoor APs are typically mounted in a horizontal orientation, as shown in Figure 192. A less typical orientation would be vertically mounted.

Figure 192. 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 802.11n with 802.11g APs in your mesh. They will NOT mesh. Additionally, dual band 11n APs will not mesh with single band 11n APs. To ensure your APs will mesh with each other, ensure they are all of the same radio type: either all 802.11g, all 802.11n single band, or all 802.11n 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.

Index