Ruckus Wireless® ZoneDirector™ 8.1

User Guide

Part Number 800-70234-001
Published August 2009

www.ruckuswireless.com

About This Guide

This guide describes how to install, configure, and manage the Ruckus Wireless® ZoneDirector™ version 8.1. 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
	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 Access Point's 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 8.1 User Guide
- Part number: 800-70234-001
- Page 88

Contents

3 Managing a Wireless Local Area Network

4 Monitoring Your Wireless Network

5 Managing User and Guest Access

6 Deploying a Smart Mesh Network

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 (also referred to as APs). ZoneDirector provides simplified configuration and updates, WLAN security control, RF management, and automatic coordination of Ethernet-connected APs.

ZoneDirector also integrates network, radio frequency (RF), and location management within a single system. User authentication is accomplished with an integrated captive portal and internal database, or forwarded to existing AAA servers, such as RADIUS or Active Directory. Once users are authenticated, client traffic is not required to pass through ZoneDirector, thereby eliminating potential bottlenecks as higher speed Wi-Fi technologies, such as 802.11n, emerge.

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 resiliency.

This user guide provides complete instructions for using the Ruckus Wireless Web interface, the wireless network management toolbox for ZoneDirector. With the Web interface, you can customize and manage all aspects of ZoneDirector and the network. You will find all management tasks have been organized as categories and topics in the Contents page.

Figure 1. ZoneDirector 3000

Figure 2. ZoneDirector 1000

ZoneDirector Physical Features

This section describes the physical features of ZoneDirector 1000 and ZoneDirector 3000.

Buttons, Ports, and Connectors

Table 1 describes the buttons, ports, connectors on ZoneDirector 1000 and ZoneDirector 3000.

Table 1. Buttons, ports, and connectors on ZoneDirector 1000 and ZoneDirector 3000

Label	ZoneDirector 1000	ZoneDirector 3000
Power	(Located on the front panel) Press this button to power on ZoneDirector.	(Located on the rear panel) Press this button to power on ZoneDirector.
Console	DB-9 port for accessing the ZoneDirector command line interface	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 2.	

Table 1. Buttons, ports, and connectors on ZoneDirector 1000 and ZoneDirector 3000

Label	ZoneDirector 1000	ZoneDirector 3000
Reset	Use the Reset button to restart ZoneDirector or to reset it to factory default settings. To restart ZoneDirector, press the Reset button once. To reset ZoneDirector to factory default settings, press the Reset button for at least five (5) seconds. For more information, refer to "Alternate Factory Default Reset Method" on page 46. *WARNING: Resetting ZoneDirector to factory default settings will erase all configuration changes that you have made.*	To restart ZoneDirector, press the Reset button once.
F/D (ZoneDirector 3000 only)	Does not exist	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 46. *WARNING: Resetting ZoneDirector to factory default settings will erase all configuration changes that you have made.*
USB	Does not exist	For Ruckus Wireless Support use only

Front Panel LEDs

Table 2 describes the LEDs on front panel of ZoneDirector.

Table 2. Front Panel LEDs

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

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 you connect the APs to ZoneDirector (through network hubs or switches) and complete 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 easily configure wireless settings on Windows Vista, Windows XP, Windows Mobile, and Windows CE.

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 controlled access to your Ruckus WLAN with a minimum of setup.

You can now fine-tune and monitor your network through the Web interface, which assists you to customize additional WLANs for authorized users, manage your users, monitor the network's safety and performance, and even 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 that 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.

CAUTION! ZoneDirector and the ZoneFlex access points can communicate with each other via Layer 2 or Layer 3. If Layer 2 connectivity is desired, both ZoneDirector and the access points must be on the same broadcast domain (VLAN) and the same IP subnet.

How APs Discover ZoneDirector on the Network

1. When an AP starts up, it sends out a DHCP discover 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 8), the DHCP offer response will also include (among others) the IP addresses of ZoneDirector devices on the network or the DNS server that can help resolve the ZoneDirector IP addresses.
   - The AP will attempt to register with the ZoneDirector device 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 previous registered with (over a locally connected ZoneDirector).
3. After the AP obtains an IP address, it first attempts to discover if there is a ZoneDirector device on the same subnet by broadcasting an Ethernet *discovery request* frame (Layer 2 LWAPP message).
   - If the AP receives response from a single ZoneDirector device, it will attempt to register with that ZoneDirector device.
   - If the AP receives response from multiple ZoneDirector devices, it will attempt to register with the ZoneDirector device that it previously registered with (if any). 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 can support.
4. If the AP does not receive a response on the L2 network, it builds a list of ZoneDirector IP addresses that it received through Option 43 in the DHCP offer response in Step 2, or it uses the DNS server information to resolve the host name `zonedirector.{DNS domain name}`.
5. The AP sends out an IP discovery packet (Layer 3 LWAPP message) to the IP address list to attempt to discover ZoneDirector devices on other subnets.
   - If the AP receives response from a single ZoneDirector device, it will attempt to register with that ZoneDirector device.
   - If the AP receives response from multiple ZoneDirector devices, it will attempt to register with the ZoneDirector device that it previously registered with (if any). 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 users that ZoneDirector can support.

If the AP does not receive response from any ZoneDirector device on the network, it goes into idle mode. After a short period of time, reattempt to discover ZoneDirector again by repeating the same discovery cycle. The AP will continue to repeat this cycle until it successfully registers with ZoneDirector.

How to Ensure That APs Can Discover ZoneDirector on the Network

If you are deploying the AP 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 AP Intended to 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 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 AP Intended to 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 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

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 for 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.

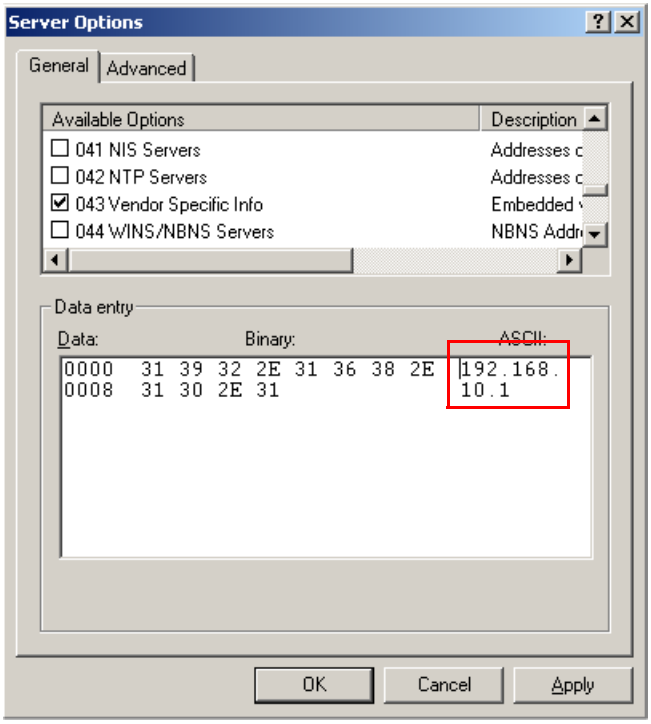
NOTE: The following procedure describes how to customize a DHCP server running on Microsoft Windows. If your DHCP server is running on a different operating system, the procedure may be different.

The procedure for configuring Option 43 on your DHCP server depends on whether both ZoneDirector and FlexMaster exist on the network, and whether you want to add the DHCP subcode for ZoneDirector.

If Only ZoneDirector Exists on the Network (No ZoneDirector Subcode)

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 **43 Vendor Specific Info** check box, and then select it.
5. Under Data Entry, position the cursor in the ASCII text area, and then type the IP address of the ZoneDirector device. In the figure below, the IP address of the ZoneDirector device is `192.168.10.1`.

Figure 3. In the ASCII area, type the IP address of the ZoneDirector device



The hexadecimal equivalent of the ZoneDirector IP address appears in the Binary text area.

NOTE: If there are multiple ZoneDirector devices on the network, type all the IP addresses in the ASCII text area. Use commas (,) to separate the IP addresses.

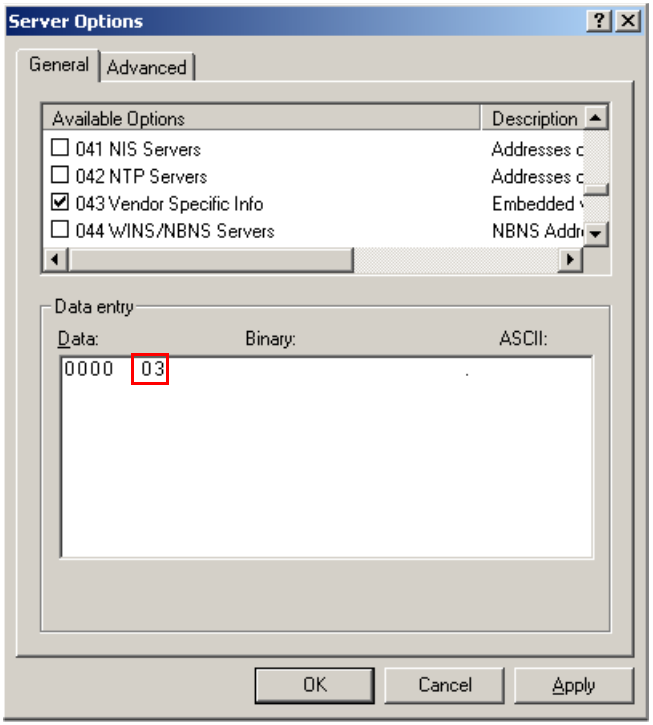
6. Click **Apply** to save your changes.
7. Click **OK** to close the Scope Options dialog box.

You have completed customizing your DHCP server to automatically provide supported APs with the ZoneDirector IP address.

If Only ZoneDirector Exists on the Network (With ZoneDirector Subcode)

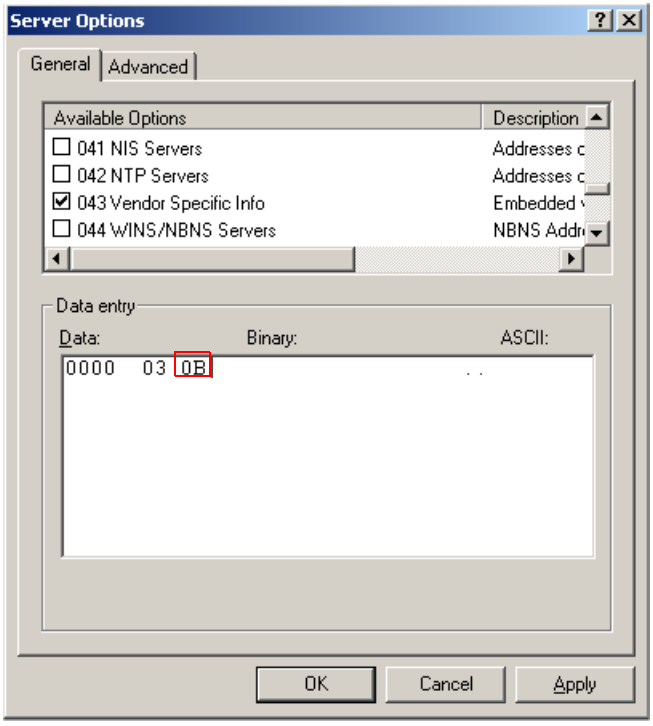
1. From Windows Administrative Tools, open **DHCP**, and then select the DHCP server you want to configure.
2. If the **Scope** folder is collapsed, click the plus (**+**) sign to expand it.
3. Right-click **Scope Options**, and then click **Configure Options**. The General tab of the Scope Options dialog box appears.
4. Under **Available Options**, look for the **43 Vendor Specific Info** check box, and then select it.
5. Under **Data Entry**, highlight the existing values, and then press **<Delete>** on your keyboard.
6. Position your cursor again after the last octet (in this example, 72) under the **Binary** text area, and then type `03` (the subcode for ZoneDirector).

Figure 4. Under the Binary text area, type 03 (the subcode for ZoneDirector)



7. After the ZoneDirector subcode (03), type the hexadecimal equivalent of the length of the ZoneDirector IP address length. For example, if the ZoneDirector IP address is `192.168.10.1`, the length in decimal is `12` and the hexadecimal equivalent is `0B`.

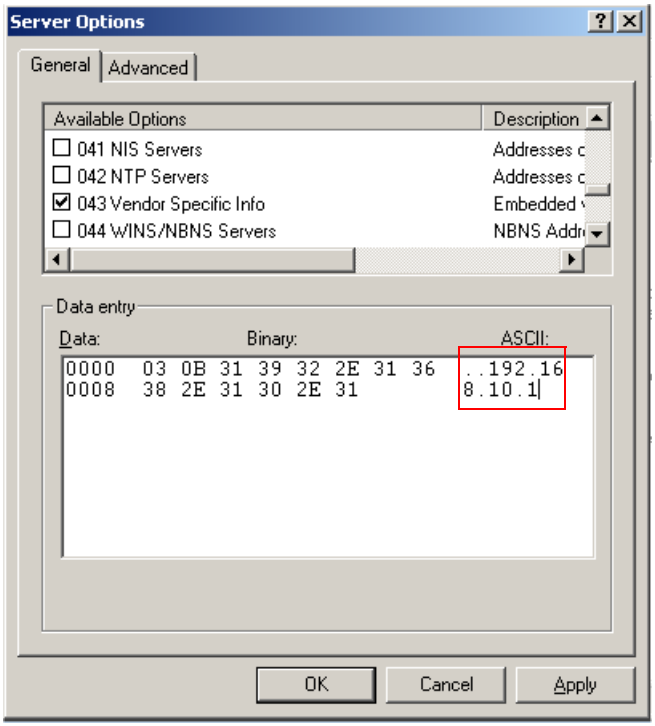
Figure 5. After the ZoneDirector subcode, type the hexadecimal equivalent of the ZoneDirector IP address length



8. Position the cursor under the ASCII text area, and then type the ZoneDirector IP address. If you typed the hexadecimal equivalent of the ZoneDirector IP address, there should be two bytes (represented by two periods) should already be filled under the ASCII text area.

   In the example below, the ZoneDirector IP address is `192.168.10.1`.

Figure 6. In the ASCII text area, type the ZoneDirector IP address



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

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

You have completed configuring DHCP Option 43 to provide supported APs with the ZoneDirector IP address.

If Both ZoneDirector and FlexMaster Exist on the Network

Before starting with this procedure, count the number of characters (including `http` or `https`, back slashes, colon, and periods) in the FlexMaster server URL and ZoneDirector IP address, and then convert these (decimal) values to hexadecimal. If there are multiple ZoneDirector devices on the network, count the total number of characters.

You will need this information when you configure DHCP Option 43 for both FlexMaster and ZoneDirector. 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 FlexMaster URL and ZoneDirector IP address that are used as examples in this procedure, including their length in decimal and hexadecimal values.

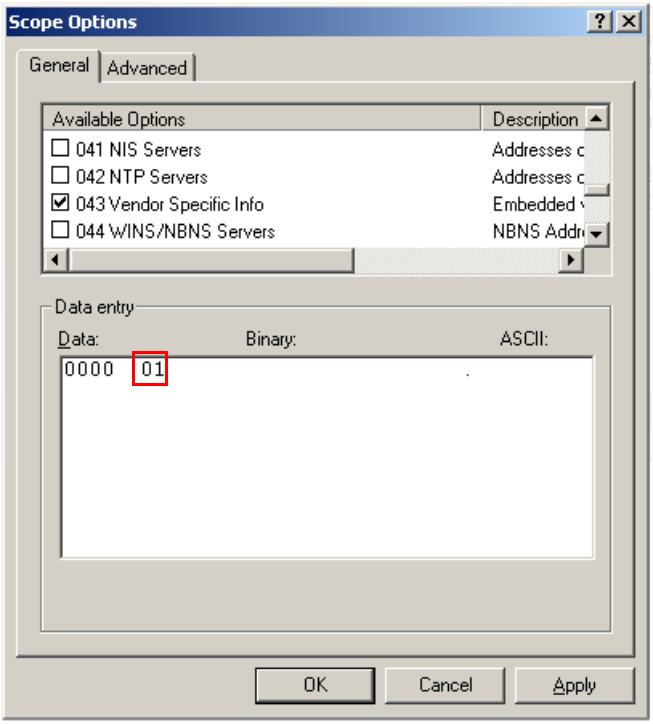
Table 3. URL/IP address values that are used as examples in this procedure

	URL / IP Address	Decimal Length	Hexadecimal Length
FlexMaster	`http://192.168.10.1/intune/server (URL)`	33	21
ZoneDirector	`192.168.10.2` (IP Address)	12	0C

Do the following on the DHCP server:

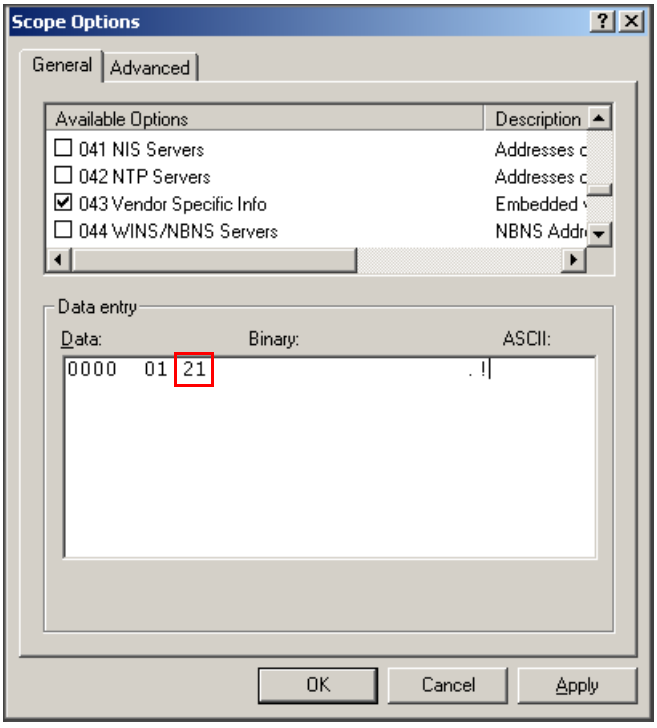
1. From Windows Administrative Tools, open **DHCP**, and then select the DHCP server you want to configure.
2. If the **Scope** folder is collapsed, click the plus (**+**) sign to expand it.
3. Right-click **Scope Options**, and then click **Configure Options**. The General tab of the Scope Options dialog box appears.
4. Under **Available Options**, look for the **43 Vendor Specific Info** check box, and then select it.
5. Under **Data Entry**, highlight the existing values, and then press **<Delete>** on your keyboard.
6. Position the cursor in the **Binary** text area, and then type `01`, the subcode for FlexMaster.

Figure 7. Type 01, the subcode for FlexMaster



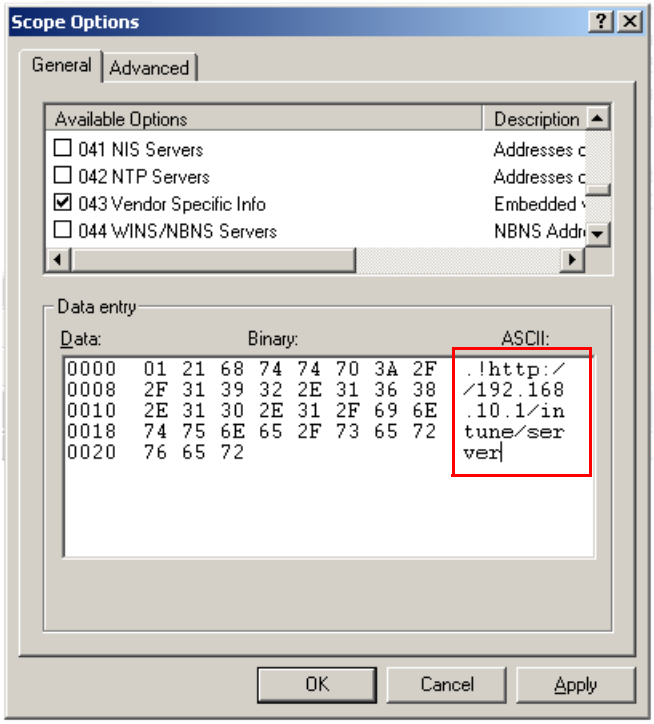
7. Under the **Binary** text area, position the cursor after the 01 subcode, and then type `21` – the hexadecimal equivalent of the FlexMaster server URL length that is used as example in this procedure.

Figure 8. After the 01 subcode for FlexMaster, type 21 – the hexadecimal equivalent of the FlexMaster server URL length



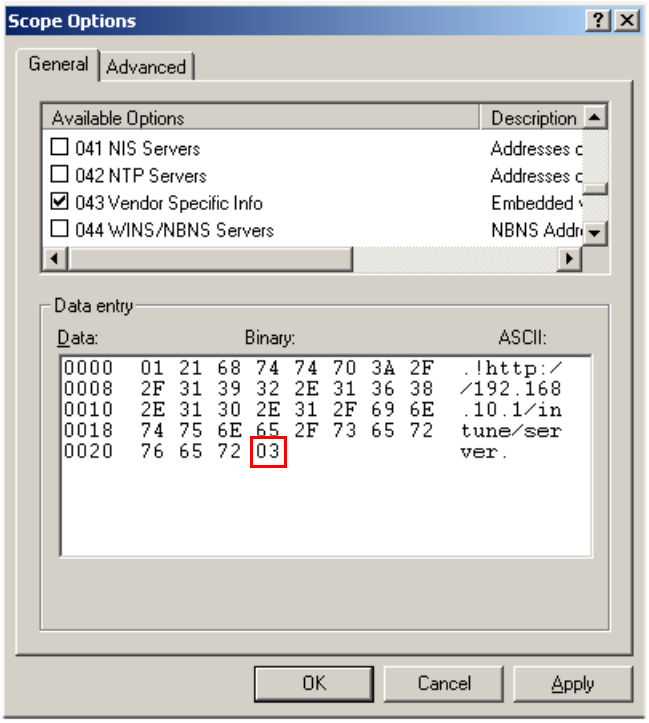
8. Position the cursor under the ASCII text area, and then type the FlexMaster server URL. In the example below, the FlexMaster server URL is `http://192.168.10.1/intune/server`.

Figure 9. In the ASCII text area, type the FlexMaster server URL



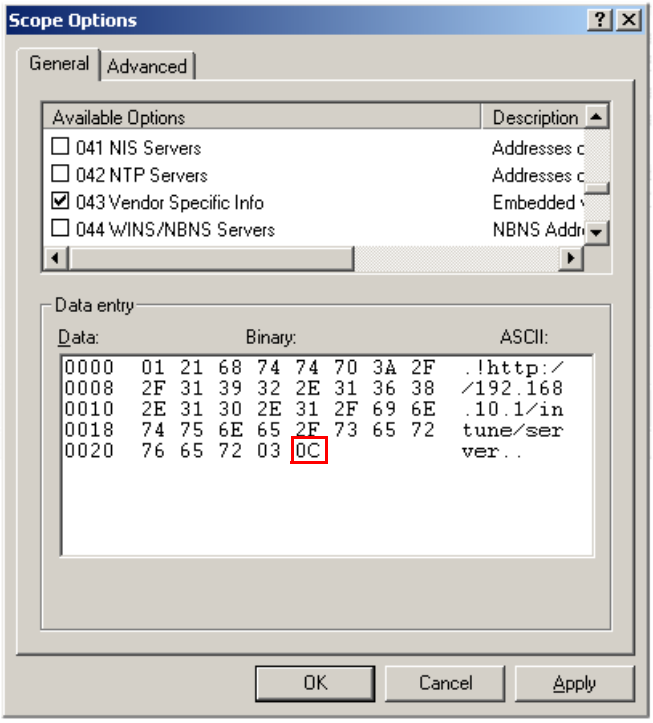
9. Position your cursor again after the last octet (in this example, 72) under the **Binary** text area, and then type `03` (the subcode for ZoneDirector).

Figure 10. Under the Binary text area, type 03 (the subcode for ZoneDirector)



10. After the ZoneDirector subcode (03), type the hexadecimal equivalent of the length of the ZoneDirector IP address length. For example, if the ZoneDirector IP address is `192.168.10.2`, the length in decimal is `12` and the hexadecimal equivalent is `0C`.

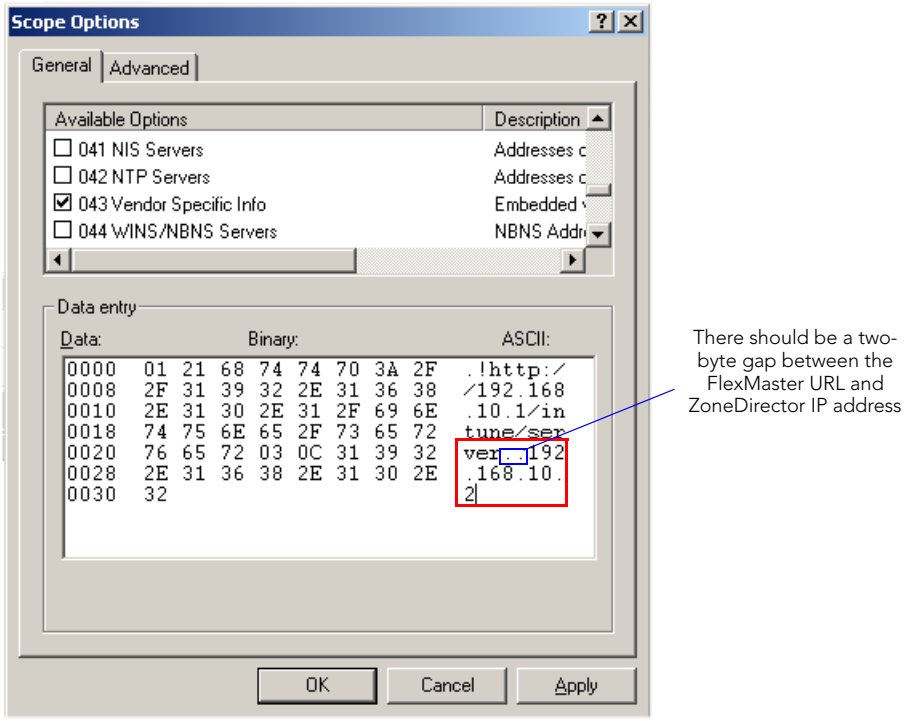
Figure 11. After the ZoneDirector subcode, type the hexadecimal equivalent of the ZoneDirector IP address length



11. Position the cursor under the ASCII text area after the FlexMaster server URL, and then type the ZoneDirector IP address. If you typed the hexadecimal equivalent of the ZoneDirector IP address, there should be two bytes

In the example below, the ZoneDirector IP address is `192.168.10.2`.

Figure 12. In the ASCII text area, type the ZoneDirector IP address (two bytes after the FlexMaster server URL)



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

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

You have completed configuring DHCP Option 43 to provide supported APs with the FlexMaster server URL and ZoneDirector IP address.

Option 3: Register ZoneDirector with a DNS Server

If you register ZoneDirector with your DNS server, supported APs that request for 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

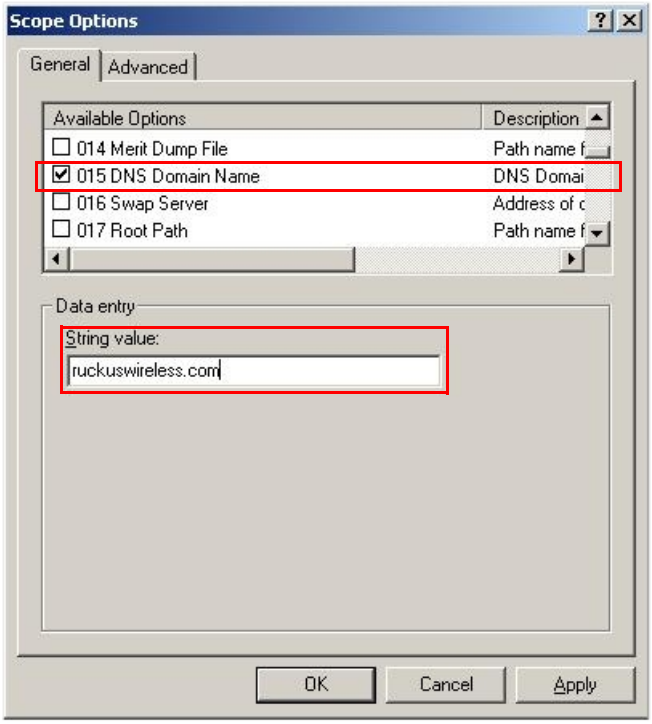
- Step 1: Set the DNS Domain Name on the DHCP Server
- Step 2: Set the DNS Server IP Address on the DHCP Server
- Step 3: Register the ZoneDirector IP Addresses with a DNS Server

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.

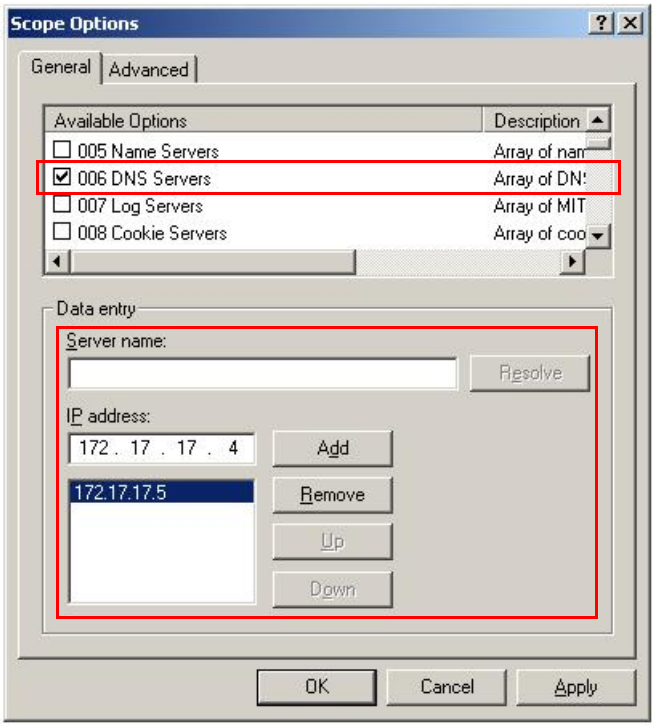
Figure 13. Select the 015 DNS Domain Name check box, and then type your company domain name in String value



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

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

Figure 14. Select the 6 DNS Servers check box, and then type your DNS server's IP address in the Data entry section



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

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

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

NOTE: 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.

Using the ZoneDirector Web Interface

The ZoneDirector administrative application is divided into five components that you can use to manage and monitor your Ruckus Wireless WLAN (including ZoneDirector and all APs).

Table 4. Components of the ZoneDirector Web interface

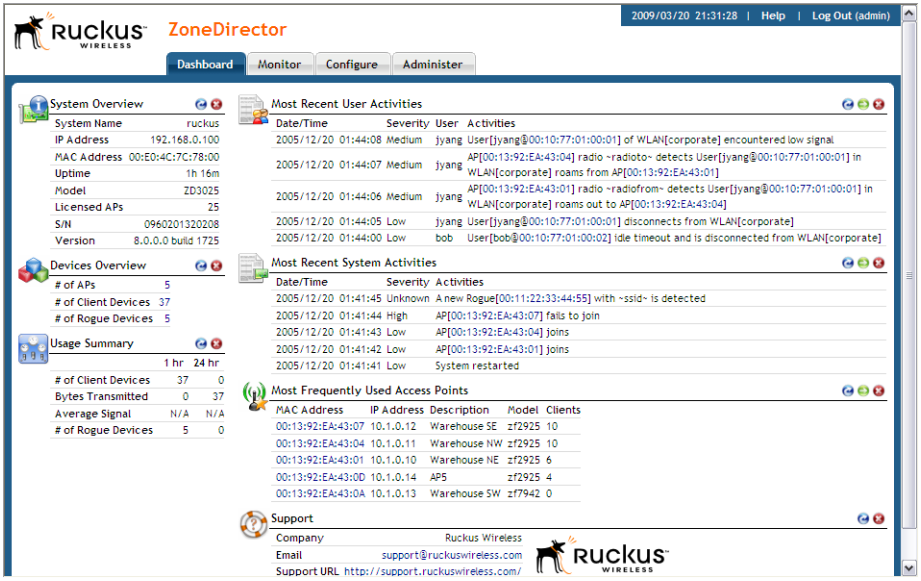
Dashboard	When you first log into your ZoneDirector with the Web interface, the Dashboard appears, displaying a number of widgets containing indicators and tables that summarize the network and its current status. Each indicator, gauge or table provides links to more focused, detailed views on elements 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 collections 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. Note: if you click any of the three tabs, the Dashboard becomes available as a fourth tab.
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.

[* = *Except for the Dashboard.*]

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 values that link to more focused, detailed views on elements of the network.

Figure 15. The Dashboard



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.

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, and software version number, among others.
- *Devices Overview*: Shows the number of APs being managed by ZoneDirector, as well as the number of clients connected to these managed APs. 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.
- *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.
- *Support*: Shows contact information for Ruckus Wireless support.

NOTE: You can sort the information (in ascending or descending order) that appears on the dashboard by clicking the column headerS.

Using Indicator Widgets

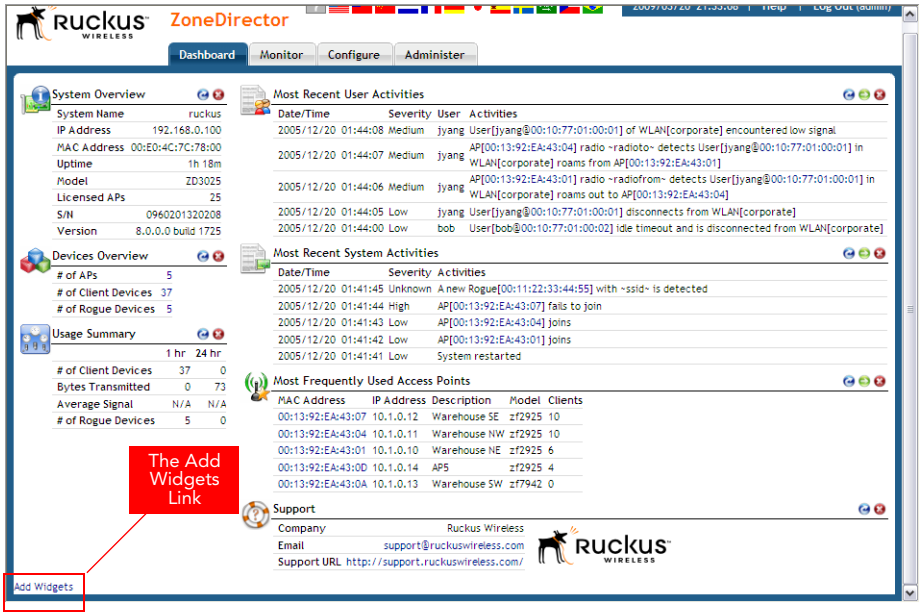
Dashboard widgets represent the indicators displayed as part of the active dashboard. Indicator widgets can be added or removed to enhance your ZoneDirector summary needs.

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.

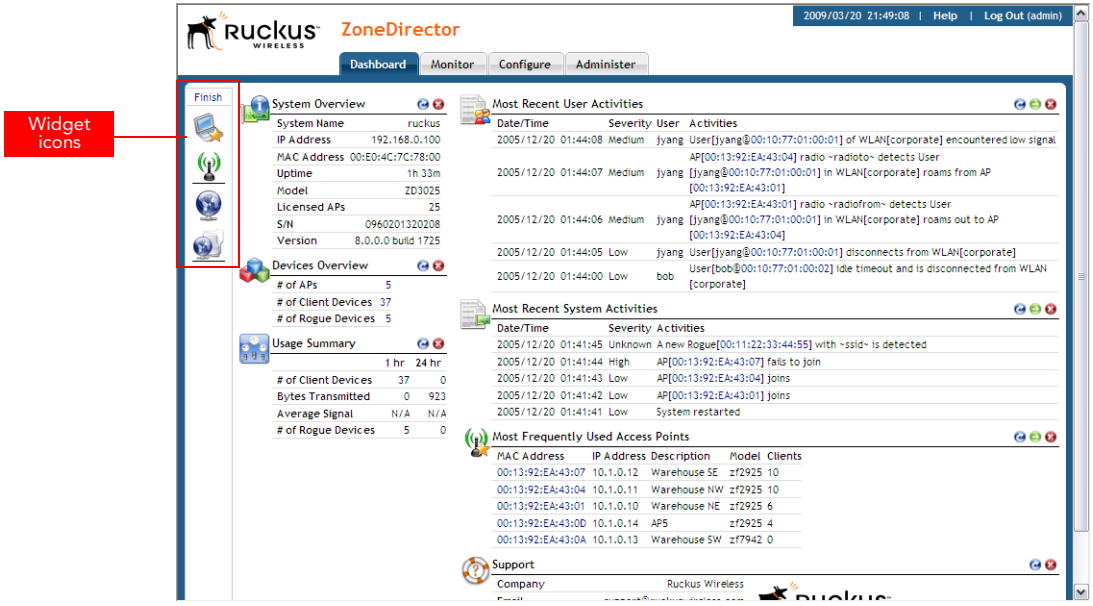
Figure 16. The Add Widgets link is at the bottom-right corner of the Dashboard



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

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

Figure 17. The widget icons appear at the top-left corner of the Dashboard

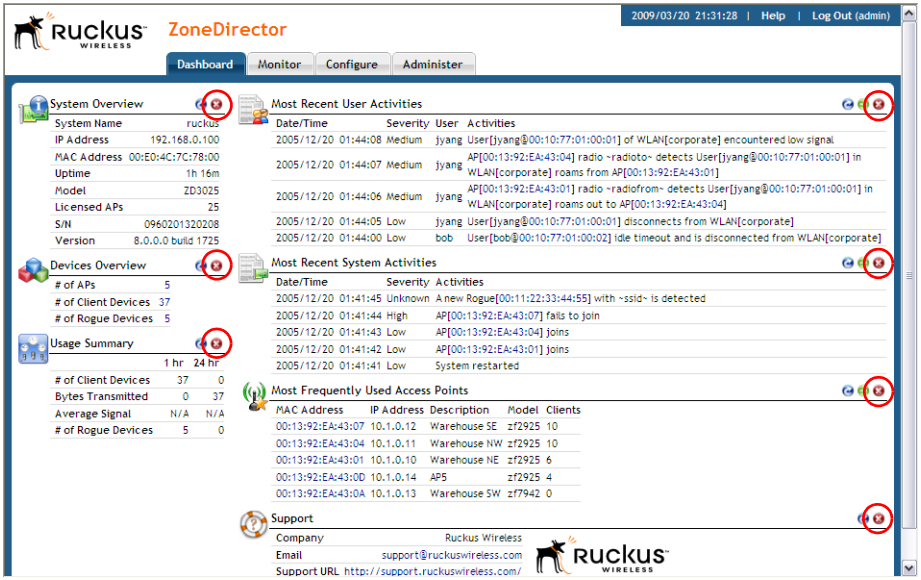


4. Click **Finish** in the Widgets pane to close it.

Removing a Widget

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

Figure 18. To remove a widget, click the corresponding red x icon



About Ruckus Wireless WLAN Security

After your initial setup, your Ruckus wireless network connects all authorized users by default to your internal WLAN. This WPA-based WLAN is configured to provide secure coverage for all authorized users. (A companion "guest" WLAN provides cleartext but controlled access for guest users.) But Ruckus Wireless offers other security options that can be applied to the internal WLAN through ZoneDirector.

These options range from a less-secure WEP key-based configuration, through the default WPA passphrase-based configuration to a higher-security, certificate-based 802.1x EAP configuration. Your choice mostly depends on what kinds of client authentication your users' client devices support.

For example, some of your WLAN users may be limited to a WEP-based security system by their client devices (computer or wireless network adapter). With the Web interface, you do have options: You can change the existing internal configuration from WPA to the less-secure WEP, or add a custom WLAN with WEP options for those users who require WEP, while retaining the original, more secure internal WPA configuration for the rest of your users. Or, you can replace the default WPA setup with a secure authentication/ encryption methodology, 802.1x EAP.

One drawback to 802.1x is the more labor-intensive setup, requiring (among other tasks) the transfer of root certificate copies to your users, who must then import the certificates into their client devices. This will prove disruptive if you have a large user audience already using your network.

ZoneDirector supports one or more WLANs, and if you need to add a WEP WLAN for those users, in addition to your WPA internal WLAN, you can easily do so. User could utilize the Zero-IT Activation to obtain the WEP key automatically or could manually enter the WEP key in their client device wireless configuration.

If you like the security of the default configuration, you can take advantage of customizable options that have no disruptive effect on your current users' connections.

All three basic options (WEP, WPA and 802.1x) are detailed in "Creating a WLAN" on page 64, and you can learn how to apply them to your Ruckus WLAN in the same section.

Controlling Device Permissions: Blocking and ACLs

ZoneDirector features a block list as well as access control list (ACL) functionality to control network permissions.

- *Block List*: When users log into a ZoneDirector network, their client devices (for example, laptop computers and PCs) are recorded and tracked. If, for any reason, you need to block a client device from network use, you can do via the ZoneDirector Web interface. For more on configuring the block list, see "Blocking Client Devices" on page 79.
- *Access Control Lists*: Access control lists (ACLs) establish which devices based on their MAC addresses are allowed to associate to a ZoneDirector-managed AP. By using the **Configure** > **Access Control** options, you define Layer 2 ACLs, also known as MAC address ACLs, which can then be applied to one or more ZoneDirector WLANs. 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. For more on configuring ACLs, see "Configuring Access Control Lists" on page 61.

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.

2

Configuring System Settings

In This Chapter

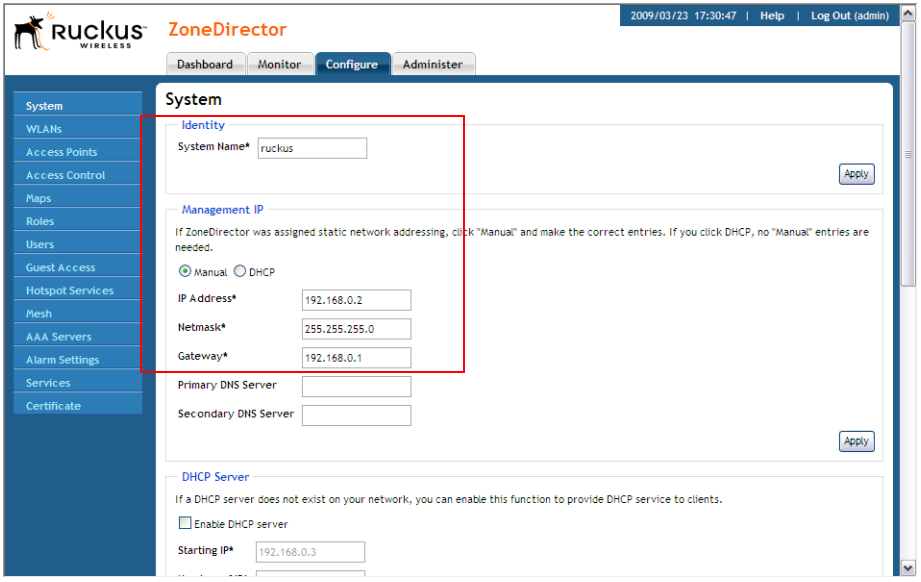
Changing the Network Addressing

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 Management IP options.

Figure 19. The Management IP options



3. Select one of the following:
   - *Manual*: If you select Manual, enter the correct information in the now-active fields (IP Address, Netmask, and Gateway are required).
   - *DHCP*: If you select DHCP, no further information is required.
4. Click **Apply** to save your settings. You will lose connection to ZoneDirector.

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.

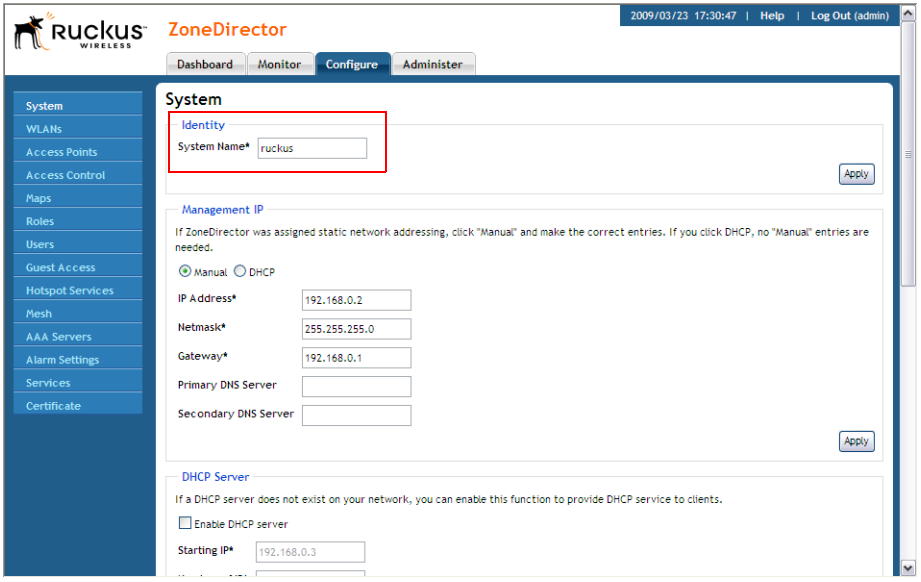
Changing the System Name

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.
3. Click **Apply** to save your settings. The change goes into effect immediately.

Figure 20. The Identity section on the Configure > System page



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. Note that before you can enable the built-in DHCP server, ZoneDirector must be assigned a manual (or static) IP address. If you configured ZoneDirector to obtain IP address from another DHCP server on the network, the options for the built-in DHCP server will not be visible on the System page.

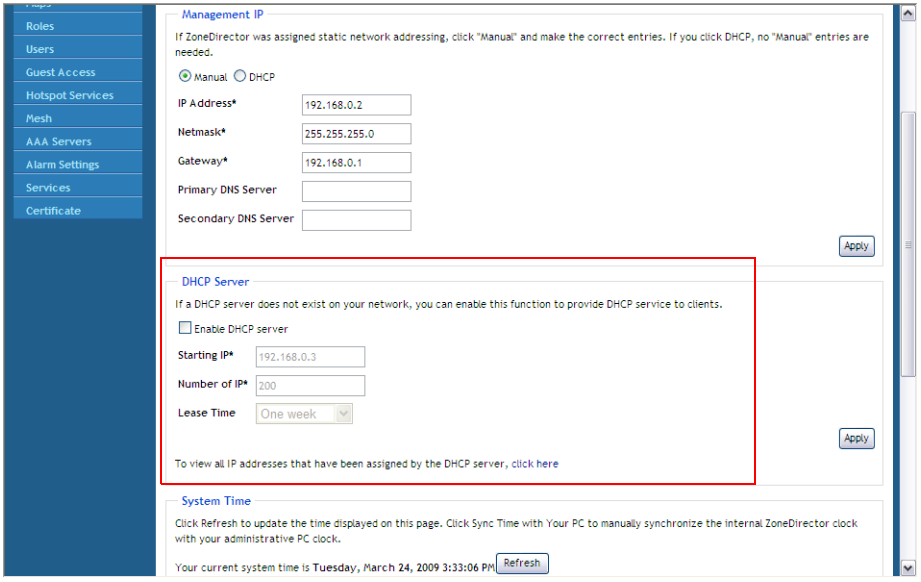
Enabling the Built-in DHCP server

NOTE: Ruckus Wireless recommends that you only enable the built-in DHCP server if there are no other DHCP servers on the network. Note that 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 "Detecting Rogue DHCP Servers" on page 94.

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.
4. Note that 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 if you want ZoneDirector to correct the value. Click OK to automatically correct the entry.
5. In **Number of IP**, type the maximum number of IP addresses that you want to allocate to requesting clients. The built-in DHCP server can allocate up to 255 IP addresses, including the one assigned to ZoneDirector. The default value is 200.
6. In **Lease Time**, select a time period during IP addresses will be allocated to DHCP clients. Options range from six hours to two weeks (default is one week).
7. Click **Apply**.

NOTE: If you typed an invalid value in any of the text boxes, an error message appears and prompts you if you want ZoneDirector to automatically correct the value. Click OK to change it to a correct value.

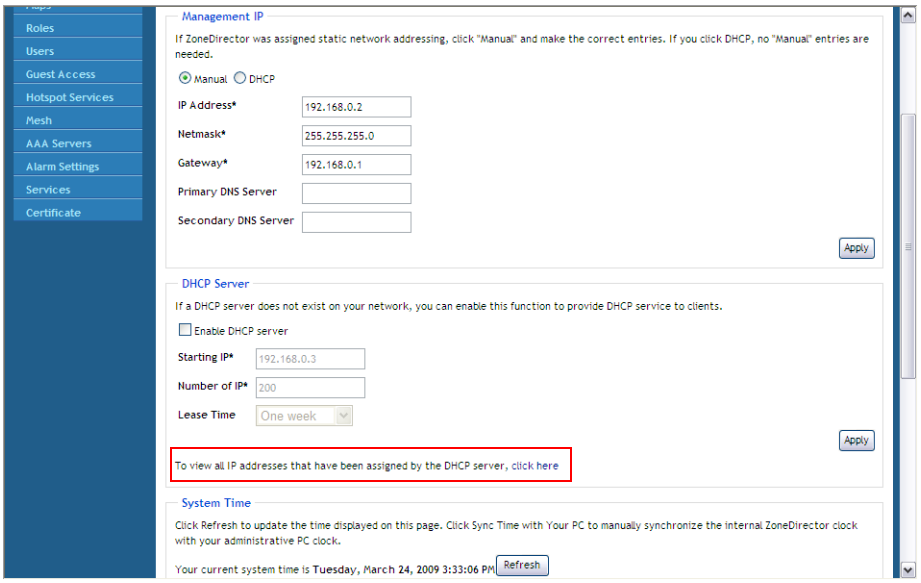
Figure 21. The DHCP Server options



Viewing DHCP Clients

To view a list of current DHCP clients, click the click here link at the end of the "To see all currently assigned IPs by 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 22. To view current DHCP clients, click the "click here" link



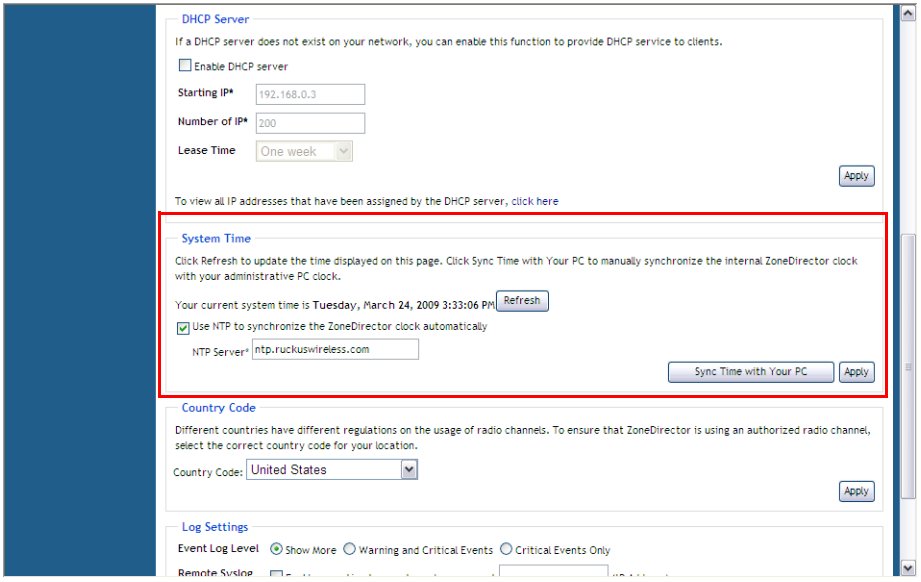
Updating the Internal Clock

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.

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

Figure 23. The System Time options



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.

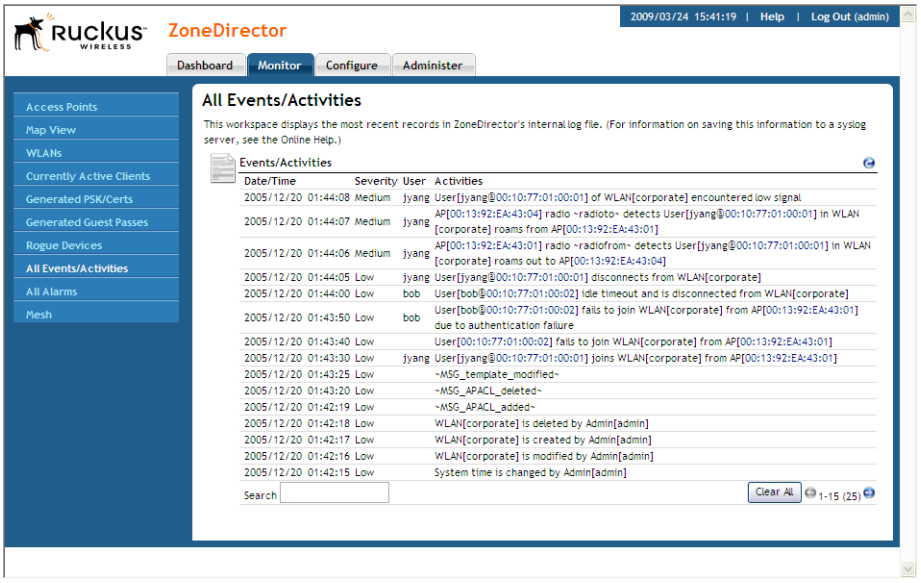
Reviewing the Current Log Contents

1. Go to **Monitor** > **All Events/Activities**.
2. Review the events and alarms listed here. See page 38.

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 24. The All Events/Activities page

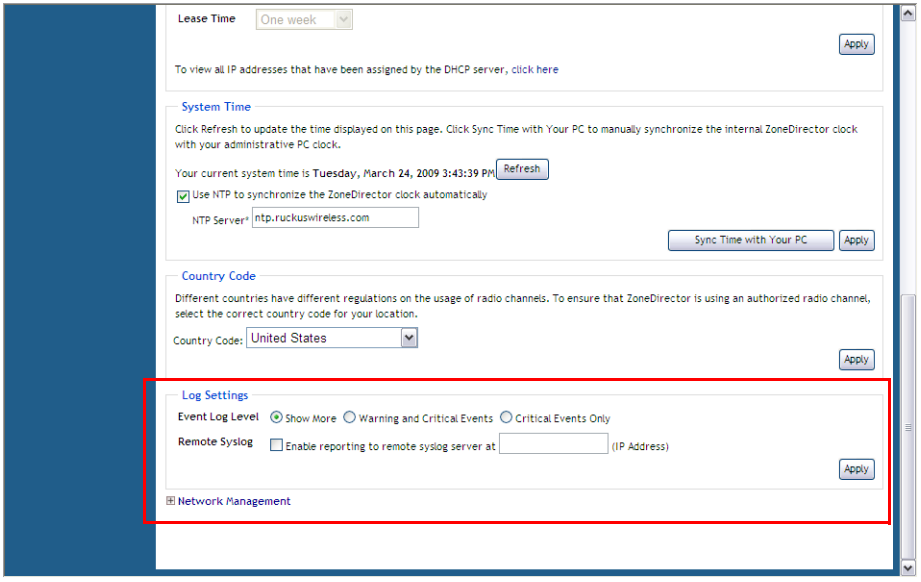


Checking the Current Log Settings

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

Figure 25. The Log Settings options



Setting Up Email Alarm Notification

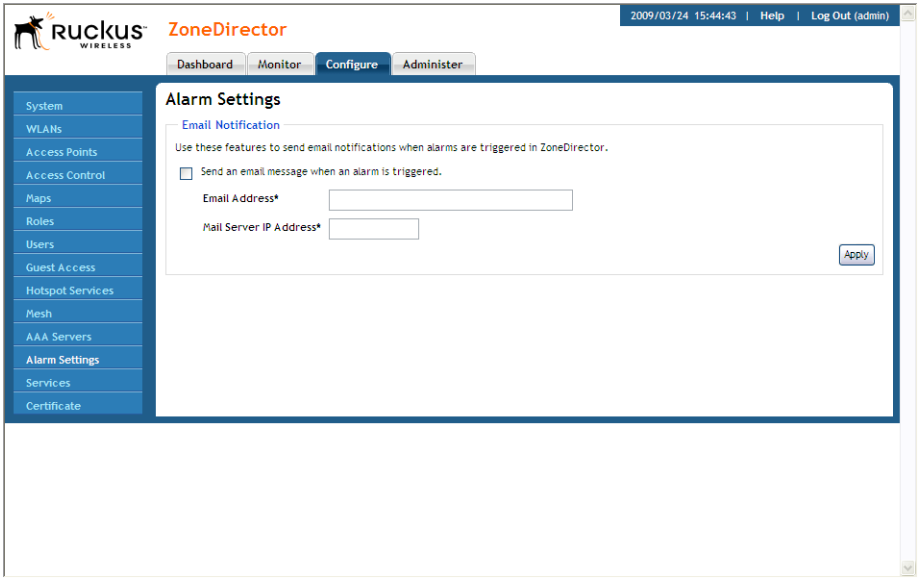
If an alarm condition is detected, ZoneDirector will record it in the event log. If you prefer, an email notification can be sent to a configured email address of your choosing.

NOTE: For the types of events that generate email alarms, refer to "Events That Trigger Alarm Notifications" in the following section.

To enable 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. In **Email Address**, type the email address to which to send the alarm message.
4. In **Mail Server IP Address**, type the IP address of your mail server.
5. Click **Apply**. The email notification feature becomes active immediately.

Figure 26. The Alarm Settings page



Events That Trigger Alarm Notifications

There are five events that trigger email alarm notifications in ZoneDirector:

- *Detection of rogue AP*: When ZoneDirector detects a rogue AP on the network, it sends the following alarm message:
  `A new rogue {rogue AP name} with {SSID} is detected.`
- *Detection of ad hoc network*: When ZoneDirector detects an ad hoc network, it sends the following alarm message:
  `A new ad-hoc network {adhoc network name} with {SSID} is detected.`
- *Lost contact with AP*: When ZoneDirector loses communication with an AP and is unable to re-establish communication after 20 minutes, it sends the following alarm message:
  `Lost contact to {AP name}.`
- *Detection of an SSID-spoofing AP*: When ZoneDirector detects that an unauthorized AP is spoofing the SSID of one of your APs, it sends the following alarm message:
  `A new SSID-spoofing {rogue AP name} with {SSID} is detected.`
- *Detection of a MAC address-spoofing AP*: When ZoneDirector detects that an unauthorized AP is spoofing the SSID of one of your APs, it sends the following alarm message:
  `A new MAC-spoofing {rogue AP name} with {SSID} is detected.`
- *Detection of rogue DHCP server*: When ZoneDirector detects a rogue DHCP server on the network, it sends the following alarm message:
  `Rogue DHCP server on {ip} is detected.`

When any of these events occur, ZoneDirector sends an email notification to the email address that you specified on the **Configure** > **Alarm Settings** page.

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 an alarm notification whenever the *Lost contact with AP* event occurs.

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 your ZoneDirector is running software version 7.0 or earlier and you want to upgrade to software version 8.1, you need to upgrade it to version 7.1 first, and then upgrade it to version 8.1. If you try to upgrade from version 7.0 to 8.1 directly, the upgrade will fail because of a file size upload limitation in version 7.0 and earlier.

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 27. The Upgrade page

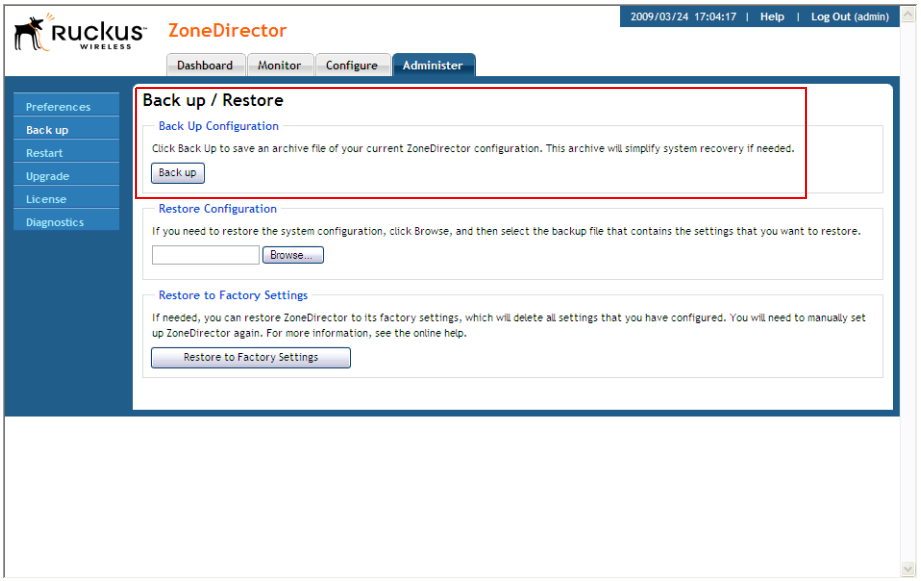
Working with Backup Files

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 ".TGZ" extension.
6. When the *Download Complete* dialog box appears, click **Close**.

Figure 28. The Back Up Configuration option



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. Review the Restore Configuration instructions, and then click **Browse**.
3. Use the Browse dialog box to locate the backup file.
4. Select the file, and then click Open. 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, and access control list, among others).

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/IP address*: Select this option if you are deploying a second ZoneDirector for failover purposes.
- Restore only configurations about WLANs, Access Controls, Roles, and Users: 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 off the Web interface. When the restore process is complete, ZoneDirector automatically restarts and your wireless network will be ready for use again.

Restoring ZoneDirector to Default Factory Settings

In certain extreme conditions, you may want to reinitialize ZoneDirector, and reset it to the "factory default" state. In such a state, the network is almost ready for use, but all your user/guest/log and other records, accounts and 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`.
A complete set of instructions is available in the 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 a factory-default state has been restored.

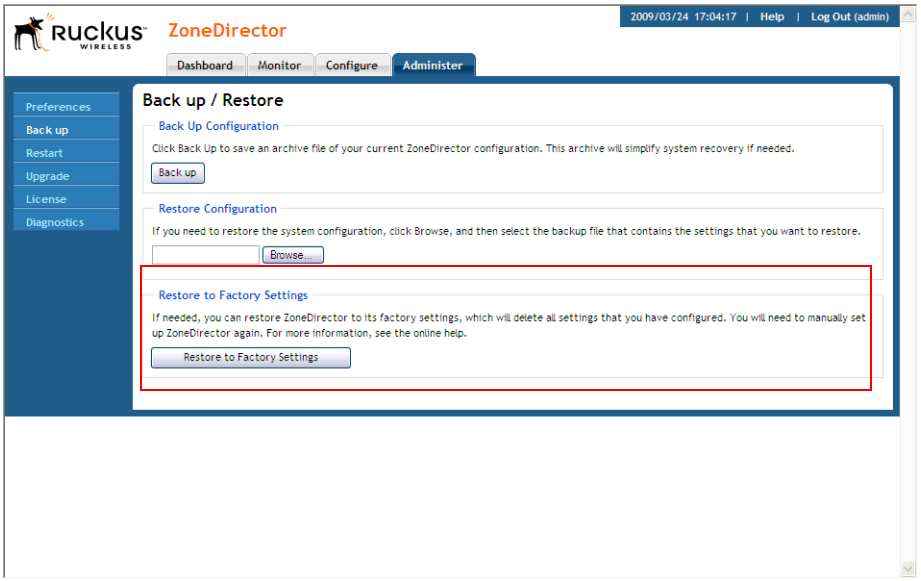
To reset your ZoneDirector to factory default settings

1. Go to **Administer** > **Backup**.
2. When the *Backup/Restore* page appears, look for **Restore to 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.

When this process begins, you will be logged out of the Web interface.

When the reset is complete, the Status LED is a blinking red, then a 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 29. The Restore to Factory Settings section



Alternate Factory Default Reset Method

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

NOTE: Do not disconnect ZoneDirector from any power source until this procedure is complete.

1. Look for a pinhole on the right side of 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 is a blinking red, then a blinking green, indicating that the system is in a "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.

To create a certificate request file

1. Go to **Configure** > **SSL Certificate**.
2. In the *Generate a Request* section, complete the following options:
   - *Common Name (IP)*: Type the IP address for your Web server. This must be an exact match (for example. `192.168.0.2`).
   - *Domain Name*: Type the fully qualified domain name of your Web server. This must be an exact match (for example, `www.ruckuswireless.com`).
   - *Organization*: Type the complete legal name of your organization (for example, `Ruckus Wireless, Inc.`). Do not abbreviate your organization name.
   - *Organization Unit*: Type the name of the division, department, or section in your organization that manages network security (for example, Network Management).
   - *Locality or 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*: Type the two-letter ISO abbreviation for your country (for example, if your organization is located in the United States, type `US`).
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-----

MIIFVjCCBD6gAwIBAgIQLfaGuqKukMumWhbVf5v4vDANBgkqhkiG9w0BAQUFAD
CBsDELMAkGA1UEBhMCVVMxFzAVBgNVBAoTDlZlcmlTaWduLCBJbmMuMR8wHQYD
VQQLBgEFBQcBAQRtMGswJAYIKwYBBQUHMAGGGGh0dHA6Ly9vY3NwLnZlcmlzaW
duLmNvbTBDBggrBgEFBQcwAoY3aHR0cDovL1NWUlNlY3VyZS1haWEudmVyaXNp
Z24uY29tL1NWUlNlY3VyZTIwMDUtYWlhLmNlcjBuBggrBgEFBQcBDARiMGChXq
BcMFowWDBWFglpbWFnZS9naWYwITAfMAcGBSsOAwIaBBRLa7kolgYMu9BSOJsp
rEsHiyEFGDAmFiRodHRwOi8vbG9nby52ZXJpc2lnbi5jb20vdnNsb2dvMS5naW
YwDQYJKoZIhvcNAQEFBQADggEBAI/S2dmm/
kgPeVAlsIHmx751o4oq8+fwehRDBmQDaKiBvVXGZ5ZMnoc3DMyDjx0SrI9lkPs
n223CV3UVBZo385g1T4iKwXgcQ7WF6QcUYOE6HK+4ZGcHermFf3fv3C1FoCjq+
zEu8ZboUf3fWbGprGRA+MR/dDI1dTPtSUG7/zWjXO5jC//0pykSldW/
q8hgO8kq30S8JzCwkqrXJfQ050N4TJtgb/
YC4gwH3BuB9wqpRjUahTiK1V1ju9bHB+bFkMWIIMIXc1Js62JClWzwFgaGUS2D
LE8xICQ3wU1ez8RUPGnwSxAYtZ2N7zDxYDP2tEiO5j2cXY7O8mR3ni0C30=
-----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.

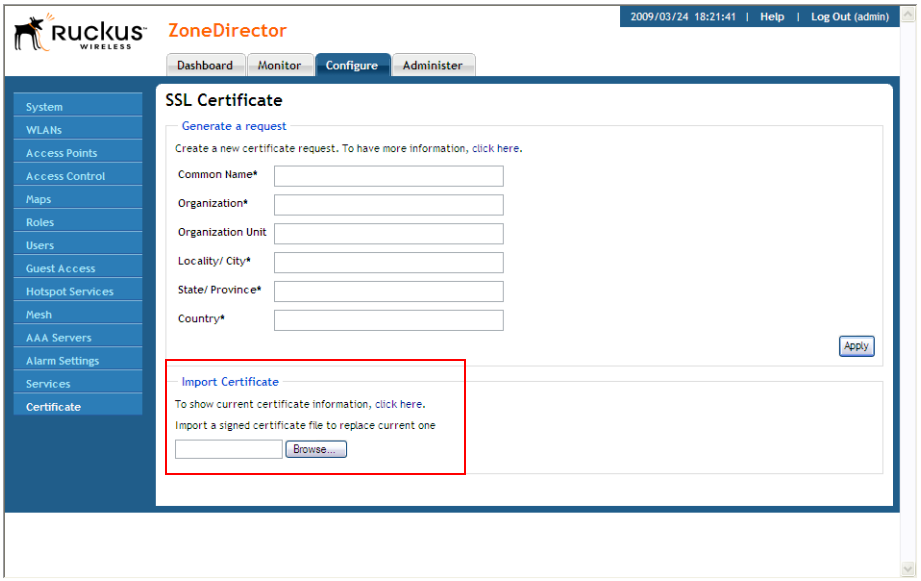
Importing an SSL Certificate

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 location (either on the local drive or a network share) that you can access from the ZoneDirector Web interface.
2. Log on to the ZoneDirector Web interface, and then click **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 finish importing the certificate file to ZoneDirector.

Figure 30. The Import Certificate section



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

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.

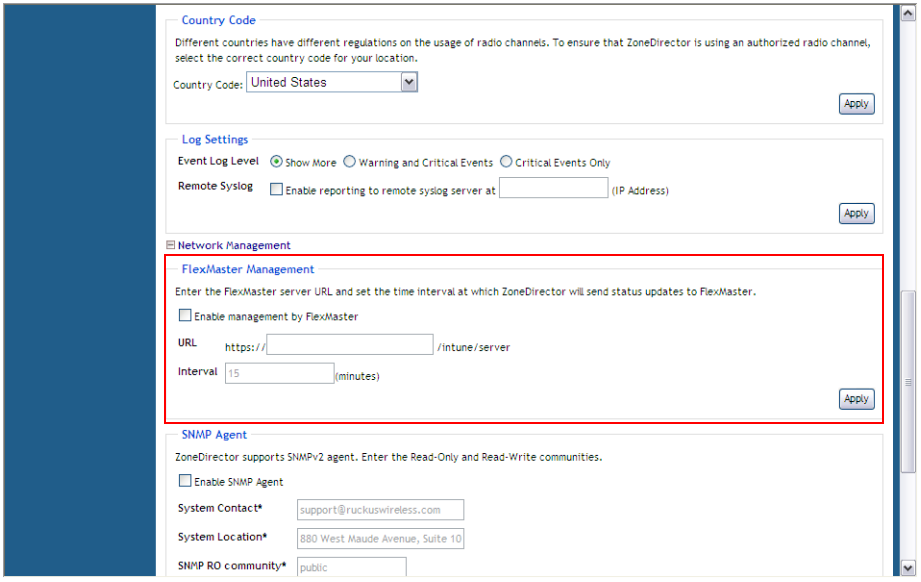
To enable FlexMaster management

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 (bottom of the page), select the **Enable management by FlexMaster** check box.
5. In **URL**, type the 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 31. The FlexMaster Management options



Configuring SNMP Support

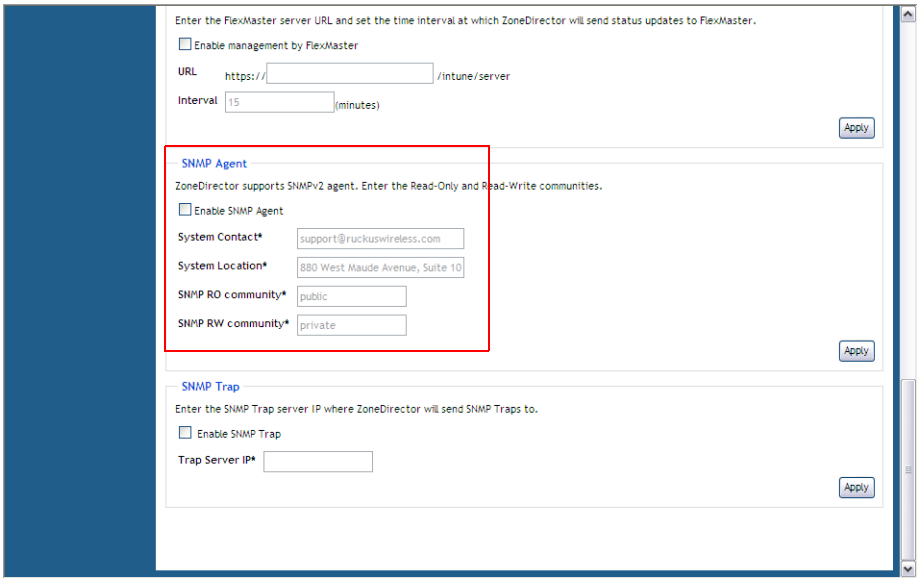
ZoneDirector provides support for Simple Network Management Protocol (SNMP) v2, which allows you to query ZoneDirector information, such as system status, WLAN list, AP list, and clients list, and to set a number of system settings. You can also enable SNMP traps to receive immediate notifications for possible AP and client issues.

Enabling the SNMP Agent

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.

1. In the Network Management section of the System page, scroll down to the bottom of the page.
2. Under the **SNMP Agent** section, select the **Enable SNMP Agent** check box.
3. 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`.
4. 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`.
5. In **System Contact**, type your email address (optional).
6. In **System Location**, type the location of the ZoneDirector device (optional).
7. Click **Apply** to save your changes.

Figure 32. Enabling the SNMP agent



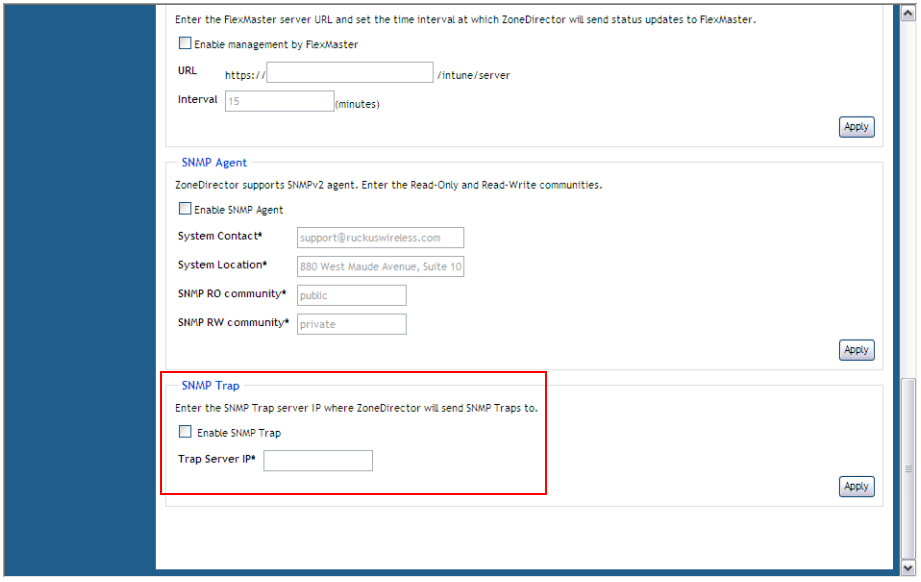
Enabling SNMP Trap Notifications

If you have an SNMP trap server 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 53).

To enable SNMP trap notifications

1. In the Network Management section of the System page, scroll down to the bottom of the page.
2. Under **SNMP Trap**, select the **Enable SNMP Trap** check box.
3. In **Trap Server IP**, type the IP address of the SNMP trap server on the network.
4. Click **Apply** to save your changes.

Figure 33. Enabling SNMP trap notifications



Trap Notifications That ZoneDirector Sends

There are seven events for which ZoneDirector will send trap notifications to the SNMP server that you specified. Table 5 lists the trap notifications that ZoneDirector sends and when they are sent.

Table 5. Trap notifications

Trap Name	Description
`ruckusZDEventAPJoinTrap`	An AP has joined ZoneDirector. The AP's MAC address is included in the trap notification.
`ruckusZDEventSSIDSpoofTrap`	An SSID-spoofing rogue AP has been detected on the network. The rogue AP's MAC address and SSID are included in the trap notification.
`ruckusZDEventMACSpoofTrap`	A MAC-spoofing rogue AP has been detected on the network. The rogue AP's MAC address and SSID are included in the trap notification.
`ruckusZDEventRogueAPTrap`	A rogue AP has been detected on the network. The rogue AP's MAC address and SSID are included in the trap notification.
`ruckusZDEventAPLostTrap`	An AP has lost contact with ZoneDirector. The AP's MAC address is included in the trap notification.

Table 5. Trap notifications

Trap Name	Description
`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.

3

Managing a Wireless Local Area Network

In This Chapter

Overview of Wireless Networks

When your ZoneDirector setup is complete, you have a fully functional wireless network, based on two secure WLANs ("internal" and "guest") with access for authorized users and guests. The internal WLAN provides "zero IT" connectivity for "standard" client devices, those computers running Windows XP/SP2 and utilizing WPA-ready NICs.

There are two scenarios in which you create additional WLANs, in addition to the internal WLAN: (1) 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.) Or, (2) to configure a specific WLAN with different security settings. For example, you may need a WLAN that utilizes WEP encryption for wireless handheld devices that only support WEP-key encryption.

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 internal WLAN, plus the needed WLANs that fulfill different wireless security requirements.

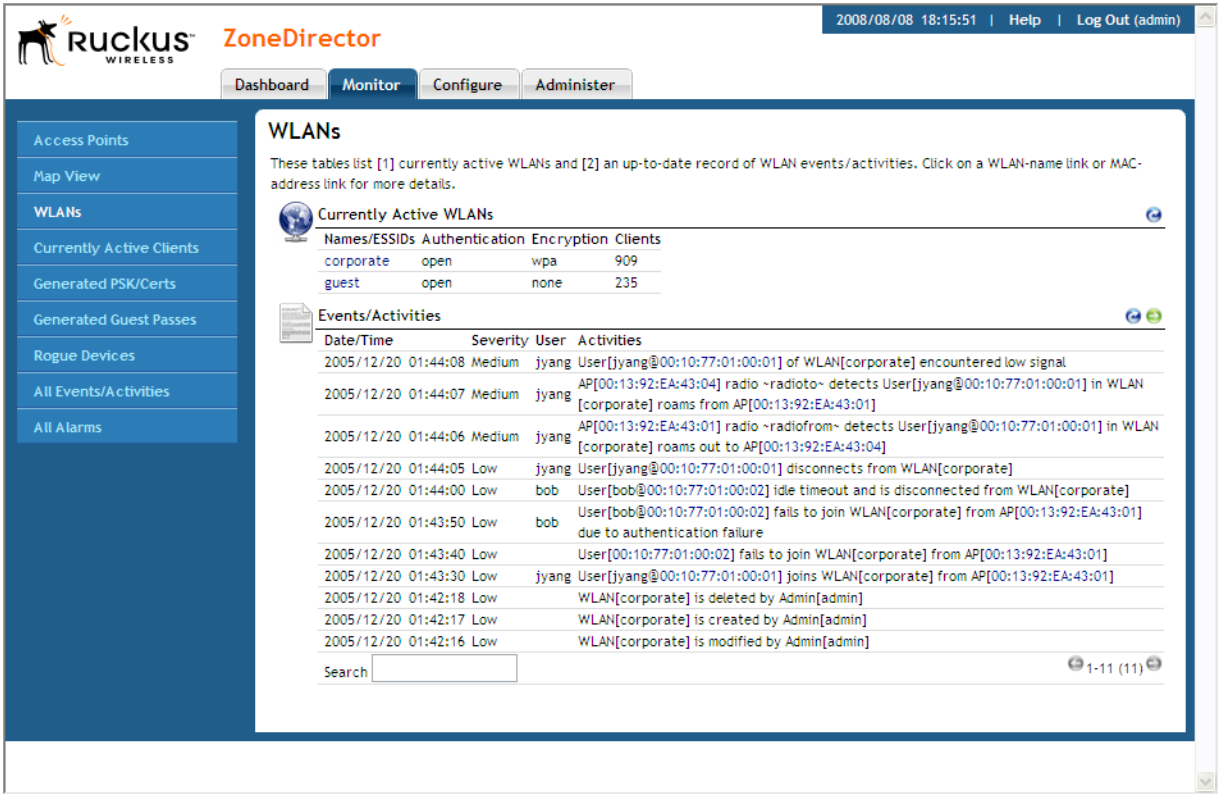
Customizing WLAN Security

The default security environment for your internal WLAN incorporates a WPA-based authentication passphrase and the TKIP encryption algorithm, and utilizes a dynamic pre-shared key. To review the default WLAN configurations and the available options, review the following procedures.

Reviewing the Initial Security Configuration

1. Go to **Monitor** > **WLANs**.
2. When the *WLANs* workspace appears, a *WLANs* table lists the two default WLANs created in the setup process: *corporate* and *guest*. The internal WLAN, *corporate*, is the one used by your authorized users, and you can review the details of its configuration by clicking the WLAN name. See Step Figure 34. on page 57.
3. You have three options with the internal WLAN: [1] continue using the current configuration, [2] fine-tune the existing WPA-based mode, or [3] replace this mode entirely with either a WEP-based mode or an 802.1x mode. The two WLAN-editing processes are described separately, in the following sections.

Figure 34. The Monitor > WLANs page



Fine-tuning the Current Security Mode

1. In the internal WLAN (*corporate*) row, click **Edit** (if you have not done so).
2. You can choose from the following options, which will enhance the default "zero IT" protection without disrupting the user's connections.
   - *WPA2*: Switch to this encryption method if you prefer the IEEE 802.11i standard.
   - *AES*: Switch to this algorithm for stronger encryption.
   - *Passphrase*: Replace the current passphrase with a new one.
3. Click **OK** to apply any changes.

Switching to a Different Security Mode

You also have the option of replacing the default internal WLANs' WPA mode with one of two other modes:

- The less-secure protection of a WEP key mode
- The more-secure protection of an 802.1x mode

Replacing your WPA configuration with 802.1x requires the users to make changes to their Ruckus wireless connection configuration—including the importation of certificates.

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 row.
3. When the *Editing (corporate)* features 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, 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 encryptions, but you do not need to create a key or passphrase.
   - **MAC Address** allows you to use an external RADIUS server to authenticate wireless clients. 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.
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. (For example, if you switch to 802.1x, you'll need to choose an authentication server from the menu.)
7. When you finish, click **OK** to apply your changes.

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. Once it is done, users can connect to the internal WLAN using 802.1x/EAP authentication.

Authenticating with an External RADIUS Server

You could 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.

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 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 could 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-Windows XP/SP2 client usage, use the wireless settings generated by ZoneDirector.

Setting Dynamic Pre-Shared Key Expiration

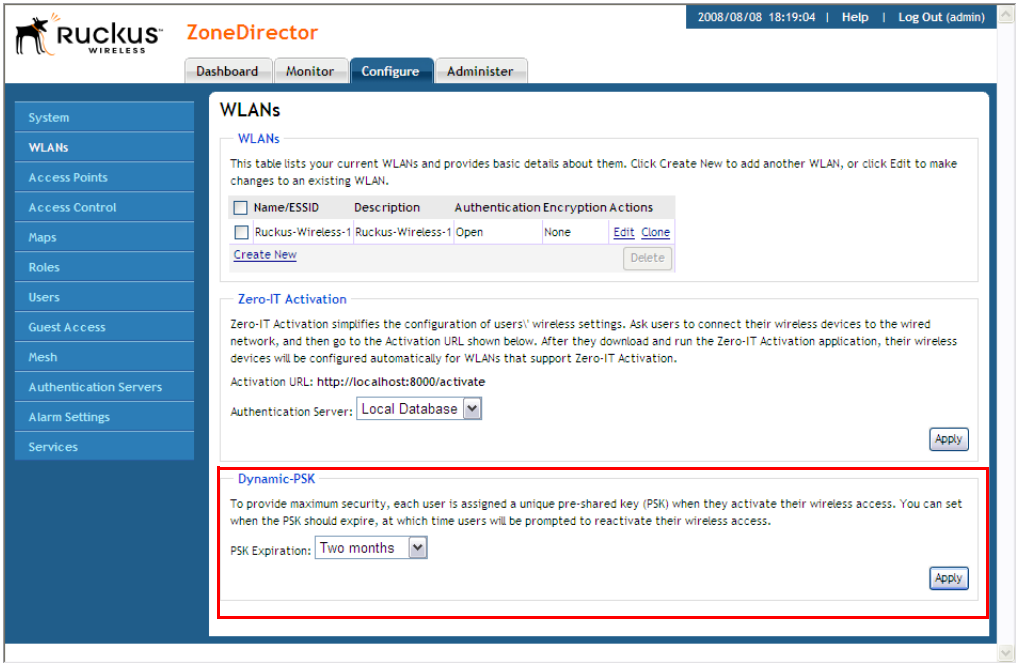
When network users first activate their access to the WLAN with Dynamic PSK enabled, a unique pre-shared key (PSK) is generated automatically for their authentication. (This was activated by default in the WLAN Setup Wizard.)

By default, all dynamic pre-shared keys expire in two months. You can control when the PSK expires, at which time the users will be prompted to re-activate their wireless access.

To set the dynamic PSK expiration

1. Go to **Configure** > **WLANs**.
2. In **PSK Expiration** under *Dynamic PSK*, select when you want the dynamic PSK to expire. Options range from **One day** to **Unlimited**.
3. Click **Apply** to save your settings. The new settings go into effect immediately.

Figure 35. The Dynamic PSK option



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.

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 ACL. The entries of the system-wide block list are added when Admin chooses to block clients from the Monitor/Current 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 other ACL list.

L2/MAC Access Control

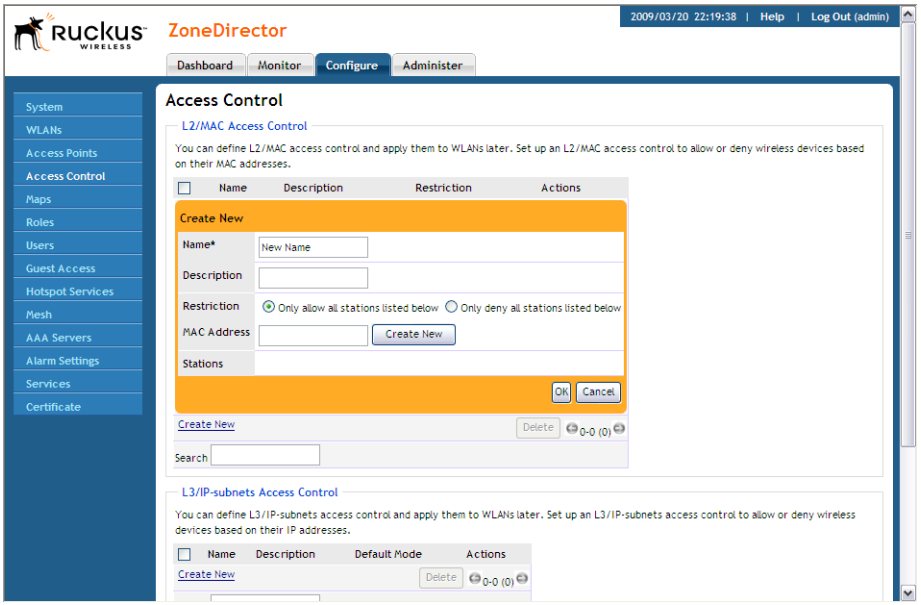
Using the Access Controls configuration options, you define Layer 2/MAC address ACLs, which can then be applied to one or more WLANs (upon WLAN creation or edit). ACLs are either allow-only or deny-only; that is, an ACL can be set up to allow only specified clients or to deny only specified clients. 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.
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 36. Configuring an L2/MAC access control list



L3/L4 Access Control

In addition to L2/MAC based ACL, ZoneDirector also provides access control option 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

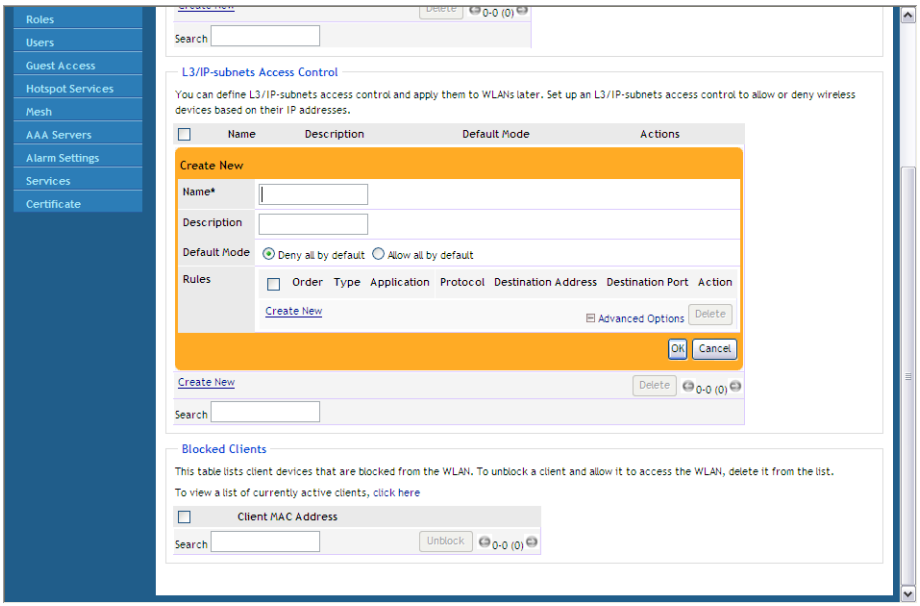
To create an L3/L4/IP address based ACL

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 editing an editing 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*: If you have a specific IP address, host name or URL to which you want to allow or deny access, type it here. 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, click **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. Repeat these steps to create up to 32 L3/L4/IP address based access rules.
9. Click **OK** to save the ACL.

Figure 37. Configuring L3/L4 access control list



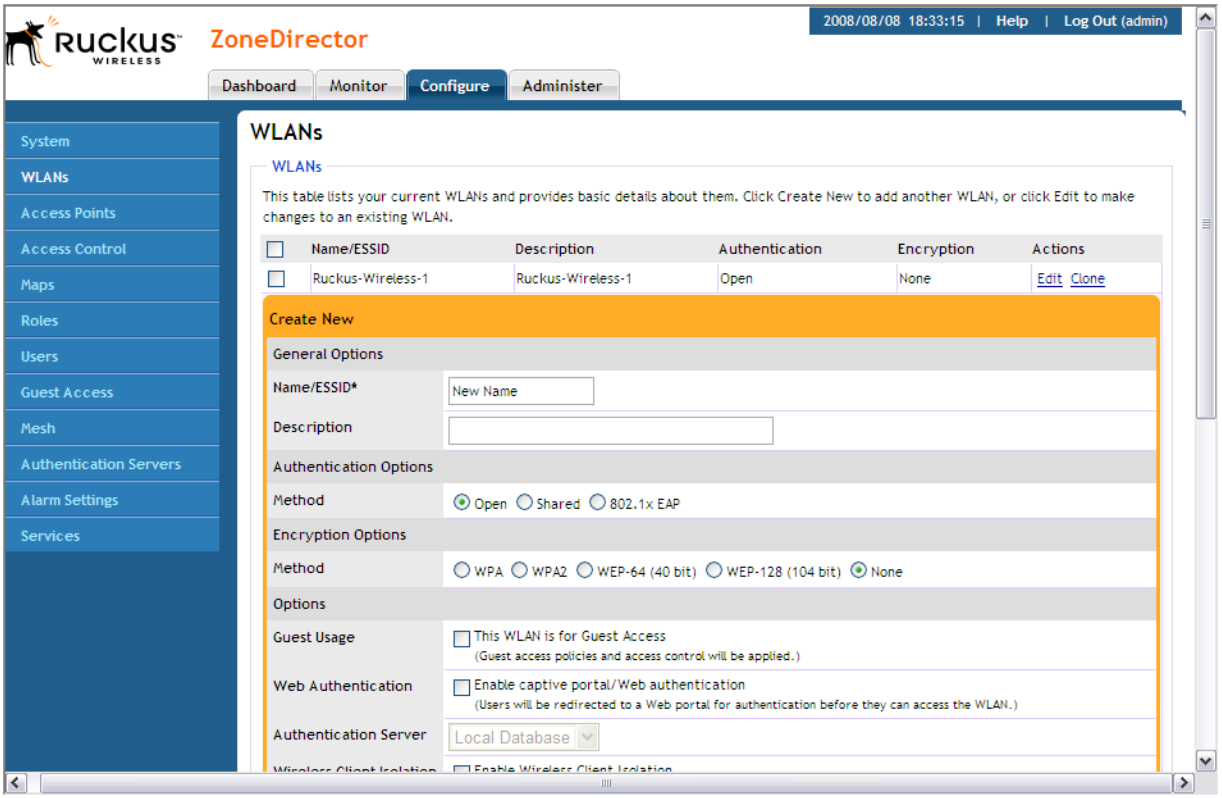
Working with WLANs

There are cases in which you might want to create additional WLANs. For example, you might want to create a WLAN for WEP-only client devices. Or you might want to create a WLAN that utilizes 802.1x/EAP and certificates. This section describes how to create such WLANs that utilize different security settings.

Creating a WLAN

1. Go to **Configure** > **WLAN**.
2. Click **Create New**.

Figure 38. The Create New form for adding a WLAN



The *Create New* workspace displays the following:

General Options

- *Name/ESSID*: Type a short name (2–31 characters/numbers) for this WLAN.
- *Description*: Enter a brief description of the qualifications/purpose for this WLAN, e.g., "Engineering" or "Voice".

Authentication Method Options

- *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. Uses a shared WEP key for authentication. Requires creation of a WEP key, as detailed below.
- *802.1x EAP*: Uses 802.1x authentication mechanism. Requires use of certificates.
- *MAC Address*: Uses the devices MAC address for both the user name and password.

Encryption Options

Method

- *None*: [Default] No encryption is applied; communications are in clear text.
- *WPA / WPA2*: (Not available to Shared authentication) Provides a higher level of encryption and is more secure. WPA and WPA2 require selection of an encryption algorithm (as detailed below).
- *WEP-64*: Provides a lower level of encryption, and is less secure, using 64-bit WEP encryption.
- *WEP-128*: Provides a higher level of encryption, using a 128-bit key for WEP encryption.

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 AP will operate in 802.11g mode.

Algorithm (Only for WPA or WPA2 encryption methods)

- *TKIP*: [Default] This algorithm is effective. It is set as the default since some client devices do not support AES.
- *AES*: This algorithm provides a high degree of security.

CAUTION! If you set the encryption algorithm to TKIP and you are using an 802.11n AP for the WLAN, the AP 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 25 clients. When this limit is reached, additional clients will be unable to associate with the AP. On the other hand, if you disable encryption or select AES, the AP will be able to support up to 100 clients. If the wireless mesh network is also enabled, the AP will be able to support less than 100 clients.

- *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/WPA2 PSK methods only. Click in this field and type the text of the passphrase used for authentication.

Options

- *Guest Usage*: If the WLAN being created is for guest access, select the This WLAN is for Guest Access check box. When selected, the Wireless Client Isolation option is automatically selected and cannot be unchecked.

  Guest WLANs are subject to guest access policies, such as redirection and subnet access restriction.

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 the Wireless Network Throughput with SpeedFlex" on page 150.

- *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.
- *Authentication Server*: When "Web Authentication" is active, use this option to designate the server used to authenticate Web-based user login. When "802.1x" authentication is active, use this option to designate either "Local Database" or a configured RADIUS server as the authentication source.
- *Wireless Client Isolation*: Wireless client isolation enables subnet restrictions for guests. When wireless client isolation is enabled for a WLAN, any stations associated to this WLAN will not be able to access the local LAN; rather, they can only access the Internet. Also, stations associated to this WLAN cannot communicate with each other, regardless of which APs they are associated to. The behavior of stations will be exactly as the stations that associate to a guest WLAN. 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. Same guest policy will be applied to guest WLAN as well as WLANs with wireless client isolation enabled.

- *Zero IT Activation*: Leave this option active (default setting), as it activates the Ruckus Wireless ZoneDirector's share in the automatic "new user" process, in which the new user's PC is efficiently (and speedily) configured for WLAN use.

CAUTION! For Zero IT Configuration to work on HP iPAQ, Internet Explorer Mobile 7.6 (or later) must be installed. If your HP iPAQ users are using earlier versions of Internet Explorer Mobile, Ruckus Wireless strongly recommends that they upgrade to the latest version before connecting to your wireless network.

Advanced Options

See Step 3. on page 68.

- 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**.

  Note that this option is only available if:
  - Authentication Option is set to 802.1x EAP.
  - Authentication Option is set to Open or Shared, and Web Authentication is enabled.
- 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. See "Configuring Access Control Lists" on page 61.
- 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.
- VLAN: Select the Attach VLAN Tag check box to activate the VLAN function, and then type the relevant VLAN ID assigned to users/clients of your wireless network. (The ID should be a number between 1 and 4094).
- Hide SSID: Activate this option if you do not want the ID of this WLAN advertised at any time. This will not affect the 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 and PDAs), Ruckus Wireless recommends enabling tunnel mode.

NOTE: The tunnel mode feature requires an additional license. You need to upload the required license file for the tunnel mode feature to work. For more information, see "Upgrading the License" on page 146.

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 102.

Configuring Client Authentication

If your users are connecting with computers running Windows XP SP2/Vista, an automatic activation script is generated for them to install security settings of WLANs configured on the Ruckus ZoneDirector. If your users are connecting with computers running early versions of Windows, Mac OS X, 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 on their computers based on these settings. The following grid records the details.

Table 6.

Authentication Options	Encryption Options	Client Configurables
Open	WPA WPA-2 WEP-64 WEP-128	User must (1) manually enter the text of the same WEP key in their wireless network configuration, or (2) must manually enter the WPA passphrase.
Shared	WEP-64 WEP-128	User must manually enter the text of the same WEP key stored in the Ruckus ZoneDirector in their wireless network configuration.
802.1x	WEP-64 WEP-128 WPA/WPA2	User must obtain and install certificates generated on their computers. No key or passphrase is required.

Creating a New WLAN for Workgroup Use

If you want to create an additional WLAN based on your existing internal 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 (who ideally are using client devices running Windows XP/SP2).
2. Go to **Monitor** > **WLANs**.

   When the *WLANs* page appears, the default *corporate* 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 *corporate* WLAN record and click **Clone**.

   A workspace appears, displaying the default settings of a new WLAN, using the same zero-IT configuration settings as "Corporate".
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 "corporate" users, you can do so as detailed in "Creating New User Roles" on page 102.

Adding New Access Points to the WLAN

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 approvals before becoming active.

The "Auto-JOIN" automatic AP activation process is active by default. If you prefer, you can disable Auto-JOIN. 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.

NOTE: For Auto-JOIN to work, the APs that you are adding must be on the same IP subnet or VLAN as ZoneDirector.

Connecting the APs to the WLAN

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.
4. Connect each AP to a power source.

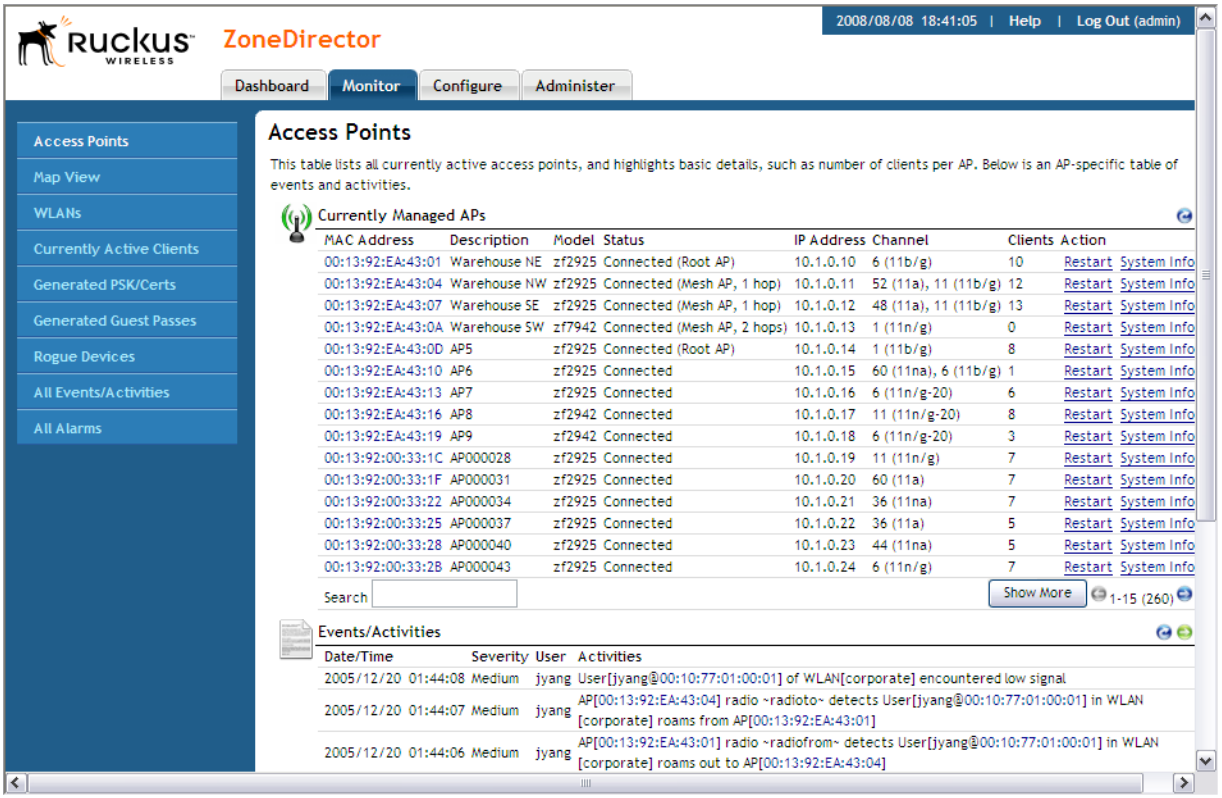
NOTE: If the Ruckus Wireless APs that you are using are POE-capable and power sources are not convenient, they will draw power through the Ethernet cabling if connected to a POE-ready hub or switch.

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 page 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 39.
   - 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 Auto-JOIN 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.
4. Click **Apply** to save your settings.

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 96 for more information.

Figure 39. The Monitor > Access Points page



Reviewing Current Access Point Policies

The Access Point Policy options include how new APs are detected and approved for use in WLAN coverage. To review and revise the general AP policy, 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 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 ZoneDirector units on the network and want specific APs to join specific ZoneDirector units, you can limit ZoneDirector discovery. To do this, select the **Limited ZD Discovery** check box, and then enter the IP addresses 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.

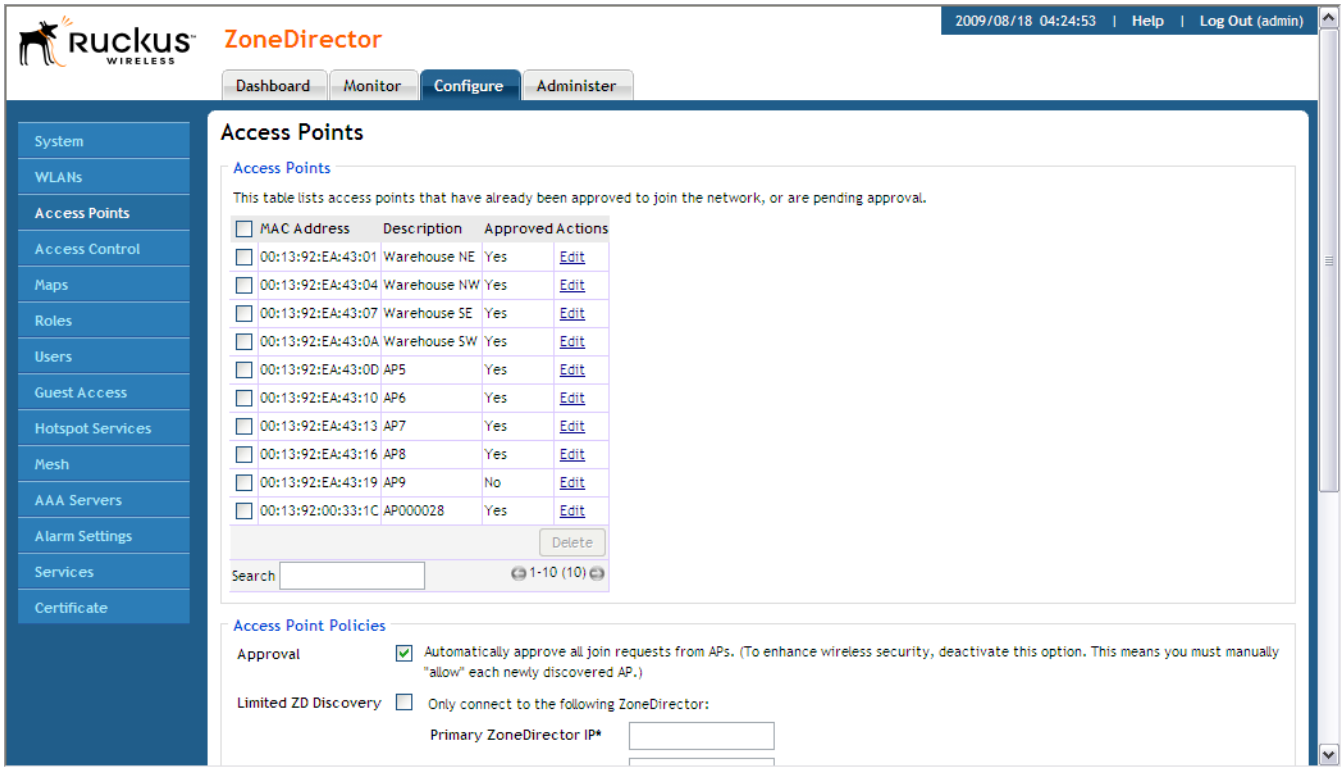
- **Management VLAN**: You can enable the ZoneDirector management VLAN if you want to separate management traffic from regular network traffic. The following options are available:
  - **Keep AP's setting**: Click this option if you want to preserve the Management VLAN settings that has been configured on the AP. Note that Management VLAN on the AP is disabled by default.
  - **Disable**: Click this option if you want to disable the Management VLAN. If the Management VLAN is enabled on the AP, it will be disabled the next time the AP is provisioned by ZoneDirector.
  - **Enable with VLAN ID**: If you want to enable the Management VLAN on all APs managed by this ZoneDirector, click this option, and then type the management VLAN ID (must be configured on the switch/router).

NOTE: If you click Enable with VLAN ID, 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 communicated via the Management VLAN.

- **Max Clients**: If you want to guarantee wireless connections to all clients, you can limit the number of wireless clients that each AP will manage. In the Max Clients box, type the maximum number of clients per AP (default is 100).

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

Figure 40. The Configure > Access Points page



Editing Access Point Parameters

You can add a description, or change the channelization, channel, or transmit power settings of a managed access point by editing the APs parameters.

To edit the parameters of an access point

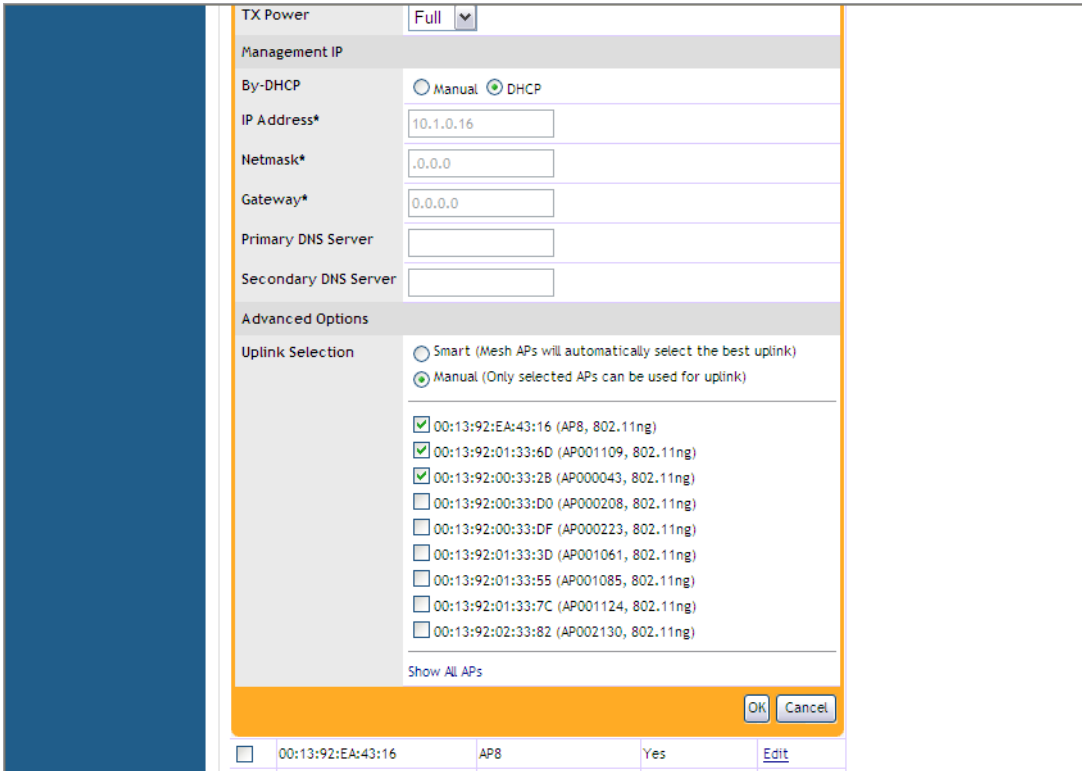
1. Go to **Configure** > **Access Points**.
2. Find the AP to edit in the *Access Points* table, and then click **Edit** under the *Action* column.
3. Edit any of the following:
   - **Description**: Enter a description for the AP, such as the location.
   - **Channelization**: (For 802.11n only) The "channel width" determines the manner in which the spectrum is used during transmission.
   - **Channel**: This is the channel used by the APs network.
   - **TX Power**: Specifies the maximum transmit power level relative to the calibrated power.

4. If the AP is currently connected to ZoneDirector, the Management IP options appear. Use these options to configure the IP settings of the AP.
   - 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 **By-DHCP**. 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 in **By-DHCP**, and then set the values for the following options:
     – IP Address
     – Netmask
     – Gateway
     – Primary DNS Server
     – Secondary DNS Server
5. Under **Advanced Options** > **Uplink Selection**, select the **Manual** radio button. The other APs in the mesh appear below the selection.
6. 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*.

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

Figure 41.



Deploying ZoneDirector WLANs in a VLAN Environment

You can set up a ZoneDirector wireless LAN as an extension of a VLAN network environment, but certain qualifications must be met due to the fact that management traffic between ZoneDirector and the APs is not VLAN-tagged. The WLAN-in-VLAN 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.

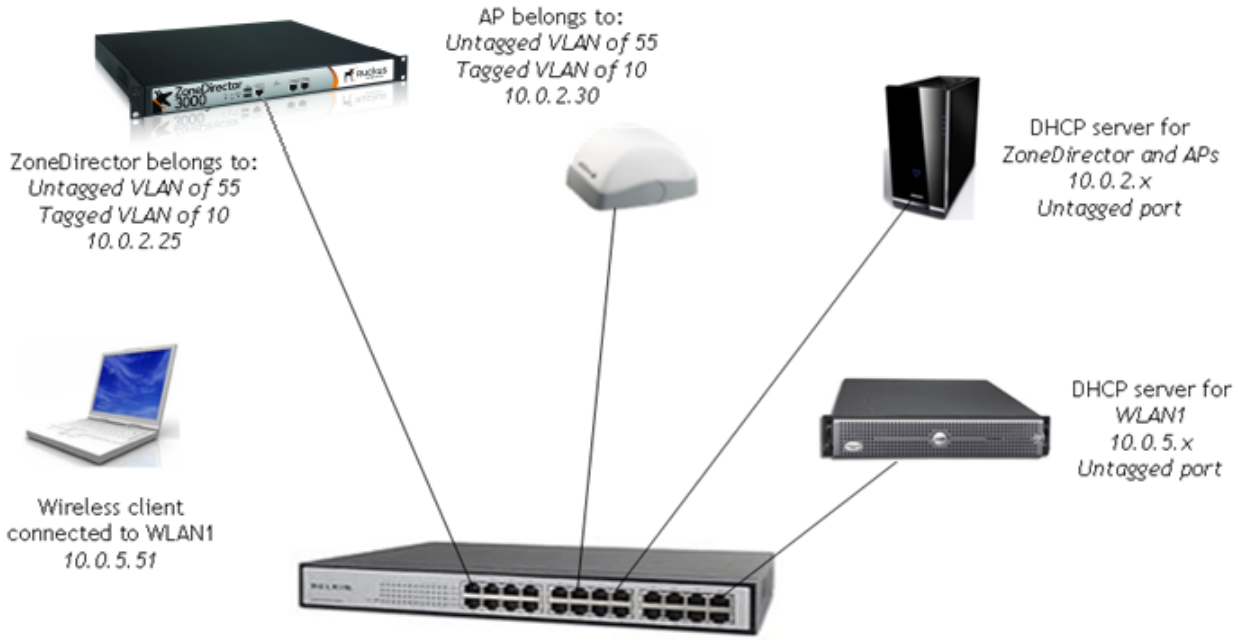
  For example, if an 802.1Q port has VLANs 2, 3, and 4 assigned to it with VLAN 2 being the Native VLAN, frames on VLAN 2 that egress (exit) the port are not given an 802.1Q header (i.e., they are plain Ethernet frames). Frames which ingress (enter) this port and have no 802.1Q header are put into VLAN 2. Behavior of traffic relating to VLANs 3 and 4 is intuitive.

- Connecting ZoneDirector and any Access Points (APs) to VLAN trunk ports in the VLAN switch
- Verifying that those trunk ports are on the same native VLAN

NOTE: All DNS, DHCP, ARP, and HTTP traffic from an unauthenticated wireless client will be passed onto ZoneDirector from the AP via the management VLAN. If the client belongs to a particular VLAN, ZoneDirector will add the corresponding VLAN tag before passing traffic to the corresponding wired network. After client authentication is performed, client traffic will directly go to the wired network from the AP, which will add the corresponding VLAN tag. This explains why it is necessary to configure tagged VLANs for all VLAN switch ports connecting to ZoneDirector and APs.

Example configuration (Figure 42): VLAN ID 55 is used for management, and wlan1 is tagged with VLAN ID 10.

Figure 42. Sample VLAN configuration



Working with WLAN Groups

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 be assigned to only one radio on an AP and it can have up to eight member WLANs. If mesh networking is also enabled, the WLAN group can only have up to six member WLANs.

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 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 **Member WLANs**, select the check boxes for the WLANs that you want to be part of this WLAN group.

6. If you have existing VLANs on the network and you need to tag the traffic from the member WLANs, select the Enable VLAN override check box, and then configure the VLAN override settings for each member WLAN. Available options include:
   - *No Change*: Click this option if you want the WLAN will keep the same VLAN tag (if you configured the "Attach VLAN Tag" option when you created the WLAN service).
   - *Untag*: Click this option if a particular WLAN is connected to a local network that does not have any VLANs.
   - *Tag*: Click this option if traffic from a particular WLAN needs to be tagged to bind with a VLAN successfully.

NOTE: WLANs that are in tunnel mode cannot be tagged.

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.

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**, select the WLAN group to which you want to assign the AP. You can only assign an AP to a single WLAN group.
4. Click **OK** to save your changes.

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.

Editing a WLAN Group

You can change the settings of an existing WLAN group at anytime.

1. Go to **Configure** > **WLANs**.
2. In the WLAN Group section, click the **Edit** link that is on the same row as the WLAN group that you want to edit. The Editing (WLAN_group_name) form appears.
3. Edit the setting as needed. You can edit the Name, Description, Member WLANs, and VLAN override settings.
4. Click **OK** to save your changes.

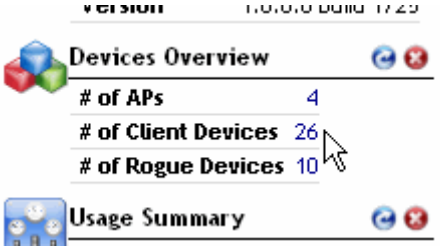
Blocking Client Devices

When users log into a ZoneDirector network, their client devices (for example, laptop computers and PCs) 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 Client Devices.

Figure 43. The Device Overview widget



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. When the *Currently Active Clients* page under the **Monitor** tab appears, review the *Clients* table.

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.

NOTE: The user can reconnect at any time, which, if this proves to be a problem, may prompt you to consider the following client option.

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 (and its user) from using your Ruckus Wireless WLAN.

Reviewing a List of Previously Blocked Clients

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

Optimizing Access Point Performance

ZoneDirector, through its Web interface, enables 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, as needed.

Assessing Current Performance by 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 86 and "Placing the Access Point Markers" on page 87.

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 88.)
2. In the *Coverage* options, click **Yes**.
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 down the new locations of relocated AP markers.
3. After physically relocating the actual APs in conformance to the Map View placements, disconnect and 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 155.
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 by Using the Access Point Table

1. Go to **Monitor** > **Access Points**.
2. When the *Access Points* page appears, review the *Currently Active APs* for specific AP settings, especially the *Channel* and *Clients* columns.
3. 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.

- *MAC Address*: This information is taken from the AP. It cannot be modified in ZoneDirector.
- *Description*: Enter a short description of this device and its current location.
- *Radio B/G Channel*: Choose a specific channel for use by 802.11b/g devices from this drop-down list.
- *TX Power*: Choose the amount of power allocated to this channel. The default setting is "Auto" and your options range from "Full" to "Min".

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

Working with Hotspot Services

A hotspot is a venue or area that provides wireless Internet access to devices with wireless networking capability, such laptops, PDAs, and other portable devices. Hotspots are usually available in public venues such as hotels, airports, restaurants, and shopping malls.

ZoneDirector has a built-in hotspot feature that you can enable and configure to provide hotspot service 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.

- *RADIUS Server*: A Remote Authentication Dial-In User Service (RADIUS) 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.

Creating a Hotspot Service

Create a hotspot service configuration that you can deploy to WLANs that you want provide hotspot service. After completing the steps below, you will need to set the WLANs that you want to provide hotspot service.

To create a hotspot service

1. Go to **Configure** > **Hotspot Services**.
2. Click **Create New**. The Create New form appears.
3. In **Login Page** (under Redirection), type the URL of the captive portal (the page where hotspot users can log in to access the service).
4. Configure optional settings as preferred:
   - In **Start Page**, configure where users will be redirected after logging in successfully. 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 Web site).
   - In **Session Timeout**, select the check box, and then set a maximum session time (in minutes) after which sessions will be restarted automatically.
   - In **Idle Timeout**, select the check box, and then set a maximum idle time (in minutes) after which idle users will be logged out automatically.
   - In **Authentication Server**, select the AAA server that you want to use to authenticate users.
   - In **Accounting Server** (if you have an accounting server setup), configure the frequency (in minutes) at which accounting data will be retrieved.
   - In **Walled Garden**, type network destinations (URL or IP address) that users can access without going through authentication.
   - In **Restricted Subnet**, type the subnets to which hotspot users will be prevented from accessing.
5. Click **OK**.

The page refreshes and the hotspot service you created appears in the list. You may now assign the WLANs that you want to provide hotspot service.

Assigning a WLAN to Provide Hotspot Service

After you create a hotspot service configuration, 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 **Available Hotspot Services**, select the name of the hotspot service that you created previously.
5. Click **OK** to save your changes.

4

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 surveys 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.
- Monitor: The Map View provides a fast scan of key network factors: APs (legitimate, neighboring and rogue), client devices, and radio frequency (RF) coverage. You can see what devices are where in your floorplan, and visually evaluate network coverage.

  Other Monitor tab options incorporated in the left column's buttons provide numeric data on WLAN performance and individual device activity. As with Dashboard, some data entries are links that take you to more detailed information. And, finally, the All Events 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.

You can import an unlimited number of floor maps to ZoneDirector. However, the total file size of all imported floor maps is limited to 2MB on ZoneDirector 1000 and 10MB on ZoneDirector 3000. An error message appears when these file size limits are reached.

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.

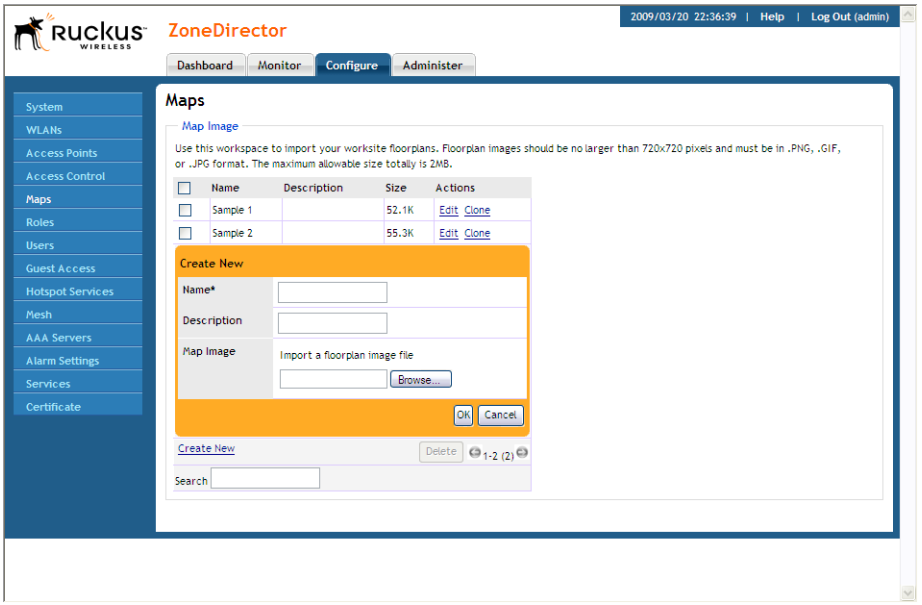
Importing the Floorplan Image

1. Go to **Configure** > **Maps**. The Maps page appears.
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 *Current 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 44. The Create New form for importing a floorplan image



Placing the Access Point Markers

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

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

1. Have the list of APs handy, with MAC addresses and locations.
2. Go to **Monitor** > **Map View** (if it is not already in view).

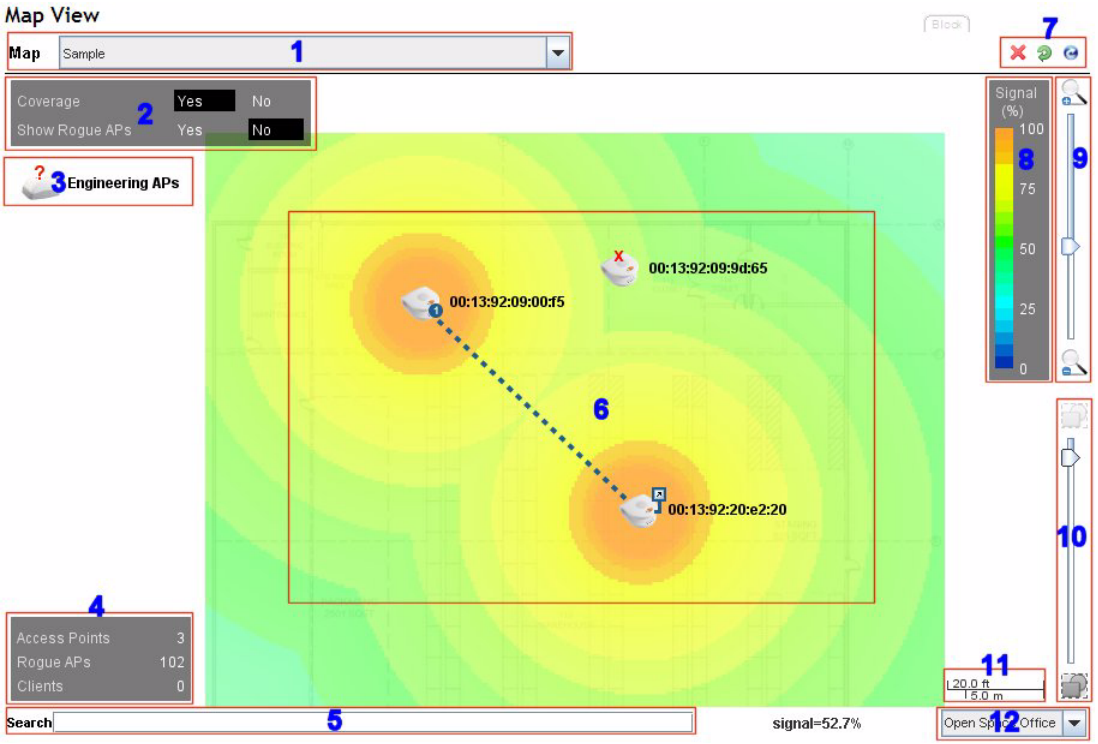
3. Look in the upper left corner for AP marker icons. There should be one for each AP, with a tiny red question mark at the top.
4. Look at the MAC address notation under the marker icon, to identify a marker.
5. Drag each marker icon from the upper left corner into its correct location on the floorplan.

When you finish, you can make immediate use of the Map View to optimize your wireless coverage, as detailed in "Optimizing Access Point Performance" on page 81.

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 45. 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 Yes enables a signal strength view of your placed APs. This 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 WLAN" on page 69), 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 90.
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 "Yes" for Coverage (see #2 above). See "Evaluating and Optimizing Network Coverage" on page 96 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. The scale works best when the floorplan view has not been zoomed in or out. The scale offers both feet and meters

as units of measure. Use a physical object as a reference to the scale in order to judge distances on your floorplan. For example, cut a piece of paper to the length of the scale, and then use that piece of paper on the floorplan to measure off distance increments.

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:

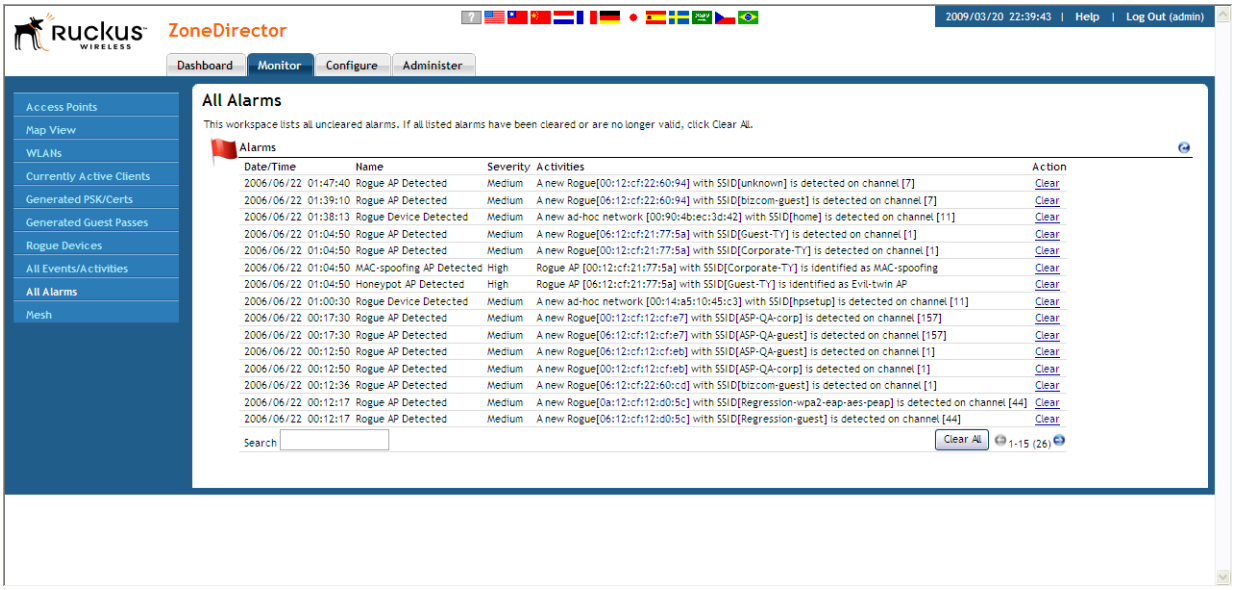
	A normal AP marker displays this devices' Ethernet MAC address below the icon. Above the icon is the "Users" count that shows the number of currently active client connections through this AP.
	An unplaced AP marker displays a "?" (question mark) above the icon.
	A rogue AP displays a smaller red icon imprinted with a "bug".
	An isolated AP displays a red "X" above the icon.
	When the wireless mesh network 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 the wireless mesh network 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 the wireless mesh network is enabled, a gray square (dimmed) with an arrow indicates that it is a Root AP without any active downlinks.

Reviewing Current Alarms

If an alarm condition is detected, ZoneDirector will record it in the events log, which, 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 46. The All Alarms page



3. Review the contents of this table. The *Activities* column is especially informative.
4. If a listed alarm condition has been resolved, click the now-active **Clear** link to the right. You also have the option of clicking **Clear All** to resolve all alarms at one time.

Reviewing Recent Network Events

You have two options for reviewing events in your network: [1] open a complete list of all events, or [2] look at specific lists of events in each Monitor tab workspace, such as the WLANs workspace "Events/Activities" table.

1. Open the ZoneDirector Dashboard and look at the *Most Recent User Activities* table and *Most Recent System Activities* table for summaries of activity in the network.
2. Go to the **Monitor** tab.

3. Click any of the specific options, such as WLANs, Access Points, or Currently Active Clients.
4. Look for an *All Events* table that specifically focuses on the selected WLAN 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.

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. The *Activities* column is especially informative.
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 users of the network on a per-client-device 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.

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

Monitoring Access Point Status

There are several ZoneDirector features you can take advantage of, to monitor the performance and status of your Ruckus wireless APs:

1. Open the Dashboard for a snapshot view of the most active APs. Click the MAC address link of any AP record to see more details.
2. Go to **Monitor** > **Map View** and click a radio frequency to see a heat-map rendering of the current RF coverage.
3. 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.
4. Click the **System Info** link to retrieve the support.txt file from an AP.

Detecting Rogue Access Points

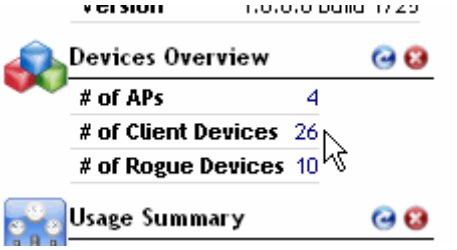
As contrasted with "neighboring" access points (APs) that are parts of a neighboring WLAN, "rogue" (unauthorized) APs pose problems for a wireless network. Usually, a rogue AP appears in the following way: an employee obtains another manufacturer's AP and connects it to the LAN, to gain wireless access 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. Click the Dashboard tab (or go to **Monitor** > **Rogue Devices**).
2. Look under *Devices Overview* for "# of Rogue Devices".

Figure 47. Rogue devices indicator



3. If there is at least once rogue device detected, click the number for more details.
4. When the **Monitor** > **Rogue Devices** page appears, two tables are listed:
   - The *Currently Active Rogue Devices* table
   - The *Known/Recognized Rogue Devices* table.
5. Review the *Currently Active Rogue Devices* table. The types of Rogue APs recognized by Zone Director are (an alarm is generated if ZoneDirector detects one of these rogue APs):
   - AP: An access point unknown to ZoneDirector.
   - AP (SSID-spoof): A rogue AP that uses the same SSID as ZoneDirector's AP, also known as *Evil-twin AP.*
   - AP (MAC-spoof): A rogue AP that has the same BSSID (MAC) of one of the virtual APs managed by ZoneDirector.

   The *Encryption* column indicates if a rogue device is encrypted or is open.

6. 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.
7. 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.
8. 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.
9. Open the Map View, and look for rogue APs icon  . 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 in 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 Ruckus Wireless 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".

Detecting Rogue DHCP Servers

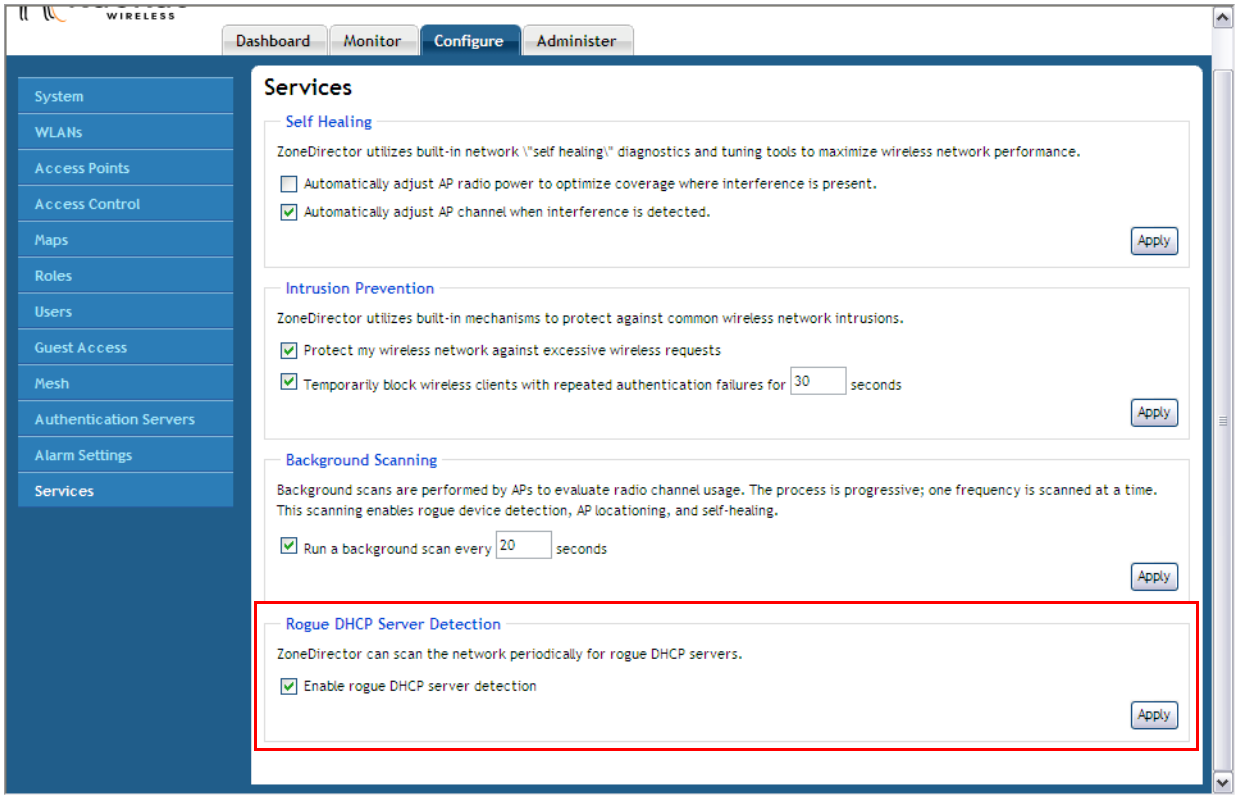
A rogue DHCP server is a DHCP server that is not under the control of network administrators and is therefore unauthorized. When a rogue DHCP server is introduced to the network, it could start assigning invalid IP addresses, disrupting network connections or preventing client devices from accessing 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 caused 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.

Figure 48. The Rogue DHCP Server Detection option



To enable rogue DHCP server detection on ZoneDirector

1. Go to **Configure** > **Services**.
2. Under Rogue DHCP Server Detection, select the **Enable rogue DHCP server detection** check box.
3. Click **Apply**.

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 server. 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
```

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. Remember that a Ruckus AP can cover an area with a radius of 30 to 50 feet using average broadcasting power settings on any frequency. Local structural obstructions may limit 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 86 for information on setting up the Map View.)
3. For the *Coverage* option, click **Yes**.
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. To turn off the heat map and restore the floorplan to view, click **No** (in the *Coverage* options).
3. Note down the new physical locations of relocated AP markers.
4. After physically relocating the actual APs in accordance with Map View repositioning, disconnect and 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.

Customizing Background Radio Frequency Scans

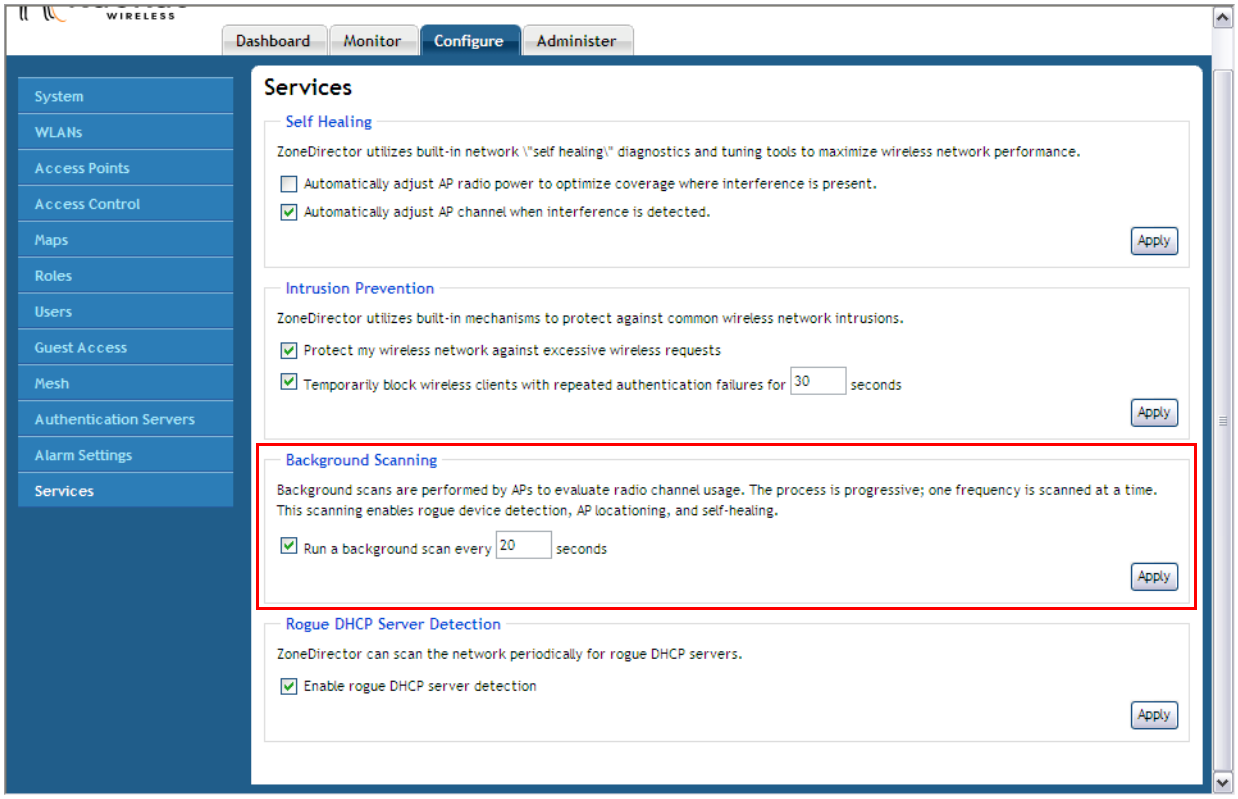
As a key element of your network monitoring, the Ruckus ZoneDirector regularly samples the activity in all Access Points to assess radio frequency (RF) usage. The scans sample one channel at a time in each AP, and do not interfere with network use. This information is then applied in Map View and other ZoneDirector monitoring features.

1. Go to **Configure** > **Services**.
2. Select the **Run background scan every** check box, and type the interval (in seconds, default is 20) that you want to set between each scan.

   You can disable this feature by clearing the check box, which results 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 **Apply** to save your settings.

Figure 49. The Background Scanning options



5

Managing User and Guest Access

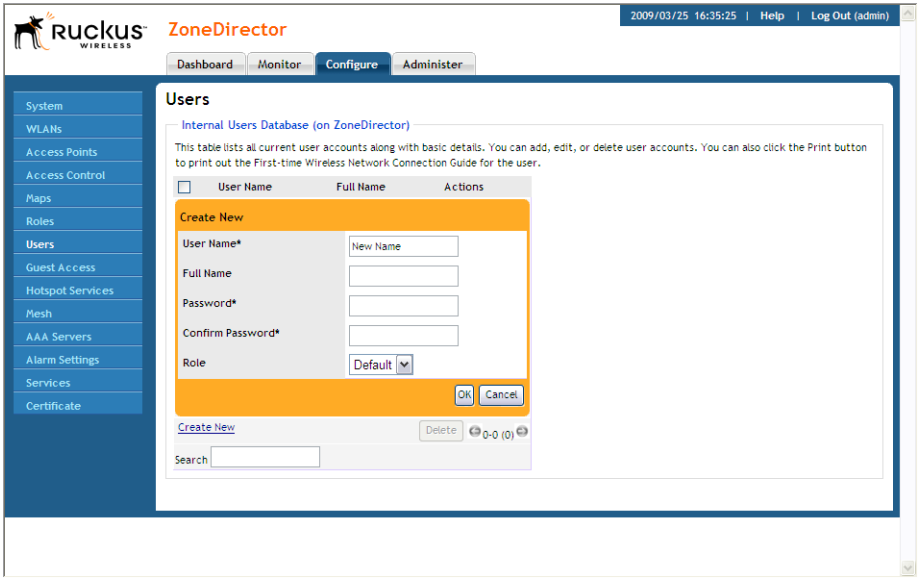
In This Chapter

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 server or RADIUS server, or to authenticate users by referring to accounts that are stored in ZoneDirector's internal user database. To use the internal user database as the default authentication source and to create new user accounts in the database, follow the steps:

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.
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 102.
5. Click **OK** to save your settings. Be sure to communicate the user name and password to the appropriate end user.

Figure 50. The Create New form for adding users to the internal database



Managing Current User Accounts

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

Changing an Existing User Account

1. Go to **Configure** > **Users**.
2. When the *Users* features appear, locate the specific user account in the *Internal User Database* panel, and then click **Edit**.
3. When the *Editing [user name]* form appears, make the needed changes.
4. If a role must be replaced, open that menu and choose a new role for this user. [For more information, see "Creating New User Roles" on page 102.]
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 Authentication* features appear, review the "Internal Users 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 users database.

Creating New User Roles

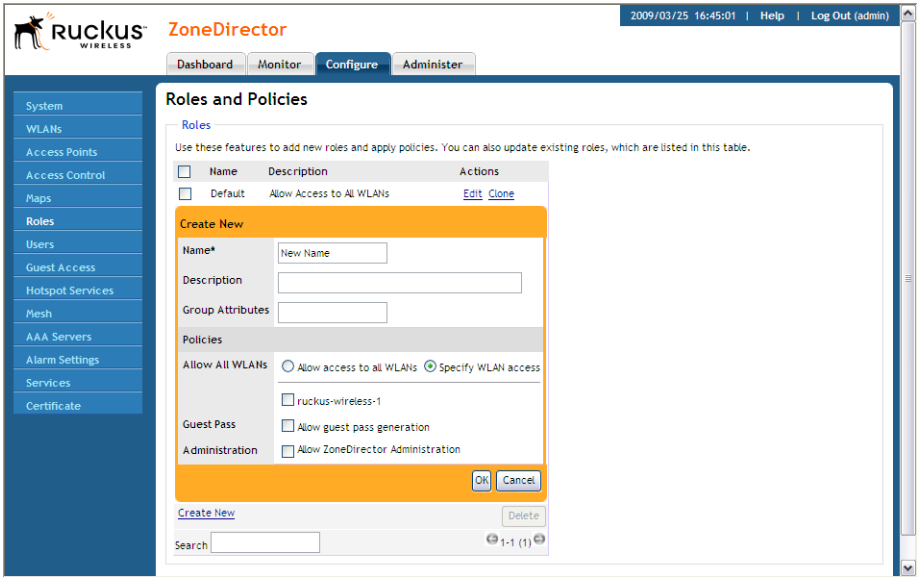
ZoneDirector provides a "Default" role that is automatically applied to all new user accounts. This role links all users to the internal WLAN and permits any user to obtain guest passes for on-site visitor use. As an alternative, you can create additional roles that you can assign to selected wireless 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.)

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 with administrator privileges and you are using Active Directory as the authentication server.* Enter the **Active Directory User Group** name here. Active Directory users with the same group attributes are automatically mapped to this user role.

NOTE: For information on how to authenticate administrators using an external authenticate server, refer to "Using an External Server for Administrator Authentication" on page 138.

   - **Allow All WLANs**: You have two options: (1) **Allow Access to all WLAN**s, 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 New WLAN for Workgroup Use" on page 69.
   - **Guest Pass**: If you want users with this role to have the permission to generate guest passes, enable this option.
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 51. The Create New form for adding a role



Managing 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-pass use of the network. There are options you can fine-tune to fit your work environment.

This section describes how to configure guest access and guest pass generation. Topics include:

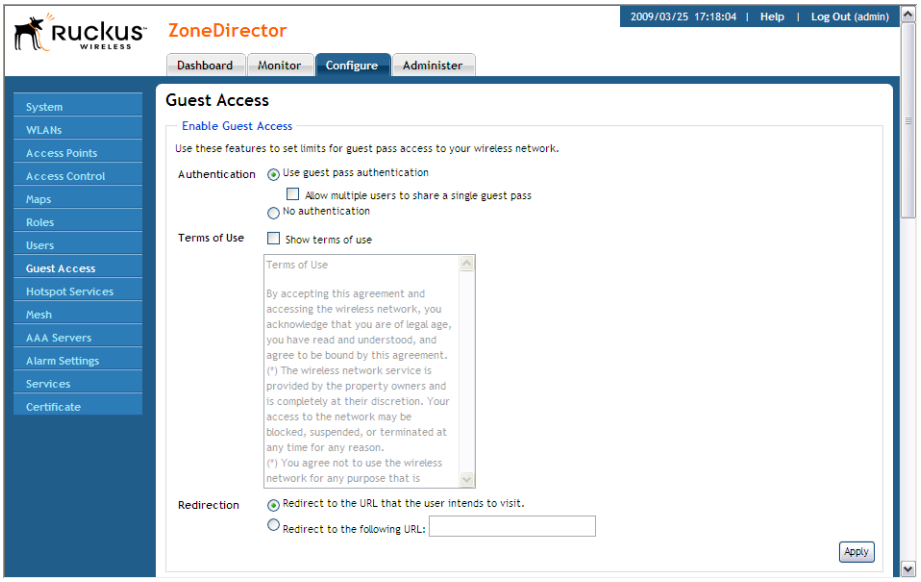
Configuring System-Wide Guest Access Policy

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. In **Redirect**, select one of the following radio buttons to use/not use redirection:
   - *Go to the original URL the user intended to*: 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 the redirected page(s), they are shown the expiration time for their guest pass.

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

Figure 52. The Guest Access page



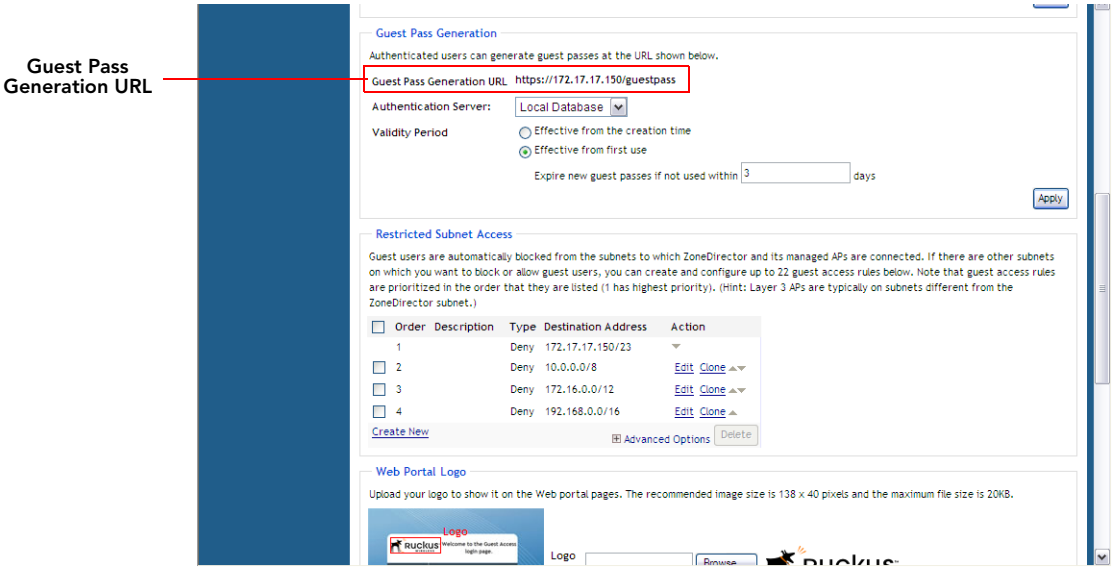
Activating Guest Pass Generation

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 *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 or Active Directory) 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 116).
   - If you want to use the local database of ZoneDirector, 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 53, the Guest Pass Generation URL is `https:192.17.17.150/guestpass`.

Figure 53. The Guest Pass Generation section on the Guest Pass page



Controlling Guest Pass Generation Privileges

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

1. Go to **Configure** > **Roles**. When the *Roles and Policies* page appears, a table lists all existing roles, including "Default".
2. Click **Edit** (in the "Default" role row).
3. In the *Policies* options, clear **Allow Guest Pass Generation** check box (if this option is active).
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.
   - **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.
   - **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.

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** > **User**.
2. At the bottom of the *Internal Users 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 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.

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 default 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. 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 109.
5. Go back to the Guest Pass Printout Customization page, 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 55).

Guest Pass Printout Tokens

Table 7 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 7. 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

Generating and Printing a Guest Pass

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

NOTE: The following procedure will guide you through generating and printing a guest pass. Before starting, make sure that you computer is connected to a local or network printer.

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.
6. On the Guest Information page, fill in the following options:
   - **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 (**Days**, **Hours**, or **Weeks**).
   - **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.
   - **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.
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 54. The Guest Information page

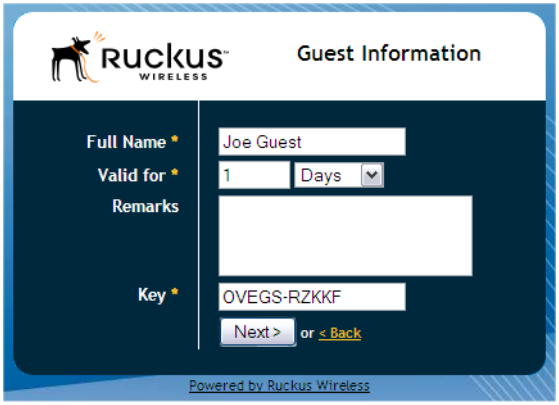


Figure 55. The Guest Pass Generated page (with customized key)

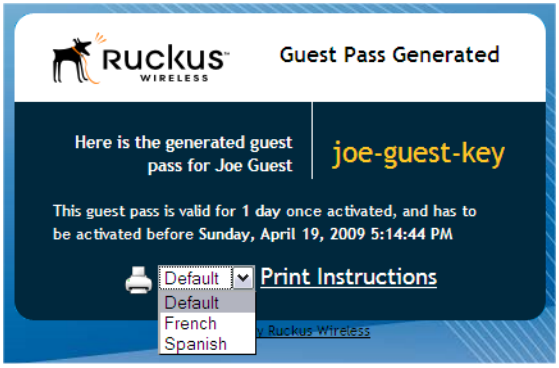
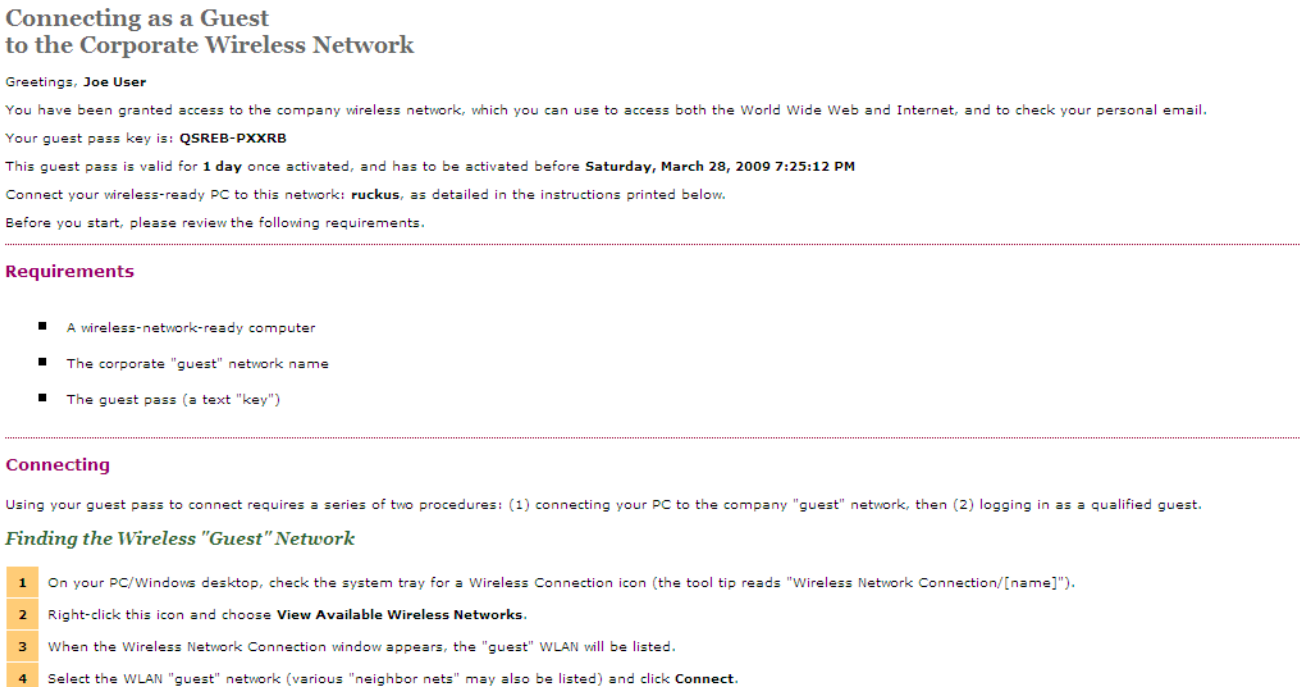


Figure 56. Sample guest pass printout



Connecting as a Guest
to the Corporate Wireless Network

Greetings, **Joe User**

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: **QSREB-PXXRB**

This guest pass is valid for **1 day** once activated, and has to be activated before **Saturday, March 28, 2009 7:25:12 PM**

Connect your wireless-ready PC to this network: **ruckus**, 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**.

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.

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 Pass > Restricted Subnet Access page.

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).

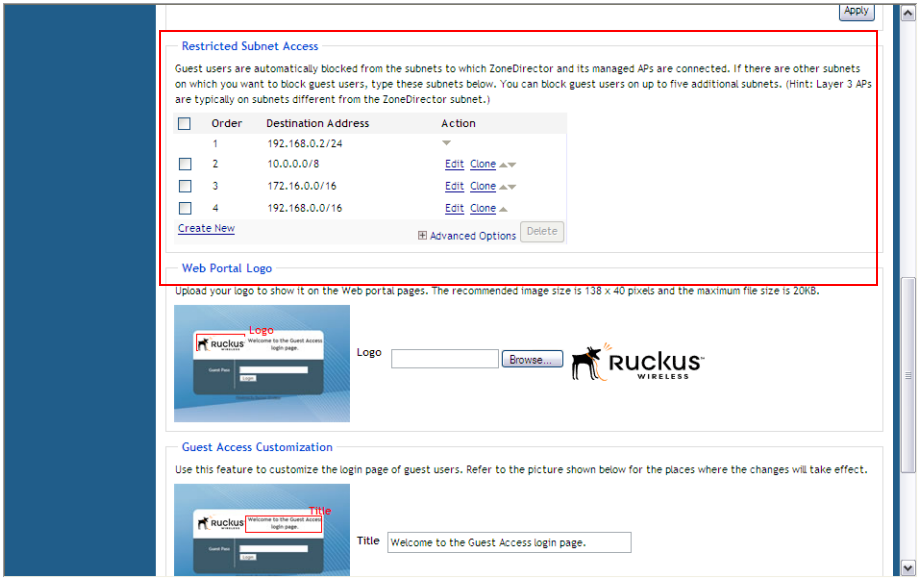
NOTE: All guests share this same subnet access policy.

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 57. The Restricted Subnet Access options



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.

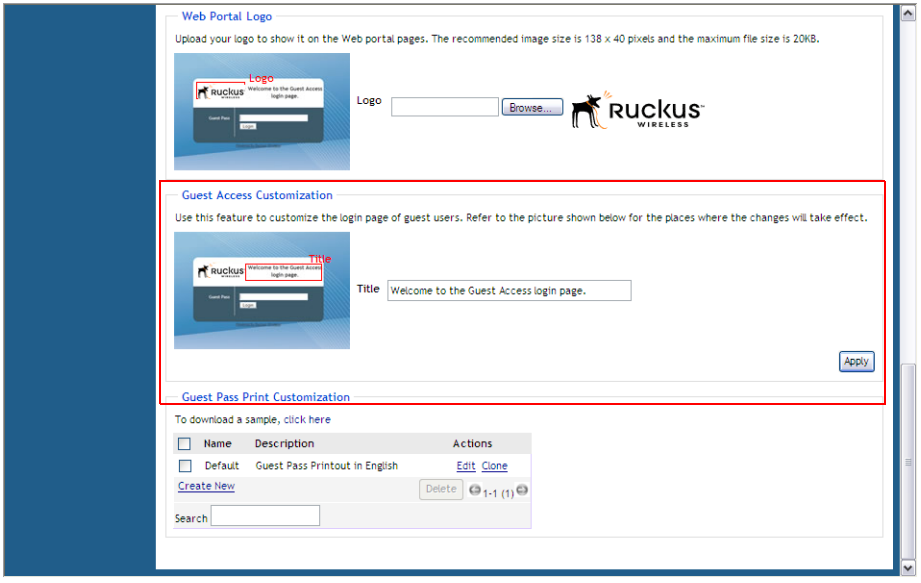
If you want to include a logo, you will need to prepare a Web-ready graphic file, in one of three acceptable formats (.JPG, .GIF or .PNG). Make sure that the logo file *does not exceed* the following:

- 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—height or width).
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 `Setting applied!` confirmation message briefly appears.

Figure 58. The Guest Access Customization options



Activating Web Authentication of Users

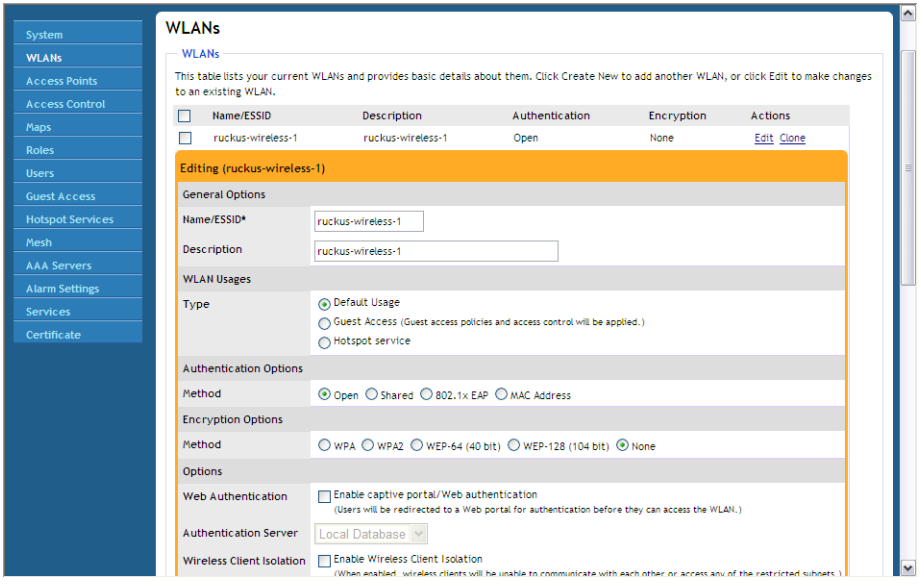
Web authentication, when activated on a WLAN, compels all users to log into a specific WLAN every time they connect. This is helpful if you are managing an Internet hotzone.

After you activate Web authentication on your hotzone/hotspot WLAN, you must then provide all users with a URL to your login page. Of course the users must be listed in an internal or external authentication database. 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.

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 59.
4. Click the check box to enable portal/Web authentication.
5. Select the preferred authentication server (for Web Authentication) 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 59. The Edit WLAN page



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-PSK/WPA2-PSK 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 Server or a RADIUS server 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 Active Directory, LDAP, RADIUS, or RADIUS Accounting server, or to create new user accounts on the internal user database.

To use an external authentication server

1. Go to **Configure** > **AAA Servers**. The Authentication Servers page appears.
2. Click the **Create New** link in the *Authentication Servers* table.
3. When the *Create New* 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 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.

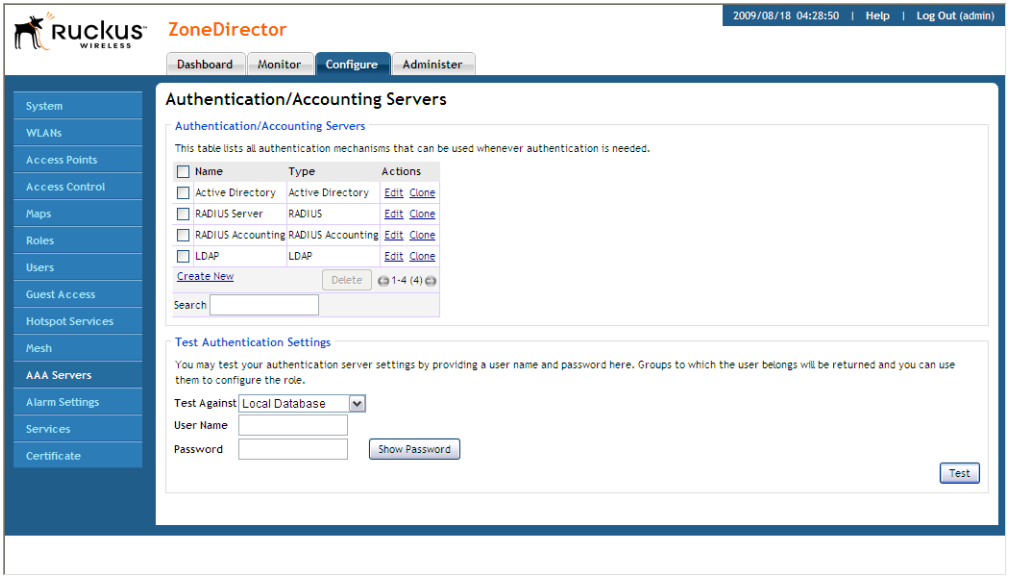
– *RADIUS Accounting*: If you select this option, you also need to enter the IP address of the RADIUS server, its port number (default is 1813), and its shared secret.

4. 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: 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**. Before testing against a RADIUS server, verify that Password Authentication Protocol (PAP) is enabled on the RADIUS server, or the test will fail.

Figure 60. The Create New form for adding an authentication server



6

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 159.

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.

Term	Definition
Mesh Node	A Ruckus ZoneFlex AP with mesh capability enabled. ZoneFlex models that provide mesh capability include: • 2741 • 2942 • 2925 • 2941 • 7762 • 7942 • 7962

Term	Definition
Root Access Point (Root AP)	A mesh node communicating to a ZoneDirector through its Ethernet (that is, wired) interface.
Mesh Access Point (Mesh AP)	A mesh node communicating to a ZoneDirector through its wireless interface.
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. There is no configurable limit to the depth of a mesh tree. A single ZoneDirector device can manage more than one mesh tree. The only limitation of how many mesh trees it can manage is dependent on the number of APs a ZoneDirector can manage. For example, a ZoneDirector 1006 can manage a mesh tree of 6 APs or two mesh trees of 3 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.

Supported Mesh Topologies

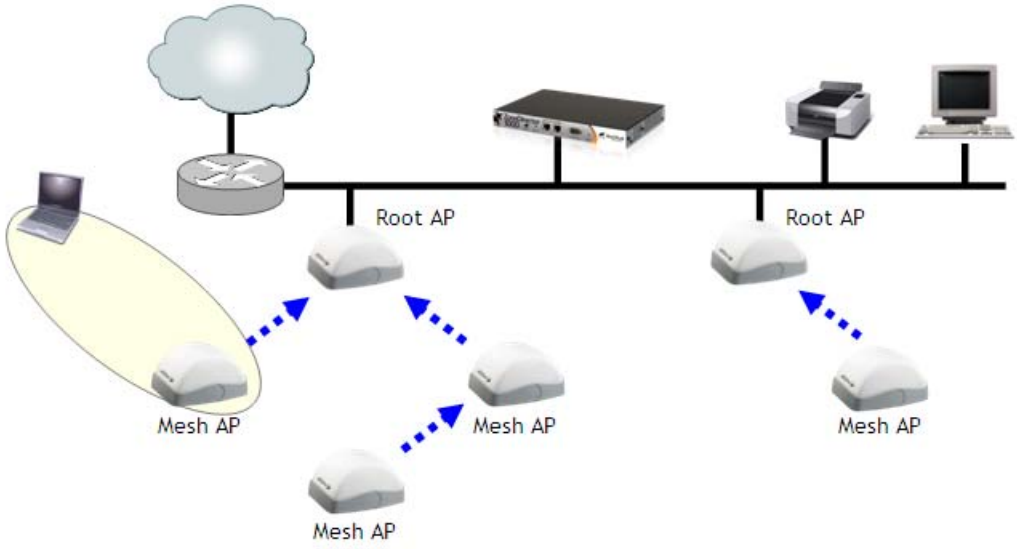
Smart mesh network supports two types of topologies:

- Standard Topology
- Wireless Bridge Topology

Standard Topology

If you need to extend the coverage of your wireless network, you can set up a mesh network using the standard topology. 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 61) to the wired LAN segment. All of the clients in each mesh tree function as wireless clients.

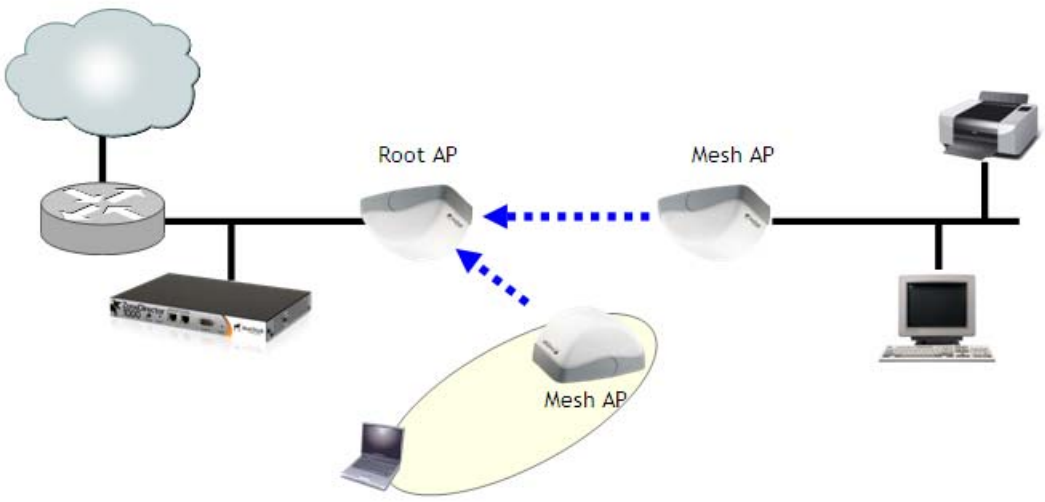
Figure 61. Mesh - standard topology



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 mesh link between the two wired segments, as shown in Figure 62 below.

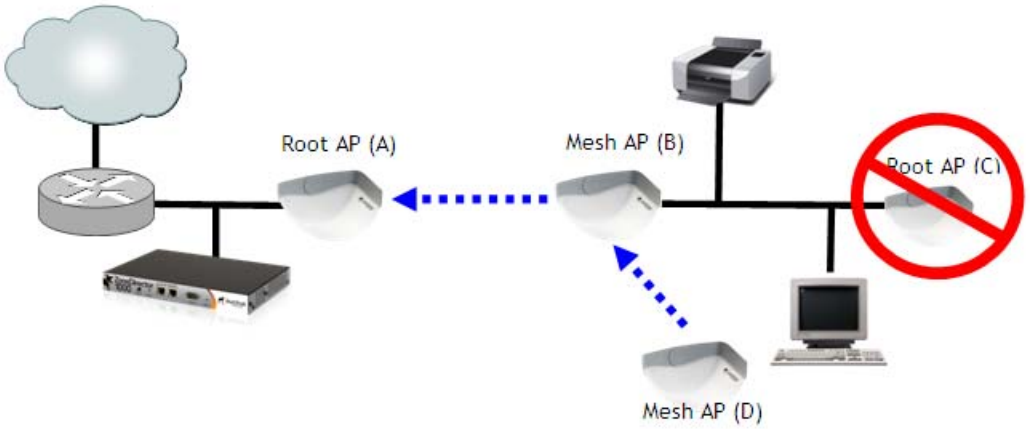
Figure 62. Mesh - wireless bridge topology



You cannot, however, connect additional wired APs to the bridged segment, as shown in Figure 63. The problem with this configuration is that because C can reach ZoneDirector through mesh link B-A and because C has its Ethernet port active, it meets both conditions (ZoneDirector reachable and Ethernet in use) to advertise that it is a Root - even though it is not a Root. Therefore this is an illegal topology.

However, additional wireless MAPs may be added in this physical location for additional coverage and capacity. In the example below in Figure A-2, RAP - C is NOT ALLOWED, as it is connected via Ethernet to this bridged wired segment. However using wireless MAP - D to extend the mesh is ALLOWED.

Figure 63. Mesh - Illegal Bridge Topology



Deploying a Wireless Mesh via ZoneDirector

Deploying a wireless mesh via ZoneDirector involves the following steps:

- "Step 1: Prepare for Wireless Mesh Deployment"
- "Step 2: Enable Mesh Capability on ZoneDirector"
- "Step 3: Provision and Deploy Mesh Nodes"
- "Step 4: Verify That the Wireless Mesh Network Is Up"

Step 1: Prepare for Wireless Mesh Deployment

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

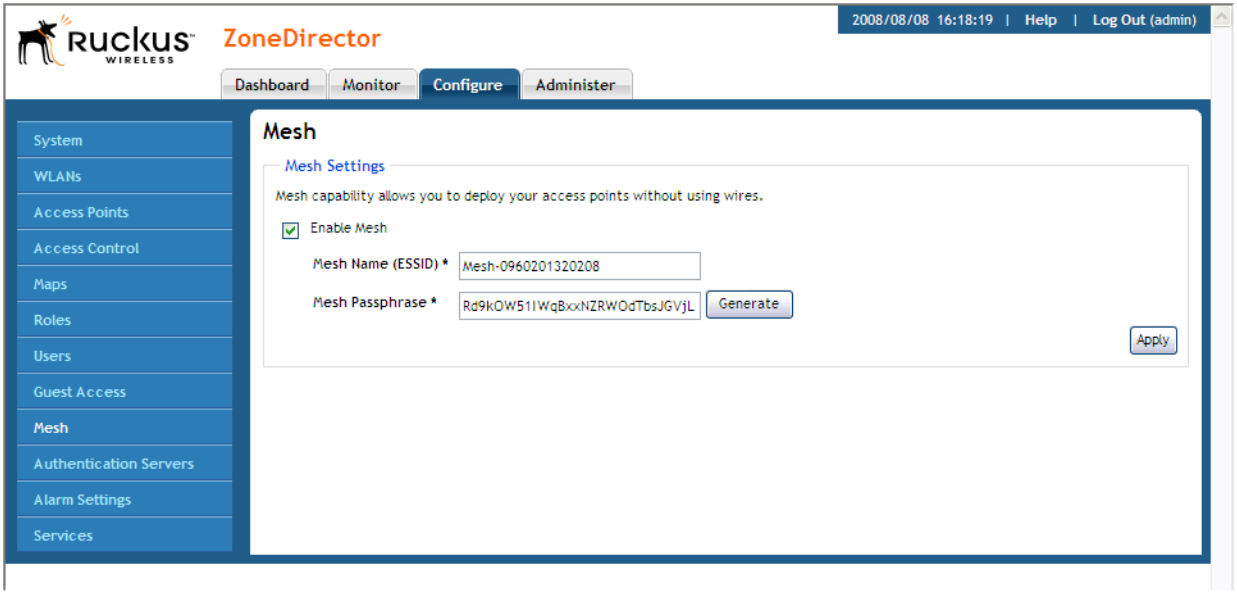
- Plan Your Wireless Mesh Network - Survey your deployment site, decide on the number of APs that you will deploy (including the number of Root APs and Mesh APs), and then create a simple sketch of where you will deploy each Root AP and Mesh AP. Remember that Root APs need to be connected to ZoneDirector 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 - ZoneFlex models that provide wireless mesh networking support include ZoneFlex 2942, ZoneFlex 7942, and ZoneFlex 2925. 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 above (for both ZoneFlex and ZoneDirector) support mesh networking.

- Enable Auto Approval - If you do not want to have to manually approve the join request 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 WLAN" on page 69.

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 page.

Figure 64. Enable Mesh in Configure > Mesh



To enable mesh capability

1. Log into the ZoneDirector Web interface.
2. Click the Configure tab.
3. On the menu, click Mesh.
4. Under Mesh Settings, select the Enable Mesh check box.
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. Click Apply to save your settings.

You have completed enabling mesh capability on ZoneDirector. You can now start provisioning and deploying the APs that you want to be part of the wireless mesh network.

Step 3: Provision and Deploy Mesh Nodes

In this step, you will connect each AP to the same wired network as ZoneDirector to provision it with mesh-related settings. After you complete provisioning an AP, you must reboot it for the mesh-related settings to take effect.

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 70.
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 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.

Repeat Steps 1 to 3 for each Mesh AP and Root 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.
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.

Figure 65. 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 or a Mesh AP. Refer to the following table:

	An AP with the upward pointing arrow is a Root AP.
	An AP with a number in a circle is a Mesh AP. The number indicates the number of hops from the mesh AP to the Root AP.

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 2925 AP), the two LEDs that indicate the mesh status are:

- WLAN/Wireless Device Association LED - Indicates downlink status and client association status
- Signal/Air Quality LED - Indicates uplink status and the quality of the AP's wireless signal

WLAN/Wireless Device Association LED

The behavior of the WLAN LED is the same on both Root AP and Mesh AP. 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 66. Behavior of the WLAN/Wireless Device Association LED

LED Color/Behavior	Root AP / Mesh AP
Solid green	No mesh downlink, and; At least one client is associated with the AP
Solid amber	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 67. Behavior of the Signal/Air Quality LED

LED Color/Behavior	Root AP	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
Slow blinking green	N/A	The AP is searching for an uplink
Off	This is a Root AP	N/A

On Dual-band ZoneFlex APs

NOTE: On dual-band ZoneFlex APs, mesh networking is enabled only on the 5GHz radio.

Two dual-band ZoneFlex AP models currently support mesh networking: ZoneFlex 7762 AP and ZoneFlex 7962 AP. Refer to the following sections for information on how to check these dual-band APs for their mesh status.

ZoneFlex 7762 AP

On ZoneFlex 7762 AP, the **STATUS** LED indicates the AP's mesh status. See the table below for more information.

Figure 68. Behavior of the Status LED

LED Color/Behavior	Description
Solid green	• This is a Root AP, 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 AP

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

Figure 69. Behavior of the 5G LED

LED Color/Behavior	Root AP	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

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 70. 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 hop)	AP is connected to ZoneDirector via its wireless interface and is *n* hops away from the Root AP.	

Figure 70. Mesh-related AP statuses

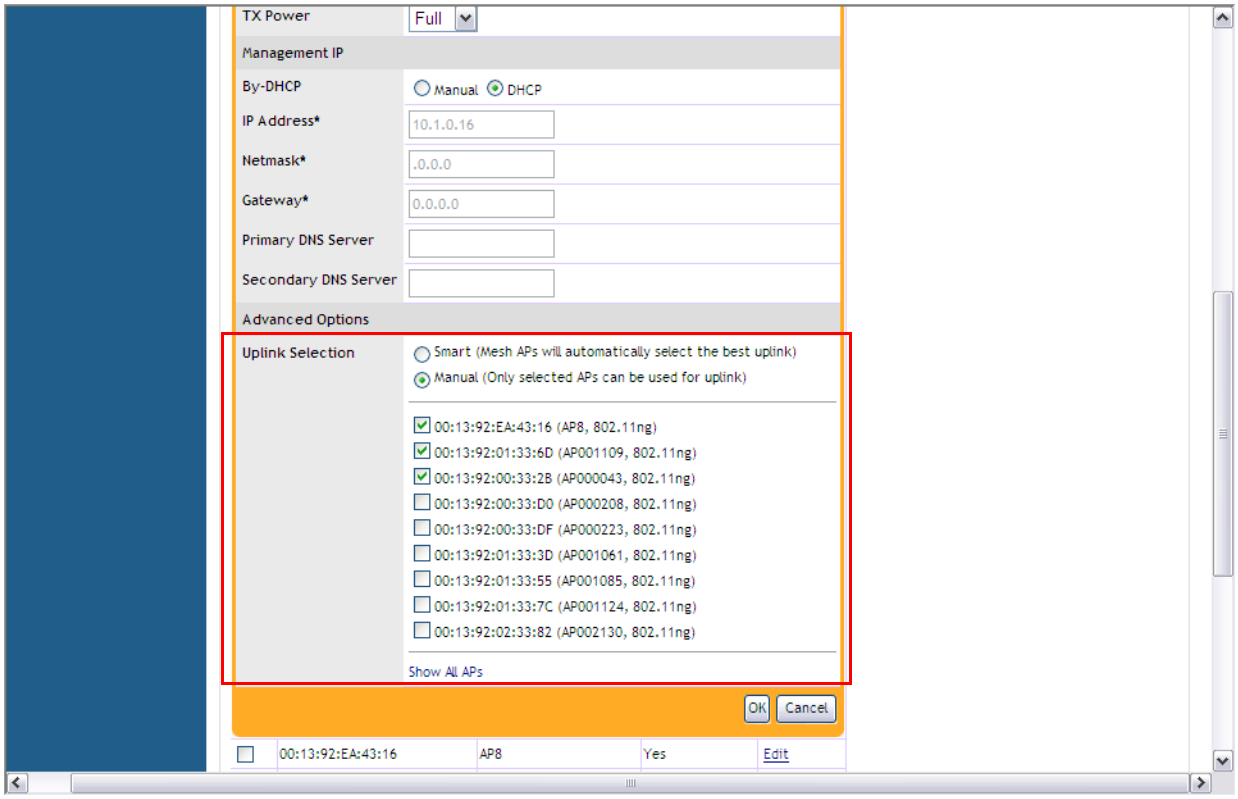
Status	Description	Recommended Action
Isolated Mesh AP	AP is disconnected from the ZoneDirector mesh	• The AP may be configured incorrectly. Verify that the mesh SSID and passphrase configured on the AP are correct. • If Uplink Selection is set to Manual, the uplink AP specified for this AP may be off or unavailable.

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.

Figure 71. Setting Uplink Selection to Manual



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 tab > Access Points page.

NOTE: A mesh network is dynamic in nature. Before attempting to resolve any mesh-related issue, please wait 15 minutes to allow the mesh network to stabilize. Some mesh-related issues are automatically resolved once the mesh network stabilizes.

Understanding Isolated Mesh AP Statuses

There are five possible reasons for a mesh AP to become isolated. The table below lists all possible Isolated Mesh AP statuses that may appear on the Monitor > Access Points page, and provides possible reasons for the isolation and the recommended steps for resolving the issue.

Status	Possible Reason
No APs in manual uplink selection	You have set uplink selection to Manual, but none of the uplink APs you specified is available or reachable. To resolve this, go to the Configure > Access Points page on the ZoneDirector Web interface, and then click SmartSelection.
No APs within hop-limit	The AP cannot find other APs within the internally defined hops. The hop limit mechanism helps ensure that mesh APs maintain a reasonable network performance. To resolve this, add additional wired APs between this isolated Mesh AP and the closest Root AP.
Searching for uplinks	The AP is still searching for uplinks. This is usually a temporary state and is typically resolved automatically within 15 minutes as the mesh network stabilizes. If there is a significant number of APs on the network, it might take longer for the AP to resolve this.

Status	Possible Reason
Config error	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 134.
No APs with matching radio type	The AP is unable to find another mesh AP with the same radio type. In the current version of Ruckus Wireless' SmartMesh technology, 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

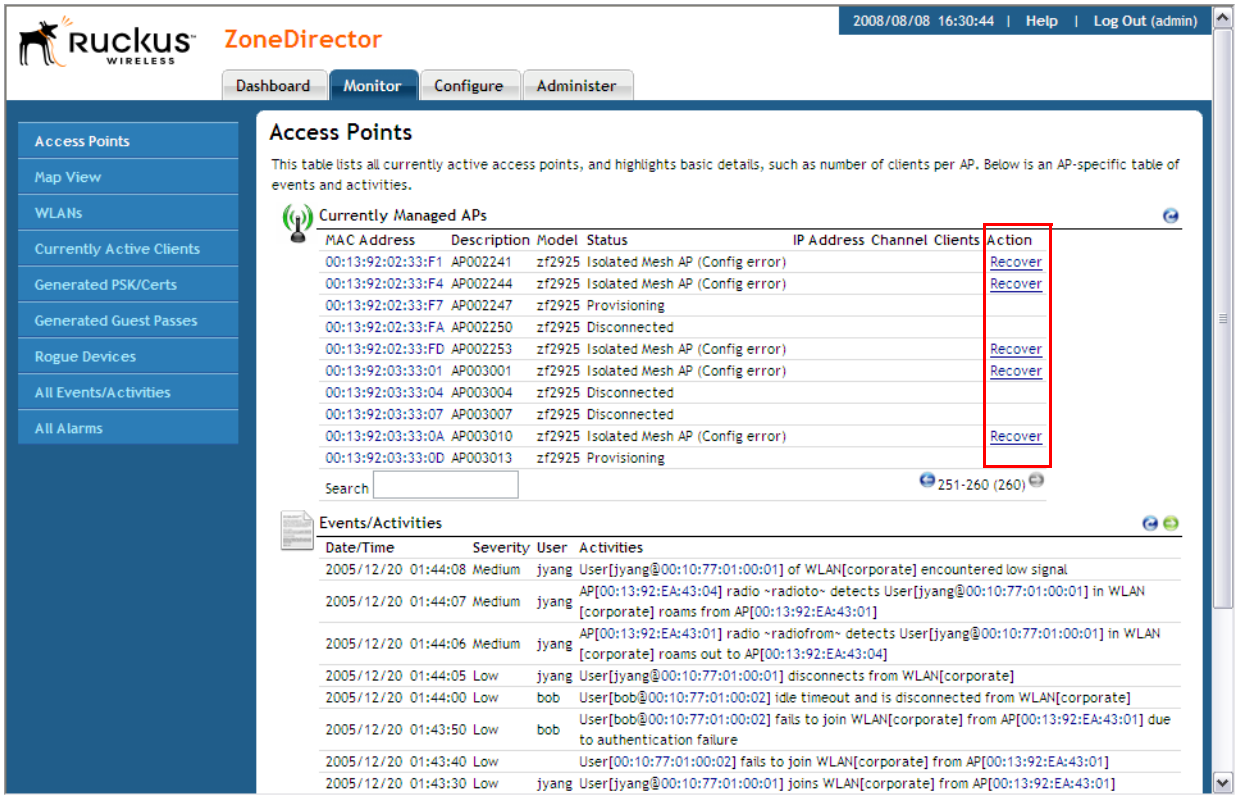
To perform these procedures, you will need:

- 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 last known mesh configuration for the AP (steps for obtaining this information are provided below).
- An SSH client, such as PuTTY and OpenSSH.

Step 1: Obtain the AP's Last Known Mesh Configuration

1. On the ZoneDirector Web interface, click the **Monitor** tab, and then click **Access Points** on the menu.
2. Under **Currently Managed APs**, look for the status message `Isolated Mesh AP (Config error)`, and then click the **Recover** link that is on the same row.

Figure 72. Click Recover to obtain the AP's last known mesh configuration



A page appears, which shows the AP's last known mesh configuration. Mesh information that appears on this page includes:

- AP's MAC Address
- Last Known Mesh SSID (mesh name)
- Last Known Mesh PSK (mesh passphrase)

3. Write down these details on a piece of paper. You will need them later in the next procedure.

Step 2: Set Up Your Computer for Wireless Connection to the AP

1. Assign the following static IP address settings to your computer:
   - IP Address: `192.168.54.34`
   - Mask: `255.255.255.252`

2. Create a wireless network from your computer. If you are running Windows XP, you can use the Wireless Network Setup Wizard to create the wireless network. Configure the wireless network with the following settings:
   - Association mode: WPA2
   - Encryption method: AES
   - SSID: Type the AP's last known SSID (which you obtained in the previous section)
   - PSK: Type the AP's last known PSK (which you obtained in the previous section)

Step 3: Connect to the AP and Update its ESSID and Passphrase

1. After you create the wireless network, position the computer close enough to the AP to allow association.
2. After your computer has associated with the AP, start the SSH client, and then connect to `192.168.54.33` (the AP's IP address).
3. Log into the AP via SSH using the same user name and password that you use to log into the ZoneDirector Web interface.
4. Enter the command `set meshcfg ssid "current_ssid"`, where current_ssid is the SSID that the mesh network is currently using.
5. Enter the command `set meshcfg passphrase "current_passphrase"`, where current_passphrase is the passphrase or PSK that the mesh network is currently using.
6. 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 159.

7

Setting Administrator Preferences

In This Chapter

Using an External Server for Administrator Authentication

ZoneDirector supports additional administrator accounts that can be authenticated using an external authentication server such as RADIUS or Active Directory. Two types of administrative privileges can be assigned to these administrator accounts:

- Full Privileges – Allow all types of configuration and management tasks
- Limited Privileges – Allow monitoring operations only

This section provides basic instructions for setting up ZoneDirector to authenticate additional administrator accounts with an external authentication server.

Step 1: Set Up Group Attributes on the Authentication Server

The tasks that you need to perform to set up group attributes on the authentication server depend on whether you are using RADIUS or Active Directory.

NOTE: For specific instructions on how to complete these tasks, refer to the documentation that is supplied with your authentication server.

If You Are Using RADIUS for Authentication

1. Set up one of the following vendor-specific attributes. Remember the attributes that you set; you will enter this information when you create administrator roles in ZoneDirector (*see Step 3*).
   - 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 ..."
2. Set up a shared secret on the RADIUS server. You will enter the same shared secret on the ZoneDirector Web interface to enable ZoneDirector to communicate with the RADIUS server for authentication.

If You Are Using Active Directory for Authentication

Set up two groups – one for administrators with *Full Privileges* and another for administrators with *Limited Privileges*. 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.

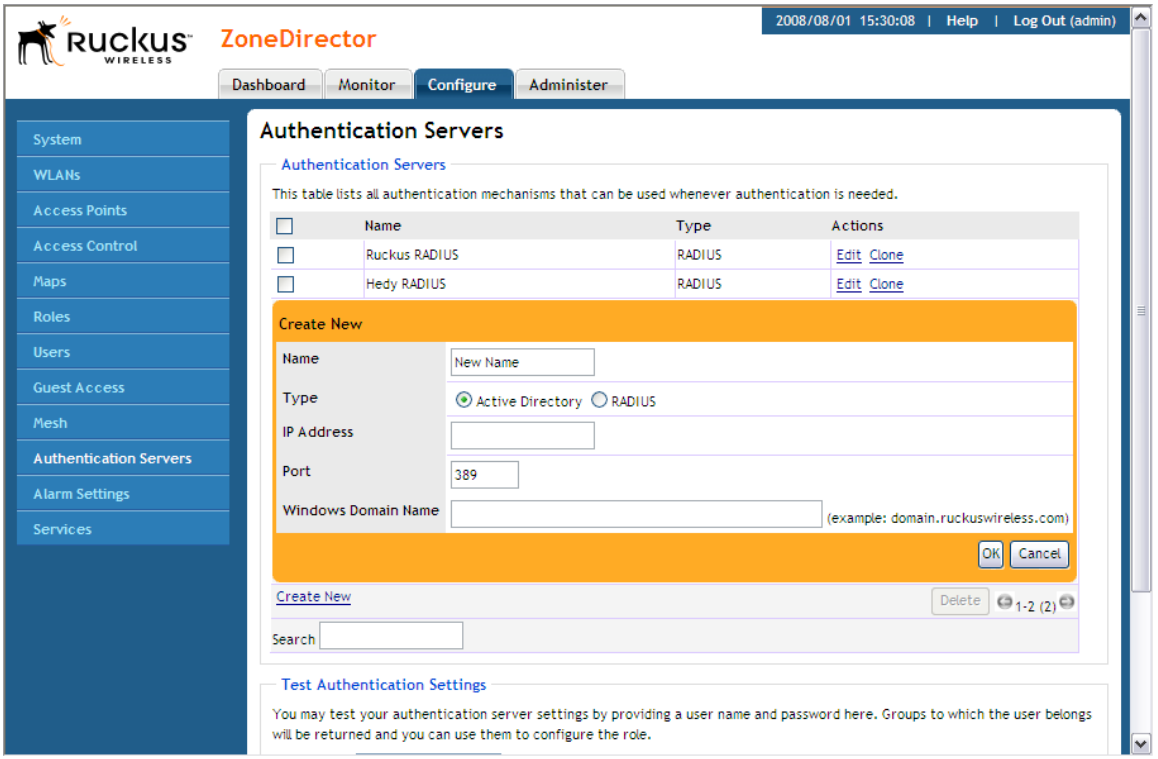
Remember the group names that you set; you will enter this information when you create administrator roles in ZoneDirector (*see Step 3*).

Step 2: Set Up ZoneDirector to Use an Authentication Server

1. Log into the ZoneDirector Web interface.
2. Click the **Configure** tab, and then click **Authentication Servers** on the menu.
3. Under Authentication Servers, click the **Create New** link. The Create New form appears.
4. In **Name**, type a name that you want to use to identify this authentication server. The actual authentication server name that will appear after you finish this procedure will include this name and the authentication server type. For example, if you type HEDY in Name and you click RADIUS in **Type** (below), the actual authentication server name that you will see is `HEDY RADIUS`.
5. In **Type**, click the type of authentication server that you want to use. Options include **Active Directory** and **RADIUS**.
6. In **IP Address**, type the IP address of the authentication server.
7. In **Port**, type the authentication port number.
   - If you are using Active Directory, the default port number is `389`.
   - If you are using RADIUS, the default port number is `1812`.
8. Configure server-specific settings:
   - If you clicked **Active Directory**, type the Active Directory domain name in **Windows Domain Name**.
   - If you clicked **RADIUS**, type the shared secret on the RADIUS that you set up in Step 1, and then retype it to confirm.
9. Click **OK**.

The Authentication Servers page refreshes and the server that you have created appears in the table. You have completed setting up ZoneDirector to use an external authentication server.

Figure 73. The Authentication Servers page



Step 3: Create an Administrator Role

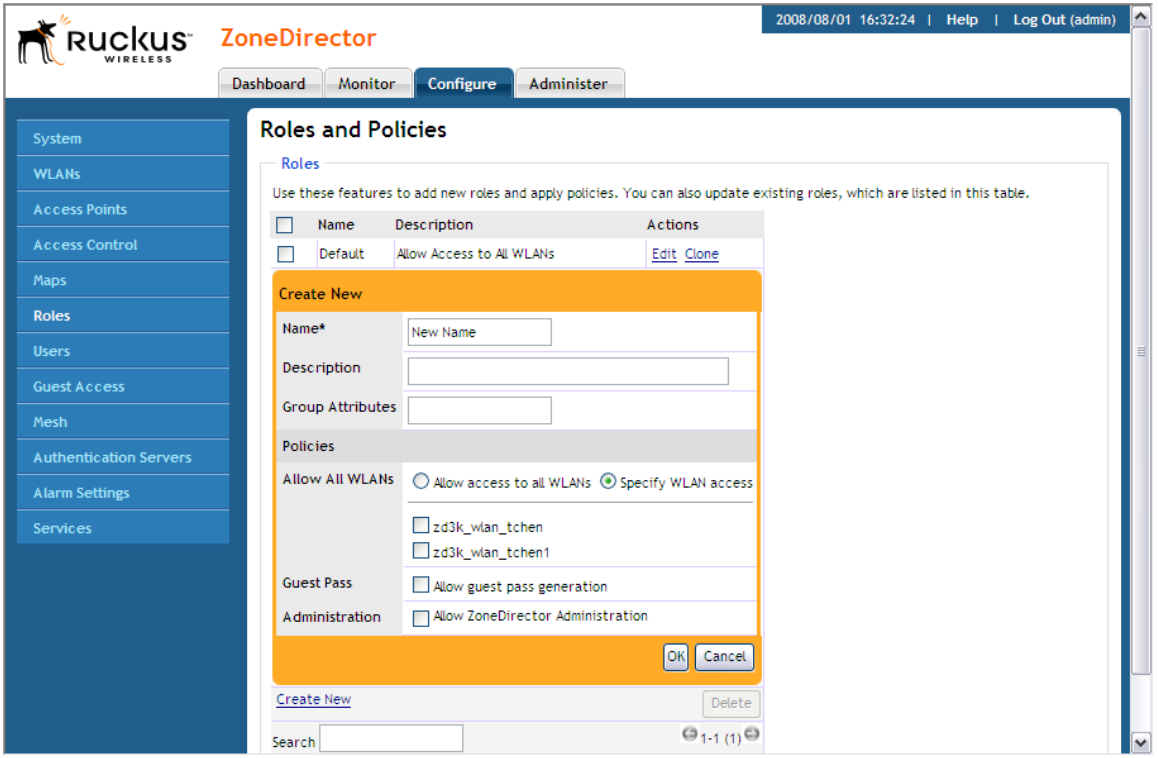
1. Click the Configure tab, and then click Roles on the menu. The Roles and Policies page appears.
2. Under Roles, click the Create New link. The Create New form appears.
3. In Name, type a unique name for this administrator role that you are creating. For example, if you are creating this role for administrators with limited privileges, you can type admin-limited.
4. In Group Attributes, type the group name or attribute that you configured on the authentication server in Step 1. For authentication to work, the group name or attribute that you type in this box must *exactly match* the attribute on the authentication server.
5. In Administration, select the Allow ZoneDirector Administration check box.

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.

6. When the privilege options appear under the check box, click the type of privileges that you want to grant this role. Options include:
   - Full privileges (Perform all configuration and management tasks)
   - Limited privileges (Monitoring and viewing operation status only)
7. Configure other settings (Description, Policies, and Guest Pass) on the page as required.
8. Click OK to save your changes.

You have completed creating an administrator role.

Figure 74. The Roles and Policies page



Step 4: Test Your Authentication Settings

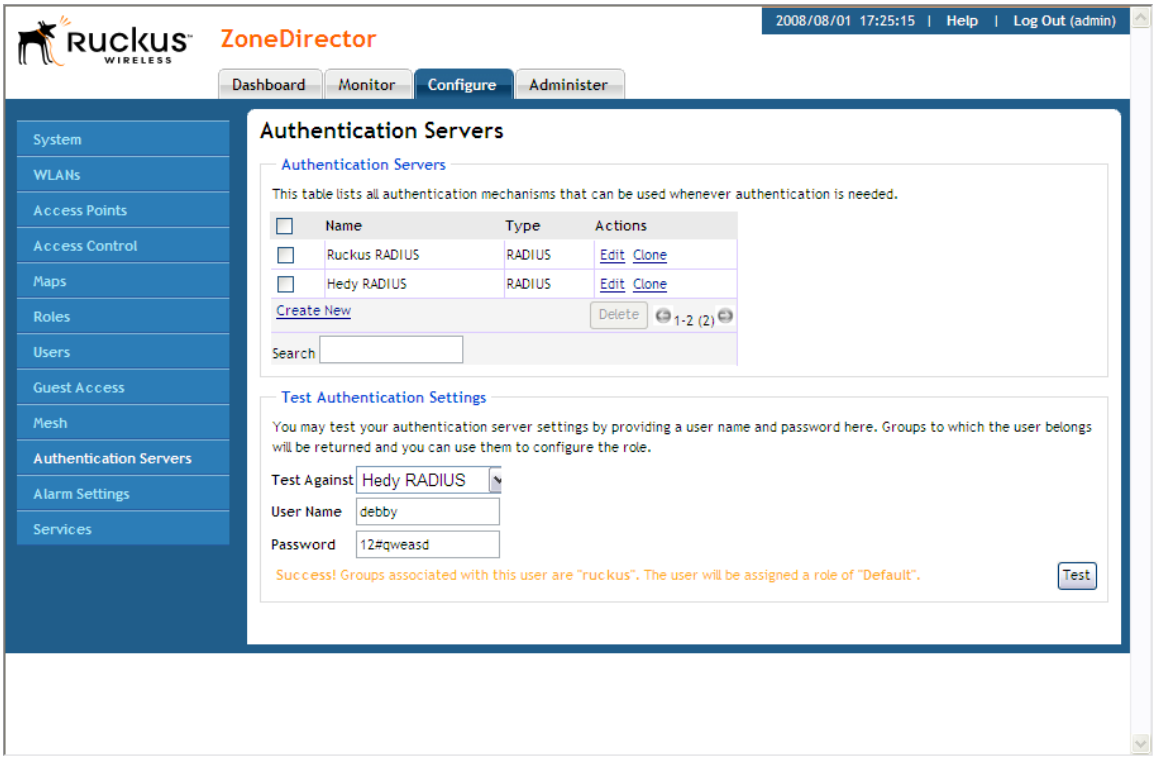
Perform this task to ensure that ZoneDirector can connect to the authentication server and retrieve the groups/attributes that you have configured for each user account.

1. Click the Configure tab, and then click Authentication Servers on the menu.
2. Under the Test Authentication Settings section, select the authentication server that you want to use from the Test Against drop-down menu.
3. In User Name and Password, enter a RADIUS or Active Directory user name and password.
4. Click Apply.

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}.
```

Figure 75. The Test Authentication Settings section on the Authentication Servers page



Step 5: Specify the Authentication Server to Use

1. Click the **Administer** tab, and then click **Preferences** on the menu.
2. Under **Administrator Name/Password**, click **Authenticate with Auth Server**.
3. On the drop-down menu, select the name of the authentication server with which administrators will authenticate. The authentication server names that appear on the drop-down menu are the same as the server names that appear on the **Configure** > **Authentication Servers** page.
4. 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.
5. Change the administrator name and password, if preferred.
6. Click **Apply**.

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}).
```

Changing the ZoneDirector Administrator User Name and Password

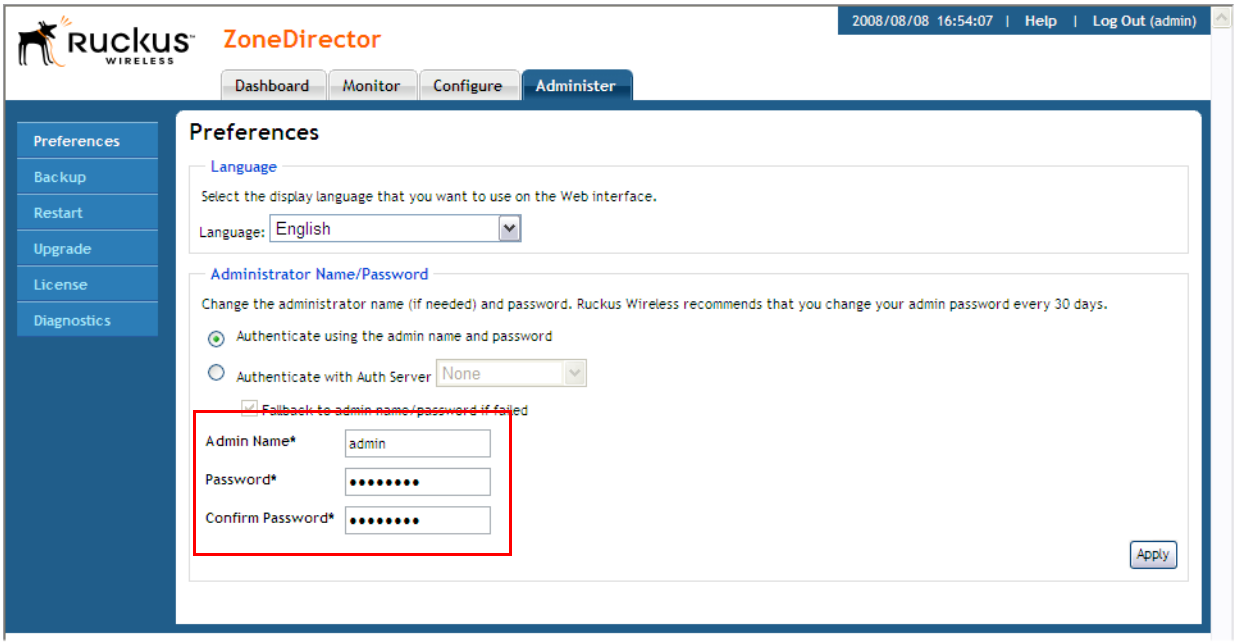
You should change your ZoneDirector administrator login password on a monthly basis, but the administrator user name should be changed only if necessary.

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*:
   - **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 76. The Preferences page



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, open the Language menu and choose your preferred language. See Figure 76.

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 the License

Depending on the number of Ruckus Wireless APs you need to manage with your ZoneDirector, you may need to upgrade your 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.

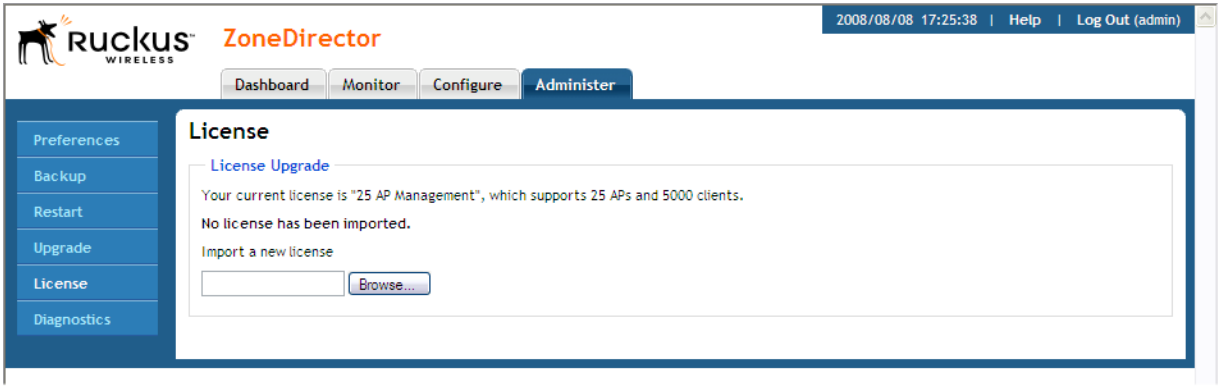
NOTE: The system does not reboot or reset after a license is imported.

NOTE: This version of ZoneDirector supports tunnel mode and Opportunistic PMK Caching (OPC). If you want to use these features, you will need to import an additional license file called Mobility License. To purchase a Mobility License, contact Ruckus Wireless or an authorized reseller.

To import a new license file

1. Go to Administer > License.
2. Click Browse to find your license.
3. Once you find your license and closed the *Browse* window, ZoneDirector immediately attempts to validate and install the license.

Figure 77. The License page



8

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 Ruckus WLAN.

At the end of the setup wizard, your Ruckus ZoneDirector automatically activates a default internal WLAN for authorized users. A key benefit of the internal WLAN is the "zero IT" configuration, which extends to new users, to make their device configuration and initial login as easy as it can be. "Zero IT" client device configuration requires the client be running Windows XP SP 2/Vista, 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 is on the client machine, check the wireless network adapter to verify the implementation of WPA.
- Option 2: Upgrade to Windows XP SP2/Vista, and if needed, acquire a wireless network adapter with WPA support. Once these changes are made, your users can attempt a "zero IT" login.
- 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.
- Option 4: Assumes that the client OS cannot be upgraded and the wireless network adapter is limited to WEP. This requires two phases:
  - *Ruckus Administration*— [1] You, the network manager, create a supplemental WLAN for the non-standard client connections, then [2] create a Role that refers to this WLAN, and [3] assign that role to the affected user account.
  - *User Configuration*— Enter the needed WEP key in the network configuration.

In most solutions, you will need to open a Windows control panel and enter a WPA passphrase which you provide, or a WEP key (if you switch internal WLAN to WEP, which means you must provide the user with a copy of the key.) Once the passphrase or key is stored in Windows on their client, they can log into the WLAN.

Fixing User Connections

If any of your users report problematic connections to the WLAN, here is one debugging technique that 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 bypassed.

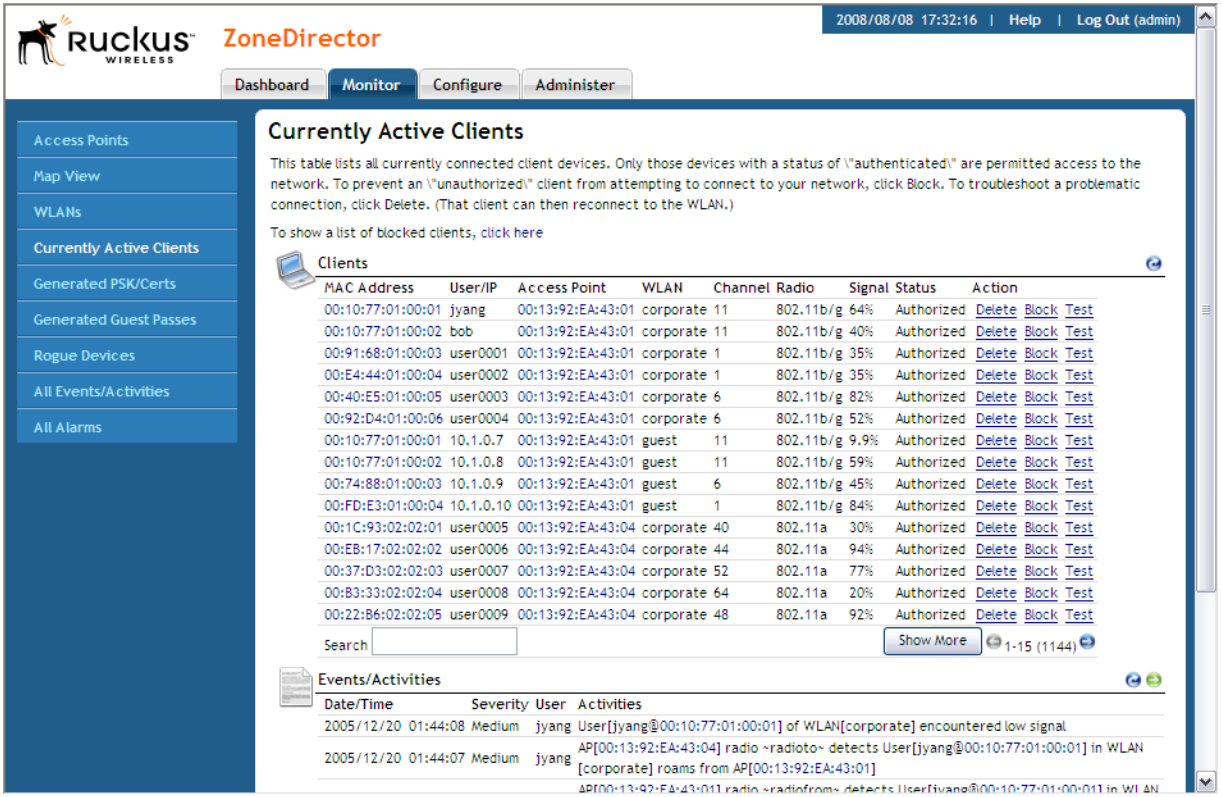
To debug an active user connection

1. Go to **Monitor** > **Currently Active Clients**.
2. When the *Currently Active Clients* page appears, locate the buggy client connection in the *Clients* table.
3. Click **Delete**.

That client will be automatically logged out of ZoneDirector.

After a minute or two, when the client has automatically re-logged into the WLAN, the Client table will re-display the client and the user will have fewer or no problems.

Figure 78. The Currently Active Clients page



If WLAN Connection Problems Persist

If the previous technique fails to resolve the user's client mis-connections, you may need to guide them through a full re-setting of their WLAN configuration. This requires your deleting the user record, then creating a new user record, at which time the user must repeat the "new user connection" process, with the two-part login and the downloading and installing of a new WLAN configuration.

1. Have the user log out of the WLAN until they receive notification from you.
2. Go to **Configure** > **Users**.
3. When the *User Authentication* features appear, locate and delete this user record from the *Internal Users Database* table.
4. Add a new user account for this user, and send notification to that 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 the Wireless Network Throughput with SpeedFlex

SpeedFlex is a wireless performance tool included in ZoneDirector that you can use to measure the downlink throughput between a wireless client and the AP with which it is associated. 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 the 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 154.

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 that is 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. 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.
7. Click the **Start** button.
   - If the target client does not have SpeedFlex installed, a message appears, informing you the SpeedFlex 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 or Mac) from the SpeedFlex interface, and then send it to the client user for installation. 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're testing AP throughput and you selected both Downlink and Uplink options, the tests might take one minute to complete.

When the tests are complete, the results appear below the Start button. Information that is shown includes the downlink/uplink throughput and the packet loss percentage during the tests.

Figure 79. The SpeedFlex interface

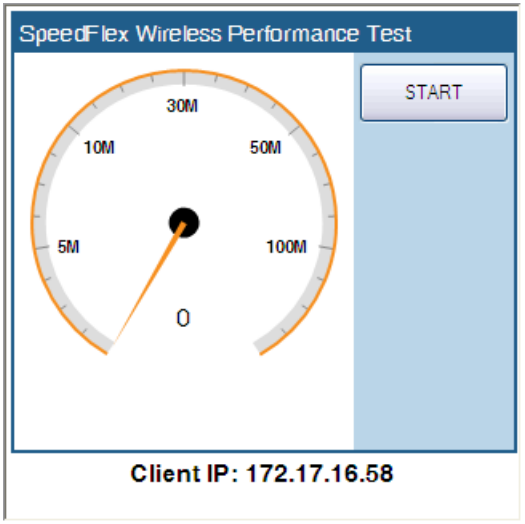


Figure 80. Click the download link for the target client's operating system

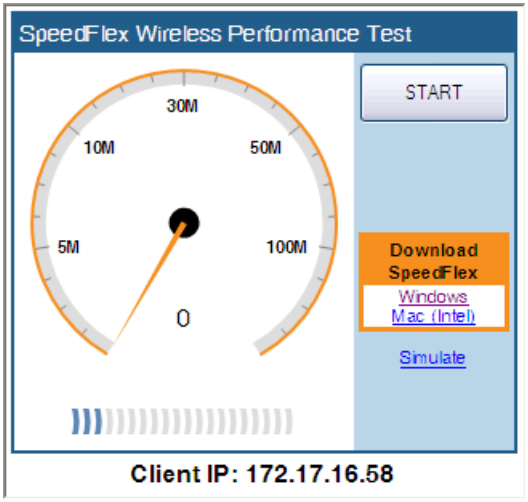


Figure 81. A progress bar appears as SpeedFlex measures the wireless throughput

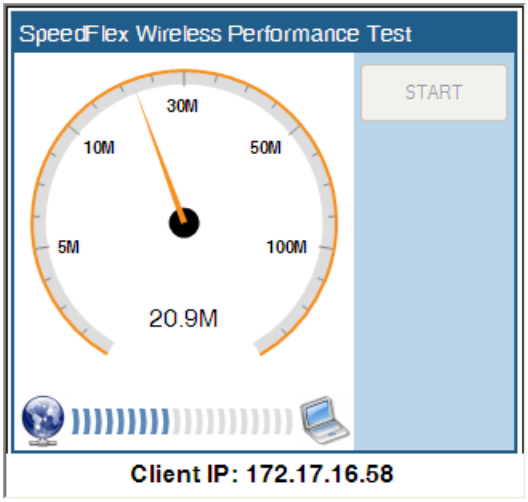
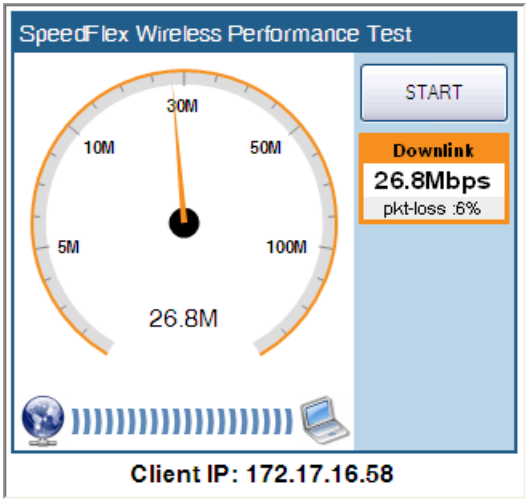


Figure 82. When the test is complete, the tool shows the downlink throughput and packet loss percentage



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 APs.

For example, if you have three Ruckus APs, open the *Radio B/G Channel* drop-down list in each AP record and choose "1", "6" and "11" in each of the three. However many APs you have, make sure that each AP has a fixed channel number not too close to the number of a nearby Ruckus AP.

Starting a Radio Frequency Scan

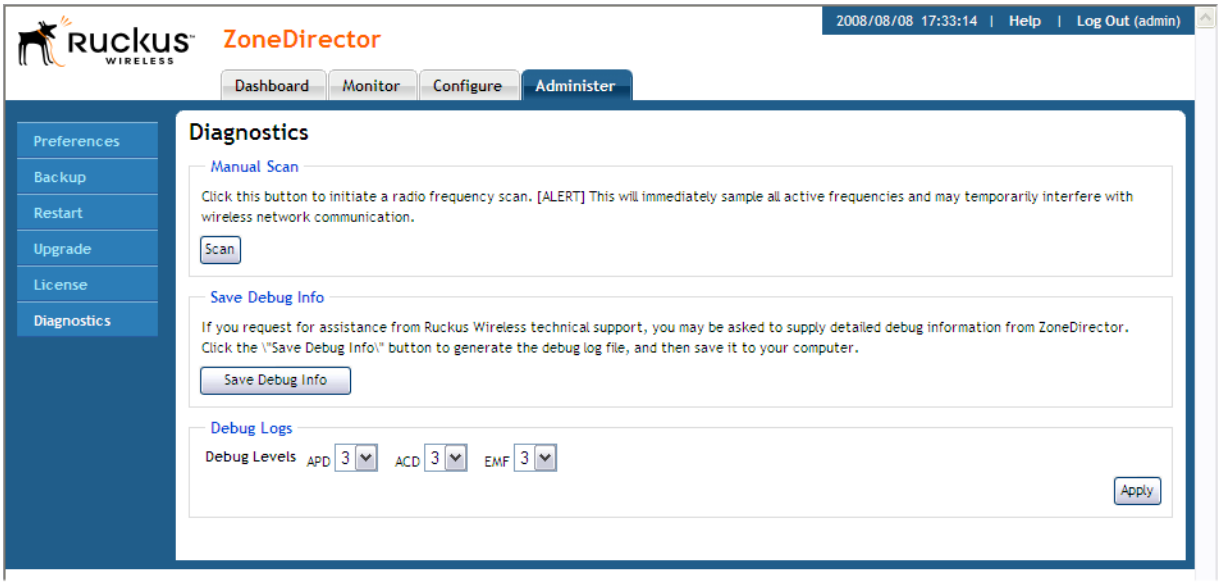
This task complements the automatic RF scanning feature that is built into the Ruckus ZoneDirector. That automatic scan assesses one radio frequency at a time, every 20 seconds or so. To manually start a complete radio frequency scan that assesses all possible frequencies in all devices at one time, 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 scanning results. This will include rogue device detection, and an updated coverage evaluation.

Figure 83. The Diagnostics page



Reviewing Self Healing and Intrusion Prevention Options

This Ruckus Wireless network feature adds automatic network adjustments to the existing monitoring functions, so that the Ruckus ZoneDirector can efficiently shift AP-specific settings and resources to improve coverage.

1. Go to **Configure** > **Services**.
2. Review and change the following self-healing options (which are all active by default):
   - **Adjust AP radio power**: If this capability is activated (default) and the TX power of a radio is auto (default), the Ruckus APs automatically reduce or maximize the transmit power to provide the best wireless service.
   - **Adjust AP channel**: If interference of any kind is detected in an AP, the radio frequency will automatically be switched.
3. Review and change the following intrusion prevention options (which are all active by default):
   - **Excessive wireless requests**: If this capability is activated (default), excessive 802.11 probe request frames and management frames launched by malicious attackers will be discarded.
   - **Repeat Authentication Failure**: If this capability is activated, any clients that repeatedly fail in attempting authentication will be temporarily blocked for a period of time. Default is 30 seconds.

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

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. Review the settings in the *Debug Log* options, and make the request adjustments with the three *Levels* drop-down lists. (If no settings were specified, ignore this step.)
   - **APD**: For information between Ruckus Wireless AP and Ruckus ZoneDirector
   - **ACD**: For information on wireless clients activities
   - **EMF**: For information regarding Web interface operations
3. If you did change the *Levels* settings, click **Apply** to save your settings.
4. In the *Save Debug Info* options, click **Save Debug Info**.
5. When the *File Download* dialog box appears, click **Save**.
6. When the *Save As* dialog box appears, pick a convenient destination folder, type a name for the file, and click Save.
7. 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.

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 *AP Summary* table for the particular Access Point record.

   The *Status* column should display "Connected."
3. Click **Restart**. 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

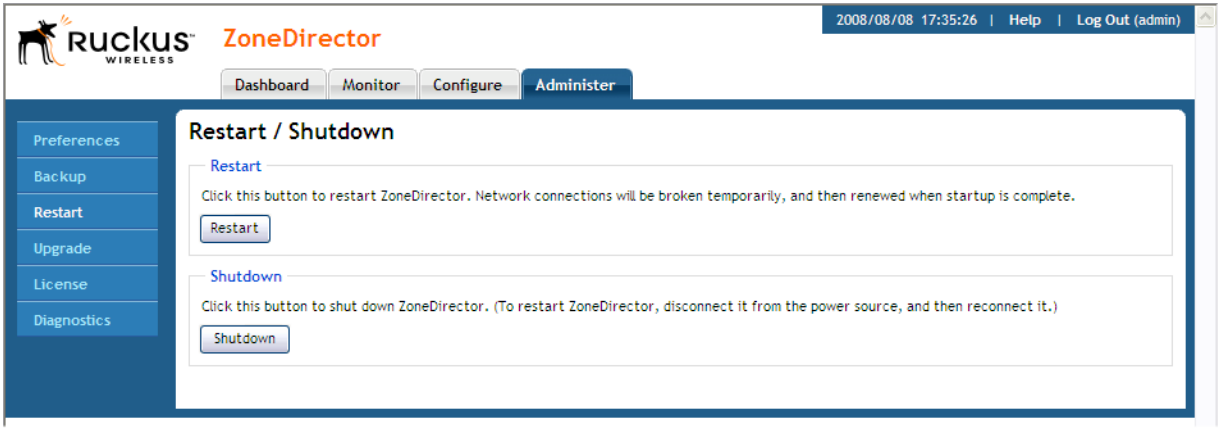
There are three "restart" options: [1] to disconnect and then reconnect the Ruckus ZoneDirector from the power source, [2] to follow this procedure which simultaneously shuts down ZoneDirector and all APs, then restarts all devices, and [3] a restart of individual APs (detailed in Restarting an Access Point.)

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 84. The Restart/Shutdown page



A

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, best performance is achieved using the newer, faster 802.11n AP - ZoneFlex 7942. However, the 802.11g APs - ZoneFlex 2942 and ZoneFlex 2925 will also form a perfectly fine mesh network.

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 (ZoneFlex 7942) or all nodes must be 802.11g (ZoneFlex 2942 or ZoneFlex 2925). You cannot mix 802.11n (ZoneFlex 7942) with 802.11g APs (ZoneFlex 2942 or ZoneFlex 2925) in a mesh. You can mix ZoneFlex 2942 with ZoneFlex 2925 in the same mesh, because they are both 802.11g.

In summary, build your mesh network as follow:

- Ensure that all APs are 802.11n - model ZoneFlex 7942
- Ensure that all APs are 802.11g - model ZoneFlex or ZoneFlex 2942

NOTE: The above restrictions apply only to AP-to-AP communication as part of a mesh, not to AP-to-client communication. For example, there is no problem for 802.11g clients to connect to an 802.11n mesh.

Calculating the Number of APs Required

This is an important step in planning your mesh network. In this step, you will calculate the number of total APs (RAPs and MAPs) that are needed to provide adequate coverage and performance for a given property.

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. Wireless is a shared medium, of course, so this aggregate bandwidth will be shared amongst the concurrent users at any given time. So 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 I used an oversubscription ratio of 4:1, such a network could actually support 40 users at 1Mbps.

But first, some background on mesh technology, and its impact on performance. A Root AP (RAP) in a mesh network has all its 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. With this background in mind, a two-step process to calculate the number of APs will be used.

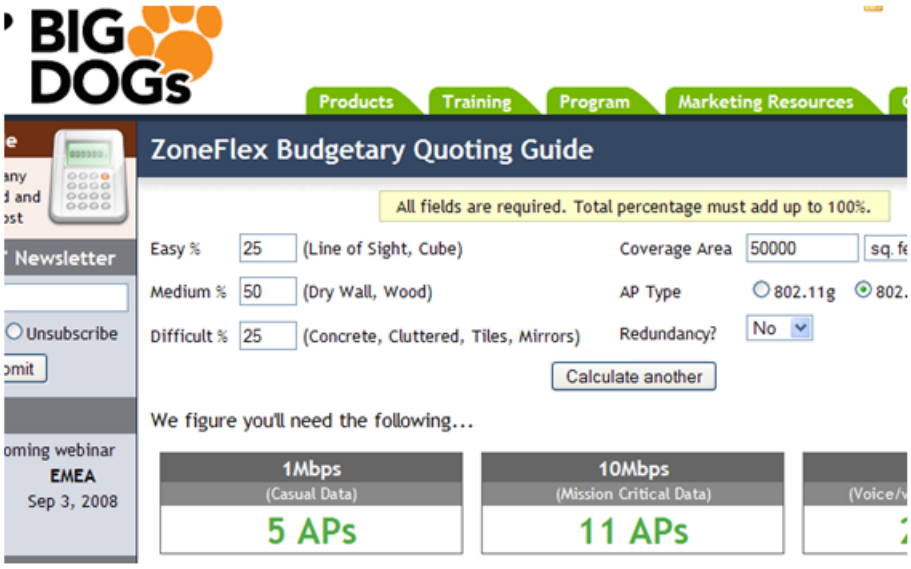
Step 1

In step 1, we assume that all APs are Roots (i.e. have an Ethernet drop available), even if this is actually not the case. This is our most optimistic number - when all APs are connected by wire. The best way to do this is to use the handy calculator provided on the Big Dogs Partner Portal at

`http://partners.ruckuswireless.com/sales_tools/quoting_guide`

Figure 85 shows a screen shot of the quoting tool. It requires you to fill in some parameters regarding the environment, square feet to cover, etc., and it generates the number of APs needed.

Figure 85. Screen shot of the quoting tool on the Big Dogs Partner Portal



A sampling of results generated by the calculator, for an environment with 25% Line of Sight/Cubicle, 50% dry wall and wood, and 25% concrete and tile, is shown in Table 8 below. This table is useful for some quick calculations on number of APs. However, it is recommended that you use the calculator on the Big Dogs Portal, so that your exact RF parameters and square feet can be entered for your particular site.

Table 8. Number of APs required (all Root)

Square Feet	# APs Needed Internet Grade (Throughput 1Mbps)	# APs Needed Enterprise Grade (Throughput 10Mbps)
10,000	4	5
20,000	4	6
50,000	5	11
100,00	9	20
200,000	15	39

Step 2

Once this ideal AP number (all Roots) is determined, it needs to be adjusted for mesh performance degradation. The mesh degradation depends heavily upon the number of APs that can be Roots - in other words the number of APs that can be cabled via Ethernet. The more APs that can be cabled as Roots, the more the performance resembles the ideal (best) case. Table 9, shown below, shows the AP Multiplier for a given RAP:MAP ratio.

Table 9. AP multiplier to account for Mesh

RAP:MAP Ratio	AP Multiplier
20%	1.8
40%	1.6
60%	1.5
80%	1.3
100%	1.0

Once the AP multiplier is determined, the formula below is used to calculate the total number of APs required for the site.

FORMULA

Total Number of APs (RAPs and MAPs) Required = #APs (from Table 8) x AP Multiplier (from Table 9)

Using an example to calculate the number of APs for a mesh is useful:

EXAMPLE: Calculate the number of APs required for enterprise grade coverage (10Mbps throughput) in a 100,000 square feet coverage area that is 25% line of sight/ cubicle, 50% dry wall and wood, and 25% concrete and tile.

STEP 1: Use the calculator on the Big Dogs Portal or use Table 8 to calculate the ideal number of APs.

From Table 8 = 20 APs

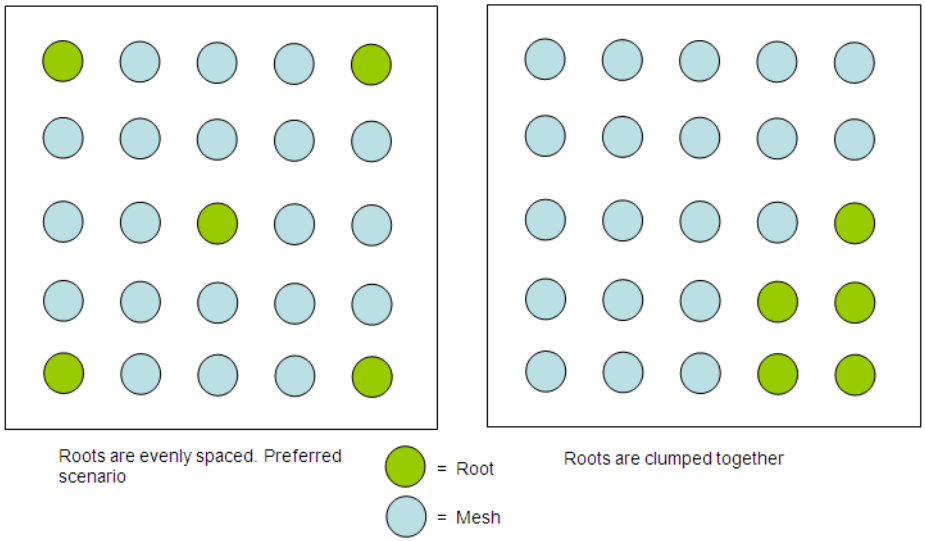
STEP 2: There are only 10 Ethernet drops available due to building considerations and some outdoor coverage requirements. Therefore the RAP:MAP ratio is 10:20, or 50%. Using Table 9, because 50% is between 40% and 60%, the more conservative (higher is more conservative) AP Multiplier of 1.6 is chosen.

# of APs = 20 x 1.6 = 32 APs (10 RAP, and 22 MAP)

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. In the example above, the number of RAPs should be increased from 1 to 2 to meet this best practice.
- More roots are better: As shown in Table 9, the more Roots 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 the Roots are distributed evenly throughout the coverage area (not clumped up close together in one area). Shown in Fig 12 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 out Roots are preferable.

Figure 86. Root Placement



- If the customer's network utilizes a wireless backhaul technology for broadband access, it is recommended to not mount the broadband wireless modem right next to a Ruckus Wireless AP. A distance of 10 feet or more would be desirable.

Signal Quality Verification

The above guidelines for planning will result in a well-designed mesh. However, it is advisable to place the APs in the planned locations temporarily using a tripod stand or other means, and actually checking the Signal Quality throughout the mesh network. In addition, once the mesh is deployed, the Signal Quality should be periodically monitored to make sure the mesh is operating optimally. Signal Quality is a measurement of the link quality of the MAP's uplink, and is available on the ZoneDirector Web interface.

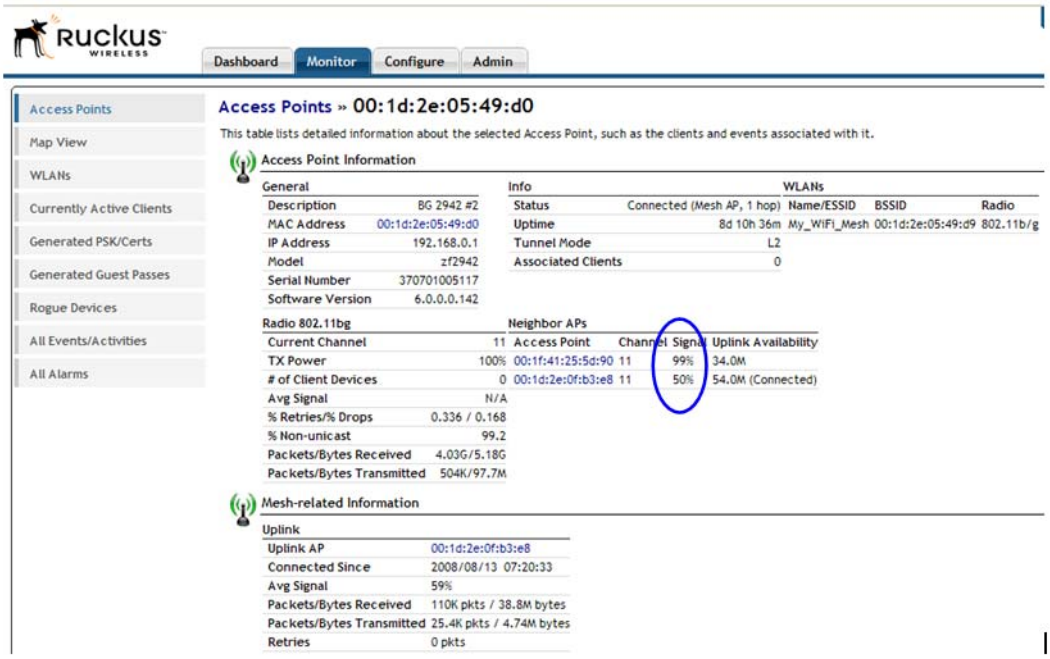
To view the Signal parameter in the Zone Director Web interface, go to the Monitor ' Access Points section, and click on the MAP being tested (click the MAC address) to see the Access Point detail screen, as shown below.

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 exist 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 87. : Check the signal quality from the ZoneDirector Web interface



In the case of the mesh above, both conditions (i) and (ii) are met - the Connected uplink is greater than 25%, and there is a 2nd uplink available as an alternate path, at 99%. Just to clarify why the lower percentage link was chosen over the 99% link, it is because that link is to a root, and the internal mesh algorithm will generally always prefer connection to a root over another MAP.

Mounting and Orientation of APs

There are 5 AP models that support mesh - ZoneFlex 7942, 7942-OT, 2942, 2942-OT, and the 2925. In general, these and other Ruckus Wireless 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.

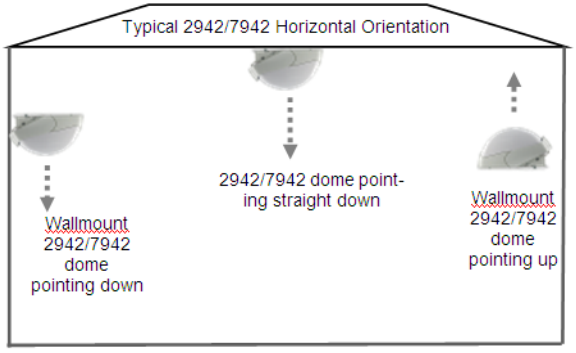
The bottom line regarding orientation and placement is that during the planning phase, it is advisable to use the Signal quality as your benchmark, as explained in the Signal Quality Verification section. Ensure that the Signal is better than 25% for trouble-free operation.

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

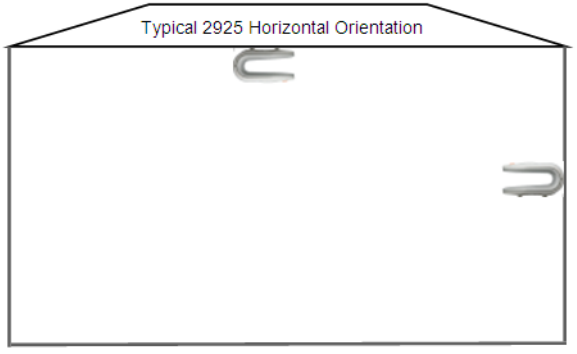
For the ZoneFlex 2942 and ZoneFlex 7942, the APs are typically oriented such that their dome is pointing either straight up or straight down.

Figure 88. : ZoneFlex 2942/7942 Horizontal Orientation



For the ZoneFlex 2925, the AP is typically oriented so that the FCC/CE label, or the S/N and MAC label on the underside of the unit is horizontally oriented, as shown in the figure below.

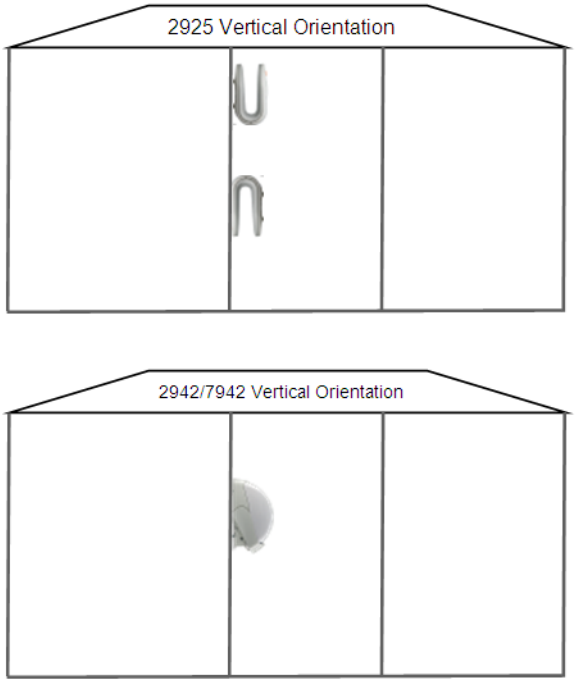
Figure 89. : ZoneFlex 2925 Horizontal Orientation



Indoor APs - Alternate 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 orientation. In such cases, the indoor APs may be mounted vertically, and will still provide good coverage. Examples of vertical mounting are shown in Figure 90.below.

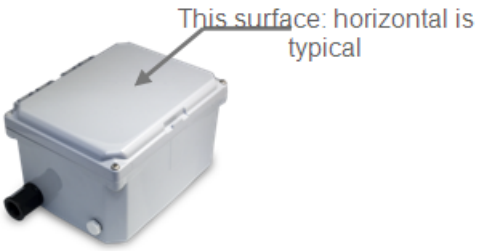
Figure 90. : ZoneFlex 2925 and 2942/7942 Vertical Orientation



Outdoor APs - Typical Horizontal Orientation

There are 2 outdoor AP models that support mesh - 2942-OT, and the 7942-OT. In both cases, a typical orientation is horizontal, as shown in Fig. 11 below. A less typical orientation would be vertically mounted.

Figure 91. : ZoneFlex 2942/7942-OT Outdoor AP 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 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. Make sure you do not have any illegal bridge topologies on your network.
2. Do not mix 802.11n with 802.11g APs in your mesh. They will NOT mesh.
3. Using the formula and example provided, calculate the number of RAPs and MAPs required for your coverage area and bandwidth requirements.
4. Ideally deploy two or more RAPs so there is an alternate path for reliability, even when capacity and coverage only require one RAP.
5. Avoid an excessive number of hops. Ideally keep hop count to 3 or less.
6. Having more Roots is better for performance.
7. Place your Root towards the middle of a coverage area so as to minimize the number of hops to reach a given MAP.
8. For multiple Roots, ensure that the Roots are distributed evenly throughout the coverage area.

9. Once the APs are mounted on a test-basis or permanently, use the Signal quality measurement to ensure that the Connected MAP uplink is 25% or better.
10. Ideally there should be at least one more uplink path for every MAP, and that the alternate path is also 25% or better.

Index

D

E

F

G

H

I

L

M

N

O

P

R

S

T

U

V

W

Z