Ruckus Wireless® ZoneFlex® 2925/2942/7942/7962/2741/7762 Access Point

User Guide

www.ruckuswireless.com

Contents

About This Guide

1 Introducing the ZoneFlex Access Point

2 Installing the Access Point

3 Navigating the Web Interface

4 Configuring the Access Point

5 Managing the Access Point

Index

About This Guide

This guide describes how to install, configure, and manage the Ruckus Wireless® ZoneFlex® 2925/2942/7942/7962/2741/7762 Access Point. 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.

> **i** **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 ZoneFlex Access Point documentation set includes the following:

- *Quick Setup Guide/Getting Started Guide*: Provides essential installation and configuration information to help you get the AP up and running within minutes.
- *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 ZoneFlex 2925/2942/7942/7962/2741/7762 Access Point User Guide
- Part number: 800-70235-001
- Page 88

1

Introducing the ZoneFlex Access Point

Overview of the ZoneFlex Access Point

Congratulations on your purchase of the Ruckus Wireless ZoneFlex Access Point! ZoneFlex Access Points are the industry's first centrally-managed Wi-Fi access points that are capable of extending wireless signals two to four times farther than a conventional access point.

Your ZoneFlex Access Point uses BeamFlex™, a patent-pending antenna technology from Ruckus Wireless that allows wireless signals to navigate around interference, extend wireless signal range, and increase speeds and capacity for wireless networks. The BeamFlex™ antenna system consists of an array of six high-gain directional antenna elements that allow ZoneFlex Access Point to find quality signal paths in a changing environment, and sustain the baseline performance required for supporting data, audio and video applications.

Your ZoneFlex Access Point can be deployed in standalone mode or as part of the ZoneFlex smart WLAN system, in which it can be managed by either FlexMaster or ZoneDirector WLAN controller.

NOTE: For more information on the ZoneFlex system (including FlexMaster and ZoneDirector), BeamFlex, and other Ruckus Wireless technologies, visit www.ruckuswireless.com.

Unpacking the ZoneFlex Access Point

1. Open the Access Point package, and then carefully remove the contents.

2. Return all packing materials to the shipping box, and put the box away in a dry location.

3. Verify that all items listed in Package Contents below are included in the package. Check each item for damage. If any item is damaged or missing, notify your authorized Ruckus Wireless sales representative.

Package Contents

A complete Access Point package contains all of the items listed below:

- ZoneFlex 2925/2942/7942/7962/2741/7762 Access Point
- A 3-foot (0.9 meter) Category 5 Ethernet cable
- A power supply adapter
- A wall mounting kit, with printed instructions
- Software License Agreement/Product Warranty Statement
- A *Quick Setup Guide* for ZoneFlex indoor APs or a *Getting Started Guide* for ZoneFlex outdoor APs

Getting to Know the Access Point Features

This section identifies the physical features of each ZoneFlex Access Point model that is discussed in this guide. Before you begin the installation process, Ruckus Wireless recommends that you become familiar with these features.

- ZoneFlex 2925
- ZoneFlex 2942/7942
- ZoneFlex 7962

NOTE: For information on the physical features of ZoneFlex 2741 and ZoneFlex 7762 outdoor APs, refer to their respective *Getting Started Guide*s.

ZoneFlex 2925

The following illustrations and tables describe the physical features of ZoneFlex 2925.

Front Panel

Figure 1 shows the front view of a ZoneFlex 2925 AP, highlighting the four LED indicators that can be used to assess both device and network status. Refer to Table 3 for information on what the LEDs indicate.

Figure 1.   ZoneFlex 2925 front panel

Refer to Table 4 below for all possible LED states and what they indicate.

Table 3.   ZoneFlex 2925 LED behavior

LED	Description
⏻	• *Off*: No power is available, or the AP is not connected to a power source. • *Green*: The AP is connected to a power source.
‹••›	• *Off*: No link activity is detected • *Yellow*: A 10Mbps-capable device has been detected. • *Flashing yellow*: Data is being exchanged through the WAN port at 10Mbps. • *Green*: A 100Mbps-capable device has been detected. • *Flashing green*: Data is being exchanged through the WAN port at 100Mbps.
📡	• *Off*: No WLAN is enabled. • *Amber*: One of the WLANs is enabled, but no wireless client has associated. • *Green*: At least one wireless client has associated.
☞	• *Off*: There is no network activity; no station detected at the WLAN port • *Amber*: There is a hardware problem affecting the WLAN port. • *Flashing red and green alternately*: A signal is being detected at the WLAN port, but at the lowest level. • *Flashing green*: A moderate signal is being detected at the WLAN port. • *Green*: A strong signal is being detected at the WLAN port.

Rear Panel Features

Figure 2 shows the rear panel of ZoneFlex 2925. For a description of each rear panel part, refer to Table 4.

Figure 2.   ZoneFlex 2925 rear panel
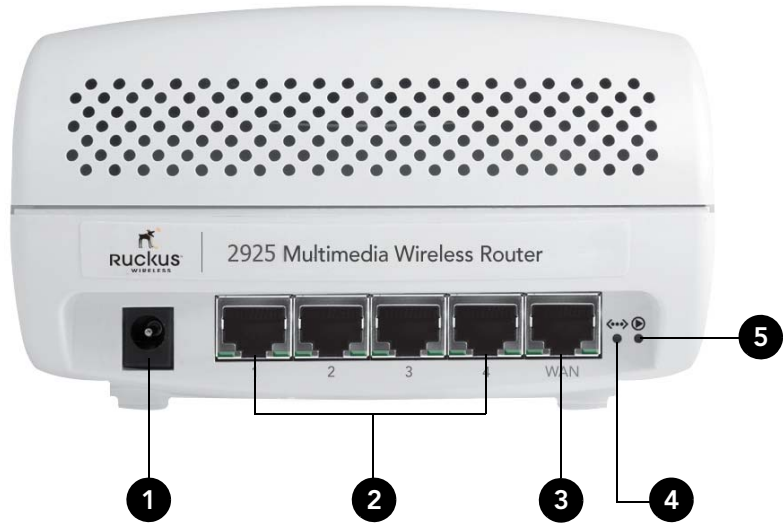
Table 4.   ZoneFlex 2925 rear panel ports, buttons, and connector

Number	Description
1	Connect the power adapter to this socket (Input 12V 1.0A DC or 5V 2.0A DC)
2	Four RJ-45 ports, supporting 10/100Mbps connections
3	One RJ-45 port, dedicated to ISP/broadband source connection
4	OTA (Over the Air) button. Not active in this model at this time.
5	Use to reset AP to "factory default" state. For more information, refer to "Resetting the Access Point to Factory Default" on page 83.

ZoneFlex 2942/7942

The side panel of ZoneFlex 2942/7942 features four LED indicators that can be used to assess both device and network status. The rear view displays the connector panel, which includes the LAN ports and the optional external antenna connection. Refer to the following illustrations and tables to learn more.

Side Panel Features

The ZoneFlex 2942/7942 chassis includes a Kensington lock (on the side of the unit opposite the OPT and DIR LEDs) and a lockable "sliding door" (shown in Figure 3) that hides and protects the rear connector I/O panel and status LEDs. As your AP may be placed in a public location, the lock and door mechanisms can help prevent tampering or theft.

Figure 3.   ZoneFlex 2942/7942 side panel features

Table 5 lists all possible LED states on ZoneFlex 2942/7942 and describes what each LED state means. It also describes how to use the HARD RESET button and other elements on the side panel.

Table 5.   ZoneFlex 2942/7942 side panel elements

Number	LED/Button Name	Description
1	OPT LED	Not used in this model
2	DIR LED	• *Off*: The Access Point is not being managed by ZoneDirector (standalone mode). • *Green*: The Access Point is being managed by ZoneDirector. • *Flashing green*: The Access Point is being managed by ZoneDirector, but is currently unable to communicate with ZoneDirector.
3	AIR LED	• *Green*: The Access Point is functioning as a mesh AP (MAP) and the wireless signal to its uplink MAP is *good* (> 24dbm). • *Fast flashing green (two flashes every second)*: The Access Point is functioning as a mesh AP (MAP) and the wireless signal to its uplink MAP is *poor* (< 24dbm). • *Slow flashing green (one flash every two seconds)*: Mesh networking is enabled, but the Access Point cannot find a mesh uplink. • *Off*: The Access Point is operating in standalone mode or, if mesh networking is enabled, the Access Point is functioning as a root AP (RAP).

Table 5.   ZoneFlex 2942/7942 side panel elements

Number	LED/Button Name	Description
4	WLAN LED	• *Green*: The wireless LAN (WLAN) service is up and at least one wireless client is associated with it. If mesh networking is enabled, there are no downlink MAPs connected to this Access Point. • *Fast flashing green (two flashes every second)*: The WLAN service is up and at least one wireless client is associated with it. Mesh networking is enabled and at least one downlink MAP is connected to this Access Point. • *Slow flashing green (one flash every two seconds)*: The WLAN service is up, but no wireless clients are currently associated with it. Mesh networking is enabled and at least one downlink MAP is connected to this Access Point. • *Amber:* The WLAN service is up, but no wireless clients are currently associated with it. Mesh networking is disabled. • *Off*: Either the WLAN is down, or it is up but no wireless clients are currently associated with it. If mesh networking is enabled, there are no downlink MAPs connected to this Access Point.
5	HARD RESET Button	Pushing and quickly releasing this internal button reboots the AP. Pushing and holding it for six seconds resets the AP to factory defaults.
6	Sliding Door	Protects the ports, buttons, and connector on rear panel
7	Kensington Lock	The Kensington lock feature, located on the opposite side of the unit from the pictured LEDs, is designed to prevent the sliding door from opening, thus locking the unit. The Kensington lock works with a Kensington MicroSaver lock.

Rear Panel Features

Figure 4 shows the rear panel of ZoneFlex 2942/7942. For a description of each rear panel part, refer to Table 6.

Figure 4.   ZoneFlex 2942/7942 rear panel features

⚡ **WARNING:** *For units with Power over Ethernet (PoE).*These products and all inter-connected equipment must be installed indoors within the same building, including the associated LAN connections, as defined by Environment A of the IEEE 802.3af Standard.

⚠ **CAUTION:** The external antenna connectors are for indoor use only. Do not connect them to outdoor antennas.

Table 6.   ZoneFlex 2942/7942 rear panel elements

Number	Item Name	Description
1	Power Adapter Plug	Connect the power adapter to this socket. (Input 110-240V AC, Output 12V 1.0A DC). Power can also be supplied via 10/100 POE port.
2	Lock Hasp	The lock hasp works with a cable or Ruckus mounts. The recommended lock type is Masterlock 120 series (D, T, Q, KAD types).
3	External RP-SMA Connector	• ZoneFlex 2942: One external antenna connector • ZoneFlex 7942: None
4	LAN Ports	• ZoneFlex 2942: Two RJ-45 ports, supporting 10/100 POE (Power over Ethernet) and 10/100Mbps connections. • ZoneFlex 7942: Two RJ-45 ports, supporting 10/100/1000 POE (Power over Ethernet) and 10/100/1000Mbps connections.
5	OPTIONAL Button	Not active in this model at this time.
6	SOFT RESET Button	Use to reset AP. This is a normal reset and does not set AP back to factory defaults.

ZoneFlex 7962

The physical features of ZoneFlex 7962 are very similar to ZoneFlex 2942/7942. It uses the same dome-type chassis with the sliding door and Kensington lock on the side panel. There are slight differences, however, in the side panel and rear panel elements. The following illustrations call out these differences Figure 5 for a photo of the ZoneFlex 7962 side panel.

Side Panel Features

Figure 5 illustrates the side panel features of ZoneFlex 7962. For a description of each rear panel part, refer to Table 7.

Figure 5.   ZoneFlex 7962 side panel

Table 7.   ZoneFlex 7962 side panel elements

Number	LED/Button Name	Description
1	OPT LED	Not used in this model
2	DIR LED	• *Off*: The Access Point is not being managed by ZoneDirector (standalone mode). • *Green*: The Access Point is being managed by ZoneDirector. • *Slow flashing green (one flash every two seconds):* The Access Point is being managed by ZoneDirector, but is currently unable to communicate with ZoneDirector. • *Fast flashing green (two flashes every second):* The Access Point is being managed by ZoneDirector and is currently being receiving configuration settings (provisioning) or a firmware update.
3	2.4G LED (WLAN)	• Green: The wireless LAN (WLAN) service is up and at least one wireless client is associated with it. • Flashing green (two flashes every second): The WLAN service is up and no wireless client is associated with it. • Off: The WLAN service is down.
4	5G LED (WLAN)	• *Green*: The wireless LAN (WLAN) service is up and at least one wireless client is associated with it. • *Flashing green (two flashes every second)*: The WLAN service is up and no wireless client is associated with it. • *Off*: The WLAN service is down.
5	HARD RESET Button	Pushing and quickly releasing this internal button reboots the AP. Pushing and holding it for six seconds resets the AP to factory default settings. *CAUTION! Resetting the AP to factory default settings will erase all settings that you configured previously.*
6	Sliding Door	Protects the ports, buttons, and connector on the rear panel
7	Kensington Lock	The Kensington lock feature, located on the opposite side of the unit from the pictured LEDs, is designed to prevent the sliding door from opening, thus locking the unit. The Kensington lock works with a Kensington MicroSaver lock.

Rear Panel Features

Figure 6 shows the rear panel of ZoneFlex 7962. For a description of each rear panel part, refer to Table 7.

Figure 6.   ZoneFlex 7962 rear panel features

Table 8.   ZoneFlex 7962 rear panel elements

Number	Item Name	Description
1	Power Adapter Plug	Connect the power adapter to this socket. (Input 110-240V AC, Output 12V 1.0A DC). Power can also be supplied via the 10/100/1000 POE port.
2	Lock Hasp	The lock hasp works with a cable or Ruckus Wireless mounts. The recommended lock type is Masterlock 120 series (D, T, Q, KAD types).
3	LAN Ports	Two RJ-45 ports, one for a 10/100/1000 POE (Power over Ethernet) connection and another for a 10/100/1000Mbps connection.
4	OPTIONAL Button	Not active in this model at this time.
5	SOFT RESET Button	Use to reset AP. This is a normal reset and does not set AP back to factory defaults.

If Your AP is Part of a Wireless Mesh Network

A wireless 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 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.

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 ZoneFlex access points.

> **NOTE:** There are no mesh-related configuration settings on your AP. Mesh settings are all configured on ZoneDirector.

If you deployed your ZoneFlex AP as part of a wireless mesh network, you can check the LEDs on the AP to determine its mesh status. The two LEDs on the ZoneFlex AP that indicate 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

> **NOTE:** ZoneFlex 7962 with software version 8.0 does not support mesh networking.

> **NOTE:** For information on the LED behaviors of ZoneFlex 2741 and ZoneFlex 7762 outdoor APs when operating in standalone mode or when it is part of a mesh network, refer to their respective *Getting Started Guides*.

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.

Table 9.   WLAN/Wireless Device Association LED behavior

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

Table 9.   WLAN/Wireless Device Association LED behavior

LED Color/Behavior	Root AP / Mesh AP
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

*Figure 7.   WLAN/Wireless Device Association LED on ZoneFlex 2942/7942 (left)
and ZoneFlex 2925 (right)*

Air/Signal Quality LED

Table 10.   Air/Signal Quality LED behavior

LED Color/Behavior	Root AP	Mesh AP
Green	N/A	• Connected to a Root AP or another Mesh AP, and; • Signal quality is good
Fast blinking green	N/A	• Connected to a Root AP or another Mesh AP, and; • Signal quality is fair

Table 10. Air/Signal Quality LED behavior

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

Figure 8. Air/Signal Quality LED on ZoneFlex 2942/7942 (left) and ZoneFlex 2925 (right)

2

Installing the Access Point

Before You Begin

Before starting with the installation, make sure that you have the required items for the installation ready. In addition, verify that the wireless stations on the network have the required components for wireless communication with the Access Point.

This section describes the pre-installation tasks that you need to perform.

Prepare the Required Hardware and Tools

You must supply the following tools and equipment:

- A notebook computer running on Windows XP/2000 and installed with one wireless 802.11a/b/g/n network card and one Ethernet card
- A modem (DSL or cable), E1/T1 router, or other device provided by your Internet Service Provider, that brings Internet access to your site
- (Optional) A network switch or a DSL/Internet gateway device.

NOTE: If the AP is deployed with ZoneDirector, follow the instructions in the *Zone-Director Quick Setup Guide*, and connect the AP to your Ethernet network.

Perform a Site Survey

Before installing the Access Point, perform a site survey to determine the optimal Access Point placement or maximum range, coverage, and network performance. When performing a site survey, consider the following factors:

- *Data rates*: Range is generally inversely proportional to data rates. The maximum radio range is achieved at the lowest workable data rate. Higher data rates will generally be achieved at closer distances.

- *Antenna type and placement*: Proper antenna configuration is a critical factor in maximizing radio range. As a general rule, radio range is increased by mounting the radio higher off of the ground with the Access Point oriented so that the dome is facing down (for recommended orientation examples, refer to Figure 9 on page 19). If you are connecting an external antenna to the Access Point, mount the Access Point so that the external antenna is pointing down.

- *Physical environment*: Clear or open areas provide better radio range than closed or filled areas. The less cluttered the operating environment, the greater the wireless range.

- *Obstructions, building materials, and sources of interference*: Physical obstructions, such as concrete pillars, steel beams, and filing cabinets, can block or hinder wireless communication. Avoid installing the Access Point in a location where there is an obstruction between sending and receiving devices. A number of machines and electronic devices that emit radio waves – cranes, wireless phones, microwave ovens, satellite dishes – interfere with and block wireless signals. Building materials used in construction also influence radio signal penetration. For example, drywall construction permits greater range than concrete blocks.

For more Access Point placement guidelines, refer to "Determine the Optimal Mounting Location and Orientation".

Determine the Optimal Mounting Location and Orientation

The location and orientation that you choose for the Access Point play a critical role in the performance of your wireless network. In general, Ruckus Wireless recommends installing the Access Point away from obstructions and sources of interference and ensuring that the Access Point's dome is pointing in the general direction of its wireless clients.

Figure 9.   Recommended orientation for maximum horizontal plane coverage
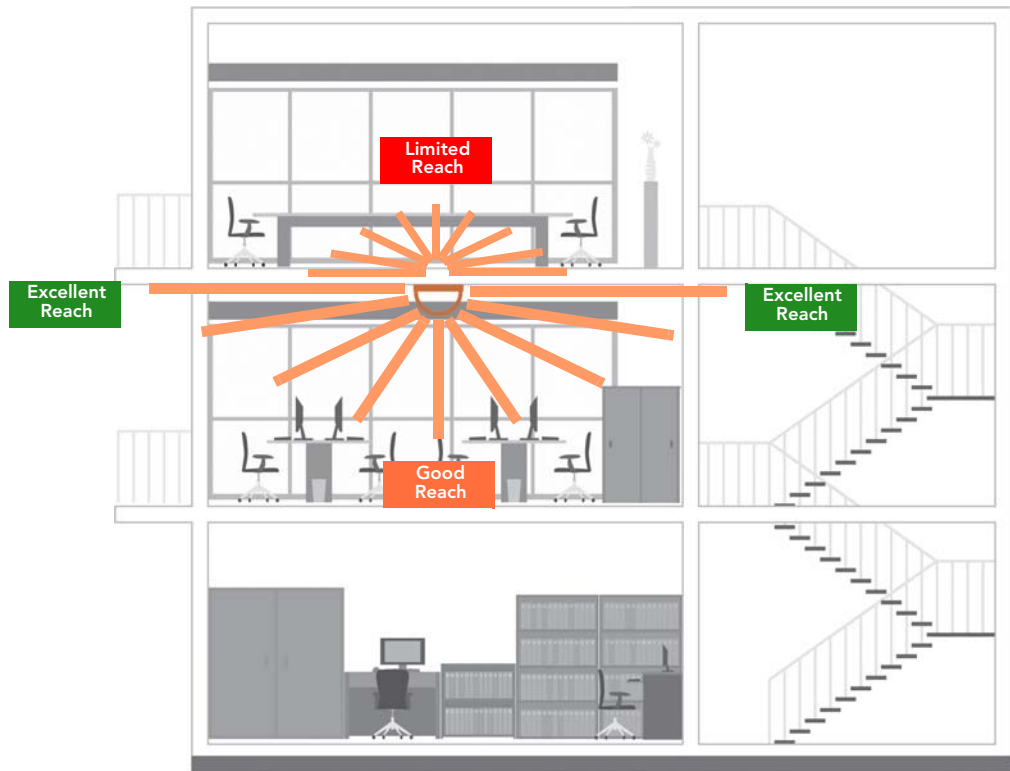
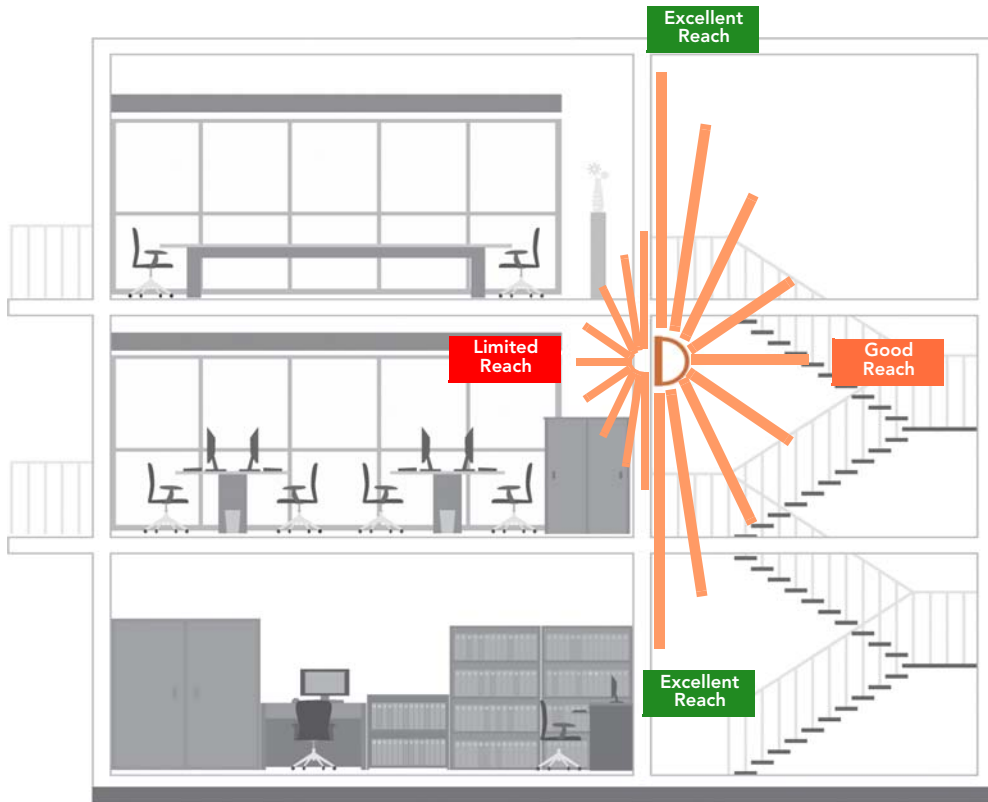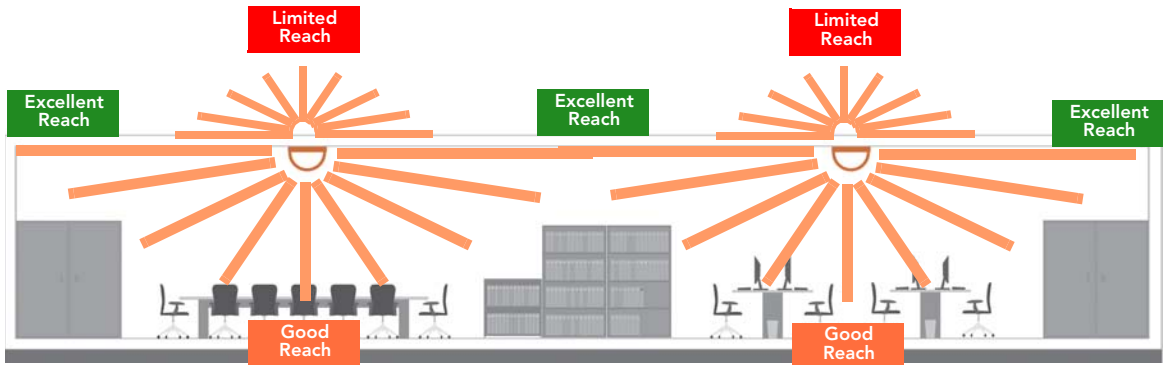*Figure 10.   Recommended orientation for maximum vertical plane coverage*

Figure 11.   Recommended orientation for maximum mesh coverage

Step 1: Preconfigure the Access Point

The procedure for completing the Access Point's essential configuration depends on whether you want it to be managed by either ZoneDirector or FlexMaster or to operate as a standalone access point. Refer to the section that is relevant to your deployment:

- Configuring for Management by ZoneDirector
- Configuring for Standalone Operation or for Management by FlexMaster

Configuring for Management by ZoneDirector

If ZoneDirector is installed on the network, you can configure the Access Point for management by ZoneDirector. Simply connect the Access Point to same Layer 2 subnet as ZoneDirector. When the Access Point starts up, it will discover and register with ZoneDirector automatically.

NOTE: In addition to using Layer 2 auto discovery to enable the Access Point to register with ZoneDirector, you can also use DHCP Option 43 or DNS. For more information, refer to the *ZoneDirector User Guide*.

CAUTION: 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.

Before starting this procedure, check the back panel of the Access Point (above the recess where the bottom connectors are located), and then write down the MAC address of the Access Point. You will need the MAC address to identify the Access Point on the ZoneDirector Web interface.

What You Will Need

Before starting with the configuration task, make sure that you have the following requirements ready:

- A computer from which you can access the ZoneDirector Web interface
- Mozilla Firefox 2.0 (or later) or Microsoft Internet Explorer 6.0 (or later) installed on the administrative computer
- One Ethernet cable
- Your *ZoneFlex Access Point* and the supplied power adapter

1. Connect the Access Point to a Power Source

1. Connect the power jack to the power connector on the rear panel of your ZoneFlex Access Point.
2. Connect the power adapter to a power source.
3. Verify that the power LED on the Access Point is green.

You have completed connecting the Access Point to a power source.

2. Connect the Access Point to the Same Subnet as ZoneDirector

1. Connect one end of an Ethernet cable to a LAN (RJ-45) port on the rear panel of the Access Point.

i NOTE: If you are using ZoneFlex 2925 AP, make sure you connect the Ethernet cable to one of the four LAN ports (not the WAN port).

2. Connect the other end of the Ethernet cable to the same Layer 2 subnet as ZoneDirector. The same Layer 2 subnet means that there should not be any router between the Access Point and ZoneDirector.
3. Log into the ZoneDirector Web interface, and then go to the **Monitor** > **Access Points** page.
4. Look for the MAC address of the Access Point, and then check its **Status** column.
   - If automatic approval is enabled, the Status column should show **Connected**.
   - If automatic approval is disabled, click the **Allow** link that is on the same row as the Access Point's MAC address. This allows the Access Point to register with ZoneDirector.

When the Status column shows **Connected**, this indicates that the Access Point has successfully registered with ZoneDirector and that it can now be moved to its destination Layer 2 or Layer 3 network.

3. Disconnect the Access Point from the Power Source

1. Disconnect the Access Point from the power source.

2. Verify that the power LED on the rear panel of the Access Point is off.

3. Continue to .

Configuring for Standalone Operation or for Management by FlexMaster

This section describes the steps you need to complete to set up the AP in standalone mode or to be managed by Ruckus Wireless FlexMaster, if you have one installed on the network.

What You Will Need

Before starting with the configuration task, make sure that you have the following requirements ready:

- An administrative computer (notebook computer) running on Microsoft Windows Vista/XP/2000
- Mozilla Firefox 2.0 (or later) or Microsoft Internet Explorer 6.0 (or later) installed on the administrative computer
- One 5.6mm-6.0mm (outside diameter) Cat5e foil screened twisted pair (FTP) solid cable
- Two Ethernet cables

1. Prepare the Administrative Computer

NOTE: The following procedure is applicable if the administrative computer is running on Windows XP or Windows 2000. If you are using a different operating system, refer to the documentation that was shipped with your operating system for information on how to modify the computer's IP address settings.

1. On your Windows XP or Windows 2000 computer, open the **Network Connections** (or **Network and Dial-up Connections**) control panel according to how the Start menu is set up:
   - On Windows XP, click **Start** > **Control Panel** > **Network Connections.**
   - On Windows 2000, click **Start** > **Settings** > **Network Connections**.

2. When the Network Connections window appears, right-click the icon for Local Area Connection, and then click **Properties**.

> **i** > **NOTE:** Make sure that you configure the Local Area Connection properties, not the Wireless Network Connection properties.

3. When the **Local Area Connection Properties** dialog box appears, select **Internet Protocol (TCP/IP)** from the scrolling list, and then click **Properties**. The **Internet Protocol (TCP/IP) Properties** dialog box appears.

4. Write down all of the currently active network settings. You will need this information later when you restore your computer to its current network configuration.

5. Click **Use the following IP address**, and then configure the IP address settings with the values listed in Table 11. For a sample configuration, refer to Figure 12.

Table 11.   Configure your computer's IP address settings

IP address	192.168.0.22 (or any address in the 192.168.0.x network—with the exception of 192.168.0.1, which is the default IP address assigned to the Access Point)
Subnet mask	255.255.255.0
Default gateway	192.168.0.1
Preferred DNS server	192.168.0.1

You can leave the **Alternate DNS server** box blank.

6. Click **OK** to save your changes and close the TCP/IP Properties dialog box.

7. Click **OK** again to close the Local Area Connection Properties dialog box.

Windows saves the IP address settings that you have configured.

Figure 12.   *Sample configuration in the Internet Protocol (TCP/IP) Properties dialog box*
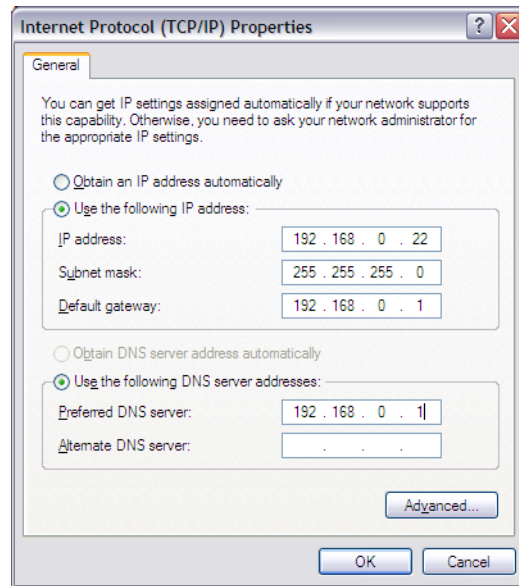
2. Connect the Access Point to the Administrative Computer

1. Connect one end of an Ethernet cable to an Ethernet port on the Access Point, and then connect the other end to the administrative computer's Ethernet port.

2. Take out the supplied power adapter from the AP package, connect the power jack to the AC connector on the rear panel of the AP, and then plug in the adapter to a power source. After a minute, the power LED on the AP turns solid green.

You have completed connecting the AP to the administrative computer.

3. Log Into the Access Point's Web Interface

1. On the administrative computer, open a Web browser window.

2. In the address or location bar, type the following address:

   `https://192.168.0.1`

3. Press <Enter> on the keyboard to connect to the Access Point's Web interface. A security alert message appears.

4. Click **Yes** or **OK** (depending on the browser) to continue. The Access Point's login page appears.

Figure 13.   The ZoneFlex Access Point login page
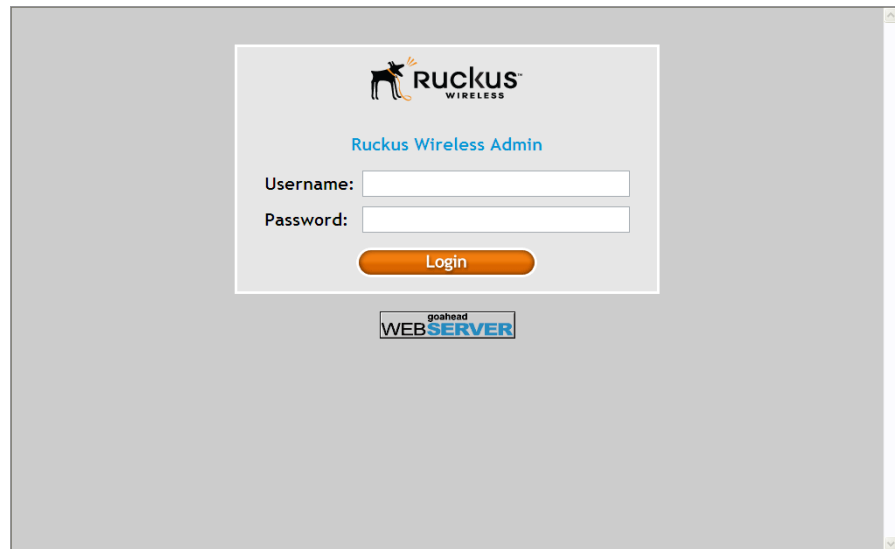
5. In **User name**, type super.

6. In **Password**, type sp-admin.

7. Click **Log In**. The Web interface appears, displaying the Device page.

8. Continue to "4. Configure the Wireless Settings" below.

4. Configure the Wireless Settings

To complete this step, you will need to configure the settings on the **Common** tab and at least one **Wireless #** tab. These are the essential wireless settings that will enable wireless devices on the network to associate with the Access Point.

For your reference, the default wireless settings on the Access Point are listed in Table 12.

Table 12.   Default wireless settings

Setting	Default Value
SSID (network name)	Wireless 1 to Wireless 8 (8 WLANs)
Encryption (security)	Disabled on all WLANs
Default management IP address	192.168.0.1

Configure Common Wireless Settings

1. On the left menu of the Web interface, click **Configuration** > **Wireless**. The Common page appears.

NOTE: ZoneFlex 7962/7762 AP has two radios (2.4GHz and 5GHz) that need to be configured separately on the Web interface. To configure the common wireless settings, click **Configuration** > **Radio 2.4G** or **Radio 5G**. The rest of the configuration procedures are the same as the other models.

---

2. Verify that the common wireless settings are configured as listed in Table 13.

Table 13.   Common wireless configuration

Setting	Recommended Value
Wireless Mode	Auto-select
Channel	SmartSelect
Country Code	• If you purchased the Access Point in the United States, this value is fixed to **United States** at the factory and is not user configurable. • If you purchased the Access Point outside the United States, verify that the value is set to your country or region. Selecting the correct country code ensures that the Access Point uses only the radio channels allowed in your country or region. *Note for ZoneFlex 7962/7762 AP users: The two radios on ZoneFlex 7962/7762 AP are always configured with the same country code setting. If you change the country code for Radio 1, for example, the same change will be applied automatically to Radio 2.*

3. If you made any changes to the **Common** tab, click **Update Settings**.

4. Continue to "Configure Wireless # Settings" below.

Figure 14. The Configuration > Wireless > Common tab
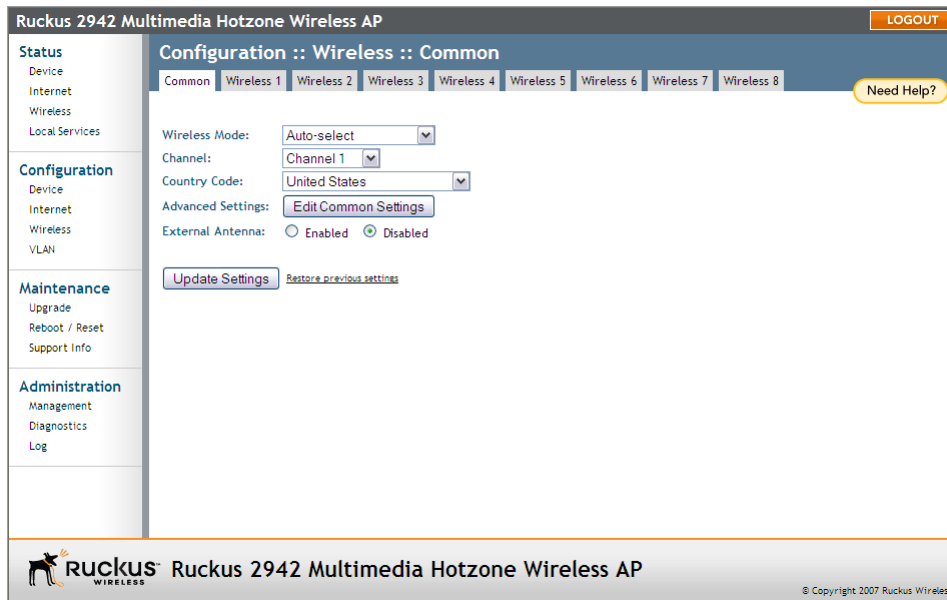
Configure Wireless # Settings

1. Click one of the **Wireless #** tabs.

2. In **Wireless Availability**, click **Enabled**.

3. In **Broadcast SSID**, click **Enabled**.

4. Clear the **SSID** box, and then type a unique and descriptive name that you want to call this wireless network.

   For example, you can type `Ruckus Wireless AP`. This SSID is the name that will help users identify this wireless network in their wireless network connection application.

> **NOTE:** You may also configure other wireless settings on this and other **Wireless #** tabs (in addition to the settings described above), although it is not necessary for completing the Access Point installation.

5. Click **Update Settings**.

You have completed configuring the basic wireless settings of the Access Point.

Figure 15.   The Configuration > Wireless > Wireless 1 tab
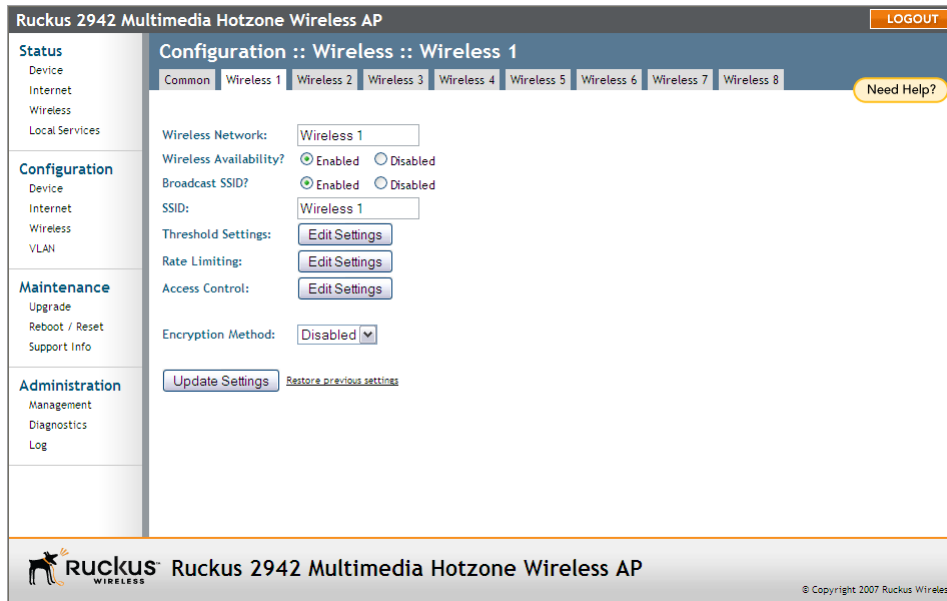
(Optional) Set the FlexMaster Server Address

If you have a FlexMaster server installed on the network and you intend to use FlexMaster to manage the Access Point, you can set the FlexMaster server address at this point. Before starting this procedure, make sure you obtain the correct FlexMaster server URL.

> **NOTE:** In addition to setting the FlexMaster server URL manually on the Access Point, you can also use DHCP Option 43 or DNS to point the Access Point to the FlexMaster server. For more information, refer to the *FlexMaster User Guide.*

1. On the menu, click **Administration** > **Management**.

2. Scroll down the page to the **TR069 / SNMP Management Choice** section.

3. Verify that the **Auto** option is selected.

4. In **FlexMaster Server URL**, type the URL of the FlexMaster server on the network. You can use either `http` or `https` to connect to the URL and include either the host name or IP address of the FlexMaster server in the URL. The following are examples of valid FlexMaster server URLs:

   ```
   http://flexmaster/intune/server
   https://flexmaster/intune/server
   http://192.168.20.1/intune/server
   https://192.168.20.1/intune/server
   ```
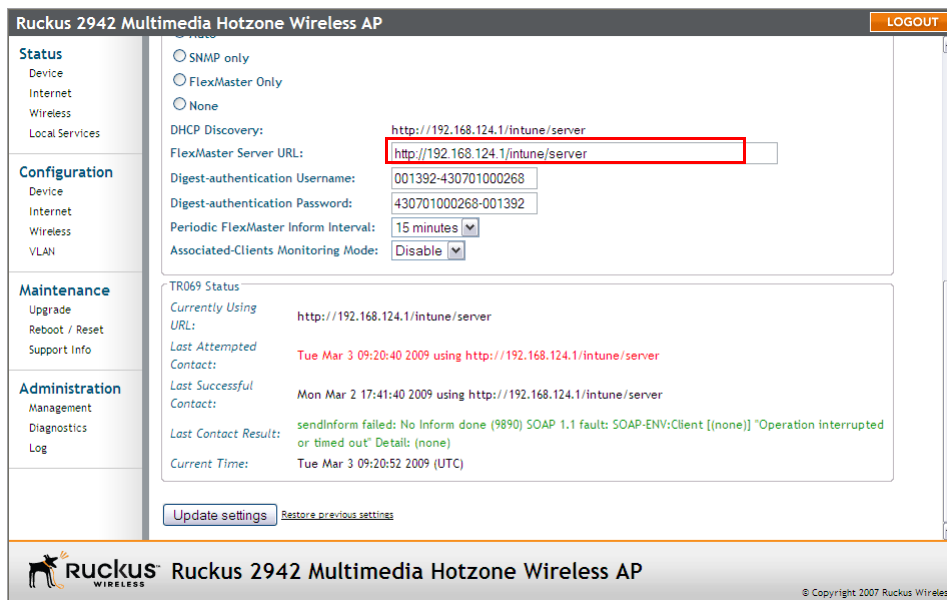
5. Click **Update Settings** to save your changes.

You have completed setting the FlexMaster server address on the Access Point.

Figure 16.   Type the FlexMaster server URL

NOTE: Instructions on how to verify that the Access Point and FlexMaster can communicate with each other are provided in "Check the TR069 Status (FlexMaster Management Only)" on page 33.

5. Disconnect the Access Point from the Administrative Computer

1. Disconnect the Access Point from the power source.

2. Verify that the power LED on the Access Point is off.

3. Disconnect the Ethernet cable from the administrative computer's Ethernet port.

6. Restore the Administrative Computer's Network Settings

1. On your Windows XP or Windows 2000 computer, open the **Network Connections** (or **Network and Dial-up Connections**) control panel according to how the Start menu is set up:

- On Windows XP, click **Start** > **Control Panel** > **Network Connections.**
- On Windows 2000, click **Start** > **Settings** > **Network Connections**.

2. When the Network Connections window appears, right-click the icon for **Local Area Connection**, and then click **Properties**.

3. When the **Local Area Connection Properties** dialog box appears, select **Internet Protocol (TCP/IP)** from the scrolling list, and then click **Properties**. The **TCP/IP Properties** dialog box appears.

4. Restore the computer's network settings by typing the original IP address settings in the **TCP/IP Properties** dialog box.

5. On the **TCP/IP Properties** dialog box, click **OK** to close it.

6. Click **OK** again to close the **Local Area Connection Properties** dialog box.

You are now ready to connect the Access Point to your network.

Step 2: Verify Access Point Operation

Before deploying the Access Point to your environment, Ruckus Wireless strongly recommends that you verify that the Access Point is operating correctly. To do this, you will need to connect the Access Point to your live network temporarily and make sure that the network connection works and that wireless clients are able to associate with the Access Point and connect to your network and the Internet.

NOTE: The network and power connections that you will be making in this step are temporary. You can perform these verification tasks indoor.

Connect the Access Point to the Network

1. Connect the Ethernet cable from a LAN (RJ-45) port on the Access Point to your network's router or switch.

2. Reconnect the Access Point to a power source.

You have completed connecting the Access Point to your live network. Perform the tasks described in the following sections to verify that the Access Point is operating normally.

Check the LEDs

Perform a spot-check using the LEDs to verify that the Access Point is operating normally. Refer to the following sections for information on how to check the LEDs on each ZoneFlex AP model.

ZoneFlex 2925

If the Access Point is operating normally and your wireless client was able to associate with it:

- The ☼ LED is green.
- The 👍 LED is green, and if traffic if passing through, it flashes green. Open a Web browser window, type www.ruckuswireless.com in the address bar, and then press <Enter>. The 👍 LED should flash green as your wireless client connects to the Ruckus Wireless Web site through the Access Point.
- The 📶 LED is green. This indicates that at least one wireless client is connected to the Access Point's WLAN service.

ZoneFlex 2942/7942

If the Access Point is operating normally and your wireless client was able to associate with it:

- The **WLAN** LED is green, and if traffic if passing through, it flashes green. Open a Web browser window, type www.ruckuswireless.com in the address bar, and then press <Enter>. The **WLAN** LED should flash green (two flashes every second) as your wireless client connects to the Ruckus Wireless Web site through the Access Point.
- If you do not have Ruckus Wireless ZoneDirector on the network, the **DIR** LED is off. This indicates that the Access Point is operating in standalone mode. If there is a ZoneDirector device on the network, the **DIR** LED is green.

ZoneFlex 7962

If the Access Point is operating normally and your wireless client was able to associate with it:

- The **2.4G** or **5G** LED is green, and if traffic if passing through, it flashes green. Open a Web browser window, type www.ruckuswireless.com in the address bar, and then press <Enter>. The **2.4G** or **5G** LED should flash green (two flashes every second) as your wireless client connects to the Ruckus Wireless Web site through the Access Point.
- If you do not have Ruckus Wireless ZoneDirector on the network, the **DIR** LED is off. This indicates that the Access Point is operating in standalone mode. If there is a ZoneDirector device on the network, the **DIR** LED is green.

ZoneFlex 7762

If the Access Point is operating normally and no wireless clients are associated with it:

- The **Power** LED is green.
- The **Status** LED shows slow blinking amber. This indicates that there are no wireless clients connected to the Access Point's WLAN service.

Associate a Wireless Client with the Access Point

1. On the administrative computer, verify that the wireless interface is enabled. On Windows XP, click **All Programs** > **Connect To** > **Wireless Network Connection** to enable the wireless interface.

2. In the system tray, right-click the (Wireless Network Connection) icon, and then click **View Available Wireless Networks**.

3. In the list of available wireless network, click the network with the same SSID as you configured in <u>"Configure Wireless # Settings"</u> on <u>page 28</u>. For example, if you set the SSID to Ruckus Wireless AP, click the wireless network named **Ruckus Wireless AP**.

4. Click **Connect**.

Your wireless client connects to the wireless network. After the wireless client connects to the wireless network successfully, the wireless client icon in the system tray changes to .

Check the TR069 Status (FlexMaster Management Only)

If you configured the Access Point to report to a FlexMaster server on the network, make sure you verify that it can successfully communicate with the FlexMaster server. You can do this by checking the TR069 status on the Access Point's Web interface.

1. Log in to the Access Point's Web interface.

2. Go to the **Administration** > **Management** page.

3. Scroll down to the **TR069 Status** section.

4. Check the value for **Last successful contact**. If it shows a date in green, this indicates that the Access Point was able successfully communicate with Flex-Master.

Disconnect the Access Point from the Network

1. Disconnect the Access Point from the power source.

2. Disconnect the Ethernet cable that runs to the Access Point's RJ45 port from your network's router or switch.

You are now ready to deploy the Access Point to its permanent mounting location.

Step 3: Deploy the Access Point

In this step, you will place the Access Point in a suitable location on the network and connect it to a power source and to your network environment.

1. Choose a Location for the Access Point

You can install the Access Point on a flat surface (for example, on a desktop or tabletop) or mount it on a wall or ceiling. When choosing a location for the Access Point, follow these guidelines:

- Allows easy viewing of the LEDs and access to the connectors, if necessary.
- Is centrally located to the wireless clients that will be connecting to the Access Point. A suitable location might be on top of a cabinet or similar furniture to optimize wireless connections to clients in both horizontal and vertical directions, allowing wider coverage.

When positioning your Access Point, ensure that:

- It is out of direct sunlight and away from sources of heat.
- Cabling is away from power lines, fluorescent lighting fixtures, and sources of electrical noise such as radios, transmitters and broadband amplifiers.
- There are no thick walls or metal shielding between the Access Point and the wireless stations.
- Water or moisture cannot enter the case of the unit.
- Air flow around the unit and through the vents in the side of the case is not restricted.

Review the recommendations in "Determine the Optimal Mounting Location and Orientation" on page 19 for help in choosing a suitable location for the Access Point.

2. Connect the Access Point to a Power Source and the Network

Once you have placed the Access Point at its installation location, you are ready to connect it to a power source and the network.

NOTE: If your ZoneFlex model supports PoE, you can also supply power to the AP from a PoE switch or injector. For information on how to make the PoE connections, refer to the documentation that was shipped with the PoE switch or injector.

1. Connect the power jack to the power connector on the rear panel of your ZoneFlex Access Point.
2. Connect the power adapter to a power source.
3. Obtain an Ethernet cable that is long enough to connect the Access Point to your network's router, switch, or hub.

4. Connect one end to a LAN port on the AP, and then connect the other end to your network's router, switch, or hub.

5. Verify that the power LED on the Access Point is green.

Congratulations! You have completed setting up the Access Point on your network. To learn how to configure and manage the Access Point, continue reading the next chapters.

Troubleshooting Installation

If the startup sequence does not work, verify that the network name (SSID) and security settings (if you enabled it) on the AP match the settings on your wireless device.

- Disconnect the AP from the power source, wait 5 seconds, then reconnect it—and wait 60 seconds before attempting a reconnection.
- Disconnect and reconnect the AP and the PC.
- Replace the Ethernet cable with a new one if the relevant LAN port LED is not illuminated. (LEDs in each port light up during a successful connection.)

If all else fails, you can reset the AP to the factory defaults (and start over).

1. Insert a straightened-out paper clip into the reset button hole (located on the back of the AP.)

2. Press and hold the **Reset** button for at least eight (8) seconds.

You can now reconnect your computer directly to the AP (as described in "2. Connect the Access Point to the Administrative Computer" on page 25), and then start over with installation, using the default network settings.

3

Navigating the Web Interface

Logging Into the ZoneFlex Web Interface

If you need to manage your AP, you do it with the features of the Ruckus Wireless Web interface (which you already used to set up the AP for use).

i **NOTE:** The following procedure assumes that you know the static IP address of the AP (now in use), or you have some means of determining the dynamic IP address in use by the AP. The PC you use for AP administration should be on the management VLAN.

To log into the Web interface

1. On the PC, open a Web browser window.

2. In the address or location bar, type the IP address of the AP. Be sure to enter it in the format:

   `https://<ip_address>`

3. Press <Enter> to connect to the Web interface.

4. If a Windows security alert dialog box appears, click **OK/Yes** to proceed. The Ruckus Wireless Admin login page appears.

5. In **Username**, type `super`.

6. In **Password**, type `sp-admin`.

7. Click **Login**.

The ZoneFlex Access Point Web interface appears.

Navigating the Web Interface

You manage the Access Point through a Web browser-based interface that you can access from any computer that is on the same subnet as the Access Point. Table 14 lists the Web interface features that are identified in Figure 17.

Figure 17.   Elements of the ZoneFlex AP Web Interface
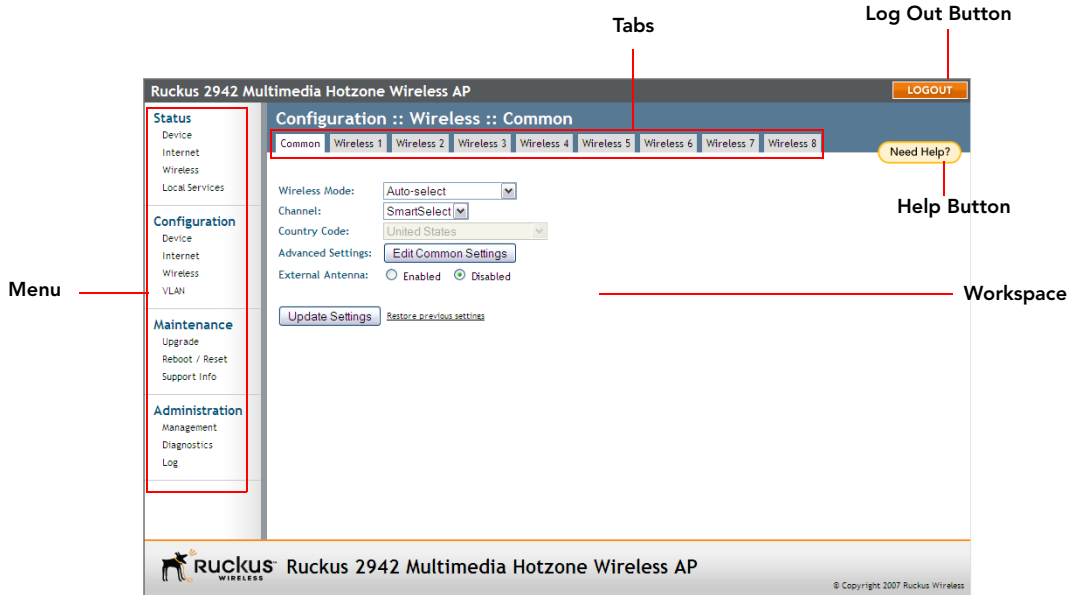
Table 14.   ZoneFlex AP Web interface elements

Element	Description
Menu	Under each category (Status, Configuration, etc.) are options that, when clicked, open the related workspace in the area to the right.
Tabs	Contains additional options for the configuration page. For example, the **Configuration** > **Wireless** page includes one tab for common wireless configuration and eight tabs for each of the available WLANs.
Workspace	This large area displays features, options and indicators relevant to your menu bar choices.
Logout Button	Click this button to log out of the AP.
Help Button	Click this button to open a help window with information related specifically to the options currently displayed in the workspace.

If You Are Using ZoneFlex AP 7962/7762

If your ZoneFlex AP model is 7962/7762, note that elements on the Web interface menu are slightly different from the other ZoneFlex AP models (and what this guide shows).

ZoneFlex 7962/7762 AP has one 2.4GHz radio (for 802.11b/g/n clients) and one 5GHz radio (for 802.11a/n clients). The wireless settings for these two radios need to be configured separately, which is why the ZoneFlex 7962/7762 AP Web interface has the **Radio 2.4G** and **Radio 5G** menu items, instead of a single **Wireless** menu item in other models.

Figure 18 highlights the differences between the ZoneFlex 7962 and ZoneFlex 2942 menus.

Figure 18.   Menu items are slightly different in ZoneFlex 7962 AP (left) and the other ZoneFlex AP models (right)
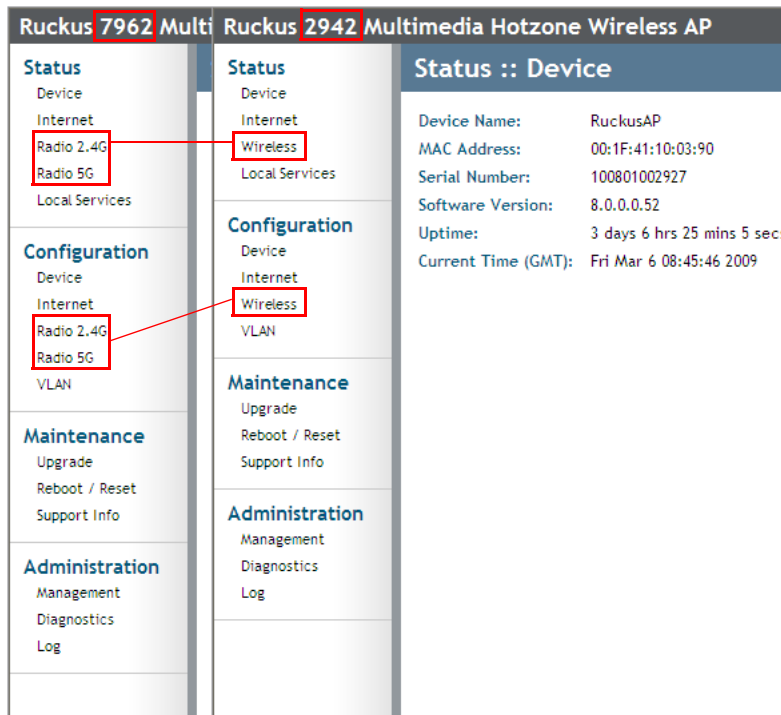
Navigating the Web Interface
If You Are Using ZoneFlex AP 7962/7762

4

Configuring the Access Point

Configuring the System Settings

The system settings refer to the device name, temperature update, and service provider login settings.

1. Go to **Configuration** > **Device**. The Configuration :: Device page appears.

2. In **Device Name**, type a new name for the device or leave as is to accept the default device name (`RuckusAP`). The device name identifies the AP among other devices on the network.

3. In **Device Location**, type the address or location where the device is deployed.

4. In **GPS Coordinates**, type the latitudinal and longitudinal coordinates of the device location.

5. In **Temperature Update**, specify how often you want the AP to update its temperature information on the Status > Device page. The default update interval is 30 seconds.

6. Under **Service Provider Login**, change the login information as required:
   - **Username**: Type the name that you want to use for logging into the Web interface. The default user name is `super`.
   - **Current Password**: Type the current administrative password. The default administrative password is `sp-admin`.
   - **New Password**: Type the new password that you want to use. The password must consist of six to 32 alphanumeric characters only.
   - **Confirm Password**: Retype the new password to confirm.

7. Click **Update Settings** to save and apply your changes.

Figure 19.   The Configuration > Device page
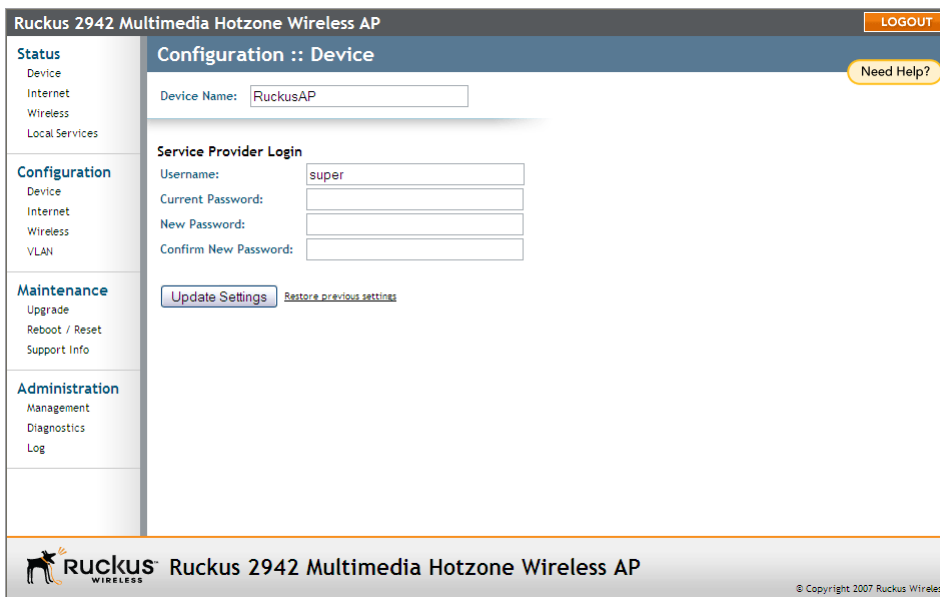
Enabling the PoE OUT Port for ZoneFlex 7762 Outdoor AP

If you are using the supplied Ruckus Wireless PoE injector for 7762 AP (and power adapter) to supply power to the AP, you can use **PoE OUT** port to supply PoE to any PoE-capable device (for example, another ZoneFlex 7762 AP or an IP-based surveillance camera). The PoE feature for the PoE OUT port needs to be enabled from the Web interface.

NOTE: If you use DC power or a PoE injector other than the one supplied with the AP, the AP will be operational but some features (such as the built-in heater and PoE for the **PoE OUT** port) will be unavailable. See Table 15 below for more information.

To enable PoE for the PoE OUT port

1. On the menu, click **Configuration** > **Device**.

2. In **Power Source**, select the **Use custom PoE injector** check box.

3. Click **Update Settings** to save your changes.

You have completed enabling PoE for the **PoE OUT** port.

Figure 20.   Select the Use custom PoE injector check box

In addition to the supplied Ruckus Wireless PoE injector for ZoneFlex 7762 AP, you can also use DC power or a standard 802.3af/802.3at PoE injector to supply power to the AP. Note, however, that some features (specifically, the built-in heater and PoE for the PoE OUT port) will be unavailable if the supplied PoE injector is not used. Refer to Table 15 for the available power options and the limitations associated with each option.

Table 15.   Power configuration options

Power Input	Operational AP	Heater	PoE for PoE OUT
Ruckus Wireless PoE injector for ZoneFlex 7762 AP (with supplied power adapter)	Yes	Yes	Yes
48V 802.3at	Yes	Yes	No
48V 802.3at	Yes	Yes	Class of power supplied with restrictions
48V 802.3af	Yes	No	No
12V DC	Yes	No	No

> **i** ⊳ **NOTE:** If the built-in heater is disabled, the lowest operating temperature that the Access Point can support is -20° C.

Configuring Network Settings

This section describes how to view and configure the AP's network settings. Topics discussed include:

Default IP Addressing Behavior

By default, the AP is configured to automatically obtain an IP address from a DHCP server on the network. If the AP does not detect a DHCP server, it automatically assigns itself the static IP address `192.168.0.1` to make it easier for you to preconfigure and deploy it your network.

Obtaining and Assigning an IP Address

There are at least two instances when you would change the IP address of the AP:

- If the current AP IP address consistently conflicts with that of any other device in your network
- If you want to switch to a static IP address from DHCP, for use in managing or maintaining the AP

Unless you are able to determine the IP address assigned by the DHCP server to the AP, it may prove helpful for anyone needing administrative access to assign a static IP address to the AP.

Figure 21.   The Configuration > Internet page
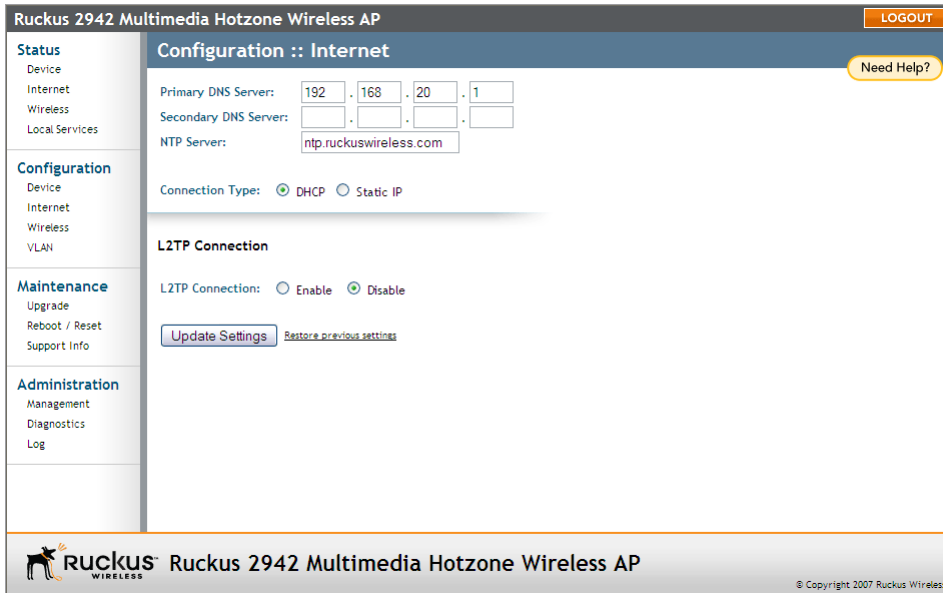
To review and modify the network configuration

1. Go to **Configuration** > **Internet**. The Internet page appears.

2. Verify that **Connection Type** is set to **Static IP**.

3. When the Static IP options appear, you can changes to the following settings:
   - **Gateway**: This is the gateway IP address of the Internet interface.
   - **Primary DNS Server**: The IP address of the primary Domain Name System (DNS) server.
   - **Secondary DNS Server**: The IP address of the secondary Domain Name System (DNS) server.
   - **NTP Server**: Hostname of the Network Time Protocol (NTP) server.

4. Click **Update Settings** to save your changes.

NOTE: For information on L2TP settings, refer to "Configuring the L2TP Settings" on page 46.

Changing the Network Connection Type

> **i**   **NOTE:** Perform this task only with guidance from your ISP. The required entries for static IP address or PPPoE should be available, if your AP connection type is changed to either of those types.

To change the connection type (DHCP or Static IP)

1. Go to **Configuration** > **Internet**. The Configuration > Internet page appears.

2. In **Connection Type**, click the type of connection that your Internet service provider (ISP) is using. Typically, connection options relate to your ISP's delivery method:
    - In certain uncommon instances, a Static IP address is provided.
    - For cable modem access, DHCP is used.

3. If you need to change from DHCP to PPPoE or Static IP, fill in the related fields according to your ISP-provided information.

4. Click **Update Settings** to save your changes.

Configuring the L2TP Settings

You can implement transparent bridging with ZoneFlex through the use of L2TP (Layer 2 Tunnelling Protocol) tunnelling. By tunnelling traffic from a ZoneFlex AP to a centralized data center, access controllers with policy enforcement software can apply rules and services. In a typical WLAN implementation, these rules include a captive portal to authenticate users' credentials.

In the case of L2TP, the ZoneFlex AP functions as a remote bridge. As such, it forwards traffic into PPP sessions over the L2TP tunnel. This implementation ensures that you have complete visibility into MAC addresses of users, as individual Wi-Fi clients are essentially placed (bridged) onto the ISP's core network.

To configure L2TP tunnelling

1. Go to **Configuration** > **Internet**.

2. Under **L2TP Connection**, click **Enable**.

3. In **L2TP Network Server IP Address**, type the IP address of the L2TP network server (LNS) to which the device will connect.

4. In **Server Secret**, type the L2TP tunnel password.

5. If your network requires PPP authentication, configure the following fields under L2TP/PPP Authentication:
    - **Username**: Type your appropriate PPP user name.
    - **Password**: Type the password appropriate to the account.
    - **Password Confirmation**: Re-enter the password.

6. Click **Update Settings** to save your settings.

As ZoneFlex devices support multiple wireless networks (SSIDs), you should define which SSID should be tunneled and which should be locally bridged. You can configure this on the VLAN page. For more information, refer to "Configuring VLAN Settings" on page 64.

Renewing or Releasing DHCP

This task should be performed only with guidance from your ISP. It serves as a troubleshooting technique when DHCP addresses to one or more networked devices prove to be unusable or in conflict with others.

1. Go to **Status** > **Internet**.

2. Review the current settings.

3. If the current **Connection Type** is **DHCP**, you will be able to see the currently-assigned IP address and subnet mask listed below.

   - To force the DHCP server to assign a new IP address to this AP, click **Renew DHCP**. This will cause a slight interruption in network service until the new IP address has been put in use.
   - To force the DHCP server to assign new IP addresses to all networked devices at the same time (including this AP), click **Release DHCP.** This will cause a temporary interruption in overall network service.

4. Click **Update Settings** to save your settings.

Figure 22.   The Status > Internet page

Configuring Common Wireless Settings

Common wireless settings are settings that are applied to all WLANs. The settings include the wireless mode, wireless channel, and country code.

To configure the wireless settings common to all WLAN

1. Go to **Configuration** > **Wireless**. The Configuration :: Wireless :: Common page appears.

> **NOTE:** If you are using ZoneFlex 7962 AP, go to **Configuration** > **Radio 2.4G** or **Configuration** > **Radio 5G**.

2. Make changes to the common wireless settings listed in the table below.

Table 16. Common Wireless settings

Setting	Description
Wireless mode	The wireless mode options include the following: • **Auto-Select**: Allows both 802.11g- and 802.11b-compliant devices to connect to the network. This is the default setting. • **2.4GHz 54 Mbps (For faster 802.11g devices only)**: Allows only 802.11g-compliant devices to join the network. • **2.4GHz 11Mbps (For slower 802.11b devices only)**: Allows only 802.11b-compliant devices to join the network
Channel	This option lets you select the channel used by the network. You can choose **SmartSelect**, or choose one of a specific number of channels. If you choose **SmartSelect**, the AP automatically selects the best channel (encountering the least interference) to transmit the signal.
Country Code	This option (if enabled) lets you select your country or region code.
Advanced Settings	Refer to "Reviewing the Advanced > Common Options" on page 49.

⚠ **CAUTION:** Selecting the incorrect country or region may result in violation of applicable laws. If you purchased the AP in the United States, you do not need to manually set the country code. Ruckus Wireless APs that are sold in the US are preconfigured with the correct country code and this setting cannot be changed.

3. Click **Update Settings** to save your settings.

Figure 23.   The Configuration > Wireless page
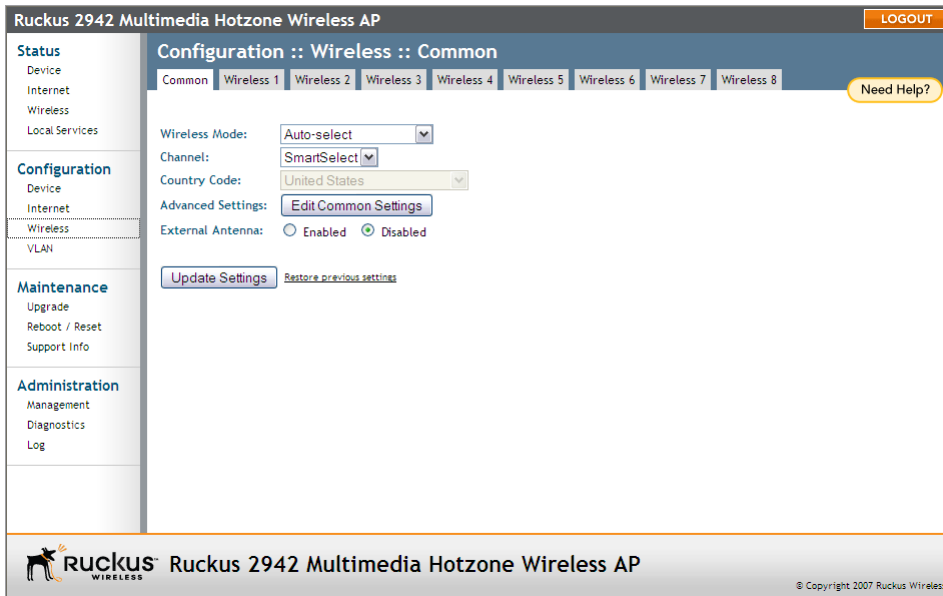
Reviewing the Advanced > Common Options

This page permits access to advanced wireless functions. These settings should only be changed by an experienced administrator. Incorrect settings can severely impact wireless performance. It is recommended that the default settings be retained for best performance.

⚠ **CAUTION:** To fully benefit from the AP's capabilities, it is advisable not to change this value unless absolutely necessary.

To configure the advanced common options

1. On the **Configuration** > **Wireless** page, click **Edit Common Settings**. The Configuration > Wireless > Advanced > Common page appears.

i   **NOTE:** If you are using ZoneFlex 7962 AP, go to **Configuration** > **Radio 2.4G** or **Configuration** > **Radio 5G**.

2. Configure the advanced settings listed in <u>Table 17</u> as required.

Table 17.   Advanced > Common options

Option	Description
Transmit Power	The default setting is **Full**. Select the level of transmit power from the drop-down menu. This option sets the maximum transmit power level relative to the predefined power (this value differs according to the current country code).
Protection Mode	(Inactive by default.) If you activate protection, you control how 802.11 devices know when they should communicate to another device. This is important in a mixed environment of both 802.11b and 802.11g clients.
	WARNING: Activating this option (and configuring the settings) boosts the interoperability of 802.11b and 802.11g devices but will severely decrease performance.
	• **CTS-only**: Choose this option to force all destination devices to acknowledge their ability to receive data when a transmission is initiated. Use this option for compliance with the Wi-Fi Alliance certification.
	• **RTS/CTS**: Choose this option to force both sending and receiving devices to confirm a data exchange on both ends before proceeding.
	For information on "Protection Mode", including specific threshold options and how they can be customized on an individual WLAN basis, see <u>"Setting Threshold Options"</u> on <u>page 51</u>.

3. Click **Update Settings** to save and apply the changes.

Figure 24. The Configuration > Wireless > Advanced > Common page
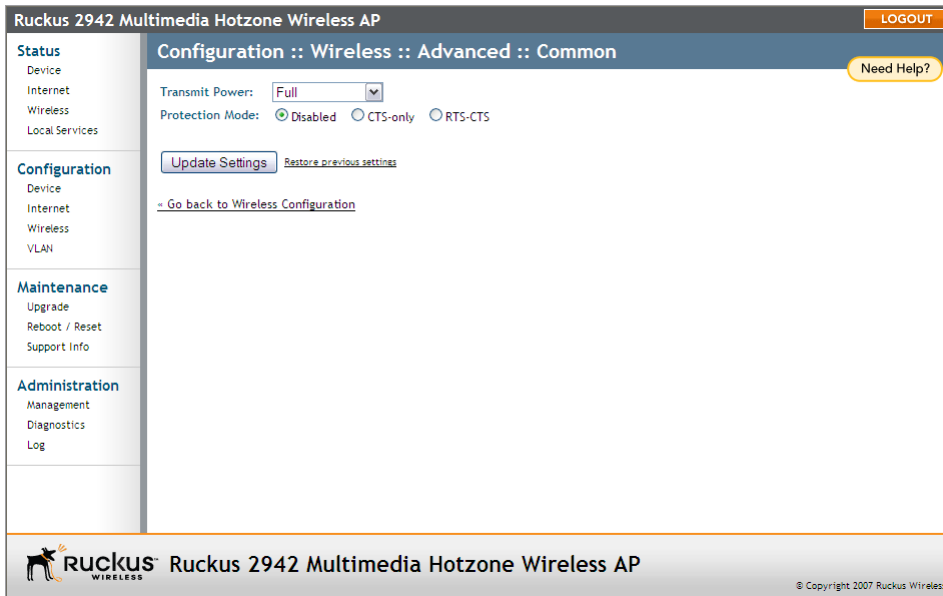
Setting Threshold Options

The following options allow you to fine-tune the "Protection Mode" behavior, set previously on the **Wireless** > **Common** page. After activating a Protection Mode, you can open each Wireless tab and customize the threshold settings, that determine what is put in effect and when.

> ⚠️ **CAUTION:** Do not customize these options unless you are an experienced network administrator or are under the guidance of an IT/support professional.

To customize Protection Mode (Threshold) settings

1. Go to **Configuration** > **Wireless**. The Configuration :: Wireless :: Common page appears.

> ℹ️ **NOTE:** If you are using ZoneFlex 7962 AP, go to **Configuration** > **Radio 2.4G** or **Configuration** > **Radio 5G**.

2. Click the tab for the Wireless # (WLAN) that you want to configure. The Configuration :: Wireless :: Wireless [#] page appears.
3. Look for **Threshold Settings**, and then click **Edit Settings**. The Configuration :: Wireless :: Advanced :: Wireless [#] page appears.

4. Review the options listed in <u>Table 18</u>, and then make any needed changes.

Table 18.   Threshold options

Option	Description
Beacon Interval	(The default value is 100.) The value indicates the frequency interval of the beacon in millisecond. A beacon is a broadcast packet by Access Point (AP) to synchronize the wireless network.
Data Beacon Rate	(The default value is 10.) The value indicates the interval of the Delivery Traffic Indication Message (DTIM). This is a countdown field that the device uses to inform its clients of the next window for listening to broadcast or multicast messages.
RTS/CTS Threshold	(The default value is 2346.) This option determines at what packet length the RTS/CTS function is triggered. A lower threshold may be necessary in environment with excessive signal noise or hidden nodes; but may result in some performance degradation.

5. Click **Update Settings** to save and apply the changes. A confirmation message appears at the top of the page.

You have completed configuring the threshold options. To reopen the previous page, click **Go back to Wireless Configuration**.

Figure 25.   Threshold settings

Configuring WLAN Settings

This section describes how to configure WLAN-specific settings, such as wireless availability, SSID, encryption, and authentication.

To configure WLAN settings

1. Go to **Configuration** > **Wireless**. The Configuration :: Wireless :: Common page appears.

NOTE: If you are using ZoneFlex 7962 AP, go to **Configuration** > **Radio 2.4G** or **Configuration** > **Radio 5G**.

2. Click one of the eight **Wireless (#)** tabs. The Configuration :: Wireless :: Wireless (#) page appears.

3. Review the WLAN options listed in <u>Table 19</u>, and then make changes as required.

Table 19. Wireless # options

Option	Description
Wireless Availability	This option controls whether or not the wireless network is available to users (Off or On).
Broadcast SSID	This option controls whether or not the WLAN SSID is visible to anyone looking for wireless networks. Disabling (hiding) the SSID requires the user must be told the correct SSID before they can connect to your network.
SSID	This is the publicly-broadcast "name" of your wireless network. A default SSID is present (which you ideally replaced in the installation process). If the default SSID is still active, it is strongly recommended that you change it. An effective SSID somehow indicates your location or group name. The "name" can be up to 32 characters in length, contain letters and numbers, and is case-sensitive.
Threshold Settings	This button opens a page where you can configure the Protection Mode you activated on the Wireless :: Common page. If Protection Mode is not active, ignore this option. For more information, see <u>"Setting Threshold Options"</u> on <u>page 51</u>.
Encryption Method	By default, all data exchanges on your wireless network are not encrypted, but you can pick an encryption method in this option, and use the extra workspace features that appear to fine-tune the encryption settings. For more information, see either <u>"Using WEP"</u> on <u>page 55</u> or <u>"Using WPA"</u> on <u>page 57</u>.

4. When you are finished, click **Update Settings** to save and apply the changes. A confirmation message appears at the top of this page.

5. Click **Go back to Wireless Configuration** to reopen the previous page.

Figure 26. WLAN settings
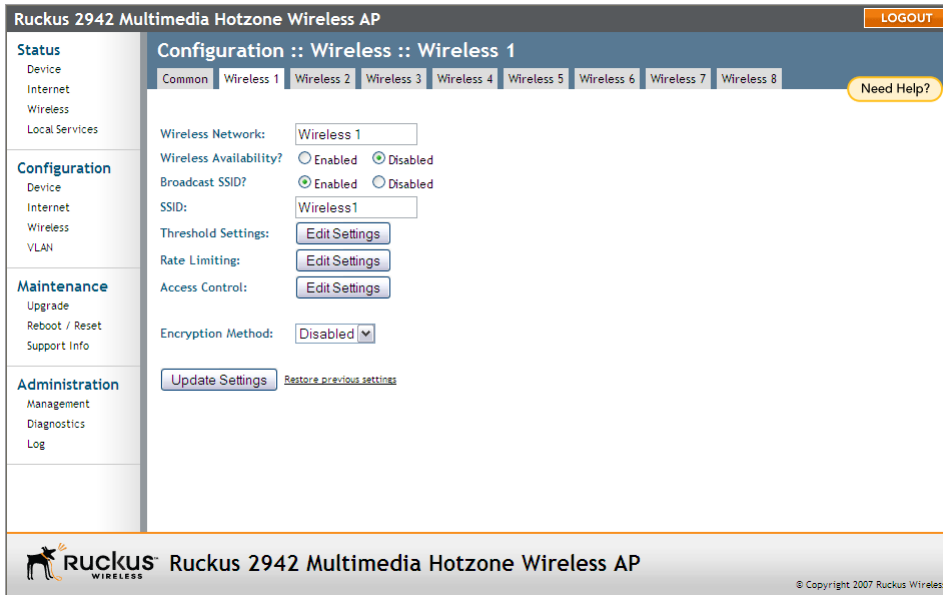
Using WEP

⚠ **CAUTION:** Do not customize these options unless you are an experienced network administrator or are under the guidance of an IT/support professional.

To configure WLAN-specific WEP encryption settings

1. Go to **Configuration** > **Wireless**. The Configuration :: Wireless :: Common page appears.

ⓘ **NOTE:** If you are using ZoneFlex 7962 AP, go to **Configuration** > **Radio 2.4G** or **Configuration** > **Radio 5G**.

2. Click the Wireless # tab that you want to configure. The Configuration :: Wireless :: Wireless[#] page appears.

3. Click the **Encryption Method** menu, and then click **WEP**. An additional set of WEP-specific encryption options appear on this page.

4. Review the encryption settings listed in <u>Table 20</u>, and then make changes as required.

Table 20.   WEP settings

Encryption Setting	Description
Authentication Mode	Your options include: • Open: No security measure is enforced. • Shared Key: The selected Default Shared Key is used. • Auto: Automatically-selected authentication mode.
Encryption Strength	• 64 bit: Specify the key with 10 hexadecimal digits or 5 ASCII characters. • 128 bit: Specify the key with 26 hexadecimal digits or 13 ASCII characters. The 128-bit cryptography is stronger privacy protection for your network and is recommended if you use WEP.
Key Entry Method	• Hexadecimal: The encryption key only accepts hexadecimal characters (0-9, A-F). • ASCII Text: The encryption key accepts ASCII characters.
Passphrase	This assists in automatic key generation. Enter some text and click the **Generate** button. The system will generate the WEP key automatically. You may specify a passphrase up to 32 characters. Please note that the algorithm used for key generation may vary from system to system. Checking the WEP keys used between wireless stations and the AP is recommended.
WEP Key	Enter the key manually according to the Key Entry Method and Encryption Strength settings.
Key Index	Choose the index, from "1" to "4", that the WEP key is to be stored in.

5. Click **Update Settings** to save and apply the changes. A confirmation message appears at the top of the page.

6. Click **Go back to Wireless Configuration** to reopen the previous page.

Figure 27.   WEP settings
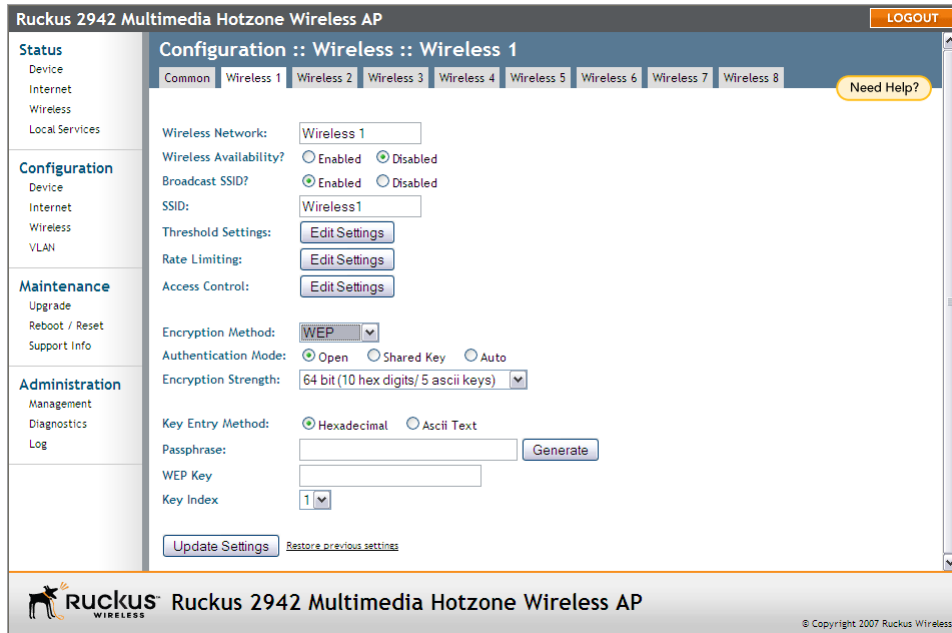
Using WPA

> ⚠ **CAUTION:** Do not customize these options unless you are an experienced network administrator or are under the guidance of an IT/support professional.

Use of WPA PSK allows automatic key generation based on a single passphrase. WPA-PSK provides very strong security, but may not be supported on older wireless devices. In some cases, the older devices can be upgraded with adapters to take advantage of WPA-PSK.

If you configure the AP with WPA-PSK, some network users will not be able to connect to your WLAN unless their devices are manually set to WPA-PSK and configured with the same passphrase.

To configure WPA encryption settings

1. Go to **Configuration** > **Wireless**. The Configuration :: Wireless :: Common page appears.

> ⓘ **NOTE:** If you are using ZoneFlex 7962 AP, go to **Configuration** > **Radio 2.4G** or **Configuration** > **Radio 5G**.

2. Click the Wireless # tab that you want to configure. The Configuration :: Wireless :: Wireless[#] page appears.

3. Click the **Encryption Method** menu, and then click **WPA**. An additional set of WPA-specific encryption options appear on this page.

4. Review the encryption settings listed in <u>Table 21</u>, and the make changes as preferred.

Table 21.   WPA settings

Encryption Setting	Description
WPA Version	Your options are WPA, WPA2 or WPA Auto. • When **WPA** is selected, the wireless client decides the version of WPA will be used. WPA is the recommended default for best compatibility. Wi-Fi WPA-capable PDAs and other gadgets are usually limited to WPA + TKIP. • **WPA2** is an advanced option. WPA2 support on Windows requires a Microsoft patch and is only available on Windows XP with Service pack 2 or later. • **WPA-Auto** is an advanced option. Only the best WPA 802.11i conforming/Wi-Fi WPA-certified client devices can operate in this mode.
WPA Authentication	PSK mode is suitable for home or personal use. 802.1x mode uses a networked RADIUS server to verify user identity. The auto mode offers both options for the wireless client to pick.
WPA Algorithm	When Auto is selected, the wireless client decides whether TKIP or AES will be used. AES is the strongest encryption and requires additional hardware support on wireless devices.You should consult the documentation of your wireless client devices. Auto is an advanced option and some wireless clients may fail to associate.
Passphrase	Enter a new passphrase between 8 and 32 characters long, using any combination of printable characters (letters, numbers, hyphens and underscores).

5. Click **Update Settings** to save and apply the changes. A confirmation message appears at the top of the page.

6. Click **Go back to Wireless Configuration** to reopen the previous page.

Figure 28. WPA settings

Customizing 802.1x Settings

⚠ **CAUTION:** Do not customize these options unless you are an experienced network administrator or are under the guidance of an IT/support professional.

If you choose "WPA" as the encryption method, you have the option to set up the AP to act as an 802.1x proxy, utilizing external authentication sources such as a RADIUS server. This provides a higher level of security, when compared to the static security process in a WEP configuration.)

Using 802.1x lets a device complete authentication prior to the exchange of data, as in a DHCP environment. Another benefit is that each BSSID can be individually configured to forward all authentication requests to its own server.

To configure WLAN-specific 802.1x authentication settings

1. Go to **Configuration** > **Wireless**. The Configuration :: Wireless :: Common page appears.

> **i**
>
> **NOTE:** If you are using ZoneFlex 7962 AP, go to **Configuration** > **Radio 2.4G** or **Configuration** > **Radio 5G**.

2. Click a Wireless # tab to configure. The Configuration :: Wireless :: Wireless[#] page appears.

3. Click the **Encryption Method** menu, then click **WPA**. The basic set of WPA-specific encryption options appear on the page.

4. Select **802.1x** as the WPA Authentication mode. Additional options appears.

5. Configure the following settings to customize your 802.1x authentication.

   - **RADIUS NAS-ID**: Enter the network ID assigned to your RADIUS server.
   - **Authentication Server [-Required-]**: Enter the information needed to establish a connection between the AP and the RADIUS server.
   - **Accounting Server [-Optional-]**: Enter the information needed to establish this connection.

6. Click **Update Settings** to save and apply the changes. A confirmation message appears at the top of this page.

7. Click **Go back to Wireless Configuration** to reopen the previous page.

Figure 29.   802.1x settings

Controlling Access to the Wireless Network

Access Control give you control over which stations are allowed to join (associate with) your WLAN networks. There are "tab" entries for each available WLAN.

Changing the Access Controls for a WLAN

1. Go to **Configuration** > **Wireless**.

> **i** **NOTE:** If you are using ZoneFlex 7962 AP, go to **Configuration** > **Radio 2.4G** or **Configuration** > **Radio 5G**.

2. Click the **Wireless #** tab for which you want to configure the access control settings.

3. Click the **Edit Settings** button after **Access Control**. The Configuration :: Wireless :: Access Control :: Wireless # page appears.

4. Select the radio button for the desired access control. (For a description of the options, see "Changing the Access Controls for a WLAN" in the previous section.) The Access Controls Table appears.

5. Click **Add new entry** to add a MAC address to the table.

6. Type the MAC address in the spaces provided.

7. Click **Update** to save your changes. Assuming all parameters you entered are acceptable, that row will be added to the table.

You have completed adding an entry to the MAC address table. If you have additional MAC addresses you want included, click **Add new entry**, and then repeat these steps until you have entered all the stations you want. There is a limit of 128 rows.

Figure 30.   Access control settings
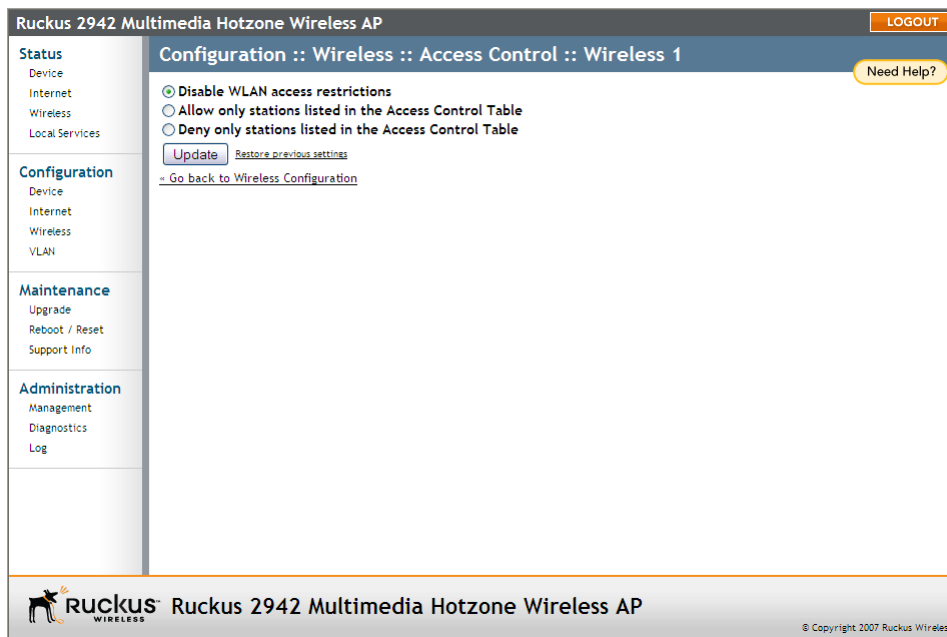
Removing MAC Addresses from the List

Simply check the box under the **Remove** column for the MAC address entry you want to remove from the table, and then click **Update**. The page refreshes and the MAC address that you removed disappears from the list.

Access Control Options

This section describes the options that you can use to control access to the wireless network.

Disabling WLAN Access Restrictions

If you select **Disable WLAN access restrictions**, then MAC-address-based restrictions on which stations can join the WLAN are disabled; thus, any station can join. If the WLAN uses encryption, then the station must still supply the correct encryption pass-phrase. The Access Controls table is hidden if the current mode is **Disable WLAN access restrictions**.

Allowing Only Stations Explicitly Listed in the Access Controls Table

If you select **Allow only stations listed in the Access Controls Tabl**e, then stations entered into the access-controls table are allowed but all others are disallowed. To add MAC addresses, see "Changing the Access Controls for a WLAN" on page 61.

Denying Only Stations Explicitly Listed in the Access Controls Table

If you select **Deny only stations listed in the Access Controls Table**, then stations entered into the access-controls table are disallowed but all others are allowed. To add MAC addresses, see "Changing the Access Controls for a WLAN" on page 61.

Access Control Table Columns

The Access Control table contains the following columns:

Address

Six text boxes appear in which you enter the desired MAC address, in hexadecimal digit form, two characters in each box. You can specify a full 12-hex-digit MAC address or enter "wildcard" characters for "don't care" digits. Allowable hex-digit characters are 0-9, a-f, and A-F. Most address-tags and software where you find MAC addresses listed include colons or dashes to separate the address-pairs; that is provided for you on the web page, so do not enter the colons or dashes.

The wildcard characters are "x", "X" and blank (space character). Wildcards are useful when you want to specify all MAC addresses from a given manufacturer. For example, by specifying only the Organizationally Unique Identifier (the first six hexadecimal digits of any MAC address from that manufacturer is its OUI) saves you having to enter all 24 million of them (the table size is limited in the AP/Router to 128 entries). Some manufacturers produce devices using more than one OUI, in which case you may need to enter each applicable one.

Name

You may optionally assign a name to a given MAC address. This helps you recognize known equipment. Names are not used by the router/AP device, they are merely an aid for recognizing equipment on your network. Names need not be specified and do not need to be unique. Names are accessible by Service Provider Technical Support personnel, so if privacy is a concern, you may wish to use generic-sounding names, such as "Room 1 TV", or not use names at all.

Remove

Check the **Remove** box for any rows that you no longer want used.

Configuring VLAN Settings

The VLAN page is used to configure the virtual LAN (VLAN) parameters of the AP. Traffic never uses VLAN tags over wireless links, but traffic originating on or destined for WLAN stations can be differentiated by a VLAN identifier as it travels over other links, such as Ethernet, DSL or Cable Internet, etc., thus given the appropriate priority as it traverses the Internet.

This section discusses the following topics:

- Navigating the VLAN Page
- Changing a VLAN ID
- Changing the Port State of a VLAN
- Changing an RJ45 Port's VLAN Tagged State

Figure 31.   The Administration > VLAN page
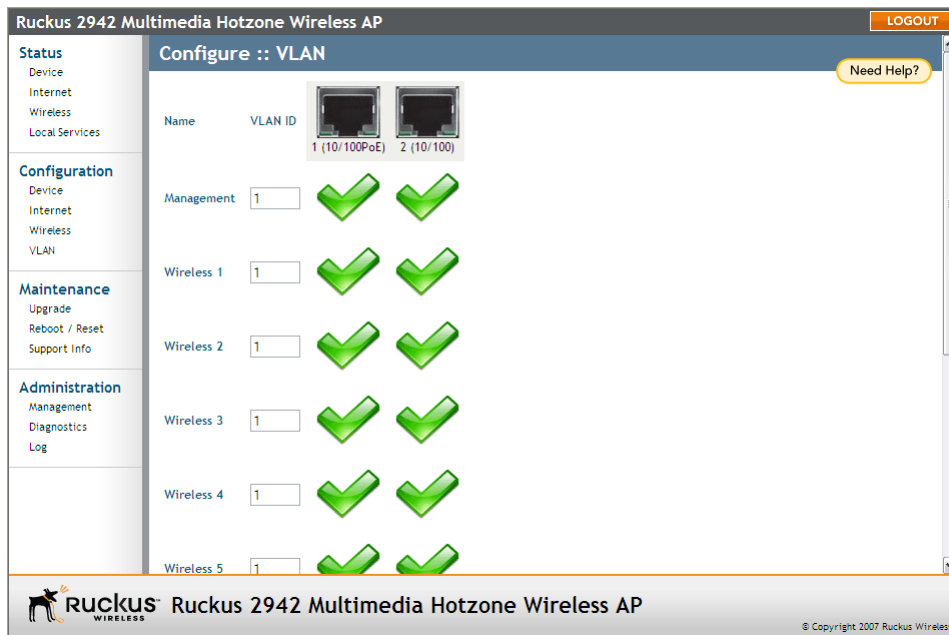
Navigating the VLAN Page

- **Name**: The name appearing in the first cell of each column identifies each "network". Here the term refers to a single broadcast-domain. There is also a "Management" network, referring to communications directly to the AP/Router.
- **VLAN ID**: If the VLAN ID field is blank or empty, no VLAN tagging will occur for that network. The state is shown by one of three images, explained below in "VLAN port state icons."

> **i** **NOTE:** If two rows (two networks) are assigned the same VLAN ID, then they are considered to be the same network.

- **VLAN tagging**: Each RJ45 port can be configured to use VLAN tagging. By default, no RJ45 port is tagged. When the icon contains a white "tag", that port is tagged; otherwise it is un-tagged. Clicking on the icon switches between tagged and un-tagged modes.

- **RJ45 port state images**: The AP may be connected to the same or different service-provider "uplinks" using the RJ45-type connectors on the back of the AP. The images of RJ45 connectors represent those RJ45 connectors on the AP. Each image includes the label of the RJ45 port which it represents. Clicking an icon switches between "tagged" and "un-tagged" modes. When the icon contains a white "tag", that port is tagged; otherwise it is un-tagged. If desired, traffic can be distinguished with different VLAN IDs, which you configure using this page.

Figure 32.   VLAN tagging

- **VLAN port state icons**: **"**Member VLAN ports**"** allow the network's traffic to flow through its associated RJ45 connector. If that port is configured for VLAN-tagging, then the "tagged member VLAN port" icon will be displayed. A "non-member VLAN port" does not allow network traffic to flow through the RJ45 connector.

  Clicking an icon toggles that VLAN port between "member" and "non-member" status. The port may automatically be marked as "tagged" where appropriate.

Figure 33.   Port state icons

- **Show me an example**: Clicking the button labeled **Show me an example** opens a few sample configurations, with an explanation of what each shows.

- **Update Settings (test)**: When you click **Update Settings (test)**, if any configuration settings changed, a connectivity-test will be run; this lasts approximately 30 seconds. If the browser and the AP/Router can communicate with the new VLAN settings, then they will remain set. If connectivity fails, then the device will revert to the previous VLAN settings. A pop-up message will tell you whether the test passed or failed and VLAN values were reverted.

- **Update Settings (no testing, override)**: When you click **Update Settings (no testing, override)**, you are saving configuration changes without a connectivity test.

Changing a VLAN ID

This task should be performed by an experienced network administrator or are under the guidance of an IT/support professional.

1. Go to **Administrator** > **VLAN**. The Administrator :: VLAN page appears.

2. Clear the value in the VLAN ID column, and type the new value.

3. Click **Update Settings (test)** to verify connectivity prior to saving changes. This prevents you from being locked out in the event you were to change the Management interface VLAN ID.

> **NOTE:** This works best in conjunction with "Changing the Port State of a VLAN" on page 66 and "Changing an RJ45 Port's VLAN Tagged State" on page 67.

Changing the Port State of a VLAN

This task should be performed by an experienced network administrator or are under the guidance of an IT/support professional.

1. Go to **Administrator** > **VLAN**. The Administrator :: VLAN page appears.

2. Click a green check mark to change the state between member, non-member, or tagged member.

3. Click **Update Settings (test)** to verify connectivity prior to saving changes. This prevents you from being locked out in the event you were to change the Management interface VLAN ID.

> **NOTE:** This works best in conjunction with "Changing a VLAN ID" on page 66 and "Changing an RJ45 Port's VLAN Tagged State" on page 67.

Changing an RJ45 Port's VLAN Tagged State

This task should be performed by an experienced network administrator or are under the guidance of an IT/support professional.

1. Go to **Administrator** > **VLAN**. The Administrator :: VLAN page appears.

2. Click an RJ-45 port icon to change the state from untagged to tagged.

3. Click Update Settings (test) to verify connectivity prior to saving changes. This prevents you from being locked out in the event you were to change the Management interface VLAN ID.

NOTE: This works best in conjunction with "Changing a VLAN ID" on page 66 and "Changing the Port State of a VLAN" on page 66.

5

Managing the Access Point

Viewing Associated Wireless Clients

A usage-monitoring capability has been built into the Access Point to help you monitor wireless clients that are associated with your wireless network.

To view associated wireless clients

1. Go to **Status** > **Wireless**. The Status :: Wireless page appears.

> **i** **NOTE:** If you are using ZoneFlex 7962 AP, go to **Status** > **Radio 2.4G** or **Status** > **Radio 5G.**

2. Click any of the Wireless tabs. Wireless clients that are associated with this particular wireless network appear under **Connected Devices**.

Figure 34.   The Status > Wireless page

Viewing Local Services

Go to **Status** > **Local Services**. The Status :: Local Services page appears, displaying a list of devices (computers, printers, access points) that are currently connected to the local network.

Figure 35. The Status > Local Services page
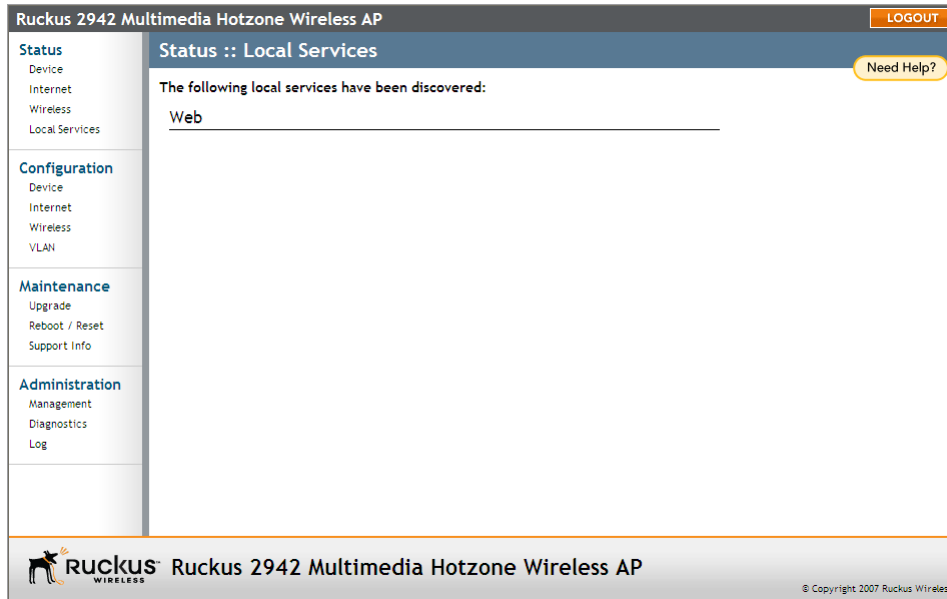
Changing the Administrative Login Settings

The default user name is `super` and the default password is `sp-admin`. To prevent unauthorized users from logging in to the Web interface using these default administrator login settings, Ruckus Wireless recommends that you change the default Web interface password immediately after your first login.

To change the default administrator login settings
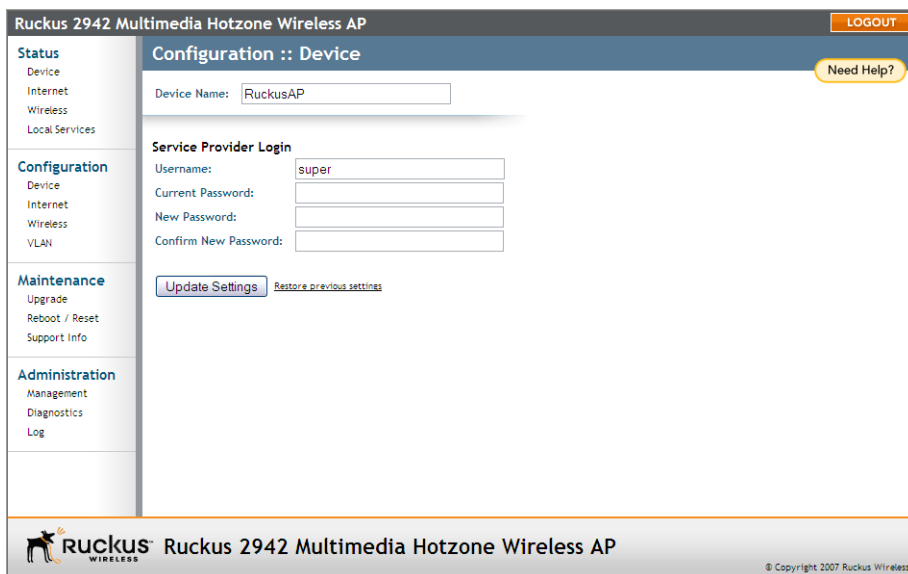
1. Log into the Web interface.

2. Go to **Configuration** > **Device**. The Device page appears.

3. Under **Service Provider Login**, change the default administrator login settings.

   ■ (Optional) In **Username**, type a new user name that you will use to log in to the Web interface. The default user name is `super`.

   ■ In **Password**, type a new password to replace the default password `sp-admin`.

   ■ In **Password Confirmation**, retype the new password.

4. Click **Update Settings**. The message *Your parameters were saved* appears.

You have completed changing the default login settings. The next time you log in to the Web interface, make sure you use these updated login settings.

Figure 36.   The Configuration > Device page

Enabling Other Management Access Options

In addition to managing the AP via a Web browser through HTTPS, several other management access options are available on the AP. These options include management access via HTTP, Telnet, and SSH.

In addition to these management access options, you can also view and set up the connection to the Ruckus Wireless FlexMaster under the **TR-069/SNMP Management Choice** options. If your ZoneFlex device is to be managed by FlexMaster, then the FlexMaster information (server URL and contact interval) is preconfigured before you receive your ZoneFlex device.

NOTE: If you are configuring the AP to be managed by FlexMaster, remember to point it to the FlexMaster server after you configure the management access options. For more information, refer to "Pointing the AP to FlexMaster" on page 77.

Figure 37.   The Administration > Management page
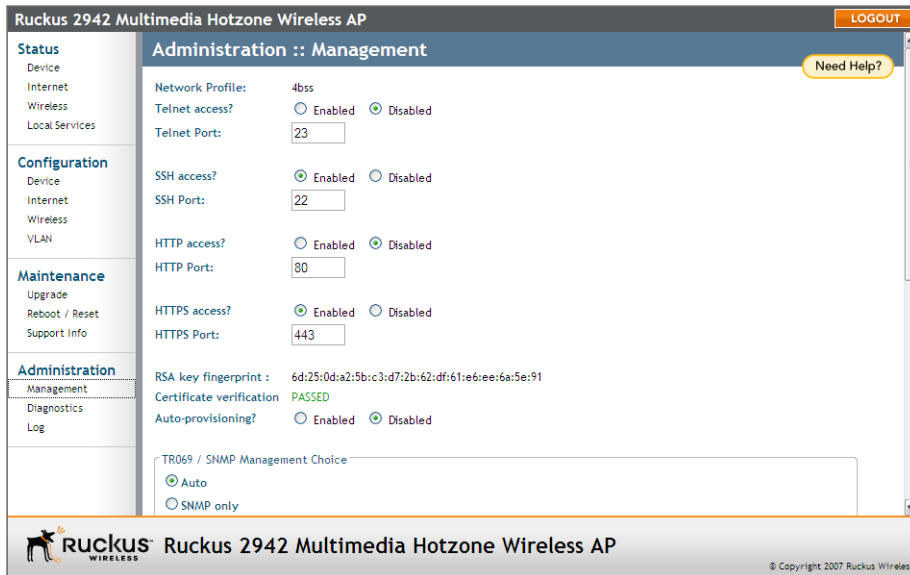
To enable other management access options

1. Go to **Administration** > **Management**. The Management page appears.

2. Review the access options listed in Table 22, and then make changes as needed.

Table 22.   Management Access Options

Option	Description
Telnet access	By default, this option is disabled (inactive).
Telnet port	This field lists the default Telnet port of 23 — only if Telnet is active. You can manually change this port number, if required.
SSH access	By default, this option is enabled (active).
SSH port	This field lists the default SSH port of 22—only if SSH is active. You can manually change this port number if required.
HTTP access	This option is disabled by default.
HTTP port	This field lists the default HTTP port of 80, if HTTP has been activated. You can manually change this port number if required.
HTTPS access	By default this option is enabled. This connection mode requires a security certificate, a copy of which has been pre-installed in the device.

Table 22.   Management Access Options

Option	Description
HTTPS port	This field lists the default HTTPS port of 443—only if HTTPS has been activated. You can manually change this port number if required.
Certification Verification	This notes whether the security certificate linked to the HTTPS settings has been passed or not.

3. If you want to use TR-069 or SNMP to manage the AP, configure the settings listed in Table 23.

Table 23.   TR-069 and SNMP Management Options

Option	Description
Auto	Enables the ZoneFlex device to connect to either SNMP server, Ruckus Wireless ZoneDirector, or Ruckus Wireless FlexMaster.
SNMP only	Only allow SNMP management
FlexMaster only	Only allow FlexMaster management
DHCP Discovery	URL of server providing DHCP
FlexMaster Server URL	URL of the FlexMaster server
Digest-authentication Username/Digest-authentication password	This information is automatically generated by the AP and used for authentication with FlexMaster. Change this value *only* if you want the AP to connect to another access control server (ACS).
Contact FlexMaster every	Interval at which the device should attempt to contact FlexMaster

Table 23.   TR-069 and SNMP Management Options

Option	Description
Associated-Clients Monitoring Mode	When enabled, the AP monitors the association and disassociation activities of wireless clients and sends this information to FlexMaster. Available options include:
	• **Disable (default)**: Select to turn off client association monitoring. When this option is selected, the AP will not send client association information to FlexMaster; Flexmaster will need to retrieve this information from the AP.
	• **Passive**: Select to enable client association monitoring and send related information to FlexMaster at the next inform interval.
	• **Active**: Select to enable client association monitoring and define the monitor interval (Interval). The AP will check for client association based on the defined Interval (in seconds), and then send related information FlexMaster as soon as an association event is detected.

4. Click **Update Settings** to save your changes. A confirmation message appears at the top of the page.

You have completed the management access options.

Viewing FlexMaster Management Status

If you configure the AP to be managed by FlexMaster, you can check the *TR-069 Status* section on the **Administration** > **Management** page.

Figure 38. *TR-069 status information*
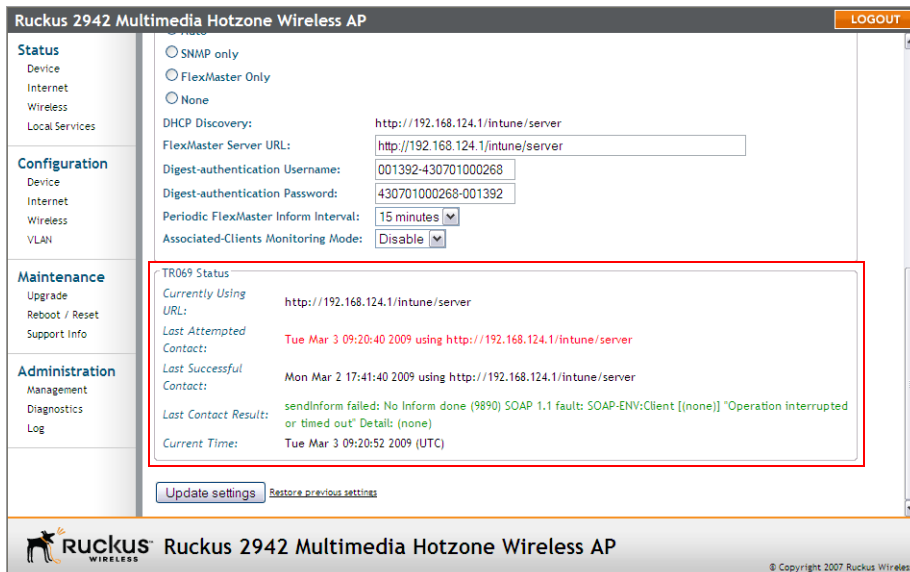
Table 24 lists the TR-069 status information that the AP provides.

Table 24. *TR-069 status information*

Status Information	Description
Currently using	Shows the FlexMaster server IP address or URL with which the AP is currently registered
Last attempted contact	Shows the date and time of the AP's last attempt to contact FlexMaster. Date and time are specified in GMT (or UTC), which are accurate if a Network Time Protocol (NTP) server is configured.
Last successful contact	Shows the date and time of the AP's last successful contact with FlexMaster.

Table 24. TR-069 status information

Status Information	Description
Current time	Shows the current date and time as known to the AP. This timestamp is accurate is an NTP server is configured on the AP. If there is no NTP server configured, this timestamp is useful as a reference for comparison of the timestamps for **Last attempted contact** and **Last successful contact**.

Pointing the AP to FlexMaster

Your ZoneFlex device is required to "call home" to register with your FlexMaster; FlexMaster does not initiate initial contact. To register successfully with FlexMaster, your ZoneFlex device must know the FlexMaster server's URL, thus entered on the device.

To point the AP to FlexMaster

1. Go to **Administrator** > **Management**.

2. Under **TR-069/SNMP Management Choice**, click **Auto**.

3. In **FlexMaster Server URL**, type the URL of the FlexMaster server.

4. Toggle the **Contact FlexMaster every** drop-down list to select how frequently the device will check the FlexMaster server for any pending configuration changes available for that ZoneFlex unit. On the FlexMaster side, this field is referred to as the Periodic Inform Interval.

5. Click **Update Settings** to save your changes.

After the AP registers with FlexMaster, this **Administration** > **Management** page will show the communication status between the AP and FlexMaster.

Enabling Logging and Sending Event Logs to a Syslog Server

If you have a syslog server on the network, you can configure the Access Point to send the device logs to the server. You will need to enable logging (logging is disabled by default), and then configure the Access Point to send logs to the syslog server.

1. Go to **Administration** > **Log**. The Administration :: Log page appears.

2. Look for **Log Status,** and then click **Enabled**.

3. After enabling logging, configure the following options:

   • **Syslog Server Address [Optional]**: To enable the AP to send messages to a syslog server as they appear, enter the IP address of the syslog server.

- **Syslog Server Port**: By default, the syslog port number is 514. If the syslog server is using a different port, enter that port number in this field.

4. Click **Update Settings** to save and apply your changes.

Figure 39.   The Administration > Log page

Sending a Copy of the Log File to Ruckus Wireless Support

The Support Info log consists of the configuration and run-time status of the AP and can be useful for troubleshooting. You have three options for sending a copy of the current log file to Ruckus Wireless Support:

- Save a copy to your local PC, then attach it to an e-mail message and send it to support
- Set up a connection to an FTP site
- Set up a connection to a TFTP site

To take advantage of these options, follow these steps

1. Go to **Maintenance** > **Support Info**. The Maintenance :: Support Info page appears.

2. Review the Upload Method options.

3. To upload a copy of the support info file to an FTP or TFTP server, click TFTP or FTP option. Clicking the FTP option prompts you to enter a User ID and Password.

4. In **Server Address**, enter the FTP or TFTP server IP address.

5. In **Filename**, enter a name for this file that you are saving.

---

i   **NOTE::** Remember to add a .TXT file extension to the file name, especially if you are using Internet Explorer as your Web Admin "host".

---

6. Click **Upload Now**.

Saving a Copy of the Current Log to Your Computer

You can also save a copy of the current log to your own computer, if needed.

1. Go to **Maintenance** > **Support Info**. The Maintenance :: Support Info workspace appears.

2. Review the Upload Method options

3. Click the **Save to local computer** option.

4. Click **Upload Now**.

5. When the "Save as..." dialog box appears, change the destination directory and change the file name if you prefer.

6. Click **Save** to save the file to your computer.

Upgrading the Firmware

You can use the Web interface to check for software updates/upgrades for the firmware built into the AP. You can then apply these updates to the device in one of two ways: (1) manual updating on an as-needed basis or (2) automating a regularly scheduled update.

Before starting, decide which option you want to take:

• Automate a regularly scheduled update

• Run a one-time manual update right now.

By default, the automatic upgrade option is active, and will check the Ruckus Wireless update server every 12 hours.

To get started with upgrading the firmware, go to **Maintenance** > **Upgrade**. When the **Maintenance** > **Upgrade** options appear, decide which upgrade method to use. Each of the three upgrade options listed on the Upgrade page are discussed in the succeeding sections.

Figure 40.   The Maintenance > Upgrade page

Upgrading Manually via the Web

1. In the **Upgrade Method** options, click **Web**.

2. Click the **Web Options URL** field, and then type the URL of the download Web site. Remember to start the URL with "http://".

3. You can change the Image Control File filename extension as noted here:
   - Replace any file names ending in `.rcks` with the `.html` extension
   - Replace any file names ending in `.fI7` with the `.html` extension

i> **CAUTION:** Do not change the **Username** or **Password** entries.

4. Click **Perform Upgrade**. A status bar appears during the upgrade process.

5. After the upgrade is completed, you must manually reboot the AP.

Upgrading Manually via FTP or TFTP

1. In the **Upgrade Method** options, click **FTP** or **TFTP**.

2. Click the host name field, and then type the URL of the server. Or click the IP address field, and then type the IP address of the server. Remember to start the URL with `ftp://`.

i> **CAUTION:** Do not change any of the Image Control File, Username, or Password entries.

3. Click **Perform Upgrade**. A status bar appears during the upgrade process.

4. After the upgrade is completed, you must manually reboot the AP.

Scheduling an Automatic Upgrade

1. In the Upgrade Method options, click the button by your preferred choice.

2. Enter the appropriate information in the Host name field or IP address field.

i> **CAUTION:** Do not change any of the Image Control File, Username, or Password entries.

3. Verify that the Auto Upgrade: Enabled option is checked (active).

4. Toggle the Interval to Check for Software Upgrade drop-down list to select your preferred interval.

5. You have two options at this point:
   - Click **Perform Upgrade**, which will start the process and the clock. The next upgrade will occur at the selected interval.

- Click **Save parameters only**. The clock starts right away, and the actual upgrade will occur at the first effective interval.

After you click one of these two options, a status bar appears during the upgrade process.

When the upgrade is complete, the AP will reboot automatically.

Rebooting the Access Point

You can use the Web User interface to prompt the AP to reboot, which simply restarts the AP without changing any of the current settings. Please note that rebooting the AP will disrupt network communications in any currently active WLANs.

To reboot the Access Point

1. Go to **Maintenance** > **Reboot/Reset**. The Maintenance :: Reboot/Reset page appears.

2. Click **Reboot Now**. After a brief pause, you will be automatically logged out of the AP.

Figure 41.   The Maintenance :: Reboot/Reset page
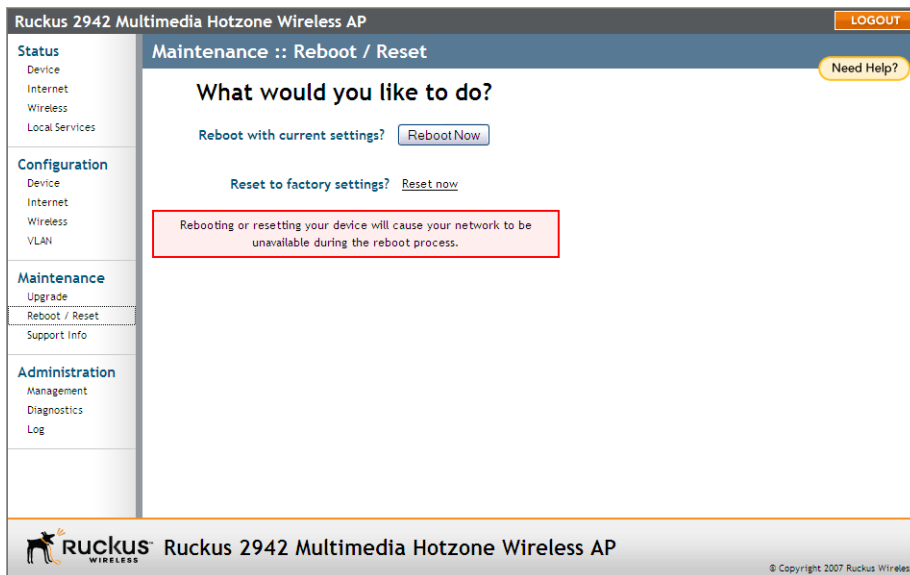
After a minute or so, you should be able to log back into the AP, which verifies that the reboot was successful. You can also check the LEDs on the AP's front panel to verify the status of the device.

Resetting the Access Point to Factory Default

> ⚠ **WARNING:** DO NOT reset the Access Point to factory default, unless you are directed to do so by Ruckus Wireless support staff or by a network administrator. Do this only if you are able to immediately reconnect the restored AP to your computer, to reconfigure it for Wi-Fi network use — as detailed in "Installing the Access Point" on page 17.

You can use the Web User interface to restore an inoperative AP to its factory default settings, which will completely erase the configuration currently active in the device. Note, too, that this will disrupt all wireless network communications through this device.

To reset the Access Point to factory default

1. Go to **Maintenance** > **Reboot/Reset**. The Maintenance :: Reboot/Reset page appears.

2. Click **Reset Now** (next to *Restore to factory settings*?).

After a brief pause, you will be automatically logged out of the AP. You must now disconnect the AP from the switch (and the network) and reconnect it to your computer, as described in "Step 1: Preconfigure the Access Point" on page 21. At this time, you can restore the network settings, then replace it in your site for full network use.

Running Diagnostics

Two network connection diagnostic tools – PING and traceroute – have been built into the AP to help you check network connections from the Web interface.

To run diagnostics for network troubleshooting

1. Go to **Administrator** > **Diagnostics**. The Administrator :: Diagnostics page appears. Two options are available:
   - Ping
   - Traceroute
2. Click the text field by the option you want to activate, and type the network address of a site you wish to connect to.
3. Click **Run Test**.

The results appear in the text field below each option.

Figure 42.   Pinging ruckuswireless.com

Figure 43.   Running traceroute on ruckuswireless.com

Where to Find More Information

If you have questions that this User Guide does not address, visit the Ruckus Wireless Support Portal at http://support.ruckuswireless.com/. The Support Portal hosts the latest versions of user documentation. You can also find answers to frequently asked questions (FAQs) for each Ruckus Wireless product type.

Index