Ruckus Wireless™ Indoor Access Point

Release 100.1.0 User Guide

For the following indoor Ruckus Wireless AP models:
- ZoneFlex 7055 Dual-Band 802.11n Wired/Wireless Wi-Fi Wall Switch
- ZoneFlex 7321 2.4/5GHz 802.11n Smart Wi-Fi Access Point
- ZoneFlex 7341 Single-Band 802.11n Access Point
- ZoneFlex 7343 Single-Band 802.11n Access Point
- ZoneFlex 7352 802.11n Smart Wi-Fi Access Point
- ZoneFlex 7363 Dual-Band 802.11n Smart Wi-Fi Access Point
- ZoneFlex 7372 and 7372-E Dual-Band 802.11n Smart Wi-Fi Access Point
- ZoneFlex 7441 802.11n DAS Access Point
- ZoneFlex 7982 Dual-Band 802.11n Smart Wi-Fi Access Point
- ZoneFlex H500 Dual-Band 802.11ac Multimedia Wi-Fi Access Point Wall Switch
- ZoneFlex R300 Dual-Band 802.11n Smart Wi-Fi Access Point
- ZoneFlex R500 Dual-Band 802.11ac Smart Wi-Fi Access Point
- ZoneFlex R600 Dual-Band 802.11ac Smart Wi-Fi Access Point
- ZoneFlex R700 Dual-Band 802.11ac Smart Wi-Fi Access Point

Part Number 800-70862-001 Rev B
Published 25 June, 2015

www.ruckuswireless.com

Copyright Notice and Proprietary Information

Destination Control Statement

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

Disclaimer

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

Limitation of Liability

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

Trademarks

Ruckus Wireless, Ruckus, Bark Logo, BeamFlex, ChannelFly, Ruckus Pervasive Performance, SmartCell, ZoneFlex, Dynamic PSK, FlexMaster, MediaFlex, MetroFlex, Simply Better Wireless, SmartCast, SmartMesh, SmartSec, SpeedFlex, ZoneDirector, ZoneSwitch, and ZonePlanner are trademarks of Ruckus Wireless, Inc. in the United States and other countries. All other product or company names may be trademarks of their respective owners.

Contents

About This Guide

1

By downloading this software and subsequently upgrading Ruckus Wireless APs to base image 100.0.0 and later, please be advised that:

- The ZoneDirector periodically connects to Ruckus and Ruckus collects the ZoneDirector serial number, software version and build number. Ruckus transmits a file back to the ZoneDirector and this is used to display the current status of the ZoneDirector Support Contract.
- The AP may send a query to Ruckus containing the AP's serial number. This allows your AP to autonomously connect with a wireless LAN controller operated by your choice of cloud service provider. Ruckus may transmit the Fully Qualified Domain Name (FQDN) or IP address of the controller that the AP will subsequently attempt to join back to the AP.
- Please be advised that this information may be transferred and stored outside of your country of residence where data protection standards may be different.

This guide describes how to install, configure and manage Release 100.1.0 Ruckus Wireless Indoor Access Points (APs). This guide is written for those responsible for installing and managing network equipment. Consequently, it assumes that the reader has basic working knowledge of local area networking, wireless networking, and wireless devices.

NOTE If release notes are available for 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

https://support.ruckuswireless.com/documents

Continue with the following:

Safety Warnings

WARNING! Only trained and qualified personnel should be allowed to install, replace, or service this equipment. The professional installer is responsible for the proper installation and configuration of this AP. The AP installation must comply with local regulatory requirements, especially with those regulating operation near military and/or weather radar systems.

WARNING! Read the installation instructions before you connect the system to its power source.

WARNING! This product relies on the building's installation for short-circuit (overcurrent) protection. Ensure that the protective device is rated not greater than 20A.

WARNING! Installation of this equipment must comply with local and national electrical codes.

WARNING! Do not operate your wireless device near unshielded blasting caps or in an explosive environment unless the device has been modified to be especially qualified for such use.

WARNING! In order to comply with FCC radio frequency (RF) exposure limits, antennas should be located at a minimum of 7.9 inches (20 cm) or more from the body of all persons.

WARNING! Ruckus Wireless strongly recommends that you wear eye protection before mounting the AP.

CAUTION! The fasteners used to mount an AP on a ceiling must be capable of maintaining a minimum pullout force of 20 lbs (9 kg) and must use all four indented holes on the mounting bracket.

CAUTION! This product and all interconnected equipment must be installed indoors within the same building, including the associated LAN connections as defined by Environment A of the IEEE 802.af Standard.

Related Documentation

In addition to this *User Guide*, each Ruckus Wireless AP documentation set includes the following:

- *Installation Guide/Getting Started Guide/Mounting 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 AP's Web interface. Online help is accessible from within the Web interface.
- *Release Notes:* Provide information about the current software release, including new features, enhancements, and known issues.

NOTE For information on Ruckus Wireless access points supported by SmartCell Gateway (SCG) controllers, virtual SmartCell Gateway (vSCG) controllers, SmartZone (SZ) controllers, ZoneDirector (ZD) controllers, Smart Access Management service (SAMs), Ruckus Wireless controller operating system (SmartZone), and FlexMaster (FM) managers, refer to their respective Release Notes and associated user documents.

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 Indoor AP 100.1.0 User Guide
- Part number: 800-70862-001 Revision A
- Page 11

Please note that we can only respond to comments and questions about Ruckus Wireless product documentation at this email address. Questions related to technical support or sales should be directed in the first instance to your network supplier.

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

Notice Type	Description
NOTE	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.

Introducing the Ruckus Wireless AP

2

In this chapter:

Overview of the Ruckus Wireless AP

Congratulations on your purchase of the Ruckus Wireless AP! Ruckus Wireless APs are the industry's most easy to use, yet robust and feature-rich Wi-Fi APs designed to bring power and simplicity together for large-scale indoor deployments.

Your Ruckus Wireless AP uses BeamFlex, a patented 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 high-gain directional antenna elements that allow Ruckus Wireless APs to find quality signal paths in a changing environment, and sustain the baseline performance required for supporting data, audio and video applications.

Your Ruckus Wireless AP can be deployed in standalone mode with or without a FlexMaster (FM) manager, or as part of the Ruckus Wireless Smart WLAN system, in which it can be managed by SmartCell Gateway (SCG), virtual SmartCell Gateway (vSCG), SmartZone (SZ), ZoneDirector (ZD), and Smart Access Management service (SAMs) controllers. The rest of this document collectively refers to the SCG, vSCG, SZ, vSZ, ZD, SAMs and other controllers as **Ruckus Wireless controllers**.

NOTE For more information on the Ruckus Wireless controllers, BeamFlex, the Ruckus Wireless controller operating system (SmartZone), and other Ruckus Wireless technologies, visit

www.ruckuswireless.com

Unpacking the Ruckus Wireless AP

1. Open the AP 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 AP package contains all of the items listed below:

- Ruckus Wireless AP
- Software License Agreement/Product Warranty Statement
- Declaration of Conformity, if required
- *Quick Setup Guide*
- (Ethernet cables, power adapters and mounting kits are optional accessories that may or may not be included depending on the SKU purchased)

Getting to Know the AP Features

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

- ZoneFlex 7055 Dual-Band Wired/Wireless Wall Switch
- ZoneFlex 7321 AP
- ZoneFlex 7341 AP
- ZoneFlex 7343 AP
- ZoneFlex 7352 AP
- ZoneFlex 7363 AP
- ZoneFlex 7372 AP
- ZoneFlex 7372-E AP
- ZoneFlex 7441 DAS AP
- ZoneFlex 7982 AP
- ZoneFlex H500 AP Wall Switch
- ZoneFlex R300 AP
- ZoneFlex R500 AP
- ZoneFlex R600 AP
- ZoneFlex R700 AP

NOTE This User Guide does not include information on Ruckus Wireless Outdoor APs or the 7731 Wireless Bridge. For information on those Ruckus Wireless models (along with Ruckus Wireless SmartCell, SCG, vSCG, SZ, ZD, SAMs, FM and MediaFlex product lines), refer to their respective documentation available from support.ruckuswireless.com

ZoneFlex 7055 Dual-Band Wired/Wireless Wall Switch

The ZoneFlex 7055 is a multiservice 802.11n dual-band concurrent two-stream wired/wireless wall switch.

NOTE The 100.x AP base images support standalone mode and FlexMaster (FM) WLAN manager operation. The SmartZone-compatible images only support SCG, vSCG, and SZ controllers. The ZD-compatible images only support ZD controllers. The 7055 requires a minimum of AP base image 100.0.0 and later to operate, or SCG 1.0 and later, vSCG 2.5 and later, SmartZone 3.2 and later, or ZD 9.6 and later to operate.

The 7055 is designed for installation in an electrical junction box. This section identifies the physical features the 7055. Before you begin the installation process, Ruckus Wireless recommends that you become familiar with these features.

Front View Features

The front view of the 7055 features four Ethernet Ports, a pass through port and a DC in socket on the bottom front panel. Refer to Table 3 for more information.

Figure 1. ZF7055 front view

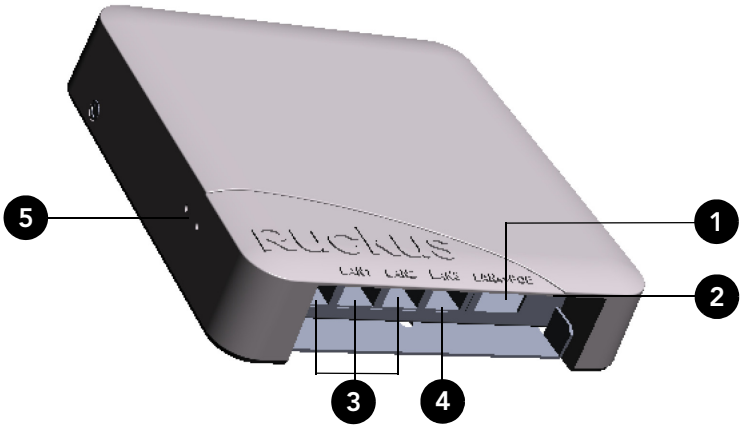


Table 3. ZF7055 front view features

Number	Name	Description
1	Pass Through port	Pass through port.
2	Power Input	Optional 48V DC power input.

Table 3. ZF7055 front view features (Continued)

Number	Name	Description
3	LAN1-LAN3	Three 10/100 RJ-45 Ethernet Ports.
4	LAN4	One 10/100 RJ-45 LAN port with PoE out. Supports 802.3af PSE Class 0/2 (depending on power input).
5	Reset buttons	Refer to "Reset Buttons" on page 17 for details.

Rear Panel Features

Figure 2 shows the rear panel of the 7055. For a description of each rear panel element, refer to Table 4.

Figure 2. ZF7055 rear panel

Table 4. ZF 7055 rear panel features

Number	Name	Description
1	PoE In LAN/Uplink	Uplink LAN port that supports 802.3af and 802.3at Power over Ethernet (PoE) input.
2	Punch down Block	110 punchdown block.
3	Pass Through Port	RJ-45 pass through port for the pass through connection.
4	LEDs	See Table 5 for LED descriptions and behaviors.

LEDs

Refer to Table 5 for descriptions of LEDs and their behaviors. The LEDs are not visible once the AP is installed.

Table 5. ZF 7055 LEDs

LED	Meaning
PWR	*Green:* On *Red:* Bootup in process *Off:* Off
WAN	*Green:* Link up. *Flashing green:* Activity. *Off:* Link down.
5G	*Off:* The WLAN service is down. *Amber:* The WLAN is up, but no clients are associated and no downlink MAPs are connected. *Green:* The WLAN is up and at least one client is associated. No downlink MAPs are connected. *Slow flashing green (one flash every two seconds):* The WLAN is up and at least one downlink MAP is connected. No clients are associated. *Fast flashing green (two flashes every second):* The WLAN is up, at least one downlink MAP is connected, and at least one client is associated.
2.4G	*Off:* The WLAN service is down. *Amber:* The WLAN is up, but no clients are associated and no downlink MAPs are connected. *Green:* The WLAN is up and at least one client is associated. No downlink MAPs are connected.
AIR	*Off:* The AP is operating in standalone mode or operating as a root AP (RAP) or a non-mesh AP. *Green:* The AP is functioning as a Mesh AP (MAP), and the wireless signal to its uplink AP is good. *Fast flashing green (two flashes every second):* The AP is functioning as a Mesh AP (MAP), and the wireless signal to its uplink AP is fair. *Slow flashing green (one flash every two seconds):* Mesh networking is enabled, but the AP is still searching for a mesh uplink.

Table 5. ZF 7055 LEDs (Continued)

LED	Meaning
DIR	*Off:* The AP is not being managed by ZoneDirector (standalone mode). *Green:* The AP is being managed by ZoneDirector. *Slow flashing green (one flash every two seconds):* The AP is being managed by ZoneDirector, but is currently unable to communicate with ZoneDirector. *Fast flashing green (two flashes every second):* The AP is being managed by ZoneDirector and is currently receiving configuration settings (provisioning) or an image update.
LAN1 - LAN4	*Green:* Link up. *Flashing green:* Activity. *Off:* Link down.

Reset Buttons

Two reset buttons on the left side of the AP are used to reboot or factory reset the AP.

Figure 3. Reset buttons

Press and hold the **Soft Reset** button for three seconds or more to reset the AP to factory defaults. Press and release the **Hard Reset** button to restart the AP.

NOTE On the 7055, the *Hard* reset button restarts the AP, while the *Soft* reset button reverts the AP to factory default settings.

ZoneFlex 7321 AP

The ZoneFlex 7321 is a best price/performance dual-band 802.11n SME AP.

NOTE The 100.x AP base images support standalone mode and FlexMaster (FM) WLAN manager operation. The SmartZone-compatible images only support SCG, vSCG, and SZ controllers. The ZD-compatible images only support ZD controllers. The 7321 requires a minimum of AP base image 100.0.0 and later to operate, or SCG 1.1 and later, vSCG 2.5 and later, SmartZone 3.2 and later, or ZD 9.4 and later to operate.

The 7321 features five LEDs on its front panel and buttons and connectors on its rear panel.

Front Panel

Figure 4 shows the top view of the 7321. For a description of front panel elements, refer to Table 6.

Figure 4. 7321 front panel

Table 6. 7321 front panel elements

LED	Description
PWR LED	• *Off*: Off. • *Red*: Boot up in process. • *Green*: On.

Table 6. 7321 front panel elements (Continued)

LED	Description
AIR LED	• *Off*: The AP is operating in standalone mode or operating as a root AP (RAP) or a non-mesh AP. • *Green*: The AP is functioning as a Mesh AP (MAP), and the wireless signal to its uplink AP is good. • *Fast flashing green* (two flashes every second): The AP is functioning as a Mesh AP (MAP), and the wireless signal to its uplink AP is fair. • *Slow flashing green* (one flash every two seconds): Mesh networking is enabled, but the AP is still searching for a mesh uplink.
DIR LED	• *Off*: The AP is not being managed by ZoneDirector (standalone mode). • *Green*: The AP is being managed by ZoneDirector. • *Slow flashing green* (one flash every two seconds): The AP is being managed by ZoneDirector, but is currently unable to communicate with ZoneDirector. • *Fast flashing green* (two flashes every second): The AP is being managed by ZoneDirector and is currently receiving configuration settings (provisioning) or an image update.
2.4G LED (WLAN)	• *Off*: The WLAN service is down. • *Amber*: The WLAN is up, but no clients are associated and no downlink MAPs are connected. • *Green*: The WLAN is up and at least one client is associated. No downlink MAPs are connected. • *Slow flashing green* (one flash every two seconds): The WLAN is up and at least one downlink MAP is connected. No clients are associated. • *Fast flashing green* (two flashes every second): The WLAN is up, at least one downlink MAP is connected, and at least one client is associated.

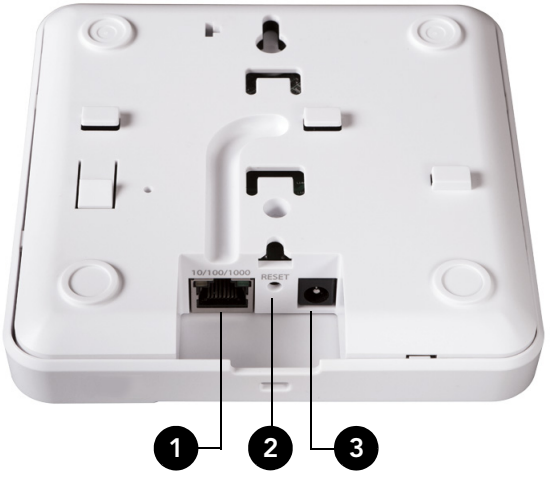
Table 6. 7321 front panel elements (Continued)

LED	Description
5G LED (WLAN)	• *Off*: The WLAN service is down. • *Amber*: The WLAN is up, but no clients are associated and no downlink MAPs are connected. • *Green*: The WLAN is up and at least one client is associated. No downlink MAPs are connected. • *Slow flashing green* (one flash every two seconds): The WLAN is up and at least one downlink MAP is connected. No clients are associated. • *Fast flashing green* (two flashes every second): The WLAN is up, at least one downlink MAP is connected, and at least one client is associated.

Rear Panel

Figure 5 shows the bottom view of the 7321. For a description of each rear panel part, refer to Table 11.

Figure 5. 7321 rear panel



ZoneFlex 7341 AP

NOTE The 100.x AP base images support standalone mode and FlexMaster (FM) WLAN manager operation. The SmartZone-compatible images only support SCG, vSCG, and SZ controllers. The ZD-compatible images only support ZD controllers. The 7341 requires a minimum of AP base image 100.0.0 and later to operate, or SCG 1.0 and later, vSCG 2.5 and later, or ZD 9.0 and later to operate.

ZoneFlex 7341 features five LEDs on its front panel and buttons and connectors on its rear panel.

Front Panel

Figure 6 shows the front panel of the ZoneFlex 7341. For a description of each front panel part, refer to Table 7.

Figure 6. ZoneFlex 7341 front panel

Table 7. ZoneFlex 7341 front panel elements

LED	Description
PWR LED	• *Off*: Off. • *Red*: Boot up in process. • *Green*: On.
OPT LED	Not used in this model.

Table 7. ZoneFlex 7341 front panel elements (Continued)

LED	Description
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 receiving configuration settings (provisioning) or a firmware update.
WLAN LED	• *Off*: The WLAN service is down. • *Amber:* The WLAN service is up and no clients are associated (standalone), or no wireless clients and no downlink MAPs are connected (RAP). • *Green*: The WLAN service is up and at least one wireless client is associated. If Mesh is enabled, no downlink MAPs are connected. • *Fast flashing green*: The WLAN service is up, at least one client is associated, and at least one Mesh downlink is connected. • *Slow flashing green*: At least one Mesh downlink is connected, and no clients are associated.
AIR LED	• *Off*: The Access Point is operating in standalone mode or operating as a root AP (RAP) or a non-mesh AP. • *Green*: The AP is functioning as a RAP or MAP and the uplink signal is *good*. • *Slow flashing green (one flash every two seconds)*: Mesh networking is enabled, but the AP is still searching for a mesh uplink. • *Fast flashing green (two flashes every second)*: The AP is functioning as a MAP and the wireless signal to its uplink AP is *fair*.

Rear Panel

Figure 7 shows the rear panel of the ZoneFlex 7341. For a description of each rear panel part, refer to Table 8.

Figure 7. ZoneFlex 7341 rear panel

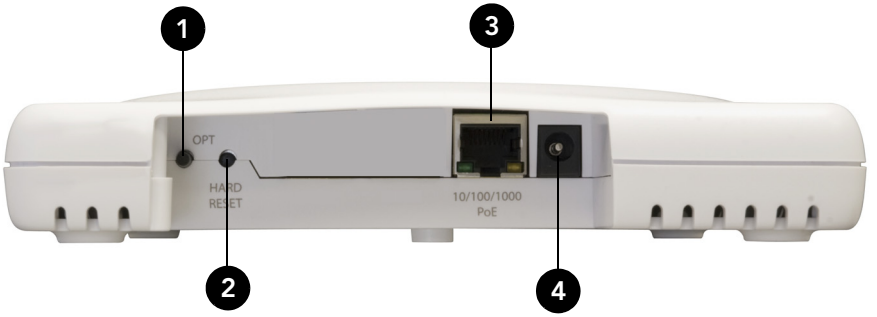


Table 8. ZoneFlex 7341 rear panel elements

Number	Item Name	Description
1	OPT Button	Not active in this model at this time.
2	HARD RESET Button	Pressing, and then quickly releasing this internal button reboots the AP. Pressing and holding it for six seconds resets the AP to factory default settings. **CAUTION!** *Resetting the AP to factory default settings erases all previously configured settings.*
3	10/100/1000 PoE Port	One RJ-45 port for a 10/100/1000 PoE (Power over Ethernet, 802.3af) connection.
4	Power	Connect the power adapter (12 VDC/1.25A) to this socket. Power can also be supplied via the 10/100/1000 PoE (802.3af) port.

ZoneFlex 7343 AP

NOTE The 100.x AP base images support standalone mode and FlexMaster (FM) WLAN manager operation. The SmartZone-compatible images only support SCG, vSCG, and SZ controllers. The ZD-compatible images only support ZD controllers. The 7343 requires a minimum of AP base image 100.0.0 and later to operate, or SCG 1.0 and later, vSCG 2.5 and later, or ZD 9.0 and later to operate.

ZoneFlex 7343 features five LEDs on its front panel, and buttons and connectors on its rear panel.

Front Panel

Figure 8 shows the front panel of the ZoneFlex 7343. For a description of each front panel part, refer to Table 9.

Figure 8. ZoneFlex 7343 front panel

Table 9. ZoneFlex 7343 front panel elements

LED	Description
PWR LED	• *Off*: Off. • *Red*: Boot up in process. • *Green*: On.
OPT LED	Not used in this model.

Table 9. ZoneFlex 7343 front panel elements (Continued)

LED	Description
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 receiving configuration settings (provisioning) or a firmware update.
WLAN LED	• *Off*: The WLAN service is down. • *Amber:* The WLAN service is up and no clients are associated (standalone), or no wireless clients and no downlink MAPs are connected (RAP). • *Green*: The WLAN service is up and at least one wireless client is associated. If Mesh is enabled, no downlink MAPs are connected. • *Fast flashing green*: The WLAN service is up, at least one client is associated, and at least one Mesh downlink is connected. • *Slow flashing green*: At least one Mesh downlink is connected, and no clients are associated.
AIR LED	• *Off*: The Access Point is operating in standalone mode or operating as a root AP (RAP) or a non-mesh AP. • *Green*: The AP is functioning as a RAP or MAP and the uplink signal is *good*. • *Slow flashing green (one flash every two seconds)*: Mesh networking is enabled, but the AP is still searching for a mesh uplink. • *Fast flashing green (two flashes every second)*: The AP is functioning as a MAP and the wireless signal to its uplink AP is *fair*.

Rear Panel

Figure 9 shows the rear panel of the ZoneFlex 7343. For a description of each rear panel part, refer to Table 10.

Figure 9. ZoneFlex 7343 rear panel

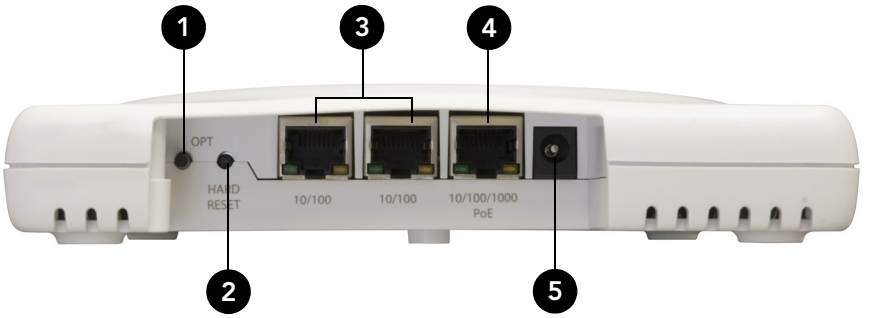


Table 10. ZoneFlex 7343 rear panel elements

Number	Item Name	Description
1	OPT Button	Not active in this model at this time.
2	HARD RESET Button	Pressing, and then quickly releasing this internal button reboots the AP. Pressing and holding it for six seconds resets the AP to factory default settings. **CAUTION!** *Resetting the AP to factory default settings erases all previously configured settings.*
3	10/100 Ports (2)	Two RJ-45 ports for 10/100Mbps connections.
4	10/100/1000 PoE Port	One RJ-45 port for a 10/100/1000 PoE (Power over Ethernet, 802.3af) connection.
5	Power	Connect the power adapter (12 VDC/1.25A) to this socket. Power can also be supplied via the 10/100/1000 PoE (802.3af) port.

ZoneFlex 7352 AP

The ZoneFlex 7352 single-band (2.4 GHz) is a best-performing, mobile-ready, two-stream AP.

NOTE The 100.x AP base images support standalone mode and FlexMaster (FM) WLAN manager operation. The SmartZone-compatible images only support SCG, vSCG, and SZ controllers. The ZD-compatible images only support ZD controllers. The 7352 requires a minimum of AP base image 100.0.0 and later to operate, or SCG 1.1.1 and later, vSCG 2.5 and later, SmartZone 3.2 and later, or ZD 9.5.1 and later to operate.

The 7352 features five LEDs on its front panel and buttons and connectors on its rear panel.

Front Panel

Figure 10 shows the top view of the 7352. For a description of each front panel part, refer to Table 11.

Figure 10. 7352 top view

Table 11. 7352 front panel elements

LED	Description
PWR LED	• *Off*: Off. • *Red*: Boot up in process. • *Green*: On.
OPT LED	Not used in this model.
DIR LED	• *Off*: The AP is not being managed by ZoneDirector (standalone mode). • *Green*: The AP is being managed by ZoneDirector. • *Slow flashing green* (one flash every two seconds): The AP is being managed by ZoneDirector, but is currently unable to communicate with ZoneDirector. • *Fast flashing green* (two flashes every second): The AP is being managed by ZoneDirector and is currently receiving configuration settings (provisioning) or an image update.
WLAN LED	• *Off*: The WLAN service is down. • *Amber:* The WLAN service is up and no clients are associated (standalone), or no wireless clients and no downlink MAPs are connected (RAP). • *Green*: The WLAN service is up and at least one wireless client is associated. If Mesh is enabled, no downlink MAPs are connected. • *Fast flashing green*: The WLAN service is up, at least one client is associated, and at least one Mesh downlink is connected. • *Slow flashing green*: At least one Mesh downlink is connected, and no clients are associated.
AIR LED	• *Off*: The AP is operating in standalone mode or operating as a root AP (RAP) or a non-mesh AP. • *Green*: The AP is functioning as a RAP or MAP and the uplink signal is *good*. • *Slow flashing green (one flash every two seconds)*: Mesh networking is enabled, but the AP is still searching for a mesh uplink. • *Fast flashing green (two flashes every second)*: The AP is functioning as a MAP and the wireless signal to its uplink AP is *fair*.

Rear Panel

Figure 11 shows the rear panel of the 7352 (and 7372). For a description of each rear panel part, refer to Table 12.

Figure 11. 7352/7372 rear panel

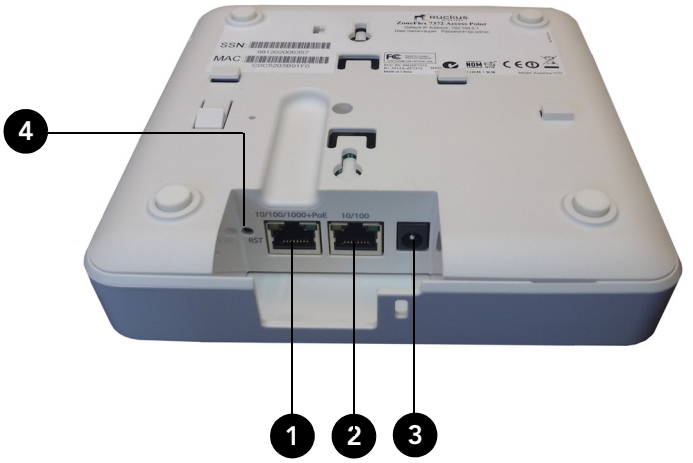


Table 12. 7352/7372 rear panel elements

Number	Item Name	Description
1	10/100/1000+PoE Port	One RJ-45 port for a 10/100/1000 PoE (Power over Ethernet, 802.3af) connection.
2	10/100 Port	One RJ-45 port for a 10/100 connection.
3	Power	Connect the power adapter (12 VDC/1.25A) to this socket. Power can also be supplied via the 10/100/1000 PoE port.
4	RST Button	Pressing, and then quickly releasing this internal button reboots the AP. Pressing and holding it for six seconds resets the AP to factory default settings. **CAUTION!** *Resetting the AP to factory default settings erases all previously configured settings.*

ZoneFlex 7363 AP

The ZoneFlex 7363 is a high-performance, 802.11n mid-range Smart Wi-Fi AP with adaptive antenna technology.

NOTE The 100.x AP base images support standalone mode and FlexMaster (FM) WLAN manager operation. The SmartZone-compatible images only support SCG, vSCG, and SZ controllers. The ZD-compatible images only support ZD controllers. The 7363 requires a minimum of AP base image 100.0.0 and later to operate, or SCG 1.0 and later, vSCG 2.5 and later, or ZD 9.0 and later to operate.

The 7363 features five LEDs on its front panel, and buttons and connectors on its rear panel.

Front Panel

Figure 12 shows the front panel of the 7363. For a description of each front panel part, refer to Table 13.

Figure 12. 7363 top view

Table 13. 7363 front panel elements

LED	Description
PWR LED	• *Off*: Off. • *Amber*: Boot up in process. • *Green*: On.
OPT LED	Not used in this model.

Table 13. 7363 front panel elements (Continued)

LED	Description
DIR LED	• *Off*: The AP is not being managed by ZoneDirector (standalone mode). • *Green*: The AP is being managed by ZoneDirector. • *Slow flashing green* (one flash every two seconds): The AP is being managed by ZoneDirector, but is currently unable to communicate with ZoneDirector. • *Fast flashing green* (two flashes every second): The AP is being managed by ZoneDirector and is currently receiving configuration settings (provisioning) or an image update.
2.4G LED (WLAN)	• *Off*: The WLAN service is down. • *Green*: The WLAN service is up, at least one client is associated, and signal quality is *good* (RSSI >= 15). • *Flashing green (two flashes every second)*: The WLAN service is up but no clients are associated. • *Amber*: The WLAN service is up, at least one client is associated, but signal quality is *poor* (RSSI < 15).
5G LED (WLAN)	• *Off: The WLAN service is down.* • *Green*: The WLAN service is up, at least one client is associated (standalone), or at least one downlink MAP is connected (RAP), or uplink RAP is connected (MAP), and signal quality is good (RSSI >= 15). • *Fast flashing green (two flashes every second)*: The WLAN service is up but no clients are associated (standalone), no downlink MAPs are connected (RAP), or no uplink RAP is connected (MAP). • *Amber*: The WLAN service is up, at least one wireless client is associated (standalone), or at least one downlink MAP is connected (RAP), or uplink RAP is connected (MAP), but signal quality is *poor* (RSSI < 15).

Rear Panel

Figure 13 shows the rear panel of the 7363. For a description of each rear panel part, refer to Table 14.

Figure 13. 7363 rear panel

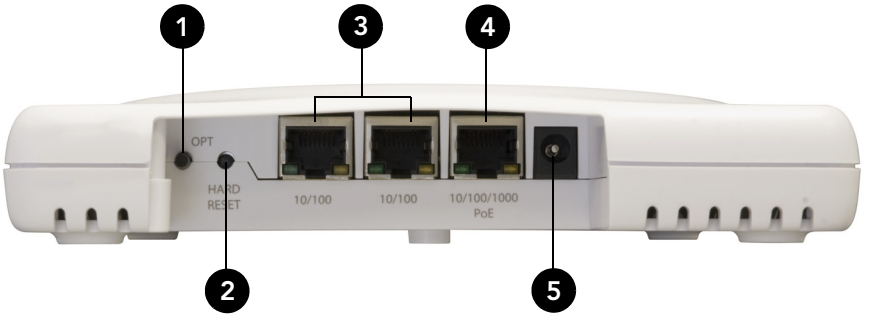


Table 14. 7363 rear panel elements

Number	Item Name	Description
1	OPT Button	Not active in this model at this time.
2	HARD RESET Button	Pressing, and then quickly releasing this internal button reboots the AP. Pressing and holding it for six seconds resets the AP to factory default settings. **CAUTION!** *Resetting the AP to factory default settings erases all previously configured settings.*
3	10/100 Ports (2)	Two RJ-45 ports for 10/100Mbps connections.
4	10/100/1000 PoE Port	One RJ-45 port for a 10/100/1000 PoE (Power over Ethernet, 802.3af) connection.
5	Power	Connect the power adapter (12 VDC/1.25A) to this socket. Power can also be supplied via the 10/100/1000 PoE (802.3af) port.

ZoneFlex 7372 AP

The ZoneFlex 7372 is a best-performing, concurrent dual-band, mobile-ready, two-stream AP.

NOTE The 100.x AP base images support standalone mode and FlexMaster (FM) WLAN manager operation. The SmartZone-compatible images only support SCG, vSCG, and SZ controllers. The ZD-compatible images only support ZD controllers. The 7372 requires a minimum of AP base image 100.0.0 and later to operate, or SCG 1.1.1 and later, vSCG 2.5 and later, SmartZone 3.2 and later, or ZD 9.5.1 and later to operate.

The 7372 features five LEDs on its front panel and buttons and connectors on its rear panel.

Front Panel

Figure 14 shows the top view of the 7372. For a description of each front panel part, refer to Table 15.

Figure 14. 7372 top view

Table 15. 7372 front panel elements

LED	Description
Power LED	• *Off*: Off. • *Red*: Boot up in process. • *Green*: On.
DIR LED	• *Off*: The AP is not being managed by ZoneDirector (standalone mode). • *Green*: The AP is being managed by ZoneDirector. • *Slow flashing green* (one flash every two seconds): The AP is being managed by ZoneDirector, but is currently unable to communicate with ZoneDirector. • *Fast flashing green* (two flashes every second): The AP is being managed by ZoneDirector and is currently receiving configuration settings (provisioning) or an image update.
AIR LED	• *Off*: The AP is operating in standalone mode or operating as a root AP (RAP) or a non-mesh AP. • *Green*: The AP is functioning as a Mesh AP (MAP), and the wireless signal to its uplink AP is good. • *Fast flashing green* (two flashes every second): The AP is functioning as a Mesh AP (MAP), and the wireless signal to its uplink AP is fair. • *Slow flashing green* (one flash every two seconds): Mesh networking is enabled, but the AP is still searching for a mesh uplink.
2.4GHz LED	• *Off*: The WLAN service is down. • *Green*: The WLAN is up and at least one client is associated. • *Amber*: The WLAN is up. No clients are associated.

Table 15. 7372 front panel elements (Continued)

LED	Description
5GHz LED	• *Off*: The WLAN service is down. • *Amber*: The WLAN is up, but no clients or downlink MAPs are associated/connected. • *Green*: The WLAN is up and at least one client is associated. No downlink MAPs are connected. • *Slow flashing green* (one flash every two seconds): The WLAN is up and at least one downlink MAP is connected. No clients are associated. • *Fast flashing green* (two flashes every second): The WLAN is up, at least one downlink MAP is connected, and at least one client is associated.

Rear Panel

The rear panel of the 7372 is the same as the 7352. See Figure 11.

ZoneFlex 7372-E AP

The ZoneFlex 7372-E is a best-performing, concurrent dual-band, mobile-ready, two-stream AP, with two RP-SMA connectors used to support dual-band 2.4GHz and 5GHz external antennas.

NOTE The 100.x AP base images support standalone mode and FlexMaster (FM) WLAN manager operation. The SmartZone-compatible images only support SCG, vSCG, and SZ controllers. The ZD-compatible images only support ZD controllers. The 7372-E requires a minimum of AP base image 100.0.0 and later to operate, or SCG 2.1 and later, vSCG 2.5 and later, SmartZone 3.2 and later, or ZD 9.6 and later to operate.

The 7372-E features five LEDs on its front panel and buttons and connectors on its rear panel.

Front Panel

Figure 14 shows the top view of the 7372-E. For a description of each front panel part, refer to Table 15.

Figure 15. 7372-E top view

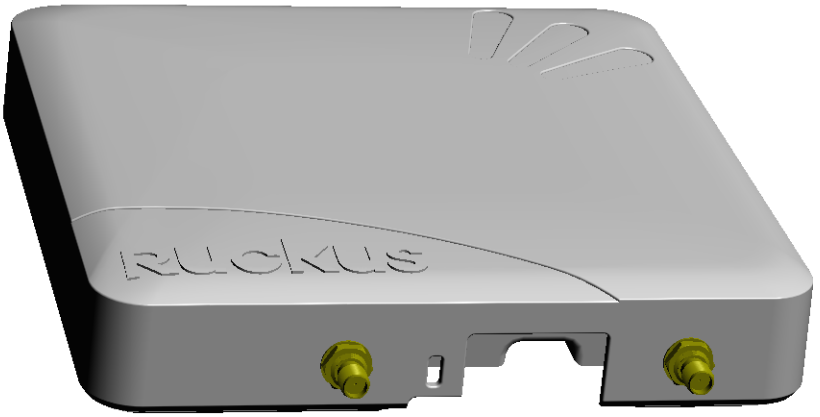


Table 16. 7372-E front panel elements

LED	Description
Power LED	• *Off*: Off. • *Red*: Boot up in process. • *Green*: On.
DIR LED	• *Off*: The AP is not being managed by ZoneDirector (standalone mode). • *Green*: The AP is being managed by ZoneDirector. • *Slow flashing green* (one flash every two seconds): The AP is being managed by ZoneDirector, but is currently unable to communicate with ZoneDirector. • *Fast flashing green* (two flashes every second): The AP is being managed by ZoneDirector and is currently receiving configuration settings (provisioning) or an image update.
AIR LED	• *Off*: The AP is operating in standalone mode or operating as a root AP (RAP) or a non-mesh AP. • *Green*: The AP is functioning as a Mesh AP (MAP), and the wireless signal to its uplink AP is good. • *Fast flashing green* (two flashes every second): The AP is functioning as a Mesh AP (MAP), and the wireless signal to its uplink AP is fair. • *Slow flashing green* (one flash every two seconds): Mesh networking is enabled, but the AP is still searching for a mesh uplink.
2.4GHz LED	• *Off*: The WLAN service is down. • *Green*: The WLAN is up and at least one client is associated. • *Amber*: The WLAN is up. No clients are associated.

Table 16. 7372-E front panel elements (Continued)

LED	Description
5GHz LED	• *Off*: The WLAN service is down. • *Amber*: The WLAN is up, but no clients or downlink MAPs are associated/connected. • *Green*: The WLAN is up and at least one client is associated. No downlink MAPs are connected. • *Slow flashing green* (one flash every two seconds): The WLAN is up and at least one downlink MAP is connected. No clients are associated. • *Fast flashing green* (two flashes every second): The WLAN is up, at least one downlink MAP is connected, and at least one client is associated.

Rear Panel

Figure 16 shows the rear panel of the 7372-E. For a description of each rear panel part, refer to Table 17.

Figure 16. 7372-E rear panel

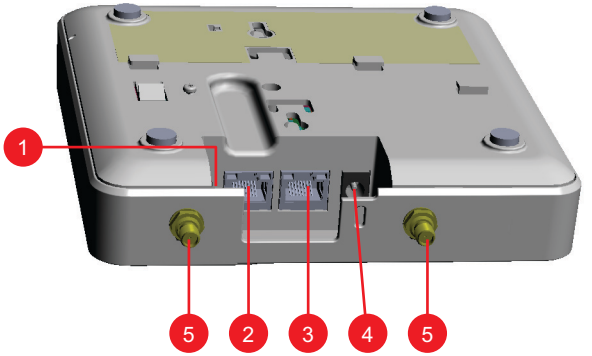


Table 17. 7372-E rear panel elements

Number	Item Name	Description
1	RST Button	Pressing, and then quickly releasing this internal button reboots the AP. Pressing and holding it for six seconds resets the AP to factory default settings. **CAUTION!** *Resetting the AP to factory default settings erases all previously configured settings.*
2	10/100/1000+PoE Port	One RJ-45 port for a 10/100/1000 PoE (Power over Ethernet, 802.3af) connection.
3	10/100 Port	One RJ-45 port for a 10/100 connection.
4	Power	Connect the power adapter (12 VDC/1.25A) to this socket. Power can also be supplied via the 10/100/1000 PoE port.
5 (two places)	RP-SMA connectors	Connect to dual-band 2.4GHz and 5GHz external antennas.

ZoneFlex 7441 DAS AP

The ZoneFlex 7441 is a Wi-Fi AP used on coax distributed antenna system (DAS) networks.

NOTE The 100.x AP base images support standalone mode and FlexMaster (FM) WLAN manager operation. The SmartZone-compatible images only support SCG, vSCG, and SZ controllers. The ZD-compatible images only support ZD controllers. The 7441 requires a minimum of AP base image 100.0.0 and later to operate, or SCG 2.5 and later, vSCG 2.5 and later, SmartZone 3.2 and later, or ZD 9.7 and later to operate.

The 7441 features five LEDs, power, network and DAS coaxial connectors on its front panel.

Front Panel

Figure 17 shows the front view of the 7441. For a description of each front panel part, refer to Table 18.

Figure 17. 7441 top view

Table 18. 7441 front panel elements

LED	Description
Ground post	Attach the ground wire using the included terminal ring and hex nuts.
Power socket	DC power socket.
Reset button	Resets the AP to factory default settings if held for more than 5 seconds.

Table 18. 7441 front panel elements (Continued)

LED	Description
10/100/1000 PoE Ethernet port	One RJ-45 port for a 10/100/1000 802.3af PoE (Power over Ethernet) connection.
PWR LED	• *Off*: Off. • *Red*: Boot up in process. • *Green*: On.
DIR LED	• *Off*: The AP is not being managed by ZoneDirector (standalone mode). • *Green*: The AP is being managed by ZoneDirector. • *Slow flashing green* (one flash every two seconds): The AP is being managed by ZoneDirector, but is currently unable to communicate with ZoneDirector. • *Fast flashing green* (two flashes every second): The AP is being managed by ZoneDirector and is currently receiving configuration settings (provisioning) or an image update.
2.4G LED	• *Off*: The WLAN service is down. • *Green*: The WLAN service is up and at least one client is associated with it. • *Flashing green*: The WLAN service is up and no clients are associated.
5G LED	• *Off: The WLAN service is down.* • *Green*: The WLAN service is up and at least one client is associated. • *Flashing green*: The WLAN service is up and no clients are associated.
AIR LED	• Not used at this time.
Cable antenna connector	• Type N female coaxial cable connector for in-building DAS wireless systems.

ZoneFlex 7982 AP

The ZoneFlex 7982 is a high-capacity, high-performing, three-stream AP for carriers and enterprises.

NOTE The 100.x AP base images support standalone mode and FlexMaster (FM) WLAN manager operation. The SmartZone-compatible images only support SCG, vSCG, and SZ controllers. The ZD-compatible images only support ZD controllers. The 7982 requires a minimum of AP base image 100.0.0 and later to operate, or SCG 1.1 and later, vSCG 2.5 and later, SmartZone 3.2 and later, or ZD 9.4 and later to operate.

The 7982 features five LEDs on its front panel and buttons and connectors on its rear panel.

Front Panel

Figure 18 shows the top view of the 7982. For a description of each front panel part, refer to Table 19.

Figure 18. 7982 top view

Table 19. 7982 front panel elements

LED	Description
Power LED	• *Off*: Off. • *Red*: Boot up in process. • *Green*: On.
DIR LED	• *Off*: The AP is not being managed by ZoneDirector (standalone mode). • *Green*: The AP is being managed by ZoneDirector. • *Slow flashing green* (one flash every two seconds): The AP is being managed by ZoneDirector, but is currently unable to communicate with ZoneDirector. • *Fast flashing green* (two flashes every second): The AP is being managed by ZoneDirector and is currently receiving configuration settings (provisioning) or an image update.
AIR LED	• *Off*: The AP is operating in standalone mode or operating as a root AP (RAP) or a non-mesh AP. • *Green*: The AP is functioning as a Mesh AP (MAP), and the wireless signal to its uplink AP is good. • *Fast flashing green* (two flashes every second): The AP is functioning as a Mesh AP (MAP), and the wireless signal to its uplink AP is fair. • *Slow flashing green* (one flash every two seconds): Mesh networking is enabled, but the AP is still searching for a mesh uplink.
2.4GHz LED	• *Off*: The WLAN service is down. • *Green*: The WLAN is up and at least one client is associated. • *Amber*: The WLAN is up. No clients are associated.

Table 19. 7982 front panel elements (Continued)

LED	Description
5GHz LED	• *Off*: The WLAN service is down. • *Amber*: The WLAN is up, but no clients or downlink MAPs are associated/connected. • *Green*: The WLAN is up and at least one client is associated. No downlink MAPs are connected. • *Slow flashing green* (one flash every two seconds): The WLAN is up and at least one downlink MAP is connected. No clients are associated. • *Fast flashing green* (two flashes every second): The WLAN is up, at least one downlink MAP is connected, and at least one client is associated.

Rear Panel

Figure 19 shows the rear panel of the 7982. For a description of each rear panel part, refer to Table 20.

Figure 19. 7982 rear panel

Table 20. 7982 rear panel elements

Number	Item Name	Description
1	ETHERNET + PoE Port	One RJ-45 port for a 10/100/1000 PoE (Power over Ethernet, 802.3af/at) connection (**Note**).
2	ETHERNET Port	One RJ-45 port for a 10/100/1000 connection.
3	12V 1.5A Power Socket	Connect the power adapter (12 VDC/1.25A) to this socket. Power can also be supplied via the ETHERNET + PoE port.
4	RESET Button	Pressing, and then quickly releasing this internal button reboots the AP. Pressing and holding it for six seconds resets the AP to factory default settings. CAUTION! *Resetting the AP to factory default settings erases all settings that you configured previously.*
Note: Class 4 device. Some PoE+ switches reserve 30W for Class 4 device by default.		

Table 21. Behavior of Ethernet port LEDs on 7982

LEDs	Description
Off	Not connected
Amber + Green	Connected to 10Mbps device
Amber	Connected to 100Mbps device
Green	Connected to 1000Mbps device

WARNING! *For units with Power over Ethernet (PoE)*. These products and all interconnected 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.

ZoneFlex H500 AP Wall Switch

The H500 is a high-capacity, high-performing, two-stream, dual-band, 802.11ac, multimedia Wi-Fi AP wall switch with adaptive antenna technology for carriers and enterprises.

NOTE The 100.x AP base images support standalone mode and FlexMaster (FM) WLAN manager operation. The SmartZone-compatible images only support SCG, vSCG, and SZ controllers. The ZD-compatible images only support ZD controllers. The H500 AP requires a minimum of AP base image 100.1.0 and later to operate, or SCG 3.1 and later, vSCG 3.0 and later, SmartZone 3.2 and later, or ZD 9.10 and later to operate.

The H500 has many options:

- It can be mounted on a standard USA- or EU-style single-gang wall outlet box.
- It can be powered by a customer-supplied IEEE 802.3af- or 802.3at-compliant PoE switch or injector, or can be powered by an optional customer-ordered DC power adapter.
- It has side cutouts for one or two bypass cables. The mounting bracket has locating hooks to keep the bypass cables aligned with the cutouts when attaching the H500 to the mounting base.
- It can have a low-power (0.5W or less) customer-supplied USB device plugged in. The USB port is intended for low-power devices such as BLE (Bluetooth low energy) beacons.

The H500 has four LEDs, one RJ-45 connector, and a reset button on its rear panel, and has one USB port (refer to Appendix: AP Support for Bluetooth Low Energy Devices), four RJ-45 connectors, and one DC power connector on its bottom panel.

About Peripheral Devices

The H500 can supply power to USB devices and PoE-powered devices, and the power supplied depends on the PoE power supplied to the H500.

- The USB port is intended for low-power devices such as BLE beacons. The maximum power that the USB port can supply is 0.5W.
- The LAN1+PoE port is intended for PoE-powered peripheral devices such as IP telephones.

For a description of the input and output power options, refer to Table 22.

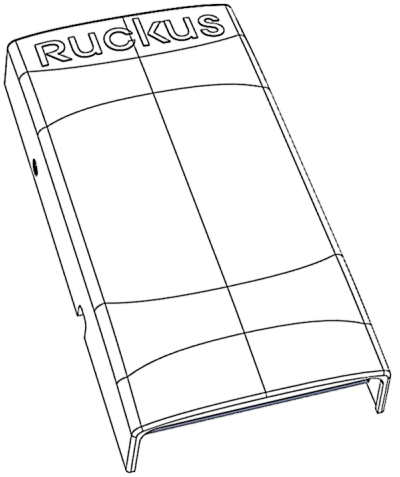
Table 22. H500 power options and available power out for PoE out and USB

H500 Power Source	Power Available for PoE Out and USB
802.3af PoE	5W total
802.3at PoE	12.95W PoE Out (802.3af Class 3) and 0.5W USB
DC power adapter (sold separately)	12.95W PoE Out (802.3af Class 3) and 0.5W USB

Front Panel

Figure 20 shows the front view of the H500.

Figure 20. H500 front view



Rear Panel

Figure 21 shows the rear view of the H500. For a description of each rear panel part, refer to Table 23.

Figure 21. H500 rear view

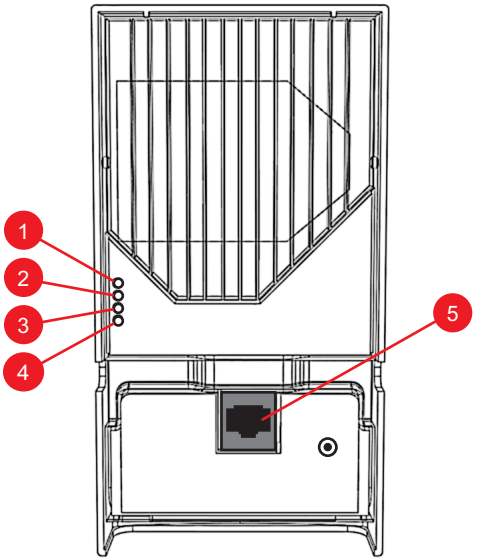


Table 23. H500 rear panel elements

No.	LED	Description
1	PWR	• *Off*: Off. • *Red*: Boot up in process. • *Green*: On.

Table 23. H500 rear panel elements (Continued)

No.	LED	Description
2	CTL	• *Off*: The AP is not being managed by a Ruckus Wireless controller (standalone mode). • *Green*: The AP is being managed by a Ruckus Wireless controller. • *Slow flashing green* (one flash every two seconds): The AP is being managed by a Ruckus Wireless controller, but is currently unable to communicate with the controller. • *Fast flashing green* (two flashes every second): The AP is being managed by a Ruckus Wireless controller and is currently receiving configuration settings (provisioning) or an image update.
3	2 (2.4GHz WLAN)	• *Off*: The 2.4GHz WLAN service is down. • *Green*: The WLAN service is up, at least one client is associated, and signal quality is good (RSSI >= 15). • *Amber*: The WLAN service is up but no clients are associated.
4	5 (5GHz WLAN)	• *Off*: The 5GHz WLAN service is down. • *Green*: The WLAN service is up, at least one client is associated, and no downlink MAPs are connected. • *Slow flashing green* (one flash every two seconds): The WLAN service is up, at least one downlink MAP is connected, and no clients are associated. • *Fast flashing green* (two flashes every second): The WLAN service is up, at least one downlink MAP is connected, and at least one client is associated. • *Amber*: The WLAN service is up, but no clients or downlink MAPs are associated or connected.
5	PoE In Port	One RJ-45 port for a 10/100/1000 PoE (Power over Ethernet, 802.3af/at Class 3 or 4) connection.

Bottom Panel

Figure 22 shows the bottom view of the H500. For a description of each bottom panel part, refer to Table 24.

Figure 22. H500 bottom panel

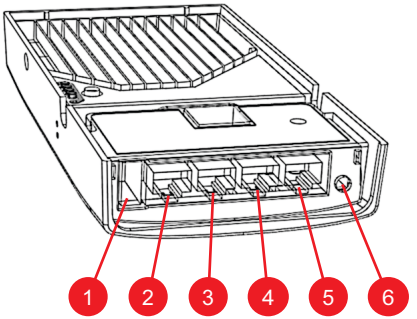


Table 24. H500 bottom panel elements

No.	Item Name	Description
1	USB port	Optional USB connector (refer to About Peripheral Devices and Appendix: AP Support for Bluetooth Low Energy Devices).
2	LAN4 port	10/100 RJ-45 Ethernet Port.
3	LAN3 port	10/100 RJ-45 Ethernet Port.
4	LAN2 port	10/100 RJ-45 Ethernet Port.
5	LAN1+PoE port	10/100 RJ-45 LAN port with PoE out. Supports 802.3af PSE Class 2 or 3 (depending on power input; refer to About Peripheral Devices).
6	48VDC port	Optional 48VDC power input connector.

Reset Buttons

Figure 23 shows and Table 25 describes the reset buttons on the side of the H500.

Figure 23. H500 side panel reset buttons

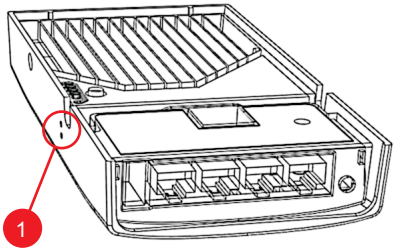


Table 25. H500 side panel elements

No.	Item Name	Description
1	Soft Reset and Hard Reset buttons	The two reset buttons on the side of the H500 are used to reboot or factory reset the AP.

- Use a straightened paper clip to press and release the **Soft Reset** button for eight seconds or more to reset the AP to factory defaults.
- Use a straightened paper clip to press and hold the **Hard Reset** button to reboot the AP. This is the same as removing power and then and restoring power to the H500.

CAUTION! *Resetting the AP to factory default settings erases all previously configured settings.*

ZoneFlex R300 AP

The R300 is a high-capacity, high-performing, two-stream, dual-band, 802.11n AP with adaptive antenna technology for carriers and enterprises.

NOTE The 100.x AP base images support standalone mode and FlexMaster (FM) WLAN manager operation. The SmartZone-compatible images only support SCG, vSCG, and SZ controllers. The ZD-compatible images only support ZD controllers. The R300 AP requires a minimum of AP base image 100.0.0 and later to operate, or SCG 2.5 and later, vSCG 2.5 and later, SmartZone 3.2 and later, or ZD 9.6.1 and later to operate.

The R300 features five LEDs on its front panel and buttons and connectors on its rear panel.

NOTE The R300 is an entry level 802.11n dual-band AP that does not support the Smart Mesh or Spectrum Analysis features, and supports a maximum of 250 unencrypted clients.

Front Panel

Figure 24 shows the top view of the R300. For a description of each front panel part, refer to Table 26.

Figure 24. R300 top view

Table 26. R300 front panel elements

LED	Description
PWR LED	• *Off*: Off. • *Red*: Boot up in process. • *Green*: On.
OPT LED	Not used in this model.
DIR LED	• *Off*: The AP is not being managed by ZoneDirector (standalone mode). • *Green*: The AP is being managed by ZoneDirector. • *Slow flashing green* (one flash every two seconds): The AP is being managed by ZoneDirector, but is currently unable to communicate with ZoneDirector. • *Fast flashing green* (two flashes every second): The AP is being managed by ZoneDirector and is currently receiving configuration settings (provisioning) or an image update.
2.4G LED (WLAN)	• *Off*: The WLAN service is down. • *Green:* The WLAN service is up and at least one client is associated. • *Amber:* The WLAN service is up and no clients are associated.
5G LED (WLAN)	• *Off*: The WLAN service is down. • *Green:* The WLAN service is up and at least one client is associated. • *Amber:* The WLAN service is up and no clients are associated.

Rear Panel

The rear panel of the R300 features one 10/100/1000 PoE Ethernet port, power socket and reset button. See Table 27 for a description of each rear panel part.

Figure 25. R300 rear panel

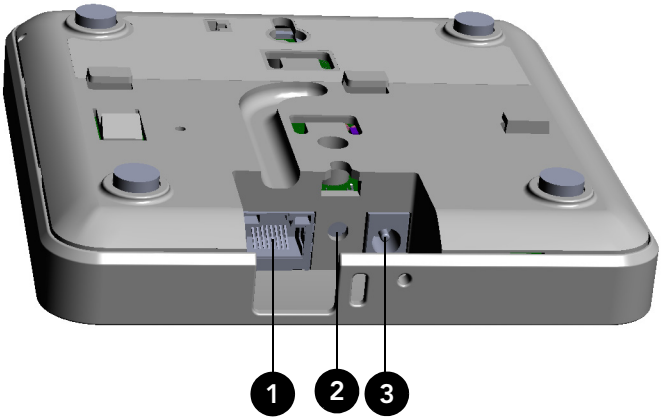


Table 27. R300 rear panel elements

Number	Item Name	Description
1	10/100/ 1000+PoE Port	One RJ-45 port for a 10/100/1000 PoE (Power over Ethernet, 802.3af) connection.
2	RST Button	Pressing, and then quickly releasing this internal button reboots the AP. Pressing and holding it for six seconds resets the AP to factory default settings. **CAUTION!** *Resetting the AP to factory default settings erases all previously configured settings.*
3	Power	Connect the power adapter (12 VDC/1.25A) to this socket. Power can also be supplied via the 10/100/1000 PoE port.

ZoneFlex R500 AP

The R500 is a high-performance 2x2:2 802.11ac dual-band AP.

NOTE The 100.x AP base images support standalone mode and FlexMaster (FM) WLAN manager operation. The SmartZone-compatible images only support SCG, vSCG, and SZ controllers. The ZD-compatible images only support ZD controllers. The R500 AP requires a minimum of AP base image 100.0.0 and later to operate, or SCG 2.5.1 and later, vSCG 3.0 and later, SmartZone 3.2 and later, or ZD 9.8.1 and later to operate.

The R500 features five LEDs on its front panel and buttons and connectors on its rear panel.

Front Panel

Figure 26 shows the top view of the R500. For a description of the front panel LEDs, refer to Table 28.

Figure 26. R500 top view

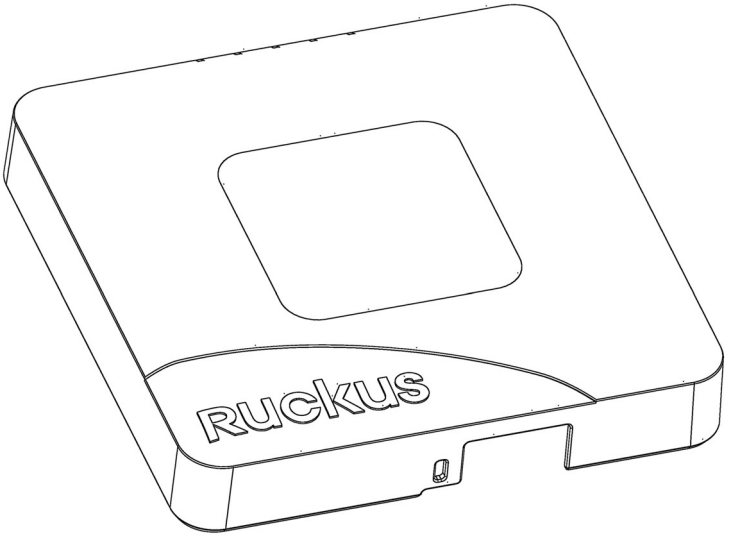


Table 28. R500 front panel LEDs

LED	Description
PWR	• *Off*: Off. • *Red*: Boot up in process. • *Green*: On.
DIR	• *Off*: The AP is not being managed by ZoneDirector (standalone mode). • *Green*: The AP is being managed by ZoneDirector. • *Slow flashing green* (one flash every two seconds): The AP is being managed by ZoneDirector, but is currently unable to communicate with ZoneDirector. • *Fast flashing green* (two flashes every second): The AP is being managed by ZoneDirector and is currently receiving configuration settings (provisioning) or an image update.
AIR	• *Off*: The AP is operating in standalone mode or operating as a root AP (RAP) or a non-mesh AP. • *Green*: The AP is functioning as a Mesh AP (MAP), and the wireless signal to its uplink AP is good. • *Fast flashing green* (two flashes every second): The AP is functioning as a Mesh AP (MAP), and the wireless signal to its uplink AP is fair. • *Slow flashing green* (one flash every two seconds): Mesh networking is enabled, but the AP is still searching for a mesh uplink.
2.4G	• *Off*: The WLAN service is down. • *Green*: The WLAN is up and at least one client is associated. • *Amber*: The WLAN is up. No clients are associated.

Table 28. R500 front panel LEDs (Continued)

LED	Description
5G	• *Off*: The WLAN service is down. • *Amber*: The WLAN is up, but no clients or downlink MAPs are associated/connected. • *Green*: The WLAN is up and at least one client is associated. No downlink MAPs are connected. • *Slow flashing green* (one flash every two seconds): The WLAN is up and at least one downlink MAP is connected. No clients are associated. • *Fast flashing green* (two flashes every second): The WLAN is up, at least one downlink MAP is connected, and at least one client is associated.

Rear Panel

The rear panel of the R500 features one 10/100/1000 PoE Ethernet port, 10/100/1000 Ethernet port, power socket and reset button. See Table 29 for a description of each rear panel part.

Figure 27. R500 rear panel

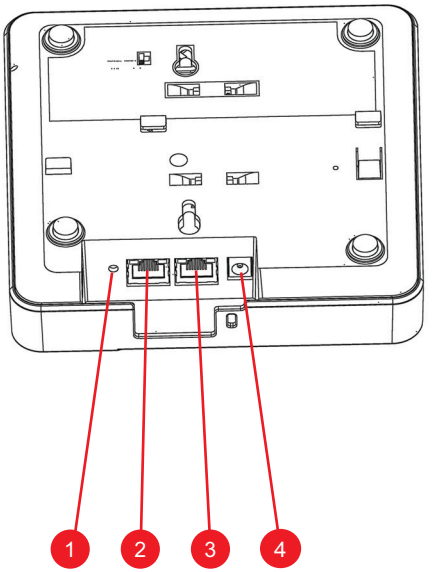


Table 29. Rear panel element descriptions

No.	Label	Description
1	**RESET** Button	Pressing, and then quickly releasing this button reboots the AP. Pressing and holding it for six seconds resets the AP to factory default settings. **CAUTION!** *Resetting the AP to factory default settings erases all settings that you configured previously.*
2	**PoE** Port	One RJ-45 port for a 10/100/1000 PoE (Power over Ethernet, 802.3af/at) connection. (The R500 is a Class 3 device.)
3	Ethernet Port	One RJ-45 port for a 10/100/1000 connection.

Table 29. Rear panel element descriptions (Continued)

No.	Label	Description
4	12VDC	Connect the power adapter (12 VDC/1.25A) to this socket. Power can also be supplied via the 10/100/1000 PoE port.

Table 30. Behavior of Ethernet port LEDs on the R500

LEDs	Description
Off	Not connected
Amber + Green	Connected to 10Mbps device
Amber	Connected to 100Mbps device
Green	Connected to 1000Mbps device

WARNING! *For units using Power over Ethernet (PoE)*. These products and all interconnected 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.

ZoneFlex R600 AP

The R600 is a high-performance 3x3:2 802.11ac dual-band AP.

NOTE The 100.x AP base images support standalone mode and FlexMaster (FM) WLAN manager operation. The SmartZone-compatible images only support SCG, vSCG, and SZ controllers. The ZD-compatible images only support ZD controllers. The R600 AP requires a minimum of AP base image 100.0.0 and later to operate, or SCG 2.5.1 and later, vSCG 3.0 and later, SmartZone 3.2 and later, or ZD 9.8.1 and later to operate.

The R600 features five LEDs on its front panel and buttons and connectors on its rear panel.

Front Panel

Figure 28 shows the top view of the R600. For a description of the front panel LEDs, refer to Table 31.

Figure 28. R600 top view

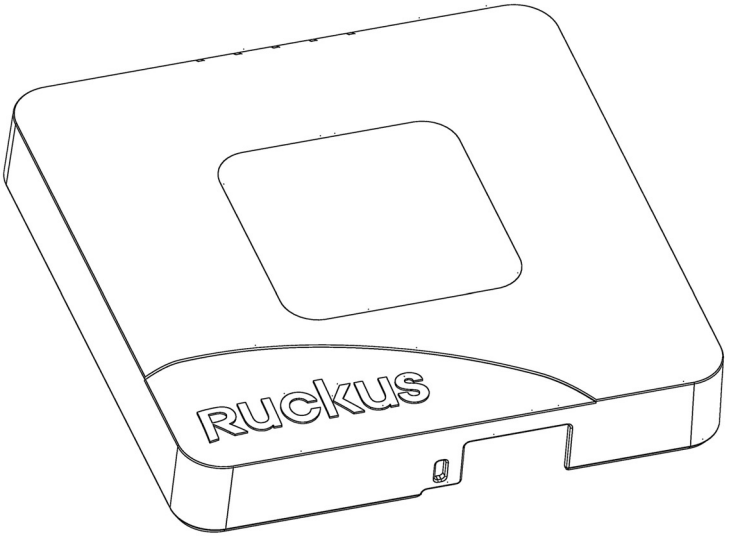


Table 31. R600 front panel LEDs

LED	Description
PWR	• *Off*: Off. • *Red*: Boot up in process. • *Green*: On.
DIR	• *Off*: The AP is not being managed by ZoneDirector (standalone mode). • *Green*: The AP is being managed by ZoneDirector. • *Slow flashing green* (one flash every two seconds): The AP is being managed by ZoneDirector, but is currently unable to communicate with ZoneDirector. • *Fast flashing green* (two flashes every second): The AP is being managed by ZoneDirector and is currently receiving configuration settings (provisioning) or an image update.
AIR	• *Off*: The AP is operating in standalone mode or operating as a root AP (RAP) or a non-mesh AP. • *Green*: The AP is functioning as a Mesh AP (MAP), and the wireless signal to its uplink AP is good. • *Fast flashing green* (two flashes every second): The AP is functioning as a Mesh AP (MAP), and the wireless signal to its uplink AP is fair. • *Slow flashing green* (one flash every two seconds): Mesh networking is enabled, but the AP is still searching for a mesh uplink.
2.4G	• *Off*: The WLAN service is down. • *Green*: The WLAN is up and at least one client is associated. • *Amber*: The WLAN is up. No clients are associated.

Table 31. R600 front panel LEDs (Continued)

LED	Description
5G	• *Off*: The WLAN service is down. • *Amber*: The WLAN is up, but no clients or downlink MAPs are associated/connected. • *Green*: The WLAN is up and at least one client is associated. No downlink MAPs are connected. • *Slow flashing green* (one flash every two seconds): The WLAN is up and at least one downlink MAP is connected. No clients are associated. • *Fast flashing green* (two flashes every second): The WLAN is up, at least one downlink MAP is connected, and at least one client is associated.

Rear Panel

The rear panel of the R600 features one 10/100/1000 PoE Ethernet port, 10/100/1000 Ethernet port, power socket and reset button. See Table 32 for a description of each rear panel part.

Figure 29. R600 rear panel

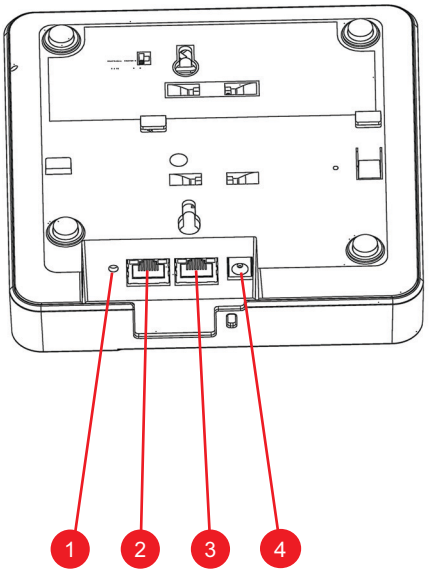


Table 32. Rear panel element descriptions

No.	Label	Description
1	**RESET** Button	Pressing, and then quickly releasing this button reboots the AP. Pressing and holding it for six seconds resets the AP to factory default settings. **CAUTION!** *Resetting the AP to factory default settings erases all settings that you configured previously.*
2	**PoE** Port	One RJ-45 port for a 10/100/1000 PoE (Power over Ethernet, 802.3af/at) connection. (The R600 is a Class 3 device.)
3	Ethernet Port	One RJ-45 port for a 10/100/1000 connection.

Table 32. Rear panel element descriptions (Continued)

No.	Label	Description
4	12VDC	Connect the power adapter (12 VDC/1.25A) to this socket. Power can also be supplied via the 10/100/1000 PoE port.

Table 33. Behavior of Ethernet port LEDs on the R600

LEDs	Description
Off	Not connected
Amber + Green	Connected to 10Mbps device
Amber	Connected to 100Mbps device
Green	Connected to 1000Mbps device

WARNING! *For units using Power over Ethernet (PoE)*. These products and all interconnected 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.

ZoneFlex R700 AP

The R700 is a high-capacity, high-performance, three-stream, 802.11ac dual-band AP with adaptive antenna technology for carriers and enterprises.

NOTE The 100.x AP base images support standalone mode and FlexMaster (FM) WLAN manager operation. The SmartZone-compatible images only support SCG, vSCG, and SZ controllers. The ZD-compatible images only support ZD controllers. The R700 AP requires a minimum of AP base image 100.0.0 and later to operate, or SCG 2.1.2 and later, vSCG 2.5 and later, SmartZone 3.2 and later, or ZD 9.7.1 and later to operate.

The R700 features five LEDs on its front panel and buttons and connectors on its rear panel.

Front Panel

Figure 30 shows the top view of the R700. For a description of each front panel part, refer to Table 34.

Figure 30. R700 top view

Table 34. R700 front panel elements

LED	Description
Power LED	• *Off*: Off. • *Red*: Boot up in process. • *Green*: On.
DIR LED	• *Off*: The AP is not being managed by ZoneDirector (standalone mode). • *Green*: The AP is being managed by ZoneDirector. • *Slow flashing green* (one flash every two seconds): The AP is being managed by ZoneDirector, but is currently unable to communicate with ZoneDirector. • *Fast flashing green* (two flashes every second): The AP is being managed by ZoneDirector and is currently receiving configuration settings (provisioning) or an image update.
AIR LED	• *Off*: The AP is operating as a Standalone or Root AP (RAP), or as a non-mesh AP. • *Green*: The AP is functioning as a Mesh AP (MAP), and the wireless signal to its uplink AP is good. • *Fast flashing green* (two flashes every second): The AP is functioning as a Mesh AP (MAP), and the wireless signal to its uplink AP is fair. • *Slow flashing green* (one flash every two seconds): Mesh networking is enabled, but the AP is still searching for a mesh uplink.
2.4GHz LED	• *Off*: The WLAN service is down. • *Green*: The WLAN is up and at least one client is associated. • *Amber*: The WLAN is up. No clients are associated.

Table 34. R700 front panel elements (Continued)

LED	Description
5GHz LED	• *Off*: The WLAN service is down. • *Amber*: The WLAN is up, but no clients or downlink MAPs are associated/connected. • *Green*: The WLAN is up and at least one client is associated. No downlink MAPs are connected. • *Slow flashing green* (one flash every two seconds): The WLAN is up and at least one downlink MAP is connected. No clients are associated. • *Fast flashing green* (two flashes every second): The WLAN is up, at least one downlink MAP is connected, and at least one client is associated.

Rear Panel

The rear panel of the R700 features one 10/100/1000 PoE Ethernet port, 10/100/1000 Ethernet port, power socket and reset button. See Table 35 for a description of each rear panel part.

Figure 31. R700 rear panel

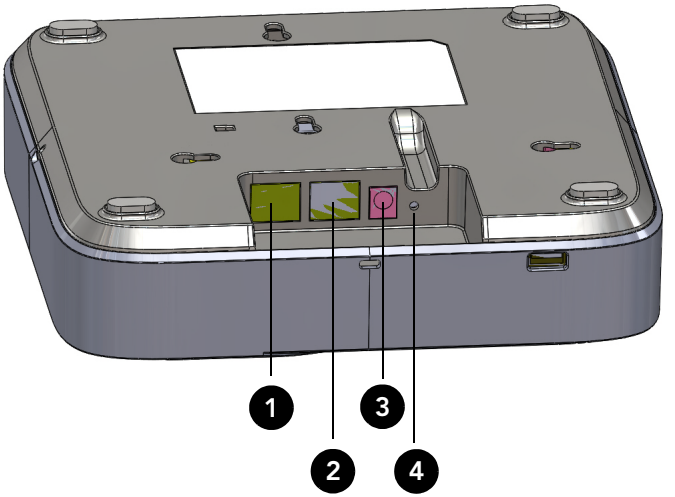


Table 35. R700 rear panel elements

Number	Item Name	Description
1	ETHERNET + PoE Port	One RJ-45 port for a 10/100/1000 PoE (Power over Ethernet, 802.3af/at) connection. (The R700 is a Class 3 device.)
2	ETHERNET Port	One RJ-45 port for a 10/100/1000 connection.
3	12V 1.5A Power Socket	Connect the power adapter (12 VDC/1.25A) to this socket. Power can also be supplied via the ETHERNET + PoE port.
4	RESET Button	Pressing, and then quickly releasing this internal button reboots the AP. Pressing and holding it for six seconds resets the AP to factory default settings. **CAUTION!** *Resetting the AP to factory default settings erases all settings that you configured previously.*

Table 36. Behavior of Ethernet port LEDs on R700

LEDs	Description
Off	Not connected
Amber + Green	Connected to 10Mbps device
Amber	Connected to 100Mbps device
Green	Connected to 1000Mbps device

WARNING! *For units using Power over Ethernet (PoE)*. These products and all interconnected 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.

Installing the AP

3

In this chapter:

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 AP.

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

- Performing a Site Survey
- Preparing the Required Hardware and Tools
- Determining the Optimal Mounting Location and Orientation

Performing a Site Survey

Before installing the AP, perform a site survey to determine the optimal AP placement for maximum range, coverage, and network performance. Ruckus Wireless Support can supply Site Survey best practices information. 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 are generally 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 antennas higher off of the ground.
- *Physical environment*: Clear or open areas provide better radio range than crowded 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 AP 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, and 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 AP placement guidelines, refer to Determining the Optimal Mounting Location and Orientation.

Preparing the Required Hardware and Tools

You must supply the following tools and equipment:

- A notebook computer running Windows (2000/XP/Vista/7) or Mac OS X with an Internet browser and one wireless 802.11a/b/g/n network card and one Ethernet card installed.
- A modem (DSL or cable), 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.
- Two Ethernet cables (Cat5e or better for PoE in)
- (Optional) An AC power adapter (sold separately),

  --or--

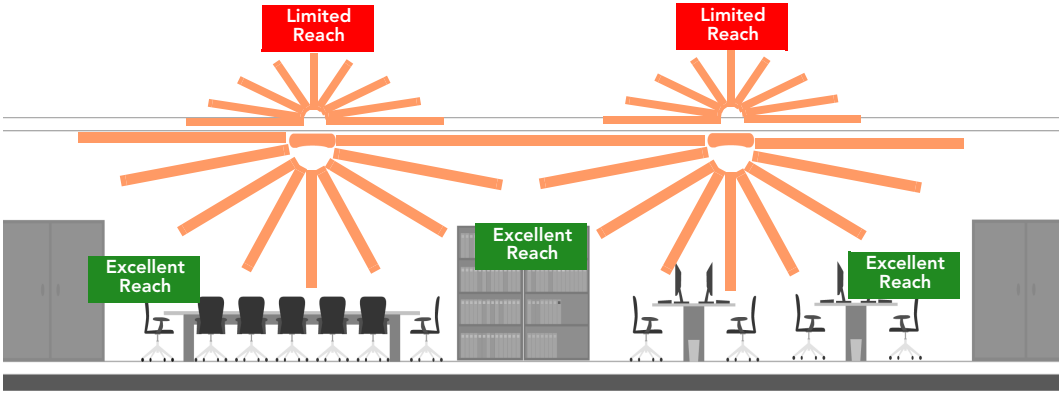
  (Optional) an 802.3af or 802.3at -compliant Power over Ethernet (PoE) switch or PoE injector.

NOTE If the AP is deployed with SCG, vSCG, SZ or ZD controllers, or with SAMs controllers, then follow the instructions in the associated controller user documents to connect the AP to your Ethernet network.

Determining the Optimal Mounting Location and Orientation

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

Figure 32. Recommended ceiling mounting orientation



When wall mounted, the APs should be staggered to maximize coverage.

Figure 33. Recommended wall mounting orientation

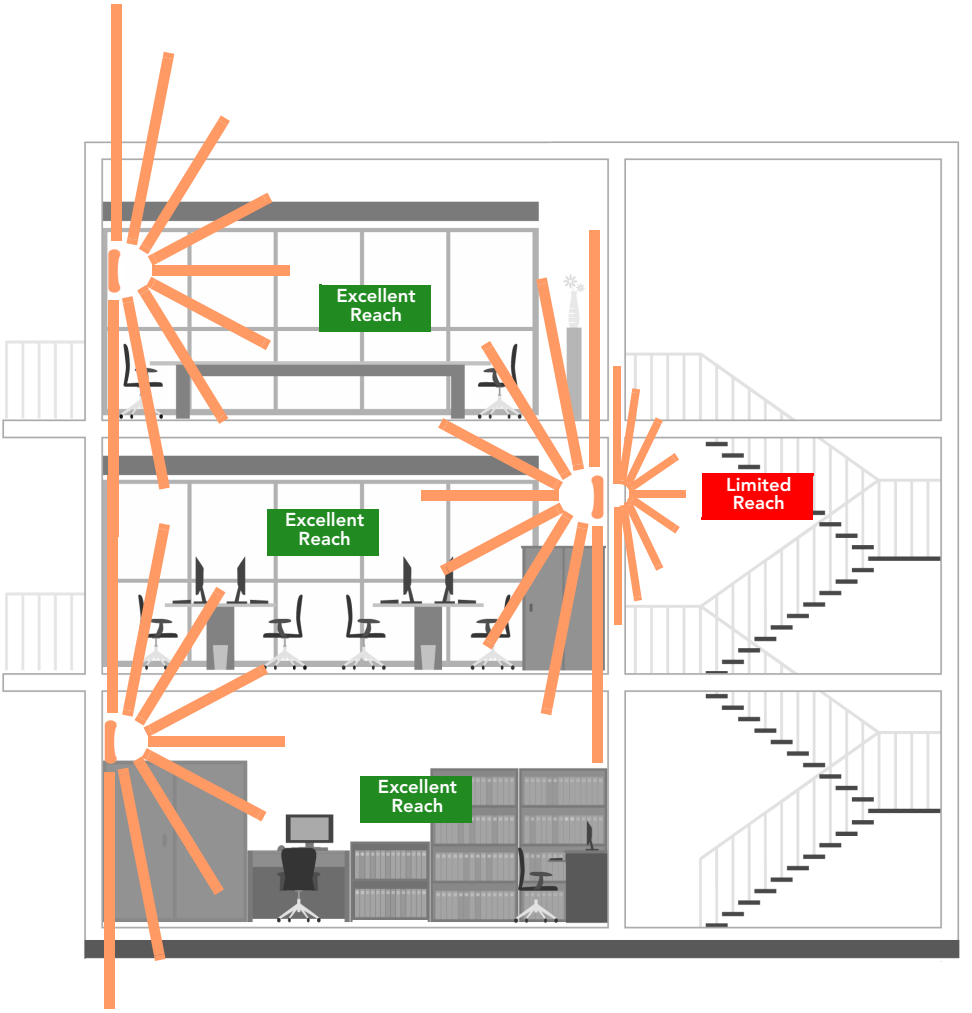
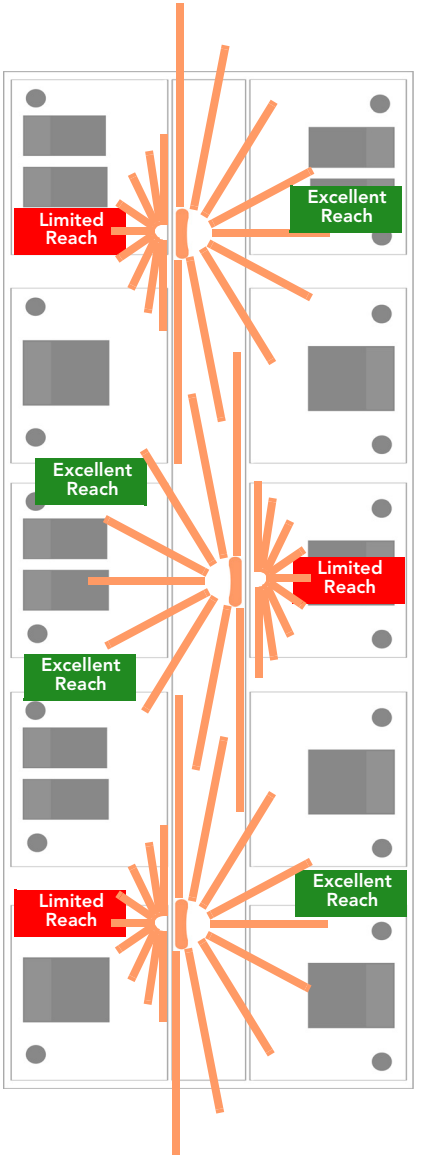


Figure 34. Recommended wall mounting in a corridor (top view)



Step 1: Preconfiguring the AP

NOTE The 100.0.0 and later APs are shipped from the factory with an AP base image, which supports standalone AP and FM-managed operation, and which does not support SCG, vSCG, SZ, ZD (or SAMs) controller operation.
After you have configured the AP with the base image as described in the following sections, the AP automatically goes out and finds any operator-defined SCG, vSCG, SZ, ZD (or SAMs) controllers. If the AP finds a controller that is configured to automatically recognize the AP, then the controller downloads the controller-specific AP firmware. If the AP does not find an SCG, vSCG, SZ, ZD (or SAMs) controller, then it retains its base image AP firmware.

NOTE If the AP has been configured with SCG or ZD controller-specific AP firmware, then it will retain that image after a factory reset. To replace a controller-specific AP image with the standalone AP firmware, please select the AP and download the specific AP image at

https://support.ruckuswireless.com/#products_grid

The procedure for completing the AP's basic configuration depends on whether you want it to be managed by SCG or ZD, or FM or to operate as a standalone AP. Refer to the section that is relevant to your deployment:

- Configuring the AP for Management by an SCG, vSCG, or SZ Controller
- Configuring the AP for Management by ZD
- Configuring the AP for Standalone Operation or for Management by FM

Configuring the AP for Management by an SCG, vSCG, or SZ Controller

When your Ruckus Wireless network is managed by an SCG, vSCG or SZ controller, you can manage APs using the controller rather than individually logging into each AP's Web interface. If SCG, vSCG or SZ controllers are installed on the network, then follow the SCG, vSCG or SZ instructions to configure the controller, and then connect the AP to your network. The AP finds the SCG, vSCG or SZ, and then downloads the SCG-, vSCG- or SZ-compatible AP image from the controller.

NOTE The AP must have some way of obtaining an IP address (IPv4 DHCP or IPv6 Auto Configuration).

Configuring the AP for Management by ZD

When your Ruckus Wireless network is managed by a ZD controller, you can manage APs using the controller rather than individually logging into each AP's Web interface. If ZoneDirector is installed on the network, then follow the instructions in the *ZoneDirector User Guide* and connect the AP to your network. The AP finds the ZD, and then downloads the ZD-compatible AP image from the controller.

NOTE The AP must have some way of obtaining an IP address (IPv4 DHCP or IPv6 Auto Configuration).

Configuring the AP for Standalone Operation or for Management by FM

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

1. Collecting the Required Materials
2. Preparing the Administrative Computer
3. Connecting the AP to the Administrative Computer
4. Logging Into the AP's Web Interface
5. Configuring the Wireless Settings
6. Disconnecting the AP from the Administrative Computer
7. Restoring the Administrative Computer's Network Settings (Optional)

1. Collecting the Required Materials

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

- An administrative computer (notebook computer) with an Ethernet port and a wireless card installed.
- A Web browser such as Chrome 39 or 40, Firefox 3.3 or later, or Internet Explorer10.0 or later installed on the administrative computer.
- One Cat5e foil screened twisted pair (FTP) solid Ethernet cable.

2. Preparing the Administrative Computer

NOTE The following procedure is applicable if the administrative computer is running Windows XP or Windows 7. 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 7 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 7, click **Start** > **Control Panel > Network and Internet > Network and Sharing Center > Change Adapter Settings**.

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

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)** (**TCP/IPv4** in Windows 7) 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 37. For a sample configuration, refer to Figure 35.

Table 37. Configure your computer's IP address settings

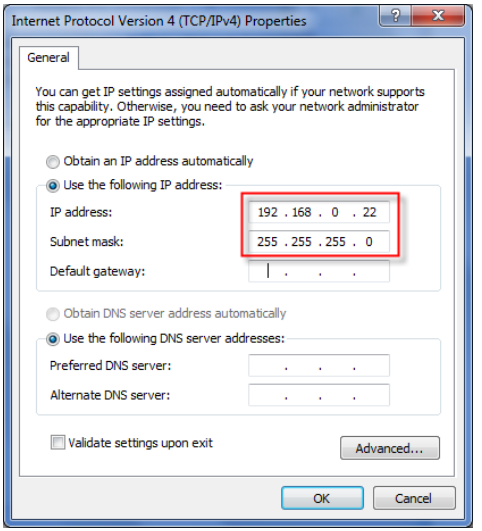
IP address	`192.168.0.22` (or any address in the 192.168.0.x network—with the exception of `192.168.0.1`, which is the default IP address assigned to the AP)
Subnet mask	`255.255.255.0`
NOTE: You can leave the *Default Gateway* and *DNS server* fields blank.	

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 d*ialog box.

Windows saves the IP address settings that you have configured.

Figure 35. Sample configuration in the Internet Protocol (TCP/IP) Properties dialog box



3. Connecting the AP to the Administrative Computer

CAUTION! Do NOT connect the AP to your live network at this point. If you connect it to a live network with an active DHCP server, the AP acquires a new IP address from DHCP and you are unable to access it via the default IP address (192.168.0.1).

1. Connect one end of an Ethernet cable to an Ethernet port on the AP, and then connect the other end to the administrative computer's Ethernet port.
2. Provide power to the AP using either an AC adapter or a PoE injector or switch.

4. Logging Into the AP'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 AP's Web interface. A security alert message appears.
4. Click **Yes** or **OK** or **Proceed anyway** (depending on the browser) to continue. The AP's login page appears.

Figure 36. The Ruckus Wireless AP login page

5 In *User name,* type `super`.

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

7 Click **Login**. The Web interface appears, displaying the *Status* > *Device* page.

8 Continue to "5. Configuring the Wireless Settings" below.

5. Configuring the Wireless Settings

To complete this step, configure the settings on the **Common** tab and at least one **Wireless #** (WLAN Number) tab. These are the essential wireless settings that enable wireless devices on the network to associate with the AP.

For your reference, the default wireless settings for the WLANs are listed in Table 38.

Table 38. Default WLAN wireless settings

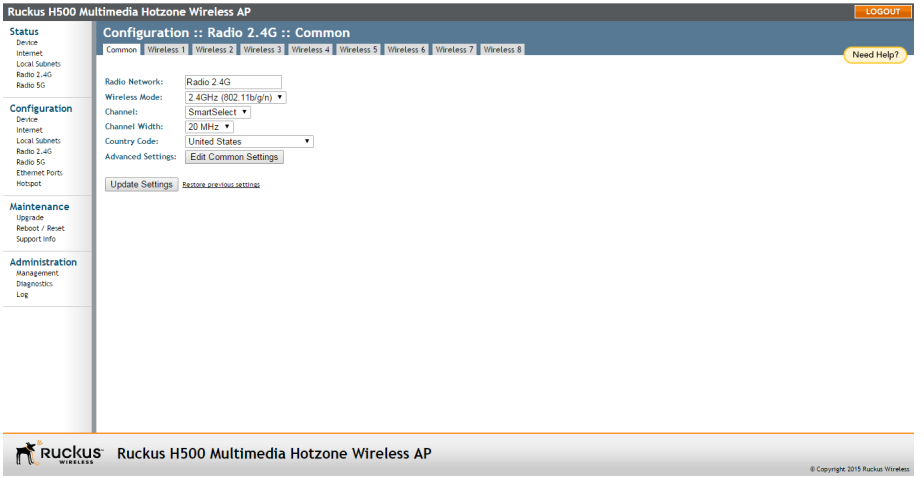
Setting	Default Value
SSID (network name)	Wireless 1 to Wireless 8 (2.4 GHz Radio) Wireless 9 to Wireless 16 (5 GHz Radio - only available on dual radio APs)
Encryption (security)	Disabled on all WLANs
Default management IP address	`192.168.0.1`

Configuring Common Wireless Settings

1 On the left menu of the Web interface, click **Configuration** > **Wireless (Radio 2.4G** or **Radio 5G** on dual-band APs). The *Configuration* > *Common* page appears.

NOTE For dual-band APs (7055, 7363, 7372, 7982, H500, R300, R500, R600, and R700), the two radios (2.4GHz and 5GHz) need to be configured separately on the Web interface. To configure the common wireless settings, click **Configuration** > **Radio 2.4G** or **Configuration** > **Radio 5G.** The rest of the configuration procedures are the same as for single-band models.

Figure 37. The Configuration > Wireless > Common tab



2 Verify that the common wireless settings are configured as listed in Table 39.

Table 39. Common wireless configuration

Setting	Recommended Value
Wireless Mode	For ZoneFlex 7321, select 2.4GHz or 5GHz mode. For other APs, the wireless mode is determined by the radio band (Wireless 2.4G or Wireless 5G).
Channel	SmartSelect.

Table 39. Common wireless configuration (Continued)

Setting	Recommended Value
Country Code	• If you purchased the AP in the United States, this value is fixed to **United States** at the factory and is not user configurable. • If you purchased the AP outside the United States, verify that the value is set to your country or region. Selecting the correct country code ensures that the AP uses only the radio channels allowed in your country or region. Note for dual-band AP users: The two radios on dual-band APs are always configured with the same country code setting. If you change the country code for Radio 1, for example, the same change is automatically applied to Radio 2.

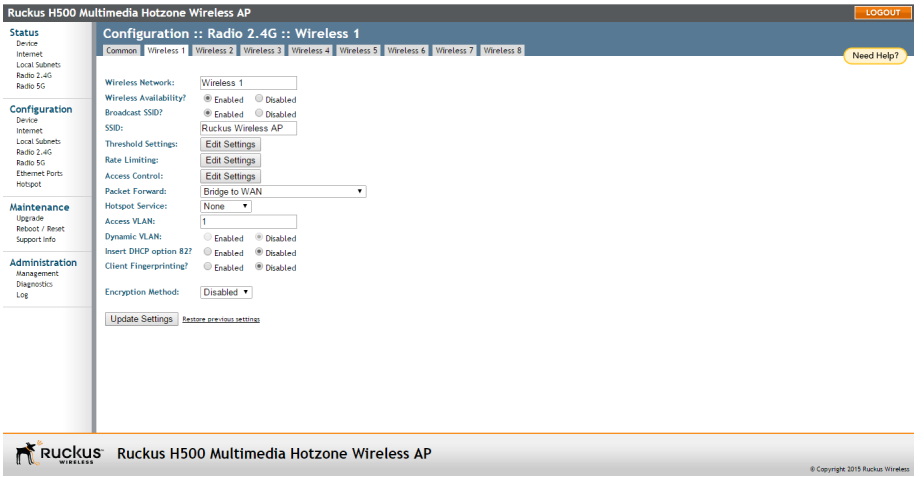
3 If you made any changes to the *Common* tab, click **Update Settings**.

4 Continue with "Configuring Wireless # (WLAN number) Settings" below.

Configuring Wireless # (WLAN number) Settings

1 Click one of the **Wireless #** (WLAN number) tabs.

Figure 38. The Configuration > Wireless > Wireless 1 tab



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 helps 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 AP installation.

5 Click **Update Settings**.

You have completed configuring the basic wireless settings of the AP.

(Optional) Setting the FlexMaster Server Address

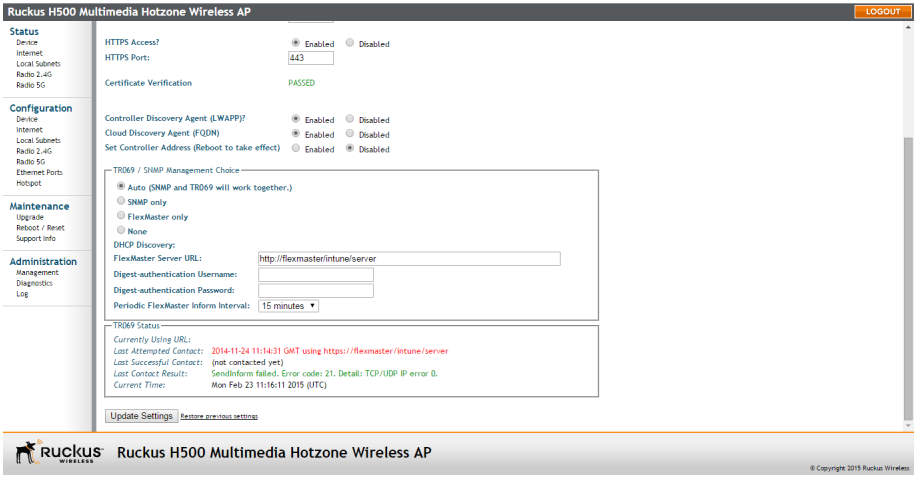
When you have a FlexMaster server installed on the network and you intend to use FlexMaster to manage the AP, you can set the FlexMaster server address at this point. Before starting this procedure, make sure you obtain the correct FlexMaster server URL.

NOTE In addition to setting the FlexMaster server URL manually on the AP, you can also use DHCP Option 43 or DNS to point the AP 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.

Figure 39. Type the FlexMaster server URL



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 AP.

NOTE Instructions on how to verify that the AP and FlexMaster can communicate with each other are provided in "Checking the TR069 Status (FlexMaster Management Only)" on page 87.

---

6. Disconnecting the AP from the Administrative Computer

1 Disconnect the AP from the power source.

2 Verify that the power LED on the AP is off.

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

7. Restoring the Administrative Computer's Network Settings (Optional)

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

- On Windows 7, click **Start > Control Panel > Network and Internet > Network and Sharing Center > Change Adapter Settings**.
- On Windows XP, click **Start** > **Control Panel** > **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)** (**TCP/IPv4** in Windows 7) from the 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 AP to your network.

Step 2: Verifying AP Operation

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

NOTE The network and power connections that you make in this step are temporary.

Continue with the following:

- Connecting the AP to the Network
- Associating a Wireless Client with the AP
- Checking the LEDs
- Checking the TR069 Status (FlexMaster Management Only)
- Disconnecting the AP from the Network

Connecting the AP to the Network

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

2 Reconnect the AP to a power source.

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

Associating a Wireless Client with the AP

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. (Other operating systems are similar).

2 Connect your admin computer to the wireless network:

- *Windows XP*: In the system tray, right-click the (Wireless Network Connection) icon, and then click **View Available Wireless Networks**.
- *Windows 7*: Left click the icon.

3 In the list of available wireless networks, click the network with the same SSID as you configured in "Configuring Wireless # (WLAN number) Settings" on page 81. 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.

Checking the LEDs

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

Single-Radio APs (7321/7352)

If the single-radio AP is operating normally and your wireless client was able to associate with it:

- The **WLAN** LED is green.
- When you do not have Ruckus Wireless ZoneDirector on the network, the **DIR** LED is off. This indicates that the AP is operating in standalone mode. If there is a ZoneDirector device on the network, then the **DIR** LED is green.

Dual-Radio APs (7055/7363/7372/7982/H500/R300/R500/R600/R700)

If the dual-radio AP is operating normally and your wireless client was able to associate with it:

- The **2.4G** or **5G** LED is green.
- When you do not have Ruckus Wireless ZoneDirector on the network, the **DIR** LED is off. This indicates that the AP is operating in standalone mode. If there is a ZoneDirector device on the network, then the **DIR** LED is green.

Checking the TR069 Status (FlexMaster Management Only)

If you configured the AP 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 AP's Web interface.

1. Log in to the AP'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 AP was able to successfully communicate with FlexMaster.

Disconnecting the AP from the Network

1. Disconnect the AP from the power source.
2. Disconnect the Ethernet cable that runs to the AP's RJ45 port from your network's router or switch.

You are now ready to deploy the AP in its permanent mounting location.

Step 3: Deploying the AP

In this step, you place the AP in a suitable location on the network and connect it to a power source and to your network environment. Continue with the following:

- 1. Choosing a Location for the AP
- 2. Connecting the AP to a Power Source and the Network

1. Choosing a Location for the AP

You can install the AP 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 AP, ensure that the location:

- Allows easy viewing of the LEDs and access to the connectors, if necessary.
- Is centrally located to the wireless clients that are connecting to the AP. 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 AP, 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 AP 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 “Determining the Optimal Mounting Location and Orientation” on page 72 for help in choosing a suitable location for the AP.

2. Connecting the AP to a Power Source and the Network

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

NOTE If your AP 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.

CAUTION! If you are using PoE, you must use a Cat5e or better Ethernet cable for the PoE connection.

---

1. Connect the power jack to the power connector on the rear panel of your Ruckus Wireless AP.
2. Connect the power adapter to a power source.
3. Obtain an Ethernet cable that is long enough to connect the AP 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 AP is green.

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

Troubleshooting the Installation

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

- Disconnect the AP from the power source, wait 5 seconds, reconnect it, and then 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 its factory defaults (and start over).

1 Insert a straightened-out paper clip into the reset button hole.

2 Press and hold the **Reset** button for at least eight (6) seconds.

You can now reconnect your computer directly to the AP (as described in "3. Connecting the AP to the Administrative Computer" on page 78), and then start over with installation, using the default network settings.

7055 Physical Installation

This section describes the physical installation instructions for mounting the 7055 to an electrical outlet box.

CAUTION! The AP and all interconnected equipment must be installed indoors within the same building, including the PoE powered network connection as described by Environment A of the 802.3af standard.

CAUTION! Ensure that you use a Cat5e or better Ethernet cable to supply PoE power and LAN connectivity running to the outlet box where the AP will be installed.

1 Prepare the electrical outlet box.

2 The 7055 can be mounted to a variety of commonly used electrical outlet box formats, including US style outlet boxes conforming to NEMA-WD6, and EU style outlet boxes conforming to BS 4662.

NOTE The 7055 comes with a bracket for a single 1-gang electrical outlet box. For adjacent outlet boxes, use the optional Ruckus Wireless ZF7055 adjacent wall bracket kit (part number 902-0111-000).

- Remove the outlet box cover from the outlet box, retaining the original box cover screws.
- Align the mounting bracket with the outlet box so that the screw holes line up (the bracket provides multiple holes for different outlet box designs), and
- Pull the Ethernet cable through the center of the mounting bracket.
- Affix the mounting bracket to the outlet box using the original outlet box cover screws. If the original outlet box screw heads extend over 2mm from the bracket, then use the enclosed low profile mounting screws instead.
- Run the required cables through the electrical outlet box allowing sufficient slack for the cables to reach the not yet installed 7055.

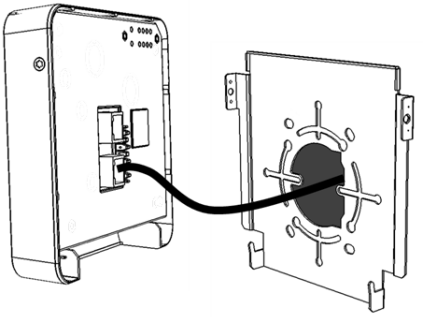
3 Connect the cables.

- Connect an Ethernet cable providing PoE power and network connectivity to the PoE In LAN / Uplink port using either a standard RJ45 connector or the 110 punch-down block (refer to Using the 110 Punch Down Block).
- If PoE power is not available, the AP can be powered using an optional DC power adapter (Ruckus part No. 902-0170-XX10, sold separately)

- If required, connect the cable providing support for pass-through devices to the Pass Through port.

NOTE The status LEDs are intentionally not visible once the 7055 is mounted. Complete any verification or troubleshooting that requires visibility of the LEDs before mounting.

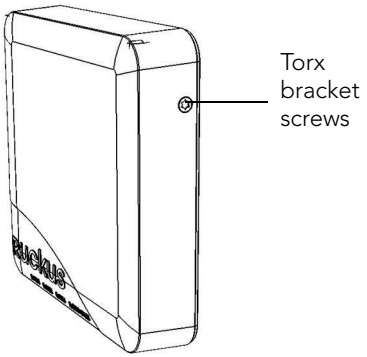
Figure 40. Attach 7055 AP cables before mounting to the bracket



4 Mount the AP to the bracket.

- Snap the AP onto the mounting bracket by hooking the two locking tabs on the bottom of the bracket into the slots on the bottom of the AP. Then push the top of the AP in toward the wall until it snaps in place.
- Use the two Torx bracket screws provided to secure the AP to the mounting bracket using a T10 Torx screwdriver.

Figure 41. Secure the 7055 AP to the bracket using Torx screws

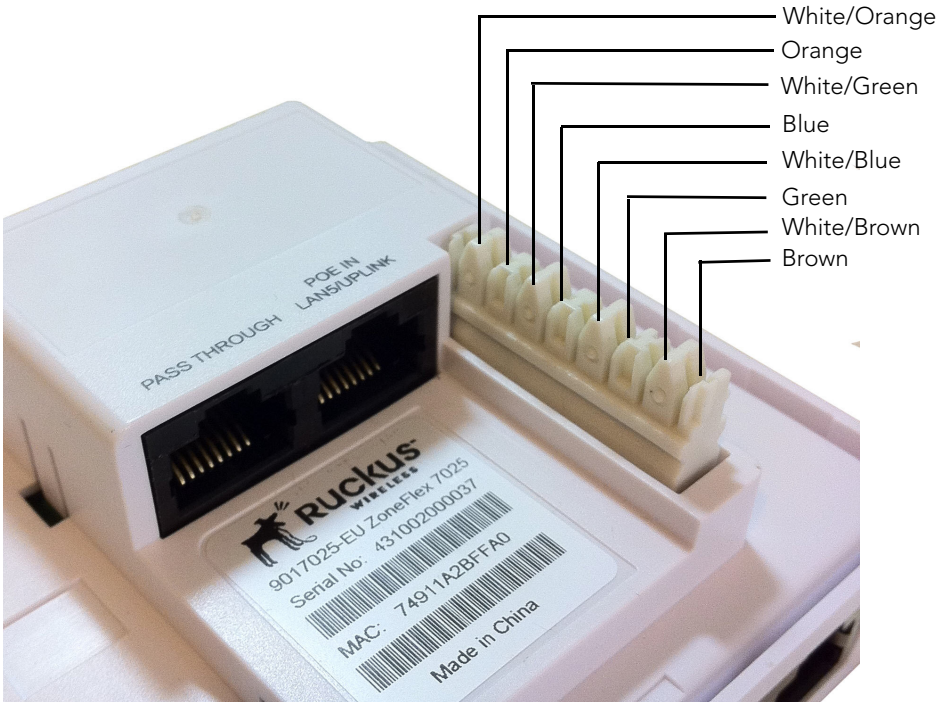


Using the 110 Punch Down Block

CAUTION! Do not connect both the Punch-down block and the Uplink port to a network. Only one connection can be used at a time.

If you prefer to use the 110 Punch-down block connector rather than the RJ-45 connector for power and network connectivity, refer to the following diagram for wiring details.

Figure 42. 7055 AP punch-down block wiring



7441 Physical Installation

The 7441 DAS AP is intended for installation in an in-building distributed antenna system (DAS) and can be co-located with other carrier or public safety services. The 7441 can be operated in standalone mode, or controlled by a ZoneDirector controller or FlexMaster server. Continue with the following:

- Distributed Antenna System Deployment
- Antenna Gain and Cable Loss
- Mounting Instructions

Distributed Antenna System Deployment

The 7441 is designed for indoor deployments where a distributed antenna system provides benefits in coverage at the expense of client density and network capacity. For example, in a multi-tenant building where tenants have their own corporate wireless networks, a DAS can be used to provide access for building management, visitors, building automation systems, etc.

There are several benefits of implementing Wi-Fi over DAS. For example, the coverage area can be shaped more efficiently, resulting in fewer APs required to adequately cover a given area.

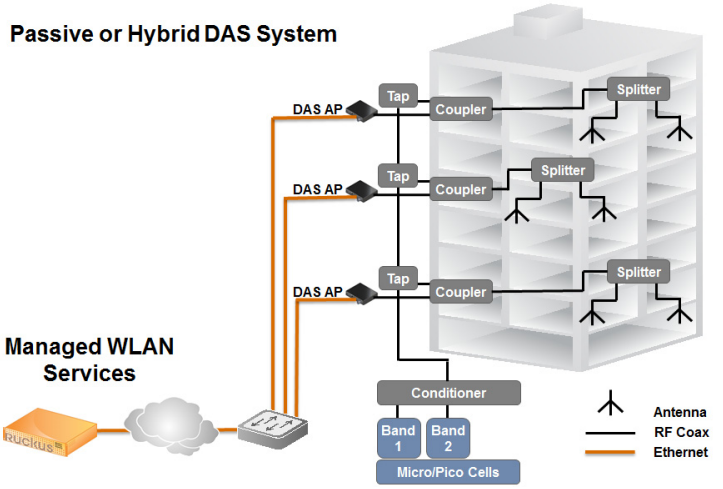
Note however, that the DAS model contains some inherent limitations, including:

- No MIMO (lower capacity)
- Limited client capacity
- Weak interference mitigation
- Poor VoWLAN quality
- No BeamFlex adaptive antenna technology
- No mesh capability
- Other 802.11 features may not work as designed over DAS

NOTE Ruckus Wireless supports all Ruckus hardware and software per the customer's support agreement, but the Wi-Fi RF coverage and performance over the DAS are the responsibility of the DAS vendor.

The 7441 DAS AP can be installed in a variety of configurations, as designed by the DAS vendor. For one example scenario in a multi-floor building, see Figure 43. DAS systems typically require RF design using sophisticated RF modeling tools in order to design effective Wi-Fi coverage on the DAS system. Detailed RF specs may be secured on the Ruckus Support Site.

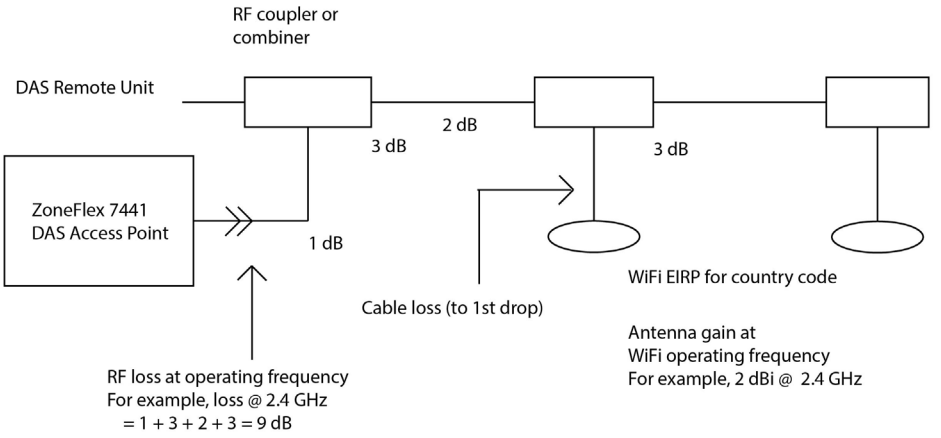
Figure 43. 7441 DAS AP installation example



Antenna Gain and Cable Loss

Figure 44 provides an example of how to calculate antenna gain and cable loss.

Figure 44. 7441 Cable Loss and Antenna Gain



Mounting Instructions

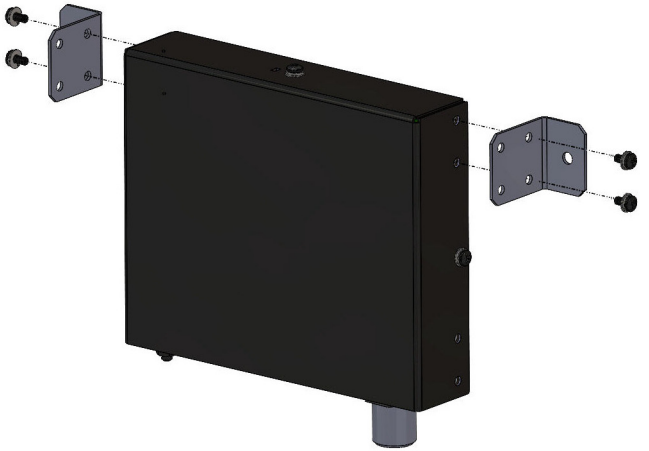
The 7441 mounting options include desktop, wall mounting (flat), wall mounting (horizontal), and DIN rail mounting. Continue with one of the following:

- Wall Mounting (Flat)
- Wall Mounting (Horizontal)
- DIN Rail Mounting
- Grounding the AP
- DIN Rail Removal

Wall Mounting (Flat)

1 Attach the wall mounting brackets to the 7441 as shown in Figure 45.

Figure 45. 7441 flat wall mount



2 Place the AP on the wall and mark the locations for screw holes.

3 Drill screw holes, place the AP onto the wall and insert screws.

Wall Mounting (Horizontal)

The 7441 can be mounted to a wall horizontally as shown in Figure 46.

Figure 46. 7442 horizontal wall mount

1 Attach the brackets to the AP as shown in Figure 46.
2 Place the AP on the wall and mark the locations for screw holes.
3 Drill screw holes, place the AP onto the wall and insert screws.

DIN Rail Mounting

Use the DIN rail clip on the rear of the AP to connect mount to a DIN rail.

1 Remove the screw on the housing back wall and use to attach the DIN rail clip to the rear of the AP as shown in Figure 47. The clip has a tab to prevent rotation which fits into the corresponding slot in the housing.

Figure 47. 7441 DIN rail clip

2 Mount the AP to the DIN rail as shown in Figure 48.

Figure 48. 7441 DIN rail mounting

Grounding the AP

1 Attach ground wire to the AP using the included terminal ring and two hex nuts as shown in Figure 49. The terminal ring can accommodate wire sizes ranging from 16 to 25 gauge.

Figure 49. Grounding the 7441 AP

DIN Rail Removal

A large, flat screwdriver inserted from the bottom of the product can be used to pry the clip off the rail.

H500 Physical Installation

Refer to the *H500 Access Point Quick Setup Guide* for physical installation instructions for initially configuring and mounting the H500 AP. You can download the *H500 Access Point Quick Setup Guide* from the Ruckus Wireless Support website at

https://support.ruckuswireless.com

Navigating the Web Interface

4

In this chapter:

Before You Begin: Preconfiguring the AP

NOTE APs are shipped from the factory with AP 100.x base image firmware, which supports standalone and FlexMaster (FM) manager operation. The AP 100.x base image does not support SmartCell Gateway (SCG), virtual SmartCell Gateway (vSCG), SmartZone (SZ), or ZoneDirector (ZD) controller operation.
After you have configured the AP with the AP 100.1.0 base image as described in the following sections, the AP can automatically search for an operator-defined SCG, vSCG, SZ, or ZD controller. When the AP finds the SCG, vSCG, SZ, or ZD controller that is configured to automatically recognize the AP, the controller downloads the required controller-compatible AP firmware, and the AP is now managed by that controller. If the AP does not find an SCG, vSCG, SZ, or ZD controller, then it retains its AP 100.1.0 base image.

NOTE In the SCG, vSCG, SZ and ZD cases, after the AP base image is overwritten with the controller-specific image and the AP no longer operates in standalone mode, the AP retains its SCG-, vSCG-, SZ- or ZD-compatible image after reboot and factory reset.
To replace a controller-compatible AP image with the AP 100.1.0 base image, please select the AP and download the required AP image at

https://support.ruckuswireless.com/#products_grid

The procedure for completing the AP's basic configuration depends on whether you want it to be managed by an SCG, vSCG, SZ, or ZD controller, or if you want it to operate as a standalone AP with or without an FM manager. Refer to the section that is relevant to your deployment:

- Configuring the AP for Management by an SCG, vSCG, or SZ Controller
- Configuring the AP for Management by ZD
- Configuring the AP for Standalone Operation or for Management by FM

Configuring the AP for Management by an SCG, vSCG, or SZ Controller

When your Ruckus Wireless network is managed by an SCG, vSCG or SZ controller, you can manage APs using the controller rather than individually logging into each AP's Web interface.

If SCG, vSCG or SZ controllers are installed on the network, then follow the SCG, vSCG or SZ instructions to configure the controller, and then connect the AP to your network. The AP finds the SCG, vSCG or SZ, and then downloads the SCG-, vSCG- or SZ-compatible AP image from the SCG, vSCG or SZ controller.

NOTE The AP must have some way of obtaining an IP address (IPv4 DHCP or IPv6 Auto Configuration).

Configuring the AP for Management by ZD

When your Ruckus Wireless network is managed by a ZD controller, you can manage APs using the controller rather than individually logging into each AP's Web interface.

If ZoneDirector is installed on the network, then follow the instructions in the *ZoneDirector User Guide* and connect the AP to your network. The AP finds the ZD, and then downloads the ZD-compatible AP image from the ZD controller.

NOTE The AP must have some way of obtaining an IP address (IPv4 DHCP or IPv6 Auto Configuration).

Configuring the AP for Standalone Operation or for Management by FM

NOTE DO NOT connect the AP to your live network at this point. If you connect it to a live network with an active DHCP server, the AP acquires a new IP address from the DHCP and you are unable to access it via the default IP address (192.168.0.1).

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

1. Collecting the Required Materials

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

- An administrative computer (notebook computer) with an Ethernet port and a wireless card installed.
- A Web browser such as Chrome 39 or later, Firefox 33 or later, or Internet Explorer 10 or later installed on the administrative computer.
- One Cat5e unshielded twisted pair (UTP) Ethernet cable.

2. Logging Into the Ruckus Wireless AP Web Interface

You can manage your AP with the integrated Web interface (which you already used to configure basic AP parameters). If your Ruckus Wireless network is managed by an SCG, vSCG, SZ, or ZD controller, then you can manage APs using the controller rather than individually logging into each AP's Web interface.

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, if VLANs are used in your network.
Refer to the AP installation or quick setup guide for instructions on how to connect an administrative computer to the AP.

1 On the PC, open a Web browser window.

2 In the address or location bar, type the IP address of the AP. Default IP address for standalone Ruckus Wireless APs:

   192.168.0.1

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

4 If a Windows security alert dialog box appears, then click **Yes** or **OK** or **Proceed anyway** (depending on the browser) to continue. The Ruckus Wireless Admin login page appears.

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

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

7 Click **Login**.

The Ruckus Wireless AP Web interface appears.

Navigating the Web Interface

You manage the AP through a Web browser-based interface that you can access from any networked computer. Table 40 lists the Web interface features that are identified in Figure 50.

Figure 50. Elements of the Ruckus Wireless AP Web Interface

Table 40. Ruckus Wireless AP Web interface elements

No.	Element	Description
1	Menu	Under each category (Status, Configuration, etc.) are options that, when clicked, open the related workspace in the area to the right.
2	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.
3	LOGOUT Button	Click this button to log out of the AP.
4	Help Button	Click this button to open a help window with information related specifically to the options currently displayed in the workspace.
5	Workspace	This large area displays features, options and indicators relevant to your menu bar choices.

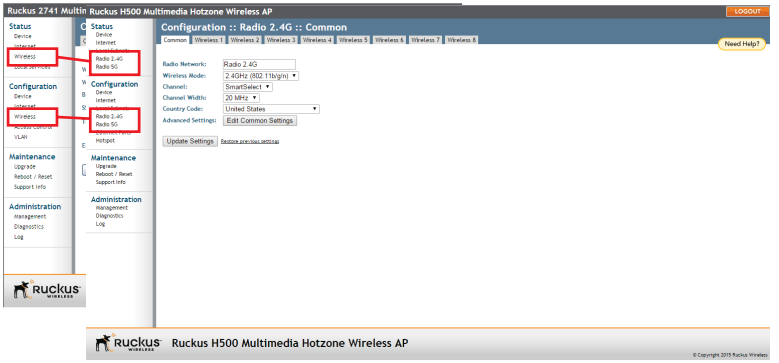
When You Are Using a Dual-Band AP

When your Ruckus Wireless AP model is dual-band, note that elements on the Web interface menu are slightly different from single band Ruckus Wireless AP models.

Dual-band APs have 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 dual-band AP Web interface has the **Radio 2.4G** and **Radio 5G** menu items, instead of a single **Wireless** menu item in single band models.

Figure 51 highlights the differences between single-radio AP and two-radio AP menus.

Figure 51. Menu items are slightly different in single band APs (left) and dual-band AP models (right)



Configuring the AP

5

NOTE If the AP has been configured with SCG, vSCG, SZ or ZD controller-compatible firmware, then the AP controller-compatible image is already installed and configured; you have completed the AP installation. When you plan to manage your Ruckus Wireless network using SCG, vSCG, SZ or ZD, refer to the associated SCG, vSCG, SZ or ZD user documents, available from the Ruckus Wireless website at

http://support.ruckuswireless.com/documents

If the AP is to be run in a standalone configuration or is to be managed by a FlexMaster manager, then continue with this section.

This chapter provides instructions for configuring Ruckus Wireless APs in a stand-alone configuration or when the AP is to be managed by a FlexMaster manager. In this chapter:

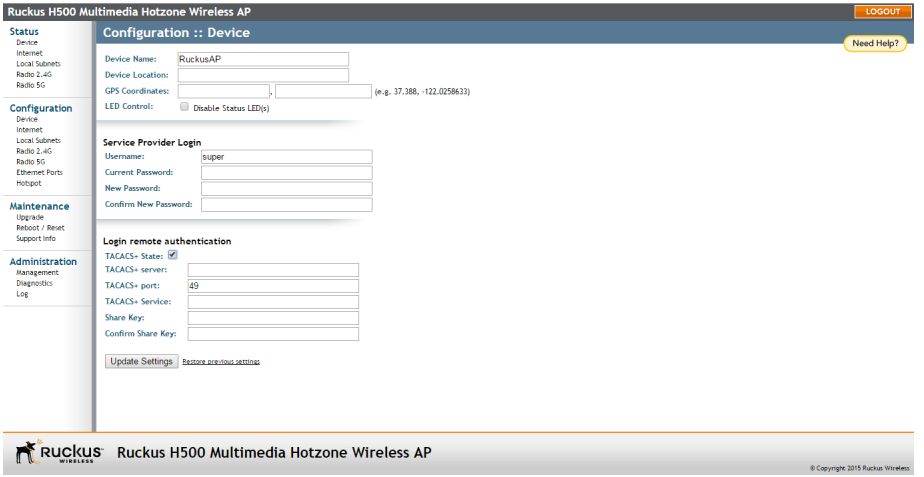
- Configuring Device Settings
- Configuring Internet Settings
- Configuring Local Subnets
- Configuring Wireless Settings
- Configuring Ethernet Ports
- Configuring Hotspot Service

Configuring Device Settings

Device settings refer to the device name, location, service provider login and other settings. (Some settings are only available on certain AP models.)

1 Select **Configuration** > **Device**. The *Configuration* > *Device* page appears.

Figure 52. The Configuration > Device page



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 Optionally, enter *Device Location* and *GPS Coordinates* to keep track of the physical location of the AP.

4 In *Temperature Update* (specific models only), enter the interval (in seconds) to record the internal temperature of the device.

5 Under *LED Control* (specific models only), check the **Disable Status LED(s)** box to turn off the status LEDs. This can be useful when the AP is installed in a public location, to avoid drawing attention to the AP.

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:* When you are changing the password, enter the existing password here.

- *New Password:* When you are changing the password, type the new password that you want to use. The default password is `sp-admin`. The password must consist of six to 32 alphanumeric characters only.
- *Confirm New Password:* Retype the new password to confirm.

7 Under *Login remote authentication,* click the **TACACS+ State** box to enable TACACS+ authentication, if required. Terminal Access Controller Access-Control System Plus (TACACS+) is an AAA protocol used to authenticate administrator login to this device. Users can be authenticated/authorized to monitor, operate or configure this device. Default is disabled. Administrators can be assigned any of the following three administration privilege levels:

- Super Admin (Perform all configuration and management tasks)
- Operator Admin (Change settings affecting single AP's only)
- Monitoring Admin (Monitoring and viewing operation status only)

8 If TACACS+ server state is enabled, then configure the TACACS+ server settings:

- *TACACS+ server:* IPv4 or IPv6 server address.
- *TACACS+ port:* 49 is the default, but it can be set to any available TCP port.
- *TACACS+ Service:* Login name.
- *Share Key:* TACACS+ Password.
- *Confirm Share Key:* TACACS+ Password.

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

Configuring Internet Settings

Internet settings define how the AP connects to your local area network and to the Internet. This section describes how to view and configure the AP's Internet settings. Topics discussed include:

VLAN Settings Overview

A Ruckus Wireless AP is in many ways like a network switch with the capability to service Wi-Fi connections. As such, like many advanced switches, Ruckus APs conform to the IEEE 802.1Q standard -- the standard that defines virtual LANs. In an 802.1Q switch, the concept of VLANs is always present. If a packet arrives without an 802.1Q header, it is assigned to the "native VLAN" or "untag VLAN."

Each of the AP's wireless interfaces can be assigned a single VLAN. When a packet enters the AP through its wireless interface, the packet is assigned to the Access VLAN configured on the *Configuration* > *Wireless* page (by default, 1).

AP Ethernet ports however, can be configured to pass all VLAN traffic (Trunk Ports) or multiple specific VLANs (General ports).

The VLAN displayed in the Web interface shows the AP's view of the VLAN environment; when a packet arrives at an AP's Ethernet port, the port's VLAN configuration helps determine if the packet is accepted or not (VLAN membership), and assigns a default VLAN (untagged VLAN) if the packet contains no 802.1Q header.

In general, if your network has VLANs deployed already, you should apply VLAN configuration to Ruckus APs so that the configuration across the network is consistent.

Configuring NTP Server and Management VLAN

NTP Server

A Network Time Protocol (NTP) Server should be configured to ensure that the AP maintains the correct time. The default Ruckus Wireless NTP Server (ntp.ruckuswireless.com) can be used if you do not have an NTP server on your network.

If you want the AP to contact a different NTP server, you can do so by going to **Configuration > Internet** and entering the host name in *NTP Server* at the top of the page.

Management VLAN

CAUTION! Changing the Management VLAN causes you to be immediately disconnected from the Web interface if the computer you are using is not on the same VLAN. Do not change the Management VLAN unless your admin PC is on the same VLAN, or you are disconnected and unable to connect again without factory resetting the AP.

If you want to place this AP's management traffic into a management VLAN, enter the VLAN ID in the *Management VLAN* field and then click **Update Settings**.

Default IP Addressing Behavior

By default, the AP is configured to automatically obtain an IPv4 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 on your network.

For IPv6, the Auto Configuration setting serves the same purpose as DHCP. The default static IPv6 address is `fc00::1`.

Obtaining and Assigning an IP Address

There are three methods of assigning IP addresses to the AP:

- DHCP / Auto Configuration
- Configuring Static IP
- Configuring PPPoE

DHCP / Auto Configuration

If you leave the AP at its default configuration, it attempts to obtain an IPv4 address from a DHCP server on the network.

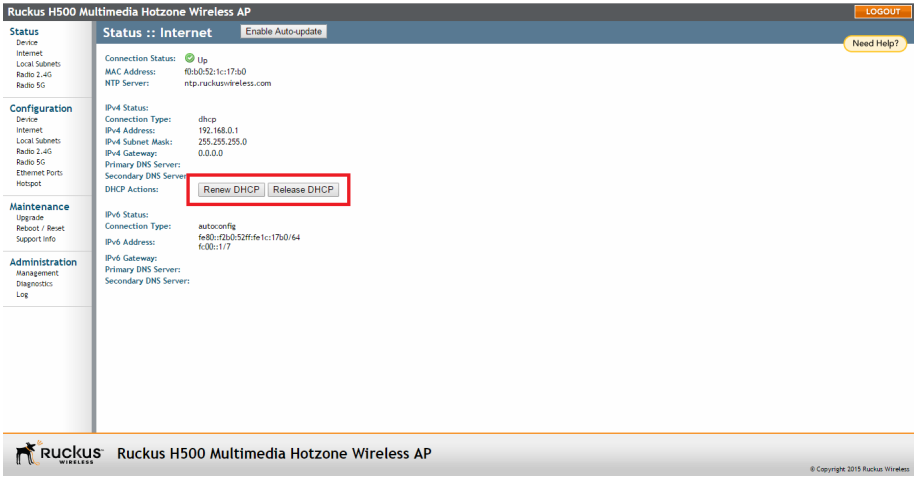
In an IPv6 network environment, the AP attempts to obtain an IPv6 address from an IPv6 Auto Configuration server.

Renewing and Releasing DHCP

This task should be performed only if you have access to the DHCP server or have some way to determine what IP address has been assigned to the AP. It serves as a troubleshooting technique when IP addresses to one or more networked devices are unusable or in conflict with others, or when the AP loses its DHCP-assigned IP address for some reason.

1 Go to **Status > Internet.**

Figure 53. Renew or Release DHCP



2 Review the current settings.

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

- To force the AP to release its DHCP-assigned IP address, click **Release DHCP**. This disconnects the user from Web interface as the system reverts to its default IP address. Log in to the device using the default IP address (192.168.0.1) and click on **Renew DHCP** to request a new lease from the DHCP server.

- Click **Renew DHCP** to request a new IP address lease from the DHCP server. **Note:** *The IP address may or may not change depending on the lease time offered to this device.*

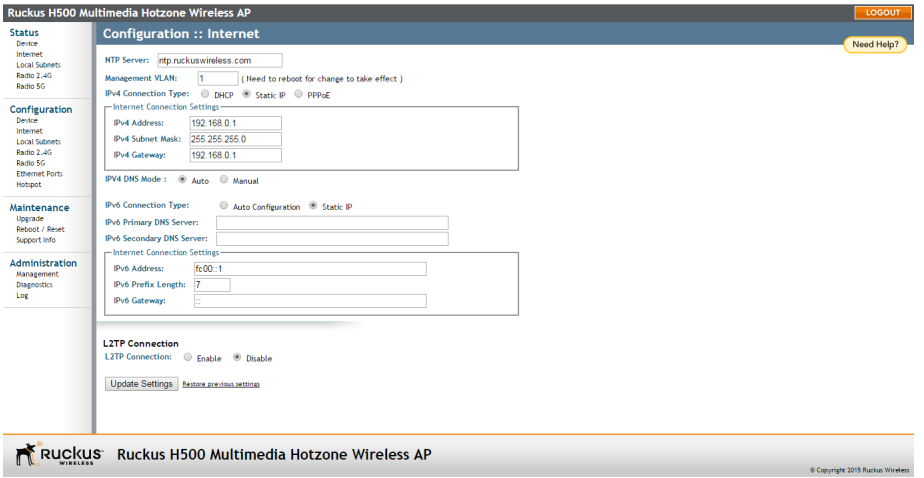
4 Click **Update Settings** to save your settings.

Configuring Static IP

Unless you are able to determine the IP address assigned to the AP by the DHCP/ Auto Configuration server, it can be useful for anyone needing administrative access to configure a static IP address.

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

Figure 54. The Configuration > Internet page



2 You can configure static addresses for IPv4, IPv6 or both. The AP maintains both sets of IP address settings when both are configured.

Static IPv4

3 In *IPv4 Connection Type,* select **Static IP**.

4 When the *Internet Connection Settings* options appear, you can make changes to the following settings:

- *IPv4 Address:* Enter the static IP address that you want to assign to the AP in IPv4 (dot-decimal) format.
- *IPv4 Subnet Mask:* Enter the subnet mask for the network.

- *IPv4 Gateway:* Enter the gateway IP address of the Internet interface.

5 To allow the DNS mode to be determined automatically, set *IPV4 DNS Mode* to **Auto.**

To set the DNS mode manually, set *IPV4 DNS Mode* to **Manual.** Then enter the following:

- *IPv4 Primary DNS Server:* The IP address of the primary Domain Name System (DNS) server.
- *IPv4 Secondary DNS Server:* The IP address of the secondary DNS server.

6 Continue with Step 7 or Step 9.

Static IPv6

7 In *IPv6 Connection Type,* select **Static IP**.

8 When the *Internet Connection Settings* options appear, you can make changes to the following settings:

- *IPv6 Primary DNS Server:* The IP address of the primary Domain Name System (DNS) server.
- *IPv6 Secondary DNS Server:* The IP address of the secondary DNS server.
- *IPv6 Address:* Enter the static IP address that you want to assign to the AP in IPv6 (colon-separated) format.
- *IPv6 Prefix Length:* Enter the prefix length for the network.
- *IPv6 Gateway:* Enter the gateway IP address of the Internet interface.

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

Configuring PPPoE

Point to Point Protocol over Ethernet (PPPoE) is a Layer 2 protocol which uses the PPP (Point to Point) protocol to connect a client system to a server system over a one to one network link. All traffic for a PPPoE connected client must go through the PPPoE server to reach the client. A PPPoE server can therefore be used to route, NAT, firewall, and perform QoS traffic shaping.

If a PPPoE server is used to distribute Internet access to subscribers, the AP can be configured with a PPPoE username and password to authenticate with the PPPoE server.

PPPoE is available only for the IPv4 connection type; PPPoE is not supported in IPv6 environments.

1 Go to **Configuration > Internet**.

2 Under *IPv4 Connection Type* select **PPPoE**.

3 Enter a *PPPoE Username.*

4 Enter a *PPPoE Password.*

5 Retype the password in *PPPoE Password Confirmation.*

6 To allow the DNS mode to be determined automatically, set *IPV4 DNS Mode* to **Auto.**

   To set the DNS mode manually, set *IPV4 DNS Mode* to **Manual.** Then enter the following:

   - *IPv4 Primary DNS Server:* The IP address of the primary Domain Name System (DNS) server.
   - *IPv4 Secondary DNS Server (optional):* The IP address of the secondary DNS server.

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

Configuring L2TP Connection Settings

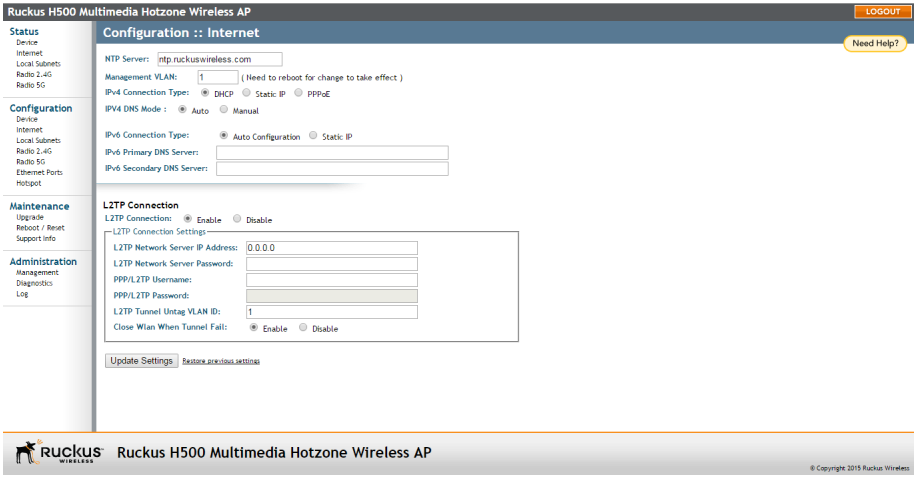
You can implement transparent bridging by using L2TP (Layer 2 Tunneling Protocol) tunneling. By tunneling traffic from an AP to a centralized data center, access controllers with policy enforcement software can apply rules and services. In a typical WLAN implementation, these rules include a captive portal to authenticate users' credentials.

In the case of L2TP, the Ruckus Wireless 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.

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

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

Figure 55. L2TP Connection



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

4 In *L2TP Network Server Password,* type the L2TP server password.

5 If your network requires PPP authentication, configure the following fields under L2TP/PPP Authentication:

- *Username:* Type your PPP user name.
- *Password:* Type the password for the account.
- *L2TP Tunnel Untag VLAN ID:* Enter the Untag VLAN ID for the L2TP tunnel.

6 In *Close WLAN When Tunnel Fail,* select **Enable** if you want to disable the WLAN when the tunnel connection is lost. This prevents clients from remaining connected to the WLAN but without Internet connectivity.

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

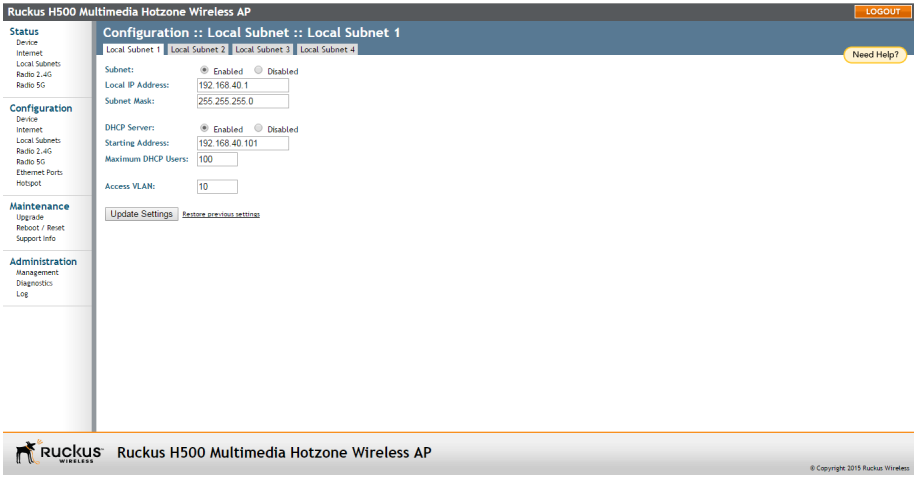
Configuring Local Subnets

Ruckus Wireless APs can be configured to provide routing/network address translation (NAT) functionality by using the Local Subnets feature. When a Local Subnet is enabled, the standalone AP serves as a gateway router with the ability to manage its own subnets, providing DHCP server and DNS cache functions for both wired and wireless clients. These clients can be assigned private IP addresses from a user-defined address pool. Traffic from the client station in private address space appears on the outside as if generated by the AP itself. In this way, the AP performs Layer 3 packet forwarding not only for Hotspot/WISPr usage, but for standard usage as well.

Up to four IP subnets can be configured per AP, each with its own address range which cannot conflict with one another.

1 Go to **Configuration > Local Subnets**. The four tabs at the top (*Local Subnet 1 - 4*) allow you to configure each of the four subnets independently.

Figure 56. Configuring local subnets and enabling router mode



2 Click **Enabled** next to *Subnet*. The local subnet configuration options appear.

3 In *Local IP Address*, enter an IP address for the gateway. The default address for Subnet 1 is `192.168.40.1`. This address can be used to access the AP's Web interface for configuration and monitoring from devices connected to this subnet.

4 In *Subnet Mask*, typically you would want to leave the setting at its default value (`255.255.255.0`) for a Class C subnet with an address pool of up to 254 addresses. An error appears if you enter an invalid IP/netmask combination.

5 In *DHCP Server*, click **Enabled** if you want to enable DHCP for this subnet. *Starting Address* and *Maximum DHCP Users* fields appear.

6 In *Starting Address*, enter an address in the same subnet as the Local IP Address (e.g., **`192.168.40.2`**).

7 In *Maximum DHCP Users*, enter the maximum number of clients that can be assigned addresses by DHCP in this subnet (valid values are 1-253 if the default subnet mask is used).

8 In *Access VLAN*, enter a VLAN ID to segment client traffic arriving from this subnet from other network traffic. (Example: if you use the default 192.168.40.1 address range, you may want to use “40” as the VLAN for this subnet.)

9 Click **Update Settings** to save your changes. The local subnet is created immediately and can now be applied to WLANs or Ethernet ports from their respective configuration pages.

Configuring Wireless Settings

This section describes how to configure the wireless settings of the AP. There are two types of wireless settings that you need to configure:

- Configuring Common Wireless Settings: Includes the wireless mode, country code, and advanced wireless settings, such as the wireless transmit power and wireless protection mode. These settings are applied to all WLANs.
- Configuring Wireless # (WLAN Number) Settings: The Wireless # tabs ("Wireless 1" through "Wireless 8" on the 2.4GHz radio and "Wireless 9" through "Wireless 16" on the 5GHz radio) provide settings for customizing each WLAN individually.

Refer to the sections below for instructions on how to configure each set of wireless settings:

- Configuring Common Wireless Settings
- Configuring Common Advanced Settings
- Configuring Wireless # (WLAN Number) Settings

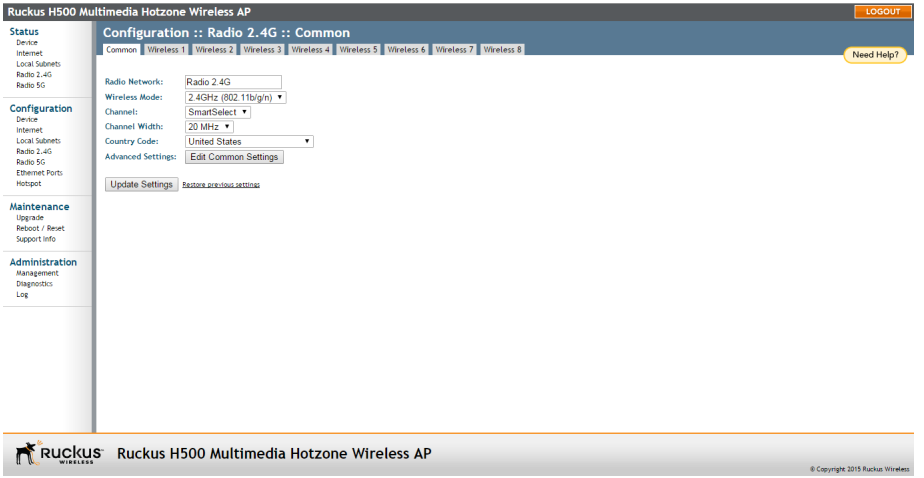
Configuring Common Wireless Settings

Common wireless settings are settings that are applied to all WLANs. On single radio APs, go to **Configuration > Wireless**. On dual radio APs, you configure these settings for the 2.4 GHz and 5 GHz radios independently by going to **Configuration > Radio 2.4G** or **Configuration > Radio 5G**.

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

NOTE If you are using a dual-band AP, then go to **Configuration** > **Radio 2.4G** or **Configuration** > **Radio 5G**.

Figure 57. The Configuration > Wireless > Common page



2 Make changes to the common wireless settings listed in Table 41.

Table 41. Common Wireless settings

Setting	Description
Radio Network	(Dual radio APs only) Allows you to change the name of the 2.4GHz and 5GHz radios (default: “Radio 2.4G” and “Radio 5G”).

Table 41. Common Wireless settings (Continued)

Wireless Mode	**On 802.11b/g APs:** 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. **On dual radio 802.11n APs:** On dual radio 802.11n APs, the wireless mode is determined by radio: For the 2.4GHz radio, the mode is set to 2.4GHz (802.11b/g/n), while for the 5GHz radio, the mode is set to 5GHz (802.11a/n). **On the 7321:** The 7321 is a single radio 802.11n AP capable of operating in either 2.4 or 5GHz mode. Use this setting to select 2.4GHz or 5GHz mode. Refer to "Band Selection on the 7321".
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.
Channel Width (11n APs only)	On 802.11n APs, the option to choose 40MHz channel width provides (theoretically) double the data capacity of a 20MHz channel. However, wider channel width means fewer channels available, and more interference with other wireless signals.
Country Code	This option (if enabled) lets you select your country or region code.
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 set the country code manually. Ruckus Wireless devices that are sold in the US are preconfigured with the correct country code and this setting is non-configurable.	
Advanced Settings	Refer to "Configuring Common Advanced Settings" on page 124.

Table 41. Common Wireless settings (Continued)

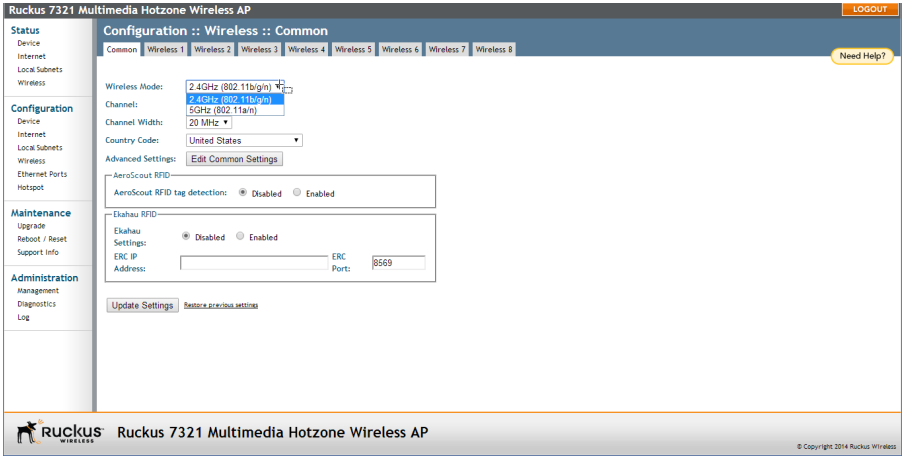
AeroScout RFID	Select **Enabled** to support AeroScout RFID tag detection. To check the status of the AeroScout communication agent (which relays location data from AeroScout Tags to the AeroScout Engine), go to the *Status* > *Wireless* page. Refer to Viewing Common Wireless Settings for more information. **NOTE:** *For other AeroScout-related configuration, refer to the AeroScout documentation that was shipped with your AeroScout Tag and AeroScout Engine.* **NOTE:** *If ZoneDirector exists on the network, then you can enable AeroScout RFID tag detection on all its managed APs at once. Refer to the ZoneDirector online help for more information.*
Ekahau RFID	Select **Enabled** to support Ekahau RFID tag detection, and then enter the IP address and port number of the Ekahau Real Time Location System Controller (ERC).
External Antenna	**NOTE:** *This option only appears if you are using the 7372-E AP.* The 7372-E AP provides an external antenna port which allows you to attach an external antenna to extend the range of your wireless network. To enable the AP to use the external antenna, select the **Enabled** option in this section. This option is disabled by default.

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

Band Selection on the 7321

The 7321 is a dual-band selectable (2.4 GHz or 5 GHz) single radio AP. This means it can operate on the 2.4 GHz band or the 5 GHz band at any time, but not both at the same time. You can select the radio band from the *Configuration* > *Wireless* page, as shown in Figure 58.

Figure 58. The 7321 can be configured to operate in either 2.4GHz or 5GHz mode



Configuring Common Advanced Settings

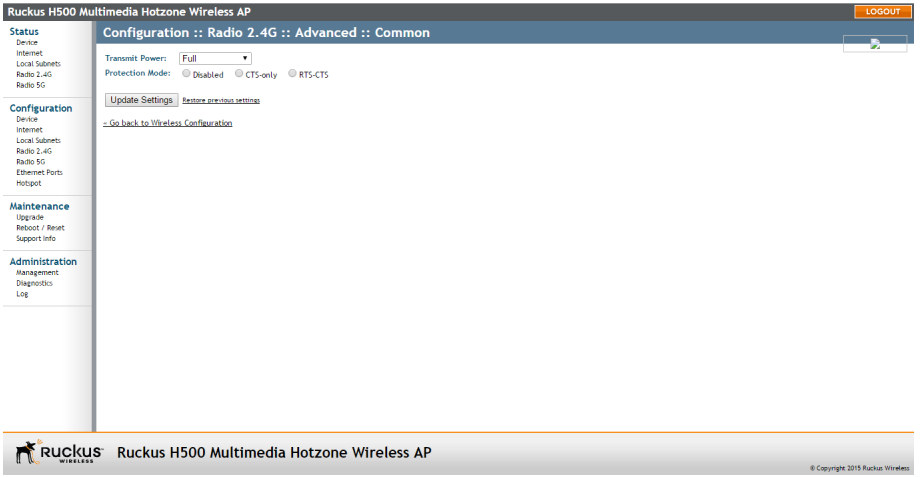
Advanced wireless settings should only be changed by an experienced administrator. Incorrect settings can severely impact wireless performance. It is recommended that the default settings are retained for best performance.

NOTE To fully benefit from the AP's capabilities, it is advisable not to change these values unless absolutely necessary.

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

NOTE If you are using a dual-band AP, go to **Configuration** > **Radio 2.4G** or **Configuration** > **Radio 5G > Edit Common Settings**.

Figure 59. The Configuration > Wireless > Advanced > Common page



2 Configure the advanced settings listed in Table 42 as required.

Table 42. Advanced common wireless settings

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	(Disabled by default.) If you activate protection, you control how 802.11 devices know when they should communicate with another device. This is important in a mixed environment of both 802.11b and 802.11g/11n clients. CAUTION! *Activating this option (and configuring the settings) boosts the interoperability of 802.11b and 802.11g/11n devices but severely decreases 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.

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

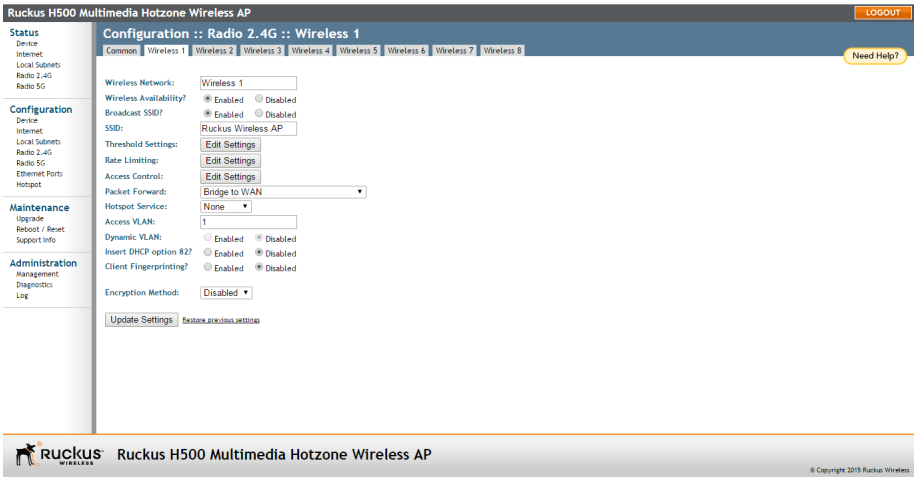
Configuring Wireless # (WLAN Number) Settings

The AP provides up to eight wireless LANs per radio that can be individually configured to provide different kinds of services for different kinds of wireless clients, traffic types or different user groups. Each WLAN can be configured with separate security settings, VLANs, access controls and rate limiting policies, among other settings.

1 Go to **Configuration** > **Wireless** (or **Configuration > Radio 2.4G/Radio 5G**). The *Configuration* > *Wireless* > *Common* page appears.

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

Figure 60. Wireless # (WLAN number) settings



3 Review the WLAN options listed in Table 43, and then make changes as required.

Table 43. WLAN options

Option	Description
Wireless Network	This wireless network name is for management purposes only, and is not visible to the user.
Wireless Availability	This option controls whether or not the wireless network is available to users (Enabled or Disabled).

Table 43. WLAN options (Continued)

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 to be told the correct SSID before they can connect to your network.
SSID	This is the publicly-broadcast “name” of your wireless network. SSIDs can contain up to 32 alphanumeric characters and are case-sensitive. The maximum SSID length can only contain between 2 and 32 characters, including characters from ! (char 33) to ~ (char 126).
Threshold Settings	This button opens a page where you can configure the Protection Mode you activated on the *Configuration* > *Wireless* > *Advanced* > *Wireless [#]* page. If Protection Mode is not active, ignore this option. For more information, refer to “Setting Threshold Options” on page 135.
Rate Limiting	This button opens a page where you can configure upload and download limits per station. For more information, refer to “Rate Limiting” on page 137.
Access Control	This button opens a page where you can configure access controls for the WLAN. For more information, refer to “Controlling Access to the Wireless Network” on page 138.
Packet Forward	**Isolated**: Selecting Isolated causes the traffic from this WLAN to terminate at the AP. **Bridge to WAN**: The default setting, Bridge to WAN forwards packets arriving on this WLAN to the WAN (uplink) port and eventually to their external destinations using Layer 2 forwarding. **Local Subnet NAT and Route to WAN**: This setting allows routing of wireless packets to their destinations using Layer 3 network address translation (NAT). **Bridge to L2TP Tunnel**: Uses Layer 2 Tunneling Protocol to deliver packets encapsulated with an L2TP header in UDP datagrams.

Table 43. WLAN options (Continued)

Hotspot Service	Select a Hotspot configuration from the list to enable Hotspot service on this WLAN, if you have configured it from the *Configuration* > *Hotspot* page. See "Configuring Hotspot Service" on page 146.
Local Subnet	This option appears if you have selected *Local Subnet NAT and Route to WAN* under *Packet Forwarding*, and allows you to choose which subnet this WLAN's traffic is part of. You must have previously configured a subnet from the *Configuration* > *Local Subnets* page before it becomes available here.
Access VLAN	Enter a VLAN ID to segment all traffic arriving from this WLAN to a specified VLAN. Default is 1.
Dynamic VLAN	This setting is available only with WPA encryption and 802.1X authentication. Dynamic VLAN allows the dynamic assignment of VLANs to clients based on RADIUS attributes. Enable this option only if your RADIUS server is configured to segment clients using dynamic VLAN.

Insert DHCP Option 82	When this option is enabled on an SSID, additional information is encapsulated in DHCP option 82 and inserted into DHCP request packets. Current format of option 82 is:
	`Circuit ID sub-option:`
	`WLAN:<IFNAME>:<VLAN>:<SSID>:<MODEL>:`
	`<HOSTNAME>:<DEVMAC>`
	This option supports the ability for a service provider to allocate IP addresses intelligently by considering information on the origin of the IP allocation request.

Client Fingerprinting	When this option is enabled, the AP attempts to identify client devices by their operating system, device type and host name, if available.
Encryption Method	By default, all data exchanges on your wireless network are not encrypted, but you can select an encryption method in this option, and use the extra workspace features that appear to fine-tune the encryption settings. Ruckus Wireless strongly recommends using WPA as the encryption method as WEP is easily circumvented. For more information, refer to either "Using WEP" on page 129 or "Using WPA" on page 131.

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.

If required, continue with the following:

- Using WEP
- Using WPA
- Customizing 802.1X Settings
- Setting Threshold Options
- Rate Limiting
- Controlling Access to the Wireless Network

Using WEP

Wired Equivalent Privacy (WEP) is a security algorithm for 802.11 wireless networks designed to provide data confidentiality comparable to that of a wired network. WEP uses a pre-shared key for encrypting data frames that is shared among all users of the wireless network. For this reason and others, WEP has been discredited as a security mechanism and should be avoided in favor of WPA if at all possible.

CAUTION! WEP encryption is easily circumvented. Therefore, Ruckus Wireless recommends using WPA whenever possible, and only use WEP if your client devices do not support WPA.

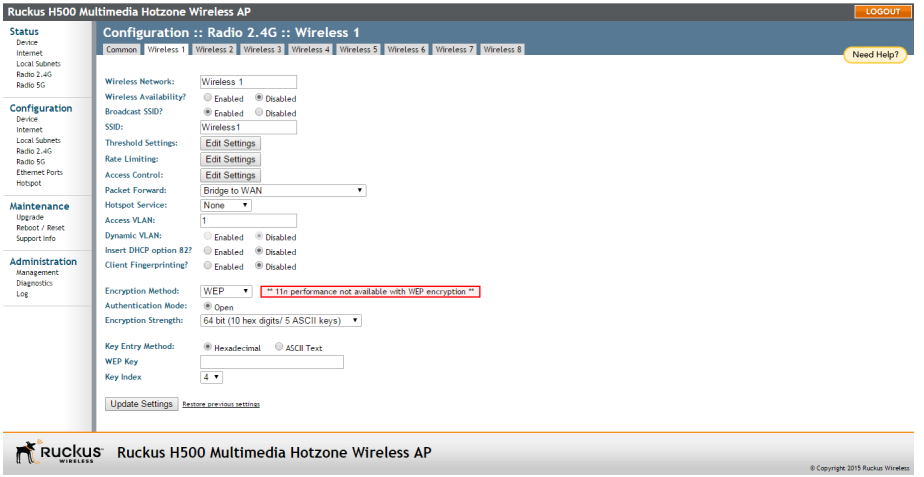
CAUTION! Using WEP encryption limits the performance of the WLAN to 802.11g rates. If you select WEP encryption for a WLAN, wireless devices that are capable of faster 802.11n transfer rates are limited to 802.11g rates. Other WLANs are unaffected.

1 Go to **Configuration** > **Wireless** or **Configuration** > **Radio 2.4G** or **Configuration** > **Radio 5G**. The *Configuration* > *Wireless* > *Common* page appears.

2 Click the **Wireless #** (WLAN number) tab that you want to configure. The *Configuration* > *Wireless* > *Wireless[#]* page appears.

3 Select **WEP** from the *Encryption Method* menu. An additional set of WEP-specific encryption options appear on this page.

Figure 61. WEP settings



4 Review the encryption settings listed in Table 44, and then make changes as required.

Table 44. WEP Options

Encryption Setting	Description
Authentication Mode	Open is the only authentication mode available with WEP encryption.
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.
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.

Using WPA

Wi-Fi Protected Access (WPA) and Wi-Fi Protected Access II (WPA2) are two security protocols developed by the Wi-Fi Alliance in response to the weaknesses of WEP.

Selecting WPA as the Encryption Method allows you to choose WPA version, WPA Authentication and WPA Algorithm. This section discusses WPA-PSK (pre-shared key). For information on WPA-Enterprise (WPA-802.1X), refer to "Customizing 802.1X Settings" on page 133.

Use of WPA-PSK (also known as WPA-Personal) allows automatic key generation based on a single passphrase. WPA-PSK provides strong security for small and medium organizations and does not require a RADIUS server, 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.

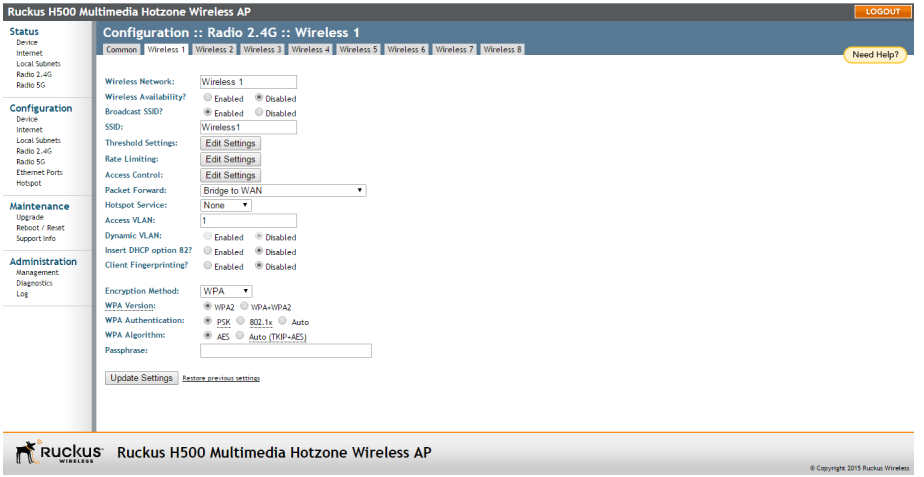
If you configure the WLAN with WPA-PSK, wireless users are not able to connect to your WLAN unless their devices support WPA-PSK and are configured with the same passphrase.

1 Go to **Configuration** > **Wireless** or **Configuration** > **Radio 2.4G** or **Configuration** > **Radio 5G**. The *Configuration* > *Wireless* > *Common* page appears.

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

3 Select **WPA** from the *Encryption Method* menu. An additional set of WPA-specific options appear on this page.

Figure 62. WPA settings



4 Review the encryption settings listed in Table 45, and then make changes as preferred.

Table 45. Encryption settings

Encryption Setting	Description
WPA Version	Your options are WPA, WPA2 or WPA Auto. • **WPA** (Wi-Fi Protected Access) is the replacement security standard adopted by the Wi-Fi Alliance in response to the security weaknesses of WEP. WPA was developed as an interim measure before ratification of the 802.11i standard, which introduced WPA2. • **WPA2** provides stronger wireless security than WPA and is the recommended option. However, older wireless clients may not be compatible with WPA2. For example, WPA2 support on Windows XP requires a Microsoft patch and is only available on Windows XP with Service pack 2 or later. • **WPA-Auto** allows both WPA and WPA2 devices to operate on the same WLAN.

Table 45. Encryption settings (Continued)

WPA Authentication	**PSK** (Pre-Shared Key) mode is suitable for home or office use. **802.1X** mode uses a RADIUS server to verify user identity. The **WPA-Auto** mode offers both options for the wireless client to choose from. For more information on how to configure 802.1X authentication, refer to "Customizing 802.1X Settings" on page 133.
WPA Algorithm	• **TKIP**: Temporal Key Integrity Protocol is an older encryption algorithm that provides stronger security than a shared WEP key, but not as strong as the newer AES algorithm. • **AES**: AES (Advanced Encryption Standard) replaces TKIP as the default (and recommended) encryption algorithm for modern wireless LANs. • **Auto**: Auto allows both encryption algorithms to be used on the same WLAN. When Auto is selected, the wireless client decides whether TKIP or AES is used. Note however that allowing TKIP reduces the performance of the WLAN (as broadcast packets are limited to slower transfer rates), and is therefore not recommended.
Passphrase	Enter a new passphrase between 8 and 32 characters, 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.

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.

In 802.1X authentication, the supplicant sends access request messages along with credentials, such as user name / password or digital certificate, to an authenticator, which forwards the credentials to the authentication server for verification. The supplicant (client device) remains in an unauthorized state until verification has been received. In unauthorized state, only 802.1X traffic is allowed; all other traffic, such as DHCP and HTTP traffic, is dropped. For its wireless interfaces, the AP can serve as the authenticator communicating between the supplicant and the authentication server.

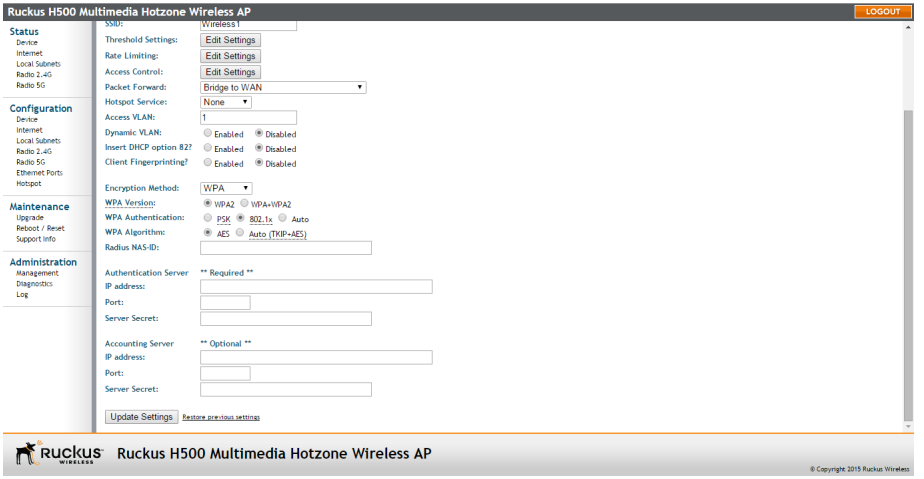
1 Go to **Configuration** > **Wireless** or **Configuration** > **Radio 2.4G** or **Configuration** > **Radio 5G**. The *Configuration* > *Wireless* > *Common* page appears.

2 Click a **Wireless #** (WLAN number) tab to configure. The *Configuration* > *Wireless* > *Wireless[#]* page appears.

3 From the *Encryption Method* menu, select **WPA**. The basic set of WPA-specific encryption options appears on the page.

4 Select **802.1X** as the *WPA Authentication* mode. Additional options appear.

Figure 63. 802.1X settings



5 Configure the following settings to customize your 802.1X authentication:

- **RADIUS NAS-ID**: Enter the Network ID assigned to your AP in the RADIUS server Client list.
- **Authentication Server**: Enter the information needed to establish a connection between the AP and the RADIUS server.

- **Accounting Server**: Optionally, 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.

NOTE Ruckus Wireless APs do not support arbitrary rate values for 802.1X clients (if client rate limiting attributes are configured on the RADIUS server). Ruckus Wireless APs support only those WLAN rate limiting values that can be set using the AP web interface. If the rate returned by the RADIUS server does not match one of these values exactly, it is approximated.

Setting Threshold Options

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

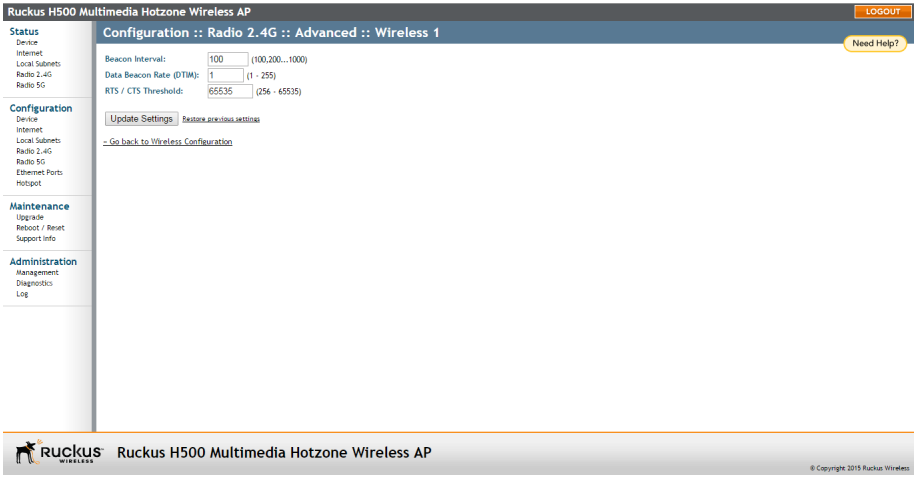
---

1 Go to **Configuration** > **Wireless** or **Configuration** > **Radio 2.4G** or **Configuration** > **Radio 5G**. The *Configuration* > *Wireless* > *Common* page appears.

2 Click the tab for the Wireless # (WLAN number) 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.

Figure 64. Threshold settings



4 Review the options listed in Table 46, and then make any needed changes.

Table 46. Threshold options

Option	Description
Beacon Interval	(The default value is 100.) The value indicates the frequency interval of the beacon in milliseconds. A beacon is a broadcast packet sent by the AP to synchronize the wireless network.
Data Beacon Rate (DTIM)	(The default value is 1.) 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 65535.) This option determines at what packet length the RTS/CTS function is triggered. A lower threshold may be necessary in an 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 the **Go back to Wireless Configuration** link.

Rate Limiting

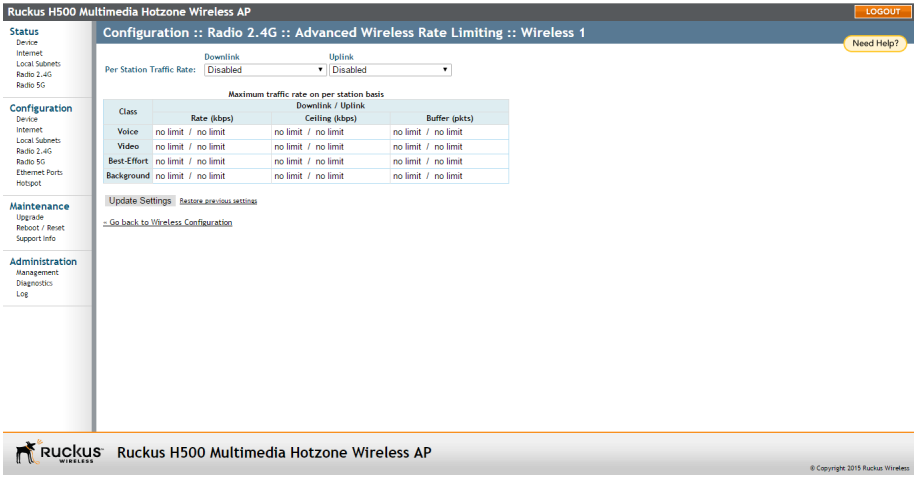
Rate Limiting allows you to cap the per client data transfer rates for a specific WLAN.

1 Go to **Configuration** > **Wireless** or **Configuration** > **Radio 2.4G** or **Configuration** > **Radio 5G**.

2 Select the WLAN number that you want to configure from the tabs at the top of the page.

3 Click the **Edit Settings** button next to *Rate Limiting*. The *Rate Limiting* page appears.

Figure 65. Limit per station traffic rates on a specific WLAN



4 Set the maximum **Downlink** and **Uplink** rate per station.

5 The table under the *Downlink* and *Uplink* selections updates to show the maximum transfer rate per station for each traffic type.

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

Controlling Access to the Wireless Network

Access Control enables you to specify the stations are allowed to join (associate with) your wireless networks. Access controls can be configured for each WLAN from its respective *Wireless #* tab.

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 passphrase. The Access Controls table is hidden if the current mode is **Disable WLAN access restrictions**.
- *Allowing Only Stations Listed in the Access Controls Table:* If you select **Allow only stations listed in the Access Controls Table**, then stations entered into the access-controls table are allowed but all others are disallowed. To add MAC addresses, refer to "Changing the Access Controls for a WLAN" on page 138.
- *Denying Only Stations 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, refer to "Changing the Access Controls for a WLAN" on page 138.

Changing the Access Controls for a WLAN

By default, the **Disable WLAN access restrictions** option is selected, which allows any wireless station to gain access to the wireless network. If you want to change this setting, follow the instructions below.

1 Go to **Configuration** > **Wireless** or **Configuration** > **Radio 2.4G** or **Configuration** > **Radio 5G**.

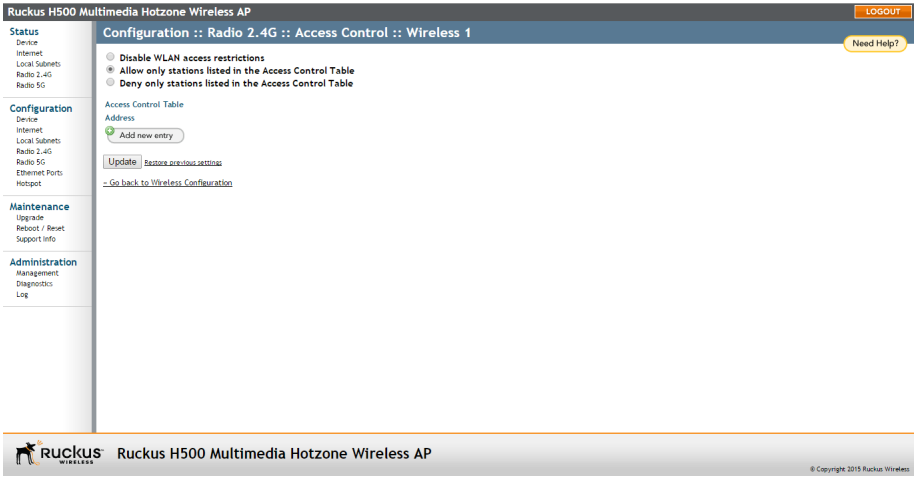
2 Click the **Wireless #** tab for which you want to configure the access control settings.

3 Click the **Edit Settings** button next to *Access Control*. The *Access Control* page appears.

4 Click **Allow only stations listed in the Access Controls Table** or **Deny only stations listed in the Access Controls Table**. (For a description of the options, refer to "Access Control Options" in the previous section.)

The *Access Control Table* appears.

Figure 66. Access control settings



5 To add a MAC address to the Access Control table, click **Add new entry**.

6 Fill out the following text boxes:

- **Address**: Six text boxes appear in which you enter the desired MAC address, in hexadecimal digit form, two characters in each box. Allowable hex-digit characters are 0-9, a-f, and A-F.

7 Click **Update** to save your changes. Assuming all parameters you entered are acceptable, that row is 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.

Removing a MAC Address

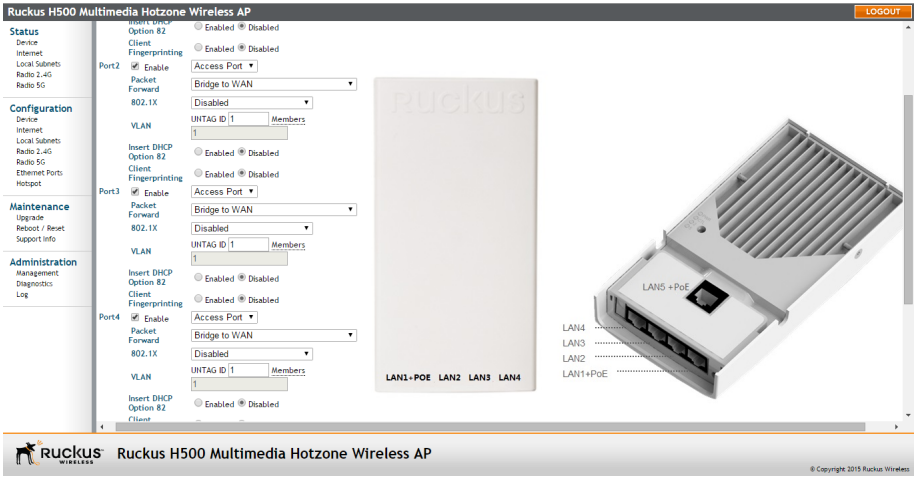
To remove a MAC address from the ACL table, click the **Cancel** button under the *Remove* column, and then click **Update**. The ACL table refreshes, and the MAC address that you deleted disappears from the table.

Configuring Ethernet Ports

The *Ethernet Ports* configuration page allows you to define how the AP's Ethernet ports behave. You can disable ports entirely, define trunking and packet forwarding behavior, configure 802.1X authentication settings, and configure VLAN settings for each port individually from this page.

1 Go to **Configuration > Ethernet Ports**.

Figure 67. The Configuration > Ethernet Ports page



2 Review Table 47 and make changes as needed for each of the ports labeled **Port1** through **Port4** (depending on AP model), which correspond to the AP's Ethernet ports.

Table 47. Configuring Ethernet ports

Setting	Description
Enable	All Ethernet ports are enabled by default. Unchecking this box next to a port disables that port entirely. If you do not want to provide wired access through the AP, uncheck (clear) the **Enable** box next to each LAN port.

Table 47. Configuring Ethernet ports (Continued)

Port Type	See "Setting Ethernet Port Type" on page 143 for more detailed information. • **Trunk port**: This port passes all VLAN traffic. • **Access Port**: This port provides network access. • **General Port**: User-defined VLAN membership.
Packet Forward	**Isolated**: Selecting Isolated causes the traffic from this port to terminate at the AP. **Bridge to WAN**: The default setting, Bridge to WAN forwards packets arriving on this port to the WAN (uplink) port and eventually to their external destinations using Layer 2 forwarding. **Local Subnet NAT and Route to WAN**: This setting allows routing of packets to their destinations using Layer 3 network address translation (NAT). **Bridge to L2TP Tunnel**: Uses Layer 2 Tunneling Protocol to deliver packets encapsulated with an L2TP header in UDP datagrams.
Local Subnet	This option appears if you have selected *Local Subnet and Route to WAN* under *Packet Forwarding*, and you have selected *Access Port* as the port type. This option allows you to select which subnet this port's traffic is part of. You must have previously configured a subnet from the *Configuration > Local Subnets* page before it becomes available here.

Table 47. Configuring Ethernet ports (Continued)

802.1X	Configure the port as an 802.1X authenticator or supplicant. The following options are available: • **Disabled**: No 802.1X controls are applied to this port. • **Authenticator (Port-based)**: Only one of the attached MAC hosts must be authorized for all hosts to be granted access to the network. • **Authenticator (MAC-based)**: Each MAC host is individually authenticated. • **Supplicant**: The port acts as a supplicant to an upstream authenticator. Configure a port as Supplicant if the port is a Trunk Port used to connect the AP to a LAN switch. See "Working with 802.1X on Wired Ethernet Ports" on page 144 for more information.
VLAN	**Untag ID**: Enter a valid VLAN ID in this field to segment traffic arriving on this port to a specific VLAN. Default is 1. Valid VLAN entries are 1-4094. **Members**: Displays the VLAN membership of the port. (Membership is configurable only for the *General* port type.) Refer to "Working with Port-Based VLANs" on page 144 for more information.

Insert DHCP Option 82	When this option is enabled for an Ethernet port, additional information is encapsulated in DHCP option 82 and inserted into DHCP request packets.
	Current format of option 82 is:
	`Circuit ID sub-option:`
	`ETH:<IFNAME>:<VLAN>:N/A:`
	`<MODEL>:<HOSTNAME>:<DEVMAC>`
	This option supports the ability for a service provider to allocate IP addresses intelligently by considering information on the origin of the IP allocation request.

Client Fingerprinting	When this option is Enabled, the AP attempts to identify client devices by their operating system, device type and host name, if available.

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

Refer to the following, as required:

- Setting Ethernet Port Type
- Working with Port-Based VLANs
- Working with 802.1X on Wired Ethernet Ports

Setting Ethernet Port Type

Ruckus Wireless AP Ethernet ports can be configured as one of the following port types:

- Trunk Port
- Access Port
- General Port

Trunk Port

Trunk Ports forward and receive tagged and untagged frames and are used for bridging switch ports together. The Trunk port is a member of all VLANs that exist on the switch, and all VLAN-tagged traffic arriving on the port is seen. If an untagged frame is received on a Trunk port, the frame is associated with the Untag VLAN (also known as “native VLAN”, by default, 1).

If a port is configured as a Trunk port, the Untag ID field can be used to define the Untag VLAN--the VLAN that the switch uses for forwarding/filtering purposes when a frame arrives without an 802.1Q header.

Access Port

Access Ports are used to provide network access. Traffic arriving on different Access Ports can be segmented into different logical networks (VLANs) using the Untag VLAN ID field. Access Ports are members of only one VLAN--the VLAN that is configured in the Untag VLAN field.

General Port

The General Port can be configured to support multiple tagged VLANs and one untagged VLAN. As Trunk Ports by definition are members of all VLANs, the General Port is the only port type for which membership is user configurable for multiple VLANs.

Working with Port-Based VLANs

The AP provides options for segmenting all incoming traffic (both wireless and wired Ethernet traffic) into specific VLANs. There are two ways to segment incoming traffic into VLANs:

- Each of the wireless interfaces (SSIDs) can be configured with a specific Access VLAN ID: (**Configuration > Wireless > Wireless [#] > Access VLAN**).
- Each of the LAN ports can be configured with an Untag VLAN ID (**Configuration > Ethernet Ports > VLAN > Untag ID**).

For Ethernet ports, the behavior of the Untag VLAN ID depends on the Port Type selected. If the port is configured as a Trunk port, it includes all VLANs (1-4094) in its membership. The VLAN Untag ID field (default = 1) can be used to redefine the "Native VLAN" for the port.

If the Ethernet port is configured as an Access Port, it can be configured with only one Untag VLAN ID and its membership includes only that one VLAN.

If the Ethernet port is configured as a General Port, it can be configured to include multiple VLANs in its membership and one Untag VLAN.

Working with 802.1X on Wired Ethernet Ports

802.1X authentication consists of the following three components:

- *Supplicant*: The supplicant sends access request messages along with credentials, such as user name / password or digital certificate, to an authenticator, which forwards the credentials to the authentication server for verification.
- *Authenticator*: The authenticator challenges the identity of the supplicant, then passes its credentials to the AAA server. If the credentials are accepted the supplicant is allowed access.
- *Authentication Server (AAA Server)*: The AAA server verifies the supplicant's credentials and permits or rejects its request for access.

For wired 802.1X, a Ruckus AP's Ethernet port can be configured as either an *Authenticator* or as a *Supplicant*, depending on which port type is selected. Table 48 and Table 49 describe the 802.1X roles available by port type.

Table 48. Authenticator support by port type

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

Table 49. Supplicant support by port type

	Trunk Port	Access Port	General Port
Supplicant	X		

The following considerations apply:

- A single port cannot be configured as both an *Authenticator* and *Supplicant* at the same time.
- Only one port per AP can be configured as a *Supplicant*.
- If the AP is connecting to a switch port with 802.1X authentication enabled, the AP's port type should be configured as a Trunk Port and its role should be configured as *Supplicant*. The switch port should be configured as a Trunk port in *Port-based Authenticator* mode.
- If there are multiple devices connected to an AP port (through a downstream switch), the port can be configured as either *Port-based* or *MAC-based Authenticator*. In Port-based mode, only one of the attached MAC hosts must be authorized for all hosts to be granted access to the network. In MAC-based mode, each MAC host is individually authenticated.
- If a Trunk Port is configured as a *Supplicant*, a user name and password must be entered to authenticate the port to the 802.1X aware LAN switch.
- If an Access Port is configured as an *Authenticator*, the administrator must define the RADIUS server that the Authenticator communicates with. All Ethernet ports of a single AP are configured with the same RADIUS server.

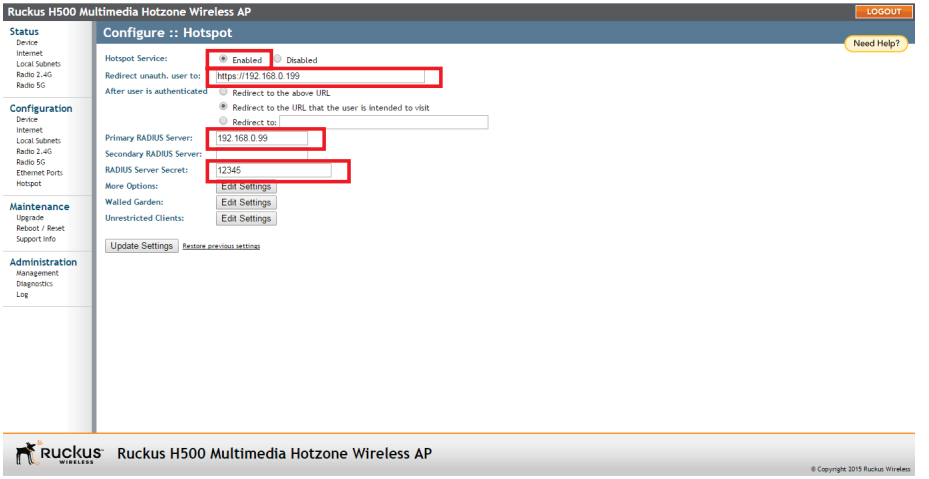
Enable MAC authentication bypass: If MAC authentication bypass is enabled, the port first attempts to authenticate the attached device by MAC address, and if that fails, it attempts to authenticate the device using 802.1X.

Configuring Hotspot Service

Hotspot service can be deployed on standalone APs through the Web interface. At a minimum, you must configure a login redirect URL and a RADIUS server to which users are authenticated. Additional options and controls are provided on subsequent pages.

1 Go to **Configuration > Hotspot**.

Figure 68. Minimum configuration settings for providing Hotspot service



2 Click **Enabled** next to *Hotspot Service*.

3 Review the settings in table Table 50, and make changes as needed.

Table 50. Hotspot configuration settings

Setting	Description
Redirect unauth. user to	Redirect unauthenticated users to the specified URL (login page).

Table 50. Hotspot configuration settings (Continued)

Setting	Description
After user is authenticated	Select where you want to redirect the user after successful authentication. • *Redirect to the above URL*: return to the login URL configured above. • *Redirect to the URL the user intended to visit*: upon successful authentication, go directly to the URL that the user originally entered (typically the browser's home page). • *Redirect to*: specify a URL to which users are redirected after authentication. This can be used to redirect users to a "Login Successful" page, or a page that offers connection time information or a Logout button.
Primary RADIUS Server	Enter the IP address of the primary RADIUS server against which users are authenticated (required).
Secondary RADIUS Server	Enter the IP address of the secondary RADIUS server, if one is available (optional).
RADIUS Server Secret	Enter the shared secret for communication with the RADIUS server (required).

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

You have completed the minimum settings for providing Hotspot service on this AP. Additional configuration options are available using the **Edit Settings** buttons on the page:

- Customizing Hotspot Optional Settings
- Creating a Hotspot Walled Garden
- Allowing Unrestricted Access by MAC Address

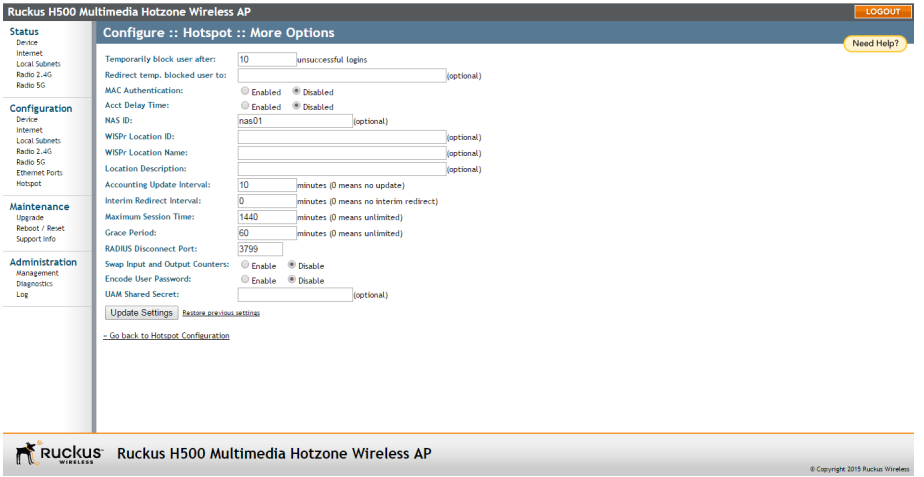
Customizing Hotspot Optional Settings

Optional Hotspot settings include a number of options for fine-tuning your Hotspot service, such as maximum session time, grace period, accounting update interval, etc.

1 Go to **Configuration > Hotspot**.

2 Click the **Edit Settings** button next to *More Options*. The *More Options* page appears.

Figure 69. Configuring optional Hotspot options



The Table 51 Hotspot options can be configured from the *Configuration > Hotspot > More Options* page:

Table 51. Optional Hotspot settings

Setting	Description
Temporarily block user after __ unsuccessful login attempts	Specify the maximum number of repeated authentication failures allowed.
Redirect temp. blocked user to	Enter a redirect URL to which blocked users are redirected.

Table 51. Optional Hotspot settings (Continued)

MAC Authentication	If enabled, the Hotspot service attempts to authenticate users based on their MAC addresses if the local Hotspot authentication has failed. If enabled, an optional MAC authentication password can be entered. If no password is specified, the system uses the client's MAC address as the password.
Acct Delay Time	This attribute indicates how many seconds the client has been trying to send this record for, and can be subtracted from the time of arrival on the server to find the approximate time of the event generating this Accounting-Request. When enabled, this attribute appears in accounting request packets with a starting value of "0", incremented each retry packet. When disabled, this attribute is not included in any accounting request packet.
NAS ID	Specify the Network Access Server identifier of this device. The NAS-ID attribute is sent in RADIUS access and accounting request messages. It can also be used as location identification when NAS-IP-Address cannot be used for this purpose.
WISPr Location ID	Specify the Hotspot location identifier. This value is provided in the RADIUS access and accounting requests. It is recommended that the value is in the form of "isocc=<ISO_Country_Code>, cc=<E.164_Country_Code>,ac=<E.164_Area_Code>,network=<SSID/ZONE>".
WISPr Location Name	Specify the hotspot location and operator's name. This value is provided in the RADIUS access and accounting requests. It is recommended that the value is in the form of "<HOTSPOT_OPERATOR_NAME>,<Location>".
Location Description	Specify the description of location. This value is provided in the HTTP redirection.
Accounting Update Interval	Specify the interval for RADIUS accounting requests.
Interim Redirect Interval	Specify the interval after which users are redirected to the login URL.
Maximum Session Time	Enter the maximum session time in minutes.

Table 51. Optional Hotspot settings (Continued)

Grace Period	Specify the maximum time that a user may disconnect from the Hotspot service and return without the need to login again.
RADIUS Disconnect Port	UDP port to listen to for accepting RADIUS disconnect requests.
Swap Input and Output Counters	Swap the value of input counters (packets, octets and giga words) and output counters in RADIUS accounting requests. This option is mainly for backward compatibility with existing ChilliSpot deployments.
Encode User Password	Encode user password with challenge string, if UAM secret is not specified; otherwise, encode user password with both challenge string and UAM secret.
UAM Shared Secret	The UAM Shared Secret is the shared secret between this AP and the HTTP server for the Redirection URL. This setting is optional.

Creating a Hotspot Walled Garden

You can use the Hotspot Walled Garden rules to designate network destinations (host address or subnet) that users can access without going through authentication. A Walled Garden is a limited environment to which an unauthenticated user is given access for the purpose of setting up an account. After the account is established, the user is allowed out of the Walled Garden. URLs are resolved to an IP address (up to four). Users will not be able to click through to other URLs that may be presented on a page if that page is hosted on a server with a different IP address. Avoid using common URLs that are translated into many IP addresses (such as www.yahoo.com), as users may be redirected to reauthenticate when they navigate through the page.

Continue with the following:

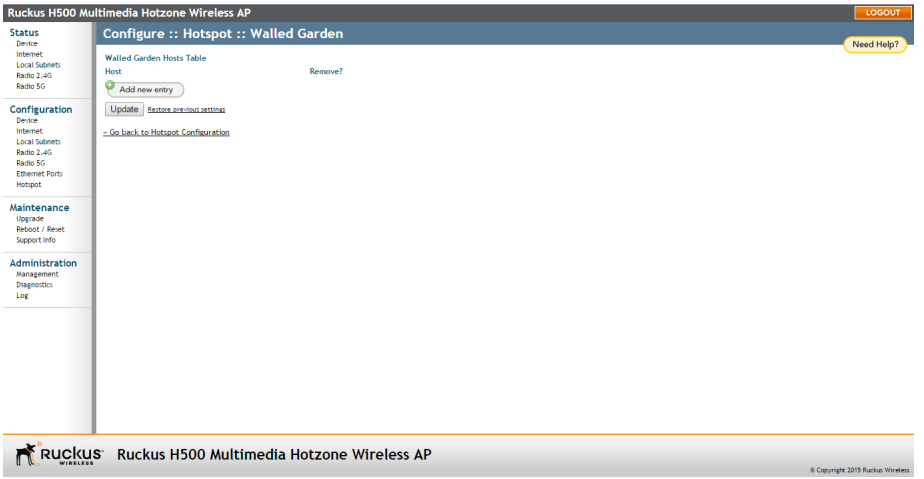
- Creating Walled Garden Rules
- Removing entries from the Walled Garden hosts table

Creating Walled Garden Rules

1 Go to **Configuration > Hotspot**.

2 Click the **Edit Settings** button next to *Walled Garden*. The *Walled Garden* page appears.

Figure 70. The Walled Garden hosts table



3 Click **Add new entry**. A field entitled *Walled Garden Host* appears.

4 In *Walled Garden Host*, enter a host name, IP address, network segment (e.g., 192.168.1.0/24) or a domain name. If a domain name is entered, it is resolved every 5 minutes.

5 Click **Update** to save your entry.

You can create up to 64 entries in the Walled Garden Hosts table.

Removing entries from the Walled Garden hosts table

1 Click the check box next to the entry you want to remove, under the **Remove?** column.

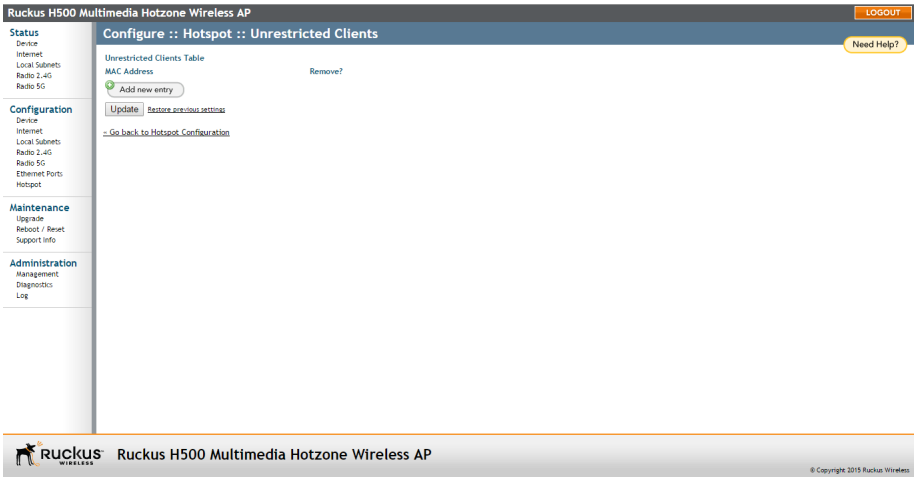
2 Click **Update**. The entry is removed from the list.

Allowing Unrestricted Access by MAC Address

1 Go to **Configuration > Hotspot**.

2 Click the **Edit Settings** button next to *Unrestricted Clients*. The *Unrestricted Clients* page appears.

Figure 71. Configuring Hotspot unrestricted clients table



3 Click **Add new entry**, and enter the MAC address of each client in the fields provided.

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

Managing the AP

6

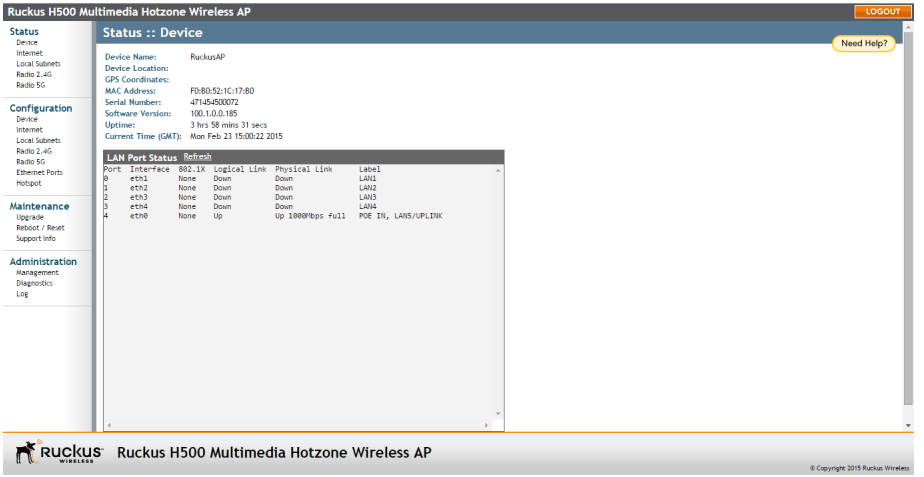
In this chapter:

This chapter provides instructions for managing standalone Ruckus Wireless APs using the AP Web interface. For information on managing your Ruckus Wireless network using SmartCell Gateway (SCG), virtual SmartCell Gateway (vSCG), SmartZone (SZ), ZoneDirector (ZD), Smart Access Management service (SAMs), or FlexMaster (FM), refer to the relevant User Guide, available from the Ruckus Wireless Support website.

Viewing Current Device Settings

The *Status* > *Device* page displays a general overview of the AP's current status, including device name, serial number, MAC address, current software version, and so on.

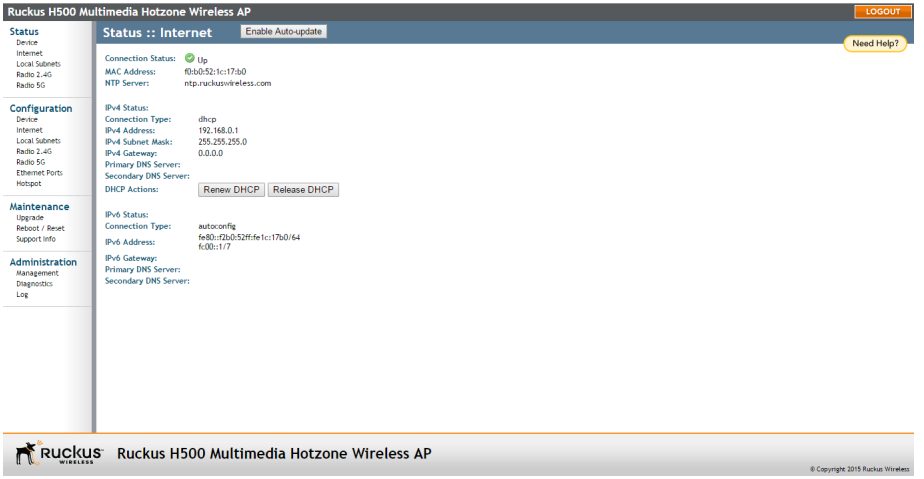
Figure 72. The Status > Device page



Viewing Current Internet Connection Settings

The *Status* > *Internet* page displays information on the AP's network settings; i.e., the settings that allow the AP to communicate with your local network and the Internet. Information includes IP address, gateway, DNS server, NTP server and connection type (method of obtaining an IP address -- DHCP or static IP).

Figure 73. The Status > Internet page

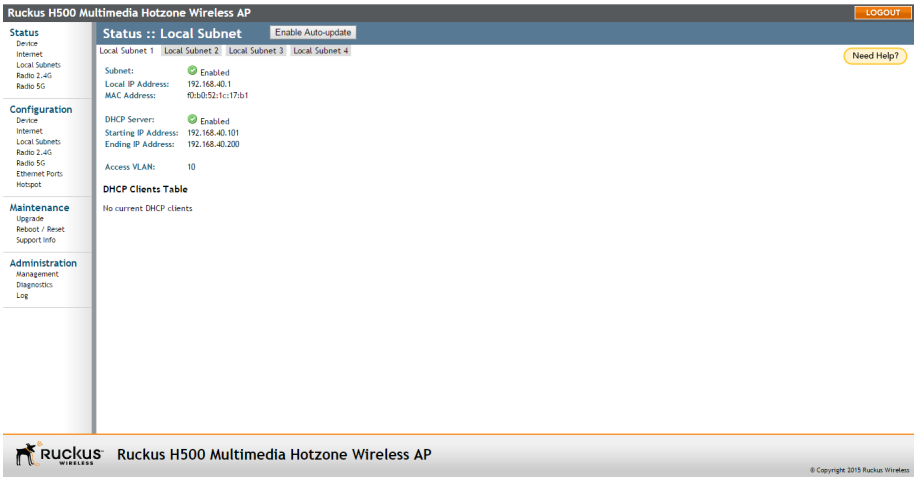


Viewing Current Local Subnet Settings

The *Status* > *Local Subnets* page can be used to view the router (local subnet) configurations and list of any clients connected to those subnets.

If you want to make changes to any of these settings, go to **Configuration > Local Subnet**. Refer to Configuring Local Subnets for more information.

Figure 74. The Status > Local Subnet page



Viewing Common Wireless Settings

If you want to view the current common wireless settings that the AP is using, go to the **Status** > **Wireless** page (on dual-band APs, go to **Status > 2.4G** or **Status > 5G**). Table 52 lists the descriptions of each common wireless setting.

Figure 75. The Status > Wireless (Radio 2.4G/5G) > Common page

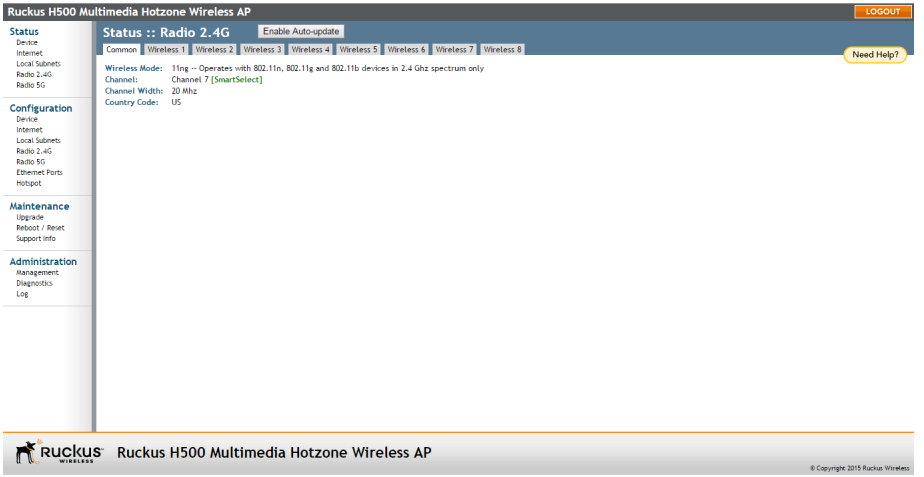


Table 52. Common Wireless settings

Setting	Description
Wireless Mode	Shows the wireless mode that the AP is currently using. Possible values include: • Auto Select: (For 802.11b/g APs only) Allows both 802.11g- and 802.11b-compliant devices to connect to the network. This is the default setting. • 2.4GHz 54 Mbps: Allows 11g devices only. • 2.4GHz 11 Mbps: Allows 11b devices only. • 11ng: Operates with 802.11n, 802.11g and 802.11b devices in the 2.4Ghz spectrum only. • 11na: Operates with 802.11n and 802.11a devices in the 5GHz spectrum only.

Table 52. Common Wireless settings (Continued)

Channel	Shows the wireless channel that the AP is currently using. If you set the wireless channel to SmartSelect, this field shows the value **Channel # [SmartSelect]**.
Channel Width	11n devices only. Displays whether the channel width is set to 20MHz or 40MHz.
Country Code	Shows the country code that the AP has been set to use. **CAUTION!** *Verify that the AP is using the correct country code to make sure it uses only the allowed radio channels in your region. Selecting the incorrect country code may result in violation of applicable laws.*
AeroScout RFID tag detection (some APs)	Shows **Enabled** if you enabled AeroScout RFID tag detection. The default setting is **Disabled**.
AeroScout Engine communication daemon (some APs)	Shows **Up** if the communication agent on the AP is able to relay location data from AeroScout Tags to the AeroScout Engine. If the communication agent is unable to relay data or AeroScout tag detection is disabled, this field shows **Down**.
Ekahau Engine communication daemon (some APs)	Shows Enabled if you have enabled Ekahau RFID tag detection. Default is disabled.
ERC IP (some APs)	Ekahau Real Time Location System RTLS Controller IP address.
ERC Port (some APs)	TCP port used by the Ekahau Real Time Location System RTLS Controller.

If you want to make changes to any of these settings, go to the **Configuration** > **Wireless** page. Refer to Configuring Common Wireless Settings for more information.

Viewing Associated Wireless Clients

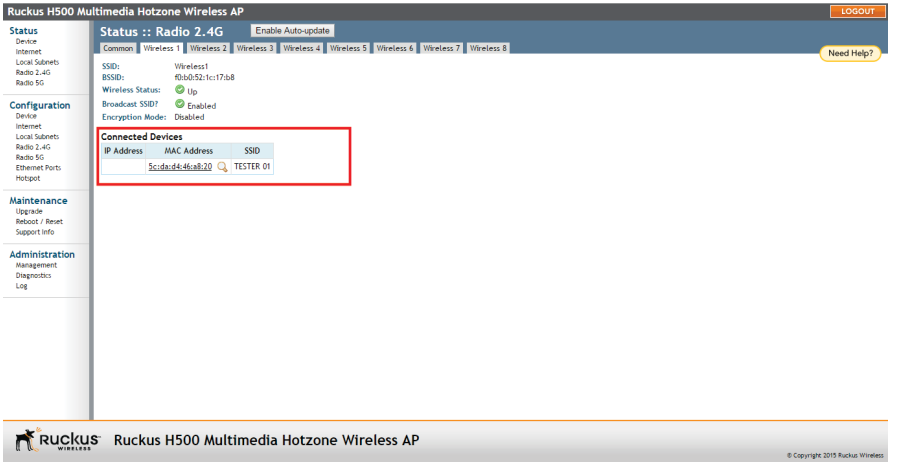
A usage-monitoring capability has been built into the AP to help you monitor wireless clients that are associated with your wireless network.

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

NOTE If you are using a dual-band AP, then 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 76. Viewing connected devices



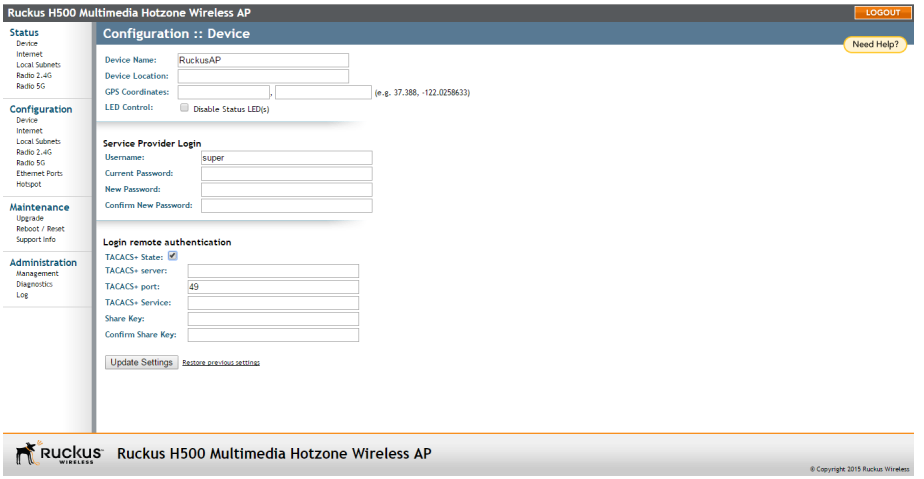
Changing the Administrative Login Settings

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.

1 Log into the Web interface.

2 Go to **Configuration** > **Device**.

Figure 77. The Configuration > Device page



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

- In *Username,* type a new user name to log in to the Web interface. The default user name is `super`.
- In *Current Password,* enter the existing password.
- In *New Password,* type a new password to replace the default password `sp-admin`. The password must consist of six to 32 alphanumeric characters only.
- In *Confirm New Password,* 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.

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.

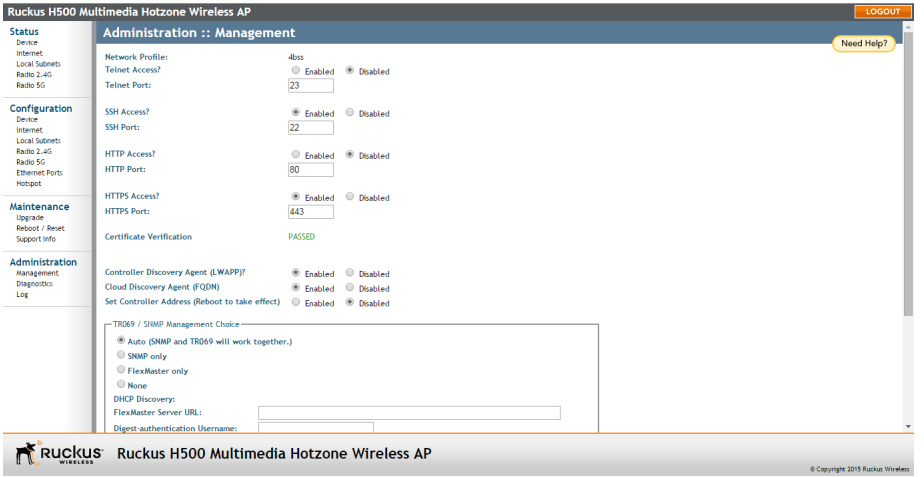
You can also view and set up the connection to a Ruckus Wireless FlexMaster server under the *TR-069/SNMP Management Choice* options. If your Ruckus Wireless device is to be managed by FlexMaster, then the FlexMaster information (server URL and contact interval) is preconfigured before you receive your Ruckus wireless 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 "Viewing FlexMaster Management Status" on page 164.

---

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

Figure 78. The Administration > Management page



2 Review the access options listed in Table 53, and then make changes as needed.

Table 53. Management Access Options

Option	Description
Telnet Access	By default, this option is disabled (inactive).

Table 53. Management Access Options (Continued)

Option	Description
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.
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.
Controller Discovery Agent (LWAPP)	• Enabled (default) -- Lightweight Access Point Protocol controller discovery on. (Refer to *Release Notes* for details.) • Disabled -- LWAPP controller discovery off.
Cloud Discovery Agent (FQDN)	• Enabled (default) -- Fully Qualified Domain Name cloud discovery on; requires enabled LWAPP controller discovery Enabled. (Refer to *Release Notes* for details.) • Disabled -- FQDN cloud discovery off.
Set Controller Address	• Enabled -- The AP uses an IP address to search for the primary and/or secondary SCG, vSCG, SZ or ZD controller. When Set Controller Address is Enabled, enter the required primary controller IP address and the optional secondary controller IP address. • Disabled (default) -- The AP does not use IP address(es) to search for SCG, vSCG, SZ or ZD controllers.
Auto-provisioning (some APs)	This setting is disabled by default, and should only be enabled if using FlexMaster server for AP management.

3 If you want to use TR-069 or SNMP to manage the AP, then configure the settings listed in Table 54.

Table 54. TR-069 and SNMP Management Options

Option	Description
Auto	Enables the Ruckus Wireless device to be managed by 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).
Periodic FlexMaster Inform Interval	Interval at which the device should attempt to contact FlexMaster. Default = 15 minutes.

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

You have completed configuring the management access options.

NOTE Remember to open any relevant firewall ports between the AP and the firmware upgrade/management server. For example, if HTTPS is used for firmware upgrades, open TCP port 443 on the firewall to allow connections through port 443. If FlexMaster server is used, open TCP ports 80 and 443 for HTTP/HTTPS communications, and TCP port 8082 for AP wake-up commands.

Continue with the following, as required:

- Viewing FlexMaster Management Status
- Pointing the AP to FlexMaster

Viewing FlexMaster Management Status

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

Figure 79. TR-069 status information

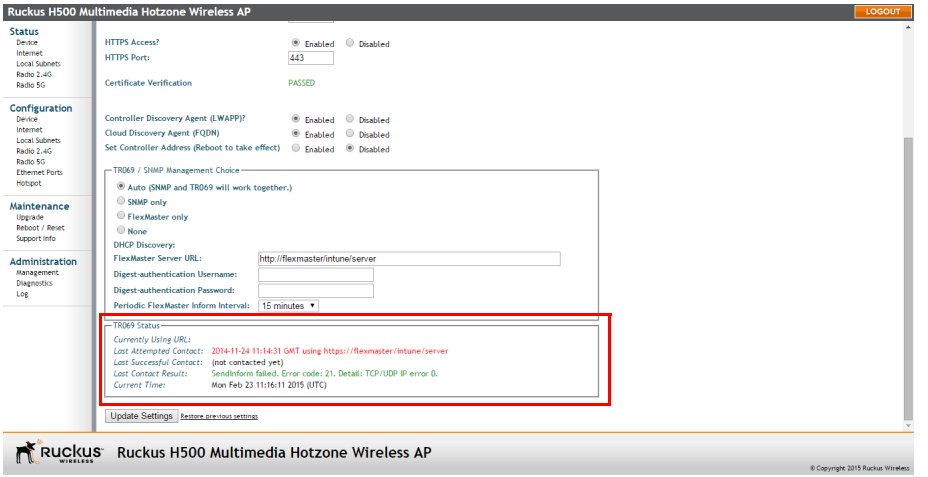


Table 55 lists the TR-069 status information that the AP provides.

Table 55. TR-069 status information

Status Information	Description
Currently Using URL	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.
Last Contact Result	Shows the result of the last attempt to contact FlexMaster (success or failure, and failure error code if applicable).

Table 55. TR-069 status information (Continued)

Status Information	Description
Current Time	Shows the current date and time as known to the AP. This timestamp is accurate if 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 Ruckus Wireless device is required to "call home" to register with your FlexMaster; FlexMaster does not initiate initial contact. To register successfully with FlexMaster, your Ruckus Wireless device must know the FlexMaster server's URL, thus entered on the device. You need TCP ports 80 and 443 between APs and FlexMaster when traversing Layer 3/firewall boundaries.

1 Go to **Administration > 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 *Periodic FlexMaster Inform Interval* drop-down list to select how frequently the device checks the FlexMaster server for any pending configuration changes available for that Ruckus Wireless 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.

Working with Event Logs and Syslog Servers

Both the *Maintenance* > *Support Info* and *Administration* > *Log* pages can be used to view the AP's current log file text. You can use the former to send the log to Ruckus Wireless support directly or save it to a local file, and use the latter to configure automatic delivery of log files to a syslog server:

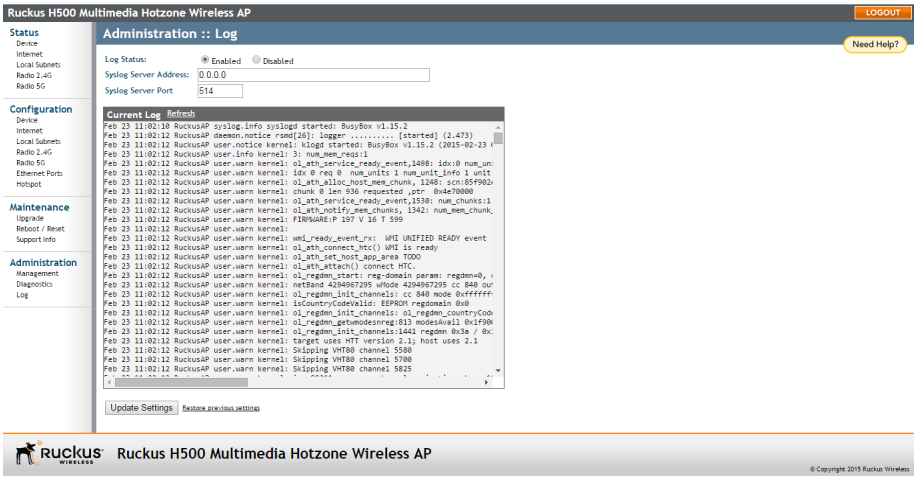
- Enabling Logging and Sending Event Logs to a Syslog Server
- Sending a Copy of the Log File to Ruckus Wireless Support
- Sending a Copy of the Log File to Ruckus Wireless Support

Enabling Logging and Sending Event Logs to a Syslog Server

If you have a syslog server on the network, you can configure the AP to send the device logs to the server. You need to enable logging (if disabled) and configure the AP to send logs to the syslog server.

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

Figure 80. The Administration > Log page



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

3 After enabling logging, configure the following options:

- *Syslog Server Address:* 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.

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:

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

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

2 Review the *Transfer Method* options.

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

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* page appears.

2 Review the *Transfer Method* options.

3 Click the **Save to Local Computer** option. Two links appear next to *Download* (**supportinfo.txt** and **tr069info.txt**).

4 Click the **supportinfo.txt** link. A new window (or tab) opens with the content of the log file displayed.

5 Choose **Save As** or **Save Page As** from your browser's **File** menu.

6 When the "Save as..." dialog box appears, find a convenient location on your local computer to save the file, and change the file extension from *.html* to *.txt*.

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

Upgrading the Firmware Image

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

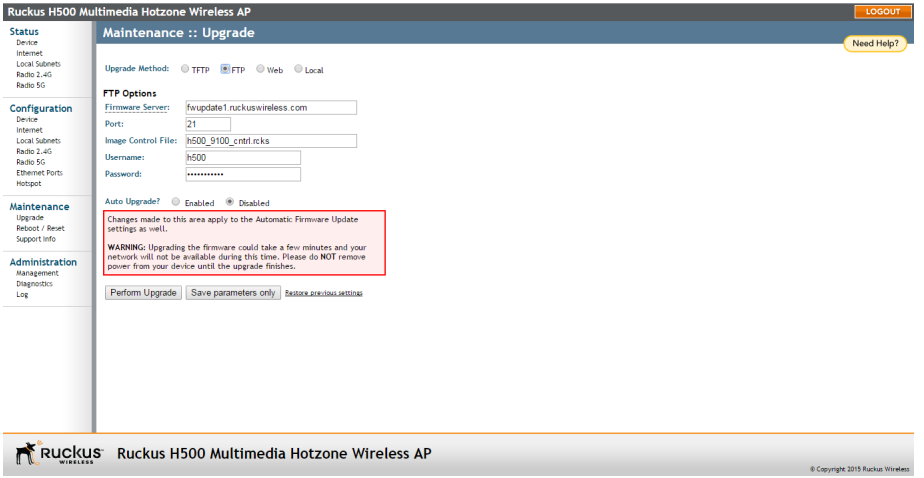
Before starting, decide which option you want to take:

- Automate a regularly scheduled update
- Run a one-time manual update right now

By default, the automatic upgrade option is disabled.

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

Figure 81. The Maintenance > Upgrade page



Continue with the following:

- Upgrading Manually via FTP or TFTP
- Upgrading Manually via the Web
- Upgrading Manually via Local File
- Scheduling Automatic Upgrades

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://`.

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.

Upgrading Manually via the Web

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

2 If instructed to choose a different URL than the default value, click the **Web Options URL** field, and then type the URL of the download Web site. Remember to start the URL with “http://”.

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

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

Upgrading Manually via Local File

If you have already saved an image file on your local computer, then you can upgrade directly using the Web interface.

1 In the *Upgrade Method* options, choose **Local**.

2 Click the **Choose File** button and locate the file on your local computer.

3 Select the file and click **OK**.

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

5 After the upgrade is completed, the AP must be rebooted.

Scheduling Automatic Upgrades

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

2 Enter the required information in the related fields.

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

---

3 Set the *Auto Upgrade* option to **Enabled**.

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

5 Choose whether to reboot immediately after upgrading, or schedule the reboot for a specific time of day using the *Schedule Reboot Time After Upgrade* list. Choosing **Any Time** (the default value) results in the AP performing a reboot immediately after the automatic upgrade is successful.

6 You have two options at this point:

- Click **Perform Upgrade**, which starts the process and the clock. The next upgrade occurs at the selected interval.
- Click **Save parameters only**. The clock starts right away, and the actual upgrade occurs at the first selected interval.

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

When the upgrade is complete, the AP automatically reboots at the time you specified in Step 5.

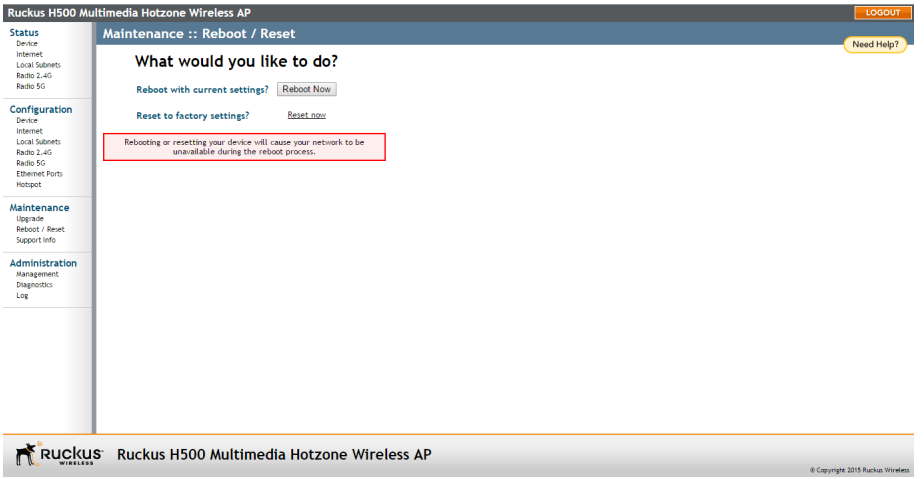
Rebooting the AP

You can use the Web 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 disrupts network communications in any currently active WLANs.

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

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

Figure 82. The Maintenance > Reboot/Reset page



After approximately one minute, 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 to verify the status of the device.

Resetting the AP to Factory Defaults

WARNING! DO NOT reset the AP to factory defaults 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 AP.

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

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

2 Click **Reset now** next to *Reset to factory settings*.

3 When the confirmation warning appears, read the message and click **OK** if you are certain that you want to restore the AP to factory defaults.

After a brief pause, you are 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: Preconfiguring the AP. 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.

1 Go to **Administration** > **Diagnostics**. The *Administration* > *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.

3 Click **Run Test**.

The results appear in the text field below each option.

Figure 83. Pinging a device

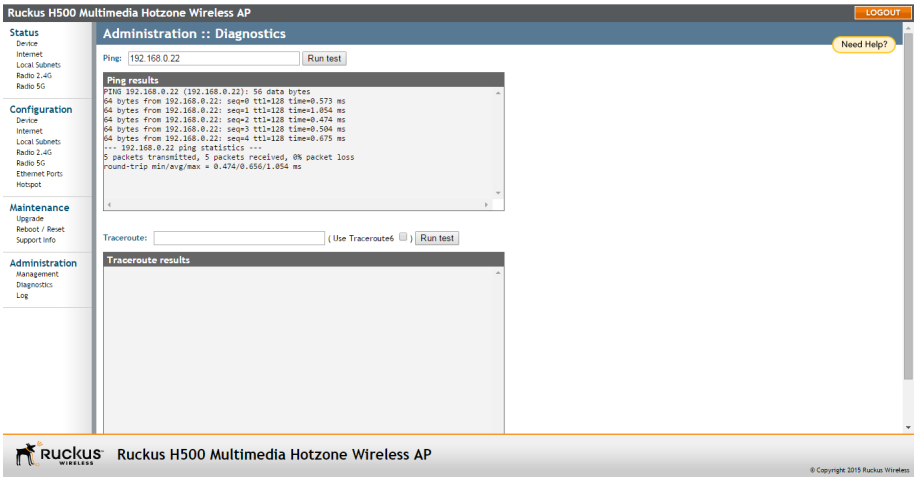
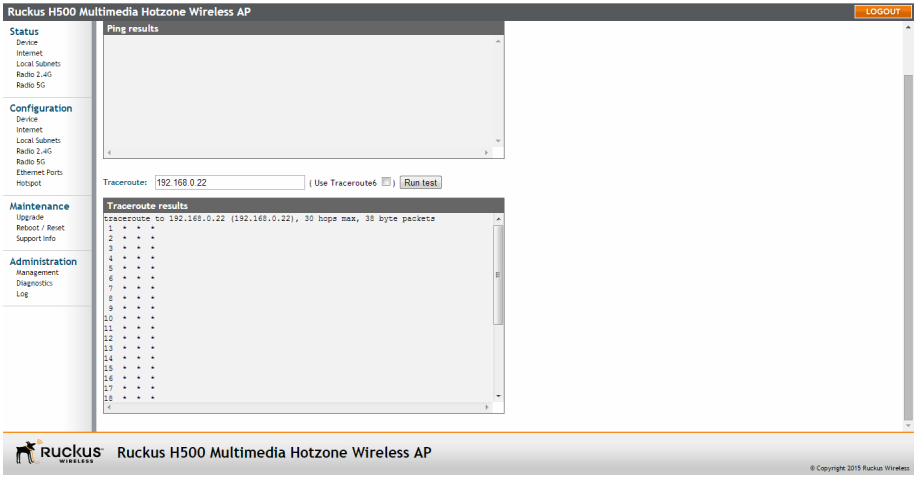


Figure 84. Running traceroute on ruckuswireless.com



Where to Find More Information

If you have questions that this User Guide does not address, visit the Ruckus Wireless Support Portal at https://support.ruckuswireless.com. The Support Portal hosts the latest versions of user documentation as well as Knowledge Base articles, software updates and a forum for community discussion of Ruckus Wireless products.

Appendix: AP Support for Bluetooth Low Energy Devices

Some Ruckus Wireless APs, such as the H500, support customer-supplied, low-power (1W or less), Bluetooth Low Energy (BLE) devices, such as BLE beacons. The BLE devices plug into a USB port on the AP, and the AP can be configured to turn power to the USB port either on or off.

The Ruckus Wireless APs with USB ports supporting BLE devices can provide power to the BLE device. The BLE devices perform whatever tasks they are designed to do without interference from or control (other than supplying USB power) by the Ruckus Wireless network equipment.

Index