Ruckus Wireless™ Outdoor Access Point

Release 100.0.0 User Guide

For the following Ruckus Wireless Outdoor Access Points:
- SmartCell 8800-S Outdoor Access Point
- ZoneFlex 7762, 7762-AC, 7762-S, 7762-S-AC and 7762-T Dual-Band 802.11n APs
- ZoneFlex 7781CM Dual-Band 802.11n AP with Integrated Cable Modem
- ZoneFlex 7782, 7782-E, 7782-N and 7782-S Dual-Band 802.11n APs
- ZoneFlex T300 and T300e Omni 802.11ac Outdoor Access Points
- ZoneFlex T301n 30-Degree Narrow Sector 802.11ac Outdoor Access Point
- ZoneFlex T301s 120-Degree Wide Sector 802.11ac Outdoor Access Point

www.ruckuswireless.com
Copyright Notice and Proprietary Information

Copyright 2015. Ruckus Wireless, Inc. All rights reserved.

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

Destination Control Statement

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

Disclaimer

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

Limitation of Liability

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

Trademarks

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

### About This Guide
- Related Documentation ........................................... 7
- Safety Warnings .................................................... 8
- Document Conventions ............................................. 9
- Documentation Feedback ........................................ 10

### 1 Introducing the Ruckus Wireless Access Point
- Overview of the Ruckus Wireless AP ............................ 12
- Installing the Access Point ....................................... 13
- Getting to Know the Access Point Features ...................... 14
  - SmartCell SC8800-S Outdoor Access Point .................... 15
  - ZoneFlex 7762 Access Point ................................ 20
  - ZoneFlex 7762-AC Access Point .............................. 23
  - ZoneFlex 7762-S Access Point ................................. 26
  - ZoneFlex 7762-S-AC Access Point ........................... 29
  - ZoneFlex 7762-T Access Point ................................. 32
  - ZoneFlex 7781CM Access Point with Cable Modem ........... 35
    - Reading the 7781CM LEDs .................................. 37
    - Powering Options .......................................... 39
    - Cable Modem Heater ....................................... 40
  - 7781CM Operation ............................................. 40
  - ZoneFlex 7782 Access Point .................................. 41
  - ZoneFlex 7782-E Access Point ............................... 44
  - ZoneFlex 7782-N Access Point ............................... 47
  - ZoneFlex 7782-S Access Point ............................... 50
  - ZoneFlex T300 Outdoor Access Point ......................... 53
  - ZoneFlex T300e Outdoor Access Point ......................... 56
  - ZoneFlex T301n Outdoor Access Point ......................... 60
  - ZoneFlex T301s Outdoor Access Point ......................... 63

### 2 Navigating the Web Interface
- Before You Begin: Preconfiguring the AP ...................... 67
3 Configuring the Access Point

Configuring Device Settings ................................................. 74
Configuring Internet Settings ............................................. 76
VLAN Settings Overview ..................................................... 77
Configuring an NTP Server ............................................... 77
Configuring the Management VLAN ................................... 77
Default IP Addressing Behavior ......................................... 78
Obtaining and Assigning an IP Address ................................ 78
DHCP/Auto Configuration .................................................. 78
Configuring a Static IP ....................................................... 80
PPPoE ............................................................................. 81
Configuring L2TP Connection Settings ................................ 82
Configuring Local Subnets ................................................... 84
Configuring Wireless Settings ............................................. 86
Configuring Common Wireless Settings ............................... 86
Reviewing Common Advanced Settings ................................. 90
Configuring Wireless # (WLAN Number) Settings ............... 91
Using WEP ................................................................. 94
Using WPA ................................................................. 96
Customizing 802.1X Settings ........................................... 99
Setting Threshold Options .............................................. 101
Rate Limiting ................................................................. 102
Controlling Access to the Wireless Network ....................... 103
Configuring Ethernet Ports ............................................... 106
Setting Ethernet Port Type ............................................... 109
Trunk Port .................................................................. 109
Access Port .................................................................. 109
General Port .................................................................. 110
Working with Port-Based VLANs .................................... 110
Working with 802.1X on Wired Ethernet Ports .................. 110
Configuring Hotspot Service ............................................ 112
Customizing Hotspot Optional Settings .................................................. 113
Creating a Hotspot Walled Garden ..................................................... 116
Removing Entries from the Walled Garden Hosts Table ...................... 117
Allowing Unrestricted Hotspot Access by MAC Address ..................... 118

4 Managing the Access Point

Viewing Current Device Settings ....................................................... 120
Viewing Current Internet Connection Settings ..................................... 121
Viewing Current Local Subnet Settings .............................................. 122
Viewing Current Wireless Settings .................................................... 123
Viewing Associated Wireless Clients ................................................. 125
Changing the Administrative Login Settings ....................................... 126
Enabling Other Management Access Options .................................... 127
Viewing FlexMaster Management Status .......................................... 131
Pointing the AP to FlexMaster ......................................................... 132
Working with Event Logs and Syslog Servers ..................................... 133
    Enabling Logging and Sending Event Logs to a Syslog Server ............ 133
    Sending a Copy of the Log File to Ruckus Wireless Support ............. 134
    Saving a Copy of the Log File to Your Computer ......................... 134
    Saving a Copy of a Support File to Your Computer ....................... 135
Upgrading the Firmware ................................................................. 136
    Upgrading Manually via FTP or TFTP ........................................... 136
    Upgrading Manually via the Web ................................................ 137
    Upgrading Manually via Local File ............................................. 137
    Scheduling Automatic Upgrades ................................................ 137
Rebooting the AP and Cable Modem ................................................ 139
Resetting the AP to Factory Defaults .............................................. 140
Running Diagnostics .................................................................... 141
Where to Find More Information ..................................................... 143

Appendix: Zone 2 APs

Index
About This Guide

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 configure and manage Release 100.0.0 Ruckus Wireless Outdoor Access Points (APs). This guide is written for those responsible for managing network equipment. Consequently, it assumes that the reader has basic working knowledge of local area networking, wireless networking, and wireless devices.

NOTE   This guide assumes that the Ruckus Wireless Outdoor APs have already been installed as described in the corresponding Mounting Guide, Installation Guide or Getting Started Guide. Refer to the Mounting Guide, Installation Guide or Getting Started Guide that shipped with your product for model-specific instructions.

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
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), virtual SmartCell Gateway (vSCG), SmartZone (SZ), and ZoneDirector (ZD) controllers, on Smart Access Management service (SAMs), and on FlexMaster (FM) managers, refer to their respective Release Notes and associated user documents.
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!** 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!** Make sure that you form a 80mm - 130mm (3”-5”) drip loop in any cable that is attached to the AP or the building. This will prevent water from running along the cable and entering the AP or the building where the cable terminates.

**CAUTION!** Be sure that grounding is available and that it meets local and national electrical codes. For additional lightning protection, use lightning rods and lightning arrestors.

**NOTE** Allowable external antenna types and antenna gains may be limited by local regulatory requirements.
Table 1 and Table 2 list the text and notice conventions that are used throughout this guide.

**Table 1. Text conventions**

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

**Table 2. Notice conventions**

<table>
<thead>
<tr>
<th>Notice Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>NOTE</td>
<td>Information that describes important features or instructions</td>
</tr>
<tr>
<td>CAUTION!</td>
<td>Information that alerts you to potential loss of data or potential damage to an application, system, or device</td>
</tr>
<tr>
<td>WARNING!</td>
<td>Information that alerts you to potential personal injury</td>
</tr>
</tbody>
</table>
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:

- ZoneFlex Outdoor Access Point 100.0.0 User Guide
- Part number: 800-70725-001 Revision B
- 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.
Introducing the Ruckus Wireless Access Point

In this chapter:

• Overview of the Ruckus Wireless AP
• Installing the Access Point
• Getting to Know the Access Point Features
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 outdoor 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.

NOTE For more information on the Ruckus Wireless system, including SmartCell Gateway (SCG), virtual SmartCell Gateway (vSCG), SmartZone (SZ), and ZoneDirector (ZD) controllers, on the Smart Access Management service (SAMs), and on the FlexMaster (FM) managers, as well as BeamFlex, and other Ruckus Wireless technologies, visit www.ruckuswireless.com
Installing the Access Point

This User Guide assumes that the Ruckus Wireless outdoor APs have already been installed and have already been initially configured as described in the corresponding Mounting Guide, Installation Guide or Getting Started Guide.

NOTE  DO NOT connect the AP to your live network when first connecting the AP to an administrative computer. If you connect it to a live network with an active DHCP server, then the AP can acquire a new IP address from DHCP and you will be unable to access it via the default IP address (192.168.0.1).

If the AP has a new IP address, then reset the AP to the factory configuration as described in the corresponding mounting or installation guide.

Because of different mounting and wiring procedures, each outdoor AP model has its own installation guide. Refer to the installation guide that shipped with your product for model-specific installation instructions. These documents are available from support.ruckuswireless.com
Getting to Know the Access Point Features

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

- SmartCell SC8800-S Outdoor Access Point
- ZoneFlex 7762 Access Point
- ZoneFlex 7762-AC Access Point
- ZoneFlex 7762-S Access Point
- ZoneFlex 7762-S-AC Access Point
- ZoneFlex 7762-T Access Point
- ZoneFlex 7781CM Access Point with Cable Modem
- ZoneFlex 7782 Access Point
- ZoneFlex 7782-E Access Point
- ZoneFlex 7782-N Access Point
- ZoneFlex 7782-S Access Point
- ZoneFlex T300 Outdoor Access Point
- ZoneFlex T300e Outdoor Access Point
- ZoneFlex T301n Outdoor Access Point
- ZoneFlex T301s Outdoor Access Point

NOTE: This guide does not include information on Ruckus Wireless Indoor APs, ZoneFlex 7731 Wireless Bridge, or ZoneFlex 7055 Multimedia Wi-Fi Wall Switches. For information on those models (along with Ruckus Wireless MediaFlex and MetroFlex product lines), refer to their respective documents available from support.ruckuswireless.com
SmartCell SC8800-S Outdoor Access Point

NOTE The 100.x AP base image supports standalone mode and FlexMaster (FM) WLAN manager operation. The RuckOS-compatible firmware images only support SCG, vSCG, and SZ controllers. The ZD-compatible firmware images only support ZD controllers.

The SC8800-S requires a minimum of AP base image 100.0.0 and later to operate, or SCG firmware 1.1 and later, or ZF firmware 9.6.1 and later to operate.

DO NOT connect the SC8800-S to a Ruckus Wireless controller with SCG firmware 1.0 or earlier, or ZF firmware 9.6.0 or earlier.

Figure 1 identifies the top-panel connectors on the AP. Table 3 describes these connectors.

Figure 1. SC8800-S top-panel connectors

<table>
<thead>
<tr>
<th>No.</th>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>5 GHz ANT 0 port</td>
<td>5GHz 50-ohm N-type connector. Can be used with an external antenna for operator-defined coverage areas and point-to-point deployments.</td>
</tr>
<tr>
<td>2</td>
<td>2.4 GHz ANT 2 port</td>
<td>2.4GHz 50-ohm N-type connector. Can be used with an external antenna for operator-defined coverage areas and point-to-point deployments.</td>
</tr>
</tbody>
</table>
Table 3. SC8800-S top-panel connectors (Continued)

<table>
<thead>
<tr>
<th>No.</th>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>2.4 GHz ANT 0 port</td>
<td>2.4GHz 50-ohm N-type connector. Can be used with an external antenna for operator-defined coverage areas and point-to-point deployments.</td>
</tr>
<tr>
<td>4</td>
<td>5 GHz ANT 2 port</td>
<td>5GHz 50-ohm N-type connector. Can be used with an external antenna for operator-defined coverage areas and point-to-point deployments.</td>
</tr>
</tbody>
</table>

Figure 2 identifies the AP bottom-panel connectors and LED locations on the AP. Table 4 describes these connectors and LEDs.

Figure 2. SC8800-S bottom-panel connectors and LED locations

Table 4. SC8800-S bottom-panel connectors

<table>
<thead>
<tr>
<th>No.</th>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Earth ground screw</td>
<td>Use this screw to attach an earth ground to the AP as required by local regulations.</td>
</tr>
<tr>
<td>2</td>
<td>AC power connector</td>
<td>You can use AC to supply power to the AP, in addition to using PoE.</td>
</tr>
</tbody>
</table>
Table 4. SC8800-S bottom-panel connectors (Continued)

<table>
<thead>
<tr>
<th>No.</th>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>PoE OUT RJ45 data connector</td>
<td>Supports 10/100/1000Mbps connections and PoE out. If the AP is powered using AC or the Ruckus Wireless PoE injector (ordered separately), then this port can supply 802.3af (15.4W) PoE to a connected PoE-capable device (for example, an IP-based surveillance camera). This port alternatively can supply 802.3at (25.5W) PoE when used with 20m (65.6 ft.) or shorter CAT5e UTP or better cable.</td>
</tr>
<tr>
<td>4</td>
<td>RESET button</td>
<td>This button resets the AP to its factory defaults, and is mounted under the RESET/PoE OUT RJ-45 waterproof gland.</td>
</tr>
<tr>
<td>5</td>
<td>PoE IN RJ45 data connector</td>
<td>Supports 10/100/1000Mbps connections, connects to the network and receives Power over Ethernet (PoE) from the Ruckus Wireless 60W PoE injector.</td>
</tr>
<tr>
<td>6</td>
<td>FIBER port</td>
<td>This waterproof gland allows you to run a fiber-optic cable into the SC8800-S chassis to an optional fiber modem.</td>
</tr>
<tr>
<td>7</td>
<td>LEDs</td>
<td>See Figure 3.</td>
</tr>
</tbody>
</table>

Figure 3 identifies the AP bottom-panel LED locations on the AP. Table 5 describes these connectors and LEDs.
Table 5. SC8800-S LED descriptions

<table>
<thead>
<tr>
<th>No.</th>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
</table>
| 1   | PWR LED | - Off: No power is available, or the AP is not connected to a power source.  
  - Solid Red: The AP is powering on.  
  - Solid Green: The AP is connected to a power source and has completed its power-on sequence. |
| 2   | DIR LED | - Off: The AP is NOT managed by ZoneDirector (standalone mode).  
  - Solid Green: The AP is managed by ZoneDirector and connection to ZoneDirector has been established.  
  - Fast Flashing Green (twice per second): The AP is managed by ZoneDirector and is currently receiving configuration settings (provisioning) or a firmware update.  
  - Slow Flashing Green (once every two seconds): The AP is managed by ZoneDirector, but is currently unable to communicate with ZoneDirector. |
Table 5. SC8800-S LED descriptions (Continued)

<table>
<thead>
<tr>
<th>No.</th>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
</table>
| 3   | AIR LED | - *Off*: The AP is operating in standalone mode or operating as a root AP (RAP) or a non-mesh AP.  
      - *Solid Green*: The AP is functioning as a Mesh AP (MAP) and the uplink signal quality is good (>24dBm).  
      - *Fast Flashing Green (twice per second)*: The AP is functioning as a Mesh AP (MAP) and the wireless signal to its uplink AP is fair.  
      - *Slow Flashing Green (once every two seconds)*: The AP is in mesh mode, but the AP is still searching for a mesh uplink. |
| 4   | 2.4G LED| - *Off*: WLAN service is down.  
      - *Amber (Yellow)*: WLAN service is up but with no client connected.  
      - *Solid Green*: WLAN service is up with at least one client connected. |
| 5   | 5G LED  | - *Off*: WLAN service is down.  
      - *Amber (Yellow)*: WLAN service is up but with no clients or downlink MAPs associated/connected.  
      - *Solid Green*: WLAN service is up with at least one client is associated. No downlink MAPs are connected.  
      - *Fast Flashing Green (twice per second)*: The WLAN is up, at least one downlink MAP is connected, and at least one client is associated.  
      - *Slow Flashing Green (once every two seconds)*: The WLAN is up and at least one downlink MAP is connected. No clients are associated. |
NOTE  The 100.x AP base image supports standalone mode and FlexMaster (FM) WLAN manager operation. The RuckOS-compatible firmware images only support SCG, vSCG, and SZ controllers. The ZD-compatible firmware images only support ZD controllers.

The 7762 requires a minimum of AP base image 100.0.0 and later to operate, or SCG firmware 1.1 and later, or ZF firmware 9.4 and later to operate.

Figure 4 and Figure 5 identify the AP external features.

Table 6. LEDs and connectors on the 7762 AP

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
</table>
| Power LED     | • Off: No power is available, or the AP is not connected to a power source.  
               | • Red: The AP is powering on.  
               | • Green: The AP is connected to a power source and has completed its power-on sequence.                                                      |
If you want to extend the range of your wireless network, you can connect external high gain antennas (5GHz only) to the standard N-type radio frequency (RF) antenna connectors on the top panel of the AP.

Table 6. LEDs and connectors on the 7762 AP (Continued)

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
</table>
| Status LED     | If the AP is operating in standalone mode:  
- **Amber**: The WLAN service is up and at least one wireless client is associated with the AP.  
- **Flashing amber**: The WLAN service is up and no wireless clients are currently associated with the AP.  
If the AP is being managed by Ruckus Wireless ZoneDirector:  
- **Green**: The AP is part of a mesh network (either as Root AP or Mesh AP) and is connected to an uplink with good signal. If mesh networking is disabled but the WLAN service is available, the Status LED is also green.  
- **Fast flashing green**: The AP is part of a mesh network (as Mesh AP) and is connected to an uplink with fair signal.  
- **Slow flashing green**: This Mesh AP is searching for an uplink or is attempting to establish communication with ZoneDirector.  
- **Off**: Mesh networking is disabled and the WLAN service is unavailable.                                                                                                                                                                                                               |
| RJ45 Connectors| Two LAN ports that support Power over Ethernet (PoE):  
- **PoE IN** port: Supports 10/100/1000Mbps connections, connects to the network and receives 802.at PoE from the supplied PoE injector (if connected).  
- **PoE OUT** port: Supports 10/100Mbps connections. If the supplied PoE injector is used, this port can supply 802.3af PoE to the connected PoE-capable device (for example, a 3G/4G small cell radio or an IP-based surveillance camera). To use this port to supply PoE, you first need to enable the PoE feature on the Web interface.                                                                                           |
| DC Connector   | In addition to PoE, you can also use direct current or DC (from a battery, for example) to supply power to the AP.                                                                                                                                                                                                                         |
Figure 5. The 7762 5GHz antenna connectors are protected by metal caps
NOTE The 100.x AP base image supports standalone mode and FlexMaster (FM) WLAN manager operation. The RuckOS-compatible firmware images only support SCG, vSCG, and SZ controllers. The ZD-compatible firmware images only support ZD controllers.

The 7762-AC requires a minimum of AP base image 100.0.0 and later to operate, or SCG firmware 1.1 and later, or ZF firmware 9.4 and later to operate.

**Figure 6 and Figure 7** identify the AP external features.

**Figure 6. 7762-AC AP parts**

---

**Table 7. 7762-AC LEDs and connectors**

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Power LED</td>
<td>• Off: No power is available, or the AP is not connected to a power source.</td>
</tr>
<tr>
<td></td>
<td>• Red: The AP is powering on.</td>
</tr>
<tr>
<td></td>
<td>• Green: The AP is connected to a power source and has completed its power-on sequence.</td>
</tr>
</tbody>
</table>
Status LED

If the AP is operating in standalone mode:

- **Amber**: The WLAN service is up and at least one wireless client is associated with the AP.
- **Flashing amber**: The WLAN service is up and no wireless clients are currently associated with the AP.

If the AP is being managed by Ruckus Wireless ZoneDirector:

- **Green**: The AP is part of a mesh network (either as Root AP or Mesh AP) and is connected to an uplink with good signal. If mesh networking is disabled but the WLAN service is available, the Status LED is also green.
- **Fast flashing green**: The AP is part of a mesh network (as Mesh AP) and is connected to an uplink with fair signal.
- **Slow flashing green**: This Mesh AP is searching for an uplink or is attempting to establish communication with ZoneDirector.
- **Off**: Mesh networking is disabled and the WLAN service is unavailable.

RJ45 Connectors

Two LAN ports that support Power over Ethernet (PoE):

- **PoE IN** port: Supports 10/100/1000Mbps connections, connects to the network and receives 802.at PoE from the Ruckus Wireless 60W PoE injector (not supplied, may be ordered separately – part number 902-0180-XX00, where XX is the country code).
- **PoE OUT** port: Supports 10/100Mbps connections. If the AP is using AC power or the Ruckus Wireless PoE injector (ordered separately), this port can supply 802.3af PoE to the connected PoE-capable device (for example, a 3G/4G small cell radio or an IP-based surveillance camera).

To use this port to supply PoE, you first need to enable the PoE feature on the Web interface. If you use PoE only to power the AP and you want to use the PoE OUT port to supply power to another device, you must use the Ruckus Wireless 60W PoE injector (part number 902-0180-XX00, where XX is the country code), which may be ordered separately.

AC Power Connector

You can use AC to supply power to the AP, in addition to using PoE.
If you want to extend the range of your wireless network, you can connect external high gain antennas (5GHz only) to the standard N-type radio frequency (RF) antenna connectors on the top panel of the AP.

Figure 7. The 7762-AC 5GHz antenna connectors are protected by metal caps.
ZoneFlex 7762-S Access Point

NOTE  The 100.x AP base image supports standalone mode and FlexMaster (FM) WLAN manager operation. The RuckOS-compatible firmware images only support SCG, vSCG, and SZ controllers. The ZD-compatible firmware images only support ZD controllers.

The 7762-S requires a minimum of AP base image 100.0.0 and later to operate, or SCG firmware 1.1 and later, or ZF firmware 9.4 and later to operate.

Figure 8 and Figure 9 identify the AP external features.

Figure 8. 7762-S AP parts

Table 8. 7762-S LEDs and connectors

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Power LED</td>
<td>• <strong>Off</strong>: No power is available or the AP is not connected to a power source.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Red</strong>: The AP is powering on.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Green</strong>: The AP is connected to a power source and has completed its power-on sequence.</td>
</tr>
</tbody>
</table>

[Diagram of AP parts and connectors]
### Status LED

If the AP is operating in standalone mode:
- **Amber**: The WLAN service is up and at least one wireless client is associated with the AP.
- **Flashing amber**: The WLAN service is up and no wireless clients are currently associated with the AP.

If the AP is being managed by Ruckus Wireless ZoneDirector:
- **Green**: The AP is part of a mesh network (either as a Root AP or Mesh AP) and is connected to an uplink with good signal. If mesh networking is disabled but the WLAN service is available, the Status LED is also green.
- **Fast flashing green**: The AP is part of a mesh network (as Mesh AP) and is connected to an uplink with a fair or good signal.
- **Slow flashing green**: This Mesh AP is searching for an uplink or is attempting to establish communication with ZoneDirector.
- **Off**: Mesh networking is disabled and the WLAN service is unavailable.

### RJ45 Connectors

Two LAN ports that support Power over Ethernet (PoE):
- **PoE IN** port: Supports 10/100/1000Mbps connections, connects to the network and receives 802.at PoE from the supplied PoE injector (if connected).
- **PoE OUT** port: Supports 10/100Mbps connections. If the supplied PoE injector is used, this port can supply 802.3af PoE to the connected PoE-capable device (for example, a 3G/4G small cell radio or an IP-based surveillance camera). To use this port to supply PoE, you first need to enable the PoE feature on the Web interface.

### DC Connector

In addition to PoE, you can also use direct current or DC (from a battery, for example) to supply power to the AP.

**NOTE**: If you connect the AP to both PoE and DC power sources at the same time, it uses PoE as the primary power source and DC power as the backup power source.
7762-S 5GHz Antenna Connectors

If you want to enable the 5GHz sections of the AP (for access or meshing), you can connect external high gain antennas (5GHz only) to the standard N-type radio frequency (RF) antenna connectors on the top panel of the AP.

Figure 9. The 7762-S 5GHz antenna connectors are protected by metal caps.

Make a note of the MAC address on this label. You will need it later.
ZoneFlex 7762-S-AC Access Point

NOTE The 100.x AP base image supports standalone mode and FlexMaster (FM) WLAN manager operation. The RuckOS-compatible firmware images only support SCG, vSCG, and SZ controllers. The ZD-compatible firmware images only support ZD controllers.

The 7762-S-AC requires a minimum of AP base image 100.0.0 and later to operate, or SCG firmware 1.1 and later, or ZF firmware 9.4 and later to operate.

Figure 10 and Figure 11 identify the AP external features.

Figure 10. 7762-S-AC parts

Table 9. 7762-S-AC LEDs and connectors

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Power LED</td>
<td>• Off: No power is available, or the AP is not connected to a power source.</td>
</tr>
<tr>
<td></td>
<td>• Red: The AP is powering on.</td>
</tr>
<tr>
<td></td>
<td>• Green: The AP is connected to a power source and has completed its power-on sequence.</td>
</tr>
</tbody>
</table>
### Status LED

If the AP is operating in standalone mode:
- **Amber**: The WLAN service is up and at least one wireless client is associated with the AP.
- **Flashing amber**: The WLAN service is up and no wireless clients are currently associated with the AP.

If the AP is being managed by Ruckus Wireless ZoneDirector:
- **Green**: The AP is part of a mesh network (either as Root AP or Mesh AP) and is connected to an uplink with good signal. If mesh networking is disabled but the WLAN service is available, the Status LED is also green.
- **Fast flashing green**: The AP is part of a mesh network (as Mesh AP) and is connected to an uplink with fair signal.
- **Slow flashing green**: This Mesh AP is searching for an uplink or is attempting to establish communication with ZoneDirector.
- **Off**: Mesh networking is disabled and the WLAN service is unavailable.

### RJ45 Connectors

Two LAN ports that support Power over Ethernet (PoE):
- **PoE IN** port: Supports 10/100/1000Mbps connections, connects to the network and receives 802.at PoE from the Ruckus Wireless 60W PoE injector (not supplied, may be ordered separately – part number 902-0180-XX00, where XX is the country code).
- **PoE OUT** port: Supports 10/100Mbps connections. If the AP is using AC power or the Ruckus Wireless PoE injector (ordered separately), this port can supply 802.3af PoE to the connected PoE-capable device (for example, a 3G/4G small cell radio or an IP-based surveillance camera).

To use this port to supply PoE, you first need to enable the PoE feature on the Web interface. If you use PoE only to power the AP and you want to use the PoE OUT port to supply power to another device, you must use the Ruckus Wireless 60W PoE injector (part number 902-0180-XX00, where XX is the country code), which may be ordered separately.

### AC Power Connector

You can use AC to supply power to the AP, in addition to using PoE.
If you want to extend the range of your wireless network, you can connect external high gain antennas (5GHz only) to the standard N-type radio frequency (RF) antenna connectors on the top panel of the AP.

Figure 11. The 7762-S-AC 5GHz antenna connectors are protected by metal caps.
ZoneFlex 7762-T Access Point

NOTE The 100.x AP base image supports standalone mode and FlexMaster (FM) WLAN manager operation. The RuckOS-compatible firmware images only support SCG, vSCG, and SZ controllers. The ZD-compatible firmware images only support ZD controllers.

The 7762-T requires a minimum of AP base image 100.0.0 and later to operate, or SCG firmware 1.1 and later, or ZF firmware 9.4 and later to operate.

Figure 12 and Figure 13 identify the AP external features.

Figure 12. 7762-T AP parts

![7762-T AP parts diagram]

Table 10. 7762-T LEDs and connectors

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Power LED</td>
<td>- Off: No power is available, or the AP is not connected to a power source.</td>
</tr>
<tr>
<td></td>
<td>- Red: The AP is powering on.</td>
</tr>
<tr>
<td></td>
<td>- Green: The AP is connected to a power source and has completed its power-on sequence.</td>
</tr>
</tbody>
</table>

Ground Screw
RJ-45/PoE Connectors
DC Connector
5GHz External Antenna Connectors
Power LED
Status LED
If you want to extend the range of your wireless network, you can connect external antennas (5GHz only) to the standard N-type radio frequency (RF) antenna connectors on the top panel of the AP.

### Table 10. 7762-T LEDs and connectors (Continued)

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status LED</td>
<td>If the AP is operating in standalone mode:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Amber:</strong> The WLAN service is up and at least one wireless client is associated with the AP.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Flashing amber:</strong> The WLAN service is up and no wireless clients are currently associated with the AP.</td>
</tr>
<tr>
<td></td>
<td>If the AP is being managed by Ruckus Wireless ZoneDirector:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Green:</strong> The AP is part of a mesh network (either as Root AP or Mesh AP) and is connected to an uplink with good signal. If mesh networking is disabled but the WLAN service is available, the Status LED is also green.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Fast flashing green:</strong> The AP is part of a mesh network (as Mesh AP) and is connected to an uplink with fair signal.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Slow flashing green:</strong> This Mesh AP is searching for an uplink or is attempting to establish communication with ZoneDirector.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Off:</strong> Mesh networking is disabled and the WLAN service is unavailable.</td>
</tr>
<tr>
<td>RJ45 Connectors</td>
<td>Two LAN ports that support Power over Ethernet (PoE):</td>
</tr>
<tr>
<td></td>
<td>• <strong>PoE IN</strong> port: Supports 10/100/1000Mbps connections, connects to the network and receives 802.at PoE from the supplied PoE injector (if connected).</td>
</tr>
<tr>
<td></td>
<td>• <strong>PoE OUT</strong> port: Supports 10/100Mbps connections. If the supplied PoE injector is used, this port can supply 802.3af PoE to the connected PoE-capable device (for example, a 3G/4G small cell radio or an IP-based surveillance camera). To use this port to supply PoE, you first need to enable the PoE feature on the Web interface.</td>
</tr>
<tr>
<td>DC Connector</td>
<td>In addition to PoE, you can also use direct current or DC (from a battery, for example) to supply power to the AP.</td>
</tr>
</tbody>
</table>
NOTE  The maximum value for the antenna gain that you should set depends on the type of external antennas that you are connecting to the AP.

Figure 13. The 7762-T 5GHz antenna connectors are protected by metal caps
NOTE  The 100.x AP base image supports standalone mode and FlexMaster (FM) WLAN manager operation. The RuckOS-compatible firmware images only support SCG, vSCG, and SZ controllers. The ZD-compatible firmware images only support ZD controllers.

The 7781CM requires a minimum of AP base image 100.0.0 and later to operate, or SCG firmware 1.1 and later, or ZF firmware 9.5.1 and later to operate.

Figure 14 and Figure 15 identify the 7781CM AP with integral Cable Modem AP (7781CM) external features.

- The 901-7781-US01 and 901-7781-WW01 DOCSIS 7781CMs and the 901-7781-JP21 JCTEA DOCSIS 7781CMs include a shroud and cable clamps to mount the 7781CMs on strand support cables.
- The 901-7781-WW11 EuroDOCSIS 7781CMs do not include a shroud or cable clamps, and are mounted using customer-supplied mounting brackets.

Figure 14.  7781CM connectors
Table 11. 7781CM connectors

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ethernet Port (under blanking cap)</td>
<td>RJ-45 port that supports 10/100/1000Mbps connections and provides 802.3af-compliant (15.4W) Power over Ethernet (PoE) output power to external devices. PoE output (and internal CM heater, if equipped) are only supported when the 7781CM receives Power Over Cable (POC) from the HFC cable plant.</td>
</tr>
<tr>
<td>Reset Button (under blanking cap)</td>
<td>Refer to the ZoneFlex 7781CM Cable Modem Access Point Installation Guide to access the reset button and either reboot the AP or reset the AP to factory defaults.</td>
</tr>
<tr>
<td>DC Connector (under blanking cap)</td>
<td>In addition to the power supplied by the coaxial cable from the cable modem termination system (CMTS) equipment, the 7781CM can also be DC powered for configuration before field deployment.</td>
</tr>
<tr>
<td>Coaxial Cable Connector B</td>
<td>Connects to the CMTS at the headend using a tap on the plant, and provides AC POC to the 7781CM. For more information, refer to the ZoneFlex 7781CM Cable Modem Access Point Installation Guide.</td>
</tr>
</tbody>
</table>

Figure 15. 7781CM LEDs
Reading the 7781CM LEDs

The six dual-purpose LEDs are used both by the CM part and the AP part of the 7781CM:

- When LED 1 (green LED) is lit, the LEDs are in Access Point mode.
- When LED 2 (white LED) is lit, the LEDs are in Cable Modem mode.

While the 7781CM is booting up, the LEDs are in CM mode. Once bootup is completed, the LEDs alternate between CM and AP modes.

NOTE The 7781CM LEDs turn off after a while. This is normal operation.

Refer to the following:
- LED Boot Sequence
- LED Online/Steady State
- Reading LEDs in Access Point Mode
- Reading LEDs in Cable Modem Mode

LED Boot Sequence

1. All LEDs blink for a few seconds.
2. LED 2 (white) stays solid on.
3. LEDs 3, 4, 5 and 6 (blue, middle green, yellow and red) blink in sequence.
4. LEDs 4, 5 and 6 (middle green, yellow and red) blink together for a few seconds.
5. LED 3 (blue) goes solid when the link to the AP is established.
6. LED 6 (red) flashes as CM tries to acquire downstream.
   - LED 6 (red) goes solid when downstream is acquired.
   - LED 3 (blue) flashes to indicate communication across the AP link.
7. LED 5 (yellow) comes on solid when upstream acquired.
8. LED 4 (middle green) on indicates that cable modem came on-line successfully.

LED Online/Steady State

- LED 1 (green) on indicates AP mode.
- LED 2 (white) on indicates CM mode.
- LEDs 3, 4, 5 and 6 (blue, middle green, yellow and red) are on.

The LEDs alternate between CM and AP modes.
NOTE  The 7781CM LEDs turn off after a while. This is normal operation.

Reading LEDs in Access Point Mode

In AP mode, LED 1 (green LED) is lit.

NOTE  The LEDs do not indicate whether the AP is in standalone mode or if ZoneDirector is managing the AP. To check if ZoneDirector is managing the AP, log into the ZoneDirector Web interface, go to the APs page, and then search for the AP’s MAC address. If you are unable to find the AP, then it is very likely in standalone mode. If you have multiple ZoneDirector devices on the network, make sure you check each one of them.

For Cable Operators, APs will typically be in ZoneDirector mode after initial boot. If the AP is unable to reach the ZoneDirector on initial boot, it remains in standalone mode.

Refer to Table 12 for a summary of AP mode LED behavior.

Table 12. 7781CM LED behavior in AP Standalone and ZoneDirector modes

<table>
<thead>
<tr>
<th>LED</th>
<th>State</th>
<th>AP Standalone Mode</th>
<th>AP ZoneDirector Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Solid Green</td>
<td>On = AP Mode.</td>
<td>On = AP Mode.</td>
</tr>
<tr>
<td>2</td>
<td>OFF</td>
<td>Off = Not AP Mode.</td>
<td>Off = Not AP Mode.</td>
</tr>
<tr>
<td>3</td>
<td>Solid Blue</td>
<td>At least one 5GHz wireless client is associated with the</td>
<td>If AP is RAP, at least one MAP is associated. If AP is MAP it is associated with a RAP. Signal strength is weak.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>access point and signal strength is weak.</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>Flashing Green</td>
<td>5GHz WLAN is up but no clients.</td>
<td>5GHz WLAN is up but no clients.</td>
</tr>
<tr>
<td></td>
<td>Solid Green</td>
<td>At least one 5GHz wireless client is associated with the</td>
<td>If AP is RAP, at least one MAP is associated. If AP is MAP it is associated with a RAP. Signal strength is strong.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>access point and signal strength is strong.</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>Solid Yellow</td>
<td>At least one 2.4GHz wireless client is associated with the</td>
<td>At least one 2.4GHz wireless client is associated with the</td>
</tr>
<tr>
<td></td>
<td></td>
<td>access point and signal strength is weak.</td>
<td>access point and signal strength is weak.</td>
</tr>
</tbody>
</table>
Reading LEDs in Cable Modem Mode

In CM mode, LED 2 (white LED) is always lit. Refer to Table 13 for a summary of CM mode LED behavior. Refer to LED Boot Sequence and LED Online/Steady State for more details.

Table 13. 7781CM LED behavior in CM mode

<table>
<thead>
<tr>
<th>LED</th>
<th>State</th>
<th>AP Standalone Mode</th>
<th>AP ZoneDirector Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>OFF</td>
<td>2.4GHz WLAN is up but no clients.</td>
<td>2.4GHz WLAN is up but no clients.</td>
</tr>
<tr>
<td>2</td>
<td>Solid White</td>
<td>At least one 2.4GHz wireless client is associated with the access point and signal strength is strong.</td>
<td>At least one 2.4GHz wireless client is associated with the access point and signal strength is strong.</td>
</tr>
<tr>
<td>3</td>
<td>Solid Blue</td>
<td>On line</td>
<td>Link</td>
</tr>
<tr>
<td>4</td>
<td>Solid Green</td>
<td>On line</td>
<td>Upstream acquired</td>
</tr>
<tr>
<td>5</td>
<td>Solid Yellow</td>
<td>Searching for downstream</td>
<td>Downstream acquired</td>
</tr>
<tr>
<td>6</td>
<td>Flashing Red</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Solid Red</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Powering Options

The 7781CM supports both DC power or AC power over cable (POC). Normally 12 VDC power is only used at the depot or when debugging. 40 to 90 VAC POC is only used when the 7781CM is mounted on a cable strand and powered via an F-type coaxial cable connected to the HFC cable plant.

The customer-ordered 1.5A 12 VDC power supply part number is 902-0169-xxxy, where xx = Country and yy = revision.

NOTE: The 7781CM does not provide PoE output or support internal heater operation when powered by 12 VDC.
Cable Modem Heater
The 901-7781-US01, 901-7781-JP21 and 901-7781-WW01 7781CM includes a built-in heater for the cable modem that permits operation at extremely low temperatures. The heater is typically on below -10° C (14° F). The heater is powered by POC only. When the 7781CM is powered by 12 VDC, the heater is disabled. The 901-7781-WW11 EuroDOCSIS 7781CM does not include a built-in heater.

7781CM Operation
Refer to the ZoneFlex 7781CM Cable Modem Access Point Installation Guide for information on Cable Modem configuration and operation.
ZoneFlex 7782 Access Point

NOTE  The 100.x AP base image supports standalone mode and FlexMaster (FM) WLAN manager operation. The RuckOS-compatible firmware images only support SCG, vSCG, and SZ controllers. The ZD-compatible firmware images only support ZD controllers.

The 7782 requires a minimum of AP base image 100.0.0 and later to operate, or SCG firmware 1.1 and later, or ZF firmware 9.5.1 and later to operate.

Figure 16 identifies the connectors and LEDs on the 7782 Omni AP. Table 14 describes the LEDs and connectors.

Figure 16. 7782 connectors and LEDs - bottom view
Table 14. 7782 LED and connector descriptions

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>PoE IN RJ45 data connector</td>
<td>Supports 10/100/1000Mbps connections, connects to the network and receives 802.3at Power over Ethernet (PoE) from the Ruckus Wireless 60W PoE injector.</td>
</tr>
<tr>
<td>PoE OUT RJ45 data connector</td>
<td>Supports 10/100/1000Mbps connections and PoE out. If the AP is powered using AC or the Ruckus Wireless PoE injector (ordered separately), then this port can supply 802.3af (up to 25W) PoE to a connected PoE-capable device (for example, a 3G/4G small cell radio or an IP-based surveillance camera). For devices requiring more than 15.4W, use short (less than 10 feet or 3m) Ethernet cables. In high-temperature environments, the amount of power available is to be determined.</td>
</tr>
<tr>
<td>Reset button</td>
<td>This button is inside the PoE OUT cable gland. Refer to the ZoneFlex 7782 Outdoor Access Point Installation Guide to access the reset button and reset the AP.</td>
</tr>
<tr>
<td>AC IN power connector</td>
<td>You can use AC to supply power to the AP, in addition to using PoE.</td>
</tr>
<tr>
<td>STATUS LED</td>
<td>When the AP is operating in standalone mode:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Amber</strong>: The WLAN service is up and at least one wireless client is associated with the AP.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Flashing amber</strong>: The WLAN service is up and no wireless clients are currently associated with the AP.</td>
</tr>
<tr>
<td></td>
<td>When the AP is being managed by Ruckus Wireless ZoneDirector:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Green</strong>: The AP is part of a mesh network (either as Root AP or Mesh AP) and is connected to an uplink with good signal. If mesh networking is disabled but the WLAN service is available, the Status LED is also green.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Fast flashing green</strong>: The AP is part of a mesh network (as Mesh AP) and is connected to an uplink with fair signal.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Slow flashing green</strong>: This Mesh AP is searching for an uplink or is attempting to establish communication with ZoneDirector.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Off</strong>: Mesh networking is disabled and the WLAN service is unavailable.</td>
</tr>
</tbody>
</table>
Table 14. 7782 LED and connector descriptions (Continued)

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>POWER LED</td>
<td>• Off: No power is available, or the AP is not connected to a power source.</td>
</tr>
<tr>
<td></td>
<td>• Red: The AP is powering on.</td>
</tr>
<tr>
<td></td>
<td>• Green: The AP is connected to a power source and has completed its power-on sequence.</td>
</tr>
</tbody>
</table>
ZoneFlex 7782-E Access Point

NOTE  The 100.x AP base image supports standalone mode and FlexMaster (FM) WLAN manager operation. The RuckOS-compatible firmware images only support SCG, vSCG, and SZ controllers. The ZD-compatible firmware images only support ZD controllers.

The 7782-E requires a minimum of AP base image 100.0.0 and later to operate, or SCG firmware 1.1 and later, or ZF firmware 9.5.1 and later to operate.

Figure 17 identifies the connectors and LEDs on the bottom of the 7782-E External Antenna AP. Figure 18 identifies the connectors on the top of the 7782-E.

If you want to extend the range of your wireless network, then you can connect external high gain antennas to the standard N-type radio frequency (RF) antenna connectors on the top panel of the AP. The antennas must have a gain of less than 9dBi to comply with FCC and CE regulations.

Figure 17.  7782-E connectors and LEDs - bottom view
### Table 15. 7782-E top-panel N-type connectors

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
</table>
| 5GHz connectors: ANT 0, ANT 1 and ANT 2 | These 5GHz 50-ohm female connectors can be used with up to three external antennas for operator-defined coverage areas and point-to-point deployments.  
- When you are connecting two 5GHz antennas to the AP, use the ANT 0 and ANT 2 5GHz connectors.  
- When you are connecting three 5GHz antennas to the AP, use the all three ANT 0, ANT 1 and ANT 2 5GHz connectors. |
Table 15. 7782-E top-panel N-type connectors (Continued)

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
</table>
| 2.4GHz connectors: ANT 0, ANT 1 and ANT 2 | These 2.4GHz 50-ohm female connectors can be used with up to three external antennas for operator-defined coverage areas and point-to-point deployments.  
- When you are connecting two 2.4GHz antennas to the AP, use the ANT 0 and ANT 2 2.4GHz connectors.  
- When you are connecting three 2.4GHz antennas to the AP, use the all three ANT 0, ANT 1 and ANT 2 2.4GHz connectors. |
| GPS connector | This 50-ohm female N-type connector is used for a standard powered external GPS antenna. The factory-supplied GPS antenna kit complies with all 7782-E AP requirements.  
If you are installing a customer-supplied antenna and extension cable, then keep the cable short or use low-loss cable to avoid excess signal attenuation. The 7782-E supplies 3.3 VDC to the GPS antenna; make sure that a customer-supplied GPS antenna does not require more than 150mA. |
ZoneFlex 7782-N Access Point

NOTE  The 100.x AP base image supports standalone mode and FlexMaster (FM) WLAN manager operation. The RuckOS-compatible firmware images only support SCG, vSCG, and SZ controllers. The ZD-compatible firmware images only support ZD controllers.

The 7782-N requires a minimum of AP base image 100.0.0 and later to operate, or SCG firmware 1.1 and later, or ZF firmware 9.5.1 and later to operate.

Figure 19 identifies the connectors and LEDs on the 7782-N 30-Degree Narrow Sector AP. Table 16 describes the LEDs and connectors.

Figure 19. 7782-N connectors and LEDs - bottom view
Table 16. 7782-N LED and connector descriptions

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>PoE IN</strong> RJ45 data connector</td>
<td>Supports 10/100/1000Mbps connections, connects to the network and receives 802.3at Power over Ethernet (PoE) from the Ruckus Wireless 60W PoE injector.</td>
</tr>
<tr>
<td><strong>PoE OUT</strong> RJ45 data connector</td>
<td>Supports 10/100/1000Mbps connections and PoE out. If the AP is powered using AC or the Ruckus Wireless PoE injector (ordered separately), then this port can supply 802.3af (15.4W) PoE to a connected PoE-capable device (for example, a 3G/4G small cell radio or an IP-based surveillance camera). For devices requiring more than 15.4W, use short (less than 10 feet or 3m) Ethernet cables. In high-temperature environments, the amount of power available is to be determined.</td>
</tr>
<tr>
<td>Reset button</td>
<td>This button is inside the PoE OUT cable gland. Refer to the ZoneFlex 7782 Outdoor Access Point Installation Guide to access the reset button and reset the AP.</td>
</tr>
<tr>
<td><strong>AC IN</strong> power connector</td>
<td>You can use AC to supply power to the AP, in addition to using PoE.</td>
</tr>
</tbody>
</table>
| **STATUS LED** | When the AP is operating in standalone mode:  
  - *Amber*: The WLAN service is up and at least one wireless client is associated with the AP.  
  - *Flashing amber*: The WLAN service is up and no wireless clients are currently associated with the AP.  
  When the AP is being managed by Ruckus Wireless ZoneDirector:  
  - *Green*: The AP is part of a mesh network (either as Root AP or Mesh AP) and is connected to an uplink with good signal. If mesh networking is disabled but the WLAN service is available, the Status LED is also green.  
  - *Fast flashing green*: The AP is part of a mesh network (as Mesh AP) and is connected to an uplink with fair signal.  
  - *Slow flashing green*: This Mesh AP is searching for an uplink or is attempting to establish communication with ZoneDirector.  
  - *Off*: Mesh networking is disabled and the WLAN service is unavailable. |
### Table 16. 7782-N LED and connector descriptions (Continued)

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>POWER LED</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Off</strong>: No power is available, or the AP is not connected to a power source.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Red</strong>: The AP is powering on.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Green</strong>: The AP is connected to a power source and has completed its power-on sequence.</td>
</tr>
</tbody>
</table>
ZoneFlex 7782-S Access Point

NOTE The 100.x AP base image supports standalone mode and FlexMaster (FM) WLAN manager operation. The RuckOS-compatible firmware images only support SCG, vSCG, and SZ controllers. The ZD-compatible firmware images only support ZD controllers.

The 7782-S requires a minimum of AP base image 100.0.0 and later to operate, or SCG firmware 1.1 and later, or ZF firmware 9.5.1 and later to operate.

Figure 20 identifies the connectors and LEDs on the 7782-S 120-Degree Sector AP. Table 17 describes the LEDs and connectors.
Table 17. 7782-S LED and connector descriptions

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>PoE IN</strong> RJ45 data connector</td>
<td>Supports 10/100/1000Mbps connections, connects to the network and receives 802.1at Power over Ethernet (PoE) from the Ruckus Wireless 60W PoE injector.</td>
</tr>
<tr>
<td><strong>PoE OUT</strong> RJ45 data connector</td>
<td>Supports 10/100/1000Mbps connections and PoE out. If the AP is powered using AC or the Ruckus Wireless PoE injector (ordered separately), then this port can supply 802.3af (15.4W) PoE to a connected PoE-capable device (for example, a 3G/4G small cell radio or an IP-based surveillance camera). For devices requiring more than 15.4W, use short (less than 10 feet or 3m) Ethernet cables. In high-temperature environments, the amount of power available is to be determined.</td>
</tr>
<tr>
<td>Reset button</td>
<td>This button is inside the PoE OUT cable gland. Refer to the ZoneFlex 7782 Outdoor Access Point Installation Guide to access the reset button and reset the AP.</td>
</tr>
<tr>
<td><strong>AC IN</strong> power connector</td>
<td>You can use AC to supply power to the AP, in addition to using PoE.</td>
</tr>
</tbody>
</table>
| **STATUS LED**      | When the AP is operating in standalone mode:  
  - **Amber**: The WLAN service is up and at least one wireless client is associated with the AP.  
  - **Flashing amber**: The WLAN service is up and no wireless clients are currently associated with the AP.  

When the AP is being managed by Ruckus Wireless ZoneDirector:  
  - **Green**: The AP is part of a mesh network (either as Root AP or Mesh AP) and is connected to an uplink with good signal. If mesh networking is disabled but the WLAN service is available, the Status LED is also green.  
  - **Fast flashing green**: The AP is part of a mesh network (as Mesh AP) and is connected to an uplink with fair signal.  
  - **Slow flashing green**: This Mesh AP is searching for an uplink or is attempting to establish communication with ZoneDirector.  
  - **Off**: Mesh networking is disabled and the WLAN service is unavailable. |
Table 17. 7782-S LED and connector descriptions (Continued)

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>POWER LED</strong></td>
<td>• <em>Off:</em> No power is available, or the AP is not connected to a power source.</td>
</tr>
</tbody>
</table>
ZoneFlex T300 Outdoor Access Point

NOTE  The 100.x AP base image supports standalone mode and FlexMaster (FM) WLAN manager operation. The RuckOS-compatible firmware images only support SCG, vSCG, and SZ controllers. The ZD-compatible firmware images only support ZD controllers.

The T300 requires a minimum of AP base image 100.0.0 and later to operate, or SCG firmware 2.5.1 and later, or ZF firmware 9.8.1 and later to operate. **DO NOT connect the T300 AP to a Ruckus Wireless Controller with ZF 9.8.0 or earlier, or to SCG 2.5.0 or earlier.**

Figure 21 identifies the LEDs and connectors on the AP. Table 18 describes these LEDs and other elements.

Figure 21. T300 LEDs and other elements
<table>
<thead>
<tr>
<th>No.</th>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Earth ground screw</td>
<td>Use this screw to attach an earth ground to the AP as required by local regulations.</td>
</tr>
</tbody>
</table>
| 2   | 5G 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. |
| 3   | 2.4G 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. |
| 4   | 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. |
## Table 18. T300 LED and other element descriptions (Continued)

<table>
<thead>
<tr>
<th>No.</th>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>DIR LED</td>
<td>- Off: The AP is not being managed by ZoneDirector (standalone mode).</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Green: The AP is being managed by ZoneDirector.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Slow flashing green (one flash every two seconds): The AP is being managed by ZoneDirector, but is currently unable to communicate with ZoneDirector.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Fast flashing green (two flashes every second): The AP is being managed by ZoneDirector and is currently receiving configuration settings (provisioning) or a firmware update.</td>
</tr>
<tr>
<td>6</td>
<td>PWR LED</td>
<td>- Off: Off.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Red: Boot up in process.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Green: On.</td>
</tr>
<tr>
<td>7</td>
<td>PoE IN RJ45 data connector</td>
<td>Supports 10/100/1000Mbps connections, and receives Power over Ethernet (PoE).</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Note:</strong> The T300 can be powered by any 802.3af PSE device. Refer to the Ruckus Wireless T300 data sheet for recommended PoE accessories.</td>
</tr>
<tr>
<td>8</td>
<td>RESET button</td>
<td>This button resets the AP to its factory defaults, and is mounted under the RESET/PoE IN RJ-45 waterproof gland.</td>
</tr>
</tbody>
</table>
ZoneFlex T300e Outdoor Access Point

NOTE  The 100.x AP base image supports standalone mode and FlexMaster (FM) WLAN manager operation. The RuckOS-compatible firmware images only support SCG, vSCG, and SZ controllers. The ZD-compatible firmware images only support ZD controllers.

The T300e requires a minimum of AP base image 100.0.0 and later to operate, or SCG firmware 2.5.1 and later, or ZF firmware 9.8.1 and later to operate. DO NOT connect the T300 AP to a Ruckus Wireless Controller with ZF 9.8.0 or earlier, or to SCG 2.5.0 or earlier.

Figure 22 identifies the LEDs and hardware on the AP. Table 19 describes these LEDs and other elements.

Figure 22. T300e LEDs and other elements
### Table 19. T300e LED and other element descriptions

<table>
<thead>
<tr>
<th>No.</th>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Earth ground screw</td>
<td>Use this screw to attach an earth ground to the AP as required by local regulations.</td>
</tr>
</tbody>
</table>
| 2   | 5G 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. |
| 3   | 2.4G 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. |
| 4   | 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. |
Table 19. T300e LED and other element descriptions (Continued)

<table>
<thead>
<tr>
<th>No.</th>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>DIR LED</td>
<td>• Off: The AP is not being managed by ZoneDirector (standalone mode).</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Green: The AP is being managed by ZoneDirector.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Slow flashing green (one flash every two seconds): The AP is being</td>
</tr>
<tr>
<td></td>
<td></td>
<td>managed by ZoneDirector, but is currently unable to communicate with Zone</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Director.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Fast flashing green (two flashes every second): The AP is being managed</td>
</tr>
<tr>
<td></td>
<td></td>
<td>by ZoneDirector and is currently receiving configuration settings (provisioning) or a firmware update.</td>
</tr>
<tr>
<td>6</td>
<td>PWR LED</td>
<td>• Off: Off.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Red: Boot up in process.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Green: On.</td>
</tr>
<tr>
<td>7</td>
<td>PoE IN RJ45 data connector</td>
<td>Supports 10/100/1000Mbps connections, and receives Power over Ethernet (PoE).</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Note:</strong> The T300e can be powered by any 802.3af PSE device. Refer to the Ruckus Wireless T300e data sheet for recommended PoE accessories.</td>
</tr>
<tr>
<td>8</td>
<td>RESET button</td>
<td>This button resets the AP to its factory defaults, and is mounted under the RESET/PoE IN RJ-45 waterproof gland.</td>
</tr>
</tbody>
</table>

Figure 23 identifies the 5GHz RF connectors on the AP. Table 20 describes these RF connectors.

If you want to extend the range of your wireless network, then you can connect external high gain antennas to the standard N-type radio frequency (RF) antenna connectors on the top panel of the AP. The antennas must have a gain of less than 9dBi to comply with FCC and CE regulations.
Table 20. T300e N-type RF connectors

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>5GHz connectors</td>
<td>These 5GHz 50-ohm female connectors can be used with up to two external antennas for operator-defined coverage areas and point-to-point deployments.</td>
</tr>
</tbody>
</table>
ZoneFlex T301n Outdoor Access Point

NOTE  The 100.x AP base image supports standalone mode and FlexMaster (FM) WLAN manager operation. The RuckOS-compatible firmware images only support SCG, vSCG, and SZ controllers. The ZD-compatible firmware images only support ZD controllers.

The T301n requires a minimum of AP base image 100.0.0 and later to operate, or SCG firmware 2.5.1 and later, or ZF firmware 9.8.1 and later to operate. DO NOT connect the T301n AP to a Ruckus Wireless Controller with ZF 9.8.0 or earlier, or to SCG 2.5.0 or earlier.

Figure 24 identifies the LEDs and connectors on the AP. Table 21 describes these LEDs and other elements.

Figure 24. T301n LEDs and other elements
### Table 21. T301n LED and other element descriptions

<table>
<thead>
<tr>
<th>No.</th>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Earth ground screw</td>
<td>Use this screw to attach an earth ground to the AP as required by local regulations.</td>
</tr>
</tbody>
</table>
| 2   | 5G 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. |
| 3   | 2.4G 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. |
| 4   | 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. |
### Table 21. T301n LED and other element descriptions (Continued)

<table>
<thead>
<tr>
<th>No.</th>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
</table>
| 5   | 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 a firmware update. |
| 6   | PWR LED        | • **Off**: Off.  
• **Red**: Boot up in process.  
• **Green**: On.                                                                                                                     |
| 7   | PoE IN RJ45 data connector | Supports 10/100/1000Mbps connections, and receives Power over Ethernet (PoE).  
**Note:** The T301n can be powered by any 802.3af PSE device. Refer to the Ruckus Wireless T301n data sheet for recommended PoE accessories. |
| 8   | RESET button   | This button resets the AP to its factory defaults, and is mounted under the **RESET/PoE IN** RJ-45 waterproof gland. |

---

---
ZoneFlex T301s Outdoor Access Point

NOTE  The 100.x AP base image supports standalone mode and FlexMaster (FM) WLAN manager operation. The RuckOS-compatible firmware images only support SCG, vSCG, and SZ controllers. The ZD-compatible firmware images only support ZD controllers.

The T301s requires a minimum of AP base image 100.0.0 and later to operate, or SCG firmware 2.5.1 and later, or ZF firmware 9.8.1 and later to operate. **DO NOT connect the T301s AP to a Ruckus Wireless Controller with ZF 9.8.0 or earlier, or to SCG 2.5.0 or earlier.**

Figure 25 identifies the LEDs and connectors on the AP. Table 22 describes these LEDs and other elements.

Figure 25. T301s LEDs and other elements
### Table 22. T301s LED and other element descriptions

<table>
<thead>
<tr>
<th>No.</th>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Earth ground screw</td>
<td>Use this screw to attach an earth ground to the AP as required by local regulations.</td>
</tr>
<tr>
<td>2</td>
<td>5G LED</td>
<td>• <strong>Off</strong>: The WLAN service is down.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <strong>Amber</strong>: The WLAN is up, but no clients or downlink MAPs are associated/connected.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <strong>Green</strong>: The WLAN is up and at least one client is associated. No downlink MAPs are connected.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <strong>Slow flashing green</strong> (one flash every two seconds): The WLAN is up and at least one downlink MAP is connected. No clients are associated.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <strong>Fast flashing green</strong> (two flashes every second): The WLAN is up, at least one downlink MAP is connected, and at least one client is associated.</td>
</tr>
<tr>
<td>3</td>
<td>2.4G LED</td>
<td>• <strong>Off</strong>: The WLAN service is down.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <strong>Green</strong>: The WLAN is up and at least one client is associated.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <strong>Amber</strong>: The WLAN is up. No clients are associated.</td>
</tr>
<tr>
<td>4</td>
<td>AIR LED</td>
<td>• <strong>Off</strong>: The AP is operating in standalone mode or operating as a root AP (RAP) or a non-mesh AP.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <strong>Green</strong>: The AP is functioning as a Mesh AP (MAP), and the wireless signal to its uplink AP is good.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <strong>Fast flashing green</strong> (two flashes every second): The AP is functioning as a Mesh AP (MAP), and the wireless signal to its uplink AP is fair.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <strong>Slow flashing green</strong> (one flash every two seconds): Mesh networking is enabled, but the AP is still searching for a mesh uplink.</td>
</tr>
</tbody>
</table>
### Getting to Know the Access Point Features

#### ZoneFlex T301s Outdoor Access Point

<table>
<thead>
<tr>
<th>No.</th>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
</table>
| 5   | 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 a firmware update. |
| 6   | PWR LED             | • **Off**: Off.  
• **Red**: Boot up in process.  
• **Green**: On. |
| 7   | PoE IN RJ45 data connector | Supports 10/100/1000Mbps connections, and receives Power over Ethernet (PoE).  
**Note:** The T301s can be powered by any 802.3af PSE device. Refer to the Ruckus Wireless T301s data sheet for recommended PoE accessories. |
| 8   | RESET button        | This button resets the AP to its factory defaults, and is mounted under the **RESET/PoE IN** RJ-45 waterproof gland. |
Navigating the Web Interface

In this chapter:

- Before You Begin: Preconfiguring the AP
- Navigating the Web Interface
- When Using a Dual-Band AP
Before You Begin: 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 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 firmware image after reboot and factory reset.

To replace controller-compatible AP firmware with the AP 100.0 base image, please select the AP and download the required AP firmware 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 a ZD Controller
- Configuring the AP for Standalone Operation or for Management by an FM Manager
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 firmware 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 a ZD Controller

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 firmware 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 an FM Manager

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 Google Chrome, Mozilla Firefox 2.0 (or later) or Microsoft Internet Explorer 6.0 (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 a Ruckus Wireless 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.
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 (or 192.168.100.2 for Cable Modem APs)

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 23 lists the Web interface features that are identified in Figure 26.

Figure 26. Elements of the Ruckus Wireless AP Web Interface

<table>
<thead>
<tr>
<th>No.</th>
<th>Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Menu</td>
<td>Under each category (Status, Configuration, etc.) are options that, when clicked, open the related workspace in the area to the right.</td>
</tr>
<tr>
<td>2</td>
<td>Tabs</td>
<td>Contains additional options for the configuration page. For example, the Configuration &gt; Wireless page includes one tab for common wireless configuration and eight tabs, one for each of the available WLANs.</td>
</tr>
<tr>
<td>3</td>
<td>LOGOUT Button</td>
<td>Click this button to log out of the AP.</td>
</tr>
<tr>
<td>4</td>
<td>Help Button</td>
<td>Click this button to open a help window with information related specifically to the options currently displayed in the workspace.</td>
</tr>
<tr>
<td>5</td>
<td>Workspace</td>
<td>This large area displays features, options and indicators relevant to your menu bar choices.</td>
</tr>
</tbody>
</table>
When Using a Dual-Band AP

If your Ruckus Wireless AP model is dual-band, then 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 27** highlights the differences between single-band and dual-band Ruckus Wireless AP menus.

**Figure 27.** Menu items are slightly different in single-band APs (left) and dual-band APs (right)
Configuring the Access Point

NOTE  If the AP has been configured with SCG, vSCG, SZ or ZD controller-compatible firmware, then the AP controller-compatible firmware 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


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

This chapter provides instructions for configuring Ruckus Wireless APs in a standalone configuration or when the AP is to be managed by a FlexMaster controller. 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, temperature update, service provider login, and other settings. (Some settings are only available on certain Ruckus Wireless models.)

1. Go to Configuration > Device.

Figure 28. 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 this AP among other devices on the network.

3. Configure the following optional settings as desired:
   - Enter Device Location to keep track of the physical location of the AP.
   - If the AP has a GPS antenna, then select the method of entering the GPS coordinates. In Coordinate Source, select GPS to have the GPS antenna automatically determine and enter the GPS coordinates, or select Manual to enter the GPS coordinates manually.
     If you selected Manual, then enter GPS Coordinates to record the physical location of the AP.
   - 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.
   - Enable Internal Heater and PoE OUT Port (specific models only) if needed.
Configuring Device Settings

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

4. 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, enter the new password. 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.

5. Under Login remote authentication, click the **TACACS+ State** box to enable the TACACS+ server interface, if required.

   **NOTE** 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 APs only)
   - **Monitoring Admin** (Monitoring and viewing operation status only)

   If the TACACS+ server state is enabled, then configure the TACACS+ server parameters:
   - **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**: Retype the TACACS+ Password.

6. 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
- Configuring an NTP Server
- Configuring the Management VLAN
- Default IP Addressing Behavior
- Obtaining and Assigning an IP Address
- Configuring L2TP Connection Settings

Figure 29. The Configuration > Internet page
VLAN Settings Overview

A Ruckus Wireless AP is like a network switch, in that it supports 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 an 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 use a different NTP server, you can do so by going to Configuration > Internet, entering the host name in NTP Server at the top of the page, and then clicking Update Settings.

Configuring the Management VLAN

NOTE 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 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** (or **192.168.100.2** for Cable Modem APs) to make it easier for you to configure 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 a Static IP
- PPPoE

**DHCP/Auto Configuration**
If you leave the AP at its default configuration, then 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.

Refer to the following:

- Renewing and Releasing DHCP
- Configuring IPv4 Auto or Manual Configuration
- Configuring IPv6 Auto Configuration

**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 prove to be unusable or in conflict with others, or when the AP loses its DHCP-assigned IP address for some reason.

1. Go to **Status > Internet**.
2  Review the current settings.

3  If the current Connection Type is **dhcp**, then 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 or 192.168.100.2 for Cable Modem APs) and click **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 changes.

### Configuring IPv4 Auto or Manual Configuration

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

1  Go to **Configuration > Internet**.

2  In IPv4 Connection Type, select **DHCP**.

3  In IPv4 DNS Mode, select **Auto** or **Manual**.
   - When you select **Auto**, the AP automatically searches for an IPv4 DNS server.
When you select Manual, also make the following entries:
- **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.

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

**Configuring IPv6 Auto Configuration**

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

1. Go to **Configuration > Internet**.
2. In **IPv6 Connection Type**, select **Auto Configuration**.
3. In **IPv6 Primary DNS Server**, enter the IP address of the primary IPv6 DNS server.
5. Click **Update Settings** to save your changes.

**Configuring a Static IP**

There are at least two instances when you need to configure a static IP address for the AP:
- If the current IP address that the AP is using consistently conflicts with that of another device on the network.
- If you want to switch from DHCP to static IP addressing to manage and maintain the AP.

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

1. Go to **Configuration > Internet**.
2. You can configure static addresses for IPv4, IPv6 or both. The AP maintains both sets of IP address settings if both are configured.
3. In **IPv4 Connection Type** or **IPv6 Connection Type**, select **Static IP**.
4. When the **Internet Connection Settings** options appear, you can make changes to the following settings:
   - (IPv6 only) **IPv6 Primary DNS Server:** The IP address of the primary IPv6 DNS server.
• (IPv6 only) **IPv6 Secondary DNS Server:** The IP address of the secondary IPv6 DNS server.

• **IPv4/IPv6 Address:** Enter the static IP address that you want to assign to the AP in either IPv4 (dot-decimal) or IPv6 (colon-separated) format.

• **IPv4 Subnet Mask or IPv6 Prefix Length:** Enter the subnet mask or prefix length for the network.

• **IPv4/IPv6 Gateway:** Enter the gateway IP address of the Internet interface.

4 (IPv4 only) In **IPv4 DNS Mode**, select **Auto** or **Manual**.

• When you select **Auto**, the AP automatically searches for an IPv4 DNS server.

• When you select **Manual**, also make the following entries:
  - **IPv4 Primary DNS Server:** The IP address of the primary DNS server.
  - **IPv4 Secondary DNS Server:** The IP address of the secondary DNS server.

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

**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 Click **Update Settings** to save your changes.
Configuring L2TP Connection Settings

You can implement transparent bridging with Ruckus Wireless APs by using L2TP (Layer 2 Tunneling Protocol) tunneling. By tunneling traffic from a Ruckus Wireless 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**.

   ![L2TP Connection](image.png)

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

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

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

5. If your network requires PPP authentication, configure the following fields for L2TP/PPP authentication:
   - **PPP/L2TP Username**: Type your PPP user name.
   - **PPP/L2TP 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 seemingly connected to the WLAN but without Internet connectivity.

7 Click **Update Settings** to save your changes.
Configuring Local Subnets

Ruckus Wireless APs can be configured to provide routing/network address translation (NAT) functionality using the Local Subnets feature. When a Local Subnet is enabled, the standalone AP serves as a gateway router that can 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 VLAN and address range which cannot conflict with one another.

1. Go to **Configuration > Local Subnets**. The **Local Subnet 1** through **Local Subnet 4** tabs allow you to configure each of the four subnets independently.

Figure 32. 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 (for example, 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 would generally 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 # (WLAN number) 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.

### 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 2.4GHz and 5GHz radios independently by going to **Configuration > Radio 2.4G** or **Configuration > Radio 5G**.

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

Figure 33. Typical Configuration > Radio 5G > Common page
2 Make changes to the common wireless settings listed in the table below.

Table 24. Common Wireless Settings

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Radio Network</td>
<td>(Dual-radio APs only) Allows you to change the name of the 2.4GHz and 5GHz radios (default: Radio 2.4G and Radio 5G).</td>
</tr>
</tbody>
</table>
| 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 54Mbps (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; that is, for the 2.4GHz radio, the mode is automatically set    |
                           |   to 2.4GHz (802.11b/g/n), while for the 5GHz radio, the mode is automatically set to 5GHz (802.11ac/a/n).                           |
| Channel                  | This option lets you select the channel used by the network. You can choose SmartSelect, or choose a specific channel. If you            |
                           |   choose SmartSelect, then 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 40 MHz channel width theoretically provides double the data capacity of a 20 MHz channel.       |
                           |   However, more channel width means fewer channels available, and more interference with other wireless signals.                     |
                           | On 802.11n APs, the option to choose 80 MHz channel width theoretically provides four times the data capacity of a 20 MHz channel. |
                           |   However, more channel width means fewer channels available, and more interference with other wireless signals.                   |
(Some APs only.) If you are using AeroScout RFID Tags in your organization to locate assets or personnel, then you can use your Ruckus Wireless AP to relay location or presence data from the AeroScout Tags to the AeroScout Engine via Wi-Fi.

To enable the AP to relay AeroScout data, click Enabled in AeroScoutRFID tag detection.

### Table 24. Common Wireless Settings (Continued)

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Country Code</strong></td>
<td>This option (if enabled) lets you select your country or region code.</td>
</tr>
<tr>
<td><strong>CAUTION:</strong></td>
<td>Selecting the incorrect country or region may result in violation of applicable laws.</td>
</tr>
<tr>
<td><strong>Country Code</strong></td>
<td>If you purchased the AP in the United States of America, you do not need to set the country</td>
</tr>
<tr>
<td><strong>code manually.</strong></td>
<td>Ruckus Wireless devices that are sold in the USA are preconfigured with the correct country</td>
</tr>
<tr>
<td><strong>CAUTION:</strong></td>
<td>code and this setting is non-configurable.</td>
</tr>
<tr>
<td><strong>Advanced Settings</strong></td>
<td>Refer to “Reviewing Common Advanced Settings” on page 90.</td>
</tr>
<tr>
<td><strong>External Antenna</strong></td>
<td><strong>NOTE:</strong> This option only appears if you are using a Ruckus Wireless AP with external antenna</td>
</tr>
<tr>
<td><strong>Gain</strong></td>
<td>ports, such as the 7782-E or the T300e AP.</td>
</tr>
<tr>
<td><strong>NOTE:</strong></td>
<td>Some Ruckus Wireless APs provide external antenna port(s), in case you want to attach</td>
</tr>
<tr>
<td><strong>Gain</strong></td>
<td>external antenna(s) to extend the range of your wireless network. To enable the AP to use</td>
</tr>
<tr>
<td><strong>Gain</strong></td>
<td>the external antenna(s), select the Enabled option in this section. This option is</td>
</tr>
<tr>
<td><strong>Gain</strong></td>
<td>disabled by default.</td>
</tr>
<tr>
<td><strong>AeroScout RFID</strong></td>
<td>(Some APs only.) Select Enabled to enable AeroScout RFID tag detection.</td>
</tr>
<tr>
<td><strong>Ekahau RFID</strong></td>
<td>(Some APs only.)</td>
</tr>
<tr>
<td><strong>Ekahau RFID</strong></td>
<td>• Select Enabled to enable Ekahau RFID tag detection.</td>
</tr>
<tr>
<td><strong>Ekahau RFID</strong></td>
<td>• Enter the Ekahau ERC IP address.</td>
</tr>
<tr>
<td><strong>Ekahau RFID</strong></td>
<td>• Enter the Ekahau ERC port.</td>
</tr>
</tbody>
</table>

3 (Some APs only.)
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 Current Wireless Settings” on page 123 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, you can enable AeroScout RFID tag detection on all its managed APs at once. Refer to the ZoneDirector online help for note-text-bullet

4  (Some APs only.) If you are using an Ekahau Real Time Location System (RTLS) in your organization, then you can use your Ruckus Wireless AP to relay location or presence data to the Ekahau Real Time Location System RTLS Controller (ERC).

- To enable the AP to relay Ekahau data, click **Enabled in Ekahau Settings**.
- If you have enabled Ekahau, then complete the following:
  - **ERC IP Address**: Enter an IP address for the Ekahau Real Time Location System RTLS Controller.
  - **ERC port**: 65538 is the default, but it can be set to any available TCP port used by the Ekahau Real Time Location System RTLS Controller.

**NOTE**  For other Ekahau-related configuration, refer to the Ekahau documentation that was shipped with your Ekahau Real Time Location System RTLS Controller.

5  Click **Update Settings** to save your changes.
Reviewing 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 be retained for best performance.

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


Figure 34. The Configuration > Wireless > Advanced > Common page

2. Configure the advanced settings listed in Table 25 as required.

Table 25. Advanced wireless common settings

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Transmit Power</td>
<td>The default setting is <strong>Full</strong>. 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).</td>
</tr>
<tr>
<td>5.8 GHz Channels</td>
<td>(Only available in certain countries selected using the <em>Country Code</em> option.) Select <strong>Enable</strong> to activate the optional 5.8GHz channels (disabled by default).</td>
</tr>
</tbody>
</table>
Configuring Wireless Settings

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 wireless clients, traffic types, or user groups. Each WLAN can be configured with separate security settings, VLANs, access controls and rate limiting policies, among other settings.


2. Click one of the eight Wireless # (WLAN number) tabs. The selected Configuration > Wireless > Wireless # (WLAN number) page appears.

Table 25. Advanced wireless common settings (Continued)

<table>
<thead>
<tr>
<th>Protection Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>(Disabled by default.) When 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.</td>
</tr>
<tr>
<td><strong>WARNING:</strong> Activating this option (and configuring the settings) boosts the interoperability of 802.11b and 802.11g/11n devices but severely decreases performance.</td>
</tr>
<tr>
<td>• <strong>CTS-only:</strong> 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.</td>
</tr>
<tr>
<td>• <strong>RTS-CTS:</strong> Choose this option to force both sending and receiving devices to confirm a data exchange on both ends before proceeding.</td>
</tr>
</tbody>
</table>

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

#### Configuring Wireless # (WLAN Number) Settings

Review the WLAN options listed in Table 26, and then make changes as required.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wireless Network</td>
<td>This wireless network name is only used for management, and is not visible to wireless clients.</td>
</tr>
<tr>
<td>Wireless Availability</td>
<td>This option controls whether or not the wireless network is available to users (Enabled or Disabled).</td>
</tr>
<tr>
<td>Broadcast SSID</td>
<td>This option controls whether or not (Enabled or Disabled) the WLAN SSID is visible to anyone looking for wireless networks. Disabling (hiding) the SSID requires the user to use the correct SSID before they can connect to your network.</td>
</tr>
<tr>
<td>SSID</td>
<td>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).</td>
</tr>
</tbody>
</table>
### Configuring Wireless Settings

#### Configuring Wireless # (WLAN Number) Settings

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Threshold Settings</strong></td>
<td>This button opens a page where you can configure the Protection Mode you activated on the <code>Configuration &gt; Wireless &gt; Advanced &gt; Wireless # (WLAN number)</code> page. If Protection Mode is not active, ignore this option. For more information, see “Setting Threshold Options” on page 101.</td>
</tr>
<tr>
<td><strong>Rate Limiting</strong></td>
<td>This button opens a page where you can configure upload and download limits per station. For more information, see “Rate Limiting” on page 102.</td>
</tr>
<tr>
<td><strong>Access Control</strong></td>
<td>This button opens a page where you can configure access controls for the WLAN. For more information, see “Controlling Access to the Wireless Network” on page 103.</td>
</tr>
</tbody>
</table>
| **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. |
| **Hotspot Service**      | Select a Hotspot configuration from the list to enable Hotspot service on this WLAN, after you have configured it from the `Configuration > Hotspot` page. Refer to “Configuring Hotspot Service” on page 112. |
| **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. |
When you are finished, click Update Settings to save and apply the changes. A confirmation message appears at the top of this page.

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.
NOTE  WEP encryption has been proven to be easily circumvented. Therefore, Ruckus Wireless recommends using WPA whenever possible, and only use WEP if your client devices do not support WPA.

NOTE  Using WEP encryption limits the performance of this WLAN to 802.11g rates, and other WLANs are unaffected. 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.

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

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

Figure 36.  WEP settings

3  In the Encryption Method menu, select WEP. An additional set of WEP-specific encryption options appears.

4  Review the encryption settings listed in Table 27, and then make changes as required.
Configuring Wireless Settings

Configuring Wireless # (WLAN Number) Settings

Click Update Settings to save and apply the changes. A confirmation message appears at the top of the 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), see “Customizing 802.1X Settings” on page 99.

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.

Table 27. WEP Options

<table>
<thead>
<tr>
<th>Encryption Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authentication Mode</td>
<td>Open is the only authentication mode available with WEP encryption.</td>
</tr>
</tbody>
</table>
| 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.
When 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/Radio 2.4/Radio 5G**. The **Configuration > Wireless > Common** page appears.

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

![Figure 37. WPA settings](image)

3. Click the **Encryption Method** menu, and select **WPA**. An additional set of WPA-specific options appear.

4. Review the encryption settings listed in **Table 28**, and then make changes as required.
### Configuring Wireless Settings

**Configuring Wireless # (WLAN Number) Settings**

**ZoneFlex Outdoor Access Point 100.0.0 User Guide, 800-70725-001 Rev B**

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

---

#### Table 28. Encryption settings

<table>
<thead>
<tr>
<th>Encryption Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>WPA Version</td>
<td><strong>WPA2</strong> provides stronger wireless security than WPA (Wi-Fi Protected Access) 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. <strong>WPA-WPA2</strong> allows both WPA and WPA2 devices to operate on the same WLAN.</td>
</tr>
<tr>
<td>WPA Authentication</td>
<td><strong>PSK</strong> (Pre-Shared Key) mode is suitable for home or personal use. <strong>802.1x</strong> mode uses a RADIUS server to verify user identity. <strong>Auto</strong> mode offers both options to the wireless client. For more information on how to configure the 802.1X mode, refer to “Customizing 802.1X Settings” on page 99.</td>
</tr>
<tr>
<td>WPA Algorithm</td>
<td><strong>AES</strong> (Advanced Encryption Standard) replaces TKIP (Temporal Key Integrity Protocol) as the default (and recommended) encryption algorithm for modern wireless LANs. 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. <strong>Auto (TKIP+AES)</strong>: 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.</td>
</tr>
<tr>
<td>Passphrase</td>
<td>Enter a new passphrase between 8 and 32 characters long, using any combination of printable characters (letters, numbers, hyphens and underscores).</td>
</tr>
</tbody>
</table>
Customizing 802.1X Settings

NOTE 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, then you have the option to set up the AP to act as an 802.1X proxy, using 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.


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

Figure 38. 802.1X settings
3. In the **Encryption Method** menu, select **WPA**. The basic set of WPA-specific encryption options appears on the page.

4. In **WPA Authentication** select the required WPA authentication type:
   - **WPA2** provides stronger wireless security than **WPA** (Wi-Fi Protected Access) 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-WPA2** allows both WPA and WPA2 devices to operate on the same WLAN.

5. Select **802.1x** as the **WPA Authentication** mode. Additional options appear.

6. In **WPA Algorithm** select one of the following:
   - **AES**: AES (Advanced Encryption Standard) replaces TKIP (Temporal Key Integrity Protocol) as the default (and recommended) encryption algorithm for modern wireless LANs.
   - **Auto (TKIP+AES)**: 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.

7. 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 (required)**: Enter the information needed to establish a connection between the AP and the RADIUS server.
   - **Accounting Server (optional)**: Enter the information needed to establish this connection.

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

NOTE  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/Radio 2.4G/Radio 5G. The Configuration > Wireless > Common page appears.

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

3  Look for Threshold Settings, and then click Edit Settings. The Configuration > Wireless > Advanced > Wireless # (WLAN number) page appears.

Figure 39.  Threshold settings
4 Review the options listed in Table 29, and then make any needed changes.

Table 29. Threshold options

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Beacon Interval</td>
<td>(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.</td>
</tr>
<tr>
<td>Data Beacon Rate (DTIM)</td>
<td>(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.</td>
</tr>
<tr>
<td>RTS/CTS Threshold</td>
<td>(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.</td>
</tr>
</tbody>
</table>

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 per-client data transfer rates for a specific WLAN.

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

2 Select the WLAN 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.

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

   The table below your selections updates to show the maximum transfer rate per station for each traffic type.

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

You have completed configuring the rate limiting options. To reopen the previous page, click the **Go back to Wireless Configuration** link.
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 # (WLAN number) tab.

Access Control List (ACL) Options
This section describes the options that you can use to control access to the wireless network.

- **Disable WLAN access restrictions:** The MAC-address-based restrictions on which stations can join the WLAN are disabled, so any station can join. If the WLAN uses encryption, then the station must still supply the correct encryption passphrase. When this option is selected, the Access Controls table is hidden.

- **Allow only stations listed in the Access Control Table:** Only stations entered into the access-controls table are allowed, but all others are disallowed. To add MAC addresses, see “Changing Access Controls for a WLAN” on page 104.

- **Deny only stations listed in the Access Control Table:** Stations entered into the access-controls table are disallowed but all others are allowed. To add MAC addresses, see “Changing Access Controls for a WLAN” on page 104.
Changing 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/Radio 2.4G/Radio 5G.
2. Click the Wireless # (WLAN number) tab for which you want to configure the access control settings.
3. Click the Edit Settings button next to Access Control.
4. Select the radio button for the desired access control. (For a description of the options, refer to “Access Control List (ACL) Options.”) The Access Controls Table appears.

Figure 41. Access control settings

5. To add a MAC address to the Access Control table, click the Add new entry button.
6. Fill out the Address text boxes: 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.
8 If you have additional MAC addresses you want included, then 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 in 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 individually configure VLAN settings for each port from this page.

1. Go to Configuration > Ethernet Ports.

Figure 42. The Configuration > Ethernet Ports page

2. Review the following table and make changes as needed for each of the ports labeled PORT 1 through PORT 4 (depending on AP model), which correspond to the AP’s Ethernet ports.

Table 30. Individual Ethernet port options

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable</td>
<td>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.</td>
</tr>
<tr>
<td>Port Type</td>
<td>See “Setting Ethernet Port Type” on page 109 for more detailed information.</td>
</tr>
<tr>
<td></td>
<td>• Trunk Port: This port passes all VLAN traffic.</td>
</tr>
<tr>
<td></td>
<td>• Access Port: This port provides network access.</td>
</tr>
<tr>
<td></td>
<td>• General Port: User-defined VLAN membership.</td>
</tr>
</tbody>
</table>
### Configuring Ethernet Ports

#### Configuring Wireless # (WLAN Number) Settings

**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.

**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 110 for more information.

Enable MAC authentication bypass: Mark to enable or clear to disable. Only available if 802.1X is enabled.

**Local Subnet**
This option appears if you have selected *Local Subnet NAT and Route to WAN* under *Packet Forward*, 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>
<thead>
<tr>
<th>Packet Forward</th>
<th>Isolated: Selecting <em>Isolated</em> causes the traffic from this port to terminate at the AP.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><strong>Bridge to WAN</strong>: The default setting, <em>Bridge to WAN</em> forwards packets arriving on this port to the WAN (uplink) port and eventually to their external destinations using Layer 2 forwarding.</td>
</tr>
<tr>
<td></td>
<td><strong>Local Subnet NAT and Route to WAN</strong>: This setting allows routing of packets to their destinations using Layer 3 network address translation (NAT).</td>
</tr>
<tr>
<td></td>
<td><strong>Bridge to L2TP Tunnel</strong>: Uses Layer 2 Tunneling Protocol to deliver packets encapsulated with an L2TP header in UDP datagrams.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>802.1X</th>
<th>Configure the port as an 802.1X authenticator or supplicant. The following options are available:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><strong>Disabled</strong>: No 802.1X controls are applied to this port.</td>
</tr>
<tr>
<td></td>
<td><strong>Authenticator (Port-Based)</strong>: Only one of the attached MAC hosts must be authorized for all hosts to be granted access to the network.</td>
</tr>
<tr>
<td></td>
<td><strong>Authenticator (MAC-Based)</strong>: Each MAC host is individually authenticated.</td>
</tr>
<tr>
<td></td>
<td><strong>Supplicant</strong>: 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.</td>
</tr>
</tbody>
</table>

See “Working with 802.1X on Wired Ethernet Ports” on page 110 for more information.

Enable MAC authentication bypass: Mark to enable or clear to disable. Only available if 802.1X is enabled.

| Local Subnet  | This option appears if you have selected *Local Subnet NAT and Route to WAN* under *Packet Forward*, 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. |
Review the following table and make changes as needed for all of the Ethernet ports.

Table 31. All Ethernet port options

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authentication Server (required)</td>
<td>Enter the authentication server IP address, port, and server secret for all Ethernet ports. Only available if 802.1X Authenticator are enabled (includes any packet forward selection).</td>
</tr>
</tbody>
</table>
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 the *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 and filtering 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.

---

**Table 31. All Ethernet port options (Continued)**

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accounting Server (optional)</td>
<td>Enter the accounting server IP address, port, and server secret for all Ethernet ports. Only available if 802.1X Authenticator are enabled.</td>
</tr>
<tr>
<td>Supplicant User Name and</td>
<td>Enter the 802.1X supplicant user name and password for all Ethernet ports. Only available if 802.1X Trunk port and Supplicant are enabled.</td>
</tr>
<tr>
<td>Supplicant Password</td>
<td></td>
</tr>
</tbody>
</table>

4. Click **Update Settings** to save your changes.
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 # (WLAN number) > 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 32 and Table 33 describe the 802.1X roles available by port type.

Table 32. Authenticator support by port type

<table>
<thead>
<tr>
<th></th>
<th>Trunk Port</th>
<th>Access Port</th>
<th>General Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port-based mode</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>MAC-based mode</td>
<td>X</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Table 33. Supplicant support by port type

<table>
<thead>
<tr>
<th></th>
<th>Trunk Port</th>
<th>Access Port</th>
<th>General Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>Supplicant</td>
<td>X</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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 tries to authenticate the device using 802.1X.
Configuring Hotspot Service

Hotspot service can be deployed on standalone Ruckus Wireless 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 43. Minimum configuration settings for providing Hotspot service

2. Click Enabled next to Hotspot Service.

3. Review the settings in Table 34, and make changes as needed.

Table 34. Hotspot configuration settings

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Redirect unauth. user to</td>
<td>Redirect unauthenticated users to the specified URL (login page).</td>
</tr>
</tbody>
</table>
Configuring Hotspot Service

Customizing Hotspot Optional Settings

Table 34. Hotspot configuration settings (Continued)

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>After user is authenticated</td>
<td>Select where you want to redirect the user after successful authentication.</td>
</tr>
<tr>
<td></td>
<td>• Redirect to the above URL: Return to the login URL configured above.</td>
</tr>
<tr>
<td></td>
<td>• 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).</td>
</tr>
<tr>
<td></td>
<td>• 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.</td>
</tr>
<tr>
<td>Primary RADIUS Server</td>
<td>Enter the IP address of the primary RADIUS server against which users are authenticated (required).</td>
</tr>
<tr>
<td>Secondary RADIUS Server</td>
<td>Enter the IP address of the secondary RADIUS server, if one is available (optional).</td>
</tr>
<tr>
<td>RADIUS Server Secret</td>
<td>Enter the shared secret for communication with the RADIUS server (required).</td>
</tr>
</tbody>
</table>

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 at the bottom of the page.

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, and so on.

1 Go to **Configuration > Hotspot**.

2 Click **More Options/Edit Settings**.
3 Configure these Hotspot options from the Configuration > Hotspot > More Options page:

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Temporarily block user after ___ unsuccessful logins</td>
<td>Specify the maximum number of repeated authentication failures allowed.</td>
</tr>
<tr>
<td>Redirect temp. blocked user to</td>
<td>Enter a redirect URL to which blocked users are redirected.</td>
</tr>
<tr>
<td>MAC Authentication</td>
<td>When 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.</td>
</tr>
</tbody>
</table>
Table 35. Optional Hotspot settings (Continued)

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Acct Delay Time</td>
<td>Accounting delay <strong>Enabled</strong> or <strong>Disabled</strong>. 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.</td>
</tr>
<tr>
<td>NAS ID</td>
<td>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.</td>
</tr>
<tr>
<td>WISPr Location ID</td>
<td>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=&lt;ISO_Country_Code&gt;, cc=&lt;E.164_Country_Code&gt;, ac=&lt;E.164_Area_Code&gt;, network=&lt;SSID/ZONE&gt;”.</td>
</tr>
<tr>
<td>WISPr Location Name</td>
<td>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 “&lt;HOTSPOT_OPERATOR_NAME&gt;, &lt;Location&gt;”.</td>
</tr>
<tr>
<td>Location Description</td>
<td>Specify the description of location. This value is provided in the HTTP redirection.</td>
</tr>
<tr>
<td>Accounting Update Interval</td>
<td>Specify the interval for RADIUS accounting requests.</td>
</tr>
<tr>
<td>Interim Redirect Interval</td>
<td>Specify the interval after which users are redirected to the login URL.</td>
</tr>
<tr>
<td>Maximum Session Time</td>
<td>Enter the maximum session time in minutes.</td>
</tr>
<tr>
<td>Grace Period</td>
<td>Specify the maximum time that a user may disconnect from the Hotspot service and return without the need to login again.</td>
</tr>
</tbody>
</table>
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 may not be able to click through to other URLs 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.

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

### 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 may not be able to click through to other URLs 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.

1 Go to **Configuration > Hotspot**.

2 Click **Walled Garden/Edit Settings**.

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

<table>
<thead>
<tr>
<th><strong>Table 35. Optional Hotspot settings (Continued)</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>RADIUS Disconnect Port</strong></td>
</tr>
<tr>
<td><strong>Swap Input and Output Counters</strong></td>
</tr>
<tr>
<td><strong>Encode User Password</strong></td>
</tr>
<tr>
<td><strong>UAM Shared Secret</strong></td>
</tr>
</tbody>
</table>
4 In *Walled Garden Host*, enter a host name, IP address, network segment (for example, 192.168.1.0/24) or a domain name. If a domain name is entered, it is resolved every five 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 Hotspot Access by MAC Address

1. Go to Configuration > Hotspot.
2. Click Unrestricted Clients/Edit Settings.
3. Click Add new entry, and enter the MAC address of a client in the fields provided.
4. Click Update to save your changes.
Managing the Access Point

In this chapter:

- Viewing Current Device Settings
- Viewing Current Internet Connection Settings
- Viewing Current Local Subnet Settings
- Viewing Current Wireless Settings
- Viewing Associated Wireless Clients
- Viewing Current Wireless Settings
- Viewing Associated Wireless Clients
- Changing the Administrative Login Settings
- Enabling Other Management Access Options
- Working with Event Logs and Syslog Servers
- Upgrading the Firmware
- Rebooting the AP and Cable Modem
- Resetting the AP to Factory Defaults
- Running Diagnostics
- Where to Find More Information

This chapter provides instructions for managing standalone Ruckus Wireless APs using the Web interface. For information on managing your Ruckus Wireless network using ZoneDirector, refer to the *ZoneDirector User Guide*, available from the Ruckus Wireless website.
Viewing Current Device Settings

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

Figure 47. The Status > Device page
Viewing Current Internet Connection Settings

The Status > Internet page displays information on the AP’s network settings; that is, 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 48. 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, then go to Configuration > Local Subnets. Refer to “Configuring Local Subnets” on page 84 for more information.

Figure 49. The Status > Local Subnet page
Viewing Current 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 > Radio 2.4G or Status > Radio 5G).

Figure 50. The Status > Wireless (Radio 2.4G/5G) Common page

Table 36 lists the descriptions of each wireless setting.

Table 36. Common Wireless settings

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wireless Mode</td>
<td>Shows the wireless mode that the AP is currently using. Possible values include:</td>
</tr>
<tr>
<td></td>
<td>- 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.</td>
</tr>
<tr>
<td></td>
<td>- 2.4GHz 54 Mbps: Allows 11g devices only.</td>
</tr>
<tr>
<td></td>
<td>- 2.4GHz 11 Mbps: Allows 11b devices only.</td>
</tr>
<tr>
<td></td>
<td>- 11ng: Operates with 802.11n, 802.11g and 802.11b devices in the 2.4GHz spectrum only.</td>
</tr>
<tr>
<td></td>
<td>- 11na: Operates with 802.11n and 802.11a devices in the 5GHz spectrum only.</td>
</tr>
</tbody>
</table>
If you want to make changes to any of these settings, go to the Configuration > Wireless/Radio 2.4G/Radio 5G page. Refer to “Configuring Common Wireless Settings” on page 86 for more information.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Channel</td>
<td>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].</td>
</tr>
<tr>
<td>Channel Width</td>
<td>11n devices only. Displays whether the channel width is set to 20MHz or 40MHz.</td>
</tr>
<tr>
<td>Country Code</td>
<td>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.</td>
</tr>
<tr>
<td>AeroScout RFID tag detection</td>
<td>(Some APs only.) Shows Enabled if you enabled AeroScout RFID tag detection. The default setting is Disabled.</td>
</tr>
<tr>
<td>AeroScout Engine communication daemon</td>
<td>(Some APs only.) 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.</td>
</tr>
<tr>
<td>Ekahau Engine communication daemon</td>
<td>(Some APs only.) Shows Enabled if you enabled Ekahau RFID tag detection. The default setting is Disabled.</td>
</tr>
<tr>
<td>ERC IP</td>
<td>(Some APs only.) Ekahau Real Time Location System RTLS Controller IP address.</td>
</tr>
<tr>
<td>ERC Port</td>
<td>(Some APs only.) TCP port used by the Ekahau Real Time Location System RTLS Controller.</td>
</tr>
</tbody>
</table>
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.


   NOTE   If you are using a dual-band Ruckus Wireless AP, go to Status > Radio 2.4G or Status > Radio 5G.

2. Click any of the Wireless # (WLAN number) tabs. Wireless clients that are associated with this particular wireless LAN appear under Connected Devices.

Figure 51. 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 into 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 52. The Configuration > Device page

3. Under Service Provider Login, change the default administrator login settings:
   - In Username, type a new user name that you will use to log in to the Web interface. The default user name is super.
   - When you are changing a password, type the existing password in Current Password.
   - In New Password, type a new password to replace the existing password. 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 using HTTPS, several other management access options are available on the AP. These options include management access using 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, then 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 131.

1. Go to Administration > Management.

Figure 53. The Administration > Management page
2. Review the access options listed in Table 37, and then make changes as needed.

Table 37. Management Access Options

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Telnet Access</td>
<td>By default, this option is disabled (inactive).</td>
</tr>
<tr>
<td>Telnet Port</td>
<td>This field lists the default Telnet port of 23 — only if Telnet is active.</td>
</tr>
<tr>
<td></td>
<td>You can manually change this port number, if required.</td>
</tr>
<tr>
<td>SSH Access</td>
<td>By default, this option is enabled (active).</td>
</tr>
<tr>
<td>SSH Port</td>
<td>This field lists the default SSH port of 22 — only if SSH is active.</td>
</tr>
<tr>
<td></td>
<td>You can manually change this port number if required.</td>
</tr>
<tr>
<td>HTTP Access</td>
<td>This option is disabled by default.</td>
</tr>
<tr>
<td>HTTP Port</td>
<td>This field lists the default HTTP port of 80, if HTTP has been activated.</td>
</tr>
<tr>
<td></td>
<td>You can manually change this port number if required.</td>
</tr>
<tr>
<td>HTTPS Access</td>
<td>By default this option is enabled. This connection mode requires a security certificate, a copy of which has been pre-installed in the device.</td>
</tr>
<tr>
<td>HTTPS Port</td>
<td>This field lists the default HTTPS port of 443 — only if HTTPS has been activated. You can manually change this port number if required.</td>
</tr>
<tr>
<td>Certificate Verification</td>
<td>This notes whether the security certificate linked to the HTTPS settings has been verified (PASSED) or not.</td>
</tr>
<tr>
<td>Controller Discovery Agent (LWAPP)</td>
<td>• Enabled (default) -- Lightweight Access Point Protocol controller discovery on. (Refer to Release Notes for details.)</td>
</tr>
<tr>
<td></td>
<td>• Disabled -- LWAPP controller discovery off.</td>
</tr>
<tr>
<td>Cloud Discovery Agent (FQDN)</td>
<td>• Enabled (default) -- Fully Qualified Domain Name cloud discovery on; requires enabled LWAPP controller discovery Enabled. (Refer to Release Notes for details.)</td>
</tr>
<tr>
<td></td>
<td>• Disabled -- FQDN cloud discovery off.</td>
</tr>
<tr>
<td>Set Controller Address</td>
<td>• 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.</td>
</tr>
<tr>
<td></td>
<td>• Disabled (default) -- The AP does not use IP address(es) to search for SCG, vSCG, SZ or ZD controllers.</td>
</tr>
</tbody>
</table>
Enabling Other Management Access Options

If you want to use TR-069 or SNMP to manage the AP, then configure the settings listed in Table 38.

Table 38. TR-069 and SNMP Management Options

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Auto-provisioning</td>
<td>This setting is disabled by default, and should only be enabled if using a FlexMaster server for AP management.</td>
</tr>
<tr>
<td>Start Recovery SSID after ___ seconds of connectivity loss</td>
<td>When connectivity is lost for this time, the recovery process is invoked. Default is 300 seconds. Enter 0 to disable this function. (Only available on selected APs.)</td>
</tr>
<tr>
<td>Continue service WLANs when in recovery mode</td>
<td>When the recovery process is invoked, the WLAN service is continued (Enabled) or halted (Disabled). (Only available on selected APs.)</td>
</tr>
<tr>
<td>Auto</td>
<td>(Default) Enables the Ruckus Wireless device to be managed by either SNMP servers, Ruckus Wireless controllers, or Ruckus Wireless FlexMaster. (Refer to Release Notes for details.)</td>
</tr>
<tr>
<td>SNMP only</td>
<td>Only allow SNMP management.</td>
</tr>
<tr>
<td>FlexMaster only</td>
<td>Only allow FlexMaster management.</td>
</tr>
<tr>
<td>None</td>
<td>Do not allow SCG, vSCG, SZ or ZD control or FlexMaster management.</td>
</tr>
<tr>
<td>DHCP Discovery</td>
<td>URL of server providing DHCP.</td>
</tr>
<tr>
<td>FlexMaster Server URL</td>
<td>URL of the FlexMaster server.</td>
</tr>
<tr>
<td>Digest-Authentication Username/Digest-Authentication Password</td>
<td>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).</td>
</tr>
<tr>
<td>Periodic FlexMaster Inform Interval</td>
<td>Interval at which the device should attempt to contact FlexMaster. (Default = 15 minutes.)</td>
</tr>
</tbody>
</table>

3 If you want to use TR-069 or SNMP to manage the AP, then configure the settings listed in Table 38.

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. (Refer to Release Notes for details.)
Viewing FlexMaster Management Status

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

Figure 54. TR-069 status information

Table 39 lists the TR-069 status information that the AP provides.

<table>
<thead>
<tr>
<th>Status Information</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Currently Using URL</td>
<td>Shows the FlexMaster server IP address or URL with which the AP is currently registered.</td>
</tr>
<tr>
<td>Last Attempted Contact</td>
<td>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.</td>
</tr>
<tr>
<td>Last Successful Contact</td>
<td>Shows the date and time of the AP's last successful contact with FlexMaster.</td>
</tr>
<tr>
<td>Last Contact Result</td>
<td>Shows the result of the last attempt to contact FlexMaster (success or failure, and failure error code if applicable).</td>
</tr>
</tbody>
</table>
Enabling Other Management Access Options

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. You need TCP ports 80 and 443 open between APs and FlexMaster when traversing Layer 3/firewall boundaries.

1. Go to Administration > Management.
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 shows the communication status between the AP and FlexMaster.

Table 39. TR-069 status information (Continued)

<table>
<thead>
<tr>
<th>Status Information</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Current Time</td>
<td>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.</td>
</tr>
</tbody>
</table>
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 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

If you have a syslog server on the network, you can configure the AP to send the device logs to the server. 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.

2. In Log Status, 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:

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

2. To upload a copy of the support info file to an FTP or TFTP server, click the Transfer Method TFTP or FTP option.
3. In Server Address, enter the FTP or TFTP server IP address.
4. In Filename, enter a name for the 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.”

5. If you selected the FTP option, then also enter a Username and Password.
6. Click Upload Now.

Saving a Copy of the Log File to Your Computer

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

2. Click the Transfer Method Save to Local Computer option. Up to three links appear next to Download (supportinfo.txt, cmssupportinfo.txt and/or tr069info.txt).
3. Click the supportinfo.txt link. A new window (or tab) opens with the content of the log file displayed.
4. Choose Save As or Save Page As from your browser’s File menu.
5. 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.
6. Click Save to save the log file to your computer.
Saving a Copy of a Support File to Your Computer

You can save a copy of the support file(s) to your own computer, if needed. The `cmsupportinfo.txt` file includes support information for an AP with integral cable modem (such as 7781CM), and the `tr069info.txt` file includes support information for an AP being managed by FlexMaster.

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

2. Click the **Transfer Method Save to Local Computer** option. Up to three links appear next to **Download** (`supportinfo.txt`, `cmsupportinfo.txt` and/or `tr069info.txt`).

3. Click the `cmsupportinfo.txt` or `tr069info.txt` link. A new window (or tab) opens with the content of the support file displayed.

4. Choose **Save As** or **Save Page As** from your browser’s **File** menu.

5. 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`.

6. Click **Save** to save the support file to your computer.
Upgrading the Firmware

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

Before starting, decide which option you want to take:

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

By default, the automatic upgrade option is disabled.

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

Figure 56. The Maintenance > Upgrade page

Upgrading Manually via FTP or TFTP

1. In the Upgrade Method options, click FTP (default) 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://.
Upgrading the Firmware
Upgrading Manually via the Web

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, type the URL of the download Web site in Url. 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 a firmware file on your local computer, you can upgrade directly using the Web interface.
1 In the Upgrade Method, select Local.
2 Click Choose File and locate the file on your local computer.
3 Select the file and click Open.
4 Click Perform Upgrade. Status messages appear during the upgrade and reboot process.

Scheduling Automatic Upgrades
1 In the Upgrade Method options, click the button for your preferred choice.
2 Enter the appropriate information in the Host name or IP address field.

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

3 Verify that the Auto Upgrade option is set to Enabled.
4 Toggle the Interval to Check for Software Upgrade drop-down list to select your preferred interval.
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.

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 effective interval.

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

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

You can use the Web interface to prompt the AP to reboot, which restarts the AP without changing any of the current settings. If your AP is equipped with an integral Cable Modem (such as a 7781CM), then you can use the AP Web interface to prompt the CM to reboot, which restarts the CM without changing any of the current settings.

Please note that rebooting the AP or CM disrupts network communications in any currently active WLANs.

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

2 To reboot the AP, click Reboot AP with current settings/Reboot Now. After a brief pause, you are logged out of the AP.

3 To reboot the CM, click Reboot Cable Modem/Reboot Now. After a brief pause, you are logged out of the AP.

Figure 57. 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.

NOTE The 7781CM AP with integral cable modem can also be remotely reset using the OID and CLI commands described in the ZoneFlex 7781CM Installation Guides.
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 “2. Logging Into the Ruckus Wireless AP Web Interface” on page 69.

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 that this disrupts all wireless network communications through this device.

2. Click Reset now (next to Reset the AP 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 the associated AP Installation Guide. 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 you wish to connect to.

3. Click Run test.

The results appear in the text field below each option.

Figure 58. Pinging an IP address
Figure 59. Running traceroute on ruckuswireless.com
Where to Find More Information

If you have questions that this User Guide does not address, visit the Ruckus Wireless Support Portal at http://support.ruckuswireless.com. The Support Portal hosts the latest versions of user documentation. You can also find answers to frequently asked questions (FAQs) for each Ruckus Wireless product type.
Appendix: Zone 2 APs

Some Ruckus Wireless access points can be purchased with the country code factory configured and locked to a regulatory region referred to as “Zone 2”. AP ordering numbers with a “Z2” in the suffix, for example 901-R700-Z200, have been factory locked to the Zone 2 country code setting. End users of these access points are not able to change the country code setting, operate the AP on non-Z2 channels, or use non-Z2 transmit power limits.

APs discover and join Ruckus Wireless controllers with matching “Zone 2” or “Z2” country code settings.

APs with locked Z2 country code settings comply with the Zone 2 regulatory limits outlined in Table 40.

Table 40. Zone 2 Regulatory Information

<table>
<thead>
<tr>
<th>SKU suffix</th>
<th>Locked</th>
<th>Country</th>
<th>Country Code</th>
<th>2.4 GHz CH 1-13 and RF Power Limit</th>
<th>5.150 GHz-5.250 GHz (W52) RF Power Limit</th>
<th>5.250 GHz-5.350 GHz CH (W53) and RF Power Limit</th>
</tr>
</thead>
<tbody>
<tr>
<td>-WWxx</td>
<td>Unlocked</td>
<td>Algeria</td>
<td>DZ</td>
<td>1-13/100mW (outdoor limited to 28mW)</td>
<td>200mW</td>
<td>Indoor: 200mW Outdoor: 1000mW</td>
</tr>
<tr>
<td>-WWxx</td>
<td>Unlocked</td>
<td>Morocco</td>
<td>MA</td>
<td>1-13/100mW</td>
<td>200mW</td>
<td>200mW</td>
</tr>
<tr>
<td>-WWxx</td>
<td>Unlocked</td>
<td>Tunisia</td>
<td>TN</td>
<td>1-13/100mW</td>
<td>200mW</td>
<td>200mW</td>
</tr>
<tr>
<td>-WWxx</td>
<td>Unlocked</td>
<td>Vietnam</td>
<td>VN</td>
<td>1-13/100mW</td>
<td>200mW</td>
<td>200mW</td>
</tr>
<tr>
<td>-WWxx</td>
<td>Unlocked</td>
<td>Israel</td>
<td>IL</td>
<td>1-13/100mW</td>
<td>200mW</td>
<td>200mW</td>
</tr>
<tr>
<td>-ILxx (Note)</td>
<td>Locked</td>
<td>Israel</td>
<td>IL</td>
<td>1-13/100mW</td>
<td>200mW</td>
<td>200mW</td>
</tr>
<tr>
<td>-Z2xx</td>
<td>Locked</td>
<td>Zone 2</td>
<td>Z2</td>
<td>1-13/100mW</td>
<td>200mW</td>
<td>200mW</td>
</tr>
</tbody>
</table>

Note: -ILxx is not used for new designs.
Index

Numerics
7762 ZoneFlex AP 20
7762-AC ZoneFlex AP 23
7762-S ZoneFlex AP 26
7762-S-AC ZoneFlex AP 29
7762-T ZoneFlex AP 32
7781CM ZoneFlex AP 35
7782 ZoneFlex AP 41
7782-E ZoneFlex AP 44
7782-N ZoneFlex AP 47
7782-S ZoneFlex AP 50
802.11ac AP
  T300 53, 56
  T301n 60
  T301s 63
802.1Q 77
802.1X 107, 110
configuration 99
rate limiting 102
WPA authentication 98
802.3af
  PoE out port 21, 24, 27, 30, 33, 42, 48, 51

A
access control 103, 104
table of contents
access control list options 103
access port 106
definition 109
access VLAN 93
ACL options 103
administrative login 126
advanced settings, wireless 88
AeroScout 88
AES WPA algorithm 98, 100
algorithm
WPA AES 98, 100
WPA auto (TKIP+AES) 98, 100
AP
  Preconfiguring Firmware 67
  Zone 2/22 144
AP factory defaults, resetting 140
AP, installing 13
associated clients 125
authenticated users login redirect URL 113
authentication
  WPA 802.1X 98
  WPA auto 98
  WPA PSK 98
  auto (TKIP+AES) WPA algorithm 98, 100
  auto WPA authentication 98
B
basic settings, Hotspot 112
beacon interval 102
BeamFlex 12
Bridge to L2TP Tunnel 93, 107
Bridge to WAN 93, 107
bridging, local 107
broadcast SSID 92
C
changing the login settings 74
channel
  width 87
  wireless 87
client fingerprinting 94
configuring WLANs 91
country code 124
controller
  Smart Access Management service (SAMS) 12
  SmartCell Gateway (SCG) 12
  SmartZone (SZ) 12
  virtual SmartCell Gateway (vSCG) 12
CTS-only protection mode 91
D
data beacon rate 102
default IP address 78
default user name and password 70
delivery traffic indication message 102
device
  location 74
  name 74
  settings 74
DHCP
  release 78, 79, 80
  renew 78, 79, 80
DHCP (auto) connection type 78
DHCP Option 82 94, 108
diagnostics 141
DTIM 102
dynamic VLAN 94

E
Ekahau 88
enable/disable individual ethernet port 106
encryption 94
ethernet individual port types 106
ethernet port
  configuration 106
  enable/disable 106
  ethernet port types 106, 109
  external antenna 88
  external antenna gain 88

F
factory defaults, resetting AP 140
firmware upgrade 136
FlexMaster 69
FlexMaster (FM) manager 12
FlexMaster management status 131
FlexMaster server URL 129
FM manager 12
  forwarding, packet 107

G
general port 106
  definition 110
  GPS coordinates 74
  guest VLAN 108

H
heater, internal 74

I
help 71
Hotspot
  basic settings 112
  network settings 112
  optional settings 113
  unrestricted access 118
  walled garden 116

J
installing an AP 13
internal heater 74
Internet settings 76
  interval, beacon 102
IP address 78
IPv4 connection type 78
IPv6 connection type 78
  isolated 93, 107

K
key index, WEP 96

L
L2TP 82
LED control 74
local bridging 107
local subnet 84, 93, 107
Local Subnet NAT and Route to WAN 93, 107
logging in 69
  login redirect URL
    authenticted users 113
    unauthorized users 112
  login remote authentication 75
  login settings 74
  logout 71

M
MAC authentication bypass 111
management access options 127
manager
  FM 12
  menu 71
  mode
    wireless 87
N
name, device 74
network 92
network settings, Hotspot 112
network time protocol server 77
O
optional settings, Hotspot 113
P
packet forwarding 93, 107
passphrase, WPA 98
ping 141
PoE out port 74
802.3af 21, 24, 27, 30, 33, 42, 48, 51
port
access 106
general 106
trunk 106
port type
ethernet 106
port-based VLAN 106, 110
PPPoE IPv4 connection type 81
Preconfiguring the AP 67
protection mode
CTS-only 91
RTS/CTS 91
PSK WPA authentication 98
R
radio network, wireless common 87
rebooting 139
releasing DHCP 78, 79, 80
renewing DHCP 78, 79, 80
resetting an AP to factory default 140
RFID
AeroScout 88
Ekahau 88
router mode 84
RTS/CTS
protection mode 91
threshold 102
S
SAMs controllers 12
SC8800-S 15
SCG controller 12
service provider login 75
Smart Access Management service (SAMs) controller 12
SmartCell Gateway (SCG) controller 12
SmartZone (SZ) controller 12
SSID 92
standalone operation 69
static IP connection type 80
syslog 133
SZ controller 12
T
T300 ZoneFlex AP 53
T300e ZoneFlex AP 56
T301n ZoneFlex AP 60
T301s ZoneFlex AP 63
tabs 71
TACACS+ server 75
tags
AeroScout 88
Ekahau 88
temperature update 74
threshold 93
RTS/CTS 102
traceroute 141
transmit power 90
trunk port 106
definition 109
Tunnel via L2TP 93, 107
U
unauthorized users login redirect URL 112
unrestricted access, Hotspot 112
URL
authenticated users login redirect 113
FlexMaster server 129
unauthorized users login redirect 112
user name 75
V
version
WPA-WPA2 98
version, WPA
WPA2 98, 100
WPA-WPA2 100
viewing associated clients 125
virtual SmartCell Gateway (vSCG) controller 12
VLAN 106, 108
dynamic 94
guest 108
overview 77
wired 110
wireless 93
vSCG controller 12

W
walled garden, Hotspot 116
web interface 69
WEP 94
WEP key index 96
width, channel 87
wireless 92
  advanced settings 88
    channel 87
    country code 88
    mode 87
wireless availability 92
wireless channel 124
wireless common
  radio network 87
wireless mode 123
wireless network 92
wireless security
  802.11X 99
  WEP 94
  WPA 96
wireless settings 86
WISPr 84
WLAN configuring 91
workspace 71
WPA 96
  802.1X authentication 98
  auto authentication 98
  passphrase 98
  PSK authentication 98
WPA version
  WPA2 98, 100
  WPA2-WPA2 98
  WPA-WPA2 100
WPA2 WPA version 98, 100
WPA-WPA2 WPA version 100

Z
Z2 APs 144
Zone 2 APs 144
ZoneDirector 68
ZoneFlex
  7762 AP 20
  7762-AC AP 23
  7762-S AP 26
  7762-S-AC AP 29
  7762-T AP 32
  7781CM AP 35
  7782 AP 41
  7782-E AP 44
  7782-N AP 47
  7782-S AP 50
  T300 AP 53
  T300e AP 56
  T301n AP 60
  T301s AP 63