



# Ruckus Wireless™ SmartCell Gateway™ 200

## Getting Started Guide for SmartZone 3.4

Part Number 800-71126-001 Rev A  
Published July 2016

[www.ruckuswireless.com](http://www.ruckuswireless.com)

## Copyright Notice and Proprietary Information

Copyright 2016. Ruckus Wireless, Inc. All rights reserved.

No part of this documentation may be used, 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 HEREIN ("MATERIAL") IS PROVIDED FOR GENERAL INFORMATION PURPOSES ONLY. RUCKUS AND ITS LICENSORS MAKE NO WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, WITH REGARD TO THE MATERIAL, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT AND FITNESS FOR A PARTICULAR PURPOSE, OR THAT THE MATERIAL IS ERROR-FREE, ACCURATE OR RELIABLE. RUCKUS RESERVES THE RIGHT TO MAKE CHANGES OR UPDATES TO THE MATERIAL AT ANY TIME.

### Limitation of Liability

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

### Trademarks

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

# Contents

<b>About This Guide</b>	
Document Conventions . . . . .	7
Related Documentation . . . . .	7
Documentation Feedback . . . . .	8
<b>1 Preparing to Set Up the SmartCell Gateway 200</b>	
Unpacking the SCG . . . . .	10
Verifying the Package Contents . . . . .	10
Rack Mount Kit Contents . . . . .	11
Before You Begin . . . . .	13
Prepare the Required Hardware and Tools . . . . .	13
Get to Know the Physical Features of the SCG . . . . .	14
<b>2 Mounting and Powering the SCG</b>	
Mounting the SCG onto a Server Rack . . . . .	22
What You Will Need . . . . .	22
Step 1: Unpack the Rack Mount Kit . . . . .	22
Step 2: Separate the Slide Rails into the Inner and Outer Parts . . . . .	23
Step 3: Install the Outer Rail Slides to the Rack Posts . . . . .	24
Step 4: Fasten the Shoulder Screws to the Server . . . . .	25
Step 5: Install the Inner Rails on the Server . . . . .	26
Step 6: Fasten the Inner Rails to the Server . . . . .	26
Step 7: Attach the Mounting Ears to the Rail Assembly . . . . .	27
Step 8: Slide the Rail Assembly into the Outer Rails and Secure to the Rack . . . . .	27
Powering On the SCG . . . . .	28
Using AC Power . . . . .	28
Using DC Power . . . . .	30
<b>3 Preparing the Interface Settings and Administrative Computer</b>	
Preparing the SCG Interface Settings to Use . . . . .	34
IPv6 Address Configuration . . . . .	34
Preparing the Administrative Computer . . . . .	35

## 4 Running the Setup Wizard and Logging On to the Web Interface

Overview of the SCG Setup Wizard . . . . .	38
Step 1: Start the Setup Wizard and Set the Language . . . . .	38
Step 2: Configure the Management IP Address Settings . . . . .	41
Important Notes About Selecting the System Default Gateway . . . . .	47
Step 3: Configure the DataPlane IP Address Settings . . . . .	48
Step 4: Configure the Cluster Settings . . . . .	49
If This Controller Is Forming a New Cluster . . . . .	50
If This Controller Is Joining an Existing Cluster . . . . .	52
Step 5: Verify the Settings . . . . .	53
Connecting Data Blades to the Network . . . . .	54
Supported SFP+ Modules . . . . .	54
Logging On to the Web Interface . . . . .	55

## 5 Configuring the SCG for the First Time

Creating an AP Zone . . . . .	58
Configuring AAA Servers and Hotspot Settings . . . . .	65
Adding an AAA Server . . . . .	65
Creating a Hotspot (WISPr) Service . . . . .	67
Creating a Registration Rule . . . . .	71
Configuring the Rule Priority . . . . .	73
Defining the WLAN Settings of an AP Zone . . . . .	74
General Options . . . . .	76
WLAN Usage . . . . .	77
Authentication Options . . . . .	77
Encryption Options . . . . .	79
Authentication & Accounting Service . . . . .	80
Options . . . . .	80
RADIUS Options . . . . .	80
Advanced Options . . . . .	82
Verifying That Wireless Clients Can Associate with a Managed AP . . . . .	83
What to Do Next . . . . .	84

## 6 Ensuring That APs Can Discover the Controller on the Network

Is LWAPP2SCG Enabled on the Controller? . . . . .	86
Obtaining the LWAPP2SCG Application . . . . .	86
Enabling LWAPP2SCG . . . . .	86
Method 1: Perform Auto Discovery of the Controller Using the SmartLicense Server . . . . .	87
Method 2: Perform Auto Discovery on Same Subnet, then Transfer the AP to Intended	

Subnet . . . . .	88
Method 3: Register the Controller with the DNS Server . . . . .	88
Method 4: Configure DHCP Option 43 on the DHCP Server . . . . .	91
Method 5: Manually Configure the Controller Address on the AP's Web Interface . . . . .	94
What to Do Next . . . . .	95

## Index

# About This Guide

This *SmartCell Gateway™ 200 Getting Started Guide* provides information on how to set up the SmartCell Gateway 200 (SCG-200 or “the controller”) appliance on the network. Topics covered in this guide include mounting, installation, and basic configuration.

This guide is intended for use by those responsible for installing and setting up network equipment. Consequently, it assumes a basic working knowledge of local area networking, wireless networking, and wireless devices.

---

**NOTE:** If release notes are shipped with your product and the information there differs from the information in this guide, follow the instructions in the release notes.

---

Most user guides and release notes are available in Adobe Acrobat Reader Portable Document Format (PDF) or HTML on the Ruckus Wireless Support website at <https://support.ruckuswireless.com/documents>.

# Document Conventions

Table 1 and Table 2 list the text and notice conventions that are used throughout this guide.

Table 1. Text conventions

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

Table 2. Notice conventions

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

## Related Documentation

In addition to this *Getting Started Guide*, each SmartCell Gateway 200 documentation set includes the following:

- *Administrator Guide*: Provides detailed information on how to configure the SCG. The Administrator Guide is available for download on the Ruckus Wireless Support website at <http://support.ruckuswireless.com>.
- *Online Help*: Provides instructions for performing tasks using the SCG web interface. The online help is accessible from the web interface and is searchable.
- *Release Notes*: Provide information about the current software release, including new features, enhancements, and known issues.

---

**NOTE:** For a complete list of documents that accompany this release, refer to the *Release Notes*.

---

## 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](mailto: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:

- SmartCell Gateway 200 Getting Started Guide for SmartZone 3.4
- Part number: 800-71126-001
- Page 88



# Preparing to Set Up the SmartCell Gateway 200

# 1

In this chapter:

- [Unpacking the SCG](#)
- [Verifying the Package Contents](#)
- [Before You Begin](#)

# Unpacking the SCG

---

**WARNING!** The SCG appliance is heavy (40 lbs/18.14kg). Two people should work together to unpack the SCG. Ruckus Wireless strongly recommends against one person attempting to perform this task alone.

---

Follow these steps to unpack the SCG appliance.

- 1 Open the SCG package, and then carefully remove the contents.
- 2 Return all packing materials into the shipping box, and then put the box away in a dry location.
- 3 Verify that all of the items listed in [Verifying the Package Contents](#) (below) are included in the package. Check each item for damage. If any item is damaged or missing, notify your authorized Ruckus Wireless sales representative immediately.

## Verifying the Package Contents

A complete SCG package contains all of the items listed below:

- One SCG appliance with two AC/DC power supply units
- One console cable (use only this cable to connect the front or rear serial port via a laptop/notebook)
- One rack mount kit (see [Rack Mount Kit Contents](#) below)
- Service Level Agreement / Limited Warranty Statement sheet
- Regulatory Statement sheet
- This *Getting Started Guide*

---

**NOTE:** The AC power cable (part number 902-0174-XX00, where XX is the two-character country code) is not supplied with the SCG appliance and may be ordered separately.

---

## Rack Mount Kit Contents

The rack mount kit contains the following items:

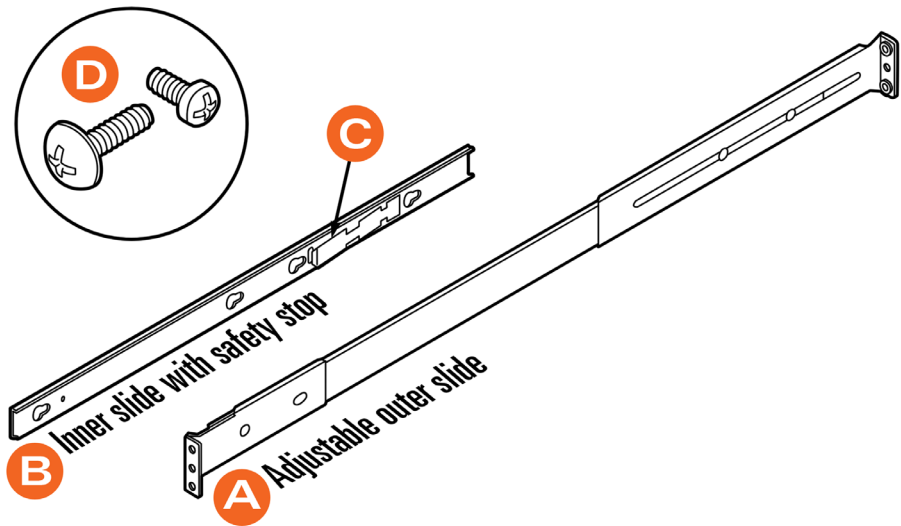
- Outer rail slide assembly (see A in [Figure 1](#))
- Inner rail slide assembly (see B in [Figure 1](#))
- Plastic bag #1, which contains the following items:
  - Four hex head shoulder screws
  - Two #10-32 x 3/8" screws
  - Two rack mounting ears
- Plastic bag #2, which contains the following items:
  - Outer slide rail screws, 8 #8-32 x 1/2 (see D in [Figure 1](#))
  - Inner slide rail screws, 8 #6-32 x 1/4 (see D in [Figure 1](#))
  - Rack screws, 2 #8-32 x 3/4 (see D in [Figure 1](#))
- The *SmartCell Gateway 200 Rack Mount Installation Guide*

---

**NOTE:** This rack mount kit includes two sets of 8-32 x 1/2" screws. One set of eight has a larger screw head size than the second set of eight. Use the set of 8-32 x 1/2" screws that best fits the rack in which you are installing the rail kit.

---

Figure 1. Rail assemblies and rail screws



# Before You Begin

Before installing and setting up the SCG, Ruckus Wireless recommends that you first complete the following pre-installation tasks.

## Prepare the Required Hardware and Tools

You must supply the following tools and equipment:

- A switch or router with 10GbE interfaces (for connecting the SCG to the backbone network)

---

**NOTE:** A fast ethernet or gigabit switch/router is required to upload management, cluster, and configurations. A 10GBE switch/router is only required if the customer is going to use tunnels.

---

- A Phillips #1 screwdriver
- A flat head screwdriver
- An administrative computer (desktop or laptop) running Windows 8/7/Vista/XP or Mac OS X, containing a minimum RAM of 13G, with a web browser installed (Google Chrome recommended). Supported web browsers include:
  - Google Chrome 15 (and later)
  - Safari 5.1.1 (and later)
  - Mozilla Firefox 8 (and later)
  - Microsoft Internet Explorer 9.0
- A grounded electrical power strip or surge suppressor to protect from circuit overload
- A standard EIA 19-inch wide rack with an available 2RU space
- Two SFP+ modules (see [Supported SFP+ Modules](#)). For a redundant setup, you will need four SFP+ modules.

---

**NOTE:** At the beginning of each procedure, this guide lists the specific tools, accessories, or equipment that you will need to complete that procedure.

---

## Get to Know the Physical Features of the SCG

The following sections identify the physical features of the SCG that are relevant to the installation and mounting instructions that this guide provides. Before you begin the installation process, Ruckus Wireless strongly recommends that you become familiar with these physical features.

### Front Panel

Figure 2 shows the SCG front panel with the bezel installed. For descriptions of the numbered parts, refer to Table 1.

Figure 2. SCG front panel with the bezel

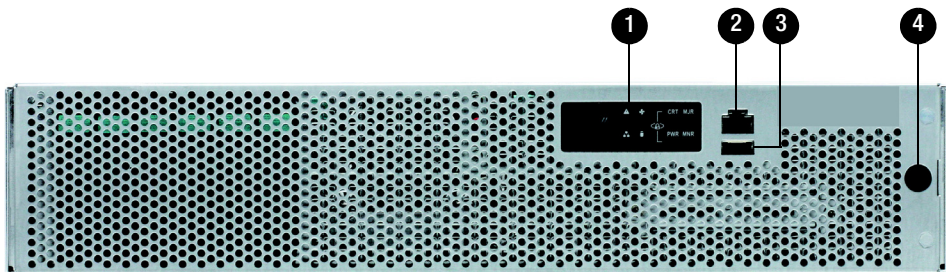


Table 1. SCG front panel parts

Number	Description
1	Control panel (see <a href="#">Control Panel on the Front Panel</a> )
2	RJ45 serial port (COM2/serial B). Use only the console cable provided to connect this port via a laptop/notebook. <b>CAUTION!</b> The SCG has two RJ45 serial ports – one on the front panel and one on the rear panel. You can only use one of these two ports at any given time. Using them simultaneously may cause both serial ports to become unresponsive.
3	Use the USB port to connect a keyboard and mouse. Use a USB stick (for a fresh installation).
4	Front bezel lock

## Front Panel Without the Bezel

Figure 3 shows the front panel of the SCG without the bezel. For descriptions of the numbered parts, refer to Table 2.

Figure 3. SCG front panel without the bezel

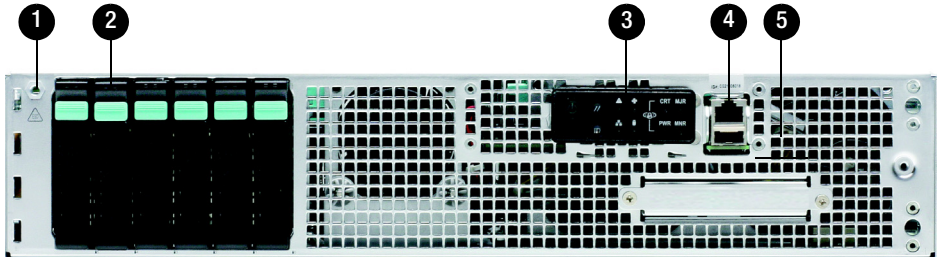


Table 2. SCG front panel parts (without the bezel)

Number	Description
1	ESD ground strap attachment
2	Hard drive bays (the SCG has two 600GB hard drives)
3	Control panel (buttons and status indicators, see <a href="#">Control Panel on the Front Panel</a> )
4	RJ45 serial port (COM2 / serial B). Use only the console cable provided to connect this port to another device. <b>CAUTION!</b> The SCG has two RJ45 serial ports – one on the front panel and one on the rear panel. You can only use one of these two ports at any given time. Using them simultaneously may cause both serial ports to become unresponsive.
5	USB port (not used)

## RJ45 Serial Port Pinouts

The following table shows the pinouts for the RJ45 serial ports on the front and rear panels.

Table 3. RJ45 serial port pinouts

Pin	Signal Name	Description
1	SPB_RTS	RTS (request to send)
2	SPB_DTR	DTR (data terminal ready)
3	SPB_OUT_N	TXD (transmit data)
4	GND	Ground
5	SPB_RI	RI (ring indicate)
6	SPB_SIN_N	RXD (receive data)
7	SPB_DCR_DCD	Data Set Ready/Data Carrier Detect
8	SPB_CTS	CTS (clear to send)

## Control Panel on the Front Panel

Figure 4 shows the control panel on the front panel of the SCG. For descriptions of the numbered parts, refer to Table 4.

Figure 4. Control panel on the SCG front panel

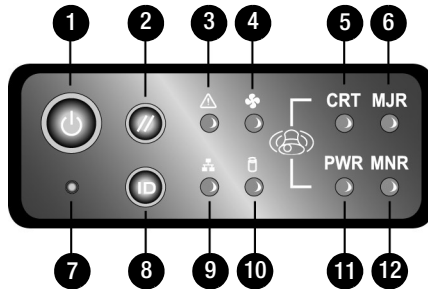


Table 4. Control panel parts

Number	Description
1	Power button
2	System reset button
3	System status LED



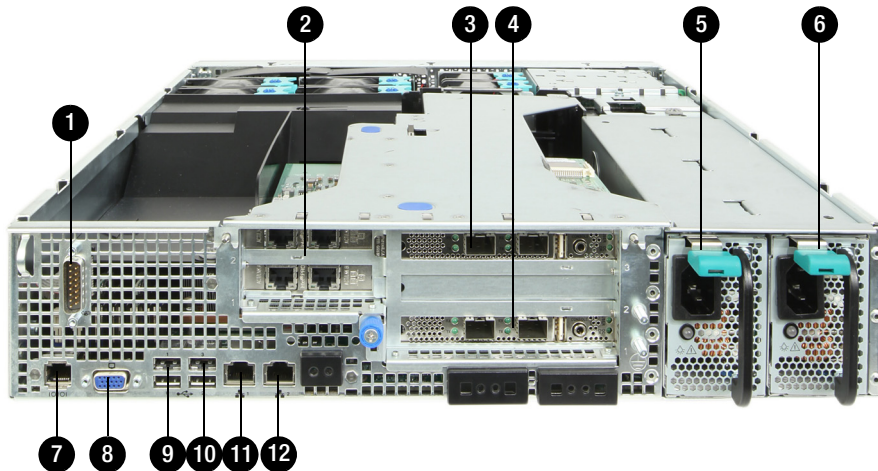
Table 4. Control panel parts (Continued)

Number	Description
4	Fan status LED
5	Critical alarm (not implemented in this release)
6	MJR alarm LED (not implemented in this release)
7	NMI pin hole button (factory reset button)
8	Chassis ID button
9	NIC1/NIC2 activity LED
10	HDD activity LED (flashing green: HDD activity; amber: HDD fault; off: no access or no HDD fault)
11	PWR alarm LED (not implemented in this release)
12	Minor alarm (amber: system unavailable; off: system available)

## Rear Panel

Figure 5 shows the rear panel of the SCG. For descriptions of the numbered parts, refer to Table 5.

Figure 5. SCG rear panel



**NOTE:** The power supply locations (numbers 5 and 6) are for AC or DC power. AC power supply is pictured.

Table 5. SCG rear panel parts

Number	Description
1	Cable connector
2	Two low-profile PCIe interface cards that include four ports – one for management traffic and three for redundancy. See <a href="#">Redundant Interfaces on the SCG</a> .
3	PCIe add-in card slot for DataPlane1
4	PCIe add-in card slot for DataPlane0
5	Power supply 2
6	Power supply 1
7	<p>RJ45 serial port (COM2/serial B). Use only the console cable provided to connect this port to another device.</p> <p><b>CAUTION!</b> The SCG has two RJ45 serial ports – one on the front panel and one on the rear panel. You can only use one of these two ports at any given time. Using them simultaneously may cause both serial ports to become unresponsive.</p> <p><b>NOTE:</b> For information on how to access and use the SCG command line interface, refer to the <i>SmartCell Gateway 200 Virtual SmartZone High-Scale Command Line interface Reference Guide</i>.</p>
8	Video connector
9	USB 0 and 1 (#1 on top)
10	USB 2 and 3 (#3 on top)
11	ETH1 GbE NIC for cluster traffic
12	ETH2 GbE NIC for control (between access points and the SCG controller) traffic

## ***NIC LEDs on the Rear Panel***

[Table 6](#) describes the behavior of the NIC LEDs on the rear panel of the SCG.

Table 6. LEDs on the SCG rear panel

<b>LED Color</b>	<b>LED State</b>	<b>NIC State</b>
Green/amber (left)	Off	10Mbps
	Green	100Mbps
	Amber	1000Mbps
Green (right)	On	Active connection
	Blinking	Transmitting or receiving data

## Redundant Interfaces on the SCG

The SCG offers network redundancy options by providing redundant interfaces for the three traffic types that it handles – control traffic, cluster traffic, and management traffic. A redundant interface pairs an active interface and a standby interface. When the active interface fails, the standby interface becomes active automatically and takes over the job of passing traffic.

To enable a redundant interfaces pair, you need to connect the member ports (see [Table 7](#)) to the same router or switch or to two different routers or switches, depending on the network environment of your organization.

[Figure 6](#) identifies the redundant interface pairs on the rear panel of the SCG and [Table 7](#) lists the member ports of each redundant interface pair.

Figure 6. Redundant interfaces on the SCG

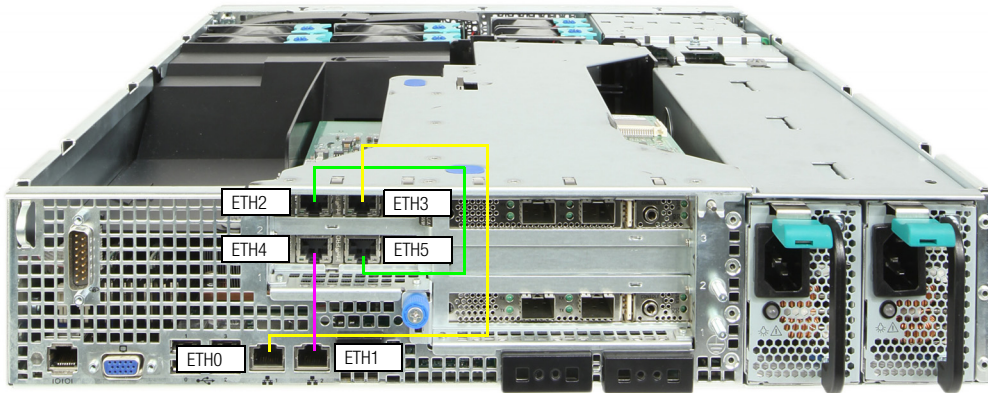


Table 7. Bridge groups, member interfaces, and traffic types

Member Ports	Bridge	Traffic Type
ETH1 and ETH3	Bridge 0	Control (SSH tunnels between APs and SCG) traffic
ETH2 and ETH4	Bridge 1	Cluster traffic
ETH2 and ETH5	Bridge 2	Management (web interface) traffic

# Mounting and Powering the SCG

# 2

In this chapter:

- [Mounting the SCG onto a Server Rack](#)
- [What You Will Need](#)
- [Step 1: Unpack the Rack Mount Kit](#)
- [Step 2: Separate the Slide Rails into the Inner and Outer Parts](#)
- [Step 3: Install the Outer Rail Slides to the Rack Posts](#)
- [Step 4: Fasten the Shoulder Screws to the Server](#)
- [Step 5: Install the Inner Rails on the Server](#)
- [Step 6: Fasten the Inner Rails to the Server](#)
- [Step 7: Attach the Mounting Ears to the Rail Assembly](#)
- [Step 8: Slide the Rail Assembly into the Outer Rails and Secure to the Rack](#)
- [Powering On the SCG](#)

## Mounting the SCG onto a Server Rack

The SCG is a 2U form factor server designed for mounting onto a standard EIA 19" server rack. The supplied mounting hardware supports mounting on server racks that are 22.5" to 32.5" deep. For racks of depth less than 22.5", use the TMLC-MOUNT21 rack mount kit (available at Avnet and manufactured by Kontron).

Before installing the SCG appliance onto a server rack, verify that all package contents (see [Unpacking the SCG](#)) are included and ensure that you have prepared all the required hardware and tools.

### What You Will Need

- 3/8-inch hex driver or wrench
- Phillips (crosshead) screwdriver, #1 and #2 bits
- Anti-static wrist strap and conductive foam pad (recommended)

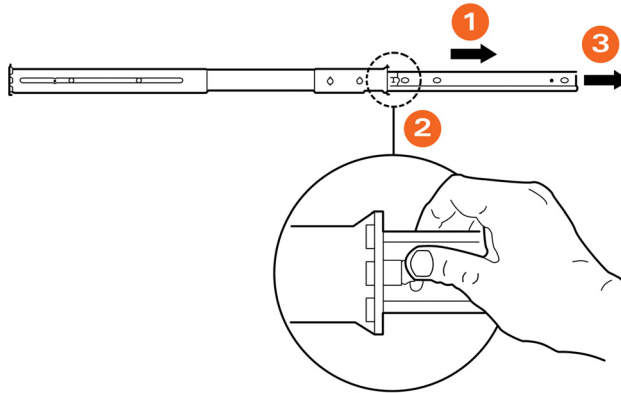
### Step 1: Unpack the Rack Mount Kit

Refer to [Rack Mount Kit Contents](#) and verify that the rack mount kit contents are complete.

## Step 2: Separate the Slide Rails into the Inner and Outer Parts

- 1 Extend the inner rail (see 1 in Figure 7) until it locks.
- 2 Press down the spring safety lock (see 2 in Figure 7) to release the inner rail.
- 3 Remove the inner rail from the rail assembly (see 3 in Figure 7).

Figure 7. Separating the slide rails

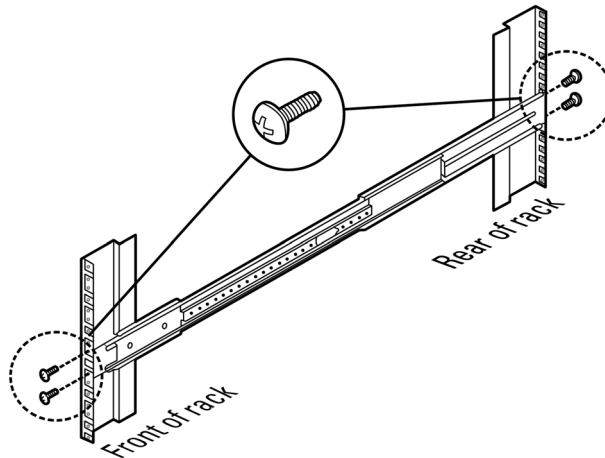


## Step 3: Install the Outer Rail Slides to the Rack Posts

**NOTE:** The two rail assemblies are NOT interchangeable. Each assembly needs to be installed into the rack by its orientation (right or left) when standing in front of the rack. The right rail assembly is identified with a BLUE sticker and the left rail assembly is identified with a GREEN sticker.

Attach the outer rail slides to the rack posts using two #8-32 x 1/2 screws at the front posts and two #8-32 x 1/2 screws at the rear posts.

Figure 8. Installing the outer rails

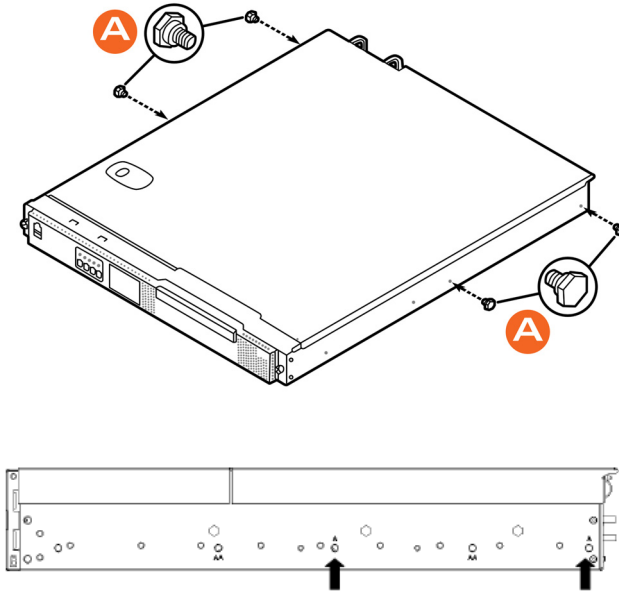




## Step 4: Fasten the Shoulder Screws to the Server

Fasten two hex head shoulder screws on each side of the server.

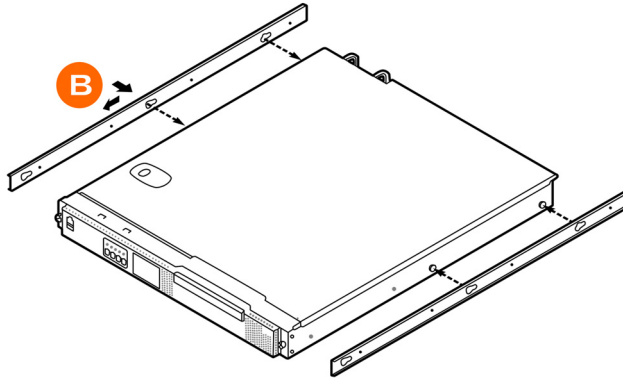
Figure 9. Fastening the shoulder screws



## Step 5: Install the Inner Rails on the Server

Install the inner rails onto the hex head shoulder screws, and then slide the inner rails forward.

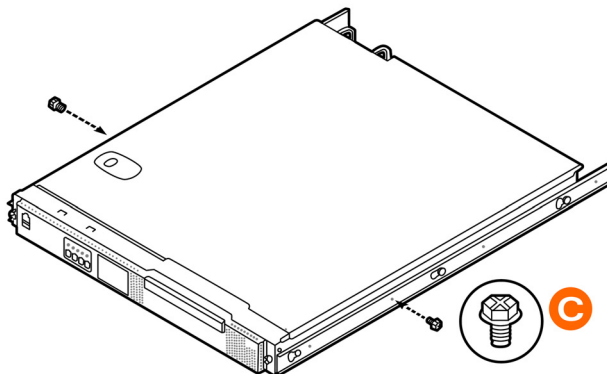
Figure 10. Installing the inner rails



## Step 6: Fasten the Inner Rails to the Server

Secure the inner rails with one #6-32 x 1/4 screw for each rail.

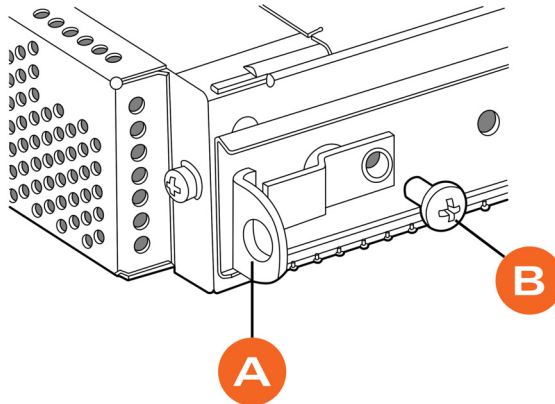
Figure 11. Securing the inner rails



## Step 7: Attach the Mounting Ears to the Rail Assembly

Attach the rack mounting ears (A) to each side of the server using the #10-32 x 3/8 screws (B).

Figure 12. Attaching the mounting ears

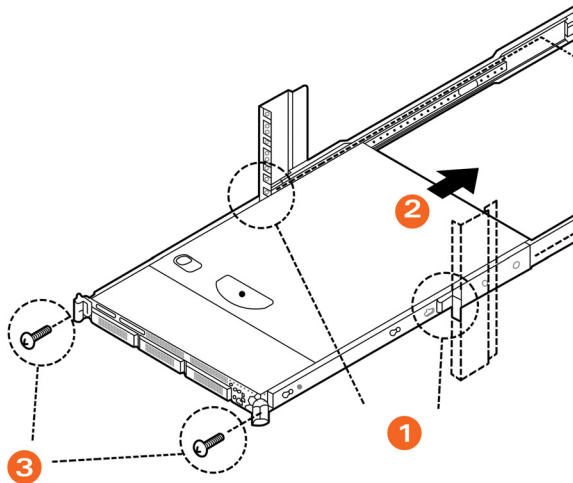


## Step 8: Slide the Rail Assembly into the Outer Rails and Secure to the Rack

**WARNING!** The SCG appliance is heavy (40 lbs/18.14kg). Two people should work together to lift and slide the appliance into the rack. Ruckus Wireless strongly recommends against one person attempting to perform this task alone.

- 1 Align the inner rails (attached to the server chassis) with the outer rail assemblies (attached to the rack).
- 2 Engage the matching rails, and then slide the server chassis into the rack until the two spring safety locks snap into position.
- 3 Press down the two spring safety locks (one on each side). See 1 in Figure 13.
- 4 Slide the server chassis all the way into the rack. See 2 in Figure 13.
- 5 Use the rack screws (#8-32 x 3/4) to secure the chassis and rack handles into the rack. See 3 in Figure 13.

Figure 13. Securing the server to the rack



Congratulations! You have completed mounting the SCG onto your server rack.

## Powering On the SCG

The SCG supports both AC and DC power. Refer to the relevant section below for instructions on how to power on the SCG.

- [Using AC Power](#)
- [Using DC Power](#)

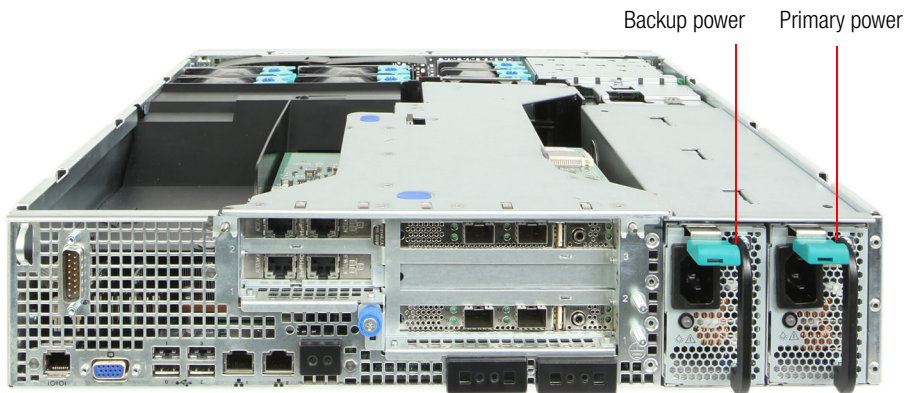
### Using AC Power

**NOTE:** The AC power cable (part number 902-0174-XX00, where XX is the two-character country code) is not supplied with the SCG appliance and may be ordered separately.

Follow these steps to use AC to supply power to the SCG.

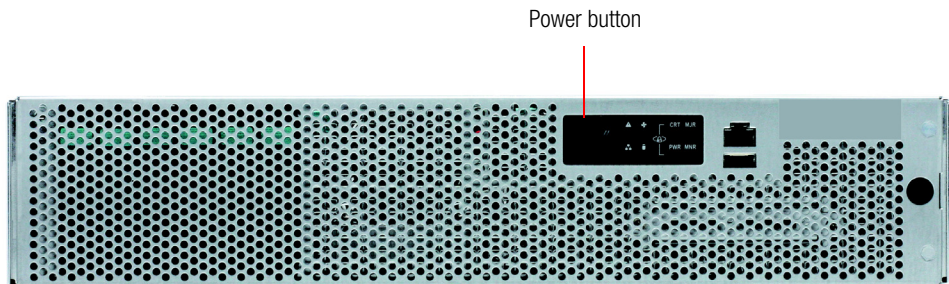
- 1 Connect the AC power cable to the primary power socket (right) on the rear panel. Optionally, connect a second AC power cable to the backup power socket (left) on the rear panel.

Figure 14. Power sockets on the SCG



- 2 Connect the other end of the power cable (or cables) to an electrical outlet.
- 3 Press the **Power** button on the control panel to power on the SCG. The MNR LED on the Control Panel turns amber while booting up, and turns off when the startup is complete.

Figure 15. Power button on the Control Panel



## Using DC Power

The DC power subsystem supports up to two redundant DC power supply units (PSUs). To remove the PSU, simply press down on the green locking tab while pulling outward on the PSU handle. To insert the PSU, slide the entire unit (green locking tab toward the top) fully into the SCG chassis until it locks in place.

If using DC power, connect -48V DC input power to the PSU. The DC input polarity is marked on the DC PSU case. In [Figure 16](#), “-” is on the left and “+” is on the right.

---

**NOTE:** Use #14-#10 AWG to the DC input connector.

---

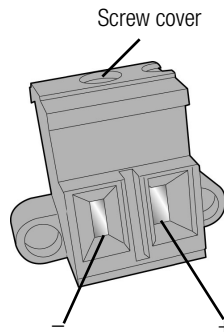
**CAUTION!** To avoid the potential for electrical shock and fire hazard, ensure that the DC wiring to the DC input connectors has adequate circuit protection in accordance with local electrical codes

---

**NOTE:** Information on how to replace the PSU is provided in the *SmartCell Gateway 200 Administrator Guide*.

---

Figure 16. DC input connector



Follow these steps to use DC to supply power to the SCG.

- 1 (When looking at the DC input connector from the angle shown above), slide the screw cover on the top of the DC input connector to the left to reveal the top screws.
- 2 Loosen the screws enough so that the DC input wires can be fully inserted into the apertures.
- 3 Insert the “-” wire into the left side aperture, and the “+” wire into the right side.
- 4 Screw the top screws down until the wires are locked in place.

- 5 Slide the screw cover back to the right.
- 6 Apply power to the DC input system. The single LED on the bottom left side of the power supply module lights green when all power outputs are available.

You have completed supplying power to the SCG using DC.

## DC Power Supply Input Voltage and Current Requirements

[Table 8](#) lists the DC power supply input voltage and current requirements.

Table 8. DC input voltage and current requirements

<b>DC Input Voltage</b>	
Nominal	-48Vdc
Minimum	-38Vdc
Rated	-48Vdc to -60Vdc
Maximum	-75Vdc
<b>DC Input Current</b>	
Maximum	13A @ -38Vdc

**CAUTION!** To avoid the potential for an electrical shock hazard, for AC power you must include a third wire safety ground conductor with the rack installation. For DC power, the two studs for chassis enclosure grounding must be used for proper safety grounding. With AC power, if the server power cord is plugged into an outlet that is part of the rack, then you must provide proper grounding for the rack itself. If the server power cord is plugged into a wall outlet, the safety ground conductor in the power cord provides proper grounding only for the server. You must provide additional, proper grounding for the rack and other devices installed in it.

## DC PSU LED

[Table 9](#) describes the behavior of the DC PSU LED.

Table 9. DC PSU LED behavior

LED State	Description
Off	No DC to all power supplies
Amber	<ul style="list-style-type: none"><li>• No DC to this PSU only (for 1+1 configuration), or;</li><li>• Power supply critical event causing a shutdown: failure, fuse blown (1+1 only), OCP (12V), OVP (12V), fan failed</li></ul>
Blinking Amber	Power supply warning events where power supply continues to operate: high temp, high power/high current, slow fan
Blinking Green	DC present / Only 5Vsb on (PS off)
Green	Output ON and OK



# Preparing the Interface Settings and Administrative Computer

# 3

In this chapter:

- [Preparing the SCG Interface Settings to Use](#)
- [Preparing the Administrative Computer](#)

## Preparing the SCG Interface Settings to Use

The SCG appliance includes three network interfaces (see [Table 10](#)) that need to be connected to the network for the appliance to work. When you run the SCG Setup Wizard later in this chapter, you will be required to assign each of these interfaces on the SCG a separate set of network settings.

---

**CAUTION!** When you run the Setup Wizard, you must configure the three SCG interfaces to be on three different subnets. Failure to do so may result in loss of access to the web interface or failure of system functions and services.

---

The following network settings are required:

- IP address: IP address in IPv4. If your network uses IPv6, see [IPv6 Address Configuration](#) for more information.
- Netmask
- Gateway
- Primary DNS server
- Secondary DNS server

Table 10. SCG interfaces

Interface	Description
AP/DataPlane	Used for AP configuration and client traffic
Cluster	Used for cluster traffic
Management (Web)	Used for management traffic. The IP address that you assign to this interface will be the IP address through which you can access the SCG via SSH or Web GUI.

### IPv6 Address Configuration

The controller supports IPv4 and dual IPv4/IPv6 operation modes. If both IPv4 and IPv6 are used on the network, the controller will keep both IP addresses. APs can be in V4 or V6 or both based on the zone configuration. By default it will be in IPv4, and if required you need to enable IPv6. Ruckus ZoneFlex APs operate in dual IPv4/v6 mode by default, so you do not need to manually set the mode for each AP.

If you enable IPv6, you have the option to manually configure an IP address in IPv6 format (128 bits separated by colons, instead of decimals) or to choose **Auto Configuration**. If you choose **Manual**, you will need to enter values for the IP address, prefix length and gateway.

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

## Preparing the Administrative Computer

Follow these steps to prepare the administrative computer that you will use to run the SCG Setup Wizard.

- 1 On the administrative computer, open the *Network Connections* (or *Network and Dial-up Connections*) control panel according to how your *Start* menu is set up:
  - **Start > Settings > Network Connections**
  - **Start > Control Panel > Network and Sharing Center > Change Adapter Settings**

---

**NOTE:** This procedure assumes Windows 7 as the operating system. Procedures for other operating systems are similar.

---

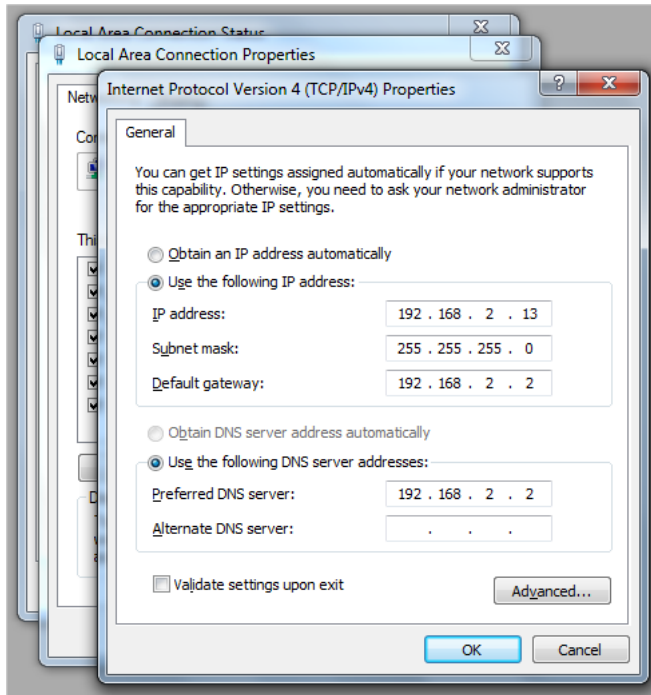
- 2 When the *Network Connections* windows appears, right click the icon for “Local Area Connection” and click **Properties**.
- 3 When the *Local Area Connection Properties* dialog box appears, click **Internet Protocol Version 4 (TCP/IPv4)** from the scrolling list, then and click **Properties**. The *TCP/IP Properties* dialog box appears.

---

**NOTE:** Write down all of the currently active settings so you can restore your computer to its current configuration later (when this process is complete).

---

Figure 17. The Internet Protocol Version 4 (TCP/IP) properties dialog box



- 4 Select **Use the following IP address** (if it is not already active) and make the following entries:
  - *IP address*: 192.168.2.13 (or any address on the 192.168.2.x network other than 192.168.2.2, which is in use by the SCG)
  - *Subnet mask*: 255.255.255.0
  - *Default gateway*: 192.168.2.2
  - *Preferred DNS server*: 192.168.2.2
- 5 Leave the *Alternate DNS Server* field empty.
- 6 Click **OK** to save your changes and exit first the *TCP/IP Properties* dialog box, then the *Local Area Connection Properties* dialog box. Your changes are put into effect immediately.

You have completed preparing the administrative computer.

# Running the Setup Wizard and Logging On to the Web Interface

# 4

In this chapter:

- [Overview of the SCG Setup Wizard](#)
- [Step 1: Start the Setup Wizard and Set the Language](#)
- [Step 2: Configure the Management IP Address Settings](#)
- [Step 4: Configure the Cluster Settings](#)
- [Step 5: Verify the Settings](#)
- [Connecting Data Blades to the Network](#)
- [Logging On to the Web Interface](#)

# Overview of the SCG Setup Wizard

Follow these steps to run and complete the SCG Setup Wizard.

[Step 1: Start the Setup Wizard and Set the Language](#)

[Step 2: Configure the Management IP Address Settings](#)

[Step 3: Configure the DataPlane IP Address Settings](#)

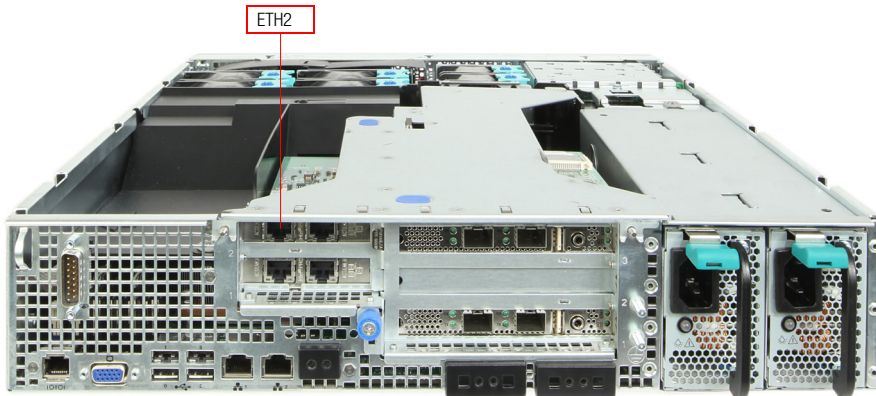
[Step 4: Configure the Cluster Settings](#)

[Step 5: Verify the Settings](#)

## Step 1: Start the Setup Wizard and Set the Language

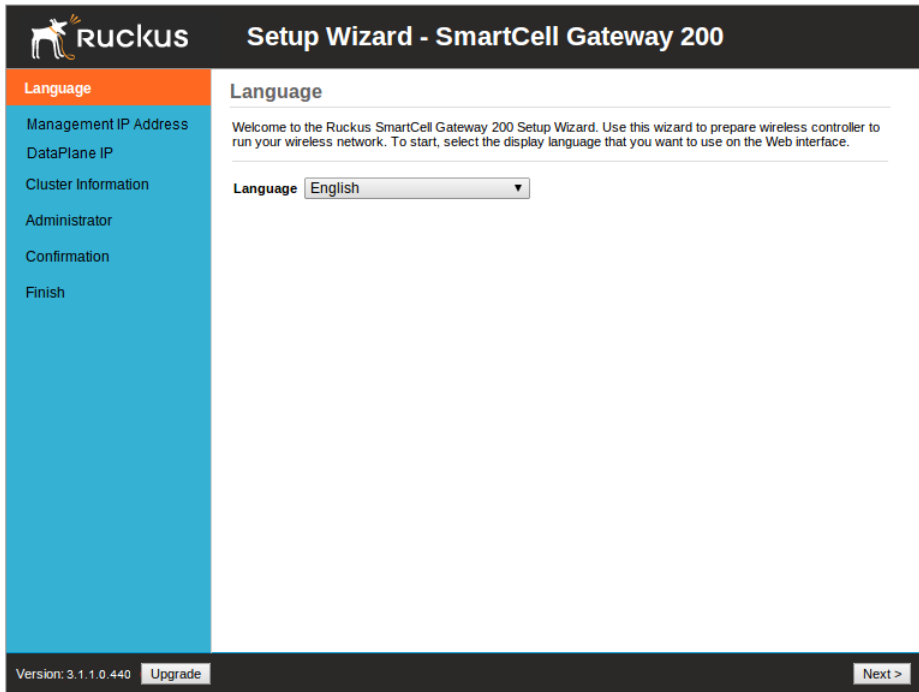
- 1 Connect one end of an Ethernet cable to ETH2 on the rear panel of the SCG, and then connect the other end to an Ethernet port on the administrative computer.

Figure 18. Location of ETH2



- 2 Start your web browser, and then enter the following in the address bar:  
`http://192.168.2.2:8080`  
The SCG Setup Wizard appears, displaying the *Language* page.

Figure 19. The Language page



- 3 Select your preferred language for the SCG web interface. Available options include:
  - English
  - Traditional Chinese
  - Simplified Chinese
- 4 Click **Next**. The *Management IP* page appears and displays options for configuring the network addressing of the following interfaces on the controller:
  - Control (AP/DataPlane)
  - Cluster
  - Management (Web)

Figure 20. The Management IP page, showing the Control (AP/DataPlane) tab

**Ruckus** Setup Wizard - SmartCell Gateway 200

Language  
**Management IP**  
DataPlane IP  
Cluster Information  
Administrator  
Confirmation  
Finish

### Management IP

Select the network addressing mode "Static" or "DHCP" or "Auto Configuration". If you select "DHCP" or "Auto Configuration", no further configuration is needed. If you select "Static", enter the relevant IP addressing information. (Fields marked with an asterisk (\*) are required.)

IP Version Support  IPv4 only  IPv4 and IPv6

Control(AP/DataPlane) Cluster Management(Web)

**IPv4**  
 Static  DHCP  
IP Address \* 172.17.26.104  
Netmask \* 255.255.254.0  
Gateway 172.17.26.1

**IPv6**  
 Static  Auto Configuration  
IP Address \* ::456/64  
Gateway ::789

Default Gateway Management(Web) Management(Web)

Primary DNS Server IPv4 Primary DNS IPv6 Primary DNS

Secondary DNS Server IPv4 Secondary DNS IPv6 Secondary DNS

Version: 3.1.1.0.440 Upgrade < Back Apply >



## Step 2: Configure the Management IP Address Settings

- 1 In *IP Version Support*, select one of the following options:
  - **IPv4 Only:** Click this option if you want the controller to obtain an IPv4 address from a DHCP server on the network.
  - **IPv4 and IPv6:** Click this option if you want the controller to obtain both IPv4 and IPv6 addresses from DHCP and DHCPv6 servers on the network.
- 2 Configure the IP address settings of the *Control (AP/DataPlane)* interface.
  - a Under the *IPv4* section, click **Static**, and then enter the network settings that you want to assign to the AP/DataPlane interface, through which client traffic and configuration data are sent and received.

---

**NOTE:** Although it is possible to use DHCP to assign IP address settings to the Control interface automatically, Ruckus Wireless strongly recommends assigning a static IP address to this interface.

---

**WARNING!** You must configure the three interfaces to be on three different subnets. Failure to do so may result in loss of access to the web interface or failure of system functions and services.

---

The following network settings are required (others are optional):

- IP address
  - Netmask
  - Default gateway
- b If you clicked **IPv4 and IPv6** at the beginning of this procedure, under the *IPv6* section, click **Auto Configuration** if you want the controller to obtain its IP address from Router Advertisements (RAs) or from a DHCPv6 server on the network. If you want to manually assign the IPv6 network address, click **Static**, and then set the values for the following:
    - *IP address (IPv6):* Enter an IPv6 address (global only) with a prefix length (for example, 1234::5678:0:c12/123). Link-local addresses are unsupported.
    - *Gateway:* Enter an IPv6 address (global or link-local) without a prefix length. Here are examples:
      - Global address without a prefix length: 1234::5678:0:c12
      - Link-local address without a prefix length: fe80::5678:0:c12

- c Click the *Cluster* tab when done.

Figure 21. The Cluster tab

**RUCKUS** Setup Wizard - SmartCell Gateway 200

Language

**Management IP**

DataPlane IP

Cluster Information

Administrator

Confirmation

Finish

**Management IP**

Select the network addressing mode "Static" or "DHCP" or "Auto Configuration". If you select "DHCP" or "Auto Configuration", no further configuration is needed. If you select "Static", enter the relevant IP addressing information. (Fields marked with an asterisk (\*) are required.)

IP Version Support  IPv4 only  IPv4 and IPv6

Control(AP/DataPlane) **Cluster** Management(Web)

**IPv4**

Static  DHCP

IP Address \*

Netmask \*

Gateway

Default Gateway\*

Primary DNS Server IPv4 Primary DNS  IPv6 Primary DNS

Secondary DNS Server IPv4 Secondary DNS  IPv6 Secondary DNS

Version: 3.1.1.0.440 Upgrade

- 3 On the *Cluster* tab, click **Static** under the *IPv4* section, and then enter the network settings that you want to assign to the cluster interface, through which cluster data will be sent and received.

**NOTE:** Although it is possible to use DHCP to assign IP address settings to the Cluster interface automatically, Ruckus Wireless strongly recommends assigning a static IP address to this interface.

**WARNING!** You must configure the three SCG interfaces to be on three different subnets. Failure to do so may result in loss of access to the web interface or failure of system functions and services.

The following network settings are required (others are optional):

- IP address
- Netmask

- Default gateway

Click the *Management (Web)* tab when done.

Figure 22. The Management (Web) tab

- 4 On the *Management (Web)* tab, configure the IP address settings of the management interface.
  - a Under the *IPv4* section, click **Static**, and then enter the network settings that you want to assign to the AP/DataPlane interface, through which client traffic and configuration data are sent and received.

**NOTE:** Although it is possible to use DHCP to assign IP address settings to the Control interface automatically, Ruckus Wireless strongly recommends assigning a static IP address to this interface.

**WARNING!** You must configure the three interfaces to be on three different subnets. Failure to do so may result in loss of access to the web interface or failure of system functions and services.

The following network settings are required (others are optional):

- IP address
- Netmask
- Default gateway

**b** If you clicked **IPv4 and IPv6** at the beginning of this procedure, under the *IPv6* section, click **Auto Configuration** if you want the management (web) interface to obtain its IP address from Router Advertisements (RAs) or from a DHCPv6 server on the network. If you want to manually assign the IPv6 network address, click **Static**, and then set the values for the following:

- *IP address* (IPv6): Enter an IPv6 address (global only) with a prefix length (for example, `1234::5678:0:c12/123`). Link-local addresses are unsupported.
- *Gateway*: Enter an IPv6 address (global or link-local) without a prefix length. Here are examples:
  - Global address without a prefix length: `1234::5678:0:c12`
  - Link-local address without a prefix length: `fe80::5678:0:c12`

**5** At the bottom of the screen (see [Figure 23](#)), select the interface that you want to set as the default system gateways for IPv4 and IPv6 (if enabled), and then type the primary and secondary DNS server addresses.

---

**NOTE:** The appropriate interface to use as the default system gateway depends on the topology of your network. See [Important Notes About Selecting the System Default Gateway](#) for more information.

---

Figure 23. Select the IPv4 and IPv6 (if enabled) default system gateways

**Ruckus Setup Wizard - SmartCell Gateway 200**

**Management IP**

Select the network addressing mode "Static" or "DHCP" or "Auto Configuration". If you select "DHCP" or "Auto Configuration", no further configuration is needed. If you select "Static", enter the relevant IP addressing information. (Fields marked with an asterisk (\*) are required.)

**IP Version Support**  IPv4 only  IPv4 and IPv6

Control(AP/DataPlane) Cluster **Management(Web)**

**IPv4**

Static  DHCP

IP Address \* 172.17.26.104

Netmask \* 255.255.254.0

Gateway 172.17.26.1

**IPv6**

Static  Auto Configuration

IP Address \* ::456/64

Gateway ::789

**Default Gateway** Management(Web) Management(Web)

**Primary DNS Server** 172.16.16.17 ::333

**Secondary DNS Server** 172.16.16.18 ::999

Version: 3.1.1.0.440 Upgrade < Back Apply >

- 6 Check the network settings that you have configured on the *Control*, *Cluster*, and *Management* tabs and the default gateway that you have selected. Verify that they are all correct.
- 7 Click the **Apply** to continue. The controller validates and applies the network settings that you have configured.

Figure 24. The controller validates and applies the network settings you have configured

**Ruckus Setup Wizard - SmartCell Gateway 200**

Language  
**Management IP**  
 Cluster Information  
 Administrator  
 Confirmation  
 Finish

**Management IP**  
 Select the network addressing mode "Static" or "DHCP" or "Auto Configuration". If you select "DHCP" or "Auto Configuration", no further configuration is needed. If you select "Static", enter the relevant IP addressing information. (Fields marked with an asterisk (\*) are required.)

IP Version Support  IPv4 only  IPv4 and IPv6

Control(AP/DataPlane) Cluster **Management(Web)**

IPv4  Static  DHCP  
 IPv6  Static  Auto Configuration

IP   
 Netmask \*   
 Gateway

Gateway

Default Gateway

Primary DNS Server    
 Secondary DNS Server

Version: 3.0.2.0.16

**CAUTION!** It may take the controller up to 15 minutes to activate its interfaces. If an error message appears after you apply the network interface settings, wait at least 15 minutes, and then try again.

**NOTE:** If the controller is unable to validate the network settings that you configured, an error message appears. If this happens, check the network settings that you configured and verify that you are able to connect to the IP address that you assigned to the *Management (Web)* interface.

- Update the IP address settings of the administrative computer with the same subnet settings that you assigned to the *Management (Web)* interface (see [Step 4](#)).

Continue to [Step 3: Configure the DataPlane IP Address Settings](#).

## Important Notes About Selecting the System Default Gateway

Depending on your network topology, you may select either the Management or Control interface as the system default gateway.

- If all of the managed APs are located in different locations on the Internet, the controller may not know all of the IP subnets of these APs. In this case, the control interface should be set as the default system gateway of the controller and you will need to add a static route to reach the management network.
- If all of the managed APs belong to a single subnet or to multiple subnets on which you can set the route statically, then you can set the management interface as the default gateway users can set default system gateway of the controller and set static routes for the controller to reach all of its managed APs.

## Step 3: Configure the DataPlane IP Address Settings

- 1 On the **DataPlane0** and **DataPlane1** tab, configure the IP address settings of DataPlane0 and DataPlane1, respectively.

**NOTE:** Although it is possible to use DHCP to assign IP address settings to the data plane interfaces automatically, Ruckus Wireless strongly recommends assigning static IP address to these interfaces.

The following network settings are required:

- IP address
- Netmask
- Default gateway

Figure 25. The DataPlane IP page

- 2 Click **Next** to continue. The *Cluster Information* page appears.



## Step 4: Configure the Cluster Settings

The actions that you need to perform in this step depends on whether you are creating a new cluster (with this controller as the first node) or you are setting up this controller to join an existing cluster.

- [If This Controller Is Forming a New Cluster](#)
- [If This Controller Is Joining an Existing Cluster](#)

**NOTE:** A SmartCell Gateway (SCG) 200 unit can only form a cluster with other SmartCell Gateway 200 units. It cannot join a cluster of SmartZone (SZ) 100 units (and vice versa).

Figure 26. The Cluster Information page

**RUCKUS** Setup Wizard - SmartCell Gateway 200

Language  
Management IP Address  
DataPlane IP  
**Cluster Information**  
Administrator  
Confirmation  
Configuration

**Cluster Information**

SCG Cluster Setting:

Cluster Name:

Controller Name:

Controller Description:

NTP Server:

AP Conversion  Convert ZoneDirector APs in factory settings to SmartCell Gateway 200 APs automatically

Choose the cluster that you would like to join.

Cluster List		
Cluster Name ↕	IP Address	Version

Ver. 3.1.1.0.440

## If This Controller Is Forming a New Cluster

Follow these steps if you want to use this controller to create a new cluster.

- 1 On the *Cluster Information* page, configure the following settings:
  - *Cluster Setting*: Select **New Cluster**.
  - *Cluster Name*: Type a name that you want to assign to this new cluster. The Cluster name must be a unique account with 4 nodes.

---

**CAUTION!** Ensure that the cluster name is a unique a/c in the available cluster-setups.

---

- *Controller Name*: Type a name for the controller in this new cluster. The Controller/Node name can be different for each.
- *Controller Description*: Type a description for the controller.
- *NTP Server*: Type the address of the NTP server from which members of the cluster will obtain and synchronize time. The default NTP server is `pool.ntp.org`.
- *AP Conversion*: Select the check box if you want ZoneFlex APs that are in factory default settings to be converted to SmartZone APs automatically when they are connected to the same subnet as the controller.

---

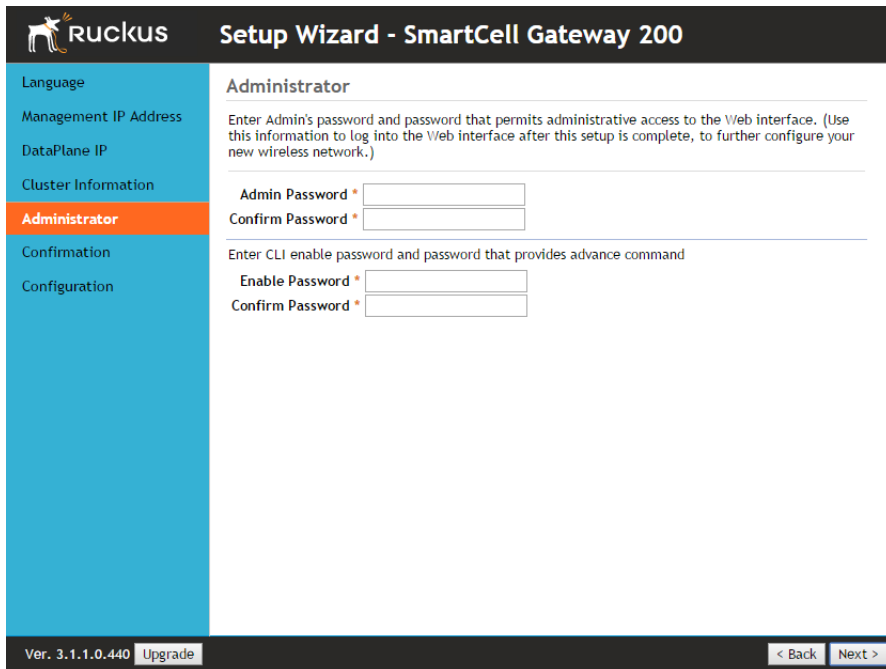
**CAUTION!** Before continuing, verify that the cluster settings are correct. Once the cluster is created, you will be unable to edit its settings without rebuilding the cluster from scratch.

---

- 2 Click **Next** to continue to the next Setup Wizard page. The *Administrator* page appears.
- 3 On the *Administrator* page, configure the web interface and CLI passwords. All fields are required.
  - *Admin Password*: Type a password that you want to use to access the web interface.
  - *Confirm Password*: Retype the password above to confirm.
  - *Enable Password*: Type a password that you want to use to enable CLI access to the controller.
  - *Confirm Password*: Retype the password above to confirm.
- 4 Click **Next** to continue. The *Confirmation* page appears and displays all the controller settings that you have configured using the Setup Wizard.

Continue to [Step 5: Verify the Settings](#).

Figure 27. Set the web interface and command line interface passwords



The screenshot displays the Ruckus Setup Wizard for a SmartCell Gateway 200. The interface is divided into a left-hand navigation menu and a main content area. The navigation menu includes options for Language, Management IP Address, DataPlane IP, Cluster Information, Administrator (which is currently selected and highlighted in orange), Confirmation, and Configuration. The main content area is titled "Administrator" and contains instructions: "Enter Admin's password and password that permits administrative access to the Web interface. (Use this information to log into the Web interface after this setup is complete, to further configure your new wireless network.)". Below this instruction are two input fields: "Admin Password \*" and "Confirm Password \*". A second set of instructions follows: "Enter CLI enable password and password that provides advance command". Below these are two more input fields: "Enable Password \*" and "Confirm Password \*". At the bottom of the screen, there is a footer bar containing the version number "Ver. 3.1.1.0.440", an "Upgrade" button, and navigation buttons for "< Back" and "Next >".

## If This Controller Is Joining an Existing Cluster

If this is not the first cluster on the network, you can set up this controller to join an existing cluster.

---

**CAUTION!** To add this controller to an existing cluster, the entire target cluster must be in a healthy state (no node must be in “out of service” state). If any member node is out of service, the join request will fail. You will need to remove any out-of-service node from the cluster before you can add a new node successfully.

---

Follow these steps to configure this controller to join an existing cluster.

- 1 Click the **Scan** button to display a list of existing clusters that this controller can join.

---

**NOTE:** The cluster discovery mechanism of the controller uses UDP port 7500. If a cluster exists on the network but the cluster list remains empty after the scan, verify that the switch to which the controller is connected does not block UDP packets and that UDP port 7500 is open on the switch.

---

- 2 When the list of clusters appears, click a cluster name to join. The *Cluster Setting* value changes to **Join Exist cluster**, and then the *Cluster Name* and *Join Exist SCG Cluster IP* boxes are populated with values from the cluster that this controller is joining. If you know the correct cluster name, you can specify the name to join.
- 3 Assign a name and description to this controller by filling out the *Controller Name* and *Controller Description* boxes.
- 4 Click **Next**.

---

**CAUTION!** When a Node is Out-of-Service, it cannot be removed gracefully from the cluster. Contact Ruckus Customer Support team to rectify this.

---

---

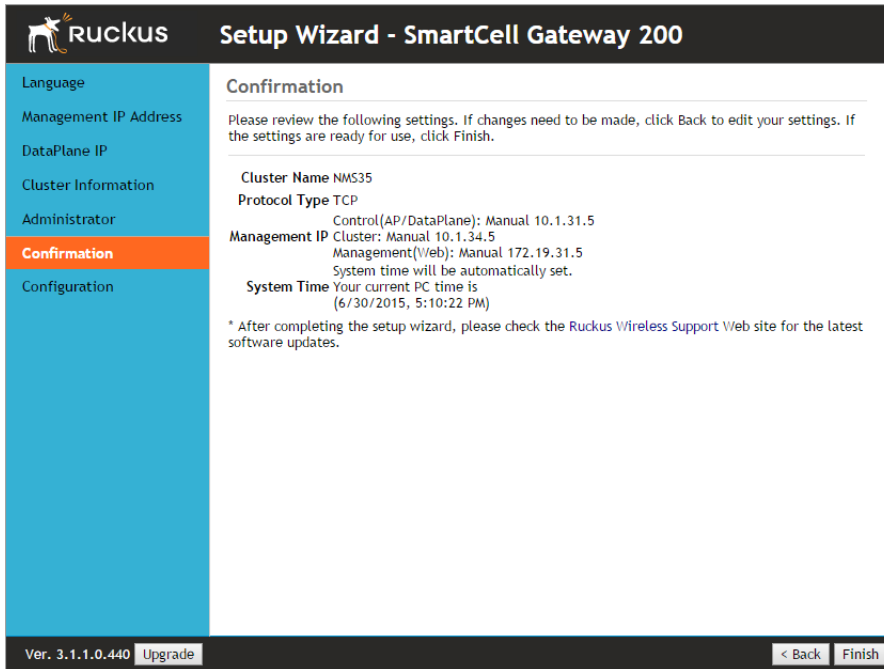
**NOTE:** If the firmware version on this controller (shown on the lower left area of the *Cluster Information* page) does not match the firmware version of the cluster, a message appears and prompts you to upgrade the controller firmware. Click **Upgrade**, and then follow the prompts to upgrade the controller to the firmware version of the cluster.

---

## Step 5: Verify the Settings

Verify that all the settings displayed on the *Confirmation* page are correct. If they are all correct, click **Finish** to apply the settings and activate the SCG on the network.

Figure 28. Verify that the settings displayed on the Confirmation page are correct



**NOTE:** If you find an incorrect setting, click the **Back** button until you reach the related page, and then edit the settings. When you finish editing the settings, click the **Next** button until you reach the *Confirmation* page again.

A progress bar appears and displays the progress of applying the settings, starting the SCG services, and activating the SCG on the network.

When the process is complete, the progress bar shows the message 100% Done. The page also shows the IP address through which you can access the SCG web interface to manage the controller.

Congratulations! You have completed the Setup Wizard. You are now ready to log on to the controller's web interface.

# Connecting Data Blades to the Network

Follow these steps to connect the data blades to the network.

- 1 Connect ETH2 to the router or switch.
- 2 Obtain two optical fiber (MMF) cables (not supplied).
- 3 Take one optical fiber cable, and then connect one SFP port on DataPlane0 to an SFP port on the 10GB router or switch.
- 4 Take the remaining optical fiber cable, and then connect one SFP port on DataPlane1 to another SFP port on the router or switch.

---

**NOTE:** The dataplane interfaces do not support auto negotiation and must therefore be connected to 10GB ports on a router or switch.

---

**NOTE:** For a list of SFP+ modules that the controller supports, see [Supported SFP+ Modules](#).

---

- 5 Connect ETH1 to another router or switch to which other controllers (if present) are connected.
- 

**NOTE:** Depending on your network setup, you may also connect ETH1 to the same router or switch to which ETH2 is connected.

---

## Supported SFP+ Modules

[Table 11](#) lists the SFP+ modules that the controller supports. For more information about these modules, visit the manufacturer's website.

Table 11. SFP+ modules supported by the SCG

Name	Product Code	Description
Intel Ethernet SFP+ SR (Short Range) Optics	E10GSFPSR	Dual Rate 10GBASE-SR/1000BASE-SX with duplex LC connector

# Logging On to the Web Interface

You can access the controller's web interface from any computer that is on the same subnet as the Management (Web) interface, which you configured in [Step 2: Configure the Management IP Address Settings](#).

Follow these steps to log on to the controller's web interface.

- 1 On a computer that is on the same subnet as the Management (Web) interface, start a web browser.
- 2 In the address bar, enter the IP address that you assigned to the Management (Web) interface and append a colon and 8443 (controller's management port number) at the end of the address.

For example, if the IP address that you assigned to the Management (Web) interface is 10.10.101.1, then you should enter:

https://10.10.101.1:8443

---

**NOTE:** While using HTTPS, as part of the security, the user is prompted to confirm that the IP is safe to continue with.

---

The controller's web interface logon page appears.

Figure 29. The controller's web interface logon page



- 3 Log on to the controller's web interface using the following logon details:
  - User Name: **admin**

- Password: **{the password that you set when you ran the SCG Setup Wizard}**

#### 4 Click **Log On**.

The web interface refreshes, and then displays the Dashboard page, which indicates that you have logged on successfully.

You are now ready to configure the controller.



# Configuring the SCG for the First Time

# 5

In this chapter:

- [Creating an AP Zone](#)
- [Configuring AAA Servers and Hotspot Settings](#)
- [Creating a Registration Rule](#)
- [Defining the WLAN Settings of an AP Zone](#)
- [Verifying That Wireless Clients Can Associate with a Managed AP](#)
- [What to Do Next](#)

## Creating an AP Zone

The first step in configuring the SCG is to create an AP zone. An AP zone functions as a way of grouping APs and applying a particular set of settings (including WLANs and their settings) to these groups of APs. Each AP zone can include up to six WLAN services.

A zone called `Staging Zone` exists by default. Any AP that registers with the SCG that is not assigned a specific zone is automatically assigned to the `Staging Zone`.

Follow these steps to create a new AP zone.

- 1 Click *Configuration > AP Zones*.
- 2 Click **Create New**.

---

**NOTE:** When you create a new AP Zone there is no **Change** button. A fresh installation of SCG does not contain all the other versions in the drop down list. Only for an upgrade, the user can choose from a drop down list containing all the AP firmware. However, Ruckus recommends that you install the latest firmware version.

---

Figure 30. Creating a new AP zone

**Create New AP Zone**

**General Options**

**Zone Name:** \*

**Description:**

**AP Firmware:** \* 3.1.0.0.253

**Country Code:**  United States

Different countries have different regulations on the usage of radio channels. To ensure that this zone is using an author select the correct country code for your location.

**Location:**  (example: Starbucks)

**Location Additional Information:**  (example: 460 N Mathilda Ave, Sunnyvale, CA, USA)

**GPS Coordinates:** Latitude:  , Longitude:  (example: 25.07858, 121.57141)

**AP Admin Logon:** \* Logon ID:  Password:

**Time Zone:**  System defined  User defined

(GMT+0:00) UTC

**AP IP Mode:**  IPv4 only  IPv6 only

**Mesh Options**

Enable mesh networking in this zone

**Radio Options**

**Radio Options b/g/n (2.4GHz)**

**Channelization:** \*  Auto

**Channel:** \*  Auto

**TX Power Adjustment:** \*  Full

**Radio Options a/n (5GHz)**

**Channelization:** \*  Auto

**Channel:** \* Indoor  Auto Outdoor  Auto

**TX Power Adjustment:** \*  Full

**AP GRE Tunnel Options**

**Tunnel Type:** \*  Ruckus GRE Support for APs behind NAT.

**Tunnel Profile:** \*  Default Tunnel Profile

3 Configure the options listed in [Table 12](#).

Table 12. Configuration options in the Create New Zone form

Option	Description
<i>General Options</i>	
Zone Name	Type a name that you want to assign to this new zone.
Description	Type a description for this new zone.

Table 12. Configuration options in the Create New Zone form (Continued)

Option	Description
AP Firmware	<p>Displays the latest AP firmware available on the SCG. If you want this zone to use a different firmware, click <b>Change</b>, and then select a firmware from the list. Ruckus recommends installing the latest firmware version. Once the latest version is upgraded, you can select it from the list.</p> <hr/> <p><b>NOTE:</b> If the SCG is fresh install user won't find other versions in the drop down list. There will not be a <b>Change</b> button to click.</p>
Country Code	<p>Different countries and regions maintain different rules that govern which channels can be used for wireless communications.</p> <p>Set the country code to the proper regulatory region ensures that your SCG network does not violate local and national regulatory restrictions.</p>
Location	Type a location name (for example, Ruckus Wireless HQ) for this AP zone
Location Additional Information	Type additional information about the AP zone (for example, 350 W Java Dr, Sunnyvale, CA 94089, United States).
GPS Coordinates	Type the longitude and latitude coordinates for the AP zone's location.
AP Admin Logon	<p>Specify the user name and password that administrators can use to log on directly to the managed access point's native web interface.</p> <p>The following boxes are provided:</p> <ul style="list-style-type: none"> <li>• <i>Logon ID</i>: Type the admin user name.</li> <li>• <i>Password</i>: Type the admin password.</li> </ul>

Table 12. Configuration options in the Create New Zone form (Continued)

Option	Description
Time Zone	<p>Specify the time zone that you want this AP zone to use by clicking one of the following options:</p> <ul style="list-style-type: none"> <li>• <b>System defined:</b> Click this option, and then select a time zone that you want to use.</li> <li>• <b>User defined:</b> Click this option, and then define the time zone settings (including the time zone abbreviation, GMT offset, and daylight saving time settings) that you want to use</li> </ul>
AP IP Mode	<p>Select the IP addressing mode that you want this AP zone to use. Options include <b>IPv4 Only</b>, <b>IPv6 Only</b> and <b>Dual</b>.</p>
<i>Mesh Options</i>	
Enable	<p>Select the <b>Enable mesh networking in this zone</b> check box if you want managed devices that belong to this zone to be able to form a mesh network automatically.</p>
<i>Radio Options</i>	
Radio Options b/g/n (2.4GHz)	<p>Configure the following 2.4GHz radio options:</p> <ul style="list-style-type: none"> <li>• <i>Channelization:</i> Select either 20MHz or 40MHz channel width.</li> <li>• <i>Channel:</i> Select Auto or manually assign a channel for the 2.4GHz radio.</li> <li>• <i>TX Power Adjustment:</i> Manually set the transmit power on all 2.4GHz radios (default is Full).</li> </ul>
Radio Options a/n/ac (5GHz)	<p>Configure the following 5GHz radio options:</p> <ul style="list-style-type: none"> <li>• <i>Channelization:</i> Select 20MHz, 40MHz, or 80MHz channel width.</li> <li>• <i>Channel (Indoor and Outdoor):</i> Select Auto or manually assign channels to the indoor and outdoor 5GHz radios.</li> <li>• <i>TX Power Adjustment:</i> Manually set the transmit power on all 5GHz radios (default is <b>Full</b>).</li> </ul>
<i>AP GRE Tunnel Options</i>	

Table 12. Configuration options in the Create New Zone form (Continued)

Option	Description
Tunnel Type	Select an option for tunneling WLAN traffic back to the controller: <ul style="list-style-type: none"> <li>• Ruckus GRE</li> <li>• SoftGRE</li> <li>• SoftGRE + IPsec</li> </ul>
Tunnel Profile	Select the tunnel profile that you want to use. If you want to use Ruckus GRE tunneling for this AP zone, you can use the default tunnel profile or you can select a profile that you created. If you want to use SoftGRE (or SoftGRE + IPsec) tunneling, you must first create a tunnel profile.  NOTE: Instructions for creating Ruckus GRE, SoftGRE, and SoftGRE + IPsec tunnel profiles are provided in the <i>Administrator Guide</i> .
Syslog Options	
	If you have a syslog server on the network and you want the SCG to send syslog data to it, select the <b>Enable external syslog server for APs in this zone</b> check box. The following boxes are provided: <ul style="list-style-type: none"> <li>• <i>IP Address</i>: Type the IP address of the syslog server.</li> <li>• <i>Port</i>: Type the port number that has been opened on the server for syslog data. The default port number is 514.</li> </ul>
Advanced Options	
Channel Mode	If you want to allow outdoor APs that belong to this zone to use wireless channels that are regulated as indoor use only, select the <b>Allow indoor channels</b> check box.
Background Scanning	If you want APs to automatically evaluate radio channel usage, enable and configure the background scanning settings on both the 2.4GHz and 5GHz radios.  By default, background scanning is enabled on both radios and set to run every 20 seconds.

Table 12. Configuration options in the Create New Zone form (Continued)

Option	Description
Smart Monitor	<p>To disable the WLANs of an AP (that belongs to this zone) whenever the AP uplink or Internet connection becomes unavailable, select the <b>Enable</b> check box. And then, configure the following options:</p> <ul style="list-style-type: none"> <li>• <i>Health Check Interval</i>: Set the interval (between 5 and 60 seconds) at which the SCG will check the AP's uplink connection. The default value is 10 seconds.</li> <li>• <i>Health Check Retry Threshold</i>: Set the number of times (between 1 and 10 times) that the SCG will check the AP's uplink connection. If the SCG is unable to detect the uplink after the configured number of retries, the SCG will disable the AP's WLANs. The default value is 3 retries.</li> </ul> <p>NOTE: When the SCG disables the AP's WLANs, the AP creates a log for the event. When the AP's uplink is restored, the AP sends the event log (which contains the timestamp when the WLANs were disabled, and then enabled) to the SCG.</p>
VLAN Pooling	<p>Select the <b>Allow VLAN Pooling overlapping</b> check box to enable VLAN pooling.</p>
Rogue AP Detection	<p>A rogue access point is any access point detected by an SCG-managed access point that is not part of the SCG network. To gain visibility into the presence of rogue access points on the network, select the <b>Report rogue access points</b> check box, and then click one of the following options:</p> <ul style="list-style-type: none"> <li>• <i>Report all rogue devices</i></li> <li>• <i>Report only malicious devices of the selected types</i> (and then select the types of malicious AP categories to report)</li> </ul>

Table 12. Configuration options in the Create New Zone form (Continued)

Option	Description
Client Load Balancing	Improve WLAN performance by enabling load balancing. Load balancing spreads the wireless client load between nearby access points, so that one AP does not get overloaded while another sites idle. Load balancing must be enabled on a per-radio basis. To enable load balancing, select the <b>Enable load balancing on [2.4GHz or 5GHz]</b> check box, and then set or accept the default <i>Adjacent Radio Threshold</i> (50dB for the 2.4GHz radio and 43dB for the 5GHz radio).
Band Balancing	Client band balancing between the 2.4GHz and 5GHz radio bands is disabled by default on all WLANs. To enable band balancing for this WLAN, select the <b>Enable band balancing on radios by distributing the clients on 2.4GHz and 5GHz bands</b> check box, and then set the percentages of client load that will be distributed between the 2.4GHz and 5GHz bands.
Location Based Services Options	Select the <b>Enable LBS service</b> check box to enable LBS on the SCG, and then select an LBS server from the list below.
Client Admission Control	Set the load thresholds on the AP at which it will stop accepting new clients
AP Reboot Timeout	Set the time after which the AP will reboot automatically when it is unable to reach the default gateway or the control interface. <ul style="list-style-type: none"> <li>• <b>Reboot AP if it cannot reach default gateway after:</b> Set the time after which the AP will reboot if it is unable to communicate with the default gateway. The default timeout is 30 minutes.</li> <li>• <b>Reboot AP if it cannot reach SCG after:</b> Set the time after which the AP will reboot if it is unable to communicate with the SCG. The default timeout is 2 hours.</li> </ul>

- 4 Click **OK** to finish creating your first AP zone. When the controller completes creating the AP zone, the following confirmation message appears:



AP zone created successfully. Do you want to view the zone information?

- 5 Click **Yes** to view the zone details, or click **No** to close the confirmation message and return to the zone list.

You have completed creating your first AP zone. You can create additional AP zones, if needed.

## Configuring AAA Servers and Hotspot Settings

---

**NOTE:** If you do not have an AAA server on the network, skip this step.

---

If you have an existing RADIUS (AAA) server on the network, you can set up hotspot services across the network using the Ruckus Wireless access points that the SCG is managing. To provide hotspot services, you need to add at least one AAA server to the SCG and create a hotspot service.

AAA servers and hotspot settings must be configured on a per-AP zone basis.

### Adding an AAA Server

Follow these steps to add an AAA server to an AP zone.

- 1 Go to *Configuration > AP Zones*.
- 2 Click the AP zone for which you want to add an AAA server. Alternatively, click the AP zone from the *Management Domains* tree.
- 3 Under the *AP Zones* menu on the sidebar, click **AAA**.
- 4 Click **Create New**. The *Create New RADIUS Server* form appears.
- 5 In the *General Options* section, configure the following settings:
  - *Name*: Type a name for the AAA server that you are adding.
  - *Description*: Type a description for the AAA server that you are adding.
  - *Type*: Click either **RADIUS** or **RADIUS Accounting**, depending on the type of RADIUS server that you are using. Click **RADIUS Accounting** to add an accounting server (All the other steps are the same as for the authentication server).
  - *Backup RADIUS*: If a backup RADIUS server exists on the network, you may enable RADIUS backup support by selecting the **Enable backup RADIUS support** check box.

- 6 Configure the options in the *Health Check Policy* section. These options define the health monitoring settings of the primary RADIUS server by the secondary RADIUS server. The secondary RADIUS is responsible for monitoring the health of the primary RADIUS and for periodically synchronizing its settings to match those of the primary RADIUS.
  - *Response Window*: Set the time (in seconds) during which the secondary RADIUS must wait for a response from the primary RADIUS. If the secondary RADIUS does not receive a response during the defined Response Window, the Zombie Period (see below) is started for the primary RADIUS. The default Response Window is 20 seconds.
  - *Zombie Period*: Set the time (in seconds) during which the secondary RADIUS must wait for a response from the primary RADIUS before marking it as “down”. If the secondary RADIUS does not receive a response during the defined Zombie Period, the Revive Interval (see below) is started for the primary server. The default Zombie Period is 40 seconds. If the primary RADIUS still does not respond when the Zombie Period expires, it will be marked as down and the secondary RADIUS will start receiving new requests from the Network Access Server (NAS).
  - *Revive Interval*: Set the time (in seconds) during which the secondary RADIUS must wait for the primary RADIUS to start responding to requests again. If the primary RADIUS starts responding before the Revive Interval expires, new requests will be forwarded to the primary RADIUS again. The default Revive Interval is 120 seconds.
  - *No Response Fail*: Click Yes to respond with a reject message to the NAS if no response is received from the RADIUS server. Click No to skip sending a response.
- 7 In the *Primary Server* section, configure the following settings:
  - *IP Address*: Type the IP address of the AAA server.
  - *Port*: Type the AAA port number. The default AAA port number is 1812.
  - *Shared Secret*: Type the AAA shared secret.
  - *Confirm Secret*: Retype the AAA shared secret that you typed above.
- 8 If you selected the **Enable backup RADIUS support** check box, the *Secondary Server* section is visible. Configure the following *Secondary Server* settings:
  - *IP Address*: Type the IP address of the secondary AAA server.
  - *Port*: Type the AAA port number. The default AAA port number is 1812.
  - *Shared Secret*: Type the AAA shared secret.

- *Confirm Secret*: Retype the AAA shared secret that you typed above.
- 9 Click **OK**. The following message appears to confirm that you have successfully added the AAA server to the SCG:

Authentication server created successfully.

The page refreshes, and then the AAA server that you created appears under the *AAA Servers Configuration* section.

Figure 31. The Create New RADIUS Serve form

The screenshot shows the 'Create New RADIUS Server' form within the 'AP Zone: ZONE-1 >> AAA Servers' section. The form is divided into several sections:

- General Options:**
  - Name: RADIUS-Server
  - Description: RADIUS Auth
  - Type:  RADIUS  RADIUS Accounting  Active Directory  LDAP
  - Backup RADIUS:  Enable Secondary Server
- Primary Server:**
  - IP Address: 134.0.0.4
  - Port: 1812
  - Shared Secret: .....
  - Confirm Secret: .....
- Secondary Server:**
  - IP Address: 134.0.0.7
  - Port: 1812
  - Shared Secret: .....
  - Confirm Secret: .....

At the bottom of the form are 'OK' and 'Cancel' buttons.

## Creating a Hotspot (WISPr) Service

**NOTE:** If you do not want to provide a Hotspot (WISPr) service to users, skip this step.

**NOTE:** Before creating a hotspot, you need to create a user defined interface. For information on how to create a user defined interface, see the *Administrator Guide*.

A hotspot service requires an AAA server. Before creating a hotspot service, make sure you have already added an AAA server to the SCG. For more information, refer to [Adding an AAA Server](#).

Follow these steps to create a hotspot service for an AP zone.

- 1 Go to **Configuration > AP Zones**.
- 2 Click the AP zone for which you want to create a Hotspot service. Alternatively, click the AP zone from the *Management Domains* tree.
- 3 Under the *AP Zones* menu on the sidebar, click **WISPr (Hotspot)**.
- 4 Click **Create New**. The *Create New Hotspot Service* form appears.
- 5 Configure the hotspot service settings listed in [Table 13](#).

Table 13. Hotspot (WISPr) service settings

Setting	Description
General Options	
Name	Type a name for this new Hotspot service that you are creating.
Description	Type a description for this new Hotspot service (for example, <code>Main Office Lobby</code> ).
Redirection	
Smart Client Support	<ul style="list-style-type: none"> <li>• <b>None:</b> Click to disable Smart Client support.</li> <li>• <b>Enable:</b> Click to enable Smart Client support.</li> <li>• <b>Only Smart Client allowed:</b> Click to allow only Smart Clients to access this hotspot service.</li> </ul>
Logon URL	Type the URL of the subscriber portal (the page where hotspot users can log in to access the service). For more information, see the section “Configuring the Logon URL” in the <i>Administrator Guide</i> .
Redirected MAC Format	Enter the format used to include the client's MAC address inside the redirected URL request.

Table 13. Hotspot (WISPr) service settings (Continued)

Setting	Description
Start Page	Set where users will be redirected after logging in successfully. You could redirect them to the page that they want to visit, or you could set a different page where users will be redirected (for example, your company website).
<b>User Session</b>	
Session Timeout	Set a time limit after which users will be disconnected from the hotspot service and required to log on again. Allowed session timeout range is between 2 and 14400 minutes. The default value is 1440 minutes.
Grace Period	Allow disconnected users a grace period after disconnection, during which clients will not need to re-authenticate. Allowed grace period range is between 1 and 14399 minutes. The default value is 60 minutes.
<b>Location Information</b>	
Location ID	Type a location ID for the hotspot, for example: isocc=us,cc=1,ac=408,network=ACMEWISP _NewarkAirport
Location Name	Type a location name for the hotspot, for example: ACMEWISP,Gate_14_Terminal_C_of_Newark _Airport

Table 13. Hotspot (WISPr) service settings (Continued)

Setting	Description
Walled Garden	<p>Click <b>Create New</b> to add a walled garden, which is a limited environment to which an unauthenticated user is given access for the purpose of setting up an account. In the box provided, type a URL or IP address to which you want to grant unauthenticated users access. You can add up to 128 network destinations to the walled garden. Network destinations can be any of the following:</p> <ul style="list-style-type: none"> <li>• IP address (for example, 10.11.12.13)</li> <li>• Exact website address (for example, <code>www.ruckuswireless.com</code>)</li> <li>• Website address with regular expression (for example, <code>*.ruckuswireless.com, *.com, *</code>)</li> </ul> <p>After the account is established, the user is allowed out of the walled garden. URLs will be resolved to IP addresses. Users will not be able to click through to other URLs that may be presented on a page if that page is hosted on a server with a different IP address.</p> <p>Avoid using common URLs that are translated into many IP addresses (such as <code>www.yahoo.com</code>), as users may be redirected to re-authenticate when they navigate through the page.</p>

**6 Click Create New.**

The page refreshes, and then the Hotspot that you created appears under the *WISPr (Hotspot) Configuration* section.

Figure 32. The Create New Hotspot Service form

The screenshot displays the configuration page for 'AP Zone: ZONE-1 >> Hotspot (WISPr) Portal'. The left sidebar shows a navigation menu with 'Hotspot (WISPr)' selected. The main content area shows a table with one entry, 'WISPr', and an 'Edit Hotspot Portal' form. The form includes sections for 'General Options' and 'Redirection'.

**General Options:**

- Portal Name: \* WISPr
- Portal Description: [Empty field]

**Redirection:**

- Smart Client Support:
  - None
  - Enable
  - Only Smart Client Allowed
- Logon URL:
  - Internal
  - External
- Redirected MAC Format: \* AA:BB:CC:DD:EE:FF (format used for including client's MAC inside)
- Start Page:
  - After user is authenticated, Redirect to the URL that user intends to visit.
  - Redirect to the following URL:

## Creating a Registration Rule

Registration rules enable the SCG to assign an AP to an AP zone automatically based on the rule that the AP matches.

Follow these steps to create a registration rule.

- 1 Go to **Configuration > AP Zones**.
- 2 On the sidebar on the left, click **AP Registration Rules**. The *AP Registration Rules* page appears.
- 3 Click **Create New**. A form appears.
- 4 In *Rule Description*, type a name that you want to assign to this rule.
- 5 In *Rule Type*, click the basis upon which you want to create the rule. Options include:

- *IP Address*: If you select this option, type the *From* (starting) and *To* (ending) IP address that you want to use.
- *Subnet Mask*: If you select this option, type the IP address and subnet mask pair to use for matching.
- *GPS Coordinates*: If you select this option, type the GPS coordinates to use for matching. Access points that have been assigned the same GPS coordinates will be automatically assigned to the AP zone that you will choose in the next step.
- *Provision Tag*: If the access points that are joining the SCG have been configured with provision tags, click the **Provision Tag** option, and then type a tag name in the *Provision Tag* box. Access points with matching tags will be automatically assigned to the AP zone that you will choose in the next step.

---

**NOTE:** Provision tags can be configured on a per-AP basis from the access point's command line interface.

---

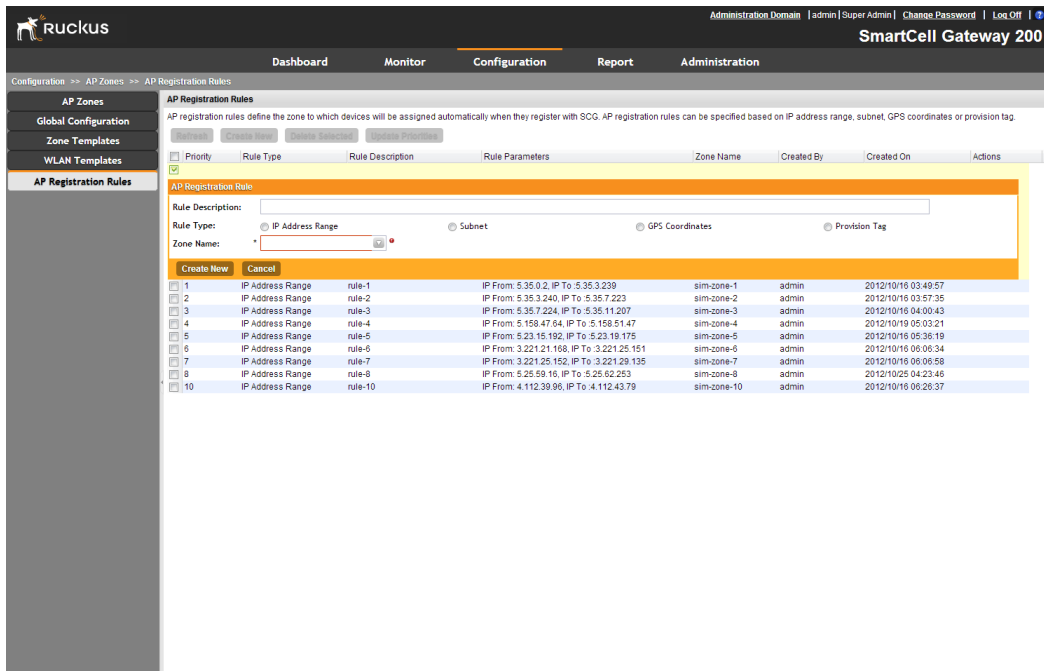
**6** In *Zone Name*, click the drop-down list to display available AP zones, and then click an AP zone to which APs that match this rule will be assigned.

**7** Click **OK**.

You have completed creating an AP registration rule.



Figure 33. Creating an AP registration rule



To create another registration rule, repeat the preceding steps. You can create as many registration rules as you need to manage access points on the network.

## Configuring the Rule Priority

The SCG applies registration rules in the same order as they appear in the AP Registration Rules table (highest to lowest priority). If you want a particular registration rule to have higher priority, you must move it up the table. Once an AP matches a registration rule, the SCG assigns the AP to the zone specified in the rule and stops processing the remaining rules.

Follow these steps to configure the rule priority.

- 1 Go to **Configuration > AP Zones**.
- 2 On the sidebar on the left, click **AP Registration Rules**. The AP Registration Rules page appears and displays the rules that you have created.
- 3 Change the priority of each registration rule as required.



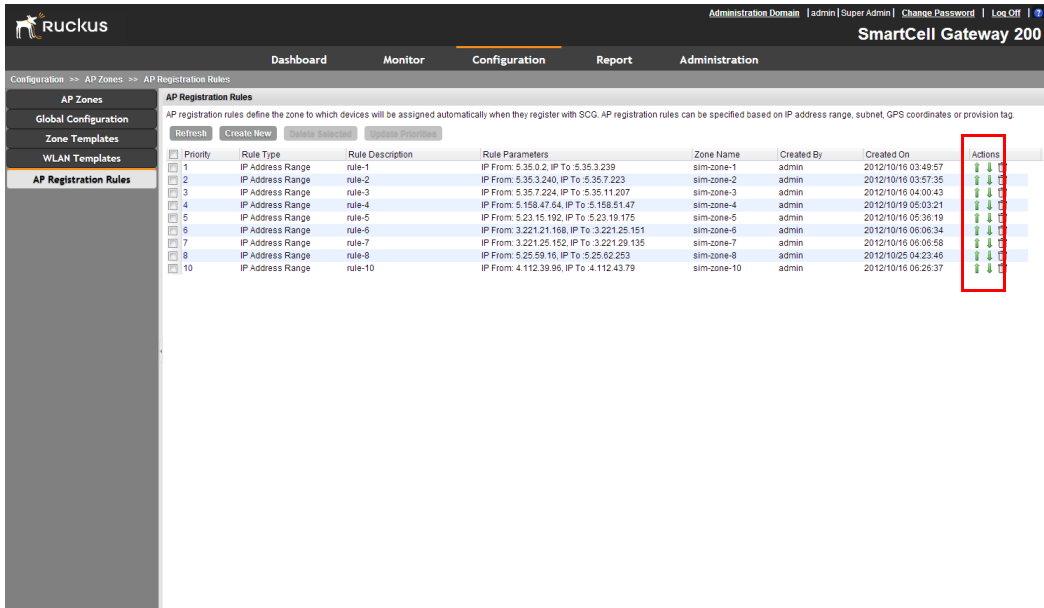
- To give a rule higher priority, move it up the table by clicking the  (up-arrow) icon that is in the same row as the rule name.
  - To give a rule lower priority, move it down the table by clicking the  (down-arrow) icon that is in the same row as the rule name.
- 4 When you finish configuring the rule priority, click **Update Priorities** to save your changes.

Figure 34. Change the rule priority by clicking the up-arrow or down-arrow



## Defining the WLAN Settings of an AP Zone

Follow these steps to configure the WLAN settings of an AP zone.

- 1 Go to **Configuration > AP Zones**.
- 2 Click the AP zone for which you want to add the WLAN settings. Alternatively, click the AP zone from the *Management Domains* tree.
- 3 Under the *AP Zones* menu on the sidebar, click **WLAN**.
- 4 Click **Create New**. The *Create New WLAN Configuration* form appears.

- 5 Configure the WLAN settings listed in [Table 14](#). You can find a detailed description of each setting in the succeeding sections.

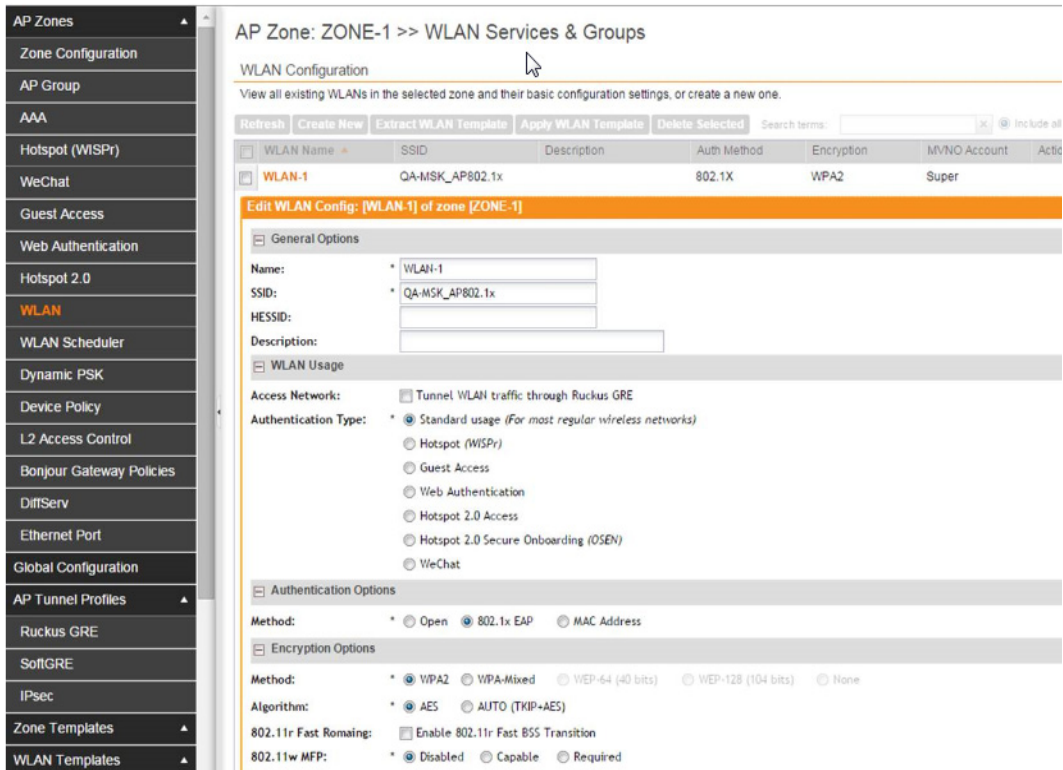
Table 14. Overview of WLAN settings

WLAN Setting	Description
General Options	Enter the WLAN name and description. See <a href="#">General Options</a> .
WLAN Usage	Select the usage type (standard WLAN or hotspot). See <a href="#">WLAN Usage</a> .
Authentication Options	Select an authentication method for this WLAN (open or 802.1X EAP). See <a href="#">Authentication Options</a> .
Encryption Options	Select an encryption method (WPA, WPA2, WPA Mixed), encryption algorithm (AES or TKIP) and enter a WPA passphrase. See <a href="#">Encryption Options</a> .
Authentication & Accounting Service	This section only appears when certain authentication options are selected. See <a href="#">Authentication &amp; Accounting Service</a> .
Options	Select whether web-based authentication (captive portal) will be used, and which type of authentication server will be used to host credentials (local database, Active Directory, RADIUS, LDAP). Also, enable or disable Wireless Client Isolation, Zero-IT Activation, Dynamic PSK and Priority for this WLAN. See <a href="#">Options</a> .
Advanced Options	Select an accounting server and configure ACLs, rate limiting, VLAN/dynamic VLAN settings, tunneling, background scanning, maximum client threshold, and service schedule. See <a href="#">Advanced Options</a> .

- 6 Click **OK** to finish creating the WLAN service.

You have completed creating your first WLAN. To create another WLAN, repeat [Step 4](#) to [Step 6](#). You can create up to six WLANs per AP zone.

Figure 35. Configuring the WLAN settings of an AP zone



## General Options

- **Name/ESSID:** Type a short name (2-31 characters) for this WLAN. In general, the WLAN name is the same as the advertised SSID (the name of the wireless network as displayed in the client's wireless configuration program). However, you can also separate the ESSID from the WLAN name by entering a name for the WLAN in the first field, and a broadcast SSID in the second field. In this way, you can advertise the same SSID in multiple locations (controlled by the same SCG) while still being able to manage the different WLANs independently. Each WLAN "name" must be unique within the SCG, while the broadcast SSID can be the same for multiple WLANs.
- **Description:** Enter a brief description of the qualifications or purpose of this WLAN (for example, Engineering or Voice).

## WLAN Usage

- In *Access Network*, select the Tunnel WLAN traffic to SCG check box if you want to tunnel the traffic from this WLAN back to the SCG. Tunnel mode enables wireless clients to roam across different APs on different subnets. If the WLAN has clients that require uninterrupted wireless connection (for example, VoIP devices), Ruckus Wireless recommends enabling tunnel mode. When you enable this option, you need to select core network for tunneling WLAN traffic back to the SCG.
- In *Authentication Type*, click one of the following options:
  - **Standard usage (For most regular wireless networks):** This is a regular WLAN suitable for most wireless networks.
  - **Hotspot service (WISPr):** Click this option if want to use a hotspot (WISPr) service that you previously created.
  - **Guest Access + Hotspot 2.0 Onboarding:** Click this option if you want guest users to use this WLAN and offer Hotspot 2.0 service to guest users.
  - **Web Authentication:** Click this option if you want to require all WLAN users to complete a web-based logon to this network every time they attempt to connect.
  - **Hotspot 2.0 Access:** Click this option if you want a Hotspot 2.0 operator profile that you previously created to use this WLAN. See the *Hotspot 2.0 Reference Guide* for this release.
  - **Hotspot 2.0 Secure Online Signup (OSEN):** Click this option if you want to use this WLAN for Hotspot 2.0 OSEN. See the *Hotspot 2.0 Reference Guide* for this release for more information.

## Authentication Options

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

- *Open [Default]:* No authentication mechanism is applied to connections. If WPA or WPA2 encryption is used, this implies WPA-PSK authentication.
- *802.1X/EAP:* Uses 802.1X authentication against a user database.

---

**NOTE:** For proxy and non-proxy cases, 802.1x is disabled for authentication and accounting with WISPr. You can choose AAA from the zone within which the WLAN is configured.

---

- *MAC Address*: Uses the MAC address of a client for authentication. MAC address authentication requires a RADIUS server and uses the MAC address as the user logon name and password. You have two options for the MAC address format to use for authenticating clients:
  - Use user defined text as authentication password (default is device MAC address)
  - Set device MAC address in 802.1x format 00-10-A4-23-19-C0. The default is 0010a42319c0.

## Encryption Options

Encryption choices include WPA2, WPA-Mixed, WEP-64, WEP-128, and none.

### Method

- *WPA2*: Enhanced WPA encryption using the stronger AES encryption algorithm.
- *WPA-Mixed*: Use this setting if your network has a mixture of older clients that only support AES and Auto (TKIP + AES).
- *WEP-64*: Provides a lower level of encryption, and is less secure, using 40-bit WEP encryption.
- *WEP-128*: Provides a higher level of encryption than WEP-64, using a 104-bit key for WEP encryption. However, WEP is inherently less secure than WPA.
- *None*: No encryption; communications are sent in clear text.

---

**CAUTION!** If you set the encryption method to WEP-64 (40 bit) or WEP-128 (104 bit) and you are using an 802.11n AP for the WLAN, the AP will operate in 802.11g mode.

---

### Algorithm (For WPA2 Encryption Only)

- *TKIP*: This algorithm provides greater compatibility with older client devices, but retains many of the security weaknesses of WEP. Therefore, if you select TKIP encryption, 11n devices will be limited to 11g transfer rates. Furthermore, the Wi-Fi Alliance will be mandating the removal of TKIP, so it should not be used.
- *AES*: This algorithm provides enhanced security over TKIP, and is the only encryption algorithm supported by the 802.11i standard. Choose AES encryption if you are confident that all of your clients will be using 802.11i-compliant NICs.
- *Auto*: Automatically selects TKIP or AES encryption based on the client's capabilities. Note that since it is possible to have clients using both TKIP and AES on the same WLAN, only unicast traffic is affected (broadcast traffic must fall back to TKIP; therefore, transmit rates of broadcast packets from 11n APs will be at lower 11g rates).

---

**CAUTION!** If you set the encryption algorithm to TKIP and you are using an 802.11n AP for the WLAN, the AP will operate in 802.11g mode.

---

---

**CAUTION!** If you set the encryption algorithm to TKIP, the AP will only be able to support up to 26 clients. When this limit is reached, additional clients will be unable to associate with the AP. On the other hand, if you select AES or none, the AP will be able to support up to 256 clients (fewer if wireless mesh is also enabled on the same radio).

---

## Authentication & Accounting Service

- *Authentication Service:* This option appears only when 802.1x EAP is selected as the authentication method. Select the authentication server that you want to use for this WLAN. Only AAA servers that you previously added appear here.
- *Accounting Service:* This option appears only when 802.1x EAP is selected in Authentication method. Additionally, you must have added a RADIUS Accounting server previously. Select the RADIUS Accounting server from the drop-down list, as a proxy for SCG.

For Authentication and Accounting Services, in the case of Hotspot WISPr, though 802.1x is disabled, the user can still select AAA from the configured zone. This is also applicable for proxy and non-proxy cases.

## Options

- *Wireless Client Isolation:* This option appears only when Standard Usage is selected as the WLAN usage type. Wireless client isolation enables subnet restrictions for connected clients. Click Enable if you want to prevent wireless clients associated with the same AP from communicating with each other locally. The default value is Disable.
- *Priority:* Set the priority of this WLAN to Low if you would prefer that other WLAN traffic takes priority. For example, if you want to prioritize internal traffic over guest WLAN traffic, you can set the priority in the guest WLAN configuration settings to “Low.” By default, all WLANs are set to high priority.

## RADIUS Options

---

**NOTE:** The *RADIUS Options* section only appears when *Authentication Type* (under *WLAN Usage*) is set to **Standard usage (For most regular wireless networks)**.

---

- *RADIUS NAS ID:* Select how the RADIUS server will identify the AP:
  - WLAN BSSID



- AP MAC
- User-defined
- *RADIUS NAS Request Timeout*: Type the timeout period (in seconds) after, which an expected RADIUS response message is considered to have failed.
- *RADIUS NAS Max Number of Retries*: Type the number of failed connection attempts after which the SCG will fail over to the backup RADIUS server.
- *RADIUS NAS Reconnect Primary*: If the SCG fails over to the backup RADIUS server, this is the interval (in minutes) at which the SCG will recheck the primary RADIUS server if it is available. The default interval is 5 minutes.
- *Call STA ID*: Use either WLAN BSSID or AP MAC as the station calling ID. Select one.

## Advanced Options

- *User Traffic Profile*: If you want this WLAN to use a user traffic profile that you previously created, select it from the drop-down menu. Otherwise, select **System Default**.
- *L2 Access Control*: If you want this WLAN to use an L2 access control policy that you previously created, select it from the drop-down menu. Otherwise, select **Disable**.
- *Device Policy*: If you want this WLAN to use a device policy that you previously created, select it from the drop-down menu. Otherwise, select **Disable**.
- *Client Load Balancing*: To disable client load balancing on this WLAN, select the **Do not perform client load balancing for this WLAN service** check box.
- *OFDM Only*: Select the check box to force clients associated with this WLAN to use only Orthogonal Frequency Division Multiplexing (OFDM) to transmit data. OFDM-only allows the client to increase management frame transmission speed from CCK rates to OFDM rates. This feature is implemented per WLAN and only affects the 2.4GHz radio.
- *BSS Min Rate*: Select this check box to set the BSS rates of management frames from default rates (CCK rates for 2.4G or OFDM rate – 6Mbps for 5G] to the desired rates. By default, BSS Min Rate is disabled.

---

**NOTE:** OFDM-only takes higher priority than BSS-minrate. However, OFDM-only relies on BSS-minrate to adjust its rate for management frames.

---

- *Mgmt Tx Rate*: To set the maximum transmit rate for management frame, select a value (in Mbps) from the drop-down list.
- *Service Schedule*: Use the Service Schedule tool to control which hours of the day, or days of the week to enable/disable WLAN service. Options include:
  - **Always On**: Click to enable this WLAN at all times.
  - **Always Off**: Click to disable this WLAN service at all times.
  - **Specific**: Click to set specific hours during which this WLAN will be enabled. For example, a WLAN for student use at a school can be configured to provide wireless access only during school hours. Click on a day of the week to enable/disable this WLAN for the entire day. Colored

cells indicate WLAN enabled. Click and drag to select specific times of day. You can also disable a WLAN temporarily for testing purposes, for example.

---

**NOTE:** The service schedule feature will not work properly if the controller does not have the correct time. To ensure that the controller always maintains the correct time, point the controller to an NTP server's IP address, as described in the section *Configuring the System Time*, of the *SCG vSZ-H Administrator Guide*.


---


- *Band Balancing:* Client band balancing between the 2.4GHz and 5GHz radio bands is disabled by default on all WLANs. To disable band balancing for this WLAN only (when enabled globally), select the **Do not perform band balancing for this WLAN service** check box.

## Verifying That Wireless Clients Can Associate with a Managed AP

The last step in the SCG setup process is to verify that APs can register with the SCG and that wireless clients can associate with the APs successfully.

Follow these steps to verify that wireless clients can connect to the network.

- 1 Verify that the SCG is connected to the backbone network.
- 2 Physically connect an AP to the same network as the SCG. If DHCP option 43 was configured correctly, this AP should be able to locate the SCG on the network and to register with it successfully.
- 3 Check the SCG Dashboard. The AP zone that you created earlier should have at least one member AP (the AP that you connected to the network in [Step 2](#)). The AP count appears green, which indicates that it is online.
- 4 Associate a wireless client with the AP. The following describes the procedure if you are using a Windows-based wireless client.
  - a In the system tray, right-click the  (Wireless Network Connection) icon, and then click **View Available Wireless Networks**.
  - b In the list of available wireless network, click the wireless network name (SSID) that you configured on the AP.
  - c Click **Connect**.

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

- 5 Start your web browser, and then enter `www.ruckuswireless.com` in the address bar.

If you are able to connect to the Ruckus Wireless website, you have completed setting up the SCG on the network. Congratulations!

## What to Do Next

For more information on configuring and managing the SCG, refer to the *SmartCell Gateway 200 Administrator Guide*, which is available for download on the Ruckus Wireless Support website at <http://support.ruckuswireless.com>.

---

**NOTE:** For a complete list of documentation that is available for this SCG release, refer to the *Release Notes*.

---

# Ensuring That APs Can Discover the Controller on the Network

# 6

Before the controller can start managing an AP, the AP must first be able to discover the controller on the network when it boots up. This chapter describes procedures that you can perform to ensure that APs can discover and register with the controller on the network.

In this chapter:

- [Is LWAPP2SCG Enabled on the Controller?](#)
- [Method 1: Perform Auto Discovery of the Controller Using the SmartLicense Server](#)
- [Method 2: Perform Auto Discovery on Same Subnet, then Transfer the AP to Intended Subnet](#)
- [Method 3: Register the Controller with the DNS Server](#)
- [Method 4: Configure DHCP Option 43 on the DHCP Server](#)
- [Method 5: Manually Configure the Controller Address on the AP's Web Interface](#)

## Is LWAPP2SCG Enabled on the Controller?

All of the controller discovery methods described in this chapter require LWAPP2SCG (the application that enables APs to discover and be managed by a controller) to be installed and enabled on the controller. See [Table 15](#) to check if your controller release includes the LWAPP2SCG application and whether it is enabled or disabled by default.

Table 15. LWAPP2SCG availability on each controller release

Controller Release	LWAPP Discovery	Default Setting	AP Compatibility
SCG 1.1.2, 2.1.2	Application installed by administrator. See <a href="#">Obtaining the LWAPP2SCG Application</a> .	Disabled	<ul style="list-style-type: none"> <li>• ZF-AP Release 9.6.x – 9.8.x</li> <li>• AP Release 100.0.x and later</li> </ul>
SCG 2.5.x	Enabled by administrator. See <a href="#">Enabling LWAPP2SCG</a> .	Disabled	
SCG 2.6.x	Enabled by administrator. See <a href="#">Enabling LWAPP2SCG</a> .	Disabled	<ul style="list-style-type: none"> <li>• ZF-AP Release 9.7.x – 9.8.x</li> </ul>
Release 3.0.x	Enabled by default	Enabled	<ul style="list-style-type: none"> <li>• AP Release 100.0.x and greater</li> </ul>

### Obtaining the LWAPP2SCG Application

If your controller release does not have the LWAPP2SCG application pre-installed, contact Ruckus Wireless Support to obtain a copy of the LWAPP2SCG application files and installation instructions.

### Enabling LWAPP2SCG

If the LWAPP2SCG application is pre-installed but disabled in your controller release, do the following to enable it:

- 1 Log on to the controller's console.
- 2 Enter **en** to enable privileged mode.
- 3 Enter **config**.
- 4 Enter **lwapp2scg**.
- 5 Enter **policy accept-all**.

You have completed enabling the LWAPP2SCG application on the controller.

# Method 1: Perform Auto Discovery of the Controller Using the SmartLicense Server

---

**NOTE:** This guide assumes that you have already activated the controller's licenses on the SmartLicense server.

---

The Ruckus Wireless SmartLicense registration server is a cloud-based, HTTPS-enabled web server that allows an access point to query information about its parent controller by sending its serial number and base MAC address.

---

**NOTE:** If you do not want to (or cannot) use the cloud-based SmartLicense registration server, you can install a local version of the registration server (called the Local License Server). For more information, see the *Local License Server User Guide*.

---

After you ensure that the controller's licenses have been activated on the SmartLicense server, you only need to connect the AP to the network, ensure that it has Internet connectivity, and then reboot the AP. Upon reboot, the AP will automatically attempt to discover its parent controller by sending the following HTTPS query to `ap-registrar.ruckuswireless.com` (the SmartLicense server URL):

```
https://ap-registrar.ruckuswireless.com/  
controller?ap_mac=APMAC&ap_serial=APSERIAL
```

where APMAC is the AP's MAC address (for example, APMAC: 74:91:1A:20:59:90) and APSERIAL (for example, APSERIAL: 311003001685) is the AP's serial number, both of which are printed on the AP's product label.

If the AP is unable to discover its parent controller after the first attempt, it will continue to do so:

- Once every 5 minutes for up to 60 minutes (12 queries)
- Once every hour for the remaining day (23 queries)
- Once every 24-hour for the remaining two weeks (12 queries)

If the AP is still unable to discover its parent controller after two weeks of uptime, this cloud-based controller discovery method will be disabled permanently. You will need to reset the AP to factory default settings to re-enable this controller discovery method.

## Method 2: Perform Auto Discovery on Same Subnet, then Transfer the AP to Intended Subnet

If you are deploying the AP and the controller on different subnets, let the AP perform auto discovery on the same subnet as the controller before moving the AP to another subnet. To do this, connect the AP to the same network as the controller. When the AP starts up, it will discover and attempt to register with the controller. Approve the registration request if auto approval is disabled. After the AP registers with the controller successfully, transfer it to its intended subnet. It will be able to find and communicate with the controller once you reconnect it to the other subnet.

---

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

---

## Method 3: Register the Controller with the DNS Server

If you register the controller with your DNS server, supported APs that request IP addresses from your DHCP server will also obtain DNS related information that will enable them to discover controllers on the network. Using the DNS information they obtained during the DHCP request, APs will attempt to resolve the controller IP address using `RuckusController.{DNS domain name}` and `zonedirector.{DNS domain name}`.

To register the controller with the DNS server, do the following.

- 1 Open the DNS zone file, and then add two records with the following information:
  - Record Key#1: RuckusController  
Type: A (IPv4 Domain Name Translation)  
Value: (IP address of the controller)
  - Record Key#2: zonedirector  
Type: A (IPv4 Domain Name Translation)  
Value: (IP address of the controller)



Figure 36. Add records for “RuckusController” and “zonedirector” to the DNS zone file

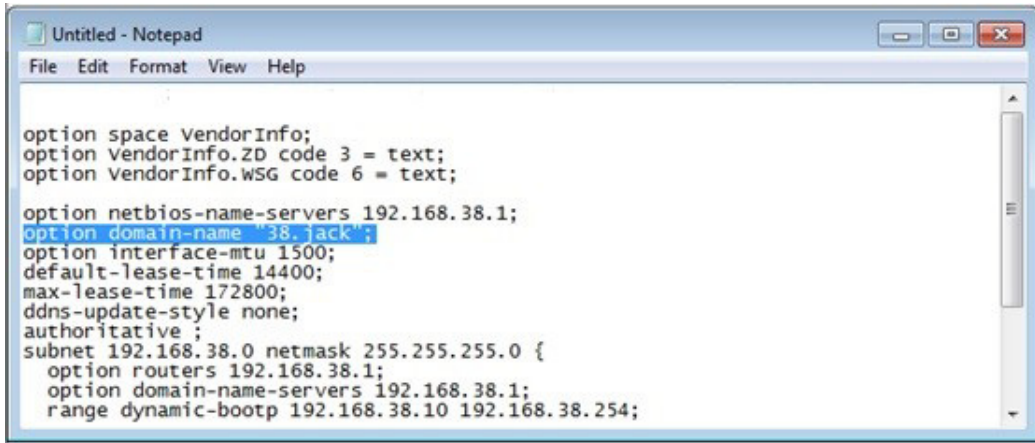
The screenshot shows the YaST Zone Editor window for the zone '38.jack'. The 'Records' tab is active, displaying the 'Record Settings' section with a record key of 'RuckusController', type 'A: IPv4 Domain Name Translation', and value '172.17.36.61'. Below this is a table of 'Configured Resource Records' with columns for Record Key, Type, and Value. The records for 'RuckusController' and 'zonedirector' are highlighted with a blue background and a red border.

Record Key	Type	Value
router4	A	172.17.22.90
router2	A	172.17.36.124
router4	AAAA	2002:3b7c:e439:9138::1
router2	AAAA	2002:3b7c:e439:9132::1
router3	A	172.17.21.37
router3	AAAA	2002:3b7c:e439:9135::1
RuckusController	A	172.17.36.61
zonedirector	A	172.17.36.61

- 2 Save the zone file.
- 3 Open the DHCP configuration file, and then insert the DNS domain name in the DHCP configuration file. For example, if the DNS domain name is “38.jack”, insert the following line into the DHCP configuration file:

```
option domain-name "38.jack"
```

Figure 37. Insert option domain-name “38.jack”



```
Untitled - Notepad
File Edit Format View Help

option space VendorInfo;
option VendorInfo.ZD code 3 = text;
option VendorInfo.WSG code 6 = text;
option netbios-name-servers 192.168.38.1;
option domain-name 38.jack;
option interface-mtu 1500;
default-lease-time 14400;
max-lease-time 172800;
ddns-update-style none;
authoritative ;
subnet 192.168.38.0 netmask 255.255.255.0 {
  option routers 192.168.38.1;
  option domain-name-servers 192.168.38.1;
  range dynamic-bootp 192.168.38.10 192.168.38.254;
```

#### 4 Save the DHCP configuration file.

When the AP obtains the DNS domain name from the DHCP server (using “Domain Name option 15” in the DHCP-offer packet), it will resolve “RuckusController.{domain-name}” and “zonedirector.{domain-name}” through the DNS server, and then it will obtain the controller’s IP address from the DNS server’s response.

---

**NOTE:** If the AP uses a static IP address or it cannot obtain the DNS domain name from the DHCP server, the AP will attempt to resolve “RuckusController” and “zonedirector” without a domain name from the DNS server as the FQDN of controller’s control interface.

---

You have completed registering the controller with the DNS server.

## Method 4: Configure DHCP Option 43 on the DHCP Server

Another method for the AP to discover the controller on the network automatically is to configure the DHCP server on the network. To do this, you will need to configure DHCP Option 43 (043 Vendor Specific Info) with the IP address of the controller on the network. When an AP requests an IP address from the DHCP server, the DHCP server will send a list of controller IP addresses to the AP. If there are multiple controller devices on the network, the AP will automatically select a controller to register with from this list of IP addresses.

DHCP Option 43 enables the DHCP server on your network to provide the controller's server address – either IP address or FQDN– (specifically, the IP address assigned to the controller's control plane or cluster plane interface) to DHCP clients, including APs that are connected to the network.

The procedure for configuring DHCP option 43 varies, depending on the DHCP server that you are using. Refer to the documentation provided with your DHCP server software for information on how to configure DHCP option 43.

---

**NOTE:** The following procedure describes how to configure DHCP option 43 on a Linux server (Fedora). If your DHCP server is running on a different platform, refer to the DHCP server documentation for the relevant instructions.

---

**CAUTION!** If you have a ZoneDirector controller on the network and you do not want APs to be managed by this ZoneDirector controller, you must disable auto approval on the ZoneDirector web interface. Log on to the ZoneDirector web interface, and then go to *Configure > Access Points > Access Points Policies* page, and then clear the **Approval** check box.

---

Follow these steps to configure DHCP option 43 (sub-code 3 and sub-code 6) on a Linux server.

- 1 Log on to your DHCP server via a console terminal (for example, PuTTY).
- 2 Go to `/etc` directory.
- 3 Run `vi dhcpd.conf`. This command opens the DHCP configuration file for editing.

- 4 At the beginning of the DHCP configuration file, insert the following lines:

```
option VendorInfo.WSG_sub6 code 6=text;
option VendorInfo.WSG_sub3 code 3=text;

option VendorInfo.WSG_sub6 "<Controller IP>";
option VendorInfo.WSG_sub3 "<Controller IP>";
```

For example, if you only have one controller on the network and its IP address is 120.0.0.3, then these lines in the DHCP configuration file should look like in [Figure 38 Sample DHCP Option 43 configuration](#).

Figure 38. Sample DHCP Option 43 configuration

```
option space VendorInfo;
option VendorInfo.WSG code 6 = text;
option VendorInfo.2D code 3 = text;

Vendor-option-space VendorInfo;
option VendorInfo.WSG "120.0.0.3";
```

If you have a two-node controller cluster on the network, use a comma to separate the control interface IP addresses in `option VendorInfo.WSG`, for example:

```
option VendorInfo.WSG "120.0.0.3,120.0.0.4"
```

where 120.0.0.3 is the control interface IP address of the first controller and 120.0.0.4 is the control interface IP address of the second controller.

- 5 Save the DHCP configuration file.
- 6 Restart the DHCP server to apply the new settings.
- 7 Verify that the LWAPP2SCG application is enabled on the controller. To verify, log on to the controller's CLI, and then enter the following command:

```
show running-config lwapp2scg
```

If LWAPP2SCG is enabled, the value for `ACL Policy` should show as `Accept all`.

Figure 39. “Accept all” indicates that LWAPP2SCG is enabled

```

sz30# show running-config lwapp2scg
  LWAPP2SCG Configuration
-----
ACL Policy                               : Accept all
Dynamic Data Transmission Port Range     : Not specified
ACL APs                                  :

```

If LWAPP2SCG is disabled, do the following to enable it:

- a Enter **config**.
- b Enter **lwapp2scg**.
- c Enter **policy**.
- d Enter one of the following commands:
  - **accept {MAC**
  - **address}**: Enter this command if you only want specific APs to be managed by the controller. See [Figure 41](#).
  - **accept-all**: Enter this command if you want all APs that discover the controller to be managed by it.

Figure 40. Options that appear after you enter the “policy” command

```

Sol-SZ1 (config) # lwapp2scg
<cr>

Sol-SZ1 (config) # lwapp2scg

Sol-SZ1 (config-lwapp2scg) # policy
  accept          Accept by ACL AP List
  accept-all     Accept All
  deny           Deny by ACL AP List
  deny-all      Deny All

Sol-SZ1 (config-lwapp2scg) # █

```

Figure 41. Enter accept [MAC address] if you only want specific APs to be managed by the controller

```
Sol-SZ1(config-lwapp2scg)# policy accept
Sol-SZ1(config-lwapp2scg)# acl-ap
  mac      AP MAC Address
  serial   AP Serial Number
Sol-SZ1(config-lwapp2scg)# acl-ap mac 6C:AA:B3:3D:66:90
Sol-SZ1(config-lwapp2scg)# acl-ap serial
<SerialNumber>   AP Serial Number(s). Please separate with comma e.g 123456789012,987654321021
Sol-SZ1(config-lwapp2scg)# acl-ap serial █
```

8 Reset the AP to factory default settings, and then connect it to a network subnet where it can communicate with the controller.

9 Reboot the AP.

After the AP reboots, it will obtain an IP address and the IP address of its parent controller from the DHCP server. Once the AP registers with the controller, it will download and install the latest SCG-AP firmware.

You have completed

## Method 5: Manually Configure the Controller Address on the AP's Web Interface

1 Log on to the AP's web interface.

2 Go to the Administration > Management page.

3 In *Primary Controller Address*, type the IP address of the controller that you want to manage the AP.

4 In *Secondary Controller Address*, type the IP address of a backup controller that you want to manage the AP if the primary controller is unavailable.

5 Click **Apply**.

You have completed manually configuring the controller's IP address on the AP's web interface.

Figure 42. Set the IP addresses of the primary and secondary controllers that you want to manage the AP

**Ruckus T300E Multimedia Hotzone Wireless AP**

**Administration :: Management**

**Status**  
 Device  
 Internet  
 Local Subnets  
 Radio 2.4G  
 Radio 5G

**Configuration**  
 Device  
 Internet  
 Local Subnets  
 Radio 2.4G  
 Radio 5G  
 Ethernet Ports  
 Hotspot

**Maintenance**  
 Upgrade  
 Reboot / Reset  
 Support Info

**Administration**  
 Management  
 Diagnostics  
 Log

**Network Profile:** 4bss

**Telnet Access?**  Enabled  Disabled

**Telnet Port:**

**SSH Access?**  Enabled  Disabled

**SSH Port:**

**HTTP Access?**  Enabled  Disabled

**HTTP Port:**

**HTTPS Access?**  Enabled  Disabled

**HTTPS Port:**

**Certificate Verification:** PASSED

**Controller Discovery Agent (LWAPP)?**  Enabled  Disabled

**Cloud Discovery Agent (FQDN)**  Enabled  Disabled

**Set Controller Address**  Enabled  Disabled

**Primary Controller Addr:**

**Secondary Controller Addr:**

**TR069 / SNMP Management Choice**

Auto (SNMP and TR069 will work together.)

SNMP only

FlexMaster only

None

**DHCP Discovery:**

**Ruckus WIRELESS** Ruckus T300E Multimedia Hotzone Wireless AP

## What to Do Next

For more information on configuring and managing the controller, refer to the *Administrator Guide* for this release, which is available for download on the Ruckus Wireless Support website at <http://support.ruckuswireless.com>.

**NOTE:** For a complete list of documentation that is available for this SCG-200 release, refer to the *Release Notes*.

# Index

## A

- AAA server 65
- AC power 28
- ACLs 75
- administrative computer 13, 35
- Administrator Guide 84
- AES 79
- AP zone 58, 74
- authentication options 77

## B

- background scanning 62
- backup RADIUS 65

## C

- cluster interface 20
- cluster name 50
- cluster setting 50
- console cable 10
- control interface 20
- control panel 16
- controller name 50
- country code 60
- creating a new cluster 50
- current requirements 31

## D

- DC input current 31
- DC input voltage 31
- DC power 30
  - input voltage 31
  - LED 32

## E

- encryption algorithm 79
- ESSID 76
- ETH0 38
- ETH1 20, 54
- ETH2 20, 38, 54
- ETH3 20
- ETH4 20

- ETH5 20

## F

- firmware version 52
- form factor 22
- front panel 14
  - control panel 16
- front panel without bezel 15

## G

- gateway 34

## H

- hotspot 65
- hotspot service 67

## I

- input voltage 31
- installation
  - required hardware 13
  - required tools 13
- interface settings 34
- interfaces
  - cluster 20
  - control 20
  - management 20
- IP address 34

## J

- joining a cluster 52

## L

- LEDs 19
  - NIC 19
- logging on 55

## M

- management interface 20, 55



mesh settings 61

## N

netmask 34

NIC LEDs 19

NTP server 50

## P

package contents 10

physical features

    front panel 14

    front panel without bezel 15

    LEDs 19

power options 28

    AC 28

    DC 30

powering on 28

pre-installation tasks 13

PSU 30

## R

rack mount kit 10, 11

RADIUS 65

RADIUS Accounting 65

rear panel 17

redundant interfaces 20

registration rule 71

    priority 73

required hardware 13

RJ45 serial port 18

router 13

rule priority 73

## S

server rack 13

setup wizard 38

SFP cables 54

SFP+ modules 13

software version 52

staging zone 58

surge suppressor 13

switch 13

## T

TKIP 79

tunnel settings 62

## U

unpacking 10

## W

web browser 13

Web interface 55

WEP-128 79

WEP-64 79

WLAN name 76

WLAN settings 74

WLAN usage 77

WPA2 79

WPA-Mixed 79



Copyright © 2006-2016. Ruckus Wireless, Inc.  
350 West Java Dr. Sunnyvale, CA 94089. USA  
[www.ruckuswireless.com](http://www.ruckuswireless.com)