

RUCKUS SmartZone 100 Getting Started Guide

Copyright, Trademark and Proprietary Rights Information

© 2021 CommScope, Inc. All rights reserved.

No part of this content may be reproduced in any form or by any means or used to make any derivative work (such as translation, transformation, or adaptation) without written permission from CommScope, Inc. and/or its affiliates ("CommScope"). CommScope reserves the right to revise or change this content from time to time without obligation on the part of CommScope to provide notification of such revision or change.

Export Restrictions

These products and associated technical data (in print or electronic form) may be subject to export control laws of the United States of America. It is your responsibility to determine the applicable regulations and to comply with them. The following notice is applicable for all products or technology subject to export control:

These items are controlled by the U.S. Government and authorized for export only to the country of ultimate destination for use by the ultimate consignee or end-user(s) herein identified. They may not be resold, transferred, or otherwise disposed of, to any other country or to any person other than the authorized ultimate consignee or end-user(s), either in their original form or after being incorporated into other items, without first obtaining approval from the U.S. government or as otherwise authorized by U.S. law and regulations.

Disclaimer

THIS CONTENT AND ASSOCIATED PRODUCTS OR SERVICES ("MATERIALS"), ARE PROVIDED "AS IS" AND WITHOUT WARRANTIES OF ANY KIND, WHETHER EXPRESS OR IMPLIED. TO THE FULLEST EXTENT PERMISSIBLE PURSUANT TO APPLICABLE LAW, COMMSCOPE DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, TITLE, NON-INFRINGEMENT, FREEDOM FROM COMPUTER VIRUS, AND WARRANTIES ARISING FROM COURSE OF DEALING OR COURSE OF PERFORMANCE. CommScope does not represent or warrant that the functions described or contained in the Materials will be uninterrupted or error-free, that defects will be corrected, or are free of viruses or other harmful components. CommScope does not make any warranties or representations regarding the use of the Materials in terms of their completeness, correctness, accuracy, adequacy, usefulness, timeliness, reliability or otherwise. As a condition of your use of the Materials, you warrant to CommScope that you will not make use thereof for any purpose that is unlawful or prohibited by their associated terms of use.

Limitation of Liability

IN NO EVENT SHALL COMMSCOPE, COMMSCOPE AFFILIATES, OR THEIR OFFICERS, DIRECTORS, EMPLOYEES, AGENTS, SUPPLIERS, LICENSORS AND THIRD PARTY PARTNERS, BE LIABLE FOR ANY DIRECT, INDIRECT, SPECIAL, PUNITIVE, INCIDENTAL, EXEMPLARY OR CONSEQUENTIAL DAMAGES, OR ANY DAMAGES WHATSOEVER, EVEN IF COMMSCOPE HAS BEEN PREVIOUSLY ADVISED OF THE POSSIBILITY OF SUCH DAMAGES, WHETHER IN AN ACTION UNDER CONTRACT, TORT, OR ANY OTHER THEORY ARISING FROM YOUR ACCESS TO, OR USE OF, THE MATERIALS. Because

some jurisdictions do not allow limitations on how long an implied warranty lasts, or the exclusion or limitation of liability for consequential or incidental damages, some of the above limitations may not apply to you.

Trademarks

ARRIS, the ARRIS logo, COMMSCOPE, RUCKUS, RUCKUS WIRELESS, the Ruckus logo, the Big Dog design, BEAMFLEX, CHANNELFLY, FASTIRON, ICX, SMARTCELL and UNLEASHED are trademarks of CommScope, Inc. and/or its affiliates. Wi-Fi Alliance, Wi-Fi, the Wi-Fi logo, Wi-Fi Certified, the Wi-Fi CERTIFIED logo, Wi-Fi Protected Access, the Wi-Fi Protected Setup logo, Wi-Fi Protected Setup, Wi-Fi Multimedia and WPA2 and WMM are trademarks or registered trademarks of Wi-Fi Alliance. All other trademarks are the property of their respective owners.

Contents

Preface.....	7
Document Conventions.....	7
Command Syntax Conventions.....	8
Document Feedback.....	8
RUCKUS Product Documentation Resources.....	8
Online Training Resources.....	9
Contacting RUCKUS Customer Services and Support.....	9
About This Guide.....	10
What's New in This Document.....	10
Preparing to Set Up the Controller.....	10
Unpacking the Controller.....	10
Verifying the Package Contents.....	10
Before You Begin.....	11
Mounting and Powering the Controller.....	16
Before You Begin.....	16
What You Will Need.....	16
Mounting the Controller.....	17
Powering On the Controller.....	22
Preparing the Interface Settings and Administrative Computer.....	23
Preparing the Controller's Interface Settings to Use.....	23
Preparing the Administrative Computer.....	24
Running the Setup Wizard and Logging On to the Web Interface.....	27
Overview of the Setup Wizard.....	27
Step 1: Start the Setup Wizard.....	28
Step 2: Configure the Port Grouping.....	29
Step 3: Configure the IP Settings.....	29
Step 4: Configure the Cluster Settings.....	34
Step 5: Verify the Settings.....	38
Connecting the Controller to the Network.....	39
Logging On to the Web Interface.....	39
Ensuring That APs Can Discover the Controller on the Network.....	41

Is LWAPP2SCG Enabled on the Controller? 41
Method 1: Perform Auto Discovery of the Controller Using the SmartLicense Server..... 42
Method 2: Perform Auto Discovery on Same Subnet, then Transfer the AP to Intended Subnet.....43
Method 3: Register the Controller with the DNS Server..... 43
Method 4: Configure DHCP Option 43 on the DHCP Server..... 45
Method 5: Manually Configure the Controller Address on the AP's Web Interface..... 49
What to Do Next..... 51

Preface

Document Conventions

The following table lists the text conventions that are used throughout this guide.

TABLE 1 Text Conventions

Convention	Description	Example
monospace	Identifies command syntax examples	<code>device(config)# interface ethernet 1/1/6</code>
bold	User interface (UI) components such as screen or page names, keyboard keys, software buttons, and field names	On the Start menu, click All Programs .
<i>italics</i>	Publication titles	Refer to the <i>RUCKUS Small Cell Release Notes</i> for more information.

Notes, Cautions, and Safety Warnings

Notes, cautions, and warning statements may be used in this document. They are listed in the order of increasing severity of potential hazards.

NOTE

A NOTE provides a tip, guidance, or advice, emphasizes important information, or provides a reference to related information.

ATTENTION

An ATTENTION statement indicates some information that you must read before continuing with the current action or task.



CAUTION

A CAUTION statement alerts you to situations that can be potentially hazardous to you or cause damage to hardware, firmware, software, or data.



DANGER

A DANGER statement indicates conditions or situations that can be potentially lethal or extremely hazardous to you. Safety labels are also attached directly to products to warn of these conditions or situations.

Preface

Command Syntax Conventions

Command Syntax Conventions

Bold and italic text identify command syntax components. Delimiters and operators define groupings of parameters and their logical relationships.

Convention	Description
bold text	Identifies command names, keywords, and command options.
<i>italic text</i>	Identifies a variable.
[]	Syntax components displayed within square brackets are optional. Default responses to system prompts are enclosed in square brackets.
{x y z}	A choice of required parameters is enclosed in curly brackets separated by vertical bars. You must select one of the options.
x y	A vertical bar separates mutually exclusive elements.
< >	Nonprinting characters, for example, passwords, are enclosed in angle brackets.
...	Repeat the previous element, for example, <i>member[member...]</i> .
\	Indicates a “soft” line break in command examples. If a backslash separates two lines of a command input, enter the entire command at the prompt without the backslash.

Document Feedback

RUCKUS is interested in improving its documentation and welcomes your comments and suggestions.

You can email your comments to RUCKUS at #Ruckus-Docs@commscope.com.

When contacting us, include the following information:

- Document title and release number
- Document part number (on the cover page)
- Page number (if appropriate)

For example:

- RUCKUS SmartZone Upgrade Guide, Release 5.0
- Part number: 800-71850-001 Rev A
- Page 7

RUCKUS Product Documentation Resources

Visit the RUCKUS website to locate related documentation for your product and additional RUCKUS resources.

Release Notes and other user documentation are available at <https://support.ruckuswireless.com/documents>. You can locate the documentation by product or perform a text search. Access to Release Notes requires an active support contract and a RUCKUS Support Portal user account. Other technical documentation content is available without logging in to the RUCKUS Support Portal.

White papers, data sheets, and other product documentation are available at <https://www.ruckuswireless.com>.

Online Training Resources

To access a variety of online RUCKUS training modules, including free introductory courses to wireless networking essentials, site surveys, and products, visit the RUCKUS Training Portal at <https://training.ruckuswireless.com>.

Contacting RUCKUS Customer Services and Support

The Customer Services and Support (CSS) organization is available to provide assistance to customers with active warranties on their RUCKUS products, and customers and partners with active support contracts.

For product support information and details on contacting the Support Team, go directly to the RUCKUS Support Portal using <https://support.ruckuswireless.com>, or go to <https://www.ruckuswireless.com> and select **Support**.

What Support Do I Need?

Technical issues are usually described in terms of priority (or severity). To determine if you need to call and open a case or access the self-service resources, use the following criteria:

- Priority 1 (P1)—Critical. Network or service is down and business is impacted. No known workaround. Go to the **Open a Case** section.
- Priority 2 (P2)—High. Network or service is impacted, but not down. Business impact may be high. Workaround may be available. Go to the **Open a Case** section.
- Priority 3 (P3)—Medium. Network or service is moderately impacted, but most business remains functional. Go to the **Self-Service Resources** section.
- Priority 4 (P4)—Low. Requests for information, product documentation, or product enhancements. Go to the **Self-Service Resources** section.

Open a Case

When your entire network is down (P1), or severely impacted (P2), call the appropriate telephone number listed below to get help:

- Continental United States: 1-855-782-5871
- Canada: 1-855-782-5871
- Europe, Middle East, Africa, Central and South America, and Asia Pacific, toll-free numbers are available at <https://support.ruckuswireless.com/contact-us> and Live Chat is also available.
- Worldwide toll number for our support organization. Phone charges will apply: +1-650-265-0903

We suggest that you keep a physical note of the appropriate support number in case you have an entire network outage.

Self-Service Resources

The RUCKUS Support Portal at <https://support.ruckuswireless.com> offers a number of tools to help you to research and resolve problems with your RUCKUS products, including:

- Technical Documentation—<https://support.ruckuswireless.com/documents>
- Community Forums—<https://forums.ruckuswireless.com/ruckuswireless/categories>
- Knowledge Base Articles—<https://support.ruckuswireless.com/answers>
- Software Downloads and Release Notes—https://support.ruckuswireless.com/#products_grid
- Security Bulletins—<https://support.ruckuswireless.com/security>

About This Guide

Using these resources will help you to resolve some issues, and will provide TAC with additional data from your troubleshooting analysis if you still require assistance through a support case or RMA. If you still require help, open and manage your case at https://support.ruckuswireless.com/case_management.

About This Guide

What's New in This Document

TABLE 2 Summary of Enhancements in RUCKUS SZ 100 Getting Started Guide

Feature	Description	Location
Review comments	Rev I is created to incorporate minor review comments.	Column width for col2 in table3 is adjusted. Duplicated rows in the topic Hardware requirements were removed.

Preparing to Set Up the Controller

Unpacking the Controller

Follow these steps to unpack the controller.

1. Open the controller 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](#) on page 10 (below) are included in the package. Check each item for damage. If any item is damaged or missing, notify your authorized Ruckus Networks sales representative immediately.

Verifying the Package Contents

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

- One SmartZone 100 appliance
- One Category 6 (Cat 6) Ethernet cable (5 ft.)
- One rack mount kit (see [Rack Mount Kit Contents](#) on page 11 below)
- Service Level Agreement/Limited Warranty Statement sheet
- Regulatory Statement sheet
- This *Getting Started Guide*

NOTE

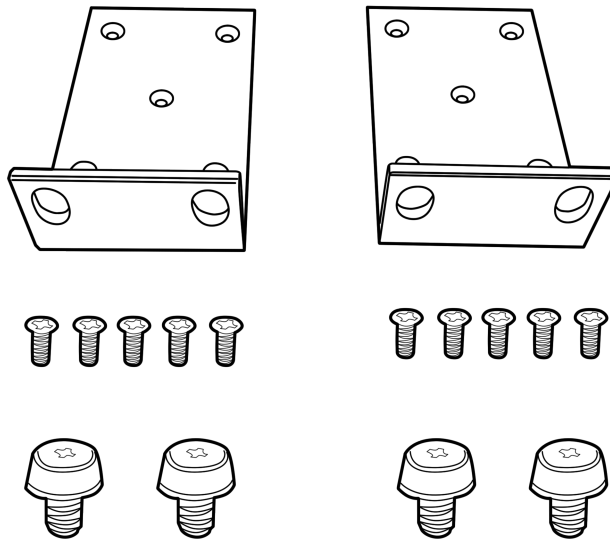
The AC power cable (part number 902-0174-XX00, where XX is the two-character country code) is not supplied with the SmartZone 100 appliance and may be ordered separately.

Rack Mount Kit Contents

The rack mount kit contains the following items:

- Mounting brackets x 2
- Rack cabinet mounting screws x 4
- Small screws x 10

FIGURE 1 Contents of the rack mount kit



Before You Begin

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

Prepare the Required Hardware and Tools

NOTE

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

Preparing to Set Up the Controller

Before You Begin

You must supply the following tools and equipment:

- A switch or router for connecting the controller to the backbone network. If you purchased SKU P01-S124-WW10 (see [Determine Which Controller SKU You Have](#) on page 12), which has two (2) 10GBASE-X (SFP+) ports, Ruckus Networks recommends using a switch or router that has 10GbE interfaces.
- 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 15G, 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 1RU space

Determine Which Controller SKU You Have

The SZ 100 has two stock keeping units (SKUs) available:

- SKU P01-S104-WW10 has four (4) 1000BASE-T (RJ-45) ports and supports option A and B.
- SKU P01-S124-WW10 has four (4) 1000BASE-T (RJ-45) and two (2) 10GBASE-X (SFP+) ports and supports option C and D.

FIGURE 2 SKU P01-S124-WW10 has two 10GBASE-X (SFP+) ports, which SKU P01-S104-WW10 does not

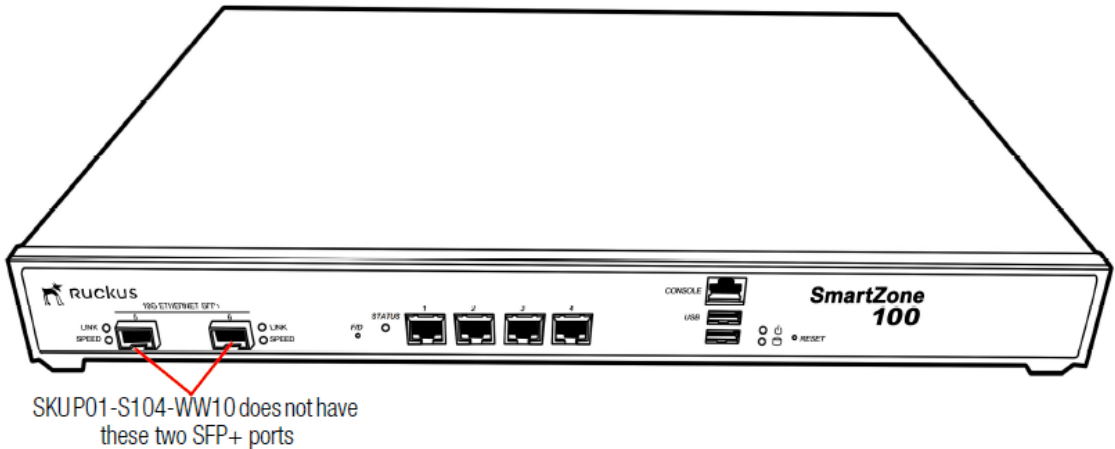


TABLE 3 SZ100 Port Configuration

Model Chassis Type	Option	GE(0)	GE(1)	GE(2)	GE(3)	10GE(4)	10GE(5)
SZ104 (4xGE)	A	MGMT/CL/CP /DP	MGMT/CL/CP /DP	MGMT/CL/CP /DP	MGMT/CL/CP /DP	N/A	N/A
SZ104 (4xGE)	B	MGMT/CL/CP	MGMT/CL/CP	DP	DP	N/A	N/A
SZ124 (4xGE +2x10GE)	C	MGMT/CL/CP /DP	MGMT/CL/CP /DP	MGMT/CL/CP /DP	MGMT/CL/CP /DP	MGMT/CL/CP /DP	MGMT/CL/CP /DP
SZ124 (4xGE +2x10GE)	D	MGMT/CL/CP	MGMT/CL/CP	DP	DP	DP	DP

GE Details:

- MGMT: Management
- CL: Cluster
- CP: Control Plane
- DP: Data Plane (Tunnel/User traffic)

Get to Know the Physical Features of the Controller

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

Front Panel

The following figure shows the controller's front panel with the bezel installed. For descriptions of the numbered parts, refer to the table below.

Preparing to Set Up the Controller

Before You Begin

FIGURE 3 The front panel of the SmartZone 100 (SKU P01-S124-WW10)

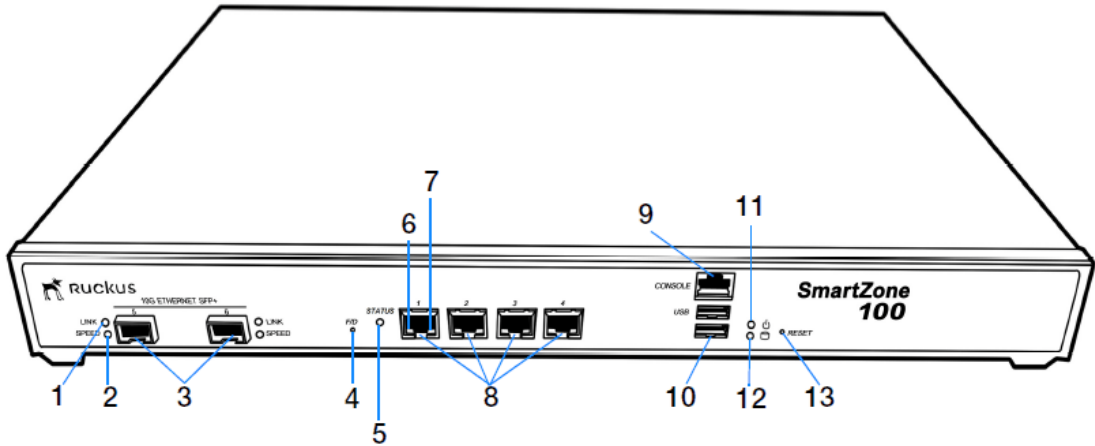




TABLE 4 Front panel parts

Number	Description
1	10G Ethernet link LED (see LEDs on the Front Panel on page 15)
2	10G Ethernet speed LED (see LEDs on the Front Panel on page 15)
3	Two 10GBASE-X (SFP+) ports (SKU P01-S124-WW10 only)
4	F/D (factory default) button. Press this button for at least 10 seconds to reset the controller to factory default settings.
5	Status LED (see LEDs on the Front Panel on page 15)
6	1000BASE-T link LED (see LEDs on the Front Panel on page 15)
7	1000BASE-T status LED (see LEDs on the Front Panel on page 15)
8	Four 1000BASE-T (RJ-45) ports
9	Console (RJ-45 serial) port
10	Two USB ports
11	Power LED (see LEDs on the Front Panel on page 15)
12	HDD LED (see LEDs on the Front Panel on page 15)
13	Reset button. Press for 5 seconds to restart the SZ 100.

LEDs on the Front Panel

The table below describes the behavior of the LEDs on the front panel.

TABLE 5 LED behavior

LED	Description
10G Ethernet link LED	Green: Operational Flashing: TX/RX data Off: Not operational
10G Ethernet speed LED	Blue: Operating at 10Gbps Yellow/Orange: Operating 1Gbps Off: Not operational
Status	Green: System operational/no fault Red: System fault Blinking red: Starting up or shutting down Slow flashing red: System shut down
1000BASE-T link LED	Green: Operational Flashing green: TX/RX data Off: Not operational
1000BASE-T speed LED	Green: 1000Mbps Amber: 100Mbps Off: 10Mbps
 Power	On: Power available Off: No power
 HDD	On: Disk I/O (usually blinking) Off: No disk I/O

Rear Panel

The figure below shows the rear panel of the SmartZone 100. For descriptions of the numbered parts, refer to the table below.

Mounting and Powering the Controller

FIGURE 4 Rear panel of the SmartZone 100

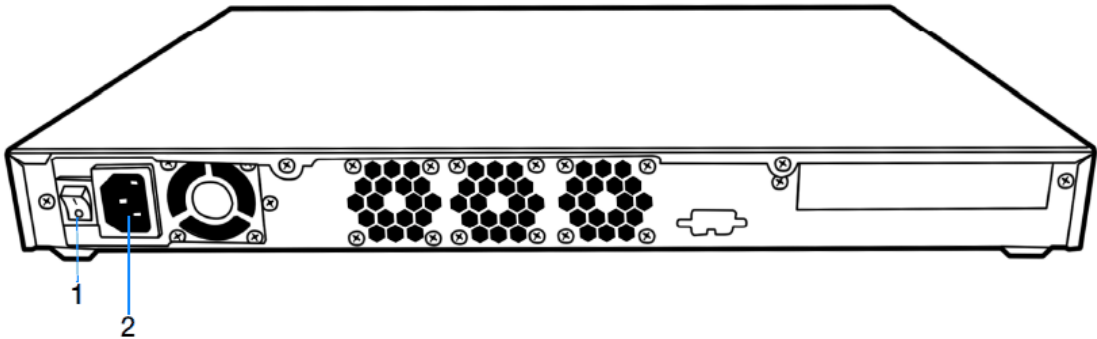


TABLE 6 SmartZone rear panel parts

Number	Description
1	Power switch
2	High efficiency (80+) power supply (110-220 VAC)

Mounting and Powering the Controller

Before You Begin

Before installing the controller onto a server rack, verify that all package contents (see [Unpacking the Controller](#) on page 10) are included and ensure that you have prepared all the required hardware and tools.

What You Will Need

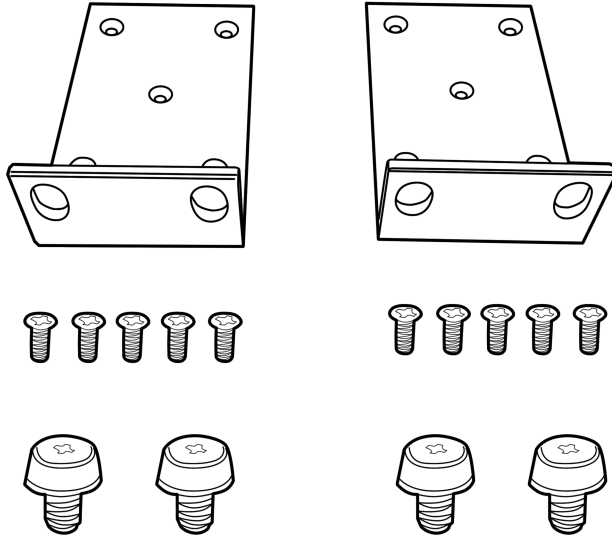
- 3/8-inch hex driver or wrench
- Phillips (crosshead) screwdriver, #1 and #2 bits
- Anti-static wrist strap and conductive foam pad (recommended)

Mounting the Controller

Follow these steps to mount the controller onto a server rack.

1. Unpack the rack mount kit that is included in the SZ100 package that you received. Refer to [Rack Mount Kit Contents](#) on page 11 and verify that the rack mount kit contents are complete.

FIGURE 5 Rack mount kit contents

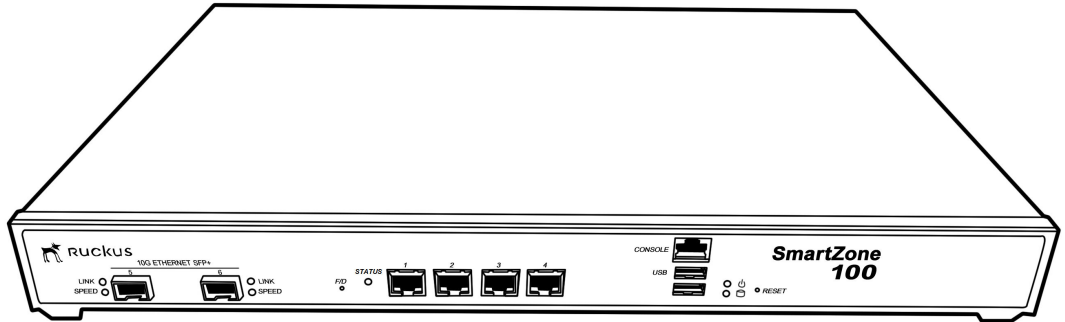


Mounting and Powering the Controller

Mounting the Controller

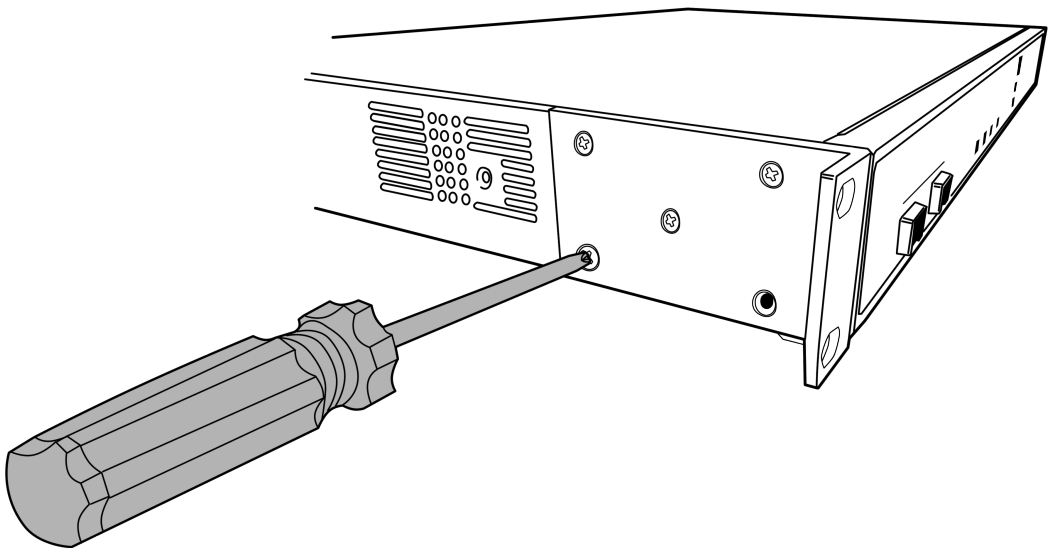
2. Find a flat and surface (such as a table) and place the SZ100 unit on top of it.

FIGURE 6 Place the SZ100 on a flat, dry surface



3. Take one mounting ear, and then use a Phillips to secure it to the right side of the chassis with the supplied mounting ear screws.

FIGURE 7 Secure the mounting ear to the right side of the chassis

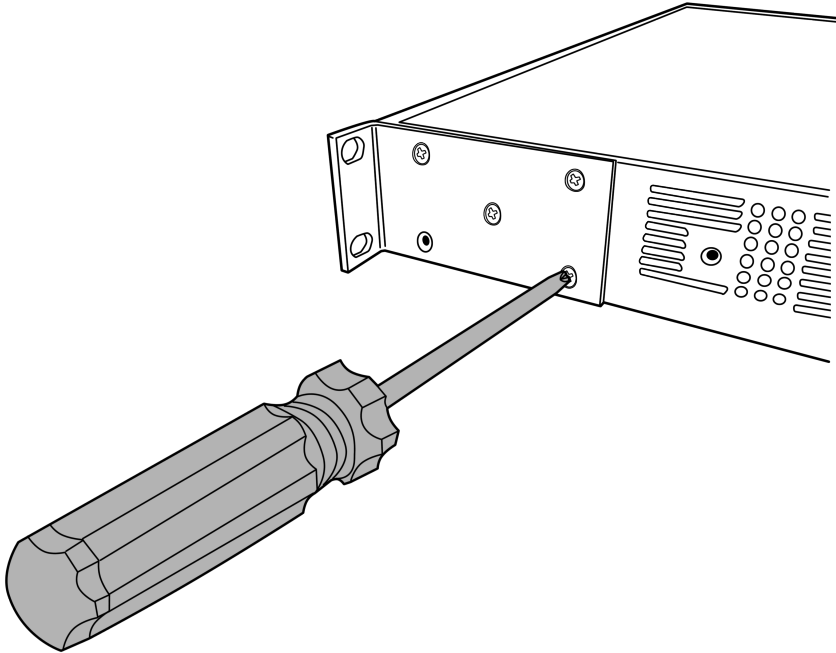


Mounting and Powering the Controller

Mounting the Controller

4. Take the remaining mounting ear, and then repeat the above procedure on the left side of the chassis.

FIGURE 8 Secure the other mounting ear to the left side of the chassis



NOTE

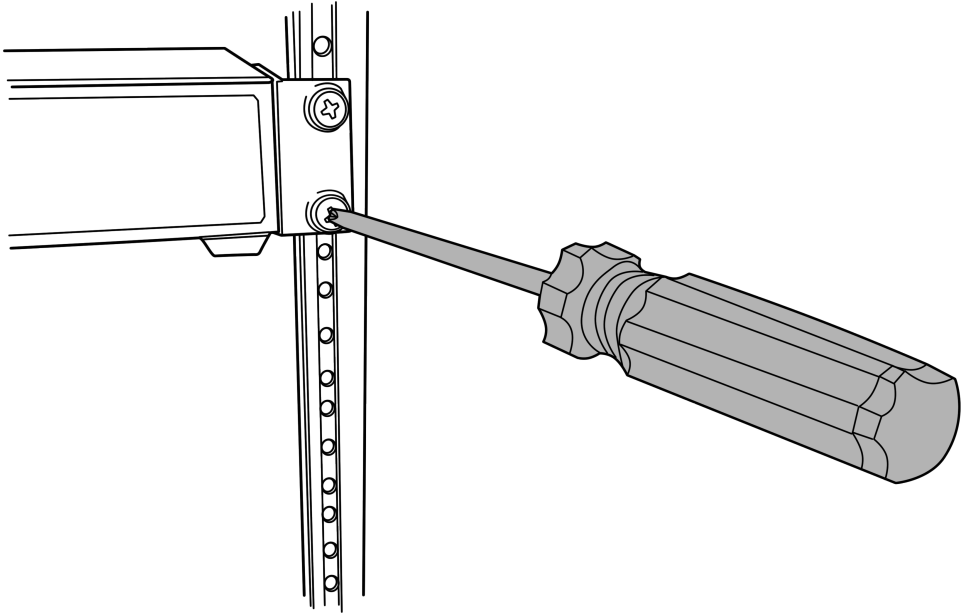
One of the bottom screw holes on each side of the chassis is unusable – it is used to secure the chassis cover to the chassis. Therefore, you can only use up to four mounting ear screws on each side. Ten mounting ear screws are supplied. So you may have two or more mounting ear screws left (depending on how many you use) when you finish.

Mounting and Powering the Controller

Mounting the Controller

5. Using the supplied four rack mounting screws, secure the SZ 100 chassis to the rack. Use two screws on each side of the chassis.

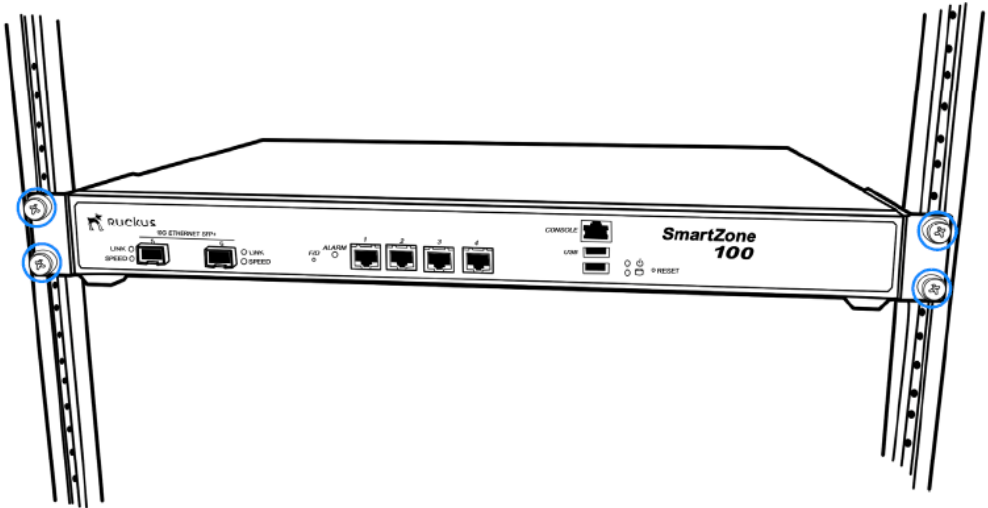
FIGURE 9 Use the supplied screws to secure the mounting ears to the rack



Mounting and Powering the Controller

Mounting the Controller

FIGURE 10 Use two mounting screws on each mounting ear



You have completed mounting the controller to a rack.

Mounting and Powering the Controller

Powering On the Controller

Powering On the Controller

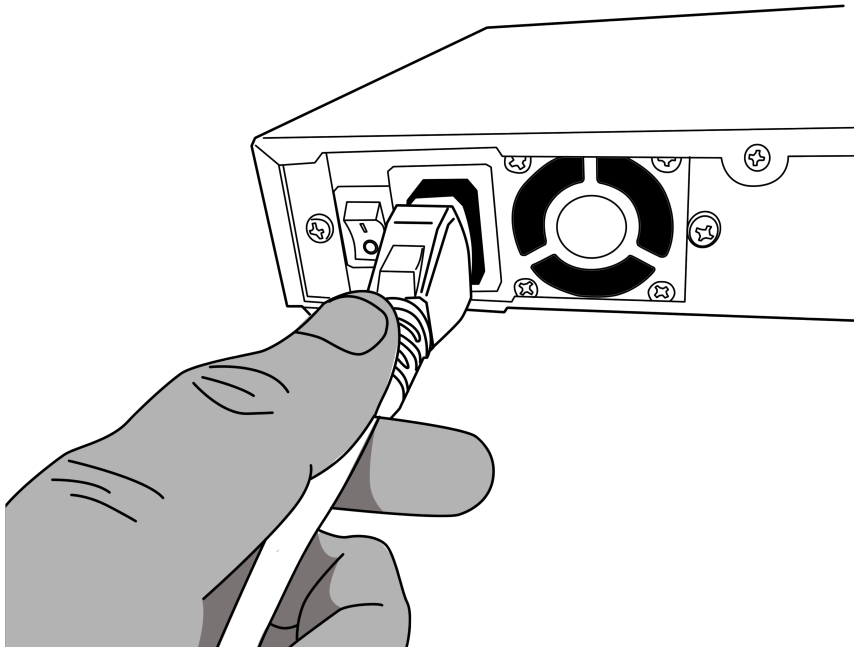
NOTE

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

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

1. Connect the AC power cable to the power socket on the rear panel.

FIGURE 11 Connect the AC cable to the power socket



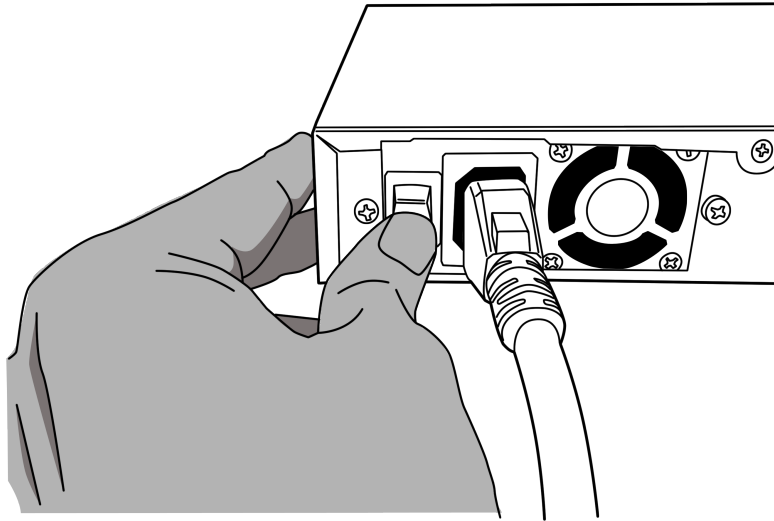
2. Connect the other end of the power cable to an electrical outlet.

Preparing the Interface Settings and Administrative Computer

Preparing the Controller's Interface Settings to Use

3. Press the power switch on the rear panel to power on the SZ 100. The power LED on the front panel turns amber while the SZ 100 boots up, and turns off when the startup is complete.

FIGURE 12 Press the power switch to power on the SmartZone 100



You have completed powering on the controller.

Preparing the Interface Settings and Administrative Computer

Preparing the Controller's Interface Settings to Use

The controller includes either one or two network interfaces (depending on the port group configuration that you will select (see [Table 8](#)) that need to be connected to the network for the appliance to work. If you select two-port configuration when you run the Setup Wizard later in this chapter, you will be required to assign each interface on the controller a separate set of network settings.

Hardware Requirement

The below table lists the details of hardware components.

Preparing the Interface Settings and Administrative Computer

Preparing the Administrative Computer

TABLE 7 Component Specific Information

Product Name	Label	Model	
CPU	Intel	i7-3770	3.40 GHz, Socket: FCLGA1155
MB	Caswell	COB-7400-000	
Power	Enhance	ENP-7025D-47XGB	
RAM	Innodisk	-	8GB DDR3 1600 DIMM
HDD	Western Digital	-	1TB, 3.5" SATA HDD



CAUTION

If you select the two-port configuration, you must configure these two controller interfaces to be on 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
- Netmask
- Gateway
- Primary DNS server
- Secondary DNS server

TABLE 8 Controller interfaces

Interface	Description
AP/ Management (Web)	Used for AP configuration, client traffic, and management traffic. The IP address that you assign to this interface will be the IP address through which you can access the controller's web interface.
AP Tunnel	Used for tunnel traffic to and from the AP

Preparing the Administrative Computer

NOTE

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

Follow these steps to prepare the administrative computer that you will use to run the 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**
2. When the **Network Connections** windows appears, right click the icon for "Local Area Connection" and click **Properties**.

Preparing the Interface Settings and Administrative Computer

Preparing the Administrative Computer

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.

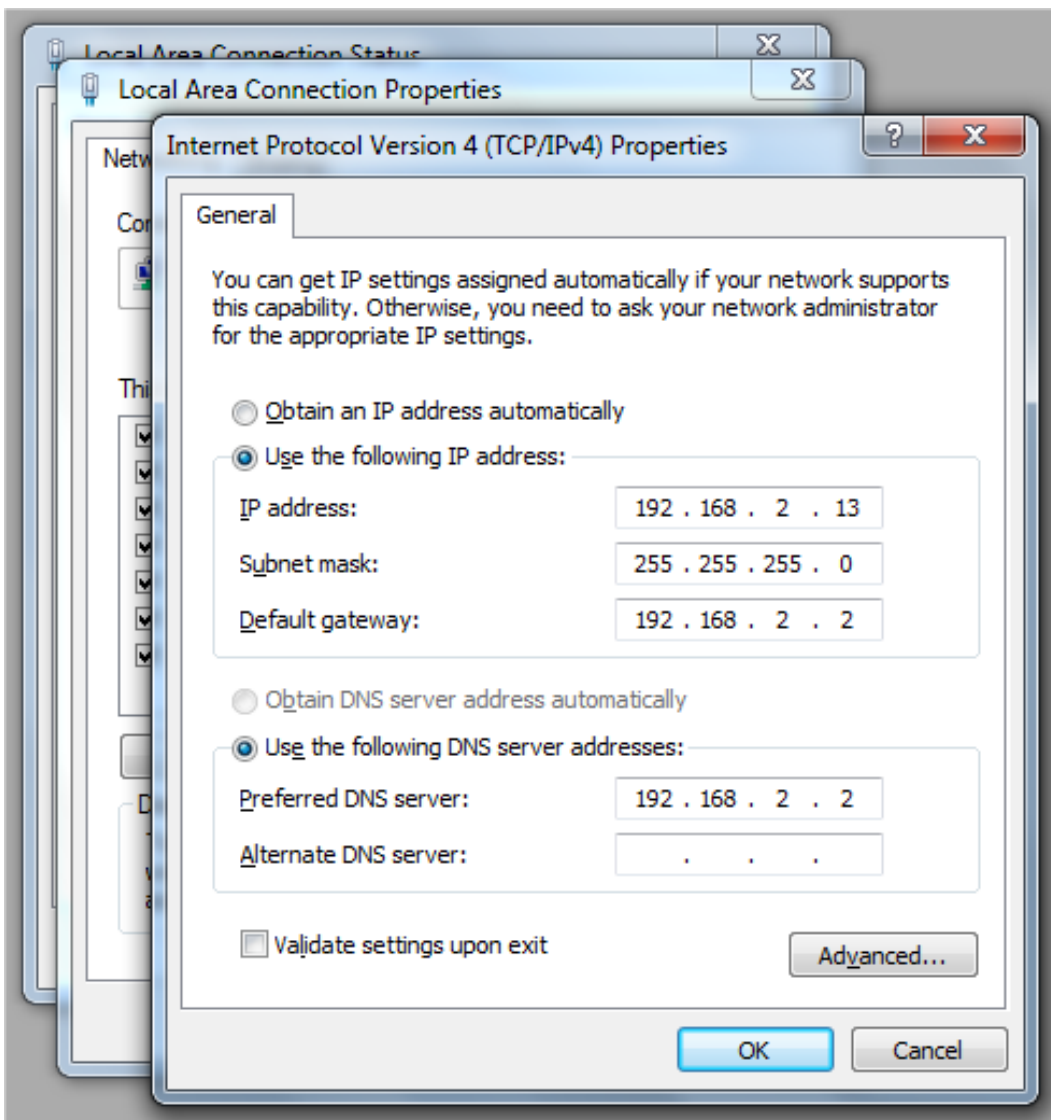
NOTE

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

Preparing the Interface Settings and Administrative Computer

Preparing the Administrative Computer

FIGURE 13 The Internet Protocol Version 4 (TCP/IP) properties dialog box



Running the Setup Wizard and Logging On to the Web Interface

Overview of the Setup Wizard

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 controller)
 - **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

Overview of the Setup Wizard

Follow these steps to run and complete the Setup Wizard.

[Step 1: Start the Setup Wizard](#) on page 28

[Step 2: Configure the Port Grouping](#) on page 29

[Step 3: Configure the IP Settings](#) on page 29

[Step 4: Configure the Cluster Settings](#) on page 34

[Step 5: Verify the Settings](#) on page 38

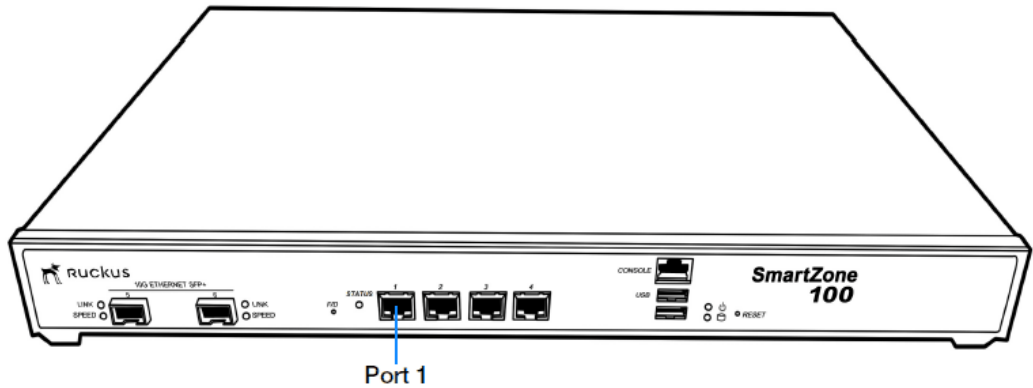
Running the Setup Wizard and Logging On to the Web Interface

Step 1: Start the Setup Wizard

Step 1: Start the Setup Wizard

1. Connect one end of an Ethernet cable to Port 1 on the front panel of the controller, and then connect the other end to an Ethernet port on the administrative computer.

FIGURE 14 Location of Port 1 on the front panel

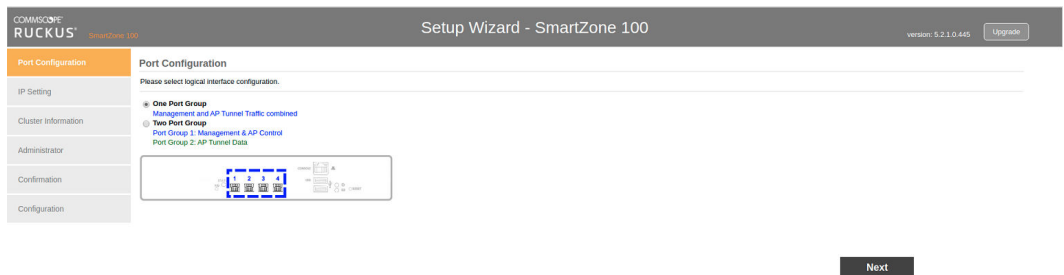


2. Start your web browser, and then enter the following in the address bar:

`https://192.168.2.2:8443`

The Setup Wizard appears, displaying the **Port Configuration** page.

FIGURE 15 The Port Configuration page with the One Port Group option selected



Step 2: Configure the Port Grouping

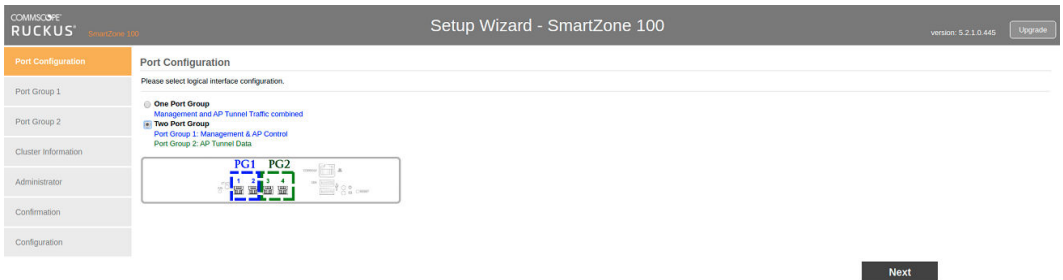
The controller offers two types of port configurations: one port group or two port groups. Select your preferred port configuration. Available options include:

- **One Port Group:** The management and AP tunnel traffic are combined on a single interface. Ruckus Networks recommends selecting this option to simplify the setup process. If you select **One Port Group**, you will need to enter one set of IP address settings.
- **Two Port Group:** The management and AP control traffic and the AP tunnel data traffic are separated. If you select **Two Port Group**, you will need to enter two sets of IP address settings.

NOTE

On the SZ104, the two 10GB ports are bound to Port Group 2.

FIGURE 16 Two-port grouping separates the management and AP control traffic from AP tunnel traffic



1. Click **Next**. The next setup wizard page that appears depends on the port configuration option that you selected.
2. Go to the relevant section in [Step 3: Configure the IP Settings](#) on page 29.

Step 3: Configure the IP Settings

The steps that you will take in this procedure will depend on the port group configuration that you selected.

- [If You Selected One Port Group](#) on page 29
- [If You Selected Two Port Groups](#) on page 31

If You Selected One Port Group

1. In **IP Version Support**, select one of the following options:
 - **IPv4 Only:** Click this option if you want the controller in IPv4 only mode.
 - **IPv4 and IPv6:** Click this option if you want the controller in both IPv4 and IPv6 mode.

Running the Setup Wizard and Logging On to the Web Interface

Step 3: Configure the IP Settings

2. Configure the IP address settings of the **Management/AP Tunnel** interface.
 - a) Under the **IPv4** section, click **Static**, and then enter the network settings that you want to assign to the interface.

NOTE

Although it is possible to use DHCP to assign IP address settings to this interface automatically, Ruckus Networks strongly recommends assigning a static IP address.

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

- IP address
 - Netmask
 - Gateway
 - Primary DNS Server
 - Secondary DNS Server
- 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
 - **NAT IP:** Enter a NAT IP address. SmartZone pushes both the private IP and the NAT IP to the AP.
 - c) In **Primary DNS Server** and **Secondary DNS Server**, enter the DNS server address for the enabled interfaces.

Running the Setup Wizard and Logging On to the Web Interface

Step 3: Configure the IP Settings

3. Click **Next**. The **Cluster Information** page appears.
Go to [Step 4: Configure the Cluster Settings](#) on page 34 to continue.

FIGURE 17 The IP Setting page, showing the options when IPv4 only is selected

The screenshot shows the 'Setup Wizard - SmartZone 100' interface. The left sidebar contains navigation options: Port Configuration, IP Setting (highlighted), Cluster Information, Administrator, Confirmation, and Configuration. The main content area is titled 'IP Setting' and includes instructions: 'Select how you want the SmartZone 100 to obtain its IPv4 (and IPv6, if supported on your network) IP address settings. To obtain an IP address automatically using DHCP, click "DHCP" for IPv4 or "Auto Configuration" for IPv6. To specify an IP address, click "Static" and then type the IP address settings in "IP Address," "Netmask," and "Gateway." An asterisk (*) indicates required information.'

IP Version Support IPv4 only IPv4 and IPv6

Management/AP Tunnel Traffic

IPv4

Static DHCP

IP Address * 192.168.92.2

Netmask * 255.255.255.240

Gateway * 192.168.92.1

Primary DNS Server 10.10.10.10

Secondary DNS Server IPv4 Secondary DNS

Next **Back**

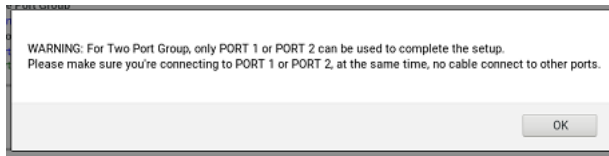
If You Selected Two Port Groups

After you click **Next** on the previous setup wizard page, a warning message appears and informs you that the administrative computer must be connected to LAN 1 (Port 1) and LAN 2 (Port 2) to complete the setup process.

Running the Setup Wizard and Logging On to the Web Interface

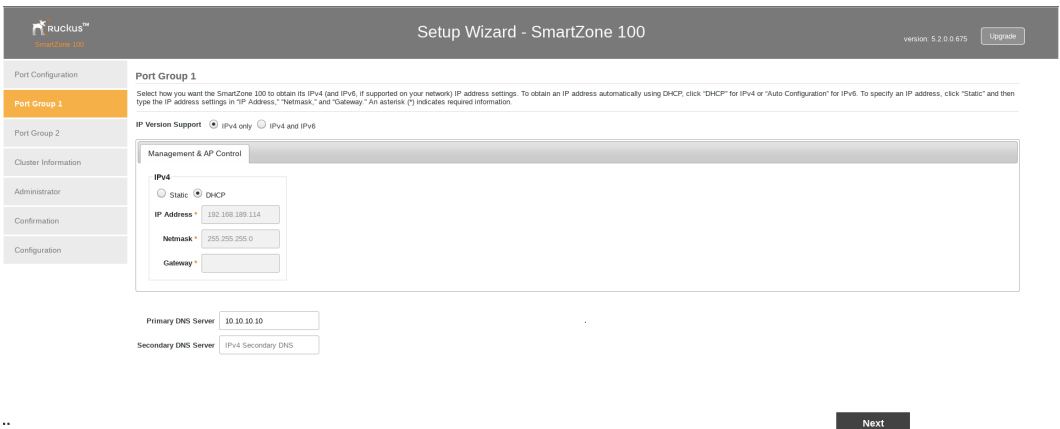
Step 3: Configure the IP Settings

FIGURE 18 A warning message appears after you select the two port group option



1. Click **OK** on the warning message to close it. The **Port Group 1** configuration page appears.

FIGURE 19 The Management & AP Control tab on the Port Group 1 page



2. In **IP Version Support**, select one of the following options:
 - **IPv4 Only:** Click this option if you want the controller in IPv4 only mode.
 - **IPv4 and IPv6:** Click this option if you want the controller in both IPv4 and IPv6 mode.

Running the Setup Wizard and Logging On to the Web Interface

Step 3: Configure the IP Settings

3. Configure the IP address settings of the **Management & AP Control** interface.
 - a) Under the **IPv4** section, click **Static**, and then enter the network settings that you want to assign to the interface.

NOTE

Although it is possible to use DHCP to assign IP address settings to the this interface automatically, Ruckus Networks strongly recommends assigning a static IP address.

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

- IP address
 - Netmask
 - Default gateway
 - NAT IP
- 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`
 - **NAT IP**: Enter a NAT IP address. SmartZone pushes both the private IP and the NAT IP to the AP.
 - c) In **Primary DNS Server** and **Secondary DNS Server**, enter the DNS server address for the enabled interfaces.

Running the Setup Wizard and Logging On to the Web Interface

Step 4: Configure the Cluster Settings

4. Click **Next**. The **Port Group 2** page appears.

FIGURE 20 The AP Tunnel Data tab on the Port Group 2 page

The screenshot shows the 'Setup Wizard - SmartZone 100' interface. The left sidebar has 'Port Group 2' highlighted. The main area is titled 'Port Group 2' and contains a 'DataPlane0' tab. Under the 'IPv4' section, the 'Manual' radio button is selected. Below it are three input fields: 'IP Address *', 'Netmask *', and 'Gateway *'. At the bottom right, there are 'Next' and 'Back' buttons.

5. On the **AP Tunnel Data** tab, click **Manual**, and then enter the network settings that you want to assign to the port group 2 interface, through which client traffic and configuration data will be sent and received.

The following network settings are required:

- IP address
- Netmask
- Default gateway

NOTE

Although it is possible to use DHCP to assign IP address settings to this interface automatically, Ruckus Networks strongly recommends assigning a static IP address.

6. Click **Next**. 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](#) on page 35
- [If This Controller Is Joining an Existing Cluster](#) on page 37

NOTE

A SmartZone (SZ) 100 unit can only form a cluster with other SmartZone 100 units of the same model. For example, a SZ104 cannot be clustered with a SZ124 unit. It cannot join a cluster of SmartZone 300 or vSZ units (and vice versa).

FIGURE 21 The Cluster Information page

The screenshot shows the 'Cluster Information' page in the Ruckus SmartZone 100 Setup Wizard. The page has a dark header with the Ruckus logo and 'SmartZone 100' on the left, and 'Setup Wizard - SmartZone 100' and 'version: 5.2.0.0.603 Upgrade' on the right. A sidebar on the left contains navigation links: Port Configuration, Port Group 1, Port Group 2, Cluster Information (highlighted in orange), Administrator, Confirmation, and Configuration. The main content area is titled 'Cluster Information' and contains the following fields: SZ Cluster Setting (New Cluster), Cluster Name, Controller Name, Controller Description, Default Country Code (United States), NTP Server (ntp.ruckuswireless.com), AP Conversion (checked), AP IP Mode (radio buttons for IPv4 only, IPv6 only, IPv4 and IPv6), and a checkbox for 'Is this controller behind NAT?'. At the bottom right, there are 'Next' and 'Back' buttons.

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:
 - **SZ Cluster Setting:** Select **New Cluster**.
 - **Cluster Name:** Type a name that you want to assign to this new cluster.
 - **Controller Name:** Type a name for this controller, which will become the controller in this new cluster.
 - **Controller Description:** Type a description for this controller.
2. In **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.

Running the Setup Wizard and Logging On to the Web Interface

Step 4: Configure the Cluster Settings

3. In **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.

4. In **AP IP Mode**, select one of the following options:
 - **IPv4 Only:** Click this option if you want APs that will be managed by this controller to use IPv4 addressing mode.
 - **IPv6 Only:** Click this option if you want APs that will be managed by this controller to use IPv6 addressing mode.



CAUTION

You can only set the device IP mode once. After you complete the Setup Wizard, the device IP mode setting will not be configurable from either the web interface or command line interface.

5. Click **Next** to continue to the next Setup Wizard page. The **Administrator** page appears.
6. 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.
 - **Confirmation Password:** Retype the password above to confirm.

Running the Setup Wizard and Logging On to the Web Interface

Step 4: Configure the Cluster Settings

7. Click **Next** to continue. The **Confirmation** page appears and displays all the controller settings that you have configured using the Setup Wizard.

FIGURE 22 Set the administrator passwords for the web interface and command line interface

The screenshot shows the 'Setup Wizard - SmartZone 100' interface. On the left is a navigation menu with options: Port Configuration, Port Group 1, Port Group 2, Cluster Information, **Administrator** (highlighted), Confirmation, and Configuration. The main content area is titled 'Administrator' and contains the following text: '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 are two password fields: 'Admin Password' and 'Confirm Password'. A horizontal line separates this section from the next, which says: 'Enter CLI enable password and password that provides advance command'. Below this are two more password fields: 'Enable Password' and 'Confirm Password'. At the bottom right, there are two buttons: 'Next' and 'Back'.

If This Controller Is Joining an Existing Cluster

If this is not the first controller 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.

NOTE

When adding a new node into an existing cluster, any ARC signature files, AP or switch firmware, and AP patches on the existing cluster will be synchronised onto the new node. Kernel Space Program (KSP) patches must be independently uploaded to the new node. Refer to the KSP documentation to ensure whether the KSP patches are applied per node and whether the cluster needs to be reloaded.

Running the Setup Wizard and Logging On to the Web Interface

Step 5: Verify the Settings

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

1. In **Cluster Setting**, click **Join Existing Cluster**.

FIGURE 23 Select Join Existing Cluster in Cluster Setting

The screenshot shows the 'Setup Wizard - SmartZone 100' interface. The top header includes the Ruckus logo, the title 'Setup Wizard - SmartZone 100', the version '5.1.1.0.495', and an 'Upgrade' button. The left sidebar lists navigation steps: Port Configuration, Port Group 1, Port Group 2, Cluster Information (selected), Administrator, Confirmation, and Configuration. The main content area is titled 'Cluster Information' and contains the following fields and options:

- SZ Cluster Setting:** A dropdown menu with 'Join Existing Cluster' selected.
- Cluster Name:** An empty text input field.
- Controller Name:** An empty text input field.
- Controller Description:** An empty text input field.
- Join Exist SZ Cluster IP:** An empty text input field.
- Admin Password*:** An empty text input field.
- Is this controller behind NAT?

At the bottom right of the form, there are two buttons: 'Next' and 'Back'.

2. In **SZ Cluster Setting**, select the cluster configuration from the drop-down menu.
3. In **Cluster Name**, type the name of the existing cluster that you want this controller to join.
4. In **Controller Name**, type a name that you want to assign to this new controller.
5. In **Controller Description**, type a description for this new controller.
6. In **Join Exist Cluster IP**, type the IP address that has been assigned to the cluster.
7. In **Admin Password**, type the existing password for the cluster. This is the password that you use to log on to the controller's web interface.
8. Click **Next** to continue to the next Setup Wizard page. The **Confirmation** page appears and displays a summary of the settings that you have configured.

NOTE

If the firmware version on this controller (shown in 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's firmware. Click **Upgrade**, and then follow the prompts to perform the upgrade.

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 controller on the network.

FIGURE 24 Review the settings you have configured

Ruckus™
SmartZone 100

Setup Wizard - SmartZone 100

version:

Port Configuration

Port Group 1

Port Group 2

Cluster Information

Administrator

Confirmation

Configuration

Confirmation

Please review the following settings. If changes need to be made, click Back to edit your settings. If the settings are ready for use, click Finish

Cluster Name Cluster-1435
Protocol Type TCP
AP IP Mode IPv4

Management IP **IPv4** Management & AP Control: Manual 192.168.69.2 **IPv6** Management & AP Control: Static fd95:2d35:eb58:691::2/64

Default Country Code US
System Time System time will be automatically set.
Your current system time is (2018-05-23 14:38:03 Epoch : 1527057483)

* After completing the setup wizard, please check the [Ruckus Wireless Support Web site](#) for the latest software updates.

Restore from Config Backup: No file chosen

A progress bar appears and displays the progress of applying the settings, starting the controller's services, and activating the controller 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 controller's web interface to manage the appliance.

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

Connecting the Controller to the Network

Follow these steps to connect the controller to the network.

1. Connect Port 1 to the router or switch.
2. Connect Port 2 to another router or switch to which other controllers (if present) are connected.

NOTE

Depending on your network setup, you may also connect Port 2 to the same router or switch to which Port 1 is connected.

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 3: Configure the IP Settings](#) on page 29.

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.

Running the Setup Wizard and Logging On to the Web Interface

Logging On to the Web Interface

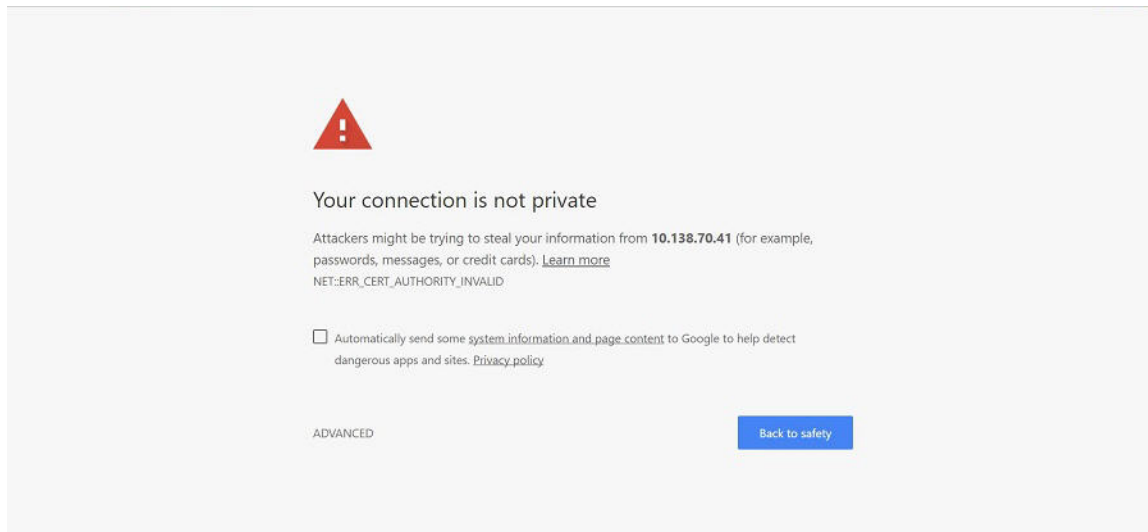
2. In the address bar, enter the IP address that you assigned to the Management (Web) interface and append a colon and 8443 (controller's management port number) at the end of the address.

For example, if the IP address that you assigned to the Management (Web) interface is 192.168.2.21, then you should enter:

```
https://192.168.2.21:8443
```

3. If a browser security warning appears, this is because the default SSL certificate (or security certificate) that the SZ is using for HTTPS communication is signed by Ruckus Networks and is not recognized by most web browsers. Click continue or proceed (depending on the browser that you are using).

FIGURE 25 Example of the browser warning that appears in Google Chrome



The controller's web interface logon page appears.

4. 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 Setup Wizard}**
5. 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. Refer to the *SmartZone 100 Administrator Guide* for information on how to configure the controller and manage APs and wireless clients.

Ensuring That APs Can Discover the Controller on the Network

Is LWAPP2SCG Enabled on the Controller?

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.

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 the following table to check if your controller release includes the LWAPP2SCG application and whether it is enabled or disabled by default.

TABLE 9 LWAPP2SCG availability on each controller release

Controller Release	LWAPP Discovery	Default Setting	AP Compatibility
Release 3.0.x and later	Enabled by default. See Enabling LWAPP2SCG on page 41.	Enabled	ZF-AP Release 9.7.x – 9.8.x AP Release 100.0.x and later

Operating Temperature of the APs

The operating temperature and humidity for the APs must be as below:

TABLE 10 Operating Temperature and Humidity Details

Operating Temperature	0°C (32°F) - 40°C (104°F)
Operating Humidity	5% to 85%, non-condensing
Humidity, Storage	95%, non-condensing

Obtaining the LWAPP2SCG Application

If your controller release does not have the LWAPP2SCG application pre-installed, contact RUCKUS 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.

Ensuring That APs Can Discover the Controller on the Network

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

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

AP Registrar is a RUCKUS-hosted cloud based software service (@ aregistrat.ruckuswireless.com) that provides customers a simple, easy to use and completely secure "controller discovery" mechanism for securely adding and registering APs to be managed by an appropriate controller.

The following are some of benefits of using the AP Registrar:

- APs are registered to the controllers using their serial numbers
- APs and controller mappings are fully controllable
- Customers can provision the AP Registrar via secure JSON APIs that are protected by a unique customer key

Configuring the AP Registrar

The AP Registrar can be programmed using RESTful JSON APIs. In order to provide security to access the AP Registrar, it is important for you to obtain a certificate from Ruckus Networks.

Please follow these IMPORTANT steps to obtain a certificate and the API Guide from Ruckus Networks to access the AP Registrar.

1. Ensure that you have purchased on-going support for all your RUCKUS equipment and products.
2. Ensure that you have a signed and fully executed NDA with Ruckus Networks. If you have not signed NDA, reach out to Ruckus Networks APR support team.
3. Ensure that you have signed the AP Registrar T&C (Terms and Conditions) document. Reach out to Ruckus Networks APR support team for the T&C document
4. Provide the domain name (FQDN - non wildcard) from where you will access the AP Registrar. This is needed to provide correct access to the API. It is recommended to set up a specific FQDN (for example, apr.customerdomain.com) and set the ARecord to the IP address from which they will need to access the AP Registrar.
5. Provide your GPG signed public key. This is needed to securely send a package back to you that contains their API key and digital certificate.
6. Provide all these details to dl-apr-support@ruckuswireless.com.

Once you complete the above steps, you will receive a package that contains the API documentation, sample code, as well as a client-side certificate that you can use to provision the AP Registrar using the APIs. Important Notes

Important notes

- To use AP Registrar API, you must pre-register an FQDN with Ruckus Networks and the company will provide an SSL certificate, signed by a recognized certificate authority and bearing the FQDN in the certificate's subject common name field.
- The certificate must be presented to the API server when making API requests. The API requester must be in possession of the certificate's private key.
- The FQDN (without wildcard) in the certificate's subject common name field must match that mentioned in the API user's user record.
- The DNS IP address of the FQDN must match the Internet routable IP address of the computer from which the API request is generated.
- If any of the above three conditions are not met, the API request will fail with a 401 error.

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}`.

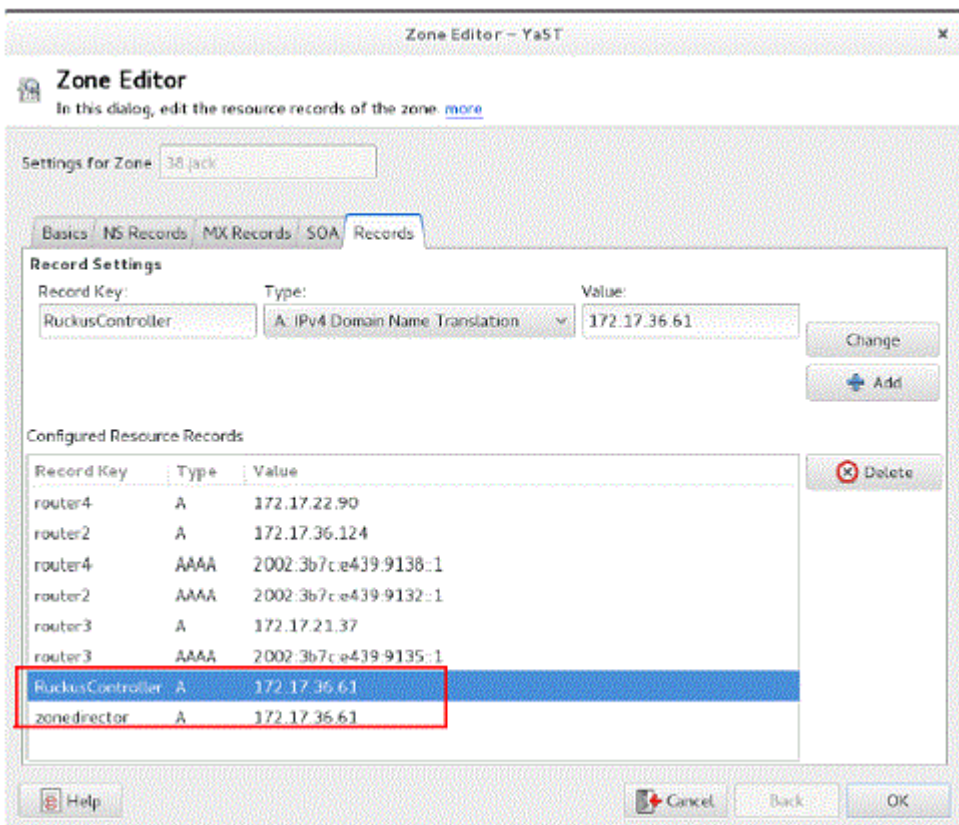
Ensuring That APs Can Discover the Controller on the Network

Method 3: Register the Controller with the DNS Server

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 26 Add records for “RuckusController” and “zonedirector” to the DNS zone file



2. Save the zone file.

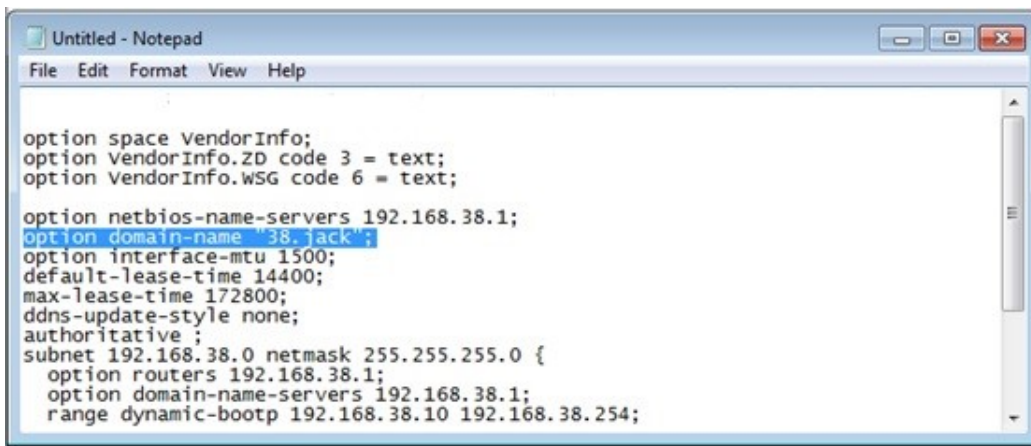
Ensuring That APs Can Discover the Controller on the Network

Method 4: Configure DHCP Option 43 on the DHCP Server

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 27 Insert option domain-name "38.jack"



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.

Ensuring That APs Can Discover the Controller on the Network

Method 4: Configure DHCP Option 43 on the DHCP Server

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 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.

Ensuring That APs Can Discover the Controller on the Network

Method 4: Configure DHCP Option 43 on the DHCP Server

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 the following figure.

FIGURE 28 Sample DHCP Option 43 configuration

```
option space VendorInfo;
option VendorInfo.WSG code 6 = text;
option VendorInfo.ZD code 3 = text;
option VendorInfo.WSGD code 7 = 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.

Ensuring That APs Can Discover the Controller on the Network

Method 4: Configure DHCP Option 43 on the DHCP Server

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 29 "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 31](#).
 - `accept-all`: Enter this command if you want all APs that discover the controller to be managed by it.

FIGURE 30 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)# █
```


Ensuring That APs Can Discover the Controller on the Network

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

FIGURE 31 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 configuring DHCP option 43 on a Linux server.

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.

Ensuring That APs Can Discover the Controller on the Network

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

5. Click **Apply**.

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

FIGURE 32 Set the IP addresses of the primary and secondary controllers that you want to manage the AP

The screenshot displays the web interface for a Ruckus T300E Multimedia Hotzone Wireless AP. The page is titled "Administration :: Management" and shows various configuration options. The "Set Controller Address" section is highlighted with a red box, indicating the primary and secondary controller addresses. Below this section, there are radio button options for TR069 / SNMP Management Choice, with "Auto (SNMP and TR069 will work together.)" selected. The Ruckus logo is visible in the bottom left corner of the interface.

Configuration Item	Value / Status
Network Profile:	4bss
Telnet Access?	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
Telnet Port:	23
SSH Access?	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
SSH Port:	22
HTTP Access?	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
HTTP Port:	80
HTTPS Access?	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
HTTPS Port:	443
Certificate Verification	PASSED
Controller Discovery Agent (LWAPP)?	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
Cloud Discovery Agent (FQDN)	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
Set Controller Address	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
Primary Controller Addr:	[Empty text field]
Secondary Controller Addr:	[Empty text field]
TR069 / SNMP Management Choice	<input checked="" type="radio"/> Auto (SNMP and TR069 will work together.) <input type="radio"/> SNMP only <input type="radio"/> FlexMaster only <input type="radio"/> None

What to Do Next

For more information on configuring and managing the controller, refer to the *SmartZone 100 Administrator Guide for Release 3.4*, which is available for download on the RUCKUS support website at <http://support.ruckuswireless.com>.

NOTE

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

COMMScope®
RUCKUS®

© 2021 CommScope, Inc. All rights reserved.
350 West Java Dr., Sunnyvale, CA 94089 USA
<https://www.commscope.com>