

RUCKUS SmartZone (ST-GA) Controller Administration Guide, 7.0.0

Supporting SmartZone Release 7.0.0

© 2024 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

CommScope and the CommScope logo are registered trademarks of CommScope and/or its affiliates in the U.S. and other countries. For additional trademark information see <https://www.commscope.com/trademarks>. All product names, trademarks, and registered trademarks are the property of their respective owners.

Patent Marking Notice

For applicable patents, see www.cs-pat.com.

Contents

Contact Information, Resources, and Conventions.....	7
Contacting RUCKUS Customer Services and Support.....	7
What Support Do I Need?.....	7
Open a Case.....	7
Self-Service Resources.....	8
Document Feedback.....	8
RUCKUS Product Documentation Resources.....	8
Online Training Resources.....	8
Document Conventions.....	9
Notes, Cautions, and Safety Warnings.....	9
Command Syntax Conventions.....	9
About This Guide.....	11
About This Guide.....	11
New in This Document.....	11
Controller Setup.....	13
RUCKUS SmartZone.....	13
What is the best SmartZone solution for my environment?.....	13
SmartZone Cluster.....	13
Single-node Cluster.....	14
Cluster Redundancy.....	14
Controller, Management and Data Planes.....	14
External Data Planes.....	14
Network Interfaces.....	14
Physical Network Interfaces.....	14
Port Group Configuration in Physical Appliances.....	15
Configuring the Control Plane.....	16
User Defined Interface.....	19
Access and Core Segmentation.....	19
Static Routing.....	19
IPv6 Configurations and Considerations.....	20
Controller DNS.....	20
Control NAT IP.....	21
Viewing the Interface and Routing Configuration of the Controller.....	22
Configuring the System Time.....	23
System Time Settings.....	24
NTP Server Authentication Settings.....	25
SmartZone Web Interface.....	27
Introduction to SmartZone Web Interface.....	27
Controller Web Interface Features.....	27
Rest API.....	27
Help with the GUI and APIs.....	28
Logging in to the Web Interface.....	28
Logging Off Using the Web Interface.....	29
Controller User Interface (UI)	29
Setting User Preferences.....	31

Managing the Access Control of the Management Interface.....	35
Global Filters Overview.....	37
Configuring Global Filters.....	37
Using the Dashboard.....	38
Warnings.....	38
Health.....	39
Understanding Cluster and AP Health Icons.....	40
Customizing Health Status Thresholds.....	40
Customizing AP Flagged Status Thresholds.....	41
Global Notifications.....	42
Using the Health Dashboard Map.....	43
Configuring the Google Map API Key Behavior.....	45
Wireless Dashboard.....	45
Wired Dashboard.....	50
Administrator and Roles.....	55
Managing Administrators and Roles.....	55
Creating User Groups.....	55
Resource Group Details.....	57
Creating Administrator Accounts.....	58
Unlocking an Administrator Account.....	60
Configuring the System Default Super Admin.....	60
Working with AAA Servers.....	63
Configuring SmartZone Admin AAA Servers.....	63
Testing AAA Servers.....	67
AAA Server Authentication.....	68
About RADIUS Support.....	69
About TACACS+ Support.....	70
About Active Directory (AD) Support.....	71
About LDAP Support.....	72
Creating Account Security.....	73
Terminating Administrator Sessions.....	78
White Label Customization.....	79
Changing the Administrator Password.....	80
Administrator Activities.....	81
SmartZone Cluster and Cluster Redundancy.....	83
Viewing System Settings.....	83
Cluster Overview.....	83
Control Planes and Data Planes.....	84
Displaying the Chassis View of Cluster Nodes.....	84
Reviewing Cluster Health and Configuration.....	85
Clearing or Acknowledging Alarms.....	86
Filtering Events.....	86
Powering Cluster Back.....	86
Rebalancing APs.....	87
Cluster Redundancy.....	88
How Cluster Redundancy Works.....	91
Enabling Cluster Redundancy.....	92
Viewing Cluster Configuration.....	96
AP Auto Rehome.....	97

Disabling Cluster Redundancy - Active-Standby from the Active Cluster.....	98
Disabling Cluster Redundancy - Active-Standby from the Standby Cluster.....	99
Deleting Cluster Redundancy - Active-Active from a target Active Cluster.....	99
Disabling Cluster Redundancy - Active-Active mode from a Current Target Active Cluster.....	99
SmartZone Network Hierarchy.....	101
SmartZone Domains.....	101
Partner Domains.....	102
AP Zones.....	103
AP Groups.....	103
WLAN Groups.....	104
Switch Groups.....	106
Onboarding Access Points and Switches.....	107
Onboarding APs and Switches.....	107
Requirements to Onboard Access Points or Switches.....	107
Introduction to Firewall Ports.....	108
Ports to Open Between Various RUCKUS Devices, Servers, and Controllers.....	108
Monitoring the Network.....	115
Monitoring the Network.....	115
Controller Network Services.....	117
Syslog.....	117
Configuring the Remote Syslog Server.....	117
Short Message Service (SMS).....	119
Configuring the Short Message Service (SMS) Gateway Server.....	119
Simple Mail Transfer Protocol (SMTP).....	120
Configuring Simple Mail Transfer Protocol (SMTP) Server Settings.....	120
Simple Network Management Protocol (SNMP).....	120
Enabling Global SNMP Notifications.....	120
Configuring SNMP v2 Agent.....	121
Configuring SNMP v3 Agent.....	121
File Transfer Protocol (FTP).....	123
Configuring File Transfer Protocol Server Settings.....	123
Controller Certificates.....	125
Importing SmartZone as Client Certificate.....	125
Assigning Certificates to Services.....	126
Generating Certificate Signing Request (CSR).....	127
Importing SmartZone (SZ) Trusted CA Certificates/Chains.....	128
DataPlane validates SmartZone.....	129
AP Validate SmartZone Controller.....	130
ECDSA 3K.....	134
Elliptic Curve Digital Signature Algorithm (ECDSA) Certificate and Keys Support.....	134
Cloud Computing Compliance Criteria Catalogue - BSI C5.....	134
Configuring ECDSA and Keys at Zone Level.....	135
Mapping Server ECDSA Certificates.....	137
Enabling ECDSA Certificates Support for RADIUS with Transport Layer Security (TLS).....	140
External Services.....	143
Location Services.....	143
Mobile Virtual Network Operator (MVNO).....	145

Managing Mobile Virtual Network Operator (MVNO) Accounts.....	145
Northbound Data Streaming.....	147
Configuring Northbound Data Streaming Settings.....	147
Setting the Northbound Portal Password.....	148
RUCKUS Cloud Services.....	149
Replacing Hardware Components	155
Installing or Replacing Hard Disk Drives.....	155
Ordering a Replacement Hard Disk.....	155
Removing the Front Bezel.....	155
Removing an HDD Carrier from the Chassis.....	156
Installing a Hard Drive in a Carrier.....	158
Reinstalling the Front Bezel.....	161
Replacing PSUs.....	161
Replacing System Fans.....	162
Upgrade.....	165
Upgrading the Controller.....	165
Performing the Upgrade.....	165
Verifying the Upgrade.....	166
Verifying Upgrade Failure and Restoring Cluster.....	166
Rolling Back to a Previous Software Version.....	167
Cautions & Limitations of Administrating a Cluster	168
Patch/Diagnostic Scripts.....	168
Uploading Patch or Diagnostic Scripts.....	168
Applying Patch or Diagnostic Scripts	169
Application Signature Packages.....	169
Step 1: Uploading the Signature Package.....	170
Step 2: Validating the Signature Package.....	170
Managing Signature Package Upgrading Conflicts.....	171
Backup and Restore.....	173
Cluster Backup.....	173
Disaster Recovery.....	173
Creating a Cluster Backup.....	173
Restoring a Cluster Backup.....	173
Restoring a Cluster Automatically on Upgrade Failure.....	174
Configuration Backup.....	176
Backing up Cluster Configuration.....	176
Scheduling a Configuration Backup.....	176
Backing Up to an FTP Server.....	177
Restoring from an FTP Server.....	179
Exporting the Configuration Backup to an FTP Server Automatically.....	185
Downloading a Copy of the Configuration Backup.....	185
Restoring a System Configuration Backup.....	185
Backed Up Configuration Information.....	186

Contact Information, Resources, and Conventions

- [Contacting RUCKUS Customer Services and Support](#)..... 7
- [Document Feedback](#)..... 8
- [RUCKUS Product Documentation Resources](#)..... 8
- [Online Training Resources](#)..... 8
- [Document Conventions](#)..... 9
- [Command Syntax Conventions](#)..... 9

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 to 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.ruckusnetworks.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 **Submit 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 **Submit a Case** section.
- Priority 3 (P3)—Medium. Network or service is moderately impacted, but most business remains functional. Click the **CONTACT** tab at the top of the page and explore the **Self-Service Online Help** options.
- Priority 4 (P4)—Low. Requests for information, product documentation, or product enhancements. Click the **CONTACT** tab at the top of the page and explore the **Self-Service Online Help** options.

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://community.ruckuswireless.com>
- 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>

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

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.ruckusnetworks.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://commscopeuniversity.myabsorb.com/>. The registration is a two-step process described in this [video](#). Create a CommScope account and then register for, and request access for, CommScope University.

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.

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.

About This Guide

- [About This Guide.....](#) 11
- [New in This Document.....](#) 11

About This Guide

The *RUCKUS SmartZone Controller Administration Guide* offers comprehensive insights for configuring and maintaining all the functional aspects of the controller. It covers essential topics such as providing an understanding of network communication, web UI guidelines and features, access privileges for administrators, onboarding network-managed equipment (including access points and switches), and configuring the necessary services for the controller to operate effectively. Additionally, this document addresses administrative tasks, such as software upgrades and configuration backups.

New in This Document

TABLE 2 Key Features and Enhancements in *Controller Administration Guide, 7.0.0 (August 2024)*

Feature	Description	Reference
Adding Icons	Throughout the guide.	-
Adding Animated GIFs	Throughout the guide.	-

Controller Setup

- RUCKUS SmartZone..... 13
- SmartZone Cluster..... 13
- Controller, Management and Data Planes..... 14
- Network Interfaces..... 14
- Configuring the System Time..... 23

RUCKUS SmartZone

RUCKUS SmartZone controllers are high-performance wireless LAN (WLAN) controllers that run the RUCKUS SmartZone operating system. SmartZone controllers are available in hardware models such as SZ100, SZ144, and SZ300. Alternatively, the virtualized version, Virtual SmartZone (vSZ-E or vSZ-H) can be installed on third-party hypervisors or cloud-hosted virtualization solutions.

What is the best SmartZone solution for my environment?

Check the hardware models available and the virtualized options in the chart below. Compare the AP Capacity and the recommended environment to determine the best controller for your network.

TABLE 3 Recommended SmartZone Product Based on Capacity and Environment

Product	Standalone Capacity	Cluster Capacity	Recommended Environment
SmartZone 100 (SZ-100) (End of Life)	1,024 access points 25,000 clients	3,000 access points 60,000 clients	60,000 clients Medium to large enterprise
SmartZone 144 (SZ-144)	2000 access points 40,000 clients	6,000 access points 120,000 clients	120,000 clients Medium to large enterprise
SmartZone 300 (SZ300)	10,000 access points 100,000 Clients	30,000 access points 300,000 clients	Service Provide
Virtual SmartZone (vSZ) - vSZ-E	1,024 access point 25,000 clients	3,000 access points 60,000 clients	3,000 access points 60,000 clients
Virtual SmartZone (vSZ) - vSZ-H	10,000 access points 100,000 Clients	30,000 access points 300,000 clients	Service Provide

NOTE

For information on how to set up the controller for the first time, including instructions for preparing your chosen hypervisor, installing the vSZ image on the hypervisor, and completing the vSZ Setup Wizard, refer to the Getting Started Guide or Quick Setup Guide specific to your controller platform.

SmartZone Cluster

RUCKUS SmartZone (SZ) architecture allows multiple SZ controllers to be deployed together in an Active-Active SmartZone Cluster. With Active-Active clustering, all nodes of a cluster are managed together as a single entity and each node actively manages APs in the network, offering AP load balancing and controller redundancy. The SmartZone Cluster offers options for adding and removing nodes in the cluster, upgrading all the members of the cluster with a single action, cluster backup, and cluster restore, among others. Refer to [SmartZone Cluster and Cluster Redundancy](#) on page 83 for detailed explanations about managing the cluster.

Controller Setup

Controller, Management and Data Planes

Single-node Cluster

One single SmartZone or Virtual SmartZone unit working alone is commonly referred to as a Single-node Cluster.

Cluster Redundancy

The Cluster Redundancy feature provides uninterrupted communication across clusters regardless of the clusters being geographically co-located or geographically separated (the latter known as geo-redundancy). For SZ300 and vSZ-H configurations, up to four SmartZone Clusters can be deployed in Active-Active or Active-Standby Cluster Redundancy mode. All controllers in Active-Active mode provide service and act as backups at the same time, while in Active-Standby mode, the Standby cluster remains idle and it can back up multiple active clusters, but only one at a time. Refer to [SmartZone Cluster and Cluster Redundancy](#) on page 83 for detailed explanations about this feature.

Controller, Management and Data Planes

SmartZone controllers consist of distinct administrative/operational planes: the Control Plane, the Data Plane, and the Management Plane. The Control Plane is responsible for communication with the network-managed equipment (switches and access points) and other members within the SmartZone Cluster, by managing and exchanging the routing table information. On the other hand, the Management Plane handles all administrative tasks related to the controller. Finally, the Data Plane is utilized to efficiently encrypt and manage network traffic, forwarding the client traffic along the path according to the logic of the control plane.

External Data Planes

Made to work seamlessly with RUCKUS SmartZone controllers, the SmartZone Data Plane appliance enables end-to-end secure tunneled WLANs from RUCKUS APs to the Data Plane, while minimizing CAPEX spending and maximizing Wi-Fi deployment flexibility and scale. SZ100-D and SZ144-D are physical appliances, while vDP offers a virtualized concept that can be deployed on mostly known hypervisors. Refer to the *RUCKUS SmartZone Tunnel and Data Plane Guide* for everything related to deploying and managing Data Planes and tunneled WLANs.

Network Interfaces

When configuring a SmartZone controller for the first time, interface and routing information must be defined. The IP address or addresses of the different interfaces of the controller are configured within the setup wizard when the controller is initially deployed; nevertheless, those settings can be modified anytime using the web interface or the CLI.

Physical Network Interfaces

The vSZ-E, SZ-100, and SZ-144 use one, single, logical interface for Management, Control, and Cluster aspects.

For Virtual SmartZone High Scale (vSZ-H) there is a chance to optionally configure different physical network interfaces for the Control, Management, and Cluster functions separately. This enhances the network performance at a hardware level by separating control, cluster, and management traffic. This is recommended mostly for high-density deployments with a large number of Access Points, heavily utilized Data services, or network policies in the company to keep the traffic in separate network domains. In these scenarios, the IP addresses of the three interfaces must belong to different subnets.

NOTE

The configuration of separate physical interfaces for Control, Management, and Cluster functions in vSZ-H cannot be altered once the controller is deployed. If adjustments are required, please restore the controller to its factory defaults and perform a new configuration. Refer to the *RUCKUS SmartZone Troubleshooting and Diagnostics Guide* for comprehensive instructions on changing the interface configuration for a working controller.

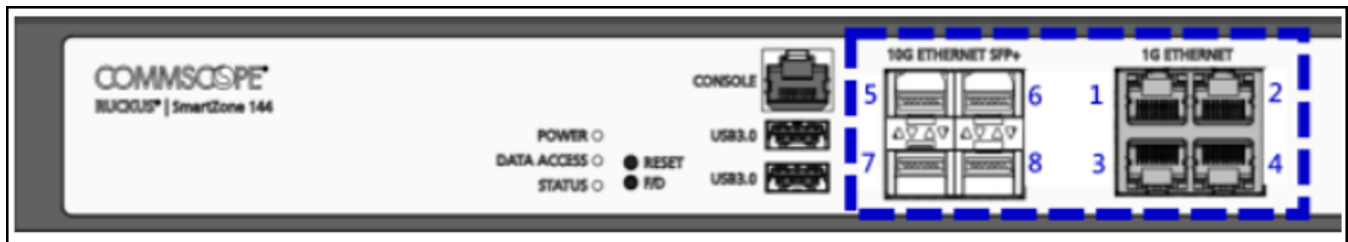
Port Group Configuration in Physical Appliances

SZ-100 and SZ-144 appliances have the option to configure the network interface in two different port-group layouts:

- Layout 1: One port group.

Management and AP tunnel combined.

FIGURE 1 SZ-144 Network Interfaces Configured as One Port Group

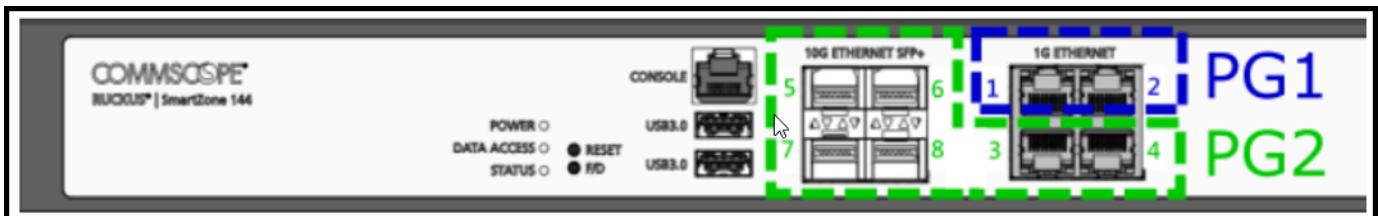


- Layout 2: Two port groups:

Port Group 1, for Management and AP control.

Port Group 2, for AP tunnel data.

FIGURE 2 SZ-144 Network Interfaces Configured as Two Port Groups



Refer to the SZ-100 or SZ-144 *Quick Setup Guide* document for port configuration instructions.

NOTE

The port group configuration for SZ100 or SZ144 cannot be modified after the controller has been put into operation. If changes are necessary, please revert the controller to its factory defaults and proceed with the reconfiguration process. Refer to the *RUCKUS SmartZone Troubleshooting and Diagnostics Guide*, for comprehensive instructions on changing the interface configuration for a working controller.

Configuring the Control Plane

Control Plane configuration includes defining the physical interface, user defined interface and static routes.

To configure a control plane:

1. Go to **Network > Data and Control Plane > Cluster**.
2. Select the control plane from the list and click **Configure**. The Edit Control Plane Network Settings form appears.
3. Configure the settings as explained in the table below.
4. Click **OK**.

NOTE

You must configure the **Control** interface, **IPv4 Cluster** interface, and **Management** interface 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.

TABLE 4 Configuring Control Plane

Field	Description	Your Action
Physical Interfaces		
IPv4-Control Interface	Indicates the management and IP control settings.	Select the IP Mode : <ul style="list-style-type: none"> ● Static (recommended)—To manually assign an IP address to this interface manually. <ul style="list-style-type: none"> - Enter the IP Address. - Enter Subnet Mask. - Enter the Gateway router address. - Enter Control NAT IP address. ● DHCP—To automatically obtain an IP address from a DHCP server on the network. <ul style="list-style-type: none"> - Enter Control NAT IP.
IPv4-Cluster Interface	Indicates the IPv4 cluster interface settings	Select the IP Mode : <ul style="list-style-type: none"> ● Static (recommended)—To manually assign an IP address to this interface manually. <ul style="list-style-type: none"> - Enter the IP Address. - Enter Subnet Mask. - Enter the Gateway router address. ● DHCP—To automatically obtain an IP address from a DHCP server on the network.
IPv4-Management Interface	Indicates the IPv4 management interface settings	Select the IP Mode : <ul style="list-style-type: none"> ● Static (recommended)—To manually assign an IP address to this interface manually. <ul style="list-style-type: none"> - Enter the IP Address. - Enter Subnet Mask. - Enter the Gateway router address. ● DHCP—To automatically obtain an IP address from a DHCP server on the network.

TABLE 4 Configuring Control Plane (continued)

Field	Description	Your Action
IPv6-Control Interface	Indicates the IPv6 control interface settings	<p>Select the IP Mode:</p> <ul style="list-style-type: none"> ● Static (recommended)—To manually assign an IP address to this interface manually. <ul style="list-style-type: none"> - Enter the IPv6 IP Address (global only) with a prefix length (for example, 1234::5678:0:C12/123) is required. Link-local addresses are unsupported. - Enter the IPv6 Gateway address (global or link-local) without a prefix length. For example, 1234::5678:0:C12 (global address without a prefix length) and fe80::5678:0:C12 (link-local address without a prefix length). ● Auto—To automatically obtain an IP address from Router Advertisements (RAs) or from a DHCPv6 server on the network.
IPv6-Management Interface	Indicates the IPv6 management interface settings	<p>Select the IP Mode:</p> <ul style="list-style-type: none"> ● Static (recommended)—To manually assign an IP address to this interface manually. <ul style="list-style-type: none"> - Enter the IPv6 IP Address (global only) with a prefix length (for example, 1234::5678:0:C12/123) is required. Link-local addresses are unsupported. - Enter the IPv6 Gateway address (global or link-local) without a prefix length. For example, 1234::5678:0:C12 (global address without a prefix length) and fe80::5678:0:C12 (link-local address without a prefix length). ● Auto—To automatically obtain an IP address from Router Advertisements (RAs) or from a DHCPv6 server on the network.
Access & Core Separation	Indicates that the management interface (core side) to be the system default gateway and the control interface (access side) to be used only for access traffic.	Select the Enable check box.
IPv4 Default Gateway & DNS	<p>Indicates the IPv4 gateway that you want to use - Control, Cluster, and Management.</p> <p>NOTE When Access & Core Separation is enabled, the Default Gateway field is hidden.</p> <p>NOTE The default gateway is NOT set to Control Interface. To properly route AP/UE traffic back through Control Interface, please make sure to enable Access & Core Separation or add static routes in Control Plane Network Settings on Web GUI.</p>	<ol style="list-style-type: none"> a. Default Gateway—Choose the Interface for which you want to assign the default gateway setting. b. Primary DNS Server—Enter the server details. c. Secondary DNS Server—Enter the server details.

TABLE 4 Configuring Control Plane (continued)

Field	Description	Your Action
IPv6 Default Gateway & DNS	<p>Indicates the IPv6 gateway that you want to use - Control, Cluster, and Management.</p> <p>NOTE When Access & Core Separation is enabled, the Default Gateway field is hidden.</p> <p>NOTE The default gateway is NOT set to Control Interface. To properly route AP/UE traffic back through Control Interface, please make sure to enable Access & Core Separation or add static routes in Control Plane Network Settings on Web GUI.</p>	<p>a. Default Gateway—Choose the Interface for which you want to assign the default gateway setting.</p> <p>b. Primary DNS Server—Enter the server details.</p> <p>c. Secondary DNS Server—Enter the server details.</p>
User Defined Interfaces		
<p>NOTE The control plane and the UDI must be on different subnets. If the control plane and UDI are on the same subnet, and assigned the same IP address, APs will be unable to communicate with the control plane. If the control plane and UDI are on the same subnet and assigned different IP addresses, hotspot clients will not be redirected to the logon URL for user authentication.</p>		
Name	Indicates the name of the interface.	Enter a name.
Physical Interfaces	Indicates the physical interface.	Select Control Interface .
Service	Indicates the service.	Select Hotspot , the hotspot must uses the control interface as its physical interface.
IP Address	Indicates the IP address that you want to assign to this interface.	Enter the IP address.
Subnet Mask	Indicates the subnet mask for the IP address.	Enter the subnet mask.
Gateway	Indicates the IP address of the gateway router.	Enter the gateway IP address.
VLAN	Indicates the VLAN ID that you want to assign to this interface.	Enter the VLAN ID.
Add	Adds the interface settings.	Click Add .
Static Routes		
Network Address	Indicates the destination IP address of this route.	Enter the IP address.
Subnet Mask	Indicates a subnet mask for the IP address.	Enter the subnet mask.
Gateway	Indicates the IP address of the gateway router.	Enter the IP address of the gateway router.
Interface	Indicates the physical interface to use for this route.	Select the interface.
Metric	Represents the number of routers between the network and the destination.	Enter the number of routers.
Add	Adds the static route settings.	Click Add .

NOTE

You can also delete or restart a control plane. To do so, select the control plane from the list and click **Delete** or **Restart** respectively.

User Defined Interface

You can only create one user-defined interface (UDI), and it must be for a hotspot service and must use the control interface as its physical interface. The control plane and the UDI must be on different subnets. If the control plane and UDI are on the same subnet, and assigned with the same IP address, APs will be unable to communicate with the control plane. If the control plane and UDI are on the same subnet and assigned different IP addresses, hotspot clients will not be redirected to the logon URL for user authentication.

NOTE

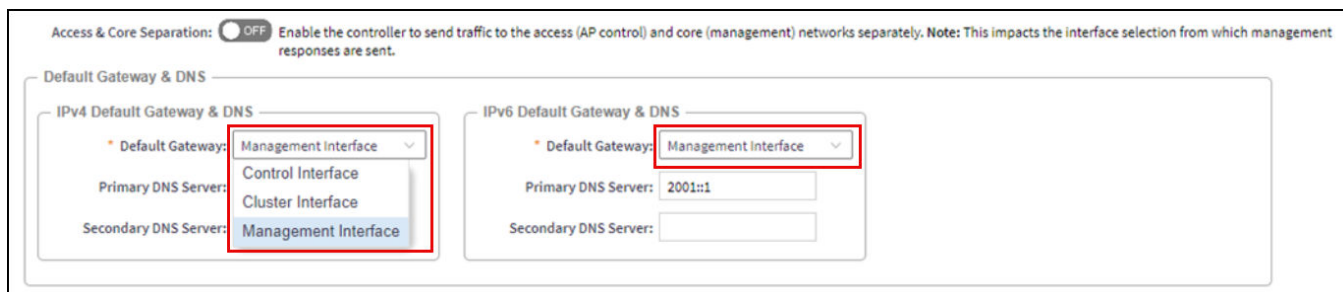
The User Defined Interface (UDI) is available in *Virtual SmartZone (High Scale and Essentials)* from Release 5.1.1.

Access and Core Segmentation

This configuration is specific to controllers using three separate physical interfaces (Control, Cluster, and Management interfaces), enabling you to configure separate routing domains through which the controller will communicate with the different parties in the network. To enable Access and Core Separation, navigate to **Network > Data and Control Plane > Cluster**; select the cluster for which you want to modify the configuration and click **Configure**; on the **Physical Interfaces** tab, click the **Access and Core Separation** toggle switch to 'ON'.

- **Enabled.** When enabled, the controller will communicate with the access points and switches using the Control Interface as the source interface. The Management Interface IP address will be used as the source for web access and other communications to external services. Ensure that you configure routable Default Gateway services within each of the Control Interface and Management Interface subnets to ensure accurate, efficient routing of communications.
- **Disabled.** When disabled, the controller will use one, single, source interface for all communications, simplifying the network configuration. Only the selected interface requires routable access to other networks and to the internet. As shown in Figure 3, you can choose which one of the interfaces will be used as the source interface for communications

FIGURE 3 Default Gateway Options when Access and Core Separation is Disabled



Static Routing

Static routing is used to manually configure routing entries. Static routes are fixed and do not change if the network is changed or reconfigured. Static routing is usually used to maximize efficiency and to provide backups in the event that dynamic routing information fails to be exchanged.

NOTE

It is important to carefully review and update the routing entries whenever changes are made to the network. This will ensure that you can maintain uninterrupted management access and AP communication.

IPv6 Configurations and Considerations

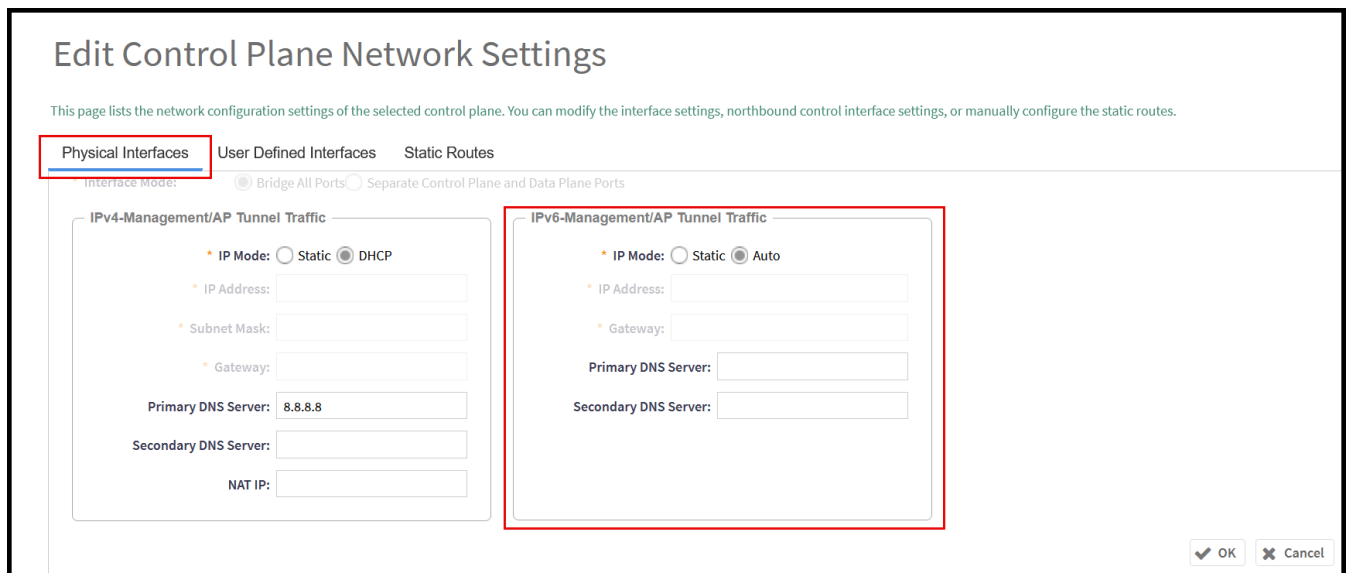
The IPv6 version support can be enabled within the installation wizard only during the initial setup process of the controller. SmartZone and Virtual SmartZone controllers offer the option to configure dual-mode IPv4/IPv6 addressing, or IPv4 only. Once configured and deployed, this configuration cannot be undone, unless the controller is set to factory defaults and re-deployed.

NOTE

Refer to the *RUCKUS Virtual SmartZone Quick Setup Guide* for additional details regarding the initial setup and the IP configuration options within the installation wizard of the controller.

To modify the current IPv6 configuration of the controller, navigate to **Network > Data and Control Plane > Cluster**, select the control plane that requires the modification, and click **Configure** (optionally, just double-click the node that requires the configuration). The **Edit Control Plane Network Settings** window opens; modify the configuration options as desired. Click **OK** to save the changes.

FIGURE 4 Edit Control Plane Network Settings Window



Controller DNS

The Control and Management Planes of the controller require a DNS server to be available. This DNS server can be a locally available server within the network, or it can be a public-access DNS server, like Google DNS or similar. It is important to make sure this DNS server is reachable by the controller.

NOTE

The DNS server mentioned in this section does not pertain to the DNS server utilized by wireless clients during their connection to the wireless network. For specific configuration instructions regarding the DNS server designated to serve WLANs and their wireless clients, refer to the *RUCKUS SmartZone Network Administration Guide*.

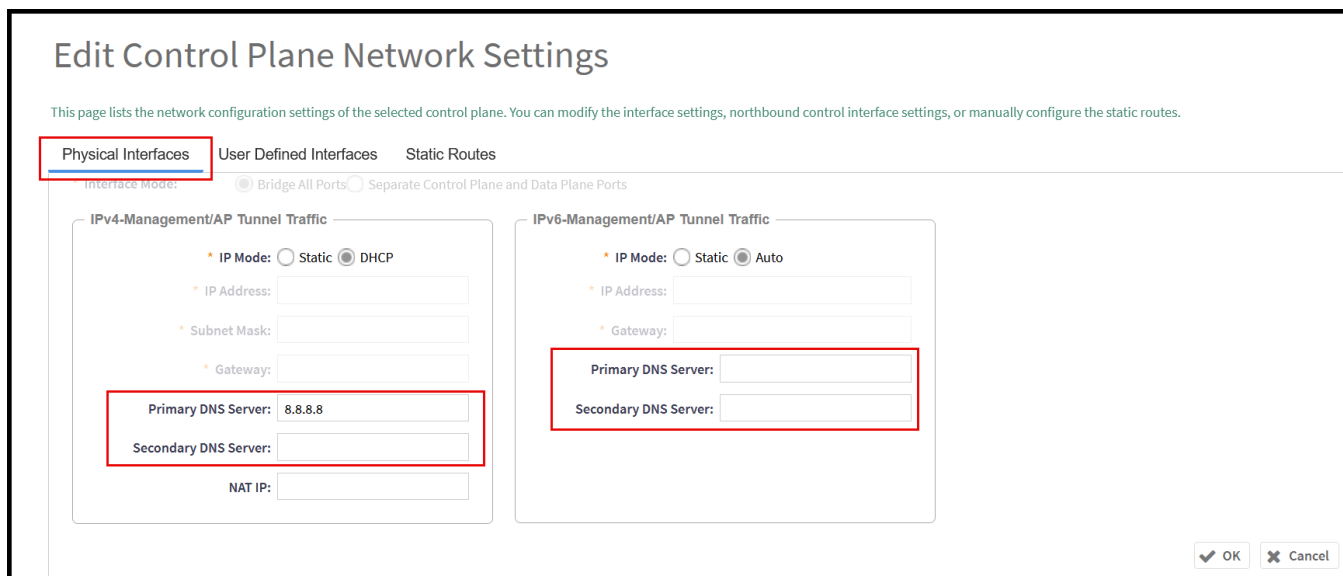
The DNS server configuration for the controller is defined within the setup wizard during the initial deployment; however, it can be updated through the web interface or the CLI, refer to *RUCKUS SmartZone Troubleshooting and Diagnostics Guide* for further details about updating the DNS server configuration using the CLI of the controller.

To update the controller's DNS configuration using the web UI:

1. From the main menu, navigate to **Network > Data and Control Plane > Cluster**.

2. Select the node from the **Control Planes** list.
3. Double-click the node in the Control Planes list or select the node and click **Configure**. The **Edit Control Plane Network Settings** window opens, and the DNS options appear at the bottom of the window.
4. Configure the IP addresses for the primary and secondary DNS servers. The secondary DNS server will be consulted by the controller after failing to connect to the primary server.

FIGURE 5 Controller DNS Configuration from the Web UI



Control NAT IP

The SmartZone controller can manage APs and switches locally, within the private LAN, or through the internet. For the SmartZone controller to manage devices across the internet, it requires a public, network address translation (NAT), IP address to be configured for the Control Plane.

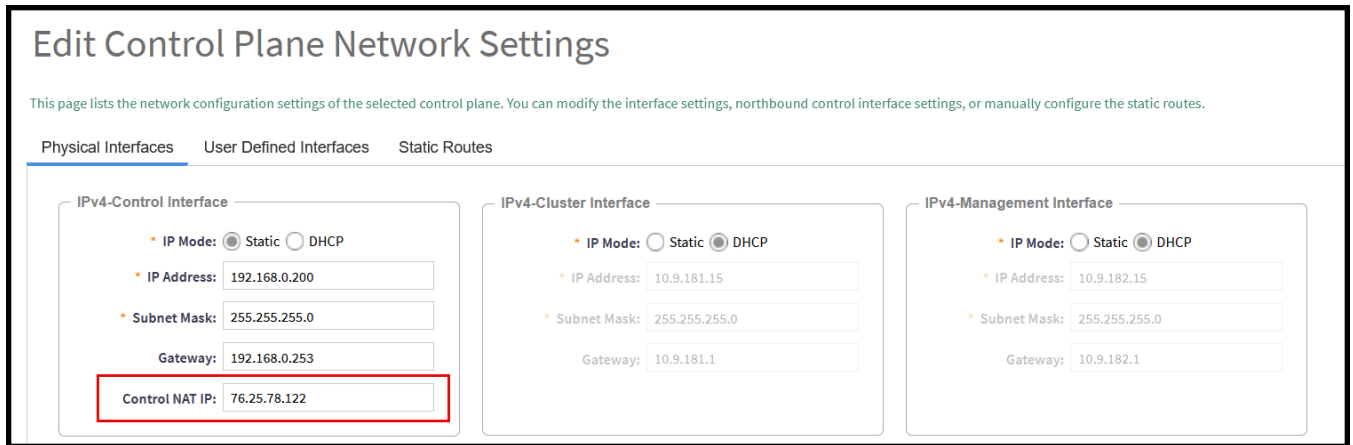
To configure the public IP address of the Control Plane:

1. From the main menu, navigate to **Network > Data and Control Plane > Cluster**.
2. Select the node from the **Control Planes** list.
3. Double-click the node in the Control Planes list or select the node and click **Configure**. The **Edit Control Plane Network Settings** window opens, and the Control Interface options appear.
4. Configure the public IP addresses for the Control Plane in the **Control NAT IP** field.

NOTE

This public IP address will be granted by your Internet Service Provider (ISP) or can be created at the Network Firewall/NAT level by the firewall administrator.

FIGURE 6 Configuring the Control NAT IP of the Controller



Viewing the Interface and Routing Configuration of the Controller

1. From the main menu, navigate to **Network > Data and Control Plane > Cluster**.
2. Select the node from the Control Planes list.
3. The IP addresses are displayed next to the node name in the Control Planes list. For additional details, scroll down to the **DETAILS** section and click the **Network Settings** tab.

FIGURE 7 Viewing the IP Address Information of the controller in the Control Planes list

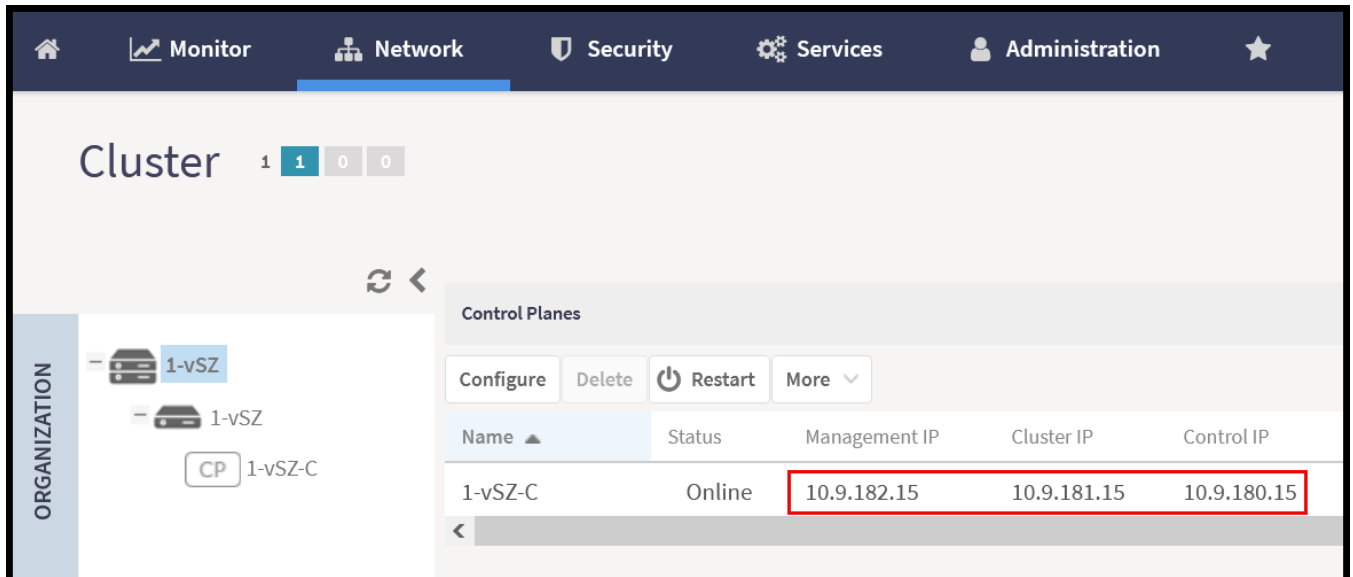


FIGURE 8 Viewing the IP Address Information of the Controller in the Network Settings Tab

	Summary	Network Settings	Configuration	Traffic & Health
DETAILS	Control Interface			
	IP Mode		Static	
	IP Address		10.9.180.15	
	Subnet Mask		255.255.255.0	
	Gateway		10.9.180.1	
	Cluster Interface			
	IP Mode		Static	
	IP Address		10.9.181.15	
	Subnet Mask		255.255.255.0	
	Gateway		10.9.181.1	
	Management Interface			

Configuring the System Time

The SmartZone controller uses Network Time Protocol (NTP) for time synchronization. There is an option to configure the primary NTP server for the controller within the setup wizard during the initial controller setup; optionally, this setting can be modified or more servers can be added at any time after the controller has been deployed.

The controller has three external Network Time Protocol (NTP) servers that are used to synchronize the time across points, cluster nodes, and virtual data planes.

Controller Setup

Configuring the System Time

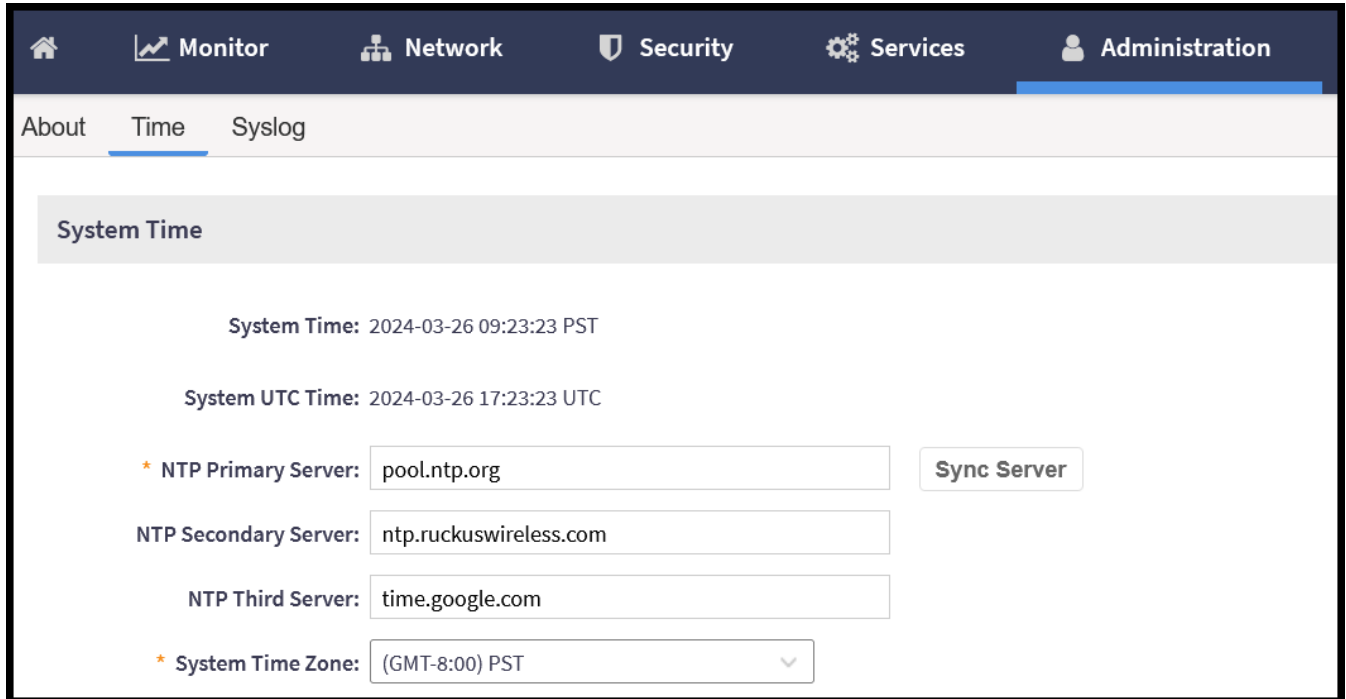
NOTE

The controller supports NTP version 4.2.6p5. The controller and access points do not accept broadcast and multicast NTP packets that would result in a timestamp. These packets are ignored by default.

To view the system time, navigate to **Administration > System > Time** from the main menu.

The **Time** tab is displayed. This tab consists of the System Time settings and the optional NTP Authentication settings for each of the configured NTP servers. Add or modify any of the variables and click **OK** at the bottom of this page to save the changes.

FIGURE 9 System Time Settings



System Time Settings

- **System Time:** It displays the current time received from the NTP server as per the configured System Time Zone.
- **System UTC Time:** Coordinated Universal Time (UTC) is the primary time standard by which the world regulates clocks and time. It is roughly equivalent to the time at the prime meridian (0 degrees longitude), located in Greenwich, England; however, UTC is not to be confused with Greenwich Mean Time (GMT). UTC is not impacted by Daylight Savings Time, meaning it remains constant throughout the year.
- **NTP Primary, Secondary, and Third Servers:** Enter the NTP server address or domain name for each of the NTP servers. Only the primary server is mandatory; secondary and third servers are optional. The secondary and third servers are used only when the primary server is not available.
- **Sync Server:** Click this button to enable the controller to sync with the configured NTP server, and then sync the cluster-follower nodes, APs, and vDPs with the controller time.
- **System Time Zone:** This setting refers to the time zone of the controller based on its geographical location. In a multiple-nodes cluster scenario where the nodes are distributed across different time zones, select a time zone that aligns with the time zone or the primary location where administrative tasks are managed.

NTP Server Authentication Settings

You can achieve secured communication with NTP servers after configuring them.

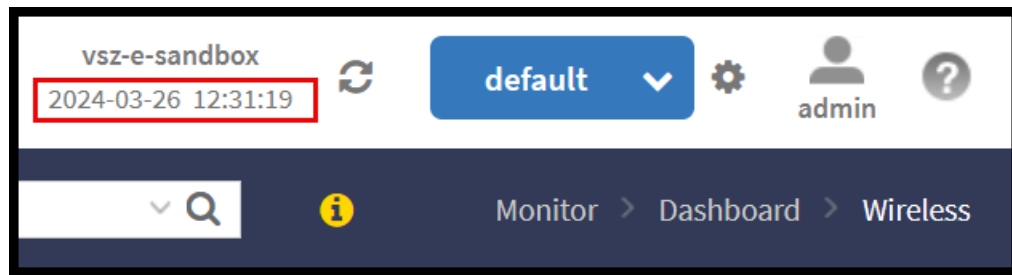
To establish this communication, in the **NTP Server Authentication** field, configure the following:

- **Key Type** as MD5 or SHA1.
- **Key ID** in the range of 1 to 65534.
- **Key or PSK** as negotiated for each of the NTP servers.

NOTE

The time information that is permanently displayed at the top of the Web UI does not reflect the configured time of the controller (System Time), instead, it refers to the local time of the web client accessing the controller Web UI. For instance, if the system time zone in the System Time setting is configured for US Pacific time, but the user is accessing the controller from Europe, the time shown at the top of the Web UI will display the local time of the web client in Europe.

FIGURE 10 Local Time of the Web Client Accessing the Controller Web UI



NOTE

Alarms and events shown in the Web UI display the local time of the web client accessing the controller. However, application logs of the controller, AP support logs, and Data Plane logs reflect UTC as per the time sync received from the configured NTP servers.

SmartZone Web Interface

- [Introduction to SmartZone Web Interface.....](#) 27
- [Setting User Preferences.....](#) 31
- [Managing the Access Control of the Management Interface.....](#) 35
- [Global Filters Overview.....](#) 37
- [Using the Dashboard.....](#) 38

Introduction to SmartZone Web Interface

RUCKUS SmartZone network controllers simplify the complexity of scaling and managing wired switches and wireless access points (APs) through a common interface to support private cloud Network as a Service (NaaS) offerings in addition to general enterprise networks.

All physical and virtual SmartZone appliances support network configuration, monitoring, provisioning, discovery, planning, troubleshooting, performance management, security, and reporting. The user-friendly SmartZone Web Interface handles network visibility from the wireless edge to the network core and enables IT administrators to perform day-to-day management tasks, troubleshoot user-connectivity problems, and define and monitor user and application policies without requiring advanced network skills and command line interface (CLI) expertise.

Controller Web Interface Features

The controller web interface is the primary graphical front end for the controller and is the primary interface.

You can use the controller web interface to take the following actions:

- Manage access points and WLANs
- Create and manage users and roles
- Monitor wireless clients, managed devices, and rogue access points
- View alarms, events, and administrator activity
- Generate reports
- Perform administrative tasks, including backing and restoring system configuration, upgrading the cluster, downloading support, performing system diagnostic tests, viewing the status of controller processes, uploading additional license, and other administrative tasks

Rest API

REST API stands for Representational State Transfer Application Programming Interface. It is an HTTP-based architectural style for designing networked applications. REST APIs allow communication between different software systems over the internet by using standard HTTP methods such as GET, POST, PUT, DELETE, and so on, to perform various operations on resources.

Overall, REST APIs provide a flexible and scalable approach to building web services, making them widely used in modern web development for building APIs that power web applications, mobile apps, IoT devices, and more.

Read/Write Support Rates

The read and write support rates in a REST API refer to the ability of the API to handle requests for reading (retrieving data) and writing (creating, updating, or deleting data) operations.

TABLE 5 SmartZone Rest API Support Rate

Release Summary	Rate (requests)
SZ API Read Support Rate	170 / min
SZ API Write Support Rate	135 / min

NOTE

To assess the performance of a REST API in terms of read and write support rates, various performance testing techniques are employed. This may involve load testing, stress testing, and benchmarking the API under different scenarios to ensure it meets performance requirements, such as response time targets and throughput thresholds, for both read and write operations.

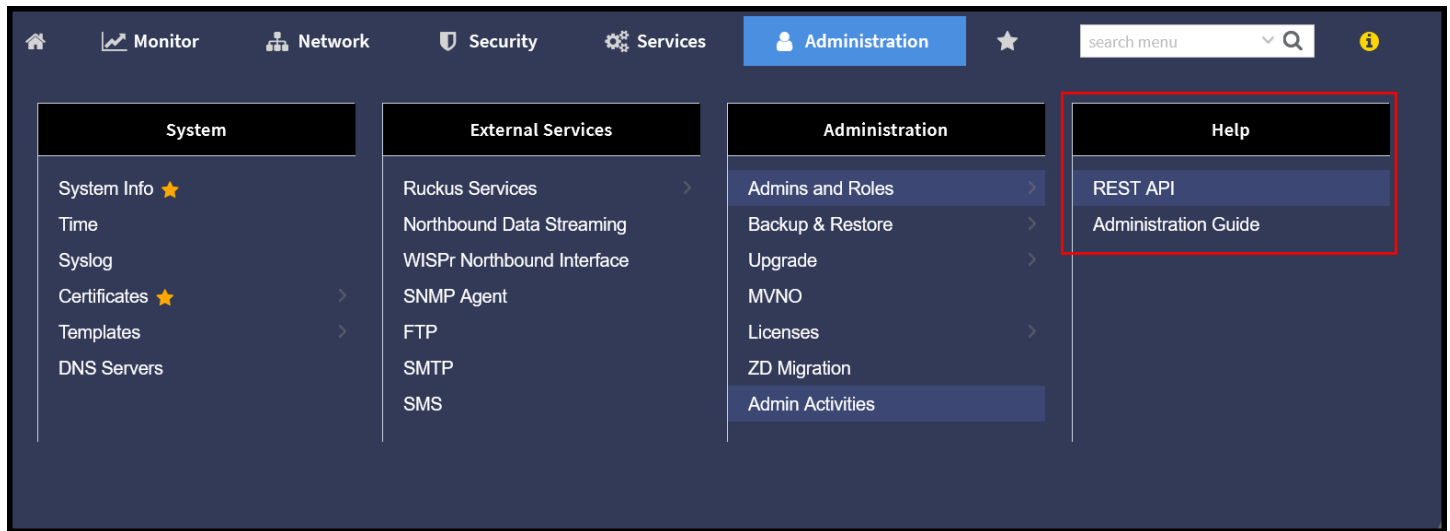
Help with the GUI and APIs

The **Help** tab provides access to online REST API and administration guides.

To access these resources, select **Administration > Help** and choose between the following two options:

- **REST API** to view the applicable *SmartZone Public API Reference Guide*
- **Administration Guide** to visit the online library containing the SmartZone documentation

FIGURE 11 Accessing Help Resources



Logging in to the Web Interface

Before you can log in to the controller web interface, you must have the IP address that you assigned to the Management (Web) interface when you set up the controller on the network using the Setup Wizard.

Once you have this IP address, you can access the controller web interface on any computer that can reach the Management (Web) interface on the IP network.

Complete the following steps to log in to the controller web interface.

1. Start a web browser on a computer that is on the same subnet as the Management (Web) interface.

The following web browsers are supported:

- Google Chrome

- Safari
 - Mozilla Firefox
 - Internet Explorer
 - Microsoft Edge
2. In the address bar, enter the IP address that you assigned to the Management (Web) interface, and append a colon (:) and 8443 (the management port number of the controller) to the end of the address.

For example, if the IP address that you assigned to the Management (Web) interface is 10.10.101.1, you should enter: <https://10.10.101.1:8443>.

NOTE

The controller web interface requires an HTTPS connection. You must append "https" (not "http") to the Management (Web) interface IP address to connect to the controller web interface. Because the default SSL certificate (or security certificate) that the controller is using for HTTPS communication is signed by RUCKUS and is not recognized by most web browsers, a browser security warning may be displayed.

The controller web interface logon page is displayed.

3. Log in to the controller web interface using the following credentials:

- **User Name:** admin
- **Password:** Password you set in the Setup Wizard

4. Click **Log On**.

The controller web interface displays the **Dashboard**, which indicates that you have logged on successfully.

Logging Off Using the Web Interface

1. On the controller web interface, click your user profile icon in the upper-right corner of the Web UI, then click Log off in the drop-down menu.

The following message is displayed: Are you sure you want to log off?

2. Click **Yes**.

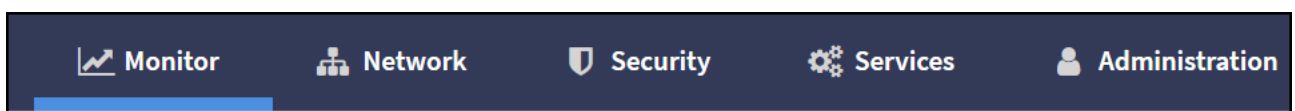
You have completed logging off the web interface

Controller User Interface (UI)

Prior to SmartZone release 6.0.0, the controller menu had a vertical layout that resulted in some menu items not being visible on the screen. To make navigation easier, a new menu was introduced in SmartZone 6.0.0 release. The new menu features logical categories, as well as the ability to mark specific menu options as favorites, search using keywords, and navigate using a breadcrumb trail.

- **Category** - The menu items are organized into distinct categories or groups making it easier to find and access specific functionalities. The categories are **Monitor**, **Network**, **Security**, **Services**, and **Administration**.

FIGURE 12 Displaying Categories on the Menu Bar



SmartZone Web Interface

Introduction to SmartZone Web Interface

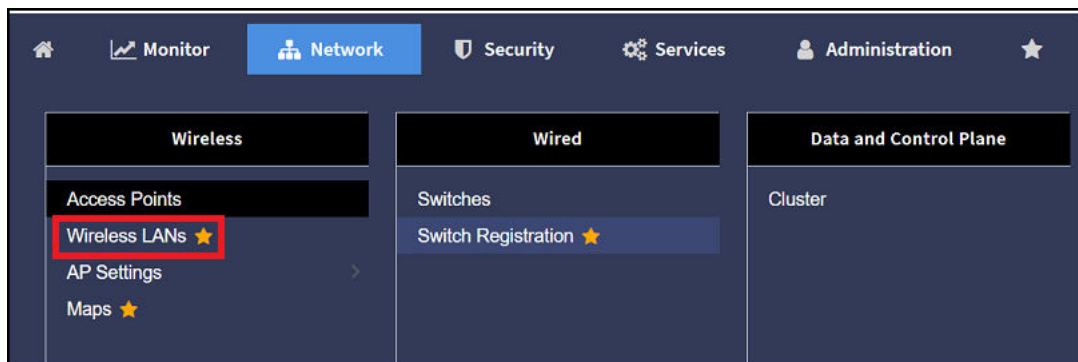
For example, the menu items under the category **Network** are displayed as per the screenshot below.

FIGURE 13 Displaying Menu Items in the Network Category



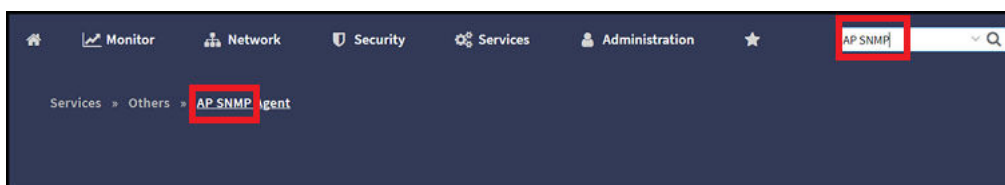
- Favorite - The **Star** icon allows you to mark menu items as favorites. This saves you time by providing quick access to the functions you use most often; simply click the star icon on the main menu to access a list of single-click links to your favorite menu options. The star icon acts like a toggle allowing you to add or remove any menu item to or from your list of favorites.

FIGURE 14 Marking Favorites



- Search - The **Search** menu facilitates UI navigation by allowing you to input specific menu keywords or specific terms. When you use the search option, it queries the system and returns results that match your input, making it easier to locate specific menu options.

FIGURE 15 Using the Search Field



- Breadcrumb Trail - The **Breadcrumb trail** a navigation aid that shows your current location within the menu hierarchy. This allows you to see where you are and easily navigate back to previous levels.

- Search History - The **Search history** provides a record of the searches you have previously conducted, listing the keywords or phrases you entered when searching for information. Hovering your mouse over an entry in the search history allows you to rerun the search or delete the entry from the search history.

FIGURE 16 Web UI Navigation Using the Breadcrumb Trail

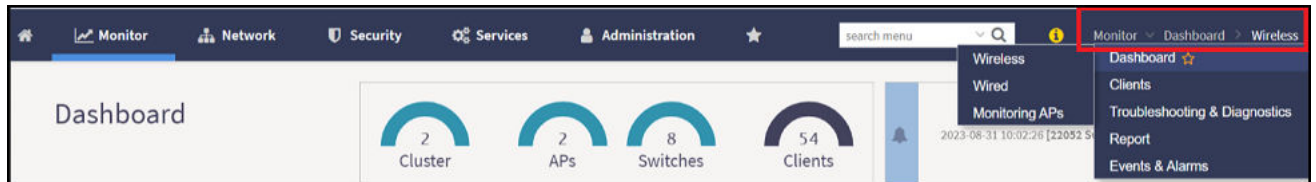


FIGURE 17 Search History



Setting User Preferences

The SmartZone Web UI allows you to configure different preferences including the language, legacy mode, and others.

To access these settings, click the user profile icon in the upper-right corner of the Web UI and select **Preferences**. The **User Preferences** window is displayed. These settings are user specific.

FIGURE 18 Accessing User Preferences

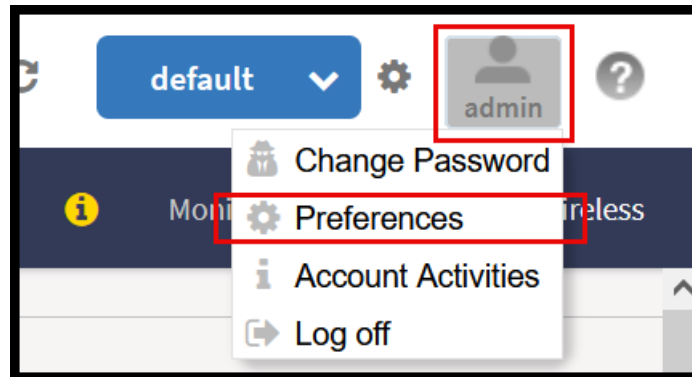
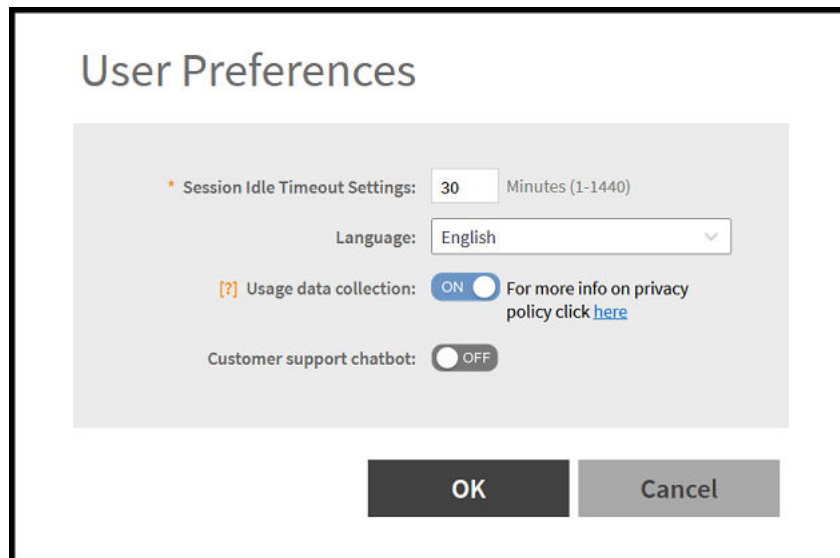


FIGURE 19 User Preferences Menu

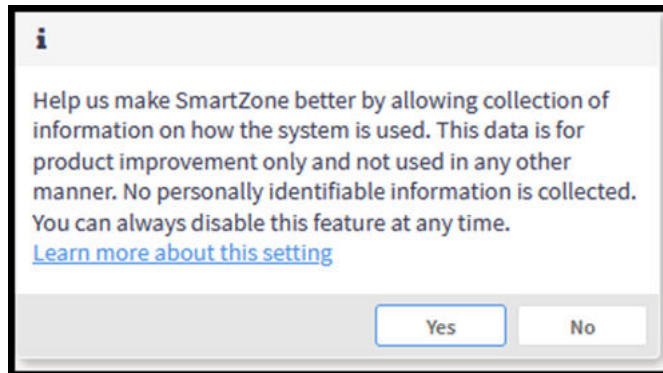


The configurable options are:

- **Session Idle Timeout Settings** - The duration in minutes that the Web UI can remain idle before you are automatically logged off.
- **Language** - Select the language of your choice from the drop-down list to view the web interface content. The following languages are supported in the application -
 - English
 - Spanish
 - Brazilian Portuguese
 - French
 - German
 - Italian
 - Russian
 - Simplified Chinese

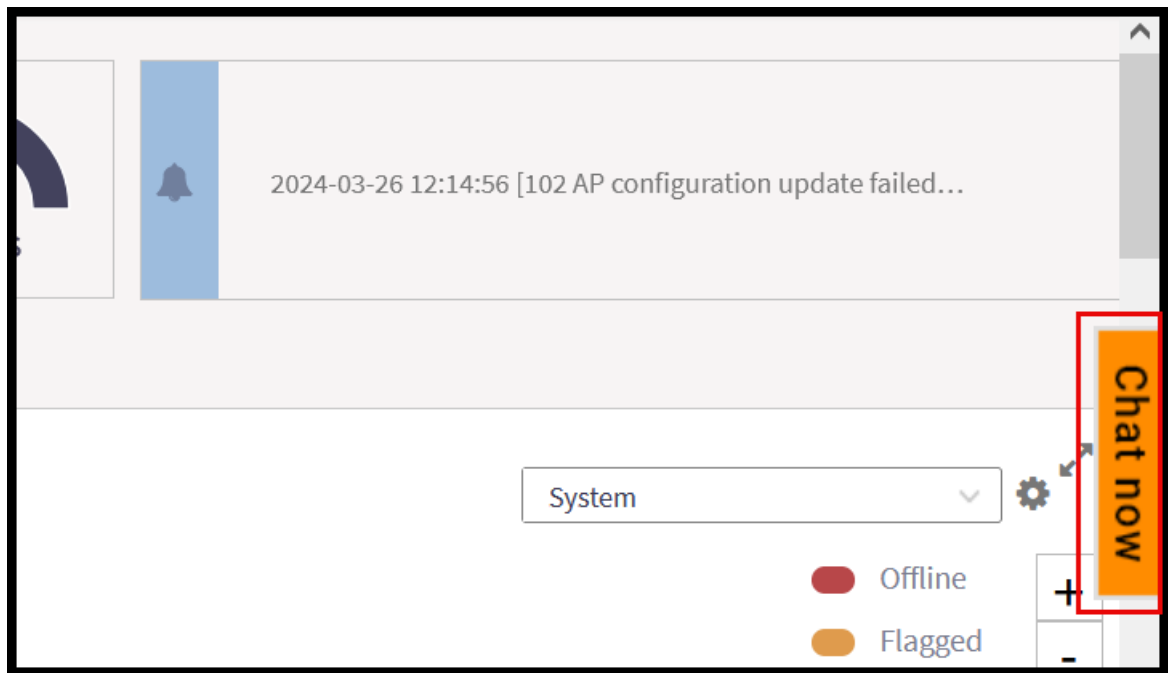
- Traditional Chinese
- Korean
- Japanese
- **Usage Data Collection** - By default, this toggle switch is **OFF** (disabled). Enable this option to collect data usage statistics and anonymous configuration information. This option helps optimize UI pages and features by learning from the way the product is used. This data is for product improvement only and is not used in any other manner. No personally identifiable information is collected.

FIGURE 20 Usage Data Collection Pop-up Message



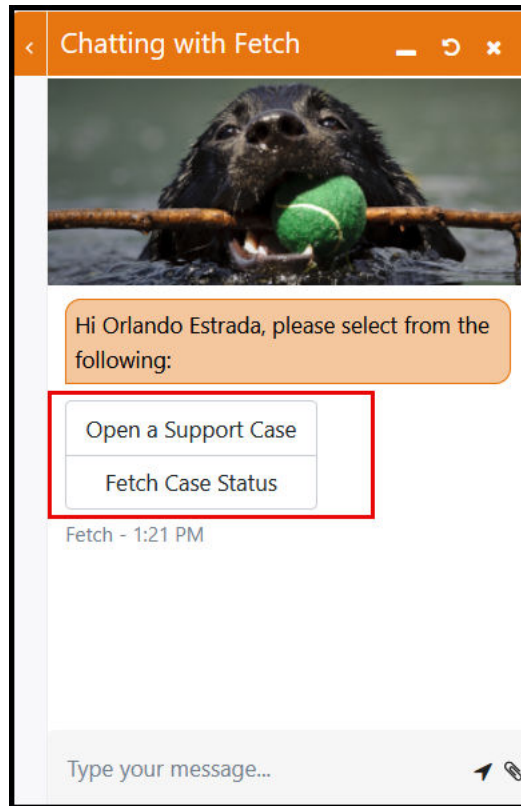
- › **Customer Support Chatbot** - By default, this option is enabled (toggled **ON**). This option enables the **Chat now** feature, accessible on the right-hand side of browser window from anywhere in the SmartZone Web UI. When you click **Chat now**, you will be prompted to log in, register, or continue as a guest. To chat with a RUCKUS support agent, you must authenticate by logging in to the service using an active RUCKUS account. Otherwise, the chat session will be restricted to accessing the Knowledge Base and online help only.

FIGURE 21 Chat Support Feature in the Web UI



Once logged in with a valid account, the **Chat Now** feature will enable you to fetch information about support cases or even open a new support ticket, if needed.

FIGURE 22 Chatting with Fetch



Managing the Access Control of the Management Interface

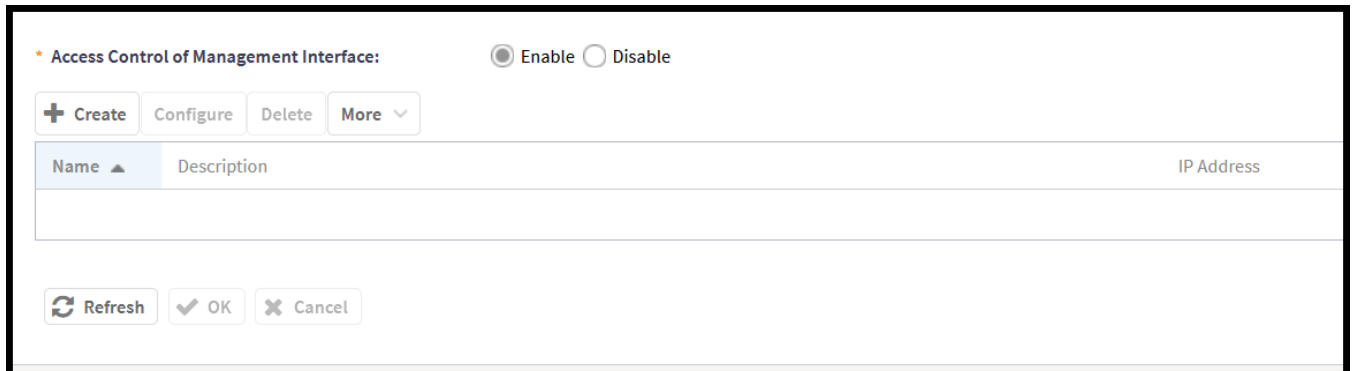
Administrators of the SmartZone controller are provided with the option of enabling Access Control Lists (ACLs) to regulate access to the Web UI. When enabled, this feature will provide access to the Web UI for only the specified IP address or addresses. Be careful when enabling this feature to ensure that the access configuration does not prohibit your access.

Complete the following steps to enable ACLs for the management interface:

1. Click **Administration > Admins and Roles > Access Control List**.

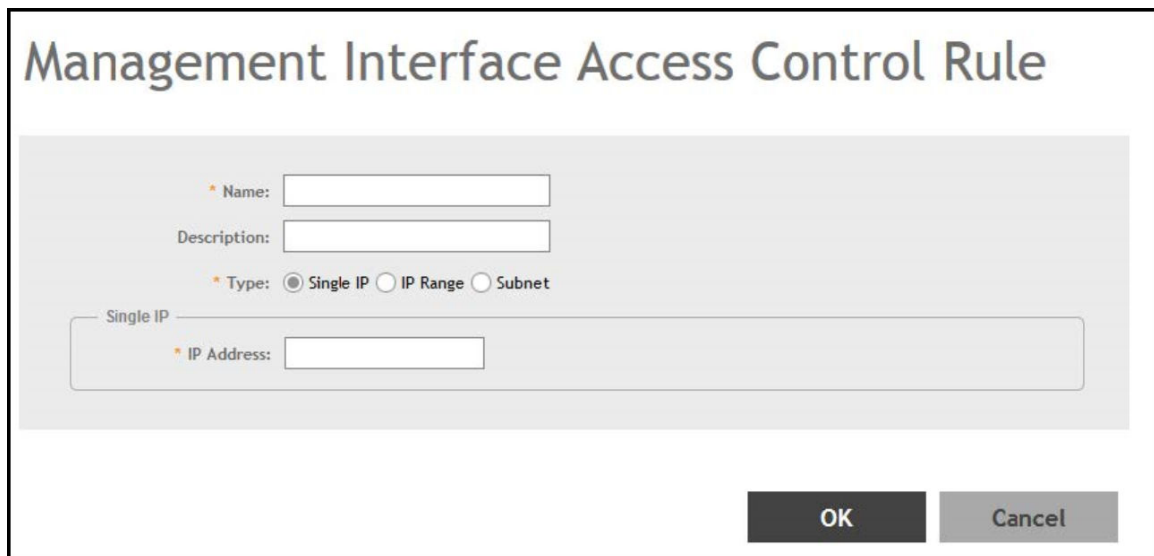
The **Access Control List** tab is displayed.

FIGURE 23 Enabling the Access Control of Management Interface Option



2. Select **Enable** to enable this feature.
3. Click **Create**.

FIGURE 24 Management Interface Access Control Rule



The **Management Interface Access Control Rule** page appears.

4. Enter the following:
 - a. **Name:** Type a name to identify the rule.
 - b. **Description:** Enter a short description for the rule.
 - c. **Type:** Select one of the following:
 - **Single IP:** Enter the IP address of the host that will be allowed access.
 - **IP Range:** Type the range of IP addresses that will be allowed access.
 - **Subnet:** Type the network address and subnet mask address of the subnet that will be allowed access.
 - d. Click **OK**.

5. Click **OK** to save the changes in the **Access Control List** tab.

NOTE

You can also edit and delete the list by selecting the options **Configure** and **Delete**, respectively, from the **Access Control List** tab.

Global Filters Overview

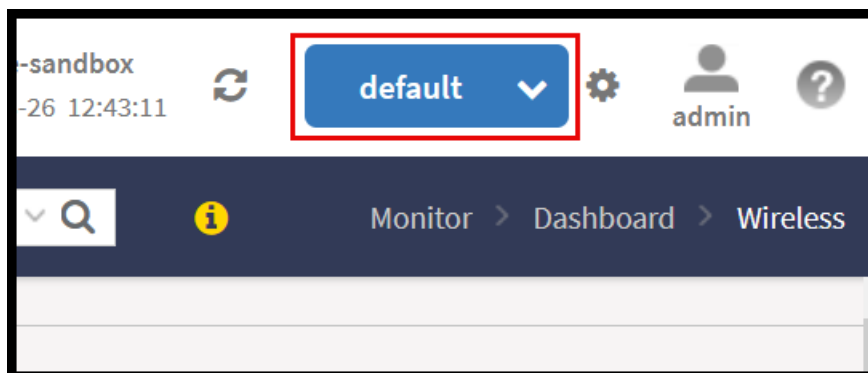
Global filters allow you to define a system scope or system context that applies to all pages of the system as you navigate to different menus. For example, if your system includes five zones, but you want to view Zone1 and Zone2 only, you can create and apply such a filter. As you navigate throughout the system, the view will be restricted to show only the data, objects, and profiles contained within Zones 1 and 2.

Configuring Global Filters

Configure the preferred filter as follows.

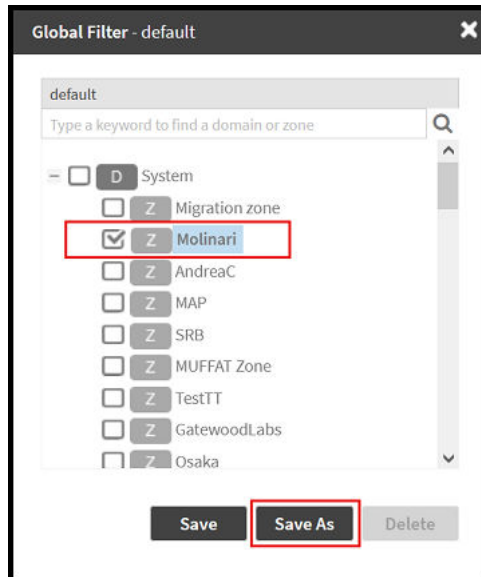
1. Click the gear icon next to the Global Filter indicator located in the upper-right corner of the Web UI.
The **Global Filter - default** window is displayed.

FIGURE 25 Global Filter Indicator



2. In the **Global Filter - default** window, check the boxes for the Domains or Zones of interest for the new filter.
3. Click **Save As** to save the selection as a new filter or click **Save** to save the selection as the default filter. Any new filter can be deleted using the **Delete** option.
4. The new filter has been created and it will be automatically selected. You can switch to a different filter from the drop-down menu available in the Global Filter indicator.

FIGURE 26 Global Filter - Create a New Filter



Using the Dashboard

The Dashboard is not only the home page of the controller Web UI. The Dashboard is a centralized place where you can monitor the SmartZone cluster, the access points and switches, and the wireless clients, as well as the traffic trends and other performance indicators.

Warnings

Warnings are displayed in the Header Bar. They are issues which are critical in nature. Warnings cannot be removed or acknowledged unless the critical issue is resolved.

FIGURE 27 Sample Warning Message



A list of warning messages that appear are as follows:

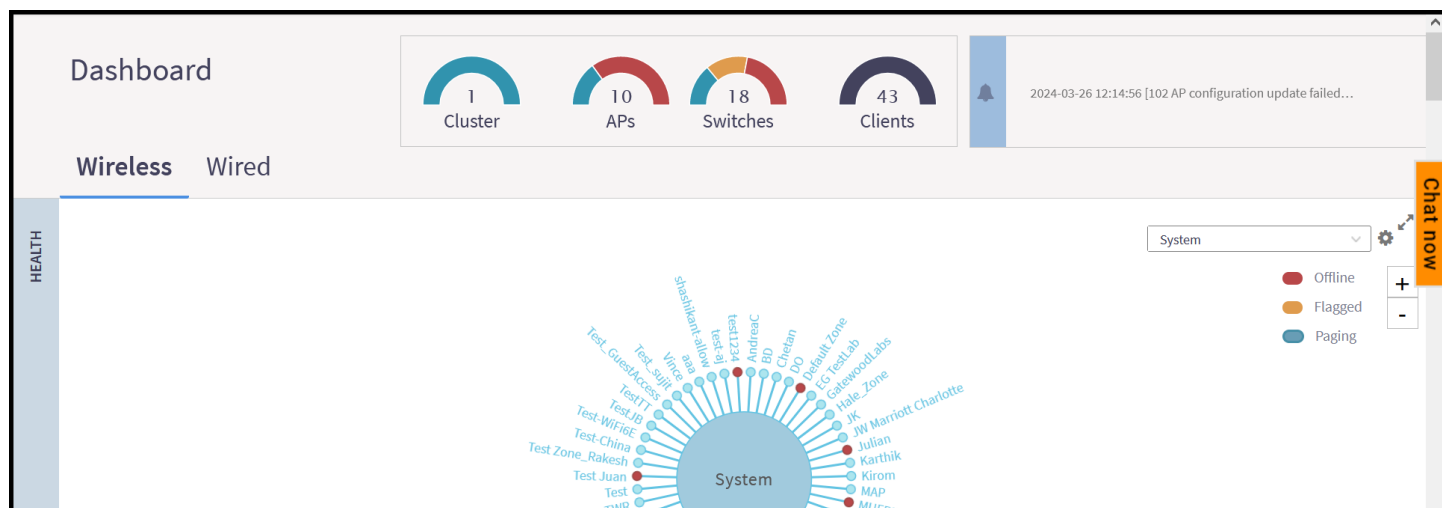
- Default 90-day support expiring soon
- System support expiring soon
- System support has expired
- Default 90-day AP license expiring soon
- Default AP license has expired
- Default 90-day RTU license expiring soon
- RTU has expired
- AP Certificate Expiration

- Node Out of Service
- Cluster Out of Service
- VM Resource Mismatch
- Suggested AP Limit Exceeded
- AP/DP version mismatch

Health

The Health dashboard gives you a very high-level overview of wireless devices such as cluster, AP and clients, and wired devices such as ICX switches. For wireless devices, it displays a world map view using Google Maps, which provides a global view of your SmartZone-controlled wireless network deployments.

FIGURE 28 Dashboard Main Panel

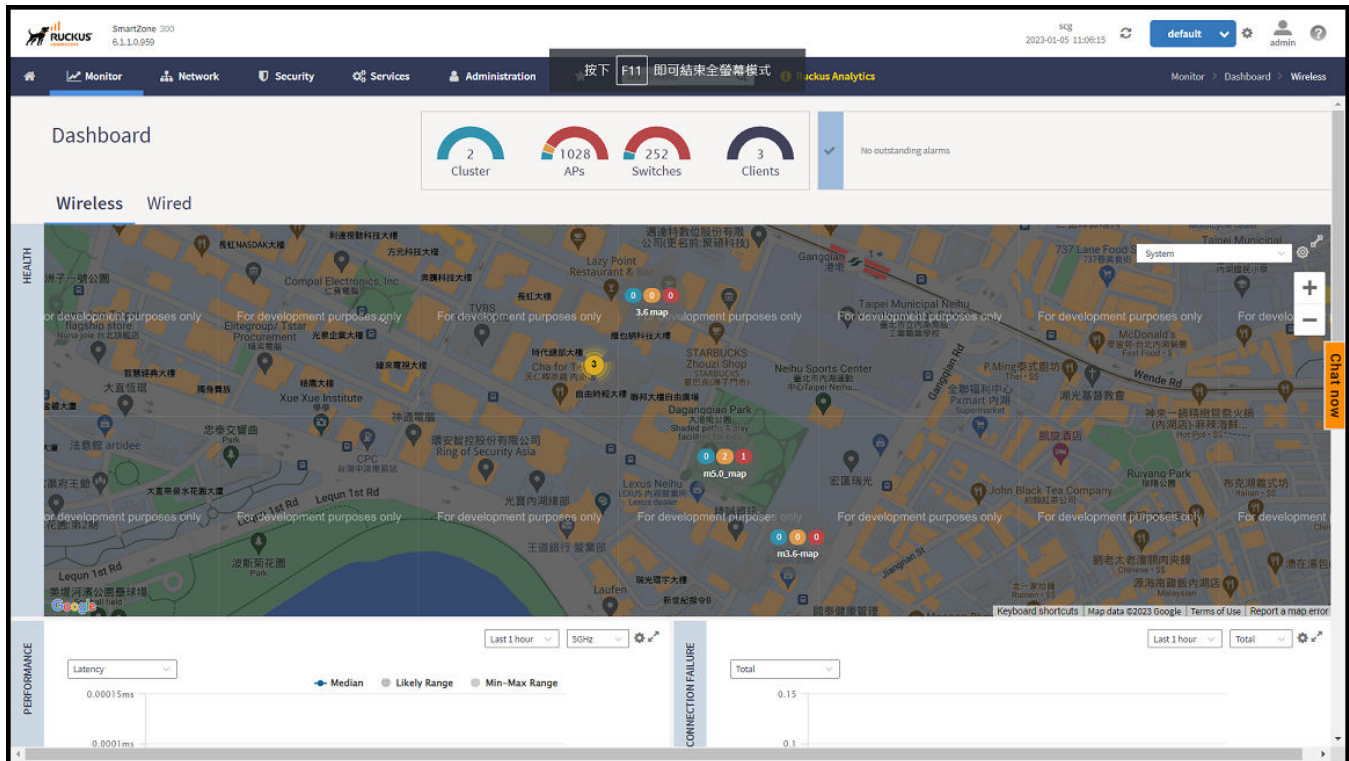


p

You must click **Wireless** or **Wired** in the dashboard to view the respective devices.

The status bar at the top of the Health dashboard contains an iconic representation of the total Cluster, AP and Client counts for the entire system. This information can be filtered to display a single zone, AP group, or venue using the drop-down filter menu. You can also customize the dashboard layout and threshold settings using the Settings (gear) icon.

FIGURE 29 Health Workspace Area



The Wired devices section provides information about the health of the switch and the traffic it handles.

Understanding Cluster and AP Health Icons

The Health dashboard status bar displays the following Cluster and AP information using three colored icons to denote the number of APs/clusters currently in that state.

The icons for both Cluster and AP status overviews are represented by the following color coding scheme:

- (Bue): Paging
- (Orange): Flagged
- (Red): Offline

Online and Offline status are self-explanatory. "Flagged" status is user-defined. You can customize the thresholds at which an AP or cluster enters the "flagged" state using the **Settings** (gear) icon in the status bar.

Customizing Health Status Thresholds

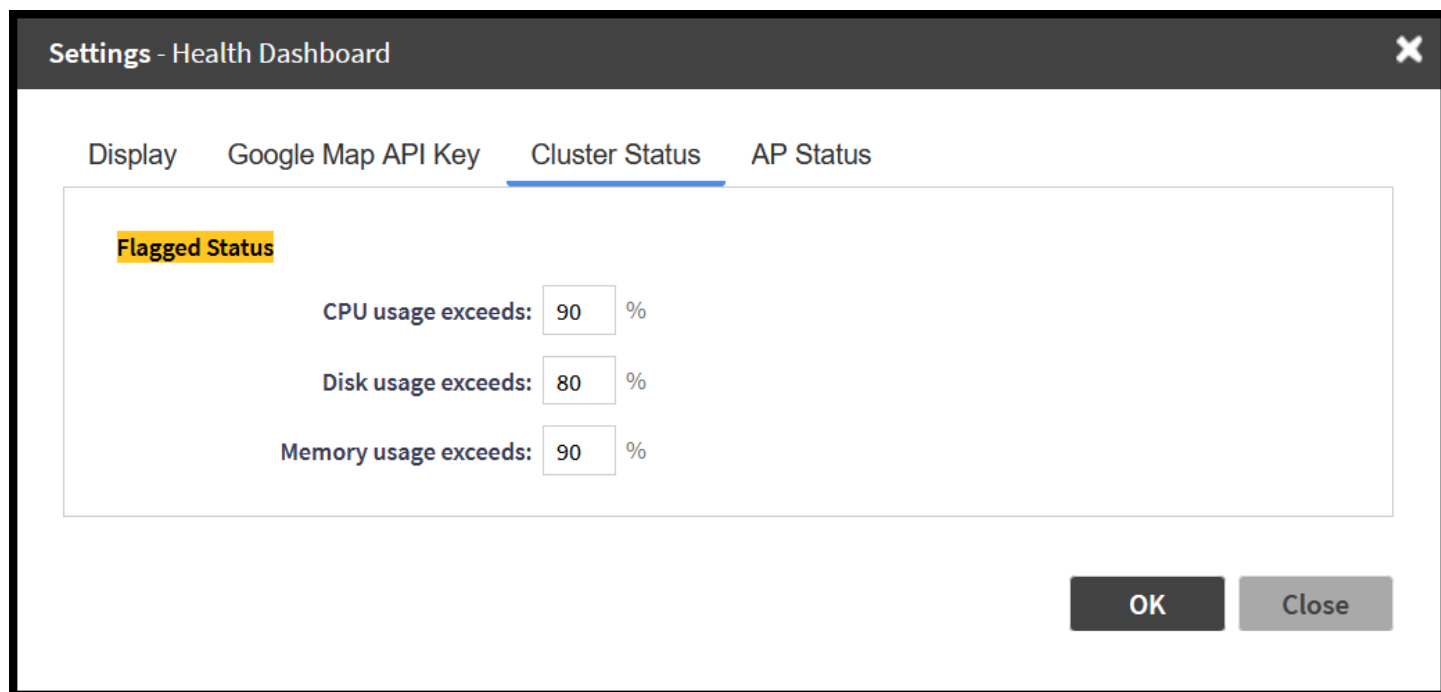
You can customize the way the controller categorizes and displays clusters and APs shown in "Flagged Status" in the status bar.

To customize the Health dashboard, click the **Settings** (gear) icon. In the **Settings - Health Dashboard** pop-up window, click the **Cluster Status** or **AP Status** tab, and configure the following:

- **Cluster Status:** Configure CPU, hard disk and memory usage percentages above which the cluster will be marked as flagged status.

- **AP Status:** Configure the criteria upon which APs will be flagged.

FIGURE 30 Setting Cluster Health Status Thresholds



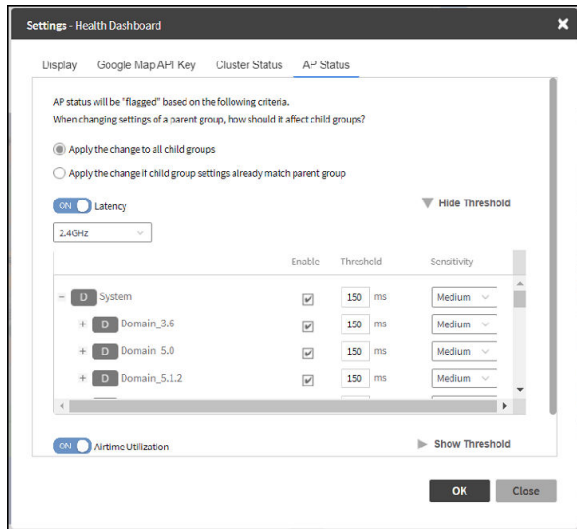
Customizing AP Flagged Status Thresholds

Use the following procedure to customize when APs will be marked as "flagged" on the Health dashboard status bar.

1. Click the **Gear** icon on the **Health** dashboard.
2. The **Settings - Health Dashboard** pop-up window appears. Click the **AP Status** tab.
3. Select the behavior of flagging policies when applying changes to parent or child groups:
 - Apply the change to all child groups
 - Apply the change if child group settings already match the parent group
4. Configure thresholds above which APs will be marked as "flagged" for the following criteria:
 - Latency
 - Airtime Utilization
 - Connection Failures
 - Total connected clients
5. Configure the radio (2.4 GHz /5 GHz/6 GHz) from the drop-down menu and select the level (system, zone, AP group) at which you want to apply the policy, and configure the **Sensitivity** control for the threshold (Low, Medium, High). Setting the Sensitivity level to Low means that an AP must remain above the threshold for a longer period of time before it will appear in the flagged category, while a High sensitivity means that APs will more quickly alternate between flagged and non-flagged status.

6. Click **OK** to save your changes.

FIGURE 31 Configuring AP Flagged Status Thresholds



Global Notifications

Notifications are integrated with existing alarms and they are displayed only when a notification alarm exists and is not acknowledged by the administrator. Notifications can be viewed from the **Content** area. Administrators can acknowledge the notification by either:

- Clearing the alarm
- Acknowledging the Alarm

For more information, refer to *RUCKUS SmartZone Network Administration Guide*.

Alarms are categorized as one of three types:

- Minor
- Major
- Critical

The administrator can change the alarm severity shown on the dashboard. To do so:

1. From the Notifications area, Click the **Setting** icon, this displays **Settings - Global Notification** window.
2. From the **Lowest alarm severity** drop-down, select the required severity level.
3. Click **OK**. Notifications corresponding to the selected alarm severity and all higher severities are displayed in the Notification area of the Dashboard.

NOTE

RUCKUS AI is configured on the SmartZone (controller) platform. When the user connects to RUCKUS AI through the controller, a status tag is displayed in the controller header and the browser redirects the user to RUCKUS AI page. Currently, this feature is dependent on RUCKUS AI.

NOTE

Global notifications will be shown in the dashboard regardless of the access level of the web interface administrator. For example, if the administrator has switch-only access, AP notifications will still be visible.

Using the Health Dashboard Map

Use the Google Maps view just as you would normally use Google Maps - including zoom, satellite view, rotate and even street view icons. You can customize the AP icon information displayed on the map using the tools in the upper-right hand corner.

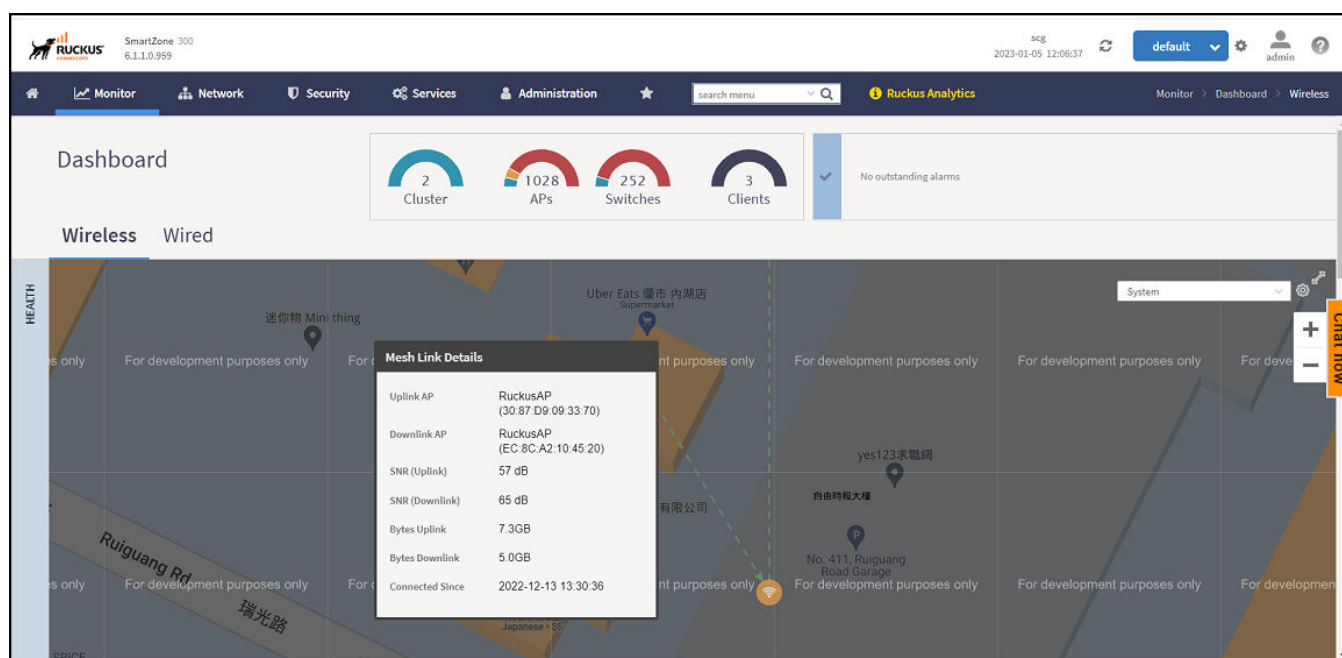
For SZ100 and vSZ-E platforms, use the **AP Status** pull-down menu to configure which AP health parameters will be displayed on the AP icons on the map. Use the Display menu to display the client count or radio channel in use.

Use the **Settings** icon to configure the information displayed in tooltips when hovering over an AP on the map. You can also change the view mode altogether, from map view to Groups, Control Planes or Data Planes view mode using the settings menu. Additionally, you can also select the checkbox to show mesh links. These links appear as dotted lines. If you hover over the mesh link on the map, a pop-up appears displaying more information such as the following:

- Uplink AP: displays the IP address of the uplink AP to which the wireless client sends data
- Downlink AP: displays the IP address of the downlink AP from which data is sent back to the wireless client
- SNR (Uplink): displays the signal-to-noise ratio in the uplink path
- SNR (Downlink): displays the signal-to-noise ratio in the downlink path
- Bytes (Uplink): displays the bytes of data transferred from the client to the uplink AP
- Bytes (Downlink): displays the bytes of data transferred from the downlink AP to the client
- Connected Since: displays the date and time when the mesh connection was established

Bytes (Uplink) and Bytes (Downlink) are aggregate counters for the mesh connection since the start of that mesh connection. If the mesh link is broken and restarts, the counter restarts. If the mesh AP connects to a different mesh root or uplink, the counter restarts.

FIGURE 32 Mesh Link Details



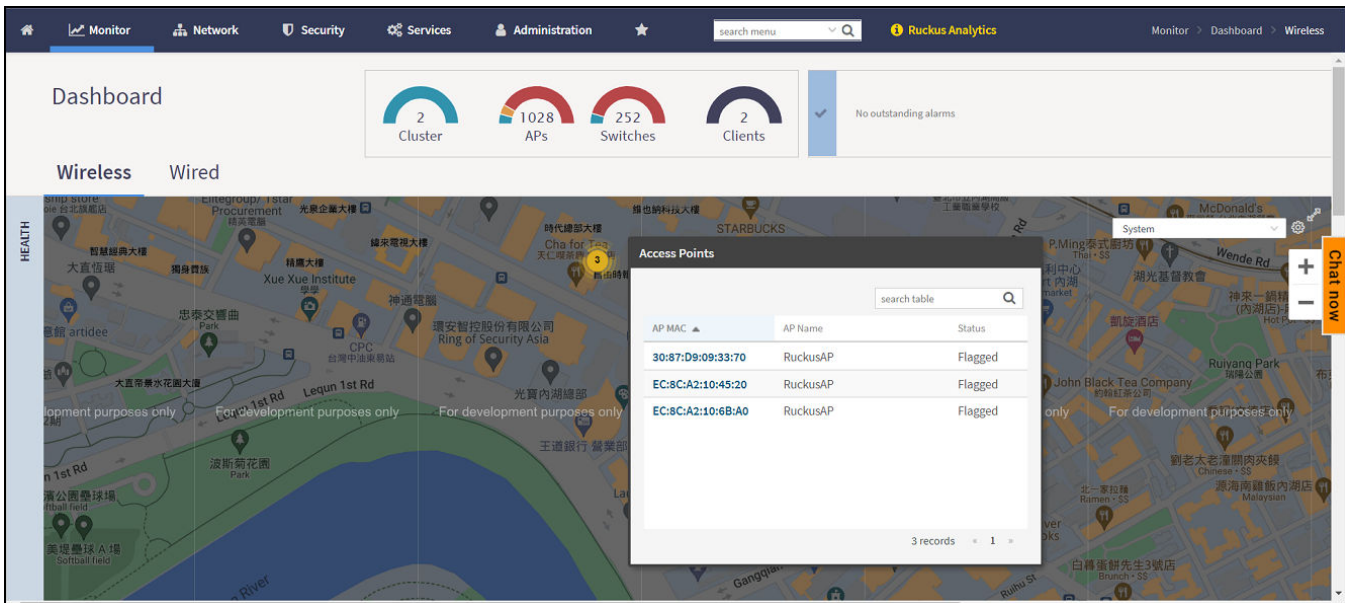
SmartZone Web Interface

Using the Dashboard

You can view and identify APs with the same GPS. If you hover over and click the clustered marker of AP on the map, a pop-up appears displaying more information such as the following:

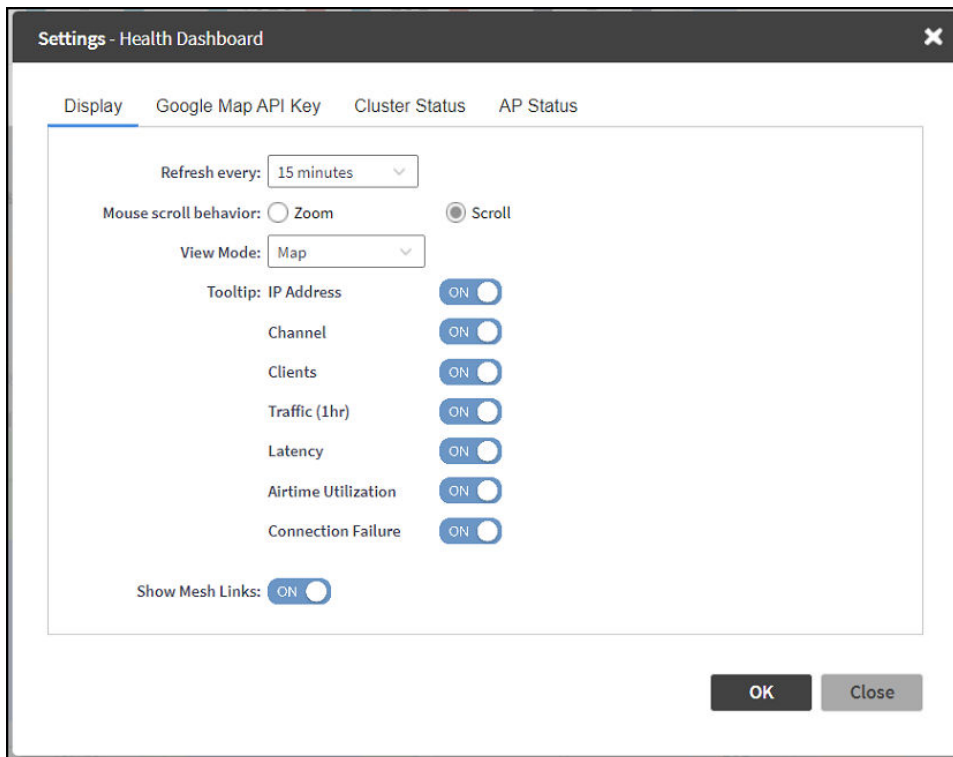
- AP MAC: Displays the MAC address of the AP
- AP Name: Displays the name assigned to the access point
- Status: Displays the status of the AP such as Online or Offline

FIGURE 33 AP Details



You can also select the Google Map API key to use the Maps service with the application.

FIGURE 34 Configuring Map Settings



NOTE

In order for your venues to appear on the world map, you must first import a map of your site floorplan.

Configuring the Google Map API Key Behavior

Refer to *RUCKUS SmartZone Controller Administration Guide* for detailed explanation of configuring the Google map API key behavior.

Wireless Dashboard

The Wireless Dashboard offers an overview of different network indicators. It consists of the following tabs that will be explained in more detail below:

- Health
- Performance
- Traffic Analysis

Health Tab

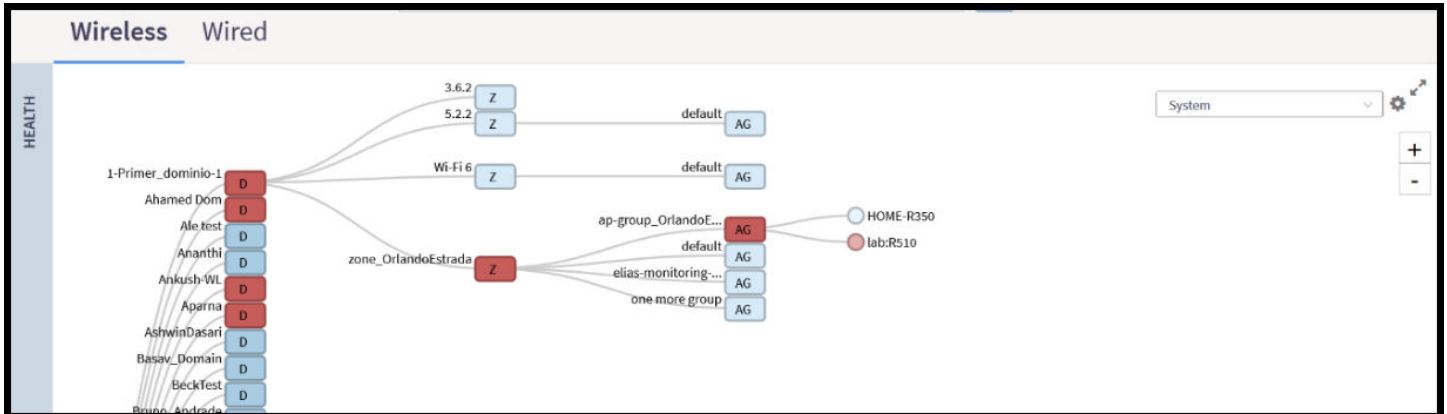
The Health tab provides administrators with an overall summary of Access Point (AP) statuses, including **Flagged**, **Offline** and **Paging** (**Paging** indicates there are more network items grouped within). Network items are displayed hierarchically, showing top-level Domains and Zones. The display is interactive, allowing you to click on any Domain or Zone to reveal the next leg of that specific hierarchy path. Additionally, an optional map view integrates with Google Maps to display the geographical locations of network items worldwide.

SmartZone Web Interface

Using the Dashboard

To simplify the graphics displayed in the Health tab and the other tabs, views can be narrowed down to specific Domains or Zones. Use the search bar in the upper-right corner of the Health tab to select the hierarchical area of interest. The search bar will reflect the currently selected domain view.

FIGURE 35 Health Tab - View Mode: Groups



Using the gear icon, the administrator can open the Health Dashboard settings where view mode options are available and additional customization options for the thresholds for the status indicators of the APs and Cluster can be found. The Health tab on the Dashboard can be organized in different views including **Map**, **Ball**, **Groups**, **Control Planes**, and **Data Planes**.

FIGURE 36 Health Dashboard Settings Window

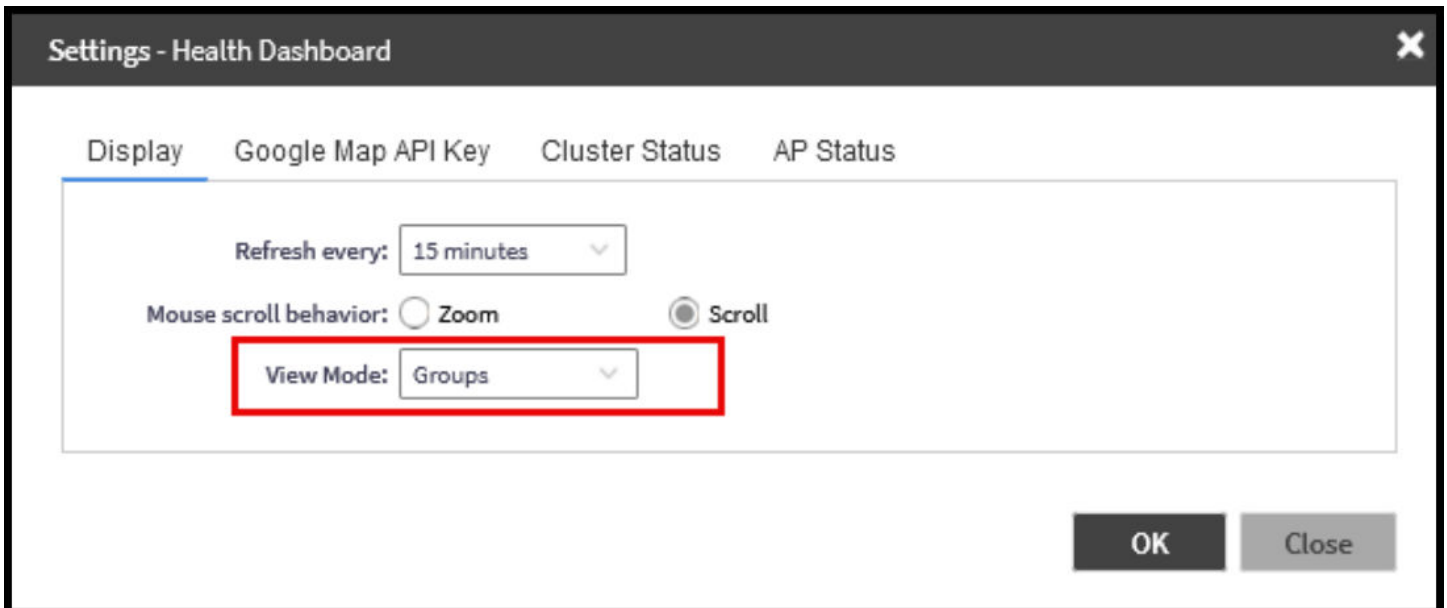
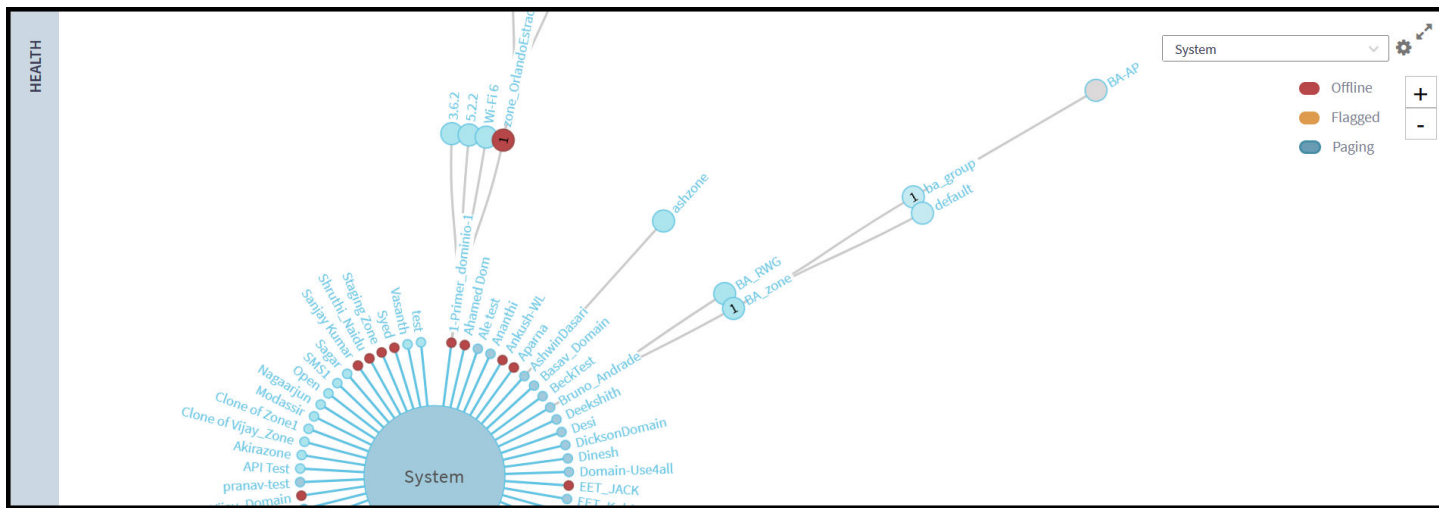


FIGURE 37 Health Tab – View Mode: Ball



NOTE

Refer to *RUCKUS SmartZone Network Administration Guide* for detailed steps on importing and configuring a floor map.

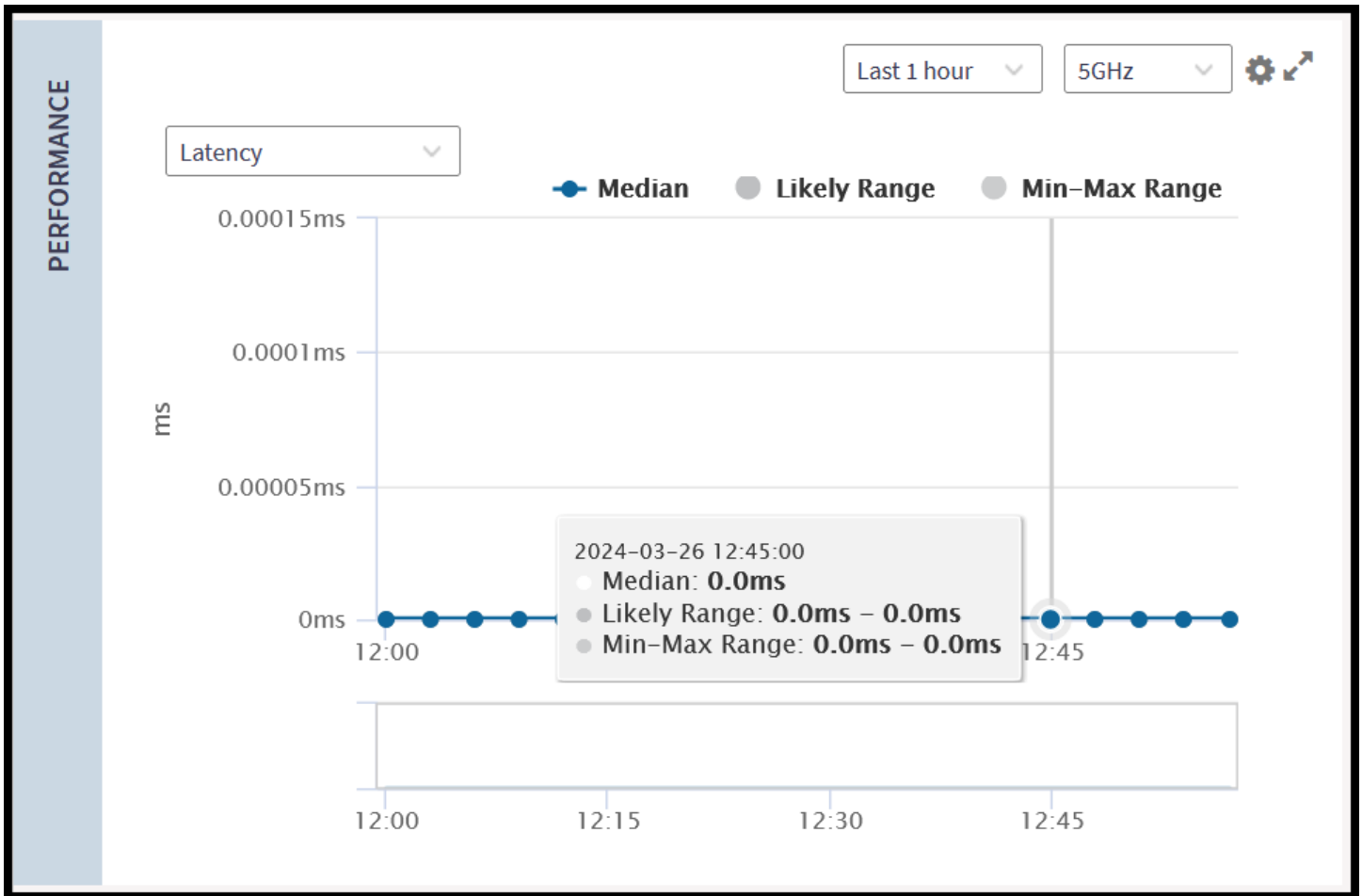
Performance Tab

The Performance tab offers insights into Latency, Airtime Utilization, and AP Capacity statistics collected over the last hour or the past 24 hours as per the selected hierarchical filter in the Health tab. The interactive time-series chart provides a graphical representation of median, likely range, and minimum and maximum performance values for the top 10 APs for a specific radio band (selectable using the drop-down menu). You can configure the number of APs for which data is aggregated and the label used for each AP (name, MAC, or IP address) by clicking the gear icon. You can selectively show or hide the data for any value type by clicking on the interactive, color-coded, value name in the key above the graph. On the time-series graph, you can view time-specific details by clicking on or hovering your cursor over a specific data point.

NOTE

Refer to *RUCKUS SmartZone Network Administration Guide* for detailed information about the different flags in the Access Points and the meaning of the indicators seen in the Tooltip.

FIGURE 38 Performance Tab



NOTE

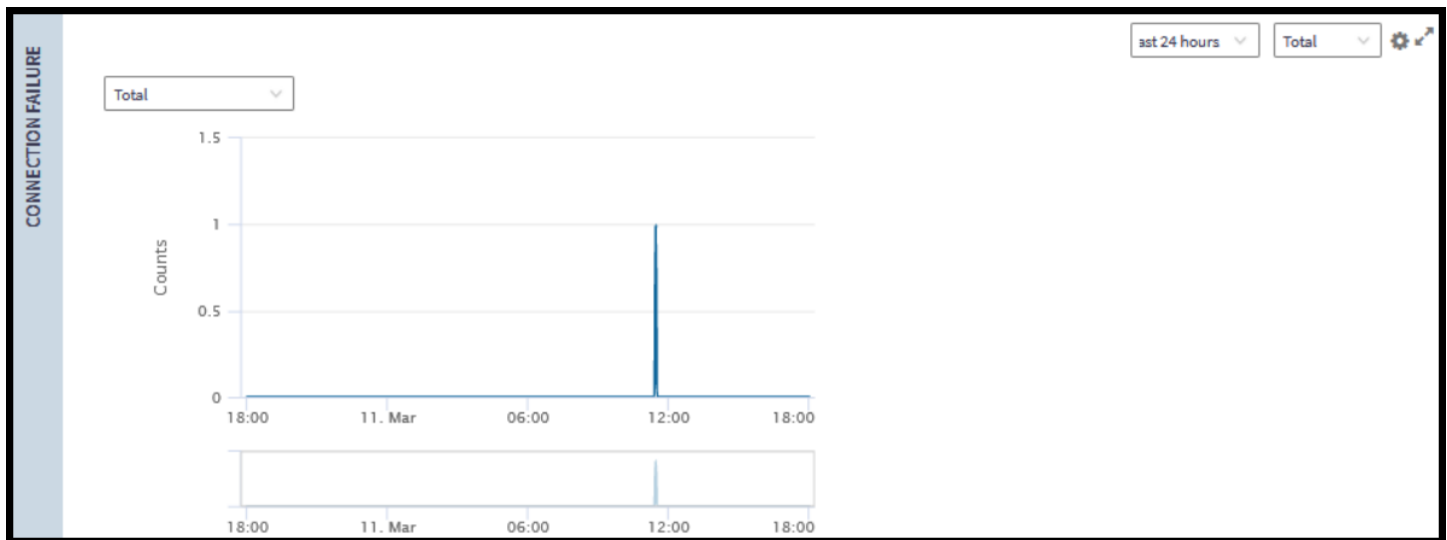
Refer to *RUCKUS SmartZone Network Administration Guide* for detailed information about the meaning and calculation of the different performance indicators seen in this tab.

Connection Failure Tab

The Connection Failure tab provides a time-series graph reflecting statistics collected over the last hour or the past 24 hours related to wireless client connection failures as per the selected hierarchical filter in the Health tab. It allows the administrator to visualize these failures either in total or by type, including **Authentication, Association, EAP, RADIUS, DHCP, and User Authentication**.

Additionally, this information can be filtered by radio band or view the total across all radio bands. You can configure the number of APs for which data is aggregated and the identifier used for each AP (name, MAC, or IP address) by clicking the gear icon.

FIGURE 39 Connection Failure Tab



NOTE

Refer to the *RUCKUS SmartZone Network Administration Guide* for detailed information about the meaning and calculation of the different connection failure indicators seen in this tab.

Traffic Analysis Tab

The Traffic Analysis tab provides administrators with a graphical view to understand and compare transmitted and received traffic trends over the last hour or the past 24 hours. The interactive time-series charts provide a graphical representation of traffic trends per-band or in total (selectable using the drop-down menu). If Total is selected, you can selectively show or hide the data for any radio band by clicking on the interactive, color-coded, band name in the key above the graph.

You can also filter the view by traffic type (TX, RX, or both) and by specific hierarchical items (such as Domain or AP Zone). For each graph, you can selectively show or hide the data for any value type by clicking on the interactive, color-coded, value name in the key above the graph.

Also, you can view time-specific details by clicking on or hovering your cursor over a specific data point. Furthermore, it showcases traffic trends based on individual hosts, OS types, and applications.

The Clients section displays, by default, the top 10 hosts, OS types, and applications, in Chart format, showing the client names. These settings are configurable to change to a table view and to change the client labeling to MAC or IP address.

FIGURE 40 Wireless Traffic Analysis Graphs

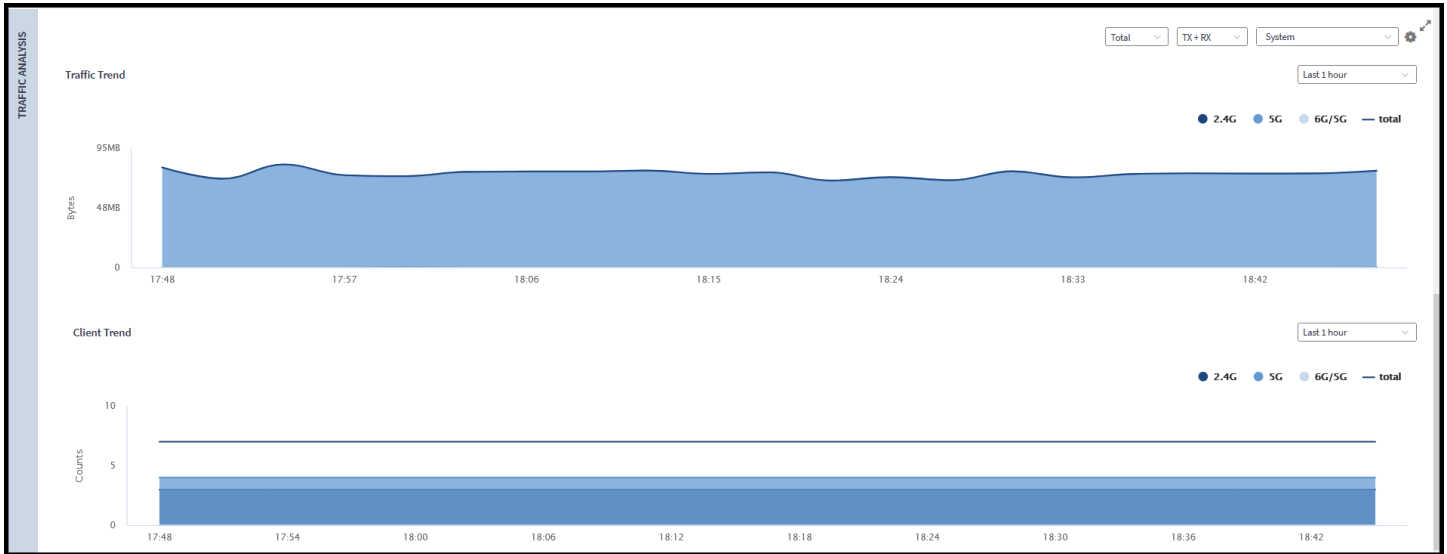
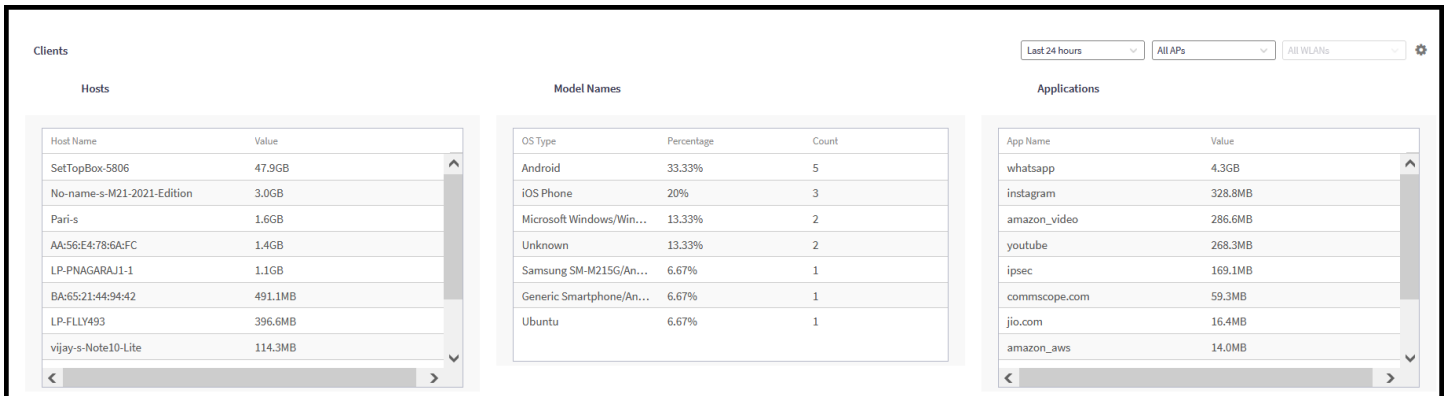


FIGURE 41 Wireless Traffic Analysis Reports



NOTE

Refer to *RUCKUS SmartZone Network Administration Guide* for detailed information about the meaning and calculation of the different traffic trend indicators seen in this tab.

Wired Dashboard

The Wired Dashboard provides an overview of switch status, traffic trends, port errors, and PoE utilization. It is divided into two main tabs: the Health Tab and the Traffic Analysis Tab.

Health Tab

The Health tab provides an overall summary of switch statuses, including **Flagged**, **Offline**, and **Paging** (**Paging** indicates there are more network items grouped within). Network items are displayed hierarchically, showing top-level Domains and Switch Groups. The display is interactive, allowing you to click on any Domain or Switch Group to reveal the next leg of that specific hierarchy path.

To simplify the graphics displayed in the Health tab, views can be narrowed down to specific Domains or Switch Groups. Use the drop-down menu in the upper-right corner of the Health tab to select the hierarchical area of interest. The currently selected hierarchy level appears highlighted.

This tab offers two modes of view: Topology and Ball (the default setting). Use the gear icon in the upper-right corner of this tab to select the view mode and the refresh interval. The refresh interval defaults to every 15 minutes.

FIGURE 42 Switch Health Tab - General Display Settings

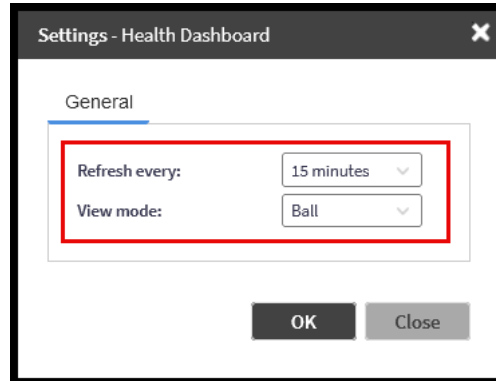
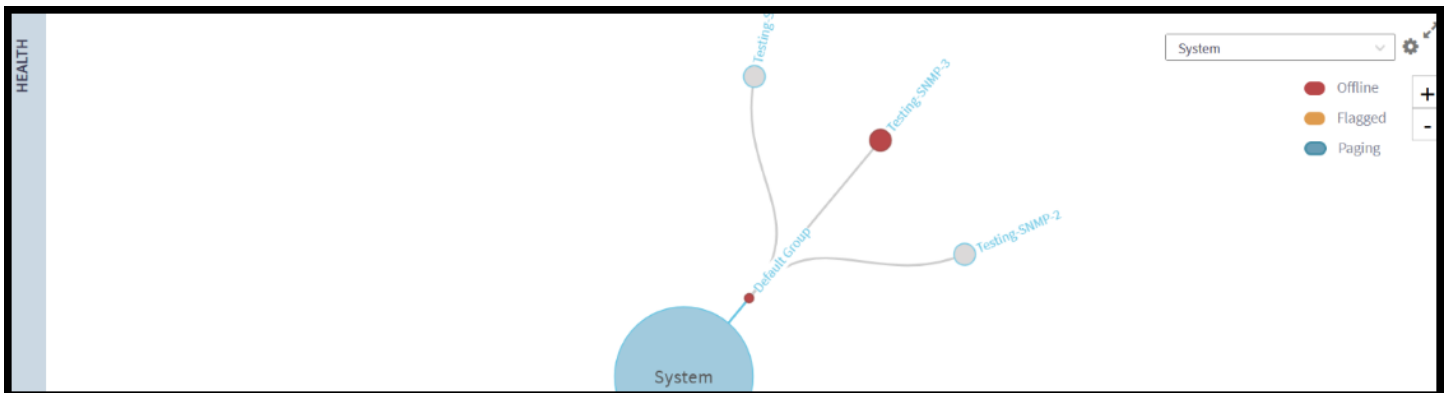
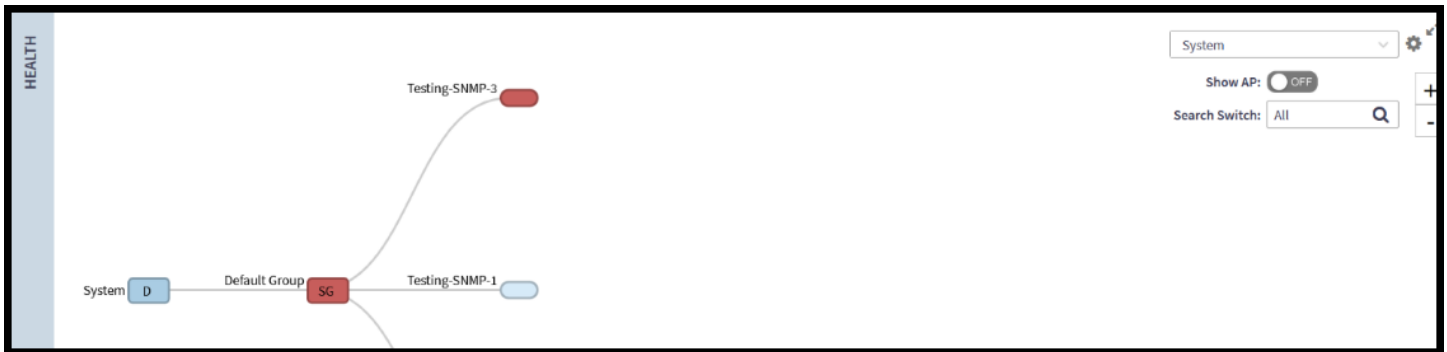


FIGURE 43 Switch Health Tab - Ball View Mode



The topology view offers the option to include in the chart the APs connected to the switches, if any. Switch the **Show AP** toggle to **ON** to search for and display APs connected to the switches.

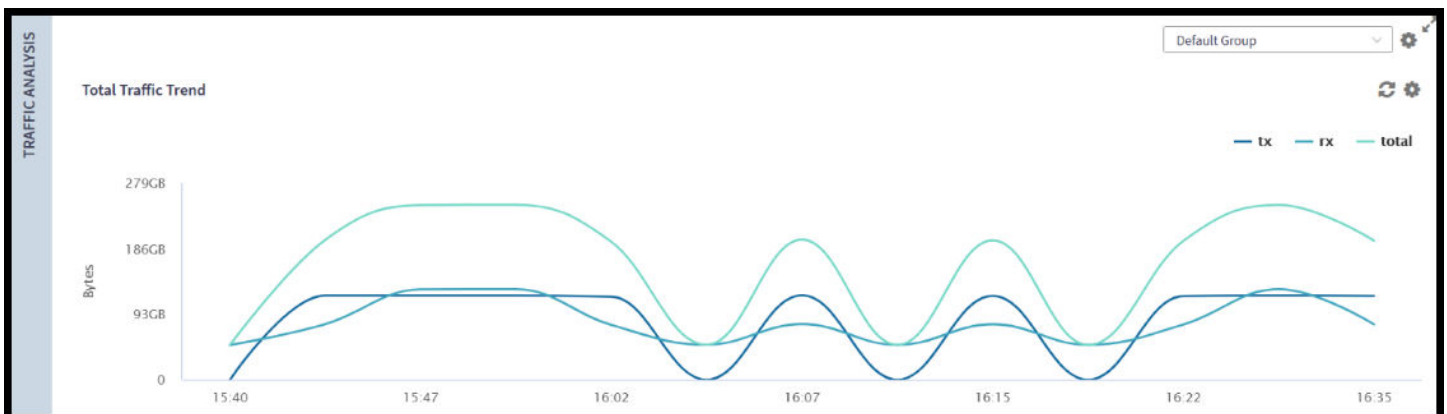
FIGURE 44 Switch Health Tab - Topology View Mode



Traffic Analysis Tab

The Traffic Analysis tab consists of different charts that can also be displayed in a table view, including the **Total Traffic Trend**. Use the drop-down menu to narrow down the content to specific Switch Groups. Clicking each interactive, color-coded, value name (**tx**, **rx**, and **total**) in the key above the graph will select or unselect the information displayed in the chart. You can customize the scope and display of the **Total Traffic Trend** data, including the system hierarchy level, the refresh interval, and the table/chart display options.

FIGURE 45 Switch Traffic Analysis Tab - Total Traffic Trend Chart



Additionally, the Traffic Analysis tab contains charts displaying switches categorized by most traffic throughput, most port errors, and highest PoE utilization. You can customize the scope and display of the **Top Switches By Traffic** data, including the number of switches for which data is displayed (minimum number is three), the view type (table or chart), and the identifier used for each switch (name, MAC, or IP address). The **Top Switches By Port Error** and **Top Switches By PoE Utilization** (watt) charts are displayed as bar charts only.

FIGURE 46 Traffic Analysis Tab - Top Switches by Traffic Chart

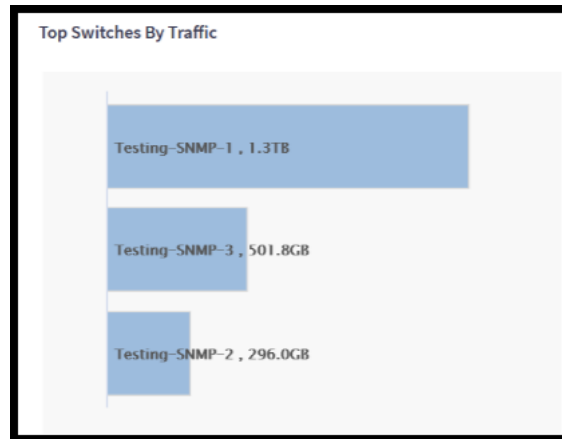
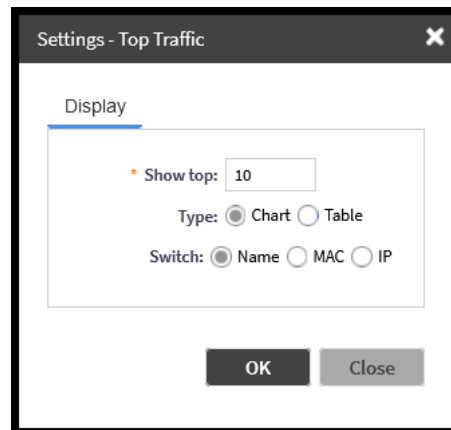


FIGURE 47 Traffic Analysis Tab - Display Settings for Top Switches by Traffic



A settings dialog box titled "Settings - Top Traffic" with a close button (X) in the top right corner. The dialog has a "Display" section with the following options:

- "Show top:" with a text input field containing the value "10".
- "Type:" with two radio buttons: "Chart" (selected) and "Table".
- "Switch:" with three radio buttons: "Name" (selected), "MAC", and "IP".

At the bottom of the dialog are two buttons: "OK" and "Close".

Administrator and Roles

- Managing Administrators and Roles..... 55
- Creating User Groups..... 55
- Creating Administrator Accounts..... 58
- Configuring the System Default Super Admin..... 60
- Working with AAA Servers..... 63
- Creating Account Security..... 73
- Terminating Administrator Sessions..... 78
- White Label Customization..... 79
- Changing the Administrator Password..... 80
- Administrator Activities..... 81

Managing Administrators and Roles

The SmartZone controller allows you to create a comprehensive database of administrators that is organized into User Groups. These groups can then be assigned specific roles, allowing for strict finely tuned control over access levels within the Web UI for performing administrative tasks.

Creating User Groups

Creating user groups and configuring their access permissions, resources, and administrator accounts allows administrators to manage a large number of users.



Perform the following steps to create user groups.

1. Select **Administration > Administration > Admins and Roles**.
2. Select the **Groups** tab.
3. Select the system domain, and click **Create**.

The **Create User Group** is displayed.






Administrator and Roles

Creating User Groups

4. Configure the following options:
 - a. Permission
 1. Name: Type the name of the user group you want to create.
 2. Description: Type a short description for the user group you plan to create.
 3. Permission: Select one of the access permission for the user group from the drop-down menu. You can also grant admin permission to generate guest passes. Select the **Custom** option to manually assign role-based permission in the **Resource** tab page.
 4. Account Security: Select the account security profile that you created to manage the administrator accounts.
 5. Click **Next**.
 - b. Resource: From **Select Resources**, choose the resources that you want to assign to this user group. If you have selected **Custom** permission option in the previous step, you can assign the required permission (**Read, Modify or Full Access**) to these resources. The resources available are SZ, AP, WLAN, User/Device/App, Admin, Guest Pass, MVNO and ICX. Click the  icon and they appear under **Selected Resources** now. Use the  icon to deselect the resources assigned to the group.

NOTE

To create User Groups, migrating Domain User Roles prior to 3.5, with DPSK permissions, Users must be granted with "User/Device/App" resource.

- c. Click **Next**.
- d. Administrator: From **Available Users**, choose the users you want to assign to this user group. Click the  icon and they appear under **Selected Users** now. Use the  icon to deselect the users assigned to the group. You can also create Administrator Accounts by clicking the  icon. The **Create Administrator Account** page appears where you can configure the administrator account settings. You can edit the user settings by clicking the  icon and delete the user from the list by clicking  icon.
- e. Click **Next**.
- f. Review: Verify the configuration of the user group. Click **Back** to make modifications to the configuration settings.
- g. Click **OK** to confirm.

You have created the user groups.

NOTE

You can also edit and delete the group configuration by selecting the options **Configure**, and **Delete** respectively, from the **Groups** tab.

Resource Group Details

The Resource Group table lists the resources available for each Resource Category. This helps the users to select the right set of resource permission for the Admin type.

TABLE 6 Resource Group

Resource	Administrative Scope
SZ	<ul style="list-style-type: none"> System Settings Cluster Settings and Cluster Redundancy Control Planes and Data Planes Firmware and Patches Cluster and Configuration Backups Licensing Cluster Stats and Health System Events and Alarms System Certificates Northbound Interface SCI Integration
AP	<ul style="list-style-type: none"> Zones and Zone Templates AP groups AP Settings AP Stats and Health Maps AP Events and Alarms Bonjour Policies Location Services Ethernet Port Profiles Tunneling Profiles and Settings AP Zone Registration
WLAN	<ul style="list-style-type: none"> WLANs WLAN Groups and Templates AAA Services L2-7 Policies Rate Limiting Application Policies Device OS Policies QoS Controls Hotspots and Portals Hotspot 2.0 Service Schedules VLAN Pools

TABLE 6 Resource Group (continued)

Resource	Administrative Scope
User/Device/App	User Roles Local Users DPSK Guest Passes Application Usage Client and Device Details
Admin	Domains Administrators Administrative Groups Administrative Activity AAA for Admins
Guest Pass	Guest Pass Guest Pass Template
MVNO	MVNO
ICX Switch	ICX Switch Switch Group Registration Rule

Creating Administrator Accounts

The controller supports the creation of additional administrator accounts. This allows you to share or delegate management and monitoring functions with other members of your organization. You can also modify the status of the administrator account by locking or unlocking it.

1. Go to **Administration > Administration > Admins and Roles**.
2. Select the **Administrators** tab.

3. Click **Create**.

The **Create Administrator Account** page appears.

FIGURE 48 Creating an Administrator Account

The screenshot shows a web form titled "Create Administrator Account". The form is contained within a light gray rectangular area. It features the following fields and labels:

- * Account Name:** A text input field.
- Real Name:** A text input field.
- * Password:** A text input field.
- * Confirm Password:** A text input field.
- Phone:** A text input field.
- Email:** A text input field.
- Job Title:** A text input field.

At the bottom right of the form area, there are two buttons: a dark gray button labeled "OK" and a light gray button labeled "Cancel".

Administrator and Roles

Configuring the System Default Super Admin

4. Configure the following:
 - a. Account Name: Type the name that this administrator will use to log on to the controller.
 - b. Real Name: Type the actual name (for example, John Smith) of the administrator.
 - c. Password: Type the password that this administrator will use (in conjunction with the Account Name) to log on to the controller.
 - d. Confirm Password: Type the same password as above.
 - e. Phone: Type the phone number of this administrator.
 - f. Email: Type the email address of this administrator.
 - g. Job Title: Type the job title or position of this administrator in your organization.
 - h. Click **OK**.

NOTE

You can also edit, delete, or unlock the admin account by selecting the options **Configure**, **Delete** or **Unlock**, from the **Administrator** tab.

NOTE

Administrator users are mapped to a different domain other than the system domain. To login use *accountname@domain*.

Unlocking an Administrator Account

When multiple user access authentications fail, the administrator account is locked. A *Super Admin* can however unlock the administrator account.

Typically, the account gets locked when the user attempts to login with a wrong user ID or password multiple times, or when the time duration/session time to access the account has ended.

You must log in as a *Super Admin* in order to unlock the account.

1. Go to **Administration > Administration > Admins and Roles**.
2. Select the **Administrators** tab.
3. From the list of accounts, select the one which needs to be unlocked. The **Status** of such an account is displayed as *Locked*.
4. Click **Unlock**.

The administrator account is now unlocked, the **Status** field against the account now displays *Unlocked*.

Configuring the System Default Super Admin

To configure the account security of system default *Super Admin* account, you can set session idle timeout, password expiration, and password reuse rules.

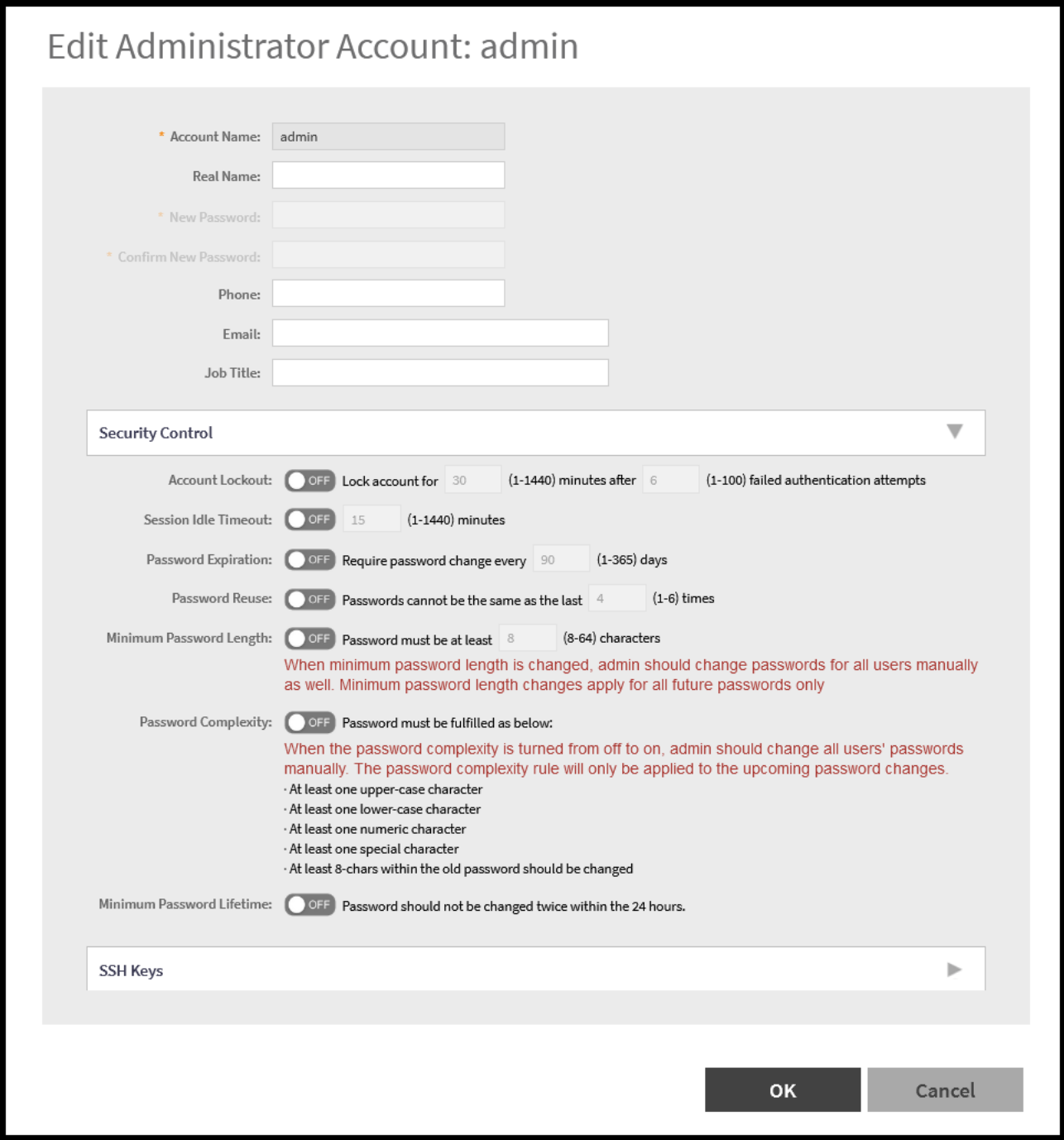
You must log in as a system default *Super Admin* to set the rules.

1. Select **Administration > Administration > Admins and Roles**.
2. Click the **Administrators** tab.

3. Select the administrator account (admin) and click **Configure** to set the additional security enhancements.

The **Edit Administrator Account** page appears.

FIGURE 49 Configuring the System Default Super Admin



Administrator and Roles

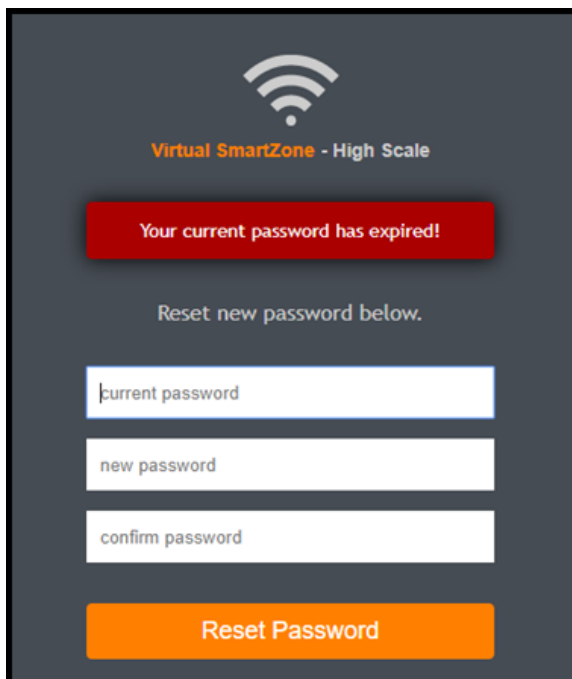
Configuring the System Default Super Admin

4. Configure the following fields:

- Real Name: Enter the name of the administrator.
- Phone: Enter the phone number.
- Email: Enter the email address.
- Job Title: Enter the role.
- Account Lockout: You can configure the security profile to lock the account based on the duration of the session or number of failed attempts to access the account. Provide the values as necessary. Click the button to enable the feature.
- Session Idle Timeout: Click the button and enter the timeout duration in minutes.
- Password Expiration: Click the button and type the number of days for which the account's password is valid. After the configured number of days, the password expires, and the account is inaccessible. You must change the password before the expiration day to have continued access to the account. By default, the password is valid for 90 days. It can be configured for validity from a minimum of 1 day, to a maximum of 365 days.

If your password has expired, you are prompted to change or reset your password as soon as you log in. Reset the password as shown in the following figure.

FIGURE 50 Resetting the Old Password



The screenshot displays a dark-themed login interface for 'Virtual SmartZone - High Scale'. At the top, there is a Wi-Fi icon. Below it, a red banner contains the text 'Your current password has expired!'. Underneath the banner, the text 'Reset new password below.' is centered. There are three white input fields stacked vertically, labeled 'current password', 'new password', and 'confirm password'. At the bottom of the form, there is a prominent orange button labeled 'Reset Password'.

- Password Reuse: Prevents the reuse of passwords. Click the button to enable this option. By default, the value is 4 (last 4 passwords cannot be reused).
- Minimum Password Length: Indicates the minimum number of characters required for a password. If there is a change in the number of characters, the Admin must manually change the passwords for all users. Enter the minimum number of characters required for a password.
- Password Complexity: Ensures that the password satisfies the following rules:
 - At least one upper-case character
 - At least one lower-case character

- At least one numeric character
- At least one special character
- At least eight characters from the previous password is changed

Select the options you want to apply.

- Minimum Password Lifetime: Ensures that the password is not changed twice within a period of 24 hours. Select the option, if appropriate.

5. Click **Ok**.

The Password Confirmation page is displayed.

6. Enter the password.

7. Click **Ok** to apply the new configuration.

Working with AAA Servers

You can configure the controller to use external AAA servers to authenticate users.

Configuring SmartZone Admin AAA Servers

To add and manage AAA servers that the controller can use to authenticate users, complete the following steps.

1. Select **Administration > Administration > Admins and Roles > AAA**.

2. In AAA servers screen, click **Create**.

The **Create Administrator AAA Server** page is displayed.

FIGURE 51 Creating an Administrator AAA Server

Create Administrator AAA Server

* Name:

[?] Default Role Mapping: OFF

User Group:

Administrator:

* Type: RADIUS TACACS+ Active Directory LDAP

* Realm:

Multiple realms supported. Use a comma (,) to separate realms (for example, home1_home2). While using wild-card(*), please make sure the realm part is as descriptive and as unique possible and also try to prevent using special characters, like @, /, #, \$, %, etc. as part of your realm from input.

TLS Encryption: OFF

Primary Server

* IP Address/FQDN:

* Port:

* Protocol: PAP CHAP PEAP

* Shared Secret:

* Confirm Secret:

Backup RADIUS: OFF Enable Secondary Server

Secondary Server

* IP Address/FQDN:

* Port:

* Protocol: PAP CHAP PEAP

* Shared Secret:

* Confirm Secret:

Failover Policy at NAS

* Request Timeout: Seconds

* Max Number of Retries: Times

OK **Cancel**

3. Enter the AAA server name.

4. For **Type**, select the type of AAA server to authenticate users:

- **RADIUS**
- **TACACS+**
- **Active Directory**
- **LDAP**

5. For **Realm**, enter the realm or service.

Multiple realms or services are supported. Separate multiple realms or services with a comma.

NOTE

Because the user login format (User Account + @ + Realm) includes a special character, the at symbol (@), the user account must not include the at symbol (@) separately on the AAA server.

6. Enable **Default Role Mapping**.

You can select **auto-mapping** for the system to automatically map between the AAA and SZ accounts.

If **Default Role Mapping** is disabled, the AAA administrator must be mapped to a local SZ Admin user with matching AAA attributes for the RADIUS, TACACS+, Active Directory, or LDAP servers.

- On a RADIUS server, the user data can use the **VSA Ruckus-WSG-User** attribute with a value depending on the SZ users or permissions you want the RADIUS user to map.
- On a TACACS+ server, the user data can use the **user-name** attribute with the **user1**, **user2**, or **user3** value depending on the SZ users or permissions you want the TACACS+ user to map.
- On an Active Directory or LDAP server, the user data can belong to the group **cn=Ruckus-WSG-User-SZAdminName** (for example, **cn=Ruckus-WSG-User-User1**, depending on the SZ users or permissions you want the Active Directory or LDAP user to map.

NOTE

You can use the mapping attributes on AAA and enable **Default Role Mapping** at the same time, but the mapping attributes override **Default Role Mapping**.

7. Under **Primary Server**, configure the settings of the primary AAA server.
 - **IP Address or FQDN** : Enter the IP address or Fully Qualified Domain Name (FQDN) of the AAA server.

NOTE

The FQDN option can be configured only for the RADIUS server.

- **Port**: Enter the UDP port that the RADIUS server is using. The default port is 1812.
- **Protocol**: Select the **PAP** or **CHAP** or **PEAP** protocol.

NOTE

For the PEAP and PAP protocols, you must configure the Trusted CA certificate to support PEAP and EAP connection.

- **Shared Secret**: Enter the shared secret.
- **Confirm Secret**: Re-enter the shared secret to confirm.
- **Windows Domain name**: Enter the domain name for the Windows server.
- **Base Domain Name**: Enter the name of the base domain.
- **Admin Domain Name**: Enter the domain name for the administrator.
- **Admin Password**: Enter the administrator password.
- **Confirm New Password**: Re-enter the password to confirm.
- **Key Attribute**: Enter the key attribute, such as UID.
- **Search Filter**: Enter a filter by which you want to search, such as objectClass=*

For **Active Directory**, configure the settings for the **Proxy Agent**.

- **User Principal Name**: Enter the Windows domain Administrator name
- **Password**: Enter the administrator password.
- **Confirm Password**: Re-enter the password to confirm.

8. For **Backup RADIUS**, if a secondary backup server is available on the network, select **Enable Secondary Server**.

9. Under **Secondary Server**, configure the settings of the secondary RADIUS server.

- **IP Address**: Enter the IP address of the AAA server.
- **IP Address or FQDN**: Enter the IP address or Fully Qualified Domain Name (FQDN) of the AAA server.

NOTE

The FQDN option can be configured only for the RADIUS and Secondary server.

- **Port**: Enter the UDP port that the RADIUS server is using. The default port is 1812.
- **Protocol**: Select the **PAP** or **CHAP** or **PEAP** protocol.

NOTE

For the PEAP and PAP protocols, you must configure the Trusted CA certificate to support PEAP and EAP connection respectively.

- **Shared Secret**: Enter the shared secret.
- **Confirm Secret**: Re-enter the shared secret to confirm.

10. Under **Failover Policy at NAS**, configure the settings of the secondary RADIUS server.
 - **Request Timeout:** Enter the timeout period in seconds. After the timeout period, an expected RADIUS response message is considered to have failed.
 - **Max Number of Retries:** Enter the number of failed connection attempts. After the maximum number of attempts, the controller tries to connect to the backup RADIUS server.
 - **Reconnect Primary:** Enter the time in minutes, after that the controller connects to the primary server.
11. Click **OK**.

NOTE

You can also edit, clone, or delete the server by selecting the options **Configure**, **Clone**, or **Delete**, from the **Administrator** tab.

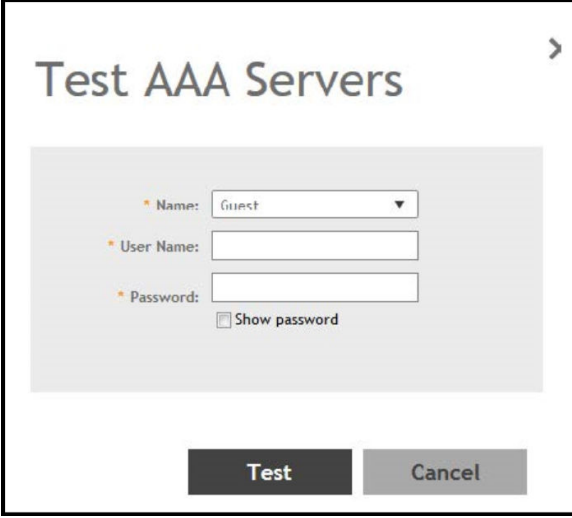
Testing AAA Servers

To ensure that the controller administrators will be able to authenticate successfully with the RADIUS server type that you selected, RUCKUS strongly recommends testing the AAA server after you set it up.

1. Go to **Security > Authentication**.
2. Select the **Proxy (SZ Authenticator)** tab, and then select the zone for which you want to test the AAA server.
3. Click **Test AAA**.

The **Test AAA Server** page appears.

FIGURE 52 Testing an AAA Server



The screenshot shows a web interface titled "Test AAA Servers". It features a light gray background for the form area. The form includes three main input fields: "Name" with a dropdown menu showing "Guest", "User Name" with a text input box, and "Password" with a text input box. Below the password field is a checkbox labeled "Show password". At the bottom of the form, there are two buttons: "Test" and "Cancel".

4. Configure the following:
 - a. **Name:** Select one of the AAA servers that you previously created.
 - b. **User Name:** Type an existing user name on the AAA server that you selected.
 - c. **Password:** Type the password for the user name you specified.

5. Click **Test**.

If the controller was able to connect to the authentication server and retrieve the configured groups/attributes, the information appears at the bottom of the page. If the test was unsuccessful, there are two possible results (other than success) that will be displayed to inform you if you have entered information incorrectly: **Admin invalid** or **User name or password invalid**. These results can be used to troubleshoot the reasons for failure to authenticate administrators with an AAA server through the controller.

AAA Server Authentication

Complete AAA-based authentication for the AAA server by performing one of the following steps.

1. Enable **Default Role Mapping** to map the external AAA users to a single SZ local admin user.
2. Apply the permissions of AAA users on SZ using the corresponding AAA server attributes.

Following is an example:

- a. Create three user groups with the following access permissions in SZ:
 - Group1 with SZ super permission
 - Group2 with SZ AP admin permission
 - Group3 with SZ read-only permission
- b. Create three SZ local users corresponding to the user groups as follows:
 - Bind User1 with Group1
 - Bind User2 with Group2
 - Bind User3 with Group3

NOTE

Following are the attribute values on AAA servers:

- RADIUS: **Ruckus-WSG-User=User1** or **User2** or **User3**.
 - TACACS+: **user-name=User1** or **User2** or **User3**.
 - Active Directory and LDAP: **Group cn=Ruckus-WSG-User-User1** or **Ruckus-WSG-User-User2** or **cn=Ruckus-WSG-User-User3**.
- c. Select **Administrator > Administrator > Admins and Roles > AAA** and click **Create** to create an Admin AAA profile.
Refer to [Configuring SmartZone Admin AAA Servers](#) on page 63.

About RADIUS Support

Remote Authentication Dial-In User Service (RADIUS) is an Authentication, Authorization, and Accounting protocol used to authenticate controller administrators.

In addition to selecting RADIUS as the server type, complete the following steps for RADIUS-based authentication to work on the controller.

1. Edit the RADIUS configuration file (**users**) on the RADIUS server to include the user names.

For example,

```
Peter  Cleartext-Password := "user_345"  
      Ruckus-WSG-User = "User2"  
  
Tony   Cleartext-Password := "user_456"  
      Ruckus-WSG-User = "User3"  
  
Steve  Cleartext-Password := "user_567"  
      Ruckus-WSG-User = "User1"  
~
```

2. On the controller web interface, select **Administration > Administration > Admins and Roles > Administrators**, and click **Create** to create an administrator account with **super** as the user name.

NOTE

Refer to [Creating Administrator Accounts](#) on page 58 . In this example, RADIUS can use User1, User2, or User3.

3. Select **Administration > Administration > Admins and Roles > Groups** and assign an administrator role to the super administrator account.

NOTE

Refer to [Creating User Groups](#) on page 55.

4. When adding a server type for administrators, select RADIUS as the authentication server type.

NOTE

Refer to [Configuring SmartZone Admin AAA Servers](#) on page 63.

5. Test the RADIUS server using the account **username@super-login**.

NOTE

The value of super-login depends on the realm configured for the AAA profile. Refer to [Creating Administrator Accounts](#) on page 58.

About TACACS+ Support

Terminal Access Controller Access-Control System Plus (TACACS+) is one of the Authentication, Authorization and Accounting protocols used to authenticate controller administrators. TACACS+ is an extensible AAA protocol that provides customization and future development features, and uses TCP to ensure reliable delivery.

In addition to selecting TACACS+ as the server type, complete the following steps for TACACS+ based authentication to work on the controller.

1. Edit the TACACS+ configuration file (**tac_plus.conf**) on the TACACS+ server to include the service user name.

For example,

```
key = test@1234
accounting file = /var/log/tac_acct.log
user = username {
    member = show
    login = cleartext "password1234!"
}
group = show {
    service = super-login {
        user-name = super <<==mapped to the user account in the controller
    }
}
```

2. On the controller web interface, select **Administration >Administration> Admins and Roles > Administrators**, and click **Create** to create an administrator account with **super** as the user name.

NOTE

Refer to [Creating Administrator Accounts](#) on page 58.

3. Select **Administration >Administration> Admins and Roles > Groups** and assign an administrator role to the super administrator account.

NOTE

Refer to [Creating User Groups](#) on page 55.

4. When adding a server type for administrators, select TACACS+ as the authentication server type.

NOTE

Refer to [Configuring SmartZone Admin AAA Servers](#) on page 63.

5. Test the TACACS+ server using the account **username@super-login**.

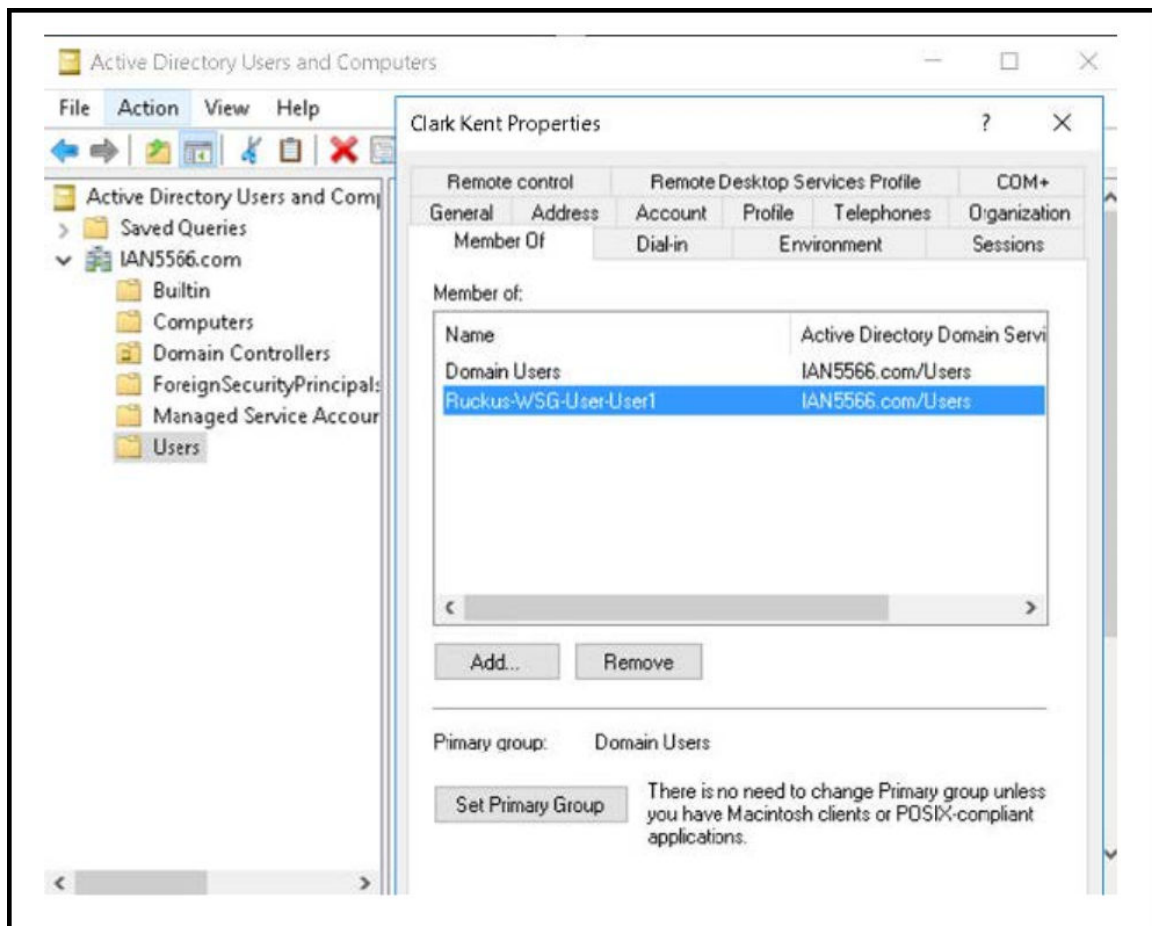
About Active Directory (AD) Support

Active Directory is a domain service that authenticates and authorizes users in a Windows environment.

In addition to selecting AD as the server type, you must also complete the following steps for AD-based authentication to work on the controller.

1. Edit the AD configuration file on the AD server to include the service user name.

FIGURE 53 About Active Directory Support



2. On the controller web interface, select **Administration > Administration > Admins and Roles > Administrators**, and click **Create** to create an administrator account with **super** as the user name.

NOTE

Refer to [Creating Administrator Accounts](#) on page 58. In this example, Active Directory can use User1 only.

3. Select **Administration > Administration > Admins and Roles > Groups**, and then assign an administrator role to the super administrator account.

NOTE

Refer to [Creating User Groups](#) on page 55.

- When you add an AAA server for administrators, select **Active Directory** as the authentication server type.

NOTE

Refer to [Configuring SmartZone Admin AAA Servers](#) on page 63.

- Test the AD server using the account **username@super-login**.

NOTE

The value of super-login depends on the realm configured for the AAA profile. Refer to [Creating Administrator Accounts](#) on page 58.

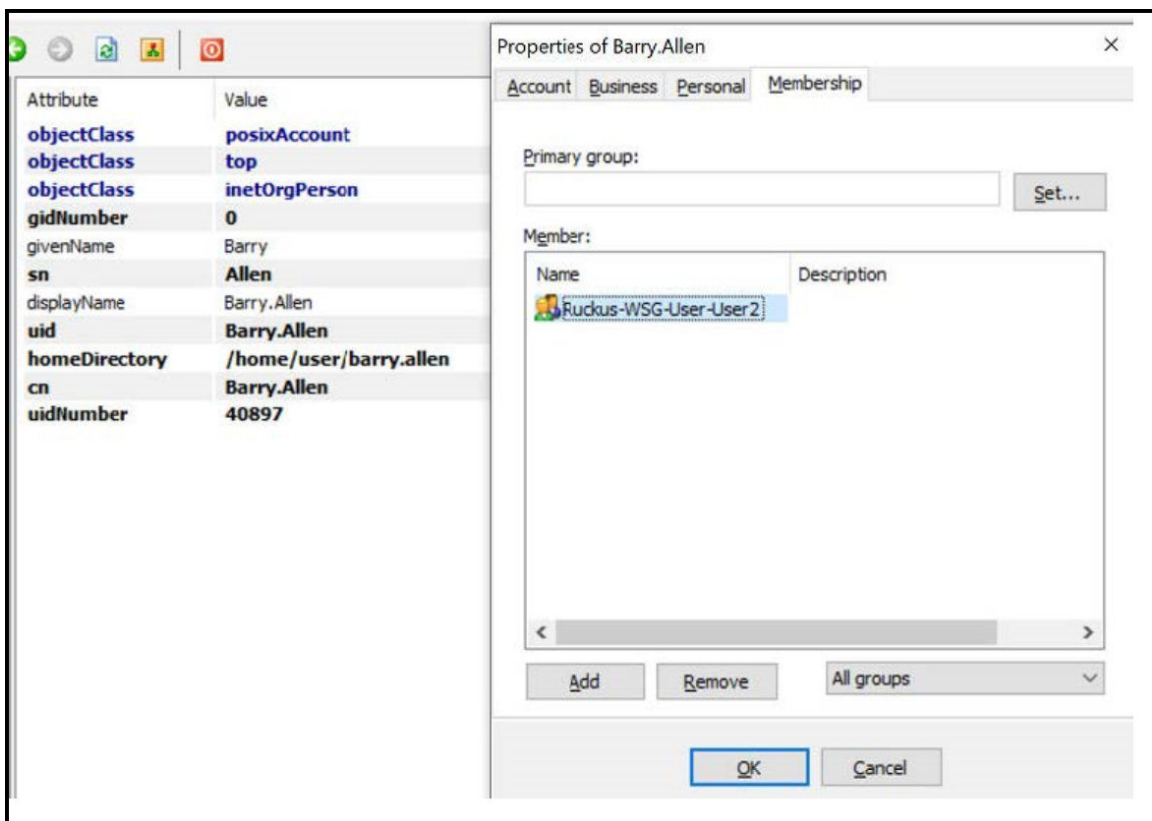
About LDAP Support

Lightweight Directory Access Protocol (LDAP) is an application protocol used to access and maintain directory information services.

In addition to selecting LDAP as the server type, you must also complete the following steps for LDAP-based authentication to work on the controller.

- Edit the LDAP configuration file on the LDAP server to include the service user name.

FIGURE 54 Supporting LDAP Configuration



2. On the controller web interface, select **Administration > Administration > Admins and Roles > Administrators**, and click **Create** to create an administrator account with **super** as the user name.

NOTE

Refer to [Creating Administrator Accounts](#) on page 58. In this example, LDAP can use User2 only.

3. Select **Administration > Administration > Admins and Roles > Groups** and assign an administrator role to the super administrator account.

NOTE

Refer to [Creating User Groups](#) on page 55.

4. When you add an AAA server for administrators, select **LDAP** as the authentication server type.

NOTE

Refer to [Configuring SmartZone Admin AAA Servers](#) on page 63.

5. Test the LDAP server using the account **username@super-login**.

NOTE

The value of super-login depends on the realm configured for the AAA profile. Refer to [Creating Administrator Accounts](#) on page 58.

Creating Account Security

Creating an account security profile enables end-users to control administrative accounts to better manage admin accounts, passwords, login, and DoS prevention.

1. Go to **Administration > Administration > Admins and Roles**.

Administrator and Roles

Creating Account Security

2. Select the **Account Security** tab.

The **Global Security** section and **Account Security** section are displayed.

FIGURE 55 Account Security page

The screenshot displays the 'Account Security' configuration page. The top navigation bar includes 'Monitor', 'Network', 'Security', 'Services', 'Administration', and 'Account Security'. The 'Administration' tab is selected, and the 'Account Security' sub-tab is active. The page is divided into two main sections: 'Global Security' and 'Account Security'.

Global Security

- Captcha for Login: OFF
- Concurrent Session(s): OFF Maximum allowed interactive concurrent session per account: 3 (3 - 10) sessions
- Concurrent Session(s): OFF Maximum allowed API concurrent session per account: 64 (64 - 2048) sessions
- SSH Authentication Method: Password Only Public Key Only Public Key and Password Public Key or Password

Account Security

Buttons: Refresh, OK, Cancel

Buttons: + Create, Configure, Delete

Name	Idle Timeout	Account Lockout	Password Expiration	Password Reuse	Two-Factor Auth	Disable Inactive Act	Minimum Password	Description
System	Default	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Default Acco...

3. From Global Security, configure the following:
 - a. **Captcha for Login:** select the option to enable Captcha for log in. The captcha feature provides additional security to ensure a human is signing into the account, and not a robot. If this feature is enabled; when you log into the web interface, the captcha characters are displayed in the login page as shown in the following example.

FIGURE 56 Captcha Enabled in the Login Page



Type the characters as shown in the captcha picture and log in. The characters in the captcha image are case sensitive and can be refreshed if not clear.

- b. **Concurrent sessions:** Click the required options and enter the number of sessions allowed:
 - **Maximum allowed interactive concurrent session per account**
 - **Maximum allowed API concurrent sessions per account**
- c. Click **OK**.

4. From **Account Security**, click **Create**.

The **Create Account Security** page is displayed.

FIGURE 57 Creating Account Security

Create Account Security

Name:

Description:

Session Idle Timeout: ON 15 (1-1440) minutes

Account Lockout: OFF Lock account for 30 (1-1440) minutes after 6 (1-100) failed authentication attempts

ON Lock account forever after 3 (1-100) failed attempts during 15 (1-1440) minute time period.

This option does not apply to AAA Admin Users.

Password Expiration: ON Require password change every 90 (1-365) days

Password Reuse: ON Passwords cannot be the same as the last 4 (1-6) times

Two-Factor Authentication: OFF Require two-factor authentication via SMS

You have to verify your one-time code first to enable it

Disable Inactive Accounts: ON Lock admin accounts if they have not been used in the last 90 (1-1000) days

Minimum Password Length: ON Password must be at least 8 (8-64) characters

When minimum password length is changed, admin should change passwords for all users manually as well. Minimum password length changes apply for all future passwords only

Password Complexity: OFF Password must be fulfilled as below:

When the password complexity is turned from off to on, admin should change all users' passwords manually. The password complexity rule will only be applied to the upcoming password changes.

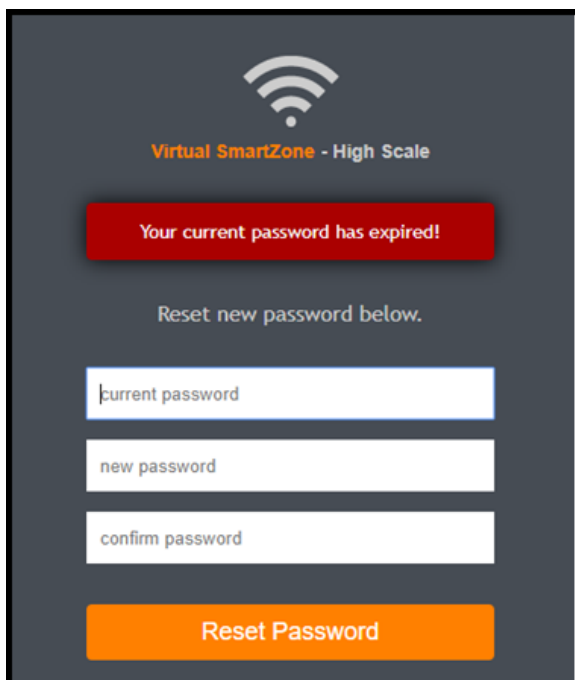
- At least one upper-case character
- At least one lower-case character

5. Configure the following:

- Name: Type the name of the security profile that you want to create.
- Description: Provide a short description for the profile.
- Session Idle Timeout: Click the button and enter the timeout duration in minutes.
- Account Lockout: You can configure the security profile to lock the account based on the duration of the session or number of failed attempts to access the account. Provide the values as necessary. Enable and configure one of the following:
 - Enter the account lockout time and number of failed authentication attempts.
 - Enter the number of failed attempts after which the account is locked and the corresponding time period. After three unsuccessful login attempts in a time interval of 15 minutes, the account is locked and must be released by an Administrator.
- Password Expiration: Click the button and type the number of days for which the account's password will be valid. After the configured number of days, the password will expire and render the account inaccessible. You must change the password before the expiration day to have continued access to the account. By default, the password is valid for a period of 90 days. It can be configured for validity from a minimum of 1 day, to a maximum of 365 days.

If your password has expired, you are prompted to change or reset your password as soon as you log in. Reset the password as shown in the figure.

FIGURE 58 Resetting the Old Password



The screenshot displays a dark grey login screen for 'Virtual SmartZone - High Scale'. At the top center is a white Wi-Fi signal icon. Below it, the text 'Virtual SmartZone - High Scale' is displayed in orange and white. A prominent red rectangular box contains the white text 'Your current password has expired!'. Underneath this box, the instruction 'Reset new password below.' is shown in light grey. Three white input fields are stacked vertically, each with a light grey border and placeholder text: 'current password', 'new password', and 'confirm password'. At the bottom of the screen, a large orange button with the white text 'Reset Password' is centered.

- Password Reuse: Prevents the reuse of passwords. Click the button to enable this option. By default, the value is 4 (last 4 passwords cannot be reused).
- Disable Inactive Accounts: Locks the admin user IDs that are inactive for the specified period of time. Click the button and specify the number of days.
- Minimum Password Length: Indicates the minimum number of characters required for a password. If there is a change in the number of characters, the Admin must manually change the passwords for all users. Enter the minimum number of characters required for a password.

Administrator and Roles

Terminating Administrator Sessions

- **Password Complexity:** Ensures that the password applies the following rules:
 - At least one upper-case character
 - At least one lower-case character
 - At least one numeric character
 - At least one special character
 - At least eight characters from the previous password is changedSelect the appropriate options.
- **Minimum Password Lifetime:** Ensures that the password is not changed twice within a period of 24 hours. Select the option.

6. Click **OK** to submit the security profile/form.

The newly created profile is added under the **Account Security** section.

NOTE

You can also edit or delete the profile by selecting the options **Configure** or **Delete**, from the **Administrator** tab.

With new enhancements to account security, SmartZone has a complete feature set to make PCI compliance very simple and straightforward. In addition to local PCI enforcement settings, SmartZone also integrates with SCI for reporting and analytics. SCI version 5.0 and later supports a PCI compliance report, which is based on the relevant PCI-related configuration settings throughout SmartZone. To facilitate the SmartCell Insight PCI report, the SmartZone is capable of sending the following information to SCI:

- Configuration messages as separated GPB messages
- WLAN configuration
- Default configuration changes
- Controller information that identifies the controller model
- Encryption details of communication, for example: CLI, SSH, telnet, Web, API
- Inactive user IDs and session timeout
- Authentication mechanism enforced on user IDs
- Enforcement of password
- Supported mechanism on SZ that can be provided to SCI
- User IDs that are locked after failed attempts
- Authentication credentials that are unreadable and encrypted during transmission
- Enforcement of password standards
- Disallowing duplicate password feature is enabled
- If rogue AP detection is enabled on each AP

To learn more about SCI and the PCI compliance report it provides, check the product page (<https://www.ruckuswireless.com/products/smart-wireless-services/analytics>) and documentation on the RUCKUS support page (<https://support.ruckuswireless.com>).

Terminating Administrator Sessions

From the **Session Management** tab, you can view and also terminate the Administrator sessions that are currently running.

1. From the controller web interface, select **Administration > Admin and Roles > Session Management**
2. Select the administrator session you want to discontinue and click **Terminate**.

The **Password Confirmation** page displays.

3. Enter the password and click **OK**. The session ends.

You can terminate all CLI and web interface sessions that you have logged in to.

White Label Customization

White Label Customization allows the Managed Service Provider (MSP) domain user or the partner domain user with the permission to access White Label Customization to customize their company logo, company icon, and company name.

Complete the following steps to display the company logo, company icon, and company name on the controller.

NOTE

If you do not have the White Label Customization permission, you cannot access white label customizations.

Complete the following steps to configure White Label Customization:

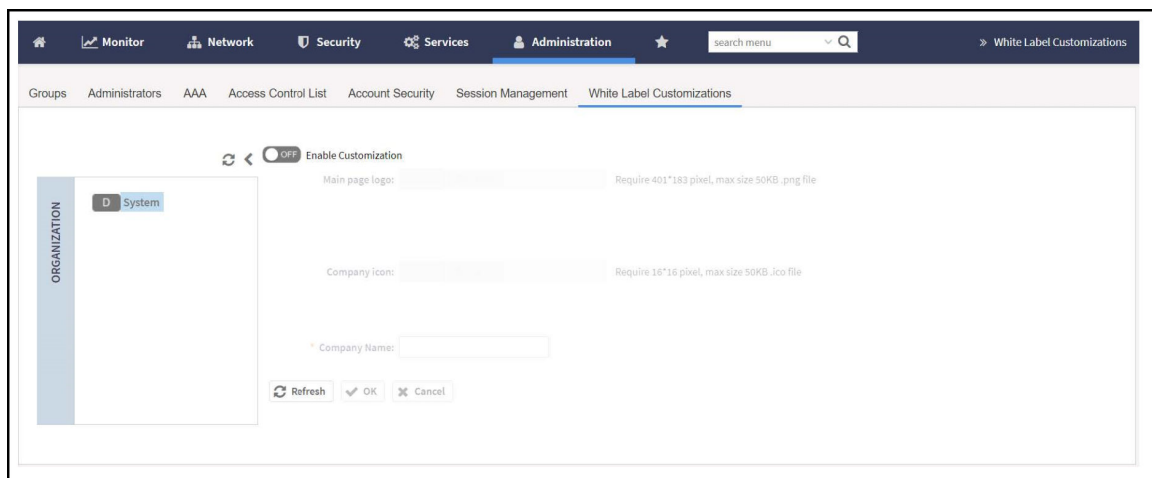
1. From the main menu, navigate to **Administration > Administration > Admins and Roles > White Label Customizations**.
2. Set the **Enable Customization** toggle switch to **ON**.

NOTE

The partner domain user can view only their own domain to configure logo, icon and name of the company.

- a) **Main page logo:** Click **Browse** to select the company logo.
- b) **Company icon:** Click **Browse** to select the company icon.
- c) **Company Name:** Enter the name of the company.

FIGURE 59 Enabling White Label Customization

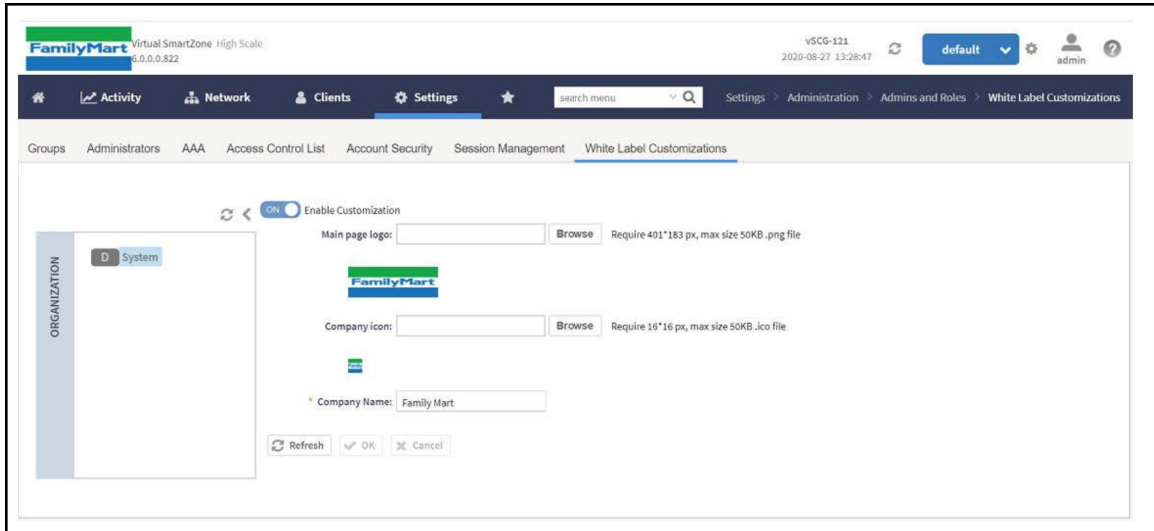


Administrator and Roles

Changing the Administrator Password

3. Click **OK** to confirm settings or click **Cancel** to disable customization.

FIGURE 60 New Logo Replaces Initial Logo



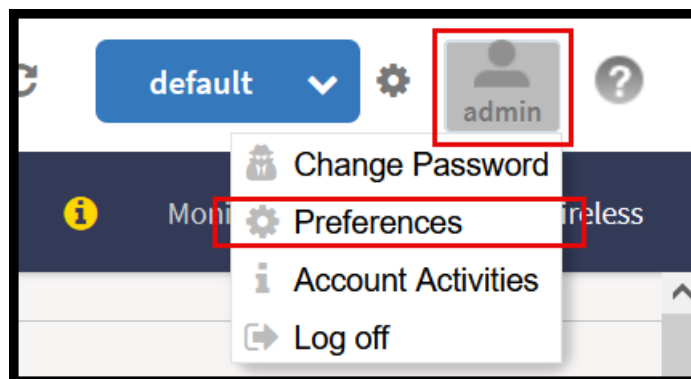
4. Click **Refresh** to refresh the page.

Changing the Administrator Password

Follow these steps for any administrator to change their own password.

1. In the Web UI, click the user profile icon in the upper-right corner.

FIGURE 61 Changing the Administrator Password



2. Enter:
 - **Old Password**—Your current password.
 - **New Password**—Your new password.
 - **Confirm Password**—Your new password.

3. Click **Change**, your new password is updated.

NOTE

The system-default admin user with SUPER_ADMIN privileges can change the password of other users. To complete this task, refer to [Creating Administrator Accounts](#) on page 58.

Administrator Activities


The controller keeps a record of all actions and configuration changes that administrators perform on the server. This feature enables you and other administrators in the organization to determine what changes were made to the controller and by whom.

1. Go to **Administration > Administration > Admin Activities**.
2. Select the **Admin Activities** tab. the **Admin Activities** page displays the administrator actions.

The following information is displayed:

- **Date and Time:** Date and time when the alarm was triggered
- **Administrator:** Name of the administrator who performed the action
- **Source IP:** Displays the IP address of the device from which the administrator manages the controller.
- **Browser IP:** IP address of the browser that the administrator used to log on to the controller.
- **Action:** Action performed by the administrator.
- **Resource:** Target of the action performed by the administrator. For example, if the action is Create and the object is Hotspot Service, this means that the administrator created a new hotspot service.
- **Description:** Displays additional details about the action. For example, if the administrator created a new hotspot service, this column may show the following: **Hotspot [company_hotspot]** .



Click  to export the administrator activity list to a CSV file. You can view the default download folder of your web browser to see the CSV file named **clients.csv**. Use a spreadsheet application (for example, Microsoft[®] Excel[®]) to view the contents of the CSV file.

SmartZone Cluster and Cluster Redundancy

- [Viewing System Settings.....](#) 83
- [Cluster Overview.....](#) 83
- [Cluster Redundancy.....](#) 88

RUCKUS SmartZone architecture allows multiple SmartZone controllers to be deployed together in an Active-Active SmartZone Cluster. With Active-Active clustering, all nodes of a cluster are managed together as a single entity and each node actively manages APs in the network, offering AP load balancing and controller redundancy. The SmartZone Cluster offers options for adding/removing nodes within the cluster, upgrading all the members of the Cluster with a single action, backing up and restoring the Cluster, and so on.

Viewing System Settings

System settings include options to view system information, configure system time, NTP servers, and DNS servers.

To view the system settings information, select **Administration > System > System Info**. The following system information is displayed:

- Controller Version
- Control Plane Software Version
- Data Plane Software Version
- Default AP Firmware Version (hover over the field to see the firmware type)
- Supported AP Model List with AP firmware and supported AP models
- Cluster Name
- Number of Planes
- System Name
- System Uptime
- Serial Number
- System Capacity of Cluster
- AP Capacity License
- AP Direct Tunnel License
- Data Plane Capacity License

Cluster Overview

The system cluster overview provides summary information of the controller cluster.

NOTE

An out-of-service node must be fixed within 45 days to avoid license disruption and to avail continuous services. A warning message on the out-of-service status of the node is listed on the header bar.

To view the cluster settings:

- From the main menu, click **Network > Cluster**.The **Cluster** page is displayed..

NOTE

The UDI is not accessible on the ESXi hypervisor as the default network driver of vSZ is VMXNET3 and it has a limitation for VLAN interface of VM. To resolve this issue, change the network driver to E1000.

Control Planes and Data Planes

Control planes and data planes are used to control traffic.

The control plane manages and exchanges routing table information. The control plane packets are processed by the router to update the routing table information. The data plane forwards the traffic along the path according to the logic of the control plane.

You can view historical and real time traffic of the nodes. To view the traffic:

1. From the Controller page, select the node.
2. Click the Traffic & Health from the lower end of the page.
3. Select the option from the drop-down:
 - **Historical Data**, and enter the time frame for which you want.
 - **Real Time Data**, enter the duration in minutes and click **Start**.

The Cluster Node Traffic and Health tab displays as shown in the diagram below.

FIGURE 62 Viewing the Cluster Traffic



Displaying the Chassis View of Cluster Nodes

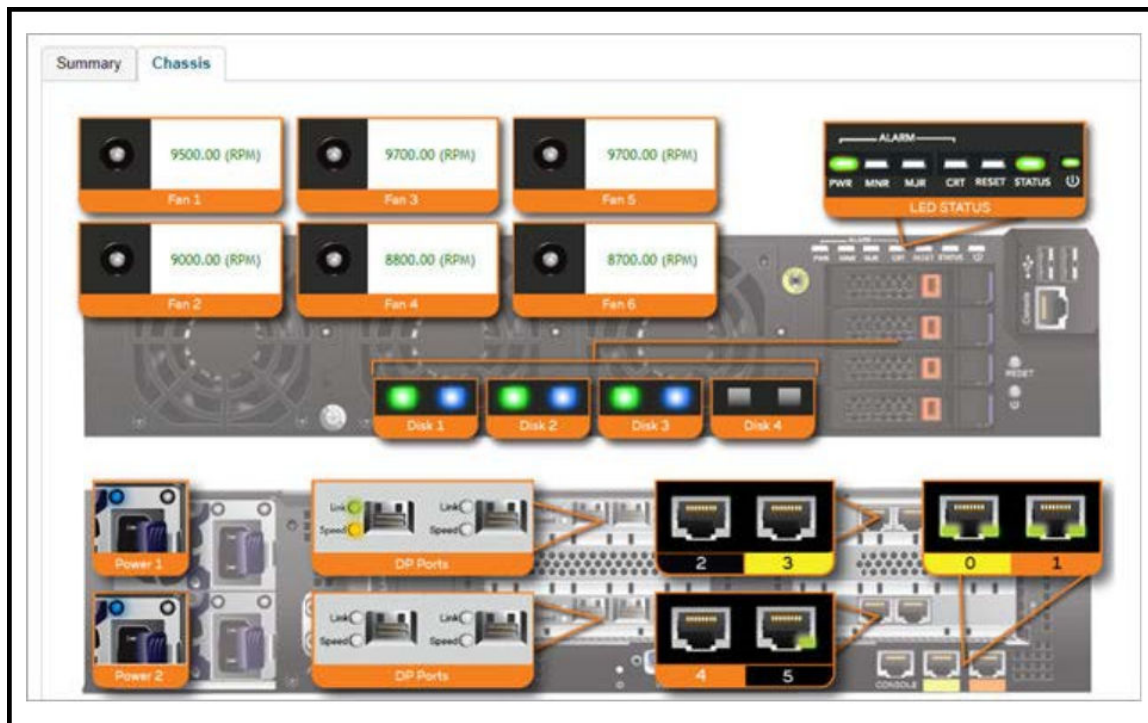
The chassis view provides a graphical representation of the control panel (on the front panel of the controller), including the LEDs.

Use the LEDs to check the status of the ports and power supplies on the controller. Fan status is also displayed on the chassis view.

To view the chassis of the cluster node:

1. From the Cluster page, select the node.
2. From the lower-left side of the page, click the **Chassis** tab to display the Chassis tab information.

FIGURE 63 Cluster Node Chassis



- port 1 and 2 are management ports
- ports (3-4 or 3-6) are data ports

Reviewing Cluster Health and Configuration

You can select the following tabs to view the status of the cluster settings:

- **Summary**—Details such as name, model, serial number, bandwidth, data driver, number of core, data interface details, management interface details, IP details, memory usage, and disk usage.
- **Network Settings**—Details such as control interface, cluster interface, management interface, DNS server, and routes. Appears only for Control Plane.
- **Configuration**—Details such as physical interfaces, user-defined interfaces, and static routes interfaces.
- **Traffic & Health**—Details on historical or real-time data such as CPU usage, memory usage, disk usage, disk IO utilization, interface, port usage for control planes and CPU-only usage, memory usage, and port usage for data planes. For control planes, the CPU usage data additionally provides information on the steal time, which is the percentage of time that a virtual CPU waits for a real CPU while the hypervisor serves another virtual processor. CPU and IO performance are measured at setup stage. The setup flow is blocked if the performance is lower than the threshold.
- **DHCP/NAT**—Details on DHP relay and NAT statistics.
- **System**—Details of process name and its health status. Appears only for Data Plane.
- **Alarm**—Details of alarms generated. You can clear alarms or acknowledge alarms that are generated.
- **Event**—Details of events that are generated.
- **DP Zone Affinity**—Details of the data plane, for example, name, profile version, version match information, DP count, and description. Appears only for Data Plane.

Clearing or Acknowledging Alarms

You can clear or acknowledge an alarm.

To clear an alarm:

1. From the **Monitor > Events and Alarms > Alarms**, select the alarm from the list.
2. Click **Clear Alarm**, the Clear Alarm form appears.
3. Enter a comment and click **Apply**.

To acknowledge an alarm:

1. From the **Alarm** tab, select the alarm from the list.
2. Click **Acknowledge Alarm**, the Are you sure you want to acknowledge the selected form appears.
3. Click **Yes**.

Filtering Events

You can view a list of events by severity or date and time.

To apply filters:

1. Go to **Monitor > Events and Alarms > Events**, select the  icon.

The Apply Filters form appears.

2. Complete the following criteria.
 - **Severity**: Select a severity level to filter the list of events.
 - **Category**: Select a category from the list.
 - **Date and Time**: Select the events by their **Start** and **End** dates.

NOTE

You can filter events that generated in the last seven days.

3. Click **OK**, all the events that meet the filter criteria are displayed on the Event page.

Powering Cluster Back

SmartZone cluster nodes may need to be shut down for physical migration/maintenance purpose.

To avoid SmartZone enter crash mode, the cluster needs to form back in time (within Two-and-Half hours). To power up the nodes, perform the following:

1. Power up all nodes at the same time period.
2. All nodes are connected by network.
3. During the setup, it is strongly recommended to configure static IP address to SmartZone interface, if the node's interface IP address settings is configured to DHCP. Make sure the DHCP server assigns a fixed IP address to the interfaces.

Rebalancing APs

AP rebalancing helps distribute the AP load across nodes that exist within a cluster.

When a multi-node cluster is upgraded, the node that reboots the last typically does not have any APs associated with it.

When you click **Rebalance APs**, the following process is triggered:

1. The controller calculates the average AP count based on the number of available control planes and data planes.
2. The controller calculates how many APs and which specific APs must be moved to other nodes to distribute the AP load.
3. The controller regenerates the AP configuration settings based on the calculation result.
4. The web interface displays a message to inform the administrator that the controller has completed its calculations for rebalancing APs.
5. Each AP that needs to be moved to a different node retrieves the updated AP configuration from the controller, reads the control planes and data planes to which it must connect, and then connects to them.

When the AP rebalancing process is complete, which typically takes 15 minutes, one of the following events is generated:

- **Event 770: Generate ApConfig for plane load rebalance succeeded.**
- **Event 771: Generate ApConfig for plane load rebalance failed.**

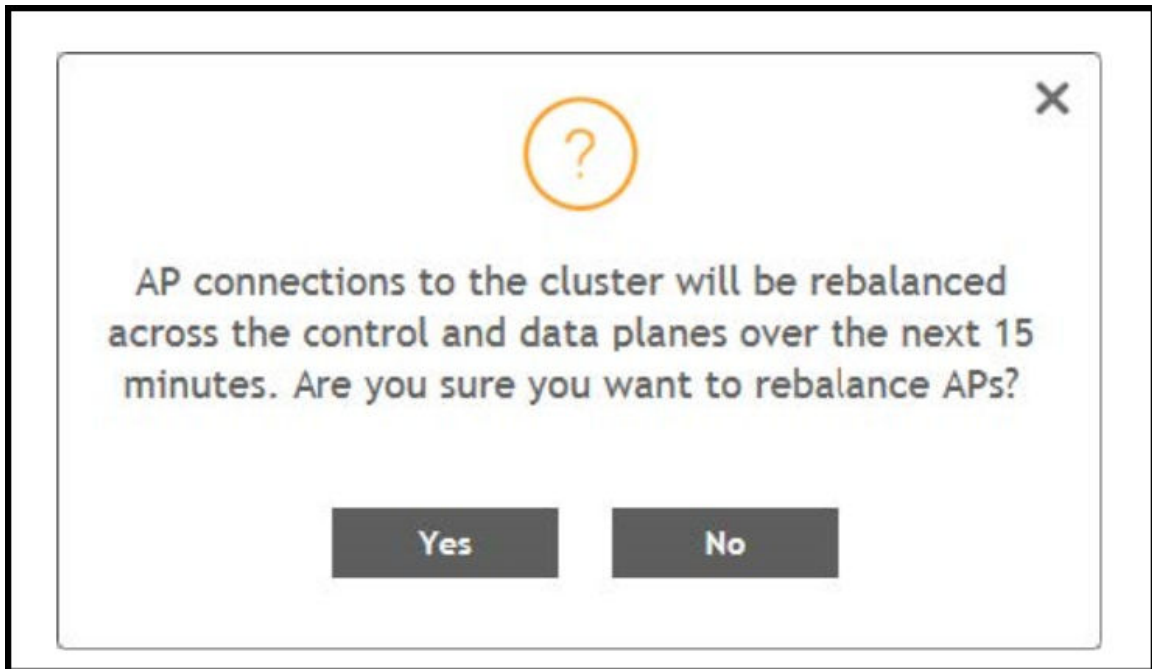
NOTE

- APs may recreate the Ruckus-GRE tunnel to a different data plane.
- Devices associated with an AP that uses the Ruckus-GRE tunnel may temporarily lose network connection for a short period of time (typically, around five minutes) during the AP rebalancing process.
- When node affinity is enabled, AP rebalancing is disallowed on those nodes.
- When data plane grouping is enabled, AP rebalancing is disallowed on those data planes.
- AP rebalancing only supports APs running release 3.2 firmware. APs running on legacy firmware will not be rebalanced.

To rebalance APs across the nodes:

1. From the main menu, go to **Network > Data and Control Plane > Cluster**.

FIGURE 64 AP Rebalancing Form



- From the **Control Planes**, select a cluster, and click **More** tab. Select **Rebalance APs** from the list, the controller rebalances AP connections across the nodes over the next 15 minutes.

NOTE

If you want to repeat this procedure, you must wait 30 minutes before the controller will allow you to rebalance APs again.

Cluster Redundancy

If you have multiple clusters on the network, you can configure cluster redundancy to enable APs managed by a particular cluster to fail over automatically to another cluster if the parent cluster goes out-of-service or becomes unavailable.

Active-Standby mode

When an active cluster becomes inaccessible for APs, external DPs (vSZ-D and SZ100-D), and ICX switches, a standby cluster restores the latest configuration of the Out-Of-Service (OOS) active cluster, and then takes over all external devices (including APs, external DPs, and ICX switches). The AP or ICX switch capacity is limited by the AP or ICX switch High Availability (HA) licenses on the standby cluster and the services license limits from the failed active cluster. When the active cluster returns to the in-service state, the end user can "rehome" all APs, external DPs, and ICX switches back to the active cluster.

The behavior of the standby cluster changes automatically when there is a configuration change in the following deployment types:

- One-to-one (one active cluster to one standby cluster) deployment

The standby cluster restores the configuration from the active cluster after the configuration synchronization is completed. The standby cluster is always in backup mode and ready to receive the APs, external DPs, and ICX switches from the out-of-service active cluster.

During a system upgrade, the ICX switches from the active cluster may fail over to a standby cluster.

To remedy this situation, use the **Rehome** or **Switchover** features on the standby cluster to move these ICX switches back to the active cluster.

By default, the standby cluster will be in **Monitor** mode and serve the active cluster only when the active cluster is out-of-service.

- Many-to-one (two or three active clusters to one standby cluster) deployment

The time taken by Standby cluster from detecting Active cluster is out-of-service to it's being ready to serve APs and external-DPs is enhanced.

When upgrading from SmartZone R3.6.x to SmartZone R5.2 with geo-redundancy enabled, first upgrade the active cluster and then the standby cluster. Once both clusters are upgraded, from the geo-redundancy page of the active cluster, click **Sync Now** to synchronize the configuration of the active and standby clusters.

TABLE 7 Standby Cluster Default Mode When Cluster Redundancy Is Enabled

Deployment	SmartZone R5.1 and Earlier	SmartZone R5.2 and SmartZone R6.0	SmartZone R6.1
1-to-1 Enable geo-redundancy with one active cluster to one standby cluster.	Monitor mode	Backup mode	Monitor mode (default) or Backup mode
Many-to-1 Enable geo-redundancy with two or three active clusters to one standby cluster.	Monitor mode	Monitor mode	Monitor mode

Active-Active Mode

When there are multiple clusters, one cluster can be the configuration source cluster, and all other active cluster restores its configuration periodically to be sure the configuration between the clusters are synchronized continually. When the active cluster becomes inaccessible for APs and external DPs (vSZ-D and SZ100-D), they failover to the target active cluster with priority

NOTE

Cluster redundancy is supported only on SZ300 and vSZ-H and fail over works only for external DPs (vSZ-D and SZ100-D).

A single standby cluster serves as a failover option for one or many distributed active clusters. Different AAA servers can be configured on active and standby clusters.

Precondition

- **Active-Standby mode**

Active-Standby cluster redundancy can be enabled only when matching the following conditions:

- All cluster nodes on both the active and standby clusters must be in service.
- The system version of both clusters must be the same.
- The IP mode must be the same.
- Both clusters must apply the same KSPs on all nodes.
- The control interface of the standby cluster can build a connection to that of the active cluster.

- **Active-Active mode**

Active-Active cluster redundancy can be enabled only when the source active cluster and target active cluster match the following conditions:

- All the cluster nodes must be in service.
- The system version of both clusters must be the same.
- The model (vSZ-H or SZ300) must be the same.
- The network interface number must be equal.
- The IP mode must be the same.

SmartZone Cluster and Cluster Redundancy

Cluster Redundancy

- Both cluster must apply the same KSPs on all nodes.
- "Schedule Configuration Sync" can be enabled only in one cluster.

Configuration

- **Active-Standby mode**

An active cluster can assign only one standby cluster, and the standby cluster can monitor up to three active clusters.

- **Active-Active mode**

Each cluster in Active-Active redundancy can configure up to three target clusters. "Schedule Configuration Sync" can be enabled only in one cluster.

It is highly recommended that you update the configuration from the source cluster until it is eventually synchronized.

Cluster Status

- **Active-Standby mode**

An active cluster works as a normal cluster and the standby cluster is in read-only mode. Only a few configurations can be configured on a standby cluster.

- **Active-Active mode**

All clusters work as a normal cluster

Configuration Backup

- **Active-Standby mode**

An active cluster can back up its configuration and push it to a standby cluster periodically if the scheduler task is configured.

- **Active-Active mode**

A source active cluster can back up its configuration and push it to a target active cluster periodically if the scheduler task is configured

Deployment Models

- **Active-Standby mode**

Beginning with SmartZone 5.1, the implementations in the following table are allowed for Active-Standby mode.

SZ300 (Active)	SZ300 (Standby)	LBO and Tunneled WLANs supported
vSZ-H (Active)	vSZ-H (Standby)	LBO only
vSZ-H/vSZ-D (Active)	vSZ-H/vSZ-D (Standby)	LBO and Tunneled WLANs supported
SZ300 (Active)	vSZ-H (Standby)	LBO only

A standby cluster can be reset as a normal cluster if you set to the factory default after disabling cluster redundancy from the active cluster. Once an Active cluster is set to factory default, it can only be made an Active cluster again either by restoring the entire cluster or by enabling cluster redundancy again. Once a Standby cluster is set to factory default, it can only be made as a Standby cluster again either by restoring the cluster or by clicking "Sync Now" on the active cluster. You can still enable the Active-Standby cluster redundancy again from the active cluster, to set Standby cluster after it has been set to factory default.

- **Active-Active mode**

A cluster in Active-Active mode must be running on either the SZ300 or vSZ-H platforms.

License Management

- **Active-Standby mode**

You must manually sync the license on a standby cluster after it has been set as standby cluster by the active cluster. The standby cluster restores the latest configuration backup files from the out-of-service active cluster, and leverages the license with the active cluster profile, except for the following types of licenses:

- Permanent AP licenses
- Default Temporary AP licenses
- Default Temporary AP License Period

NOTE

- High Availability (HA) AP licenses must be purchased for the standby cluster. The standby cluster work only with High Availability (HA) AP licenses and do not sync or accept any regular AP licenses from any source.
- Active clusters do not accept High Availability (HA) AP licenses; only regular AP licenses must be used.

- **Active-Active mode**

Licenses in each active cluster are independent.

How Cluster Redundancy Works

The following simplified scenario describes how cluster redundancy works and how managed APs fail over from one controller cluster to another.

- **Active-Standby mode**

This mode offers limited UI configurations as most of them are read-only configurations on Standby cluster.

1. After you enable and configure cluster redundancy on the controller, managed APs will obtain IPs of all nodes in Active cluster as server list, and all IPs of all nodes in Standby cluster as failover list, which is shown in AP as:

```
{
  "Server List":["IP_A1", "IP_A2", "IP_A3", "IP_A4"],
  "Failover List":["IP_B1", "IP_B2", "IP_B3", "IP_B4"]
}
```

2. If Cluster A goes out of service or becomes unavailable, APs managed by Cluster A will attempt to connect to the IP addresses (one node at a time) specified for Cluster A.
3. If managed APs are unable to connect to the IP addresses specified for Cluster A, they will attempt to connect to the IP addresses (one node at a time) specified for Cluster B.
4. If managed APs are able to connect to one of the IP address specified for Cluster B, they fail over to Cluster B. APs will move to the zone it belongs to when failover.

NOTE

The standby cluster to which APs fail over must have sufficient license seats to accommodate the new APs that it will be managing. If Standby cluster has insufficient license seats, some APs may not get HA license and these APs will be rejected by the standby cluster.

- **Active-Active mode**

Configurations can be made using the UI.

1. After you enable and configure cluster redundancy on the controller, the IPs of failover list come from all the target active clusters (up to 3) configured in current active cluster are prioritized per cluster, but the nodes in cluster are randomized.

For example, if you enable the cluster redundancy with active-active mode on current active cluster A and configure following active clusters with priority:

- a. Cluster B
- b. Cluster C
- c. Cluster D

The managed APs will obtain IPs of all nodes in cluster A as server list, and all IPs of all nodes in target active clusters as failover list, which is shown in AP as:

```
{  
  "Server List":["IP_A1", "IP_A2", "IP_A3", "IP_A4"],  
  "Failover List":["IP_B4", "IP_B2", "IP_B3", "IP_B1"], ["IP_C1", "IP_C4", "IP_C2", "IP_C3"], ["IP_D2", "IP_D1", "IP_D4", "IP_D3"]  
}
```

2. If Cluster A goes out of service or becomes unavailable, APs managed by Cluster A will attempt to connect to the IP addresses (one node at a time) specified for Cluster A.
3. If managed APs are unable to connect to the IP addresses specified for Cluster A, they will attempt to connect to the IP addresses (one node at a time) specified for Cluster B, and will try next Cluster C if APs unable to connect the IP address (one node at a time) specified for Cluster B.
4. If managed APs are unable to connect to the IP addresses specified for Cluster C, they will attempt to connect to the IP addresses (one node at a time) specified for Cluster D, and will start all over again from Cluster A if all IP addresses unable to connect.

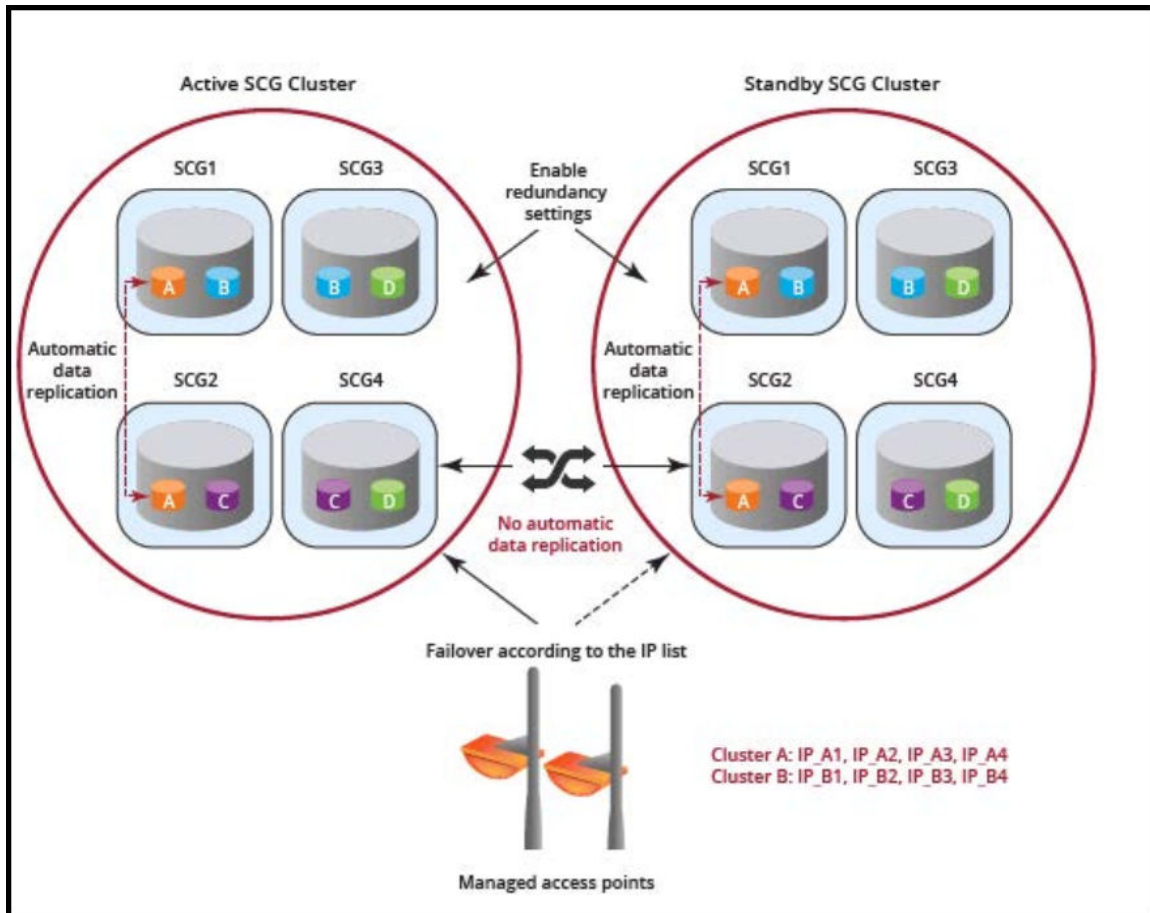
Enabling Cluster Redundancy

Cluster redundancy enables APs to fail over automatically to another cluster if their parent cluster goes out-of-service or becomes unavailable.

Before you configure cluster redundancy for Active-Standby mode, consider the following items:

- Cluster redundancy is disabled by default.
- Super administrators and system administrators have the capability to configure the cluster redundancy settings.
- The super administrator and system administrator usernames and passwords can be different in the active and standby clusters.
- Up to three active clusters are supported beginning with SmartZone 5.0.
- The standby cluster can serve AP failover from one active cluster at a time.
- Some AAA configurations have a secondary server which acts as the backup for AAA. Therefore, AAA configuration for the standby cluster in geo-redundancy provides only the primary AAA configuration used on the standby cluster.
- A secondary server for non-proxy RADIUS and proxy RADIUS does not support High Availability standby in SmartZone 5.1.
- A "SUPPORT-HA-EU" license is required for upgrading a standby cluster.
- A SmartZone support license cannot be used to upgrade the standby cluster.
- It is highly recommended to enable cluster redundancy only in multi-node clusters. For single-node clusters, the external devices (AP, DP, and switch) may failover between clusters with a latency.

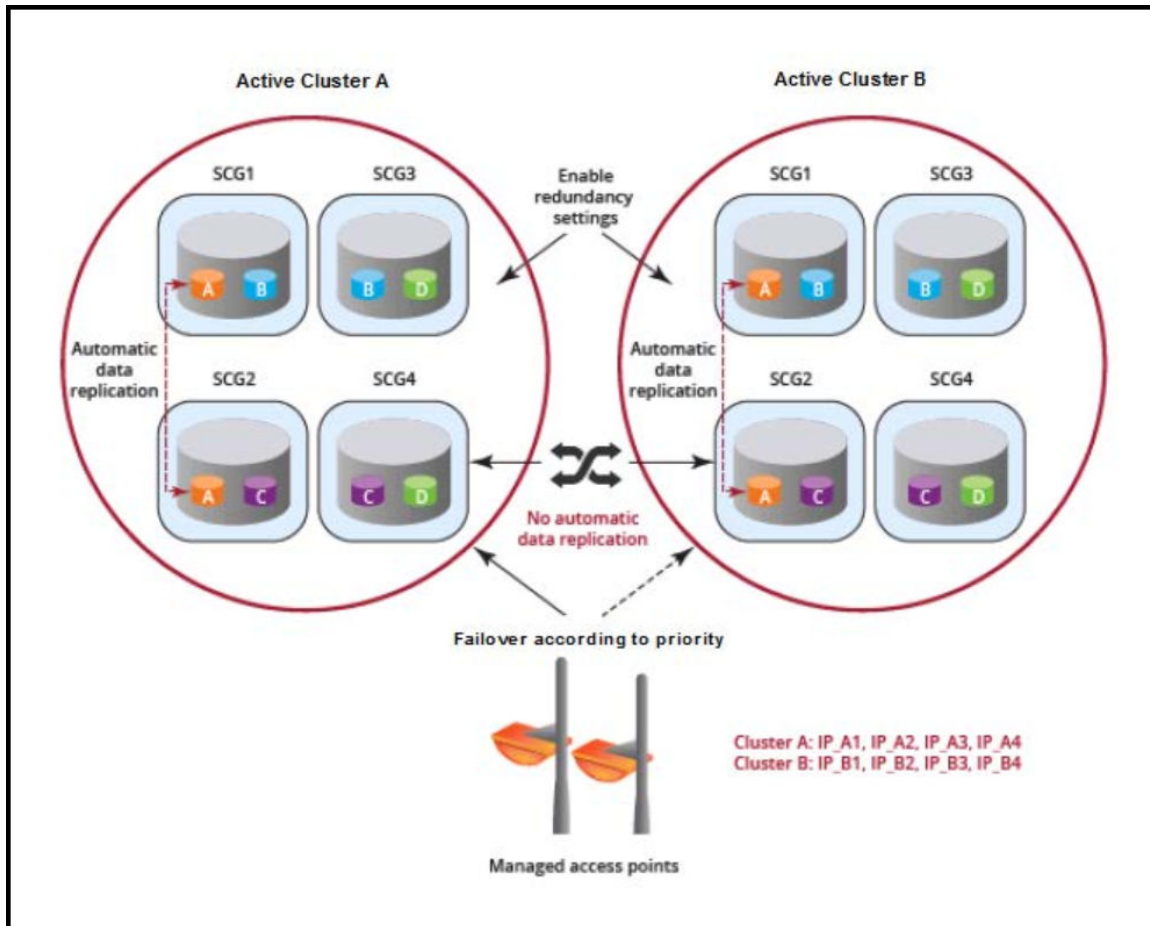
FIGURE 65 Cluster Redundancy for Active-Standby Mode



Before you configure cluster redundancy for Active-Active mode, consider the following items:

- Cluster redundancy is disabled by default.
- Super administrators and system administrators have the capability to configure the cluster redundancy settings.
- The super administrator and system administrator usernames and passwords can be different in all active clusters.
- Each cluster in Active-Active redundancy can configure up to three target clusters.
- Allow only one cluster enable configuration scheduler sync.
- Licenses in the source active cluster and the target active cluster are independent.
- The following features are disabled in the target active cluster after the configuration is restored from the source active cluster:
 - Configuration FTP export
 - Configuration backup scheduler task
 - Cluster redundancy configuration sync scheduler task
- For adding external devices (APs and external DPs), the devices must be registered to the source active cluster (for which the **Schedule** option must be enabled in **Configuration Sync**) before dispatching these devices to the desired target active cluster.
- Target active clusters receive a configuration backup file from the source active cluster and restore it periodically. It is highly recommended to update the configuration from the source active cluster.

FIGURE 66 Cluster Redundancy for Active-Active Mode



NOTE

It is highly recommended to enable cluster redundancy only in a multi-node cluster. If cluster redundancy is enabled in a single-node cluster, external devices (APs, DPs, and ICX switches) may fail over between clusters with a perceivable latency.

Complete the following steps to enable cluster redundancy.

1. Select **System > Cluster**. The **Cluster** page is displayed.
2. Select the cluster, scroll down, and click the **Configuration** tab.
3. On the right side of the **Configuration** area, click **Configure**. The **Edit Cluster** page is displayed.
4. In the **Cluster Redundancy** area, enable the **Enable Cluster Redundancy** option.
5. Choose one of the following types to enable cluster redundancy:
 - **Active-Standby**: You can configure up to three active clusters and one standby cluster to support APs, vSZ-Ds, and ICX switches failover to the standby cluster.

NOTE

Only switches running FastIron 08.0.95b and later fail over to the standby cluster. Failover switches must be approved or rejected according to the switch High Availability license on the standby cluster.

For more information, refer to *RUCKUS SmartZone Software Licensing Guide*.

- a. **Timing to serve Active cluster:** Determines when the standard cluster turns to backup mode and manages external devices (APs, DPs, and ICX switches).
 - **Active out-of-service:** Only when active cluster is out-of-service (default setting).
 - **Always:** Always on service.

When the standby cluster rehomes, the timing to server the active cluster cannot be configured. If the standby cluster upgrades from SmartZone R5.2 and SmartZone 6.0 to SmartZone R6.1, it carries the same **Mode** as SmartZone R5.2 and SmartZone 6.0, and the **Serve Active Cluster Timing** will be **Always on service**.

- b. Enter the admin **Password** of the standby cluster.
- c. For **Management IP** and **Port**, enter at least one IP address and port number of the standby cluster.

NOTE

In **Configuration Sync**, the **Schedule** option is enabled by default.

- d. For **Time**, select the duration in HH:MM format from the list to periodically sync the configurations.
- e. Click **OK**. A confirmation dialog box is displayed.

- **Active-Active:** To support AP and vSZ-D failover from one active cluster to another active cluster, you can configure up to three target clusters to an active cluster.

NOTE

Switches do not support Active-Active mode failover.

- a. For **Password**, enter the admin password of the active cluster.
- b. For **Management IP** and **Port**, enter at least one IP address and port number of the active cluster, and click **Add**.

NOTE

To prioritize the cluster, select the cluster from the list position using **Up** or **Down**. To remove the cluster from the list, select the cluster and click **Delete**.

NOTE

In **Configuration Sync**, the **Schedule** option is enabled by default.

- c. For **Interval**, select the interval to sync and restore the configuration to the target active clusters. If you select **Monthly** or **Weekly**, select the respective day.
- d. For **Hour** and **Minutes**, select the hour and minutes to periodically sync the configurations.
- e. Click **OK**. A confirmation dialog box is displayed.

6. Click **OK**.

NOTE

Once the standby cluster IP address and port has been configured, the active cluster begins to sync configuration to the standby cluster.

NOTE

You can also edit the standby cluster by selecting **Configure** from the **Edit Cluster** page.

Viewing Cluster Configuration

After you have configured cluster redundancy, you can view details of the active and standby clusters.

NOTE

Cluster redundancy is supported only on the SZ300 and vSZ-H platforms.

Complete the following steps to view the cluster configuration.

1. Go to **Network > Data and Control Plane > Cluster**.

The **Cluster** page is displayed.

2. Select the cluster, scroll down, and click the **Configuration** tab. You can view the cluster details listed in the following table.

TABLE 8 Cluster Details

Field	Description	Active Cluster	Standby Cluster
Cluster Configuration			
IP Support	Displays the IP support version.	Yes	Yes
Cluster Redundancy			
Status	Displays the cluster redundancy status.	Yes	Yes
Cluster Redundant Role	States whether the cluster is an active or a standby cluster.	Yes	Yes
Mode	States whether the cluster is in monitor mode or backup mode. <ul style="list-style-type: none"> • Monitor mode: Standby cluster serves the active cluster only when the active cluster is out-of-service. • Backup mode: Standby cluster is always ready to accept external devices from the active cluster. Click Alter monitoring status to turn on or turn off the monitoring status of the active cluster. To remove the active cluster, select it from the list and click Delete .	No	Yes
Active Cluster	Displays the cluster name and control IP addresses of the cluster.	Yes	Yes
Standby Cluster	Displays the cluster name, management IP addresses, and control IP addresses of the cluster.	Yes	No
Serve Active Cluster Timing	Indicates when the standard cluster turns to backup mode and manages external devices (APs, DPs, and ICX switches). <ul style="list-style-type: none"> • Only when active cluster is out-of-service (default setting) • Always on service 	No	Yes
Schedule Configuration Sync	<ul style="list-style-type: none"> • Status: Displays sync status. • System Time Zone: Displays the system time zone set. • Time: Displays the sync time followed every day. • Last Trigger Time: Displays the date and time the clusters synced last. Applies to both scheduled sync or manually sync. • Next Trigger Time: Displays the date and time of the next scheduled sync. • Sync Now: Triggers manual configuration sync operation. 	Yes	No
State	Displays the system configuration sync state.	Yes	No
Progress Status	Displays the progressive status of the system configuration sync.	Yes	No

AP Auto Rehome

The **AP Auto Rehome** functionality allows APs to fail back to the source active cluster automatically in an Active-Active cluster deployment.

In an Active-Active cluster redundancy environment, clusters are usually deployed at different geographical locations. When the source active cluster fails, APs seamlessly failover to a target active cluster and remain operational. If the target cluster fails for any reason, the APs may fail back to the source active cluster (if it is in-service); otherwise, the APs failover to another target active cluster. However, instead of waiting for another failover scenario or manually rehomeing individual APs, the **AP Auto Rehome** functionality automatically rehome the APs to the source active cluster. You can enable **AP Auto Rehome** and configure the primary cluster and fallback attempt interval from the SmartZone web interface. When the feature is enabled, APs being managed by a target active cluster will periodically check availability of the source active cluster and automatically rehome.

NOTE

AP Auto Rehome is configurable only for a cluster that is in Active-Active redundancy mode.

NOTE

AP Auto Rehome is supported only on SZ300 and vSZ platforms.

NOTE

AP Auto Rehome is configurable only at the zone level.

Complete the following steps to apply the AP Auto Rehome configuration on an AP zone.

1. From the menu, click **Network > Wireless > Access Points**.

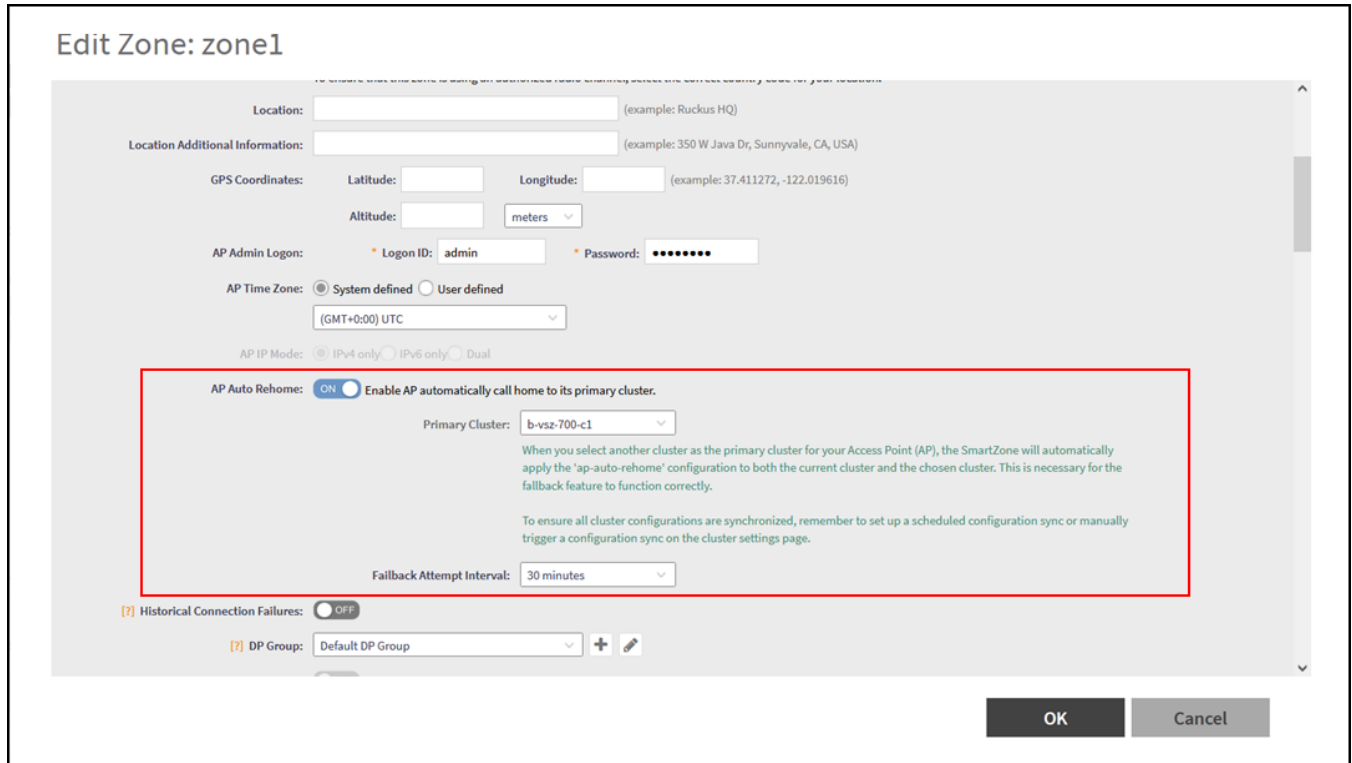
FIGURE 67 Access Points Page

MAC Address	AP Name	Zone	IP Address	AP Firmware	Configuration Status	Last Seen	Data Plane	Administrative State	Registration State	Model
D8:38:FC:36:89:70	AP16-R610	FR-5604-Bing-v4	100.102.20.16	6.1.1.0.1068	Up-to-date	2022/10/14 15:20:05	[100.102.40.228]23...	Unlocked	Approved	R610
28:B3:71:1E:FF:B0	AP48-R850	FR5604-WDS-v4	100.102.20.48	6.1.1.0.1068	Up-to-date	2022/10/14 15:20:04	[100.102.40.228]23...	Unlocked	Approved	R850
74:3E:2B:29:23:C0	AP2-R710	Abon-v4	100.103.4.142	6.1.1.0.947	New Configuration	2022/07/06 16:43:11	N/A	Locked	Approved	R710
28:B3:71:2A:83:40	AP38-R850	FR-5604-Bing-v4	100.102.20.38	6.1.1.0.1068	New Configuration	2022/09/01 10:08:23	N/A	Unlocked	Approved	R850
34:8F:27:18:86:D0	AP6-Abon-T310C	Abon-v4	100.103.4.146	6.1.1.0.947	New Configuration	2022/07/06 16:44:31	N/A	Locked	Approved	T310C
94:BF:C4:2F:FE:80	AP36-R610	Default Zone	100.102.20.36	6.1.1.0.1068	New Configuration	2022/09/16 13:45:24	N/A	Unlocked	Approved	R610
EC:8CA2:10:40:E0	AP15-R510	FR-5604-Bing-v6	6.1.1.0.1068	6.1.1.0.1068	New Configuration	2022/09/01 10:08:28	N/A	Unlocked	Approved	R510
D8:38:FC:36:89:90	AP26-R610	FR-5604-Bing-v6	2001:b030:251:...	6.1.1.0.1068	Up-to-date	2022/10/14 15:20:20	[2001:b030:2516:13...	Unlocked	Approved	R610

2. Select the zone that is created in the Active-Active cluster redundancy mode, and click the **Edit** option. To configure a cluster in Active-Active mode, refer to *RUCKUS SmartZone Controller Administration Guide*.

The **Edit Zone** page is displayed.

FIGURE 68 Editing a Zone



3. Under **General Options**, for **AP Auto Rehome**, click the **Enable AP automatically call home to its primary cluster** to toggle the switch to **ON**.
4. For **Primary Cluster**, select the primary cluster from the list of active clusters.
5. For **Fallback Attempt Interval**, select the time interval from the list. This is the time interval to trigger the AP Auto Rehome configuration on the primary cluster.

The available time intervals are **1 day**, **4 hours**, **30 Minutes** (default), and **30 Seconds**. Default value is 30 minutes.

6. Click **OK**.

Disabling Cluster Redundancy - Active-Standby from the Active Cluster

To disable the cluster redundancy from the active standby cluster when the active cluster is in-service, perform these steps.

1. Go to **Network > Data and Control Plane > Cluster**.
The **Cluster** page appears.
2. Select the cluster, scroll down and click the **Configuration** tab.
3. On the right side of the **Configuration** area, click **Configure**.

The **Edit Cluster** page appears.

4. In the **Cluster Redundancy** area, click the **Enable Cluster Redundancy** option, if this option is enabled and the button appears blue in color.
5. Click **OK**.

If the active cluster is out-of-service, use the Disabling Cluster Redundancy - Active-Standby from the Standby Cluster task.

Disabling Cluster Redundancy - Active-Standby from the Standby Cluster

To disable the cluster redundancy from the standby cluster, perform these steps.

NOTE

Only an out-of-service active cluster can be deleted from the standby cluster.

1. Go to **Network > Data and Control Plane > Cluster**.
The **Cluster** page appears.
2. Select the cluster, scroll down and click the **Configuration** tab.
3. From the **Active Cluster** list, select the cluster and click **Delete**.

Deleting Cluster Redundancy - Active-Active from a target Active Cluster

To delete a target active cluster form active-active cluster redundancy mode, perform these steps.

1. Go to **Network > Data and Control Plane > Cluster**.
The **Cluster** page appears.
2. Select the cluster, scroll down and click the **Configuration** tab.
3. On the right side of the **Configuration** area, click **Configure**.
The **Edit Cluster** page appears.
4. In the Cluster Redundancy area, click the **Enable Cluster Redundancy** option, if this option is enabled and the button appears blue in color.
In **Type**, choose **Active-Active**.
5. From the Target Active Cluster list, select the cluster and click **Delete**.

Disabling Cluster Redundancy - Active-Active mode from a Current Target Active Cluster

You can disable a current target cluster in an active-active cluster redundancy mode. To do so, perform these steps:

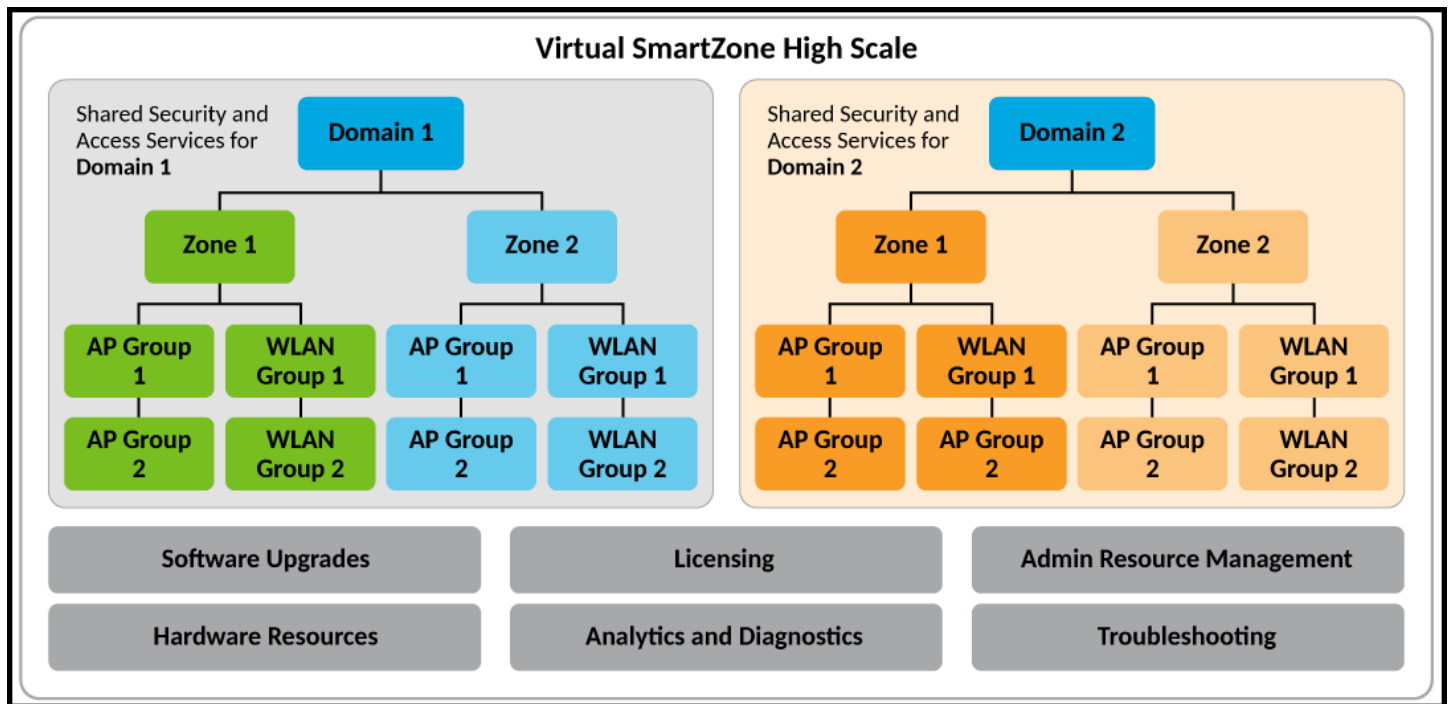
1. Go to **Network > Data and Control Plane > Cluster**.
The **Cluster** page appears.
2. Select the cluster, scroll down and click the **Configuration** tab.
3. On the right side of the **Configuration** area, click **Configure**.
The **Edit Cluster** page appears.
4. In the Cluster Redundancy area, click the **Enable Cluster Redundancy** option to switch off the option.
5. Click **OK**.

SmartZone Network Hierarchy

- SmartZone Domains..... 101
- AP Zones..... 103
- WLAN Groups..... 104
- Switch Groups..... 106

The SmartZone controller implements a hierarchical structure that enables administrators to exercise precise control over access points, switches, wireless LANs (WLANs), and their associated services. This hierarchical organization facilitates the management of diverse networks, ranging from small single-location enterprises to large Managed Service Providers (MSPs) servicing multiple locations. With centralized, redundant, and failure-resilient control, administrators can efficiently oversee network operations across a wide range of environments.

FIGURE 69 SmartZone Network Hierarchy



SmartZone Domains

The SmartZone 300 and Virtual SmartZone High-Scale platforms are designed to meet the needs of large enterprises and service providers. These advanced platforms offer robust features, including the ability to create Domains and Partner Domains for effective network segmentation. Each Domain or Partner Domain provides separate administrative access and can be configured with tailored network services. This flexibility allows organizations to efficiently manage diverse and unrelated network domains within their infrastructure.

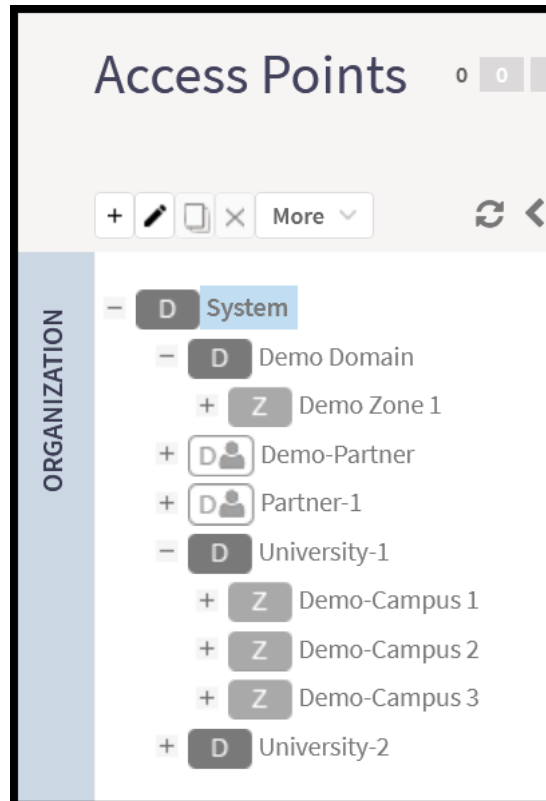
RUCKUS recommends utilizing Domains specifically when there is a need to establish distinct administrative boundaries within a network environment. In essence, Domains are employed to segregate different administrative realms, ensuring that each administrator is responsible for managing only a designated Domain. This segmentation restricts their access and prevents them from viewing or controlling other Domains within the network. By implementing Domains in this manner, organizations can enhance security, streamline management tasks, and maintain clear delineations of administrative responsibilities across their network infrastructure.

Designed for smaller enterprises, the SZ-100, SZ144, and Virtual SmartZone Essentials platforms do not support the options for multiple Domains and Partner Domains. Instead, these controllers automatically generate a single default System Domain, within which AP Zones and AP groups can be created.

Partner Domains

Partner Domains offer the same network services and capabilities as regular Domains, with the exception that Partner Domains are specifically designed to address the needs of operators who require separation between tenants, each with their own unique configurations, profiles, and system objects. The key features of Partner Domains include tenant isolation, privacy, and role-based access control. Both Partner and regular Domains can coexist within the same System Domain. However, administrators of Partner Domains do not have access to other segments within the System Domain hierarchy. Partner Domains can be distinguished from regular Domains in the System Domain hierarchy by the silhouette in the Partner Domain icon.

FIGURE 70 Domains and Partner Domains



AP Zones

Depending on the scale and characteristics of the network infrastructure, AP Zones may serve as representations of various physical locations, such as individual buildings within a campus or distinct campuses within a larger organization. It is important to note that each AP Zone establishes an internal framework governing the behavior of access points (APs) and wireless LANs (WLANs) within its boundaries, effectively creating a closed network environment. APs located in neighboring locations that do not belong to the same AP Zone are categorized as rogue APs, despite being managed by the same controller. As a result, these neighboring APs are excluded from considerations such as load balancing, channel selection, roaming, and other network optimization calculations. This segregation ensures that network operations remain optimized and secure within each designated AP Zone, enhancing overall performance and reliability across the network infrastructure.

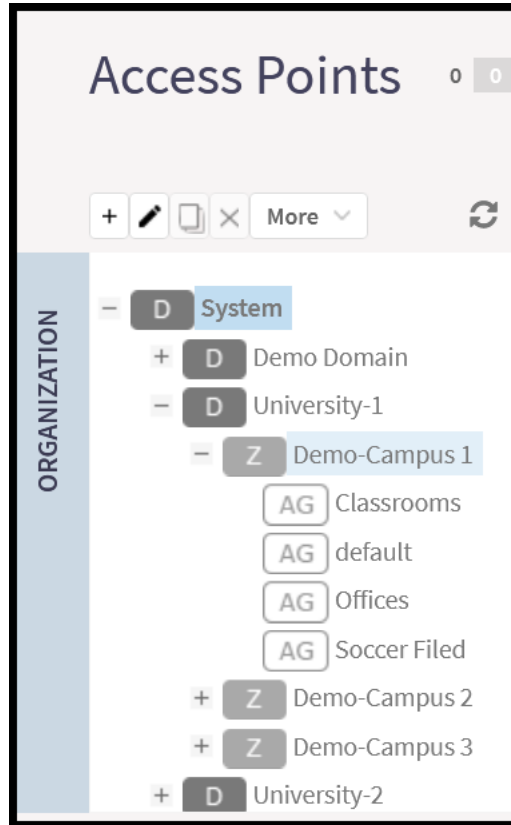
Furthermore, AP Zones share resources such as WLAN Groups and services like RADIUS authentication, guest access, and others, providing administrative flexibility and centralized management capabilities for each of the zones.

AP Groups

AP Groups provide a more detailed level of configuration segmentation within each of the zones, empowering administrators to organize access points (APs) based on various criteria such as type, capabilities, and configuration restrictions. For instance, administrators can group APs according to the specific environment where they are deployed, ensuring that all APs within the group possess consistent configuration characteristics. This may include settings such as transmission power for antennas and radio band selection for APs deployed in open areas, Ethernet port configuration for APs installed in hotel rooms, or LED visibility preferences for APs situated in hallways or hospital rooms. By grouping APs in this manner, administrators can streamline management tasks and ensure that each AP receives the appropriate configuration settings tailored to its deployment environment.

Additionally, AP Groups can share equal or similar SSID configurations, further simplifying WLAN administration and ensuring uniformity across the network. Nevertheless, administrators have the flexibility to override AP Zone or AP Group configurations on individual APs when necessary, providing granular control over network settings as needed.

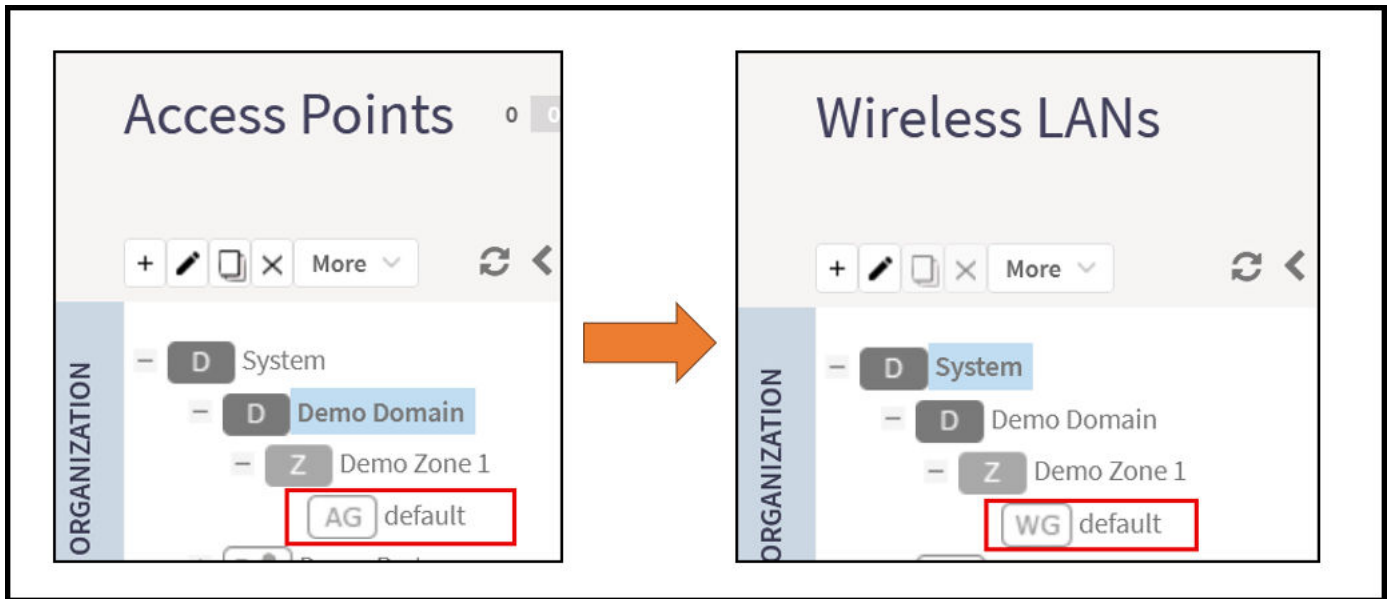
FIGURE 71 AP Domains, Zones, and Groups



WLAN Groups

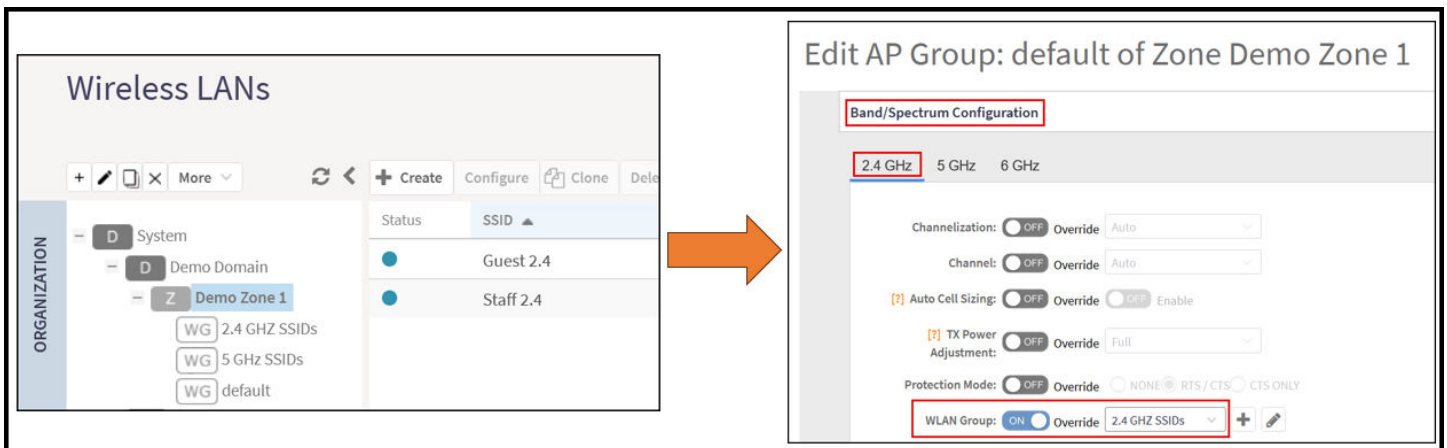
By default, when an AP Zone is created, a default WLAN Group is automatically created and assigned to the AP Zone and any AP Group within it; however, a new WLAN Group can be created on demand, and the administrator can override the default assignment at the AP Group level or at the individual AP level. The example below shows the newly created AP Zone called Demo-Campus 1, as well as the default AP Group and default WLAN Group that were automatically assigned to the Zone.

FIGURE 72 Automatic Creation of the Default AP Group and WLAN Group



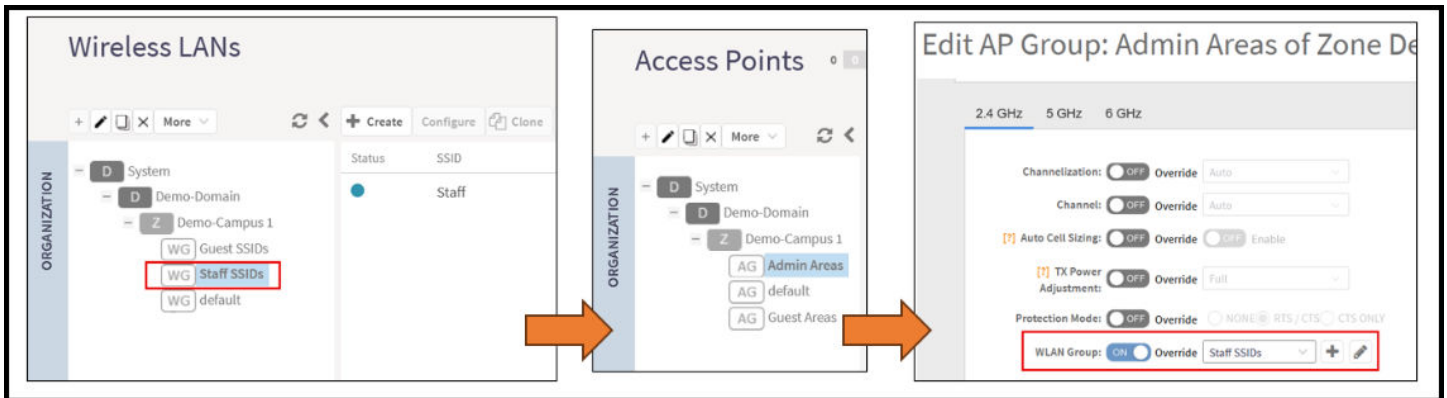
Grouping the SSIDs (WLANs) helps the administrator to assign WLAN Groups to different segments of the network, as necessary, by binding the WLAN Groups to AP Groups. Refer to the below use case example where the administrator has assigned a different WLAN Group to each radio band (2.4 GHz or 5 GHz).

FIGURE 73 Assigning a different WLAN Group to each radio band of an AP Group



One more use case example involves a different approach. Here, the network administrator of a hotel has decided to broadcast different SSIDs in the guest areas and the administrative areas. As seen, the WLAN Group “Staff SSIDs” is assigned to the AP Group “Admin Areas” in the 2.4 GHz band.

FIGURE 74 Assigning a different WLAN Group to each AP Group



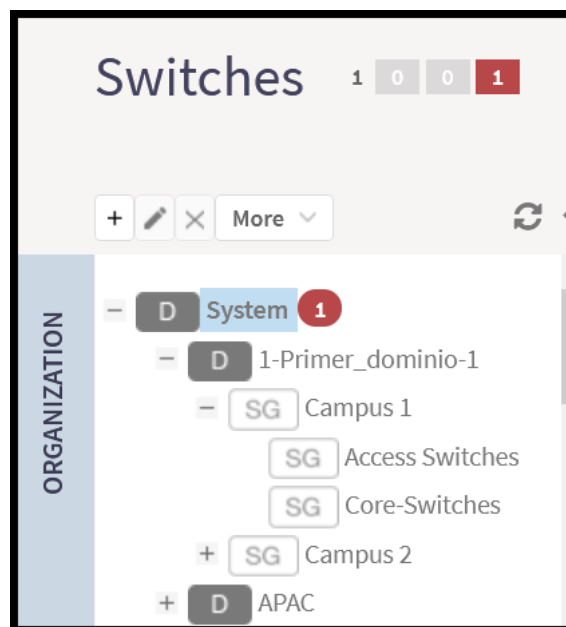
NOTE

For more information, refer to how to create or modify WLANs, WLAN Groups, and AP Groups, and all possible configuration options related to them.

Switch Groups

Like AP Groups, Switch Groups offer a granular configuration scheme for groups of switches that may share equal or similar environments, purposes, locations, and so on. Using Switch Groups, the administrator can segment the switch inventory based on configuration, firmware version, and so on. Switches don't offer the chance to create Switch Zones, if further sub-grouping of switches is desired, SmartZone allows for one additional sub-level of grouping, also called a Switch Group.

FIGURE 75 SmartZone Switch Groups



Onboarding Access Points and Switches

- Onboarding APs and Switches..... 107
- Introduction to Firewall Ports..... 108
- Ports to Open Between Various RUCKUS Devices, Servers, and Controllers..... 108

Switches and access points must know the IP address of the controller and it must be reachable by them so they can start communication for the onboarding process. There are different methods for APs and Switches to learn this information, which will be discussed in the following sections. Some additional parameters may be required, such as SSL certificates for secured end-to-end communication, low latency environments, and rule-free access through firewalls for specific IP ports.

Onboarding APs and Switches

Onboarding a switch or AP can be defined as the process of having the AP or Switch contact the controller for the first time and having it fully managed by the controller. It involves the automatic process of getting the appropriate firmware loaded on the AP or Switch and successful configuration synchronization.

Requirements to Onboard Access Points or Switches

To ensure the successful onboarding of the managed equipment in the controller, the administrator should verify the following aspects:

- **Sufficient AP Capacity Licenses or Switch Capacity licenses:** Confirm that there are enough licenses in the controller to accept the required equipment.
- **System Capacity of the Controller:** Ensure the current amount of onboarded APs and Switches does not exceed the capacity of the controller.
- **Supported Model:** Verify that the AP model or Switch model is supported in the current version of the controller.
- **Country Code Matching:** Ensure that the hard-coded country code in the AP matches the country code configured in the controller.
- **AP MAC OUI Validation:** Check if the AP MAC address adheres to the validation rules. OUI Validation rules check the first three octets of the AP MAC address.
- **AP/Switch Registration Rules:** Confirm that the AP or Switch can be accepted or make sure it is manually approved.
- **AP Certificate Validity:** Verify that the AP certificate is valid or that certificate validation is disabled in the controller.
- **TPM switch type is allowed:** Ensure the controller is configured to accept switches with self-signed certificates.
- **Network Connectivity:** Ensure that the AP and Switch are reachable by the controller and that the required ports for communication are open in the firewall.

During the normal onboarding process, it is expected for the APs to reboot at least twice when doing the firmware update and the configuration sync. Using the LED indicators on the AP helps to understand the current stage of the AP onboarding process.

NOTE

Refer to the *RUCKUS SmartZone Network Administration Guide* for a full understanding of the above items and additional information related to onboarding APs and Switches to the controller.

Introduction to Firewall Ports

An important part of a stateful firewall is the ability to track the state of traffic connections.

This is a security measure intended to help prevent intrusions and spoofs. The firewall attempts to make sure any incoming connection is matched with a known active connection that was initiated from inside the firewall. Any packets that do not comply with these rules or are specifically allowed (well-known protocols such as FTP servers and others) are typically dropped. Different ports are necessary to allow various communications for control, data, and management traffic.

Ports to Open Between Various RUCKUS Devices, Servers, and Controllers

The below table lists ports that must be opened in the network firewall to ensure that the vSZ-D/SZ/vSZ (controller), managed APs, and RADIUS servers can communicate with each other successfully.

TABLE 9 Ports to Open Between Various RUCKUS Devices, Servers, and Controllers

From (Sender)	To (Listener)	Communication Port Number	Layer 4 Protocol	Interface	Configurable from Web Interface?	Purpose
AP	Control plane of : SZ-100 SZ-300 vSZ	21	TCP	Control	No	ZD and Solo APs can download SZ AP firmware and convert themselves to SZ APs.
AP	AP	1883	TCP	Control	No	AP-AP communication for neighbor AP information exchange in FT, Client Load Balance, etc.
AP	Control plane of : SZ-100 SZ-300 vSZ	22	TCP	Control	No	SSH Tunnel for management
AP ZD	SZ	69	UDP	Control	No	ZD Migration

TABLE 9 Ports to Open Between Various RUCKUS Devices, Servers, and Controllers (continued)

From (Sender)	To (Listener)	Communication Port Number	Layer 4 Protocol	Interface	Configurable from Web Interface?	Purpose
AP	vSZ control plane	91 (AP firmware version 2.0 to 3.1.x) and 443 (AP firmware version 3.2 and later)	TCP	Control	No	<p>AP firmware upgrade APs need Port 91 to download the Guest Logo and to update the signature package for the ARC.</p> <p>NOTE Starting with SZ 3.2 release, the controller uses an HTTPS connection and an encrypted path for the firmware download. The port used for AP firmware downloads has been changed from port 91 to 443 to distinguish between the two methods. To ensure that all APs can be upgraded successfully to the new firmware, open both ports 91 and 443 in the network firewall.</p>
AP	RAC (RADIUS Access Controller)	1813	UDP	Management, Cluster, Control	No	<p>RADIUS_Auth profile defines both inbound and outbound traffic. Information specified here is for inbound traffic only.</p> <p>NOTE The Management interface is applicable when vSZ-H is in single-interface mode. If in 3-interface mode, Access and Core separation disabled, it depends on the configured Management traffic interface.</p>
AP	SZ	5353	UDP	Control	No	Resolves hostnames to IP addresses
AP DP	SZ	8200	TCP	Control	No	Captive Portal OAuth service port for HTTP

Onboarding Access Points and Switches

Ports to Open Between Various RUCKUS Devices, Servers, and Controllers

TABLE 9 Ports to Open Between Various RUCKUS Devices, Servers, and Controllers (continued)

From (Sender)	To (Listener)	Communication Port Number	Layer 4 Protocol	Interface	Configurable from Web Interface?	Purpose
AP DP	SZ	8222	TCP	Control	No	Captive Portal OAuth service port for HTTPS
AP DP	SZ	8280	TCP	Control	No	Captive Portal Web Proxy service port for HTTPS
AP-MD	SZ-MD	9191	TCP	Cluster	No	Communication between AP-MD and SZ-MD
AP	vSZ control plane	12223	UDP	Control	No	LWAPP discovery sends image upgrade request to ZD-APs via LWAPP (RFC 5412).
AP UE	SZ	18301	UDP	Management, Cluster, Control	No	SpeedFlex tests the network performance between AP, UE, and SZ.
ICX	vSZ control plane	22	TCP	Control	No	SSH Tunnel.
ICX	vSZ control plane	443	TCP	Control	No	Access to the vSZ/SZ control plane over secure HTTPS.
SZ	External FTP server	20-21	TCP	Control, Cluster, Management	No	Transfer data to external FTP servers
Follower SZ nodes	Master SZ node	123	UDP	Cluster	No	Sync system time among SZ nodes
SZ	External Licensing Server	443	TCP	Management	No	Download licensing and support entitlements from the licensing server.
SZ	External Licensing server	443	TCP	Management	No	Download licensing and support entitlements from the licensing server.
SZ-RAC	External AAA	1812	UDP	Management, Cluster, Control NOTE The Management interface is applicable when vSZ-H is in single-interface mode. If in 3-interface mode, Access and Core separation disabled, it depends on the configured Management traffic interface.	Yes	To Support RADIUS Proxy Authentication
SZ	SZ	5671-5672	TCP	Cluster	No	RabbitMQ inter-node cluster communication
SZ	SZ	6379, 6380	TCP	Cluster	No	Internal communication among SZ nodes
SZ	SZ	7000	TCP/UDP	Cluster	No	Cassandra (database) cluster communication and data replication

TABLE 9 Ports to Open Between Various RUCKUS Devices, Servers, and Controllers (continued)

From (Sender)	To (Listener)	Communication Port Number	Layer 4 Protocol	Interface	Configurable from Web Interface?	Purpose
SZ	SZ	7500	UDP	Cluster	No	SZ Clustering Operation
SZ	SZ	7800	TCP/UDP	Cluster	No	Cluster node communication for cluster's operations
SZ	SZ	7800-7805	TCP	Cluster	No	A protocol stack using TCP on JGroups library for node to node communication
SZ	SZ	7810	TCP	Cluster	No	A protocol stack using FD_SOCKET on JGroups library for node-to-node communication
SZ	SZ	7811	TCP	Cluster	No	A protocol stack using FD_SOCKET on JGroups library for node-to-node communication
SZ	SZ	7812	TCP	Cluster	No	A protocol stack using FD_SOCKET on JGroups library for node-to-node communication
SZ	SPoT	8883 NOTE The connection between the controller and vSPoT is an outbound connection, so it depends on the destination IP address. If the destination IP address falls in the subnet of one interface, it is routed to that interface. Otherwise, it is routed via the default route.	TCP	Management, Cluster, Control	No	Communication between SZ and SPoT
SZ	SZ	9300-9400	TCP	Cluster	No	Internal communication between nodes within the cluster (ElasticSearch database)
SZ local modules	SZ memproxy	11211	TCP	Cluster	No	Internal proxy for saving in-memory data to memcached
SZ	SZ	11311	TCP	Cluster	No	Memory cache server
SZ	SZ	33434-33534	UDP	Management, Cluster, Control	No	ICX Troubleshooting (traceroute).
SZ CS	DP	65534, 65535	TCP	Management	No	DP Debug
TACACS+ Server	TACACS+ Server	49	TCP	Management, Cluster, Control	No	TACACS+

Onboarding Access Points and Switches

Ports to Open Between Various RUCKUS Devices, Servers, and Controllers

TABLE 9 Ports to Open Between Various RUCKUS Devices, Servers, and Controllers (continued)

From (Sender)	To (Listener)	Communication Port Number	Layer 4 Protocol	Interface	Configurable from Web Interface?	Purpose
DNS Server	DNS	53	TCP/UDP	Management, Cluster, Control	No	DNS
DHCP Server	SZ	67,68	UDP	Management, Cluster, Control	No	DHCP
Walled-Garden Web Server	Captive Portal with HTTP Proxy	80	TCP	Management, Cluster, Control	No	WISPr_WalledGarden
SNMP Client	SZ	161	UDP	Management	No	Simple Network Management Protocol (SNMP)
LDAP Server	RAC	389	TCP/UDP	Management, Cluster, Control	Yes	SZ to LDAP
SZ	rsyslog	514	TCP/UDP	Management, Cluster, Control	No	Remote Syslog
DHCP v6 Server	SZ	546, 547	UDP	Management, Cluster, Control	No	DHCPv6 Protocol
LDAPS Server	RAC	636	TCP	Management, Cluster, Control	Yes	SZ to LDAPS Server
AAA server	SZ	2083 (RadSec)	TCP	Management, Cluster, Control	No	The default destination port number for RADIUS over TLS is TCP/2083 (As per RFC-6614)
AAA server	SZ	2084 (CoA/DM Over RadSec)	TCP	Management, Cluster, Control	No	SZ as RadSec server listens on port 2084 for incoming TLS connection from client (AAA Client) to process CoA/DM messages over RadSec.
AD Server (MSTF-GC)	RAC	3268	TCP	Management, Cluster, Control	Yes	SZ to AD (MSTF-GC)
External AAA Server (free RADIUS)	SZ-RAC (vSZ control plane)	3799	UDP	Management, Cluster, Control	No	Supports Disconnect Message and CoA (Change of Authorization) which allows dynamic changes to a user session such as disconnecting users and changing authorizations applicable to a user session.
JITC CAC	SZ	4443	TCP	Control	No	Since SZ 5.1.2 release, mainly for JITC CAC login support. This port is opened for NGINX to configure for client certificate authentication.
Legacy Public API Client	SZ	7443	TCP	Management	No	Deprecated Public API
Any	Management interface	8022	No (SSH)	Management	Yes	When the management ACL is enabled, you must use port 8022 (instead of the default port 22) to log on to the CLI or to use SSH.
Any	vSZ control plane	8090	TCP	Control	No	Allows unauthorized UEs to browse to an HTTP website
Any	vSZ control plane	8099	TCP	Control	No	Allows unauthorized UEs to browse to an HTTPS website
Any	vSZ control plane	8100	TCP	Control	No	Allows unauthorized UEs to browse using a proxy UE

TABLE 9 Ports to Open Between Various RUCKUS Devices, Servers, and Controllers (continued)

From (Sender)	To (Listener)	Communication Port Number	Layer 4 Protocol	Interface	Configurable from Web Interface?	Purpose
Any	vSZ management plane	8443 NOTE The Public API port has changed from 7443 to 8443.	TCP	Management	No	Access to the controller web interface via HTTPS
Any	vSZ control plane	9080	HTTP	Management, Control	No	Northbound Portal Interface for hotspots
Any	vSZ control plane	9443	HTTPS	Management, Control	No	Northbound Portal Interface for hotspots
Client device	SZ control Plane	9997	TCP	Control	No	Internal Subscriber Portal in HTTP
Any	vSZ control plane	9998	TCP	Control	No	Hotspot WISPr subscriber portal login/logout over HTTPS

TABLE 10 vDP/ SZ300 DP Data Group(PG-2):

From (Sender)	To (Listener)	Port Number	Layer 4 Protocol	Interface	Configurable from Web Interface?	Purpose
AP vSZ_D	vSZ control plane	22	TCP	Control, Cluster, Management	No	SSH Tunnel

NOTE

The destination interfaces are meant for three-interface deployments. In a single-interface deployment, all the destination ports must be forwarded to the combined management and control interface IP address.

NOTE

Communication between APs is not possible across NAT servers.

Monitoring the Network

- Monitoring the Network..... 115

Monitoring the Network

When you select a System, Domain, Zone, or AP Group from the hierarchy tree, respective contextual tabs appear at the bottom of the page.

These tabs are used to monitor the selected group. The following tables list the tabs that appear for System, Domain, Zone, and AP Group.

TABLE 11 System, Domain, Zone, and AP Groups Monitoring Tabs for SZ300 and vSZ-H platforms

Tabs	Description	System	Domain	Zone	AP Groups
General	Displays group information	Yes	Yes	Yes	Yes
Configuration	Displays group configuration information.	Yes	Yes	Yes	Yes
Health	Displays historical health information.	Yes	Yes	Yes	Yes
Traffic	Displays historical traffic information.	Yes	Yes	Yes	Yes
Alarm	Displays alarm information.	Yes	Yes	Yes	Yes
Event	Displays event information.	Yes	Yes	Yes	Yes
Clients	Displays client information. NOTE Selecting the Enable client visibility regardless of 802.1X authentication check box bypasses 802.1X authentication for client visibility. This option allows you to view statistical information about wired clients even without enabling 802.1X authentication.	Yes	Yes	Yes	Yes
WLANs	Displays WLAN information.	Yes	Yes	Yes	NA
Services	Displays information on the list of services.	Yes	Yes	Yes	NA
Administrators	Displays administrator account information.	Yes	NA	NA	NA

Additionally, you can select System, Domain, or Zone and click **More** to perform the following operations as required:

- **Move**
- **Create New Zone from Template**
- **Extract Zone Template**
- **Apply Zone Template**
- **Change AP Firmware**
- **Switchover Cluster**
- **Trigger Preferred Node**

TABLE 12 System, Zone, and AP Groups Monitoring Tabs for SZ100 and vSZ-E platforms

Tabs	Description	System	Zone	AP Groups
General	Displays group information	Yes	Yes	Yes
Configuration	Displays group configuration information.	Yes	Yes	Yes

TABLE 12 System, Zone, and AP Groups Monitoring Tabs for SZ100 and vSZ-E platforms (continued)

Tabs	Description	System	Zone	AP Groups
Health	Displays historical health information.	Yes	Yes	Yes
Traffic	Displays historical traffic information.	Yes	Yes	Yes
Alarm	Displays alarm information.	Yes	Yes	Yes
Event	Displays event information.	Yes	Yes	Yes
Clients	Displays client information. NOTE Selecting the Enable client visibility regardless of 802.1X authentication check box bypasses 802.1X authentication for client visibility. This option allows you to view statistical information about wired clients even without enabling 802.1X authentication.	Yes	Yes	Yes
WLANs	Displays WLAN information.	Yes	Yes	NA
Services	Displays information on the list of services.	Yes	Yes	NA
Troubleshooting	Displays client connection and spectrum analysis	Yes	Yes	Yes
Administrators	Displays administrator account information.	Yes	NA	NA

Additionally, you can select System, Zone or AP Group and click **More** to perform the following operations as required:

- **Create New Zone from Template**—Does not apply to Zone and AP group management.
- **Extract Zone Template**—Does not apply to System and AP group management.
- **Apply one Template**—Does not apply to System and AP group management.
- **Change AP Firmware**—Does not apply to System and AP group management.
- **Switchover Cluster**—Does not apply to System and AP group management.

Controller Network Services

- Syslog..... 117
- Short Message Service (SMS)..... 119
- Simple Mail Transfer Protocol (SMTP)..... 120
- Simple Network Management Protocol (SNMP)..... 120
- File Transfer Protocol (FTP)..... 123

Syslog

Configuring the Remote Syslog Server

The controller maintains an internal log file of current events and alarms, but this internal log file has a fixed capacity. Configure the log settings so you can keep copies of the logs that the controller generates.

At a certain point, the controller will start deleting the oldest entries in log file to make room for newer entries. If you want to keep a permanent record of all alarms and events that the controller generated, you can configure the controller to send the log contents to a syslog server on the network.

Follow these steps to configure the remote syslog server:

1. Go to **Administration > System Info > Syslog**.
2. Select the **Enable logging to remote syslog server** check box.
3. Configure the settings as explained in the following table.
4. Click **OK**.

TABLE 13 Syslog Server Configuration Settings

Field	Description	Your Action
Primary Syslog Server Address	Indicates the syslog server on the network.	<ol style="list-style-type: none"> a. Enter the server address. b. Enter the Port number. c. Choose the Protocol type. d. Click Ping Syslog Server. If the syslog server is reachable, a flashing green circle and the message Success appears after the button.
Secondary Syslog Server Address	Indicates the backup syslog server on the network, if any, in case the primary syslog server is unavailable.	<ol style="list-style-type: none"> a. Enter the server address. b. Enter the Port number. c. Choose the Protocol type. d. Click Ping Syslog Server. If the syslog server is reachable, a flashing green circle and the message Success appears after the button.

TABLE 13 Syslog Server Configuration Settings (continued)

Field	Description	Your Action
Application Logs Facility	Indicates the facility for application logs.	<ol style="list-style-type: none"> Select the option from the drop-down. Range: 0 through 7. Select one of the following Filter Severity: <ol style="list-style-type: none"> Emerg Alert Crit Error Warning Notice Info Debug: Default option
Administrator Activity Logs Facility	Indicates the facility for administrator logs.	<ol style="list-style-type: none"> Select the option from the drop-down. Range: 0 through 7. Select one of the following Filter Severity: <ol style="list-style-type: none"> Emerg Alert Crit Error Warning Notice Info Debug: Default option
Other Logs Filter Severity	Indicates the facility for comprehensive logs.	Select one of the following Filter Severity : <ol style="list-style-type: none"> Emerg Alert Crit Error Warning Notice Info Debug: Default option
Event Facility	Indicates the facility for event logs.	Select the option from the drop-down. Range: 0 through 7.
Event Filter	Indicates the type of event that must be sent to the syslog server.	Choose the required option: <ul style="list-style-type: none"> All events — Send all controller events to the syslog server. Allevntsexceptclientassociation/disassociationevents — Send all controller events (except client association and disassociation events) to the syslog server. All events above a severity — Send all controller events that are above the event severity to the syslog server.

TABLE 13 Syslog Server Configuration Settings (continued)

Field	Description	Your Action
Event Filter Severity applies to Event Filter > All events above a severity	Indicates the lowest severity level. Events above this severity level will be sent to the syslog server.	Select the option from the drop-down. a. Critical b. Major c. Minor d. Warning e. Informational f. Debug : Default option
Priority	Indicates the event severity to syslog priority mapping in the controller.	Choose the Syslog Priority among Error , Warning , Info and Debug , for the following event severities: <ul style="list-style-type: none"> ● Critical ● Major ● Minor ● Warning ● Informational ● Debug

Short Message Service (SMS)

Configuring the Short Message Service (SMS) Gateway Server

You can define the external gateway services used to distribute guest pass credentials to guests.

To configure an external SMS gateway for the controller follow the below steps.

1. Go to **Administrator > External Services > SMS**.
2. Select the **Enable Twilio SMS Server** check box to use an existing Twilio account for SMS delivery.
3. Enter the following Twilio Account Information:
 - **Server Name**, type the name of the server.
 - **Account SID**, type the account number.
 - **Auth Token**, type the token number to authenticate the external SMS gateway.
 - **From**, type the phone number from which the message must be sent.
4. Click **OK**.

You have completed adding an SMS gateway to the controller. You will receive a guest pass key from your Twilio Trial account.

Simple Mail Transfer Protocol (SMTP)

Configuring Simple Mail Transfer Protocol (SMTP) Server Settings

If you want to receive copies of the reports that the controller generates or to email guest passes to users, you need to configure the SMTP server settings and the email address from which the controller will send the reports.

Follow these steps to configure the SMTP server settings.

1. Go to **Administrator > External Services > SMTP**.
2. Select **Enable SMTP Server**.
3. Enter the **Logon Name** or user name provided by your ISP or mail administrator. This might be just the part of your email address before the @ symbol, or it might be your complete email address. If you are using a free email service (such as Hotmail™ or Gmail™), you typically have to type your complete email address.
4. Enter the associated **Password**.
5. For **SMTP Server Host**, enter the full name of the server provided by your ISP or mail administrator. Typically, the SMTP server name is in the format **smtp.company.com**.
6. For **SMTP Server Port**, enter the SMTP port number provided by your ISP or mail administrator. Often, the SMTP port number is **25** or **587**. The default SMTP port value is **25**.
7. For **Mail From**, enter the source email address from which the controller sends email notifications.
8. For **Mail To**, enter the recipient email address to which the controller sends alarm messages. You can send alarm messages to a single email address.
9. Select the **Encryption Options**, if your mail server uses encryption.
 - **TLS**
 - **STARTTLS**Check with your ISP or mail administrator for the correct encryption settings that you need to set.
10. Click **Test**, to verify if the SMTP server settings are correct. The test completed successfully form appears, click **OK**.
11. Click **OK**.

Simple Network Management Protocol (SNMP)

Enabling Global SNMP Notifications

The controller supports the Simple Network Management Protocol (SNMP v2 and v3), which allows you to query controller information, such as system status, AP list, etc., and to set a number of system settings using a Network Management System (NMS) or SNMP MIB browser.

You can also enable SNMP traps to receive immediate notifications for possible AP and system issues.

The procedure for enabling the internal SNMP agents depends on whether your network is using SNMPv2 or SNMPv3. SNMPv3 mainly provides security enhancements over the earlier version, and therefore requires you to enter authorization passwords and encryption settings, instead of simple clear text community strings.

Both SNMPv2 and SNMPv3 can be enabled at the same time. The SNMPv3 framework provides backward compatibility for SNMPv1 and SNMPv2c management applications so that existing management applications can still be used to manage the controller with SNMPv3 enabled.

Configuring SNMP v2 Agent

To configure SNMP v2 Agent settings:

1. Go to **Services > Others > AP SNMP Agent**. The **AP SNMP Profile** page is displayed.
2. To configure the SNMPv2 Agent, click **Create** and update the details as explained in the following table.

TABLE 14 SNMP v2 Agent Settings

Field	Description	Your Action
Name	Indicates the AP SNMP profile name.	Enter a name.
Description	Provides a brief explanation of the profile.	Enter a brief explanation.
Community	Indicates that applications which send SNMP Get-Requests to the controller (to retrieve information) will need to send this string along with the request before they will be allowed access.	Enter a name.
Privilege	Indicates the privileges granted to this community.	Select the required privileges: <ul style="list-style-type: none"> ● Read-Only—Privilege only to read. ● Read-Write—Privilege only to read and write. ● Notification—Privilege to: <ul style="list-style-type: none"> - Trap—Choose this option to send SNMP trap notification. - Inform—Choose this option to send SNMP notification. <ol style="list-style-type: none"> a. Enter the Target IP address. b. Enter the Target Port number. c. Click Add.

NOTE

You can also edit or delete an SNMPv2 agent. To do so, select the SNMPv2 agent from the list and click **Configure** or **Delete** respectively.

3. Click **OK**.

Configuring SNMP v3 Agent

1. Go to **Services > Others > AP SNMP Agent**.
2. To configure the SNMPv3 Agent, click **Create** and update the details as explained in the following table.

TABLE 15 SNMPv3 Agent Settings

Field	Description	Your Action
Name	Indicates the AP SNMP profile name.	Enter a name.
Description	Provides a brief explanation of the profile.	Enter a brief explanation.
User	Indicates that applications which send SNMP Get-Requests to the controller (to retrieve information) will need to send this string along with the request before they will be allowed access.	Enter a name.

TABLE 15 SNMPv3 Agent Settings (continued)

Field	Description	Your Action
Authentication	Indicates the authentication method.	<p>Choose the required option:</p> <ul style="list-style-type: none"> ● SHA—Secure Hash Algorithm, message hash function with 160-bit output. <ul style="list-style-type: none"> a. Enter the Auth Pass Phrase. b. Choose the Privacy option. <ul style="list-style-type: none"> - None: Use no privacy method. - DES: Data Encryption Standard, data block cipher. - AES: Advanced Encryption Standard, data block cipher. c. Enter a Privacy Phrase, 8 through 32 characters. ● MD5—Message-Digest algorithm 5, message hash function with 128-bit output. <ul style="list-style-type: none"> a. Enter the Auth Pass Phrase. b. Choose the Privacy option. <ul style="list-style-type: none"> - None: Use no privacy method. - DES: Data Encryption Standard, data block cipher. - AES: Advanced Encryption Standard, data block cipher. c. Enter a Privacy Phrase, 8 through 32 characters.
Privilege	Indicates the privileges granted to this community.	<p>Select the required privileges:</p> <ul style="list-style-type: none"> ● Read-Only—Privilege only to read. ● Read-Write—Privilege only to read and write. ● Notification—Privilege to: <ul style="list-style-type: none"> - Trap—Choose this option to send SNMP trap notification. - Inform—Choose this option to send SNMP notification. <ul style="list-style-type: none"> a. Enter the Target IP address. b. Enter the Target Port number. c. Click Add.

NOTE

You can also edit or delete an SNMPv3 agent. To do so, select the SNMPv3 agent from the list and click **Configure** or **Delete** respectively.

3. Click **OK**.

File Transfer Protocol (FTP)

Configuring File Transfer Protocol Server Settings

The controller enables you to automatically back up statistics files, reports, and system configuration backups to an external File Transfer Protocol (FTP) server.

However, before you can do this, you must add at least one FTP server to the controller.

Follow these steps to add an FTP server to which the controller will export data automatically:

1. Go to **Administrator > External Services > FTP**.
2. Click **Create**, the Create FTP Server from appears.
3. Enter an **FTP Name** that you want to assign to the FTP server that you are adding.
4. Select the required **Protocol**; **FTP** or **SFTP** (Secure FTP) protocol.
5. Enter the **FTP Host**, IP address of the FTP server.
6. Enter the **FTP Port**, number. The default FTP port number is 21.
7. Enter a **User Name** for the FTP account that you want to use.
8. Enter a **Password** that is associated with the FTP user name.
9. For **Remote Directory**, enter the remote FTP server path to which data will be exported from the controller. The path must start with a forward slash (/)
10. To verify that the FTP server settings and logon information are correct, click **Test**. If the server and logon settings are correct, a confirmation message stating, "**FTP server connection established successfully**" appears.
11. Click **OK**.

NOTE

You can edit or delete an existing FTP setting. To do so, select the FTP setting from the list and click **Configure** or **Delete** respectively.

Controller Certificates

- Importing SmartZone as Client Certificate..... 125
- Assigning Certificates to Services..... 126
- Generating Certificate Signing Request (CSR)..... 127
- Importing SmartZone (SZ) Trusted CA Certificates/Chains..... 128
- DataPlane validates SmartZone..... 129
- AP Validate SmartZone Controller..... 130
- ECDSA 3K..... 134

Importing SmartZone as Client Certificate

When you have an SSL certificate issued by the certificate provider, you can import it into the controller and use it for HTTPS communication.

To complete this procedure, you will need the following:

- The signed server certificate
- The intermediate CA certificate (at least one)
- The private key file

NOTE

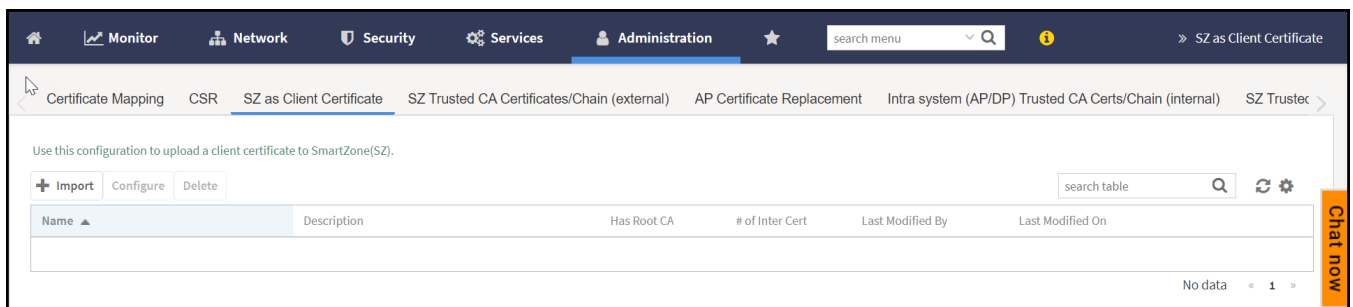
The file size of each signed certificate and intermediate certificate must not exceed 8192 bytes. If a certificate exceeds 8192 bytes, you will be unable to import it into the controller.

To import a signed server certificate, perform the following:

1. Copy the signed certificate file, intermediate CA certificate file, and private key file to a location (either on the local drive or a network share) that you can access from the controller web interface.
2. Click **Administration > System > Certificates > SZ as a Client Certificate**.

This displays **SZ as a Client Certificate** page.

FIGURE 76 SZ as Client Certificate



3. Click **Import**, this displays **Import Client Certificate** page.

FIGURE 77 Import client Certificate

Import Client Certificate

* Name:

Description:

Client Certificate

* Client Certificate: Browse Clear

Intermediate CA certificate: Browse Clear

Browse Clear

Browse Clear

Root CA certificate: Browse Clear

* Private Key: Browse Clear

Validate OK Cancel

4. Enter the following:
 - Name: Type a name to identify the certificate.
 - Description: Enter a short description about the certificate.
 - **Client Certificate:** To upload any of the options in this section, select the corresponding check box, click **Browse** and select the location in your local system and upload the certificate.

NOTE

For **Intermediate CA certificates**, if you want to upload additional intermediate CA certificates to establish a chain of trust to the signed certificate, you can select up to four certificates. Only CRT or PEM format is supported for the CA certificate.

NOTE

If you are using this SSL certificate for a Hotspot 2.0 configuration, you must also import a root CA certificate.

NOTE

Private Key can be imported through uploading file or using Customer Signing Request (CSR).

5. Click **OK**.

You can also edit, clone or delete the profile by selecting the options **Configure**, or **Delete** from the **SZ as Client Certificate** page.

Assigning Certificates to Services

You can map certificates to services

To specify the certificate that each secure service will use:

1. In the main menu, click **Administration**. Under **System** menu, hover mouse over the **Certificates** and select **Certificate Mapping**.

2. Select the certificate that you want to use for each of the following services:
 - **Management Web**—Used by Web UI and Public API traffic.
 - **AP Portal**—Used by Web Auth WLAN.
 - **Hotspot (WISPr)**—Used by WISPr WLAN control (Northbound Interface, Captive Portal, and Internal Subscriber Portal) traffic.
 - **Ruckus Intra-device Communication**—Used by AP control traffic.
3. To view the public key, click **View Public Key**, the Certificate Public Key form appears with the public key.
4. Click **OK**.

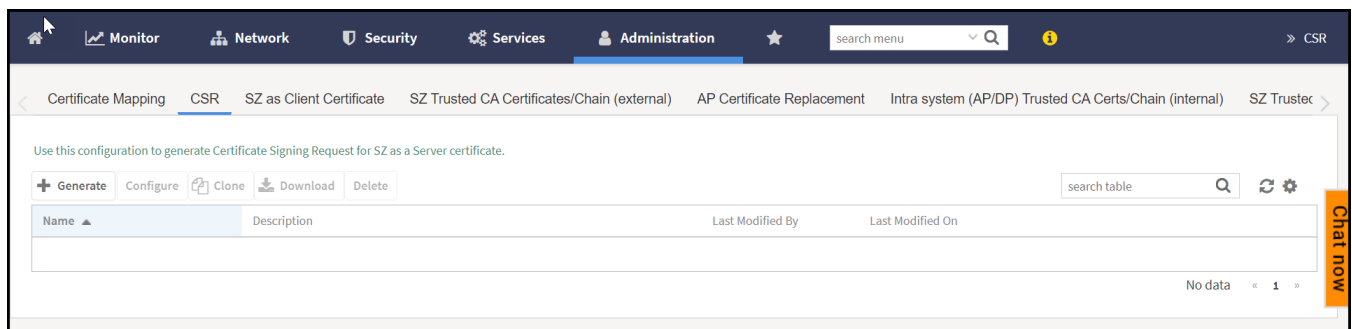
Generating Certificate Signing Request (CSR)

If you do not have an SSL certificate, you will need to create a Certificate Signing Request (CSR) file and send it to an SSL certificate provider to purchase an SSL certificate.

To create a CSR file:

1. Click **Administration > System > CSR**. This displays the Certificate Signing Request (CSR) page.

FIGURE 78 Certificate Signing Request (CSR)



2. Click **Generate**. This displays the **Generate CSR** form.
3. Enter the following:
 - **Name**: Type a name to identify the CSR.
 - **Description**: Enter a short description for this CSR.
 - **Common Name**: A fully qualified domain name of your web server. This must be an exact match (for example, **www.ruckuswireless.com**).
 - **Email**: An email address (for example, **joe@ruckuswireless.com**).
 - **Organization**: Complete legal name of your organization (for example, **Google, Inc.**). Do not abbreviate your organization name.
 - **Organization Unit**: Name of the division, department, or section in your organization that manages network security (for example, **Network Management**).
 - **Locality/City**: City where your organization is legally located (for example, **Sunnyvale**).
 - **State/Province**: State or province where your organization is legally located (for example, **California**). Do not abbreviate the state or province name.
4. Select the **Country**.

Controller Certificates

Importing SmartZone (SZ) Trusted CA Certificates/Chains

5. Click **OK**, the controller generates the certificate request. When the certificate request file is ready, web browser downloads the file automatically.
6. Go to the default download folder of your web browser and locate the certificate request file. The file name is **myreq.zip**.
7. Use a text editor (for example, Notepad) to open the certificate request file.
8. Go to the website of your preferred SSL certificate provider, and then follow the instructions for purchasing an SSL certificate.
9. When you are prompted for the certificate signing request, copy and paste the entire content of myreq.csr, and then complete the purchase.
10. After the SSL certificate provider approves your CSR, you will receive the signed certificate via email.
11. Copy the content of the signed certificate, and then paste it into a text file.
12. Save the file.

NOTE

You can also edit, clone, download or delete a CSR by selecting the options **Configure**, **Clone**, **Download** or **Delete** respectively.

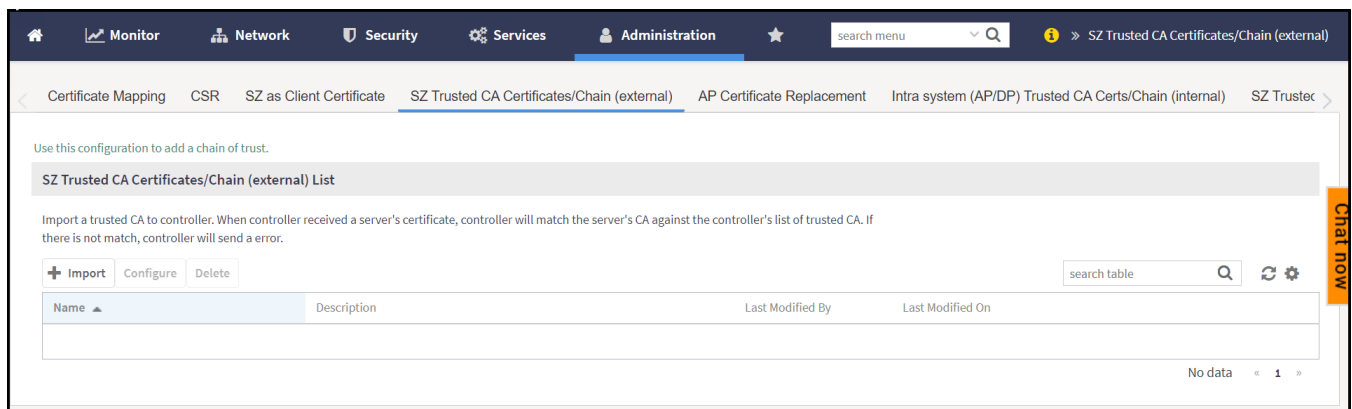
Importing SmartZone (SZ) Trusted CA Certificates/Chains

When a controller receives a server's certificate, it matches the server's CA against the list of trusted CAs it has. If there is no match, the controller sends an error.

To import a CA certificate, perform the following:

1. Click **Administration > System > Certificate** and select **SZ Trusted CA Certificates/Chain (external)**. This displays **SZ Trusted CA Certificates/Chain (external)** page.

FIGURE 79 SZ Trusted CA Certificates/Chains



2. Click **Import**. This displays the **Import CA Certs (Chain)** window.
3. Enter the following details:
 - a. **Name:** Type a name to identify the CA Certificate.
 - b. **Description:** Enter a short description for the CA Certificate.
 - c. **Intermediate CA Certificates:** Click **Browse** and select the file from your local system. If you need to upload multiple intermediate CA certificates to establish a chain of trust to the signed certificate, you can select up to four certificates.

- d. Root CA Certificate: Click **Browse** and select the file from your local system.
 - e. Click **OK** to add the newly imported certificate.
4. Click **OK**.

NOTE

You can also edit or delete a CA certificate by selecting the options **Configure** or **Delete** respectively.

NOTE

The controller does not support the CA certificate with p7b (windows format), only CRT or PEM format is supported. If the Certificates signed by CA chain has more than 5 chain length then you can upload only the Root CA of the certificate.

DataPlane validates SmartZone

DataPlane validates the incoming SmartZone certificate to check if the certificate is valid.

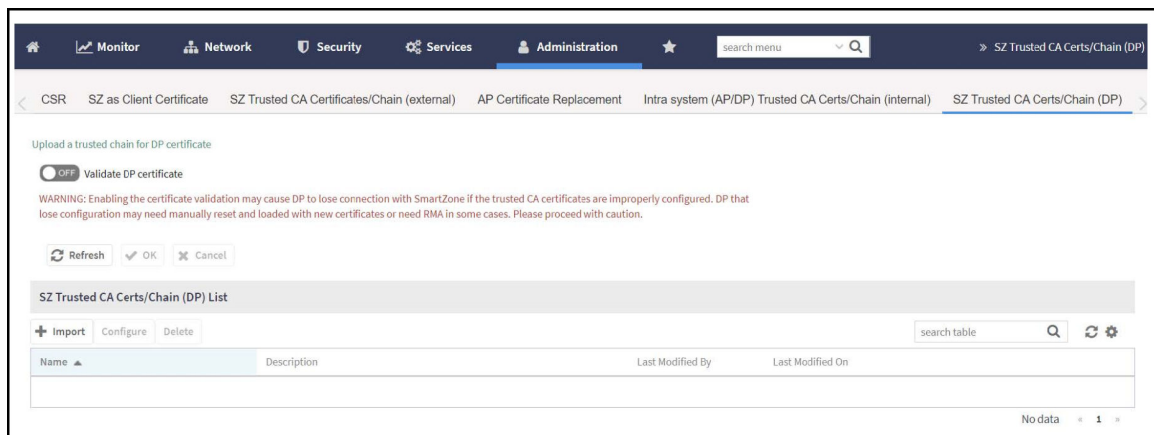
When the Dataplane discovers SmartZone for the first time, Dataplane validates if the SmartZone has the same certificate. If the certificates match then the connection is establishes otherwise it is terminated.

To upload the certificate, perform the below steps:

DataPlane Setup script

1. Import the DataPlane setup script and upload the certificate in SZone Trusted CACerts/Chain (DP).

FIGURE 80 Upload DataPlane Certificate

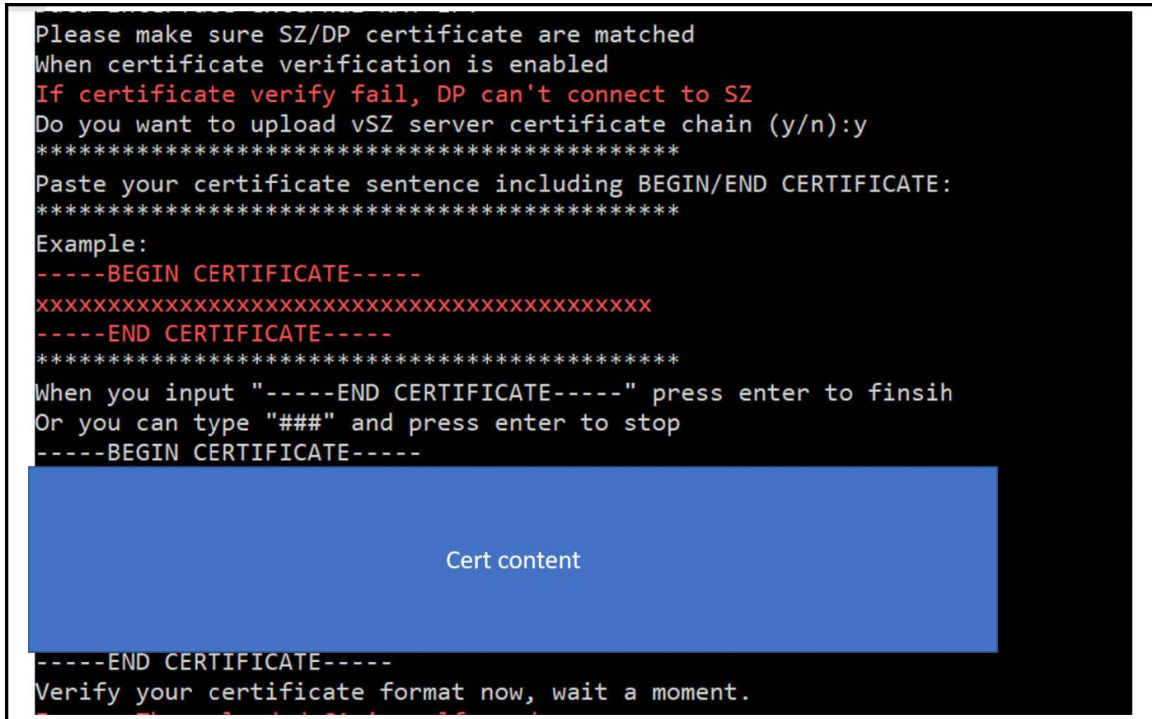


Controller Certificates

AP Validate SmartZone Controller

- Copy the entire trusted cert content including the "-----BEGIN CERTIFICATE-----" and "-----END CERTIFICATE-----".

FIGURE 81 Setup Upload Certificate



```
Please make sure SZ/DP certificate are matched
When certificate verification is enabled
If certificate verify fail, DP can't connect to SZ
Do you want to upload vSZ server certificate chain (y/n):y
*****
Paste your certificate sentence including BEGIN/END CERTIFICATE:
*****
Example:
-----BEGIN CERTIFICATE-----
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
-----END CERTIFICATE-----
*****
When you input "-----END CERTIFICATE-----" press enter to finish
Or you can type "###" and press enter to stop
-----BEGIN CERTIFICATE-----
Cert content
-----END CERTIFICATE-----
Verify your certificate format now, wait a moment.
```

- After the setup process, users should be able to enable the server validation via the DataPlane CLI.

The upload command is `enable->config->controller->set_trust_chain`

- For vDP the upload command is `show dp_root_ca`. The root CA is generated in the location `/etc/dp_config/discover` and use this root CA to sign a client cert for vDP TLS connection.
- For physical DP, it should use the MIC cert to do TLS connection. The certificate should pass the validation with Ruckus root CA.

AP Validate SmartZone Controller

Access Point (AP) can validate the SZ by SZ's Public Key or trusted certificates.

Smart Zone can edit the Domain name after the installation

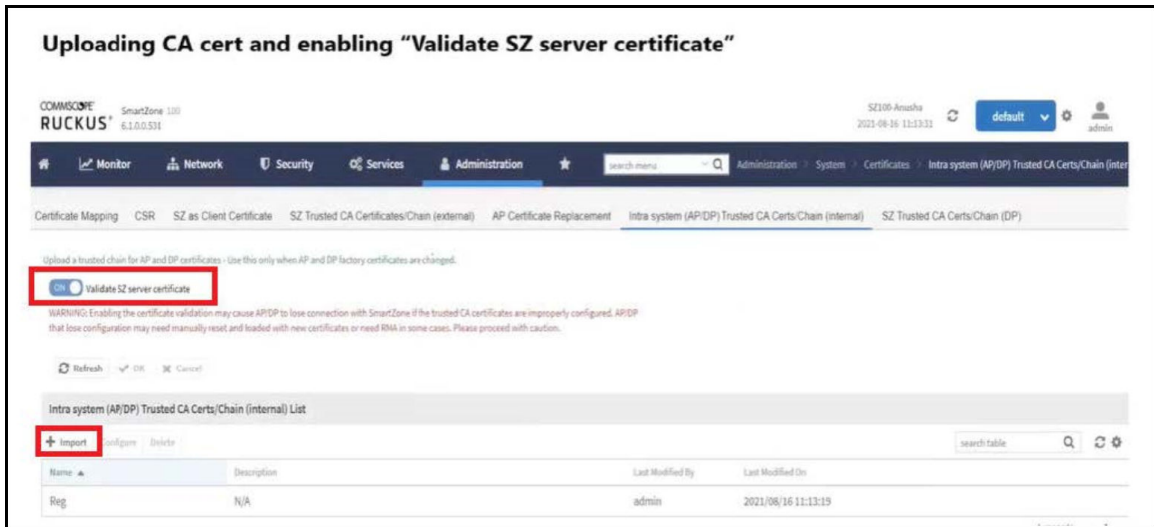
Smart Zone can show the Infra (Communicator) certificate's pem data.

When Server validation is enabled, SZ will push the configurations to AP.

Follow the below steps for the validation of server certificates:

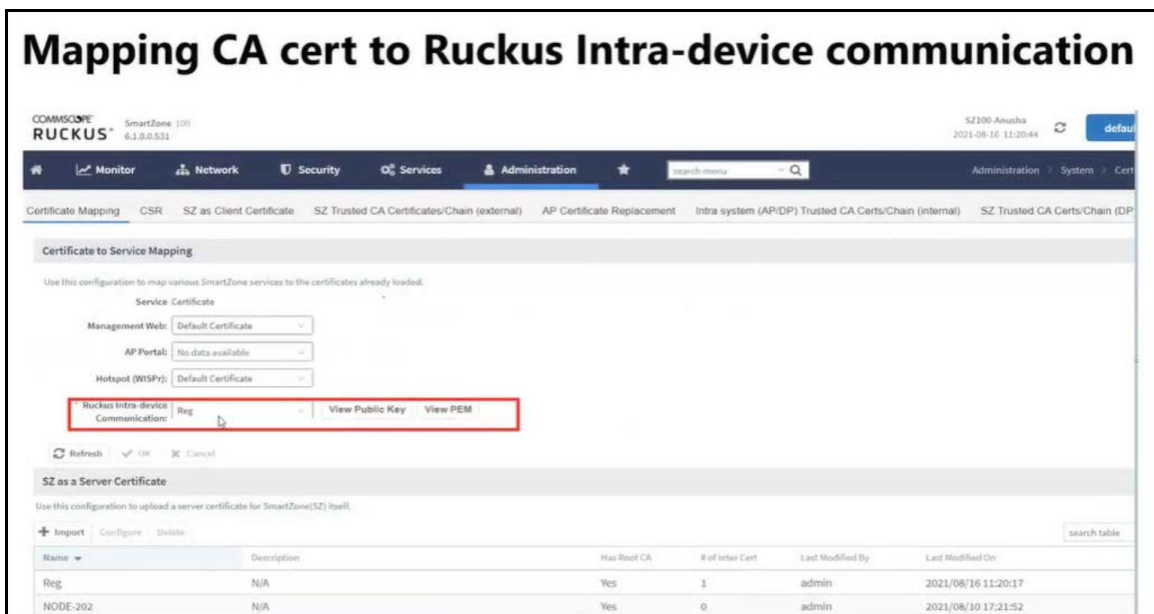
- Go to **Administration > Intra System (AP/DP) Trusted Certs/Chain (Internal)**.

FIGURE 82 SZ Certificate Validation



2. Click "Import" to add valid trusted CA certificate/chain as per the figure above.
3. Enable the "Validate Server certificate".
4. The configuration will be pushed to SCG managed AP's.
5. Upload the certificate in the **Administration>Certificate Mapping> SZ as a Certificate**.
6. Map Server certificate to Ruckus Intra-Device Communication also change the below heading from Mapping CA Cert to Mapping Server Certificate.

FIGURE 83 Mapping CA Certificate



Controller Certificates

AP Validate SmartZone Controller

- The certificate will be validated when AP connects to SCG.
- Configuration Method:

Part 1: Using Public Key

The certificate mapping is done in Administration>System>Certificates> Certificate Mapping.

- Copy the public key from the above marked "View Public key", Enter the Public key in AP CLI using command " set scg pubkey <publickey> ".
- Enable the server cert validation in AP using command "set scg server-validate enable".
- If public key matches The AP will be listed in staging zone.

Success message : ssl_cert_verify_callback:294 SSL Verification OK.

In Ap CLI execute command "get scg ".

```
SCG gwloss|serverloss timeouts: 1800|7200
Controller Cert Validation : enable
Controller Cert Validation Result: success
-----
OK
rksccli: █
```

- If public key is not matching error message,
In Ap CLI execute command "get scg ".

```
Controller Cert Validation : enable
Controller Cert Validation Result: failed
-----
```

SSL certificate verification failed.

ERROR: check_http_status:542 Curl error: Peer certificate cannot be authenticated with given CA certificates."

Part 2: Using CA Cert

- In AP CLI configure ca cert using command "set scg trusted-cert ".


```

rkscli: set scg trusted-cert
*****
Paste your certificate sentence including BEGIN/END CERTIFICATE:
Example:
-----BEGIN CERTIFICATE-----
XXXXXXXXXXXXXXXXXXXX
-----END CERTIFICATE-----
*****
When you complete all certificate, please type press "CERT-DONE" to finish
Or you can type "###" and press enter to stop
-----BEGIN CERTIFICATE-----
MIIEjzCAvegAwIBAgIJA0iIFySsSakQMA0GCSqGSIb3DQEBAUAMF4xCzAJBgNV
BAYTAKlOMQwwCgYDVQQIDANLQVIXDTALBgNVBACMBEJscmUxDzANBgNVBAoMB1J1
Y2t1c2EPMA0GA1UECwwGUnVja3VzMRAdDgYDVQDDAadyb290X2NhMB4XDITxMDky
MzEwMTYwMVVoXDTM2MDkxOTEmTYwMVowXjELMAKGA1UEBhMCSU4xDDAKBgNVBAgM
A0tBUjENMA5GA1UEBwwE0mxyZTEPMA0GA1UECgwGUnVja3VzMQ8wDQYDVQQLDAZS
dWNrdXMxEDA0BgNVBAMMB3Jvb3RfY2EwggGIMA0GCSqGSIb3DQEBAQUAA4IBjwAw
ggGKAoIBGQCaNqu0eTLT6Fpa1slxSKeMIJiaaFDJ7AiqhBA7RG5fjZ51zCpicKhJ
AiofLaU+LLQiasLHcejtmR25M9PK6LjLXkxi7tuV6QEKl/xIqIFZzi3K0LGvv9i
p/NaugBIFcGhrJSBw1ch3JOM0TbWT0HFBWeldiF47aqKNqbteUyMQG1JaXoqCzI
hGQudV5a5lFlSaCREwdfayzQ6LeeBsYust4YzeeFD1WIW3iJGfZnZQdeIR9vhtT
jimTMUMnRp1D00T5TA+zFbFwM7kkh6W6cdeFqGzxvk3NT2TiyXfSmVf5ZdJD070L
CE1+fVWAagNzMja9S6G2WtAZmddQR0HRlpfr+zyNS9qj40nFKz6/Tw84kk5kgJu
bgAweu4TJnBc5Kie0c99VWZ2d3FtUbvE3wL3ewhA+YpQ2nh8+m0tdWnCBuKpSx5J
01MjgHusUzIZ3zy+TEg41coHdwZRAz7oR+vh6o+QCGcjVDlq9N4oyVYHpPjPOGfm
fyIlxIC9JgcCAwEAAANQME4wHQYDVR00BBYEFDWSRJdz750MD72vqijxyZ8im2HB
MB8GA1UdIwQYMBaAFDWSRJdz750MD72vqijxyZ8im2HBMAwGA1UdEwQFMAMBAf8w
DQYJKoZIhvcNAQEMBQADggGBAFhXn18/TGfSZUsE0tZ6vNtGThVGIzon8d8aESVG
0g0//le/f0nXmZP2dvmVbStckOUKvAkURxzULVe5d8mxKMYiTwoVGkN+pkllFMn4
chYa2cJ08pCeysHiIdT9RtygvP62CBjppq+a8YjsKXPgiHY0nW0dUKjUJ+z6hg0K
fqtXc8q3ePdu09GJm+ws7K/+CxKW5DKQdLyL/Ew7LfyA2j7ogdXqYmlWbDSzxtFE
3bymmmIx9Lty7Uhn4DoB107yDMoL3Z5rYUzyd3igPpf2GD71arhfGkKwCBu04cHgcg
QhCnwatXfXN4Ntb0RU4bvDvxvHCh86LF1LmigrZjRuAyAZn25LdicsffEXWTtChv
2c6B0TQvuucdsIB5K00h1QLsbRmoksMi7BgTVj1Fd1/uAUKS31W/IzaVCNb8Sw1L
gardUR401pXe0MXACR2x1U8CLzC199eFLfK//om7drVnBCR0BgQJy3E0Q6XcP4r
FJncWkB8bvtgt6tQdd7YXa+VsQ==
-----END CERTIFICATE-----
"CERT-DONE"
Set SZ public key/cert done
OK
rkscli: █

```

- Enable the server cert validation in AP using command “set scg server-validate enable”.
- If CA certificate is validated the AP will be listed in staging zone.

9. Domain name configuration:

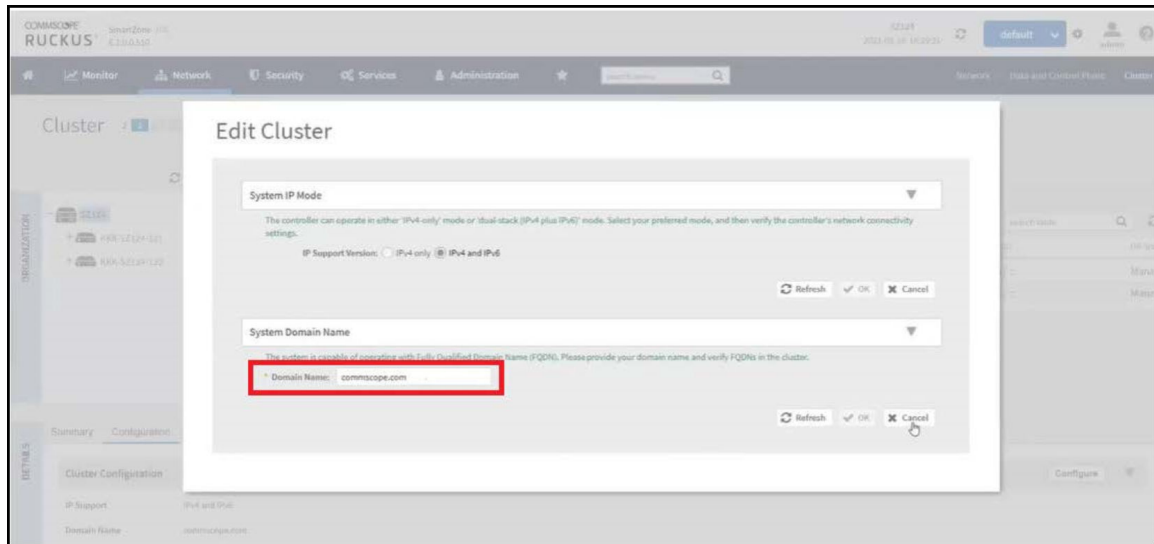
For release 6.1 fresh installation of domain name is mandatory to support AP/DP validate the controller feature. FQDN (Fully Qualified Domain Name) consists of domain name and the host name. The below table is an example of cluster deployment based on the domain name in a cluster deployment.

TABLE 16 Cluster Deployment

Cluster Domain Name	Node#	Host Name	FQDN
ruckus.com	Master	Master	master.ruckus.com
	Slave1	Slave1	slave1.ruckus.com
	Slave2	Slave2	slave2.ruckus.com
	Slave3	Slave3	slave3.ruckus.com

Domain name can be modified after installation by navigating to **Network > Data and control Plane > Cluster > Select the cluster > Configuration > Configure**.

FIGURE 84 Edit Cluster



ECDSA 3K

Elliptic Curve Digital Signature Algorithm (ECDSA) Certificate and Keys Support

The ECDSA is a digital signature algorithm which uses keys derived from elliptic curve cryptography.

The SmartZone provides an option to disable/enable the ECDSA certification on a per-zone basis. The APs in the zone with ECDSA certificate enabled receives an additional controller-signed certificate from the SmartZone. The 2K MIC (Manufacturer Installed Certificates) on the APs is still used as the trust anchor for the SmartZone. The 2K MIC and corresponding key (2k length) remains untouched, backward compatibility of the zone only allows 2K certificate/key.

The SmartZone managed APs issue ECDSA signed certificates which are valid only among the same SmartZone cluster nodes.

The ECDSA is faster than RSA in key generation and signing operations. Signature algorithms are used in TLS handshake and SSH authentication.

Cloud Computing Compliance Criteria Catalogue - BSI C5

The C5 catalogue specifies minimum requirements for secure cloud computing.

By adhering the BSI C5 requirements and guidelines, RUCKUS AP provides a secure, reliable, and trustworthy communication environment.

The following are the secure features in AP and SmartZone:

- Uses a stronger certificate and key in both client and server authentication.
- Removes weak ciphers and algorithms.
- Replaces DropbearSSH to OpenSSH on AP.

Configuring ECDSA and Keys at Zone Level

To configure ECDSA certificates, enable the **SSH/TLS Key Enhance Mode**.

By default, the **SSH/TLS Key Enhance Mode** is disabled.

This configuration is available only with new installation and upgraded versions of the Access Points. The ECDSA certificates are available only after enabling the **SSH/TLS Key Enhance Mode**. To generate and share the ECDSA certificates, AP should join and be a part of this zone.

To enable **SSH/TLS Key Enhance Mode** at the zone level, perform the following:

1. Click **Network > Wireless > Access Points**
This displays the **Access Points** page.
2. In the system tree, click **Create Domain/Zone/Group (+)** icon.
This displays the **Create Zone** page.

3. In the **Create Zone** page, navigate to **General Options** section and enable the **SSH/TLS Key Enhance Mode**.

FIGURE 85 SSH/TLS Key Enhance Mode

The screenshot shows the 'Create Zone' configuration interface. The 'General Options' section is expanded, displaying various settings. The 'SSH/TLS Key Enhance Mode' checkbox is circled in red and is currently set to 'OFF'. Other visible settings include AP Firmware (6.1.2.0.895), Country Code (United States), Location (example: Ruckus HQ), Location Additional Information (example: 350 W Java Dr, Sunnyvale, CA, USA), GPS Coordinates (Latitude, Longitude, Altitude), AP Admin Logon (Logon ID, Password), AP Time Zone (System defined, User defined), AP IP Mode (IPv4 only, IPv6 only, Dual), Historical Connection Failures (OFF), DP Group (Default DP Group), and SSH Tunnel Encryption (AES 128, AES 256). The 'Mesh Options' section is partially visible at the bottom.

After enabling the **SSH/TLS Key Enhance Mode**, navigate to **Administration > System > Certificates > Certificate Mapping** to map the server's ECDSA certificates.

Mapping Server ECDSA Certificates

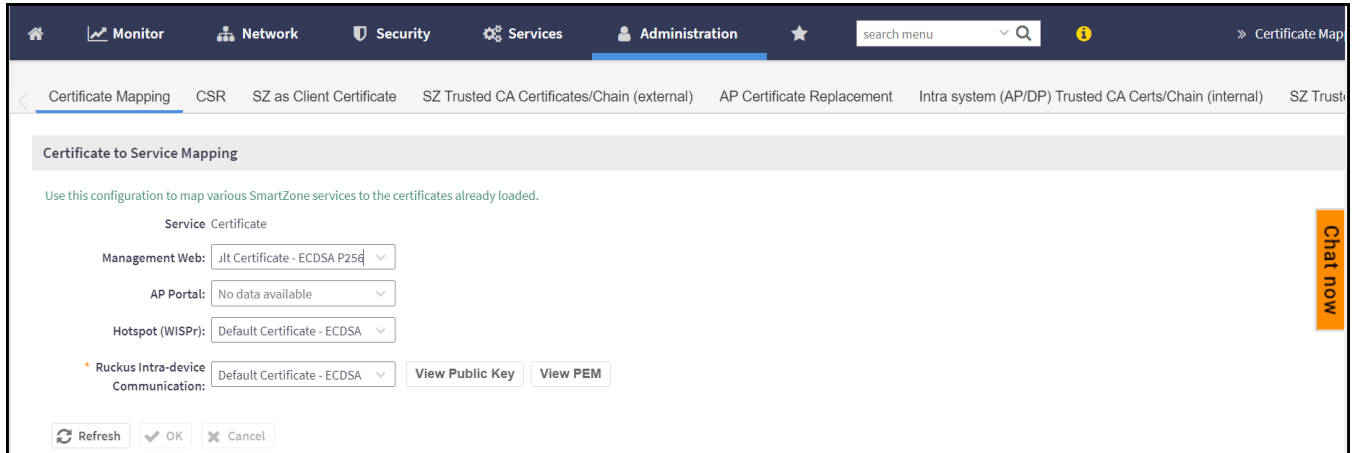
After enabling the **SSH/TLS Key Enhance Mode** at the zone level. You can map the ECDSA certificates to SmartZone (server certificate). This mapping ensures that SmartZone (server) is using 2K/3K RSA or ECDSA certificates during the TLS handshake.

To map the ECDSA certificates, perform the following:

1. Click **Administration > System > Certificates > Certificate Mapping**.

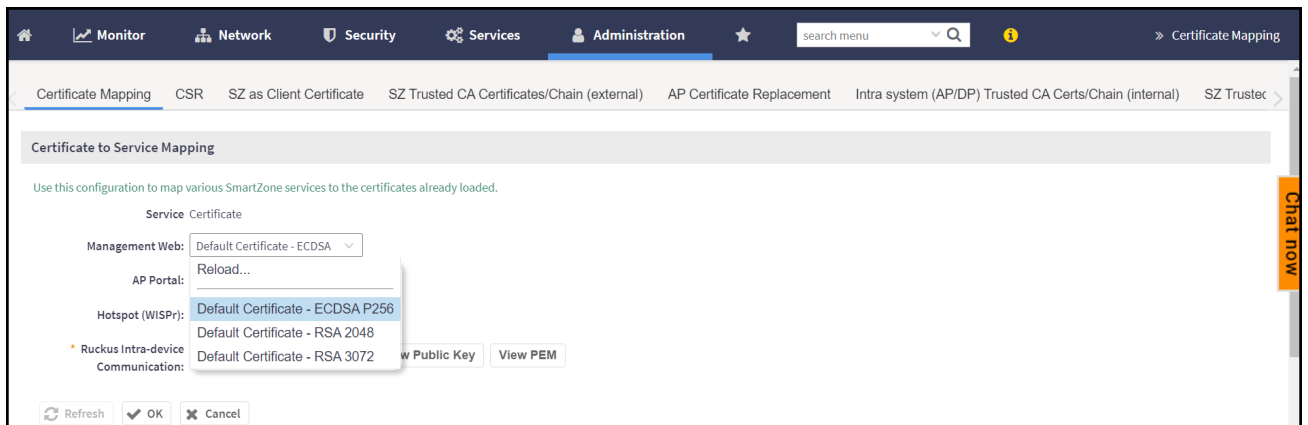
This displays **Certificate Mapping** page.

FIGURE 86 Certificate Mapping



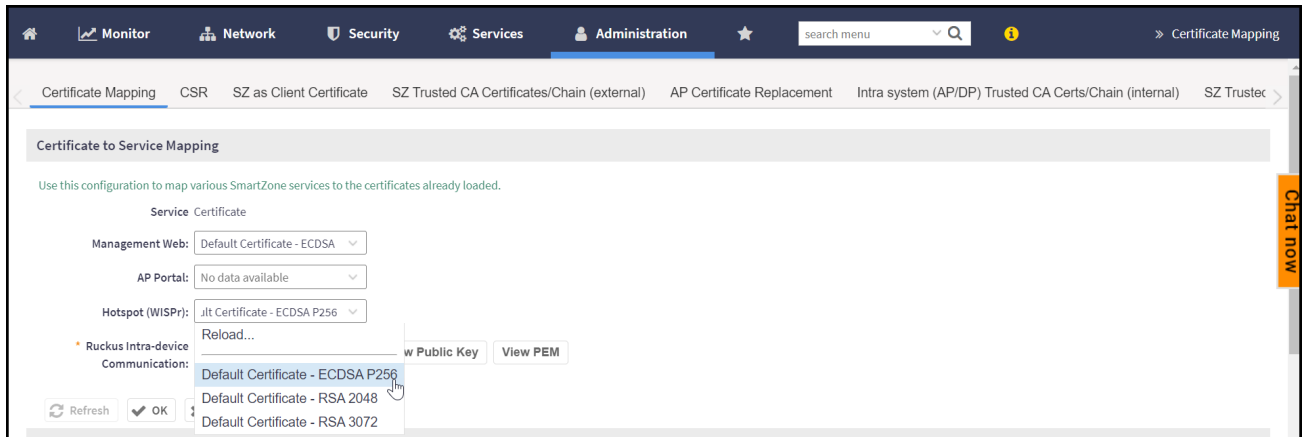
- **Management Web:** SmartZone uses 2K/3K based certificates to map the services when user access SmartZone user interface via web browser.

FIGURE 87 Management Web



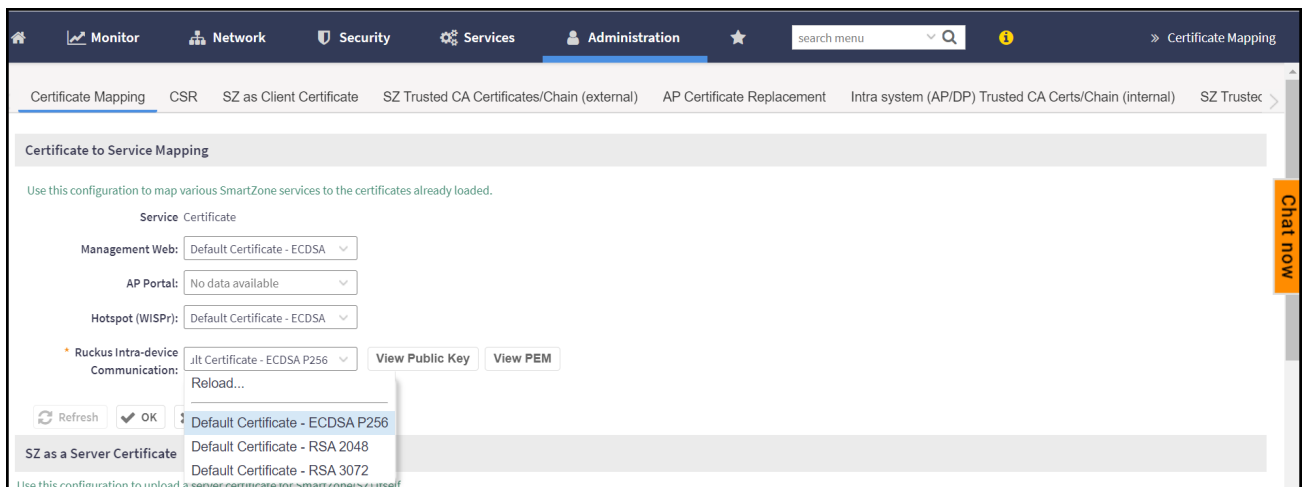
- **Hotspot (WISPr):** SmartZone re-directs the login portal to connected user (via web browser) for authentication.

FIGURE 88 Hotspot (WISPr)



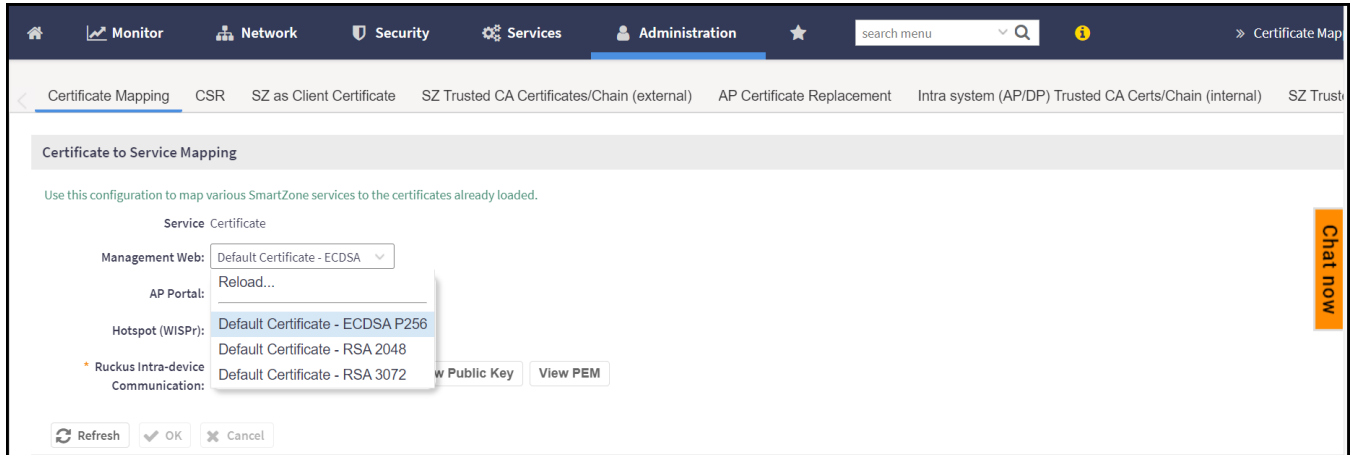
- **Ruckus Intra-device Communications:** SmartZone uses 2K/3K based certificates to map the services when AP/ICX joins the SSH/TLS Key Enhance Mode enabled zone/switch group.

FIGURE 89 Ruckus Intra-device Communication



2. You view the new ECDSA certificates in the **Certificate to Service Mapping** section.

FIGURE 90 ECDSA Certificates



3. Click the drop-down menu and select the pre-loaded certificate to map various SmartZone services.
 - **ECDSA P256**: This supports the signing of data with Elliptic Curve methods. The signing and verification is performed using P256 method. The calculation is hash of the message (h), public key (QA) and private key (dA).
 - **RSA 2048**: This is an asymmetric encryption. Each side has a public and private key. The default 2K certificate is renamed as RSA 2048.
 - **RSA 3072**: This is again an asymmetric encryption. RSA can work with keys of different keys of length.
4. Select the certificates and click **OK** and the settings are mapped to various SmartZone services.

Enabling ECDSA Certificates Support for RADIUS with Transport Layer Security (TLS)

Transport Layer Security (TLS) encrypts communication between a client and server.

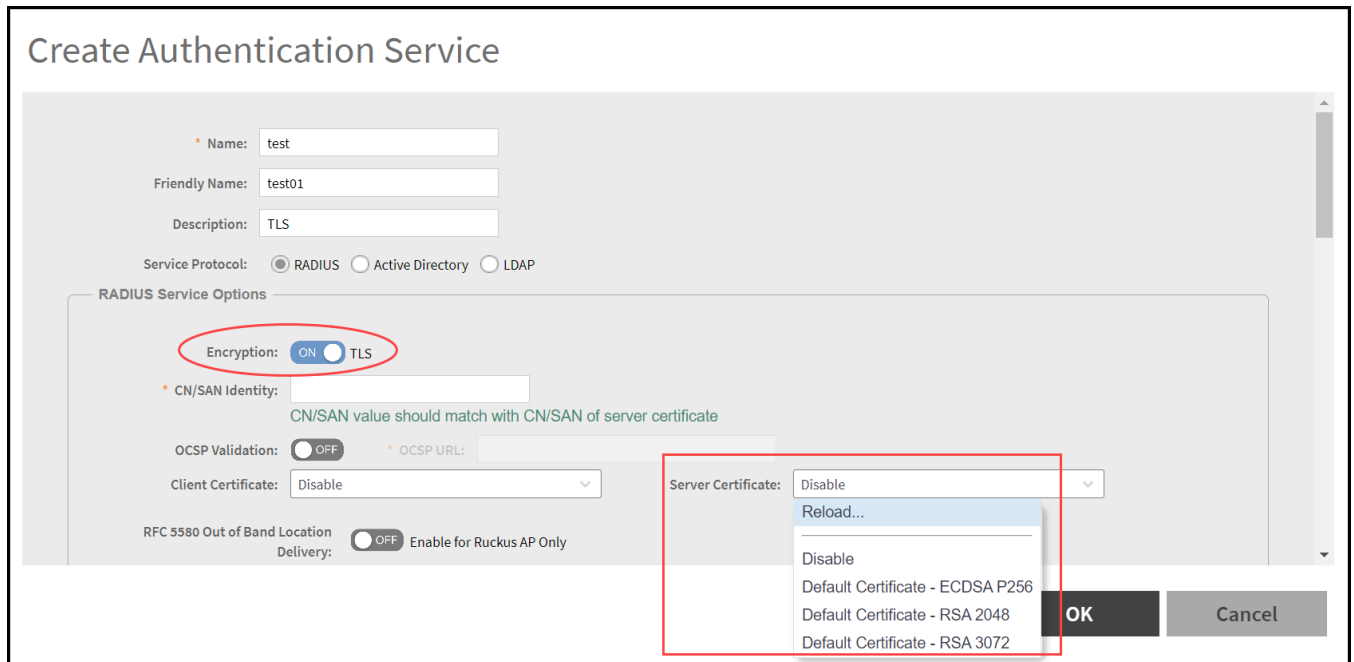
To enable TLS encryption from **Proxy (SZ Authenticator)**, perform the following:

1. Click **Security > Authentication > Proxy (SZ Authenticator)**.
This displays the **Proxy (SZ Authenticator)** page.
2. In the **Proxy (SZ Authenticator)**, click **Create**.
This displays **Create Authentication Service** page.

3. Navigate to **RADIUS Service Options** and enable **Encryption TLS**.

The ECDSA certificates are enabled for RADIUS server.

FIGURE 91 Encryption TLS_Authentication Service



To enable TLS encryption from **Proxy**, perform the following:

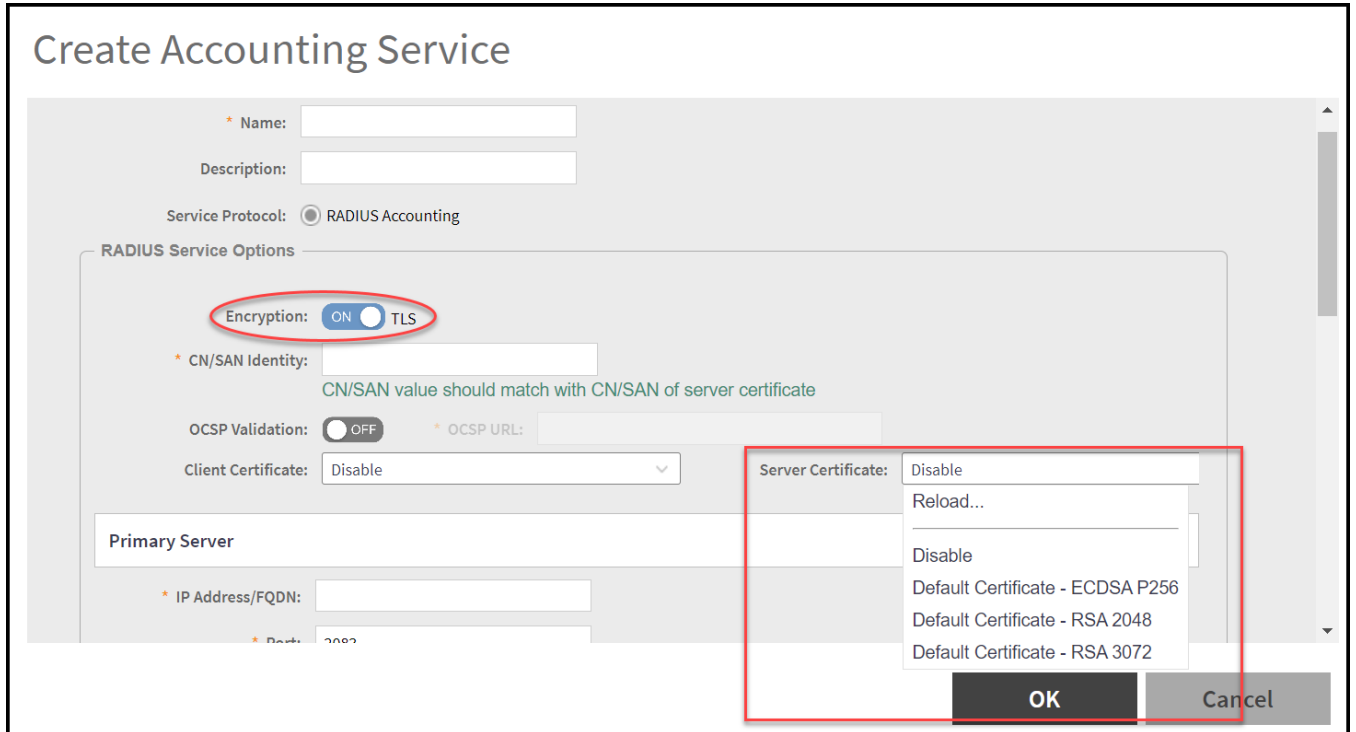
1. Click **Security > Accounting > Proxy**.
This displays **Proxy** page.
2. In the **Proxy**, click **Create**.
This displays the **Create Accounting Service** page.
3. Navigate to **RADIUS Service Options** and enable **Encryption TLS**.

The ECDSA certificates are enabled for RADIUS server.

NOTE

The ECDSA certificates is available only for RADIUS service protocol option.

FIGURE 92 Encryption TLS_Accounting Service



External Services

- Location Services..... 143
- Mobile Virtual Network Operator (MVNO)..... 145
- Northbound Data Streaming..... 147
- RUCKUS Cloud Services..... 149

Location Services

If your organization purchased the RUCKUS Smart Positioning Technology (SPoT) location service, the controller must be configured with the venue information that is displayed in the SPoT Administration Portal.

After completing purchase of the SPoT location service, you will be given account login information that you can use to log in to the SPoT Administration Portal. The SPoT Administration Portal provides tools for configuring and managing all of your venues (the physical locations in which SPoT service is deployed). After a venue is successfully set up, you must enter the same venue information in the controller.

1. From the main menu, go to **Administration > External Services > Ruckus Service > Ruckus Location Services (SPoT)**.

The **Ruckus Location Services (SPoT)** tab is displayed.

2. Click **Create**.

The **Create LBS Server** dialog box is displayed.

FIGURE 93 Creating a Location-Based Server

The screenshot shows a dialog box titled "Create LBS Server". It contains the following fields and controls:

- Venue Name:** A text input field.
- Server Address:** A text input field.
- Port:** A text input field containing the value "8883".
- Password:** A text input field.
- TLS Version:** A dropdown menu with "tlsv1.2" selected.
- Buttons:** "OK" and "Cancel" buttons at the bottom.

3. In the **Venue Name** field, type the venue name for the server.
4. In the **Server Address** field, type the server IP address.

NOTE

The server address must be entered in IPv4 address format. The LBS server does not support configuration of IPv6 addresses.

5. In the **Port** field, type the port number to communicate with the server.

NOTE

The default port number is 8883.

6. In the **Password** field, type the password to access the server.
7. From the **TLS Version** list, select the TLS version.

8. Click **OK**.

NOTE

You can also edit, clone, and delete the location-based services by selecting the **Configure**, **Clone**, and **Delete** options respectively from the **Ruckus Location Services (SPoT)** tab.

NOTE

The connection between the controller and vSPoT is an outbound connection, so it depends on the destination IP address. If the destination IP address falls in the subnet of one interface, it is routed to that interface. Otherwise, it is routed through the default route.

Mobile Virtual Network Operator (MVNO)

Managing Mobile Virtual Network Operator (MVNO) Accounts

A Mobile Virtual Network Operator (MVNO) uses a host carrier network to service its mobile users. An MVNO account is created for each operator and the MVNO page lists the accounts that are created.

1. Go to **Administration > Administration > MVNO**.

The **MVNO** page appears displaying information about MVNO accounts created.

2. Click **Create** to create an MVNO account.

The **The Mobile Virtual Network Operator** page appears.

External Services

Mobile Virtual Network Operator (MVNO)

3. Configure the following:

a. The Mobile Virtual Network Operator Summary

1. Domain Name: Type a domain name to which this account will be assigned
2. Description: Type a brief description about this domain name.

b. AP Zones of Mobile Virtual Network Operator: Displays the AP zones that are allocated to this MVNO account

1. Click **Add AP Zone**. The **Add AP Zone** page appears.
2. AP Zone: Select the AP zone you want to add to the MVNO account from the drop-down menu.
3. Click **OK**.

NOTE

You can only select a single AP zone at a time. If you want to grant the MVNO account management privileges to multiple AP zones, select them one at time.

c. WLAN Services: Configure the WLAN services to which the MVNO account that you are creating will have management privileges.

1. Click **Add WLAN**. The **Add WLAN** page appears.
2. SSID: Select the WLAN to which the MVNO account will have management privileges.

NOTE

You can only select one WLAN service at a time. If you want to grant the MVNO account management privileges to multiple WLAN service zones, select them one at time.

3. Click **OK**.

d. Super Administrator: Configure and define the logon details and management capabilities that will be assigned to the account.

1. Account Name: Type the name that this MVNO will use to log on to the controller.
2. Real Name: Type the actual name (for example, John Smith) of the MVNO.
3. Password: Type the password that this MVNO will use (in conjunction with the Account Name) to log on to the controller.
4. Confirm Password: Type the same password as above. f) In Phone, type the phone number of this MVNO.
5. Phone: Type the phone number of the administrator.
6. Email: Type the email address of this MVNO.
7. Job Title: Type the job title or position of this MVNO in his organization.

e. RADIUS Server for Administrator Authorization and Authentication: See [Configuring SmartZone Admin AAA Servers](#) on page 63 for more information.

4. Click **OK**.

You have created an MVNO account.

NOTE

You can also edit and delete the account by selecting the options **Configure**, and **Delete** respectively, from the **MVNO** page.

Northbound Data Streaming

SmartCell Insight (SCI) and other third-party Google Protocol Buffers (GPB) listeners use data from the controller to analyze performance and generate reports about the Wi-Fi network.

Configuring Northbound Data Streaming Settings

Configuring the Northbound Data Streaming settings in the controller enables data transfer from the controller to the Northbound Data Streaming server using the Message Queuing Telemetry Transport (MQTT) protocol.

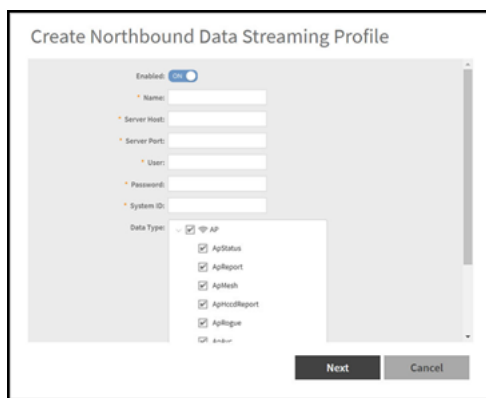
NOTE

You can create a maximum of two SCI profiles simultaneously.

Complete the following steps to configure the Northbound Data Streaming server settings.

1. From the main menu, go to **Administrator > External Services > Northbound Data Streaming**.
2. Click **Create**. The **Create Northbound Data Streaming Profile** dialog box is displayed.

FIGURE 94 Creating a Northbound Data Streaming Profile



3. Complete the following options:
 - **Enabled:** Set to **ON** to configure the Northbound Data Streaming profile.
 - **Name:** Enter the profile name.
 - **Server Host:** Enter the IP address of the Northbound Data Streaming host server.

NOTE

An SCI profile supports only the IPv4 format.

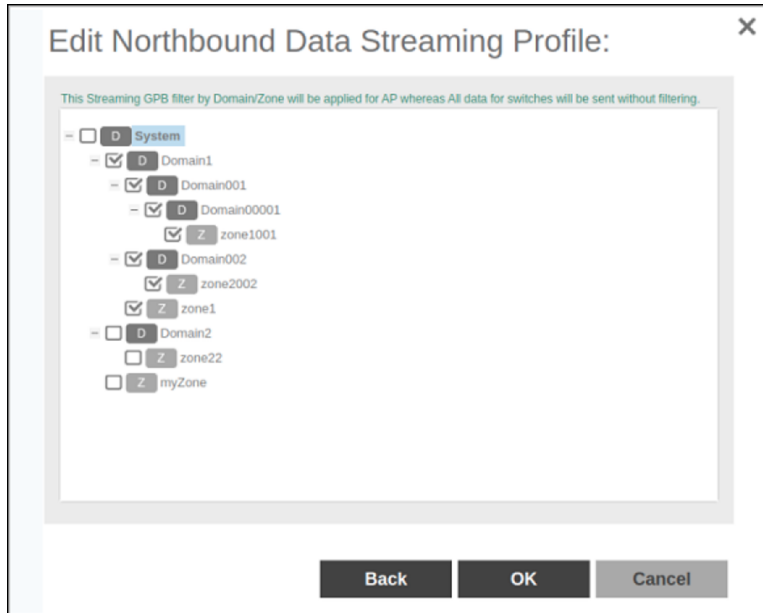
- **Server Port:** Enter the port number using which the Northbound Data Streaming server and the controller can communicate and transfer data. The ports must be allowed on the firewall.
 - **User:** Enter the name of the user.
 - **Password:** Enter the password for the user.
 - **System ID:** Enter the ID of the Northbound Data Streaming system to access.
 - **Data Type:** Select the required options for the specific data types that must be sent to the Northbound Data Streaming server from the SCI server.
4. Click **Next**.

External Services

Northbound Data Streaming

- For APs, from the **System** tree, select the required domain or zone to send KPIs or statistics to the Northbound Data Streaming server. For switches, KPIs or the statistics are sent to SCI or Northbound Data Streaming server without filtering.

FIGURE 95 Selecting the Zone or Domain



- Click **OK**.

The Northbound Data Streaming profile is listed on the Northbound Data Streaming page.

The **Status** column displays the current connection status of the SCI profile.

NOTE

You can also edit or delete a Northbound Data Streaming profile by selecting the Northbound Data Streaming profile and clicking the **Configure** or **Delete** option.

Setting the Northbound Portal Password

Third-party applications use the northbound portal interface to authenticate users and retrieve user information during the user equipment (UE) association.

Complete the following steps to configure the northbound portal interface.

- From the main menu, go to **Administrator > External Services > WISPr Northbound Interface**.
- Set to **ON** to enable the **Enable Northbound Portal Interface Support**.
- For **User Name**, enter the name of the user.
- For **Password**, enter the password of the user.
- Click **OK**.

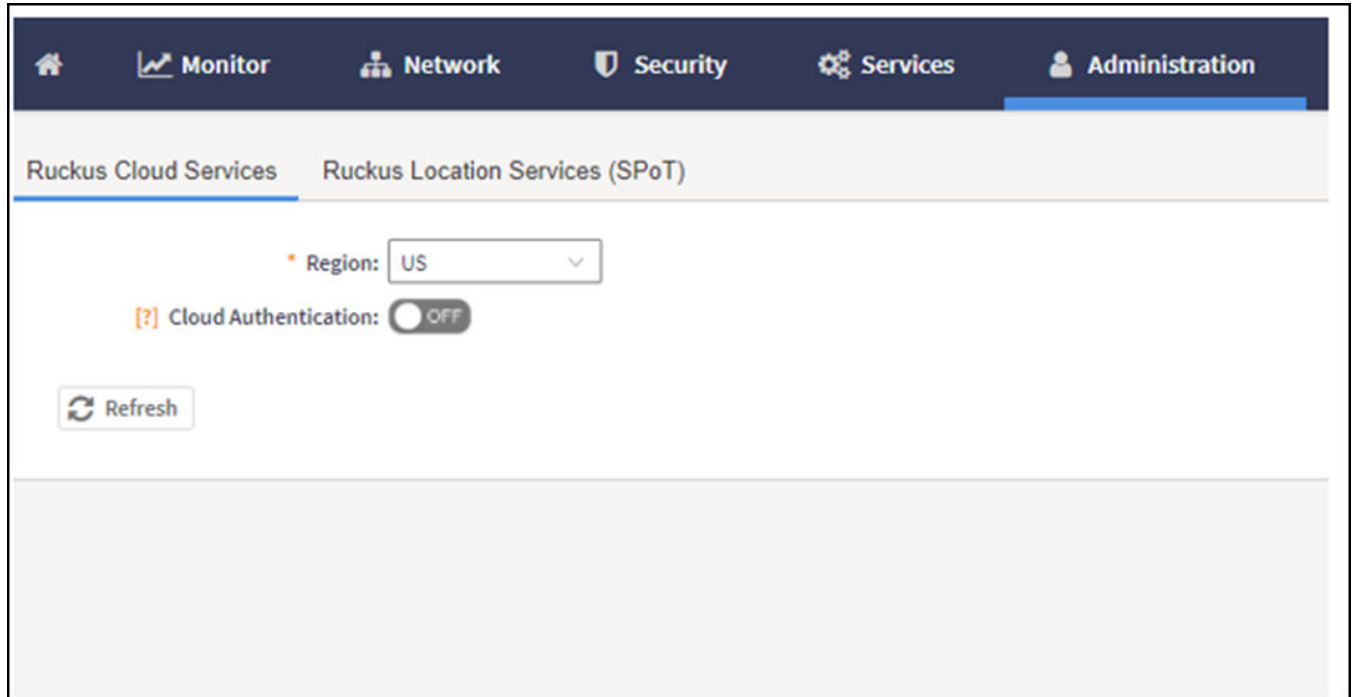
RUCKUS Cloud Services

Complete the following steps to enable cloud analytics on SmartZone.

1. From the main menu, go to **Administration** > **External Services** > **Ruckus Services**, and select **Ruckus Cloud Services**.

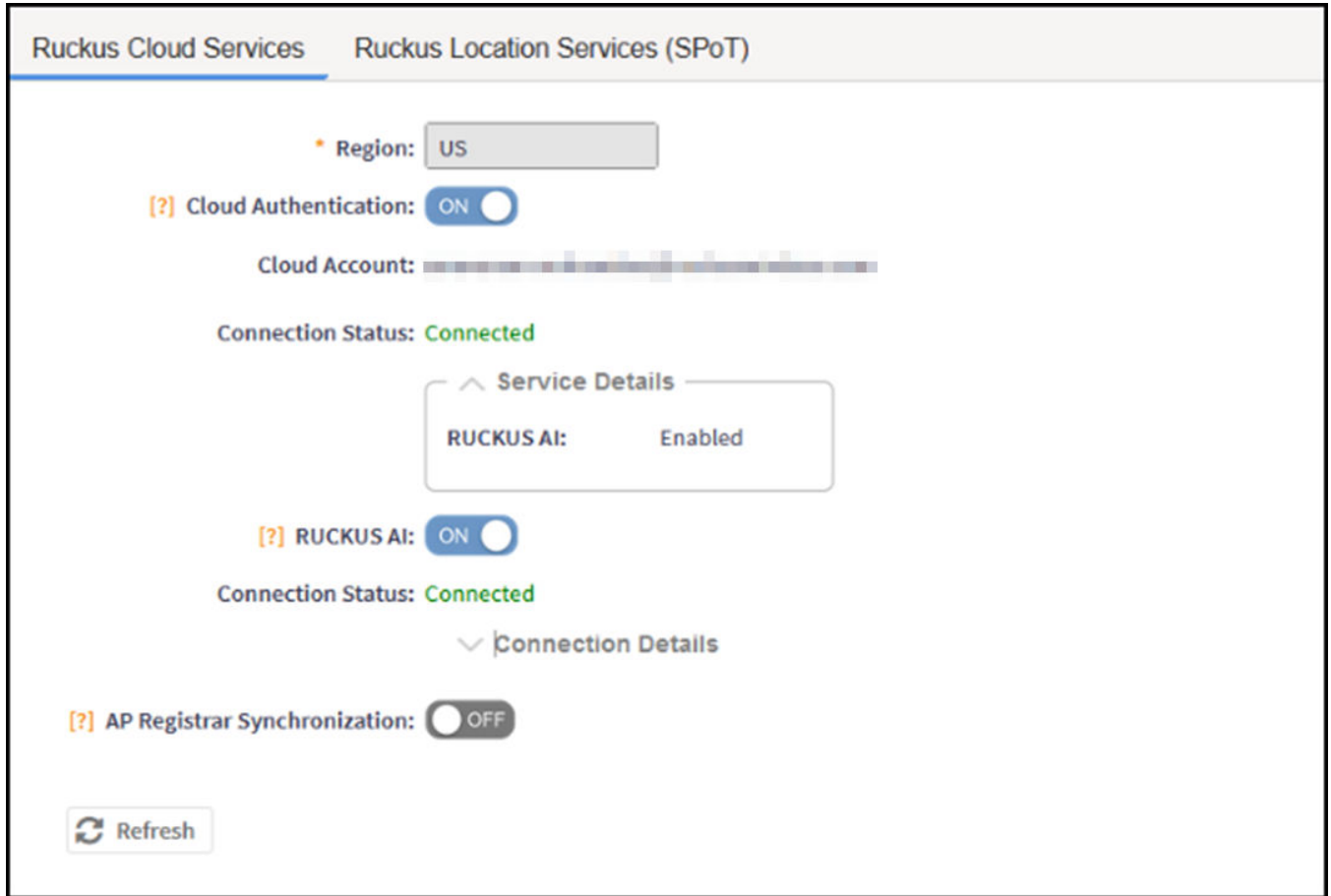
The **Ruckus Cloud Services** page is displayed.

FIGURE 96 Configuring Cloud Services



- For **Region**, select a specific cluster region to control. Options include US, EU, and Asia.

FIGURE 97 The Log in Page

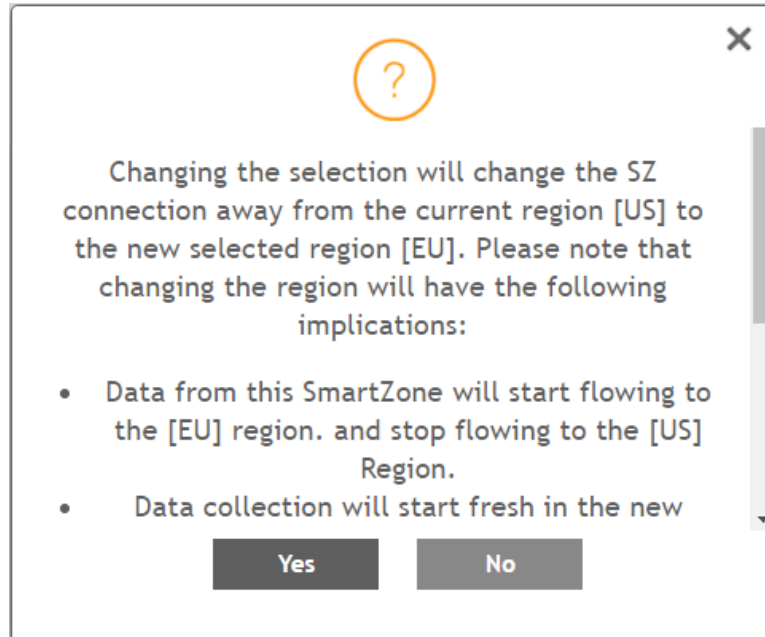


NOTE

The option to select a region is available only when **Cloud SZ Services** is disabled.

A confirmation dialog box is displayed.

FIGURE 98 Confirming the Region Change



3. Click **Yes** to confirm.

An error message is displayed if the cluster receives an unexpected response.

4. Select **Cloud SZ Services**.

You are redirected to sign in to your RUCKUS Cloud account for authentication. The RUCKUS cloud account name, connection status, and service details for RUCKUS Cloud front are displayed.

NOTE

The **Service Details** within **Connection Status** display the list of SmartZone enabled and disabled services.

5. Select **RUCKUS AI**.

The connection status for RUCKUS Cloud AI is displayed.

6. Select AP Registrar Synchronization.

FIGURE 99 Selecting Export All Batch Provisioning APs

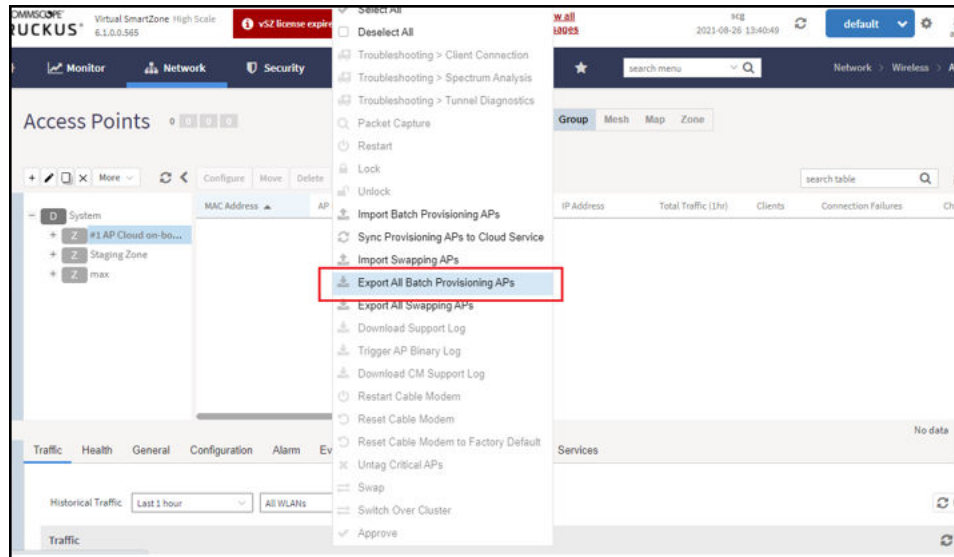
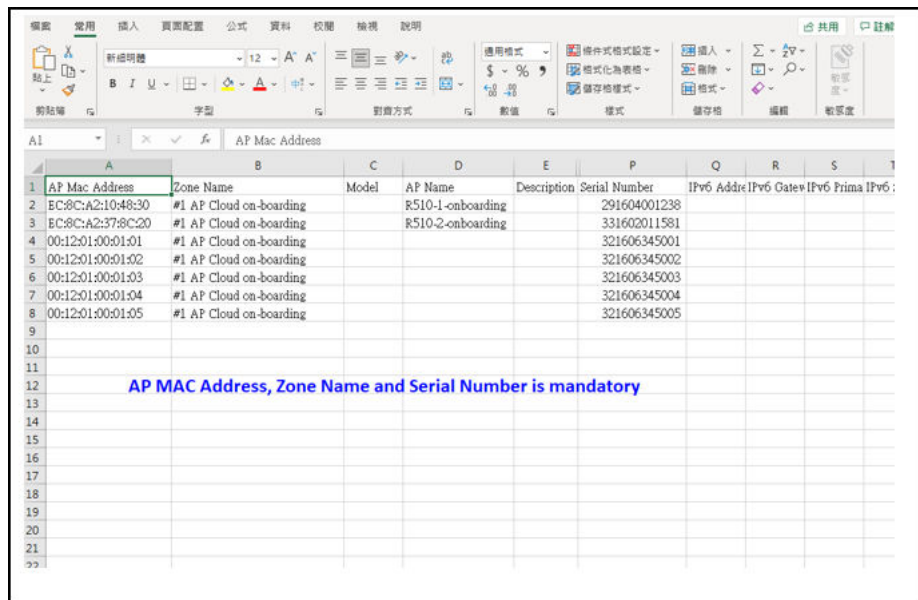


FIGURE 100 Exporting the CSV File



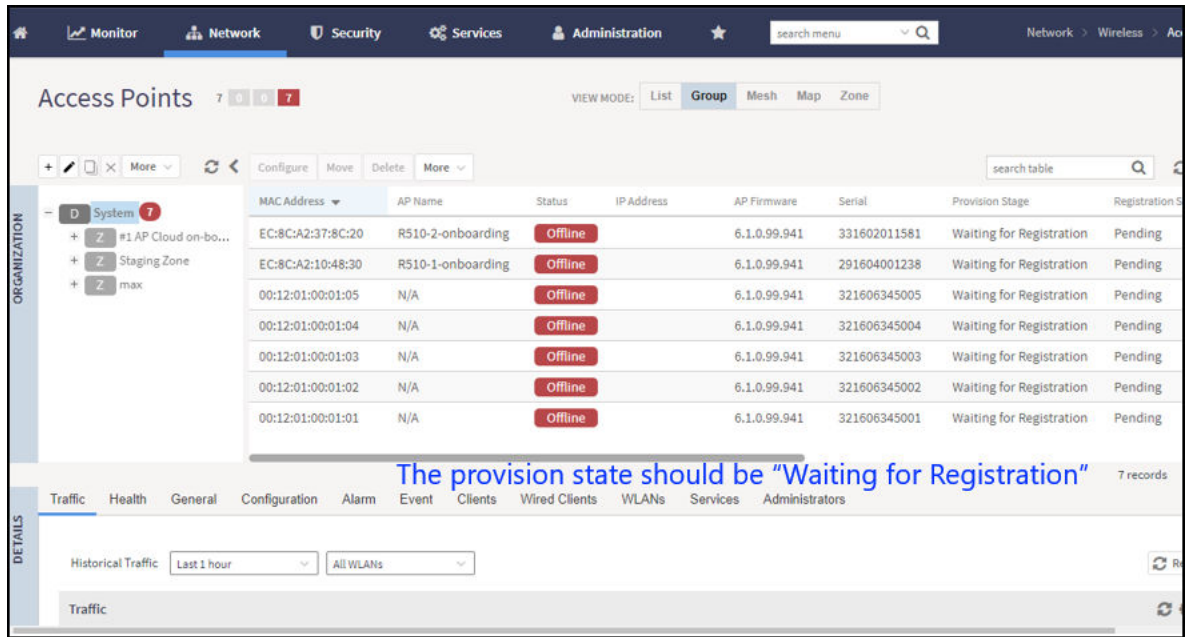
7. Go to **Network > Access points**. Select an AP and click **More..**. From the list, select **Export All Batch Provisioning APs**. A blank provisioning AP template is exported from SZ. Ensure that the AP MAC address, the zone name, and the serial number are entered in the CSV file.

- Import the provisioning AP list to an AP Zone.

NOTE

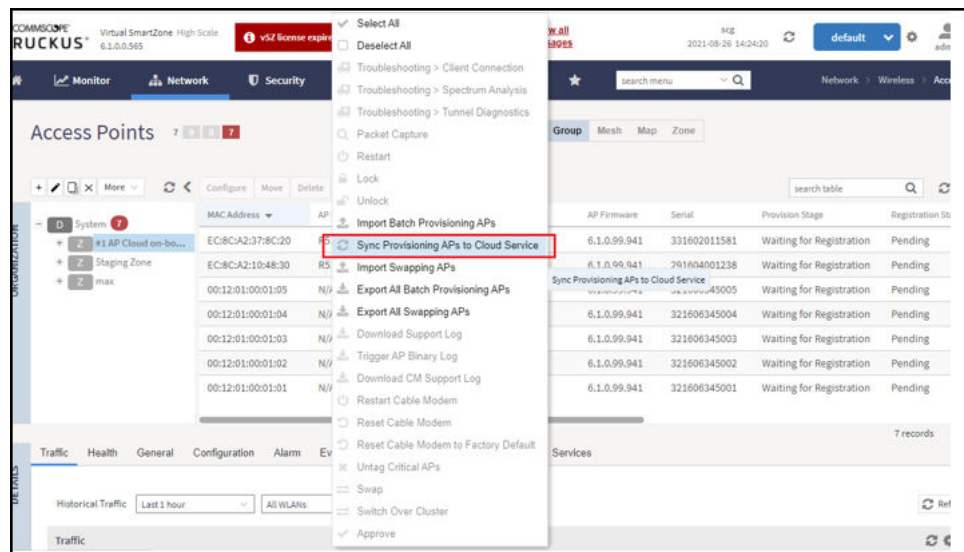
The provision stage of the AP should be "Waiting for Registration".

FIGURE 101 Importing CSV File



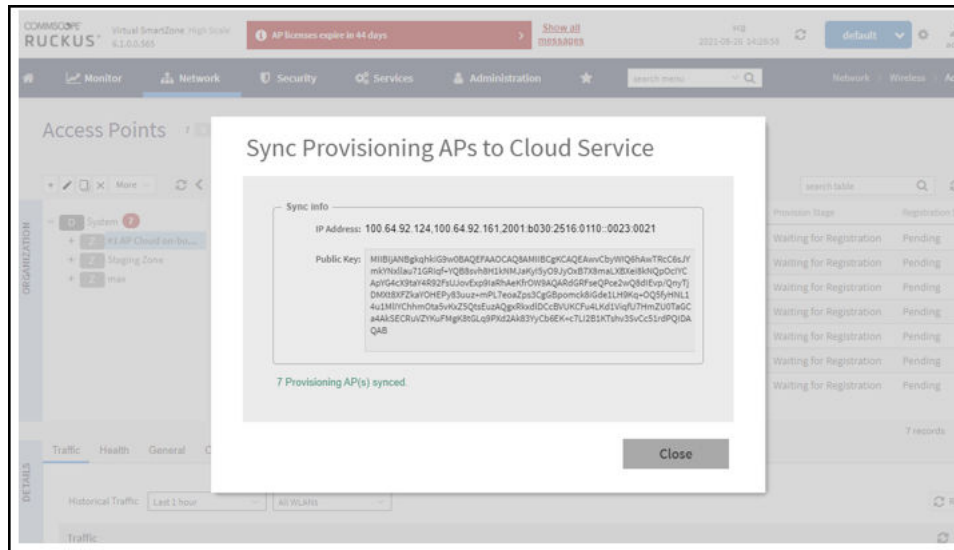
- Click **More**, and select **Sync Provisioning APs to Cloud Service** from the list.

FIGURE 102 Selecting Sync Provisioning APs to Cloud Service



10. Ensure synchronization is successful.

FIGURE 103 Ensuring Synchronization Success



Replacing Hardware Components

- [Installing or Replacing Hard Disk Drives.....](#) 155

Installing or Replacing Hard Disk Drives

You can install up to six hot-swappable SAS or SATA hard disk drives on the controller. The drives go into carriers that connect to the SAS/SATA backplane board once the carriers with drives attached are inserted back into the drive bays. The controller ships with six drive carriers.



CAUTION

If you install fewer than six hard disk drives, the unused drive bays must contain the empty carriers that ship with the server to maintain proper cooling.

Ordering a Replacement Hard Disk

To order a replacement hard disk for the controller, contact your RUCKUS sales representative and place an order for FRU part number 902-0188-0000 (Hard Drive, 600GB, 10K RPM, 64MB Cache 2.5 SAS 6Gb/s, Internal).



CAUTION

Use only FRU part number 902-0188-0000 as replacement hard disk for the controller. Using other unsupported hard disks will render the controller hardware warranty void.

Removing the Front Bezel

You must remove the front bezel to add or replace a hard drive in one of the drive bays. It is not necessary to remove the front chassis cover or to power down the system. The hard drives are hot-swappable.

Follow these steps to remove the front bezel of the controller.

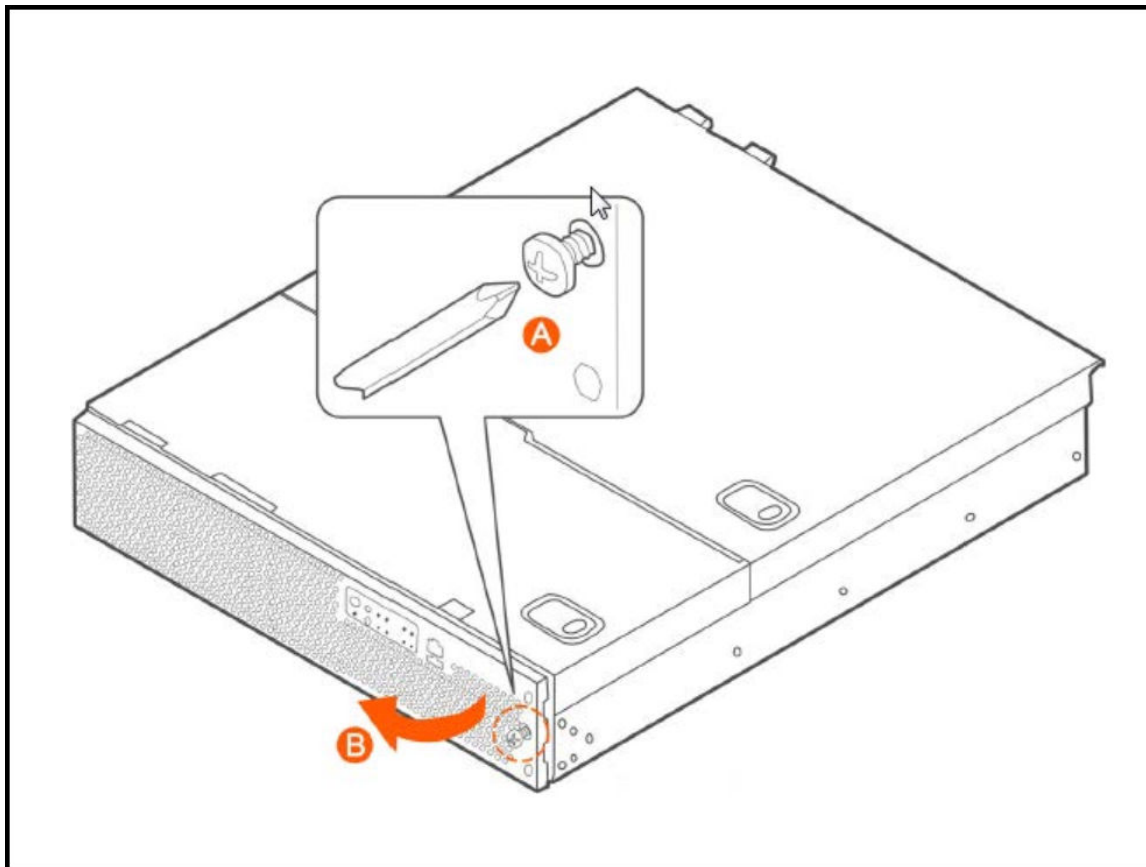
You need to remove the front bezel for tasks such as:

- Installing or removing hard disk drives or an SD flash card
- Observing the individual hard disk drive activity/fault indicators
- Replacing the control panel LED/switch board

The server does not have to be powered down just to remove the front bezel.

1. Loosen the captive bezel retention screw on the right side of the bezel (see A in [Figure 104](#)).
2. Rotate the bezel to the left to free it from the pins on the front panel (see B in [Figure 104](#)), and then remove it.

FIGURE 104 Removing the front bezel



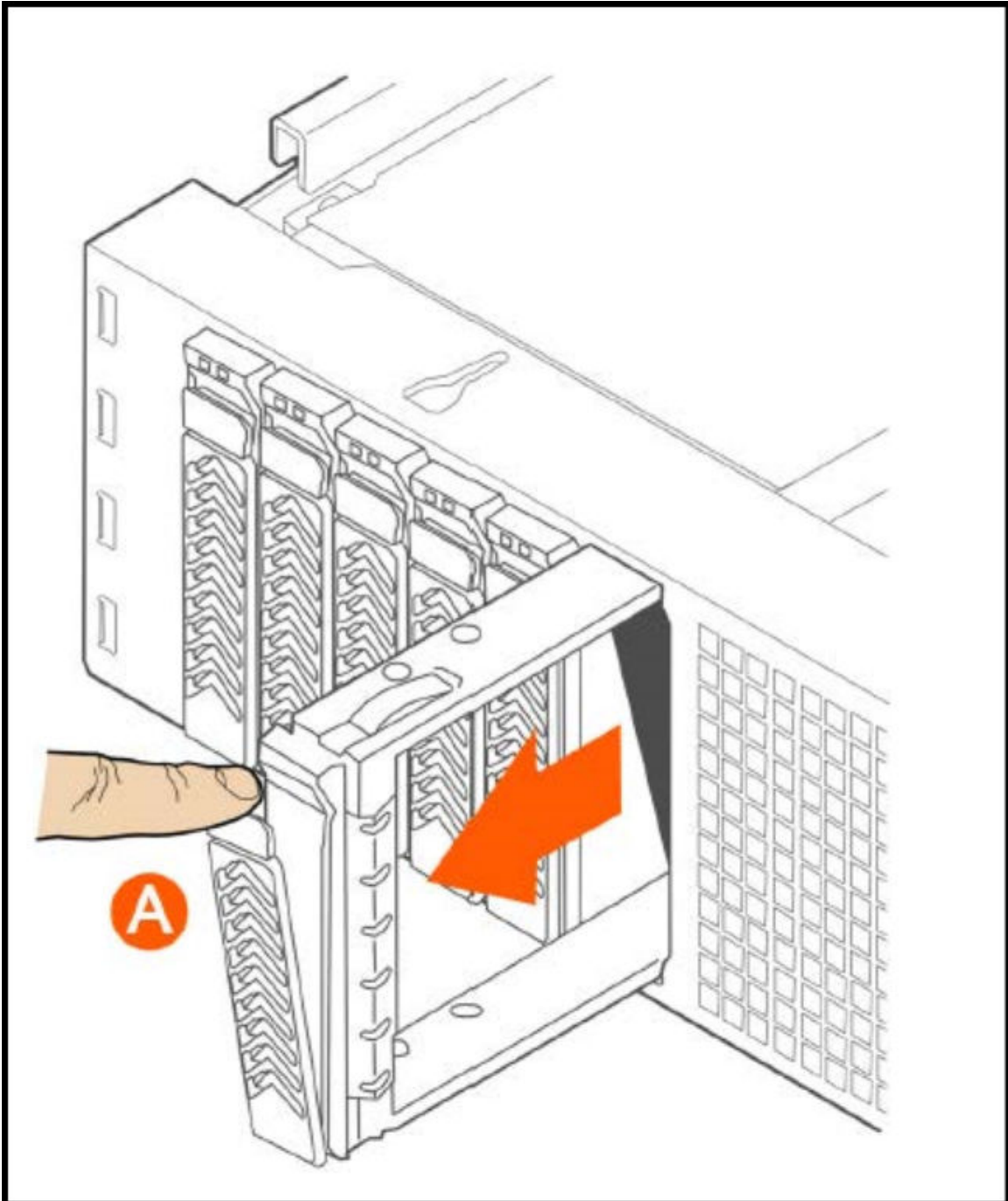
Removing an HDD Carrier from the Chassis

Follow these steps to remove a hard disk drive carrier from the chassis.

1. Remove the front bezel (see [Removing the Front Bezel](#) on page 155).
2. Select the drive bay where you want to install or replace the drive.
Drive bay 0 must be used first, then drive bay 1 and so on. The drive bay numbers are printed on the front panel below the drive bays.
3. Remove the drive carrier by pressing the green button to open the lever.
(See A in [Figure 105](#)).

4. Pull the drive carrier out of the chassis.

FIGURE 105 Removing the drive carrier

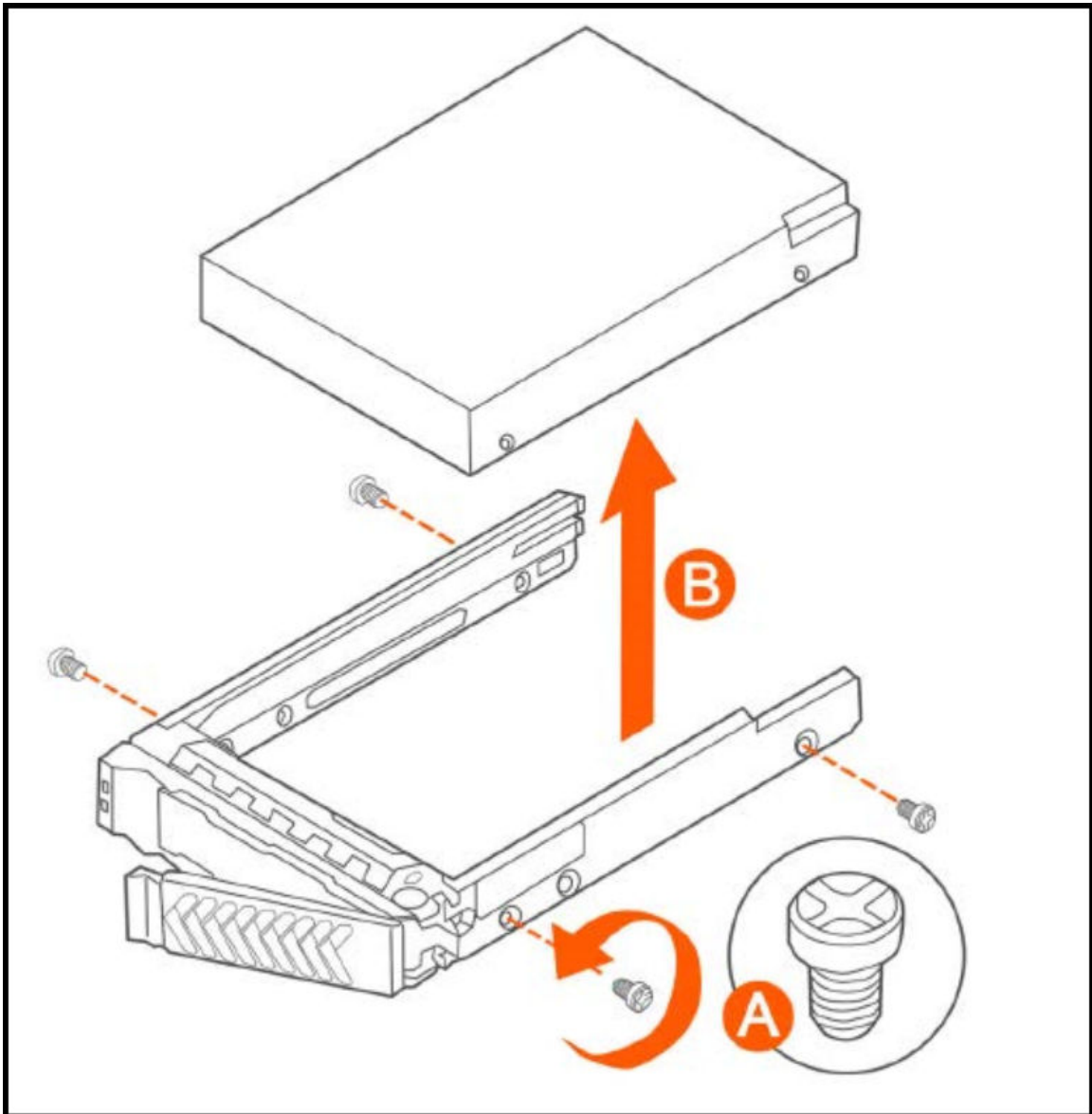


Installing a Hard Drive in a Carrier

Follow these steps to install a hard drive in a drive carrier.

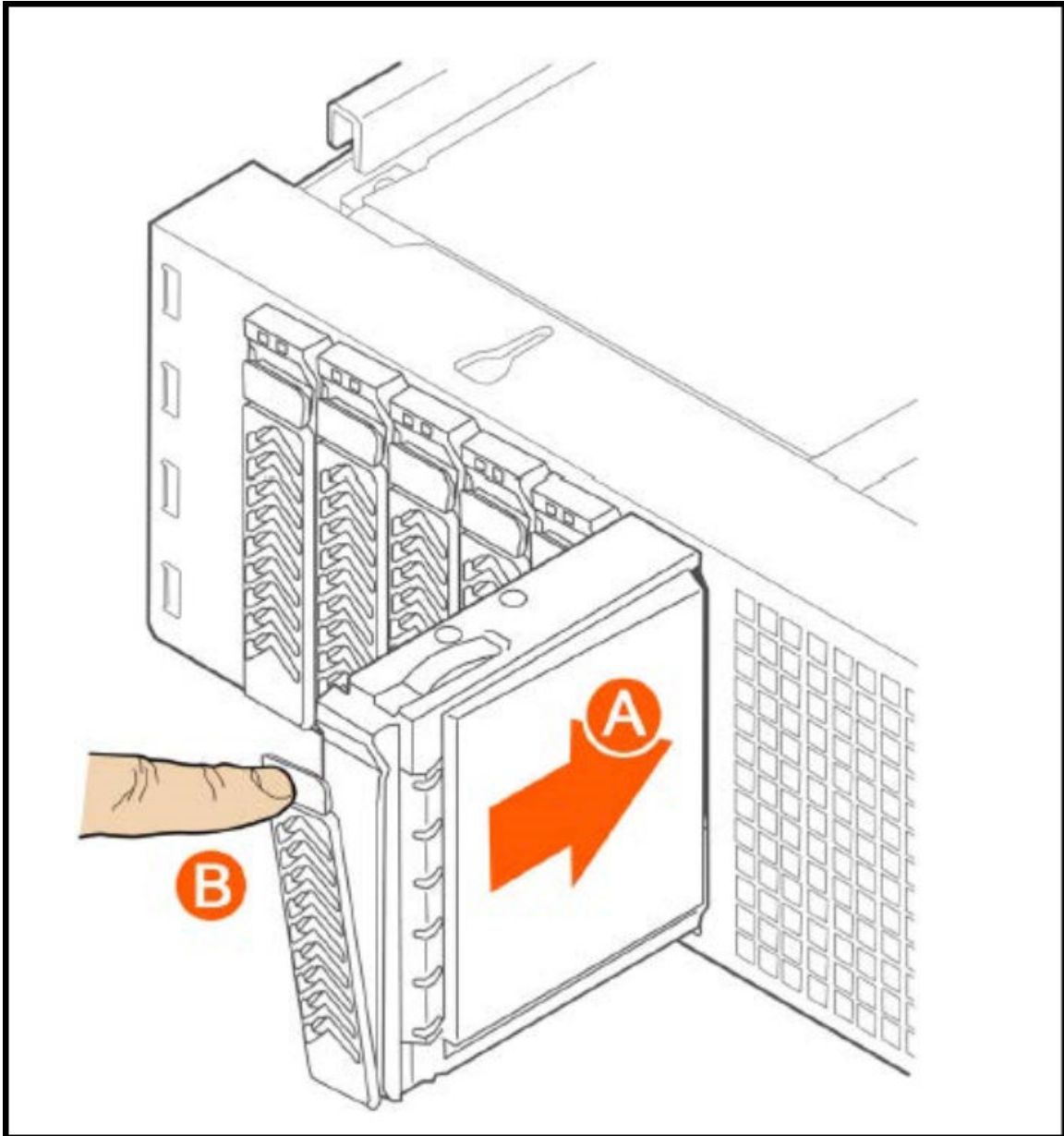
1. If a drive is already installed (that is, if you are replacing the drive), remove it by unfastening the four screws that attach the drive to the drive carrier (see A in [Figure 106](#)). Set the screws aside for use with the new drive.
2. Lift the drive out of the carrier (see B in [Figure 106](#)).

FIGURE 106 Removing the hard drive



3. Install the new drive in the drive carrier (see A in [Figure 107](#)), and then secure the drive with the four screws that come with the carrier (see B).

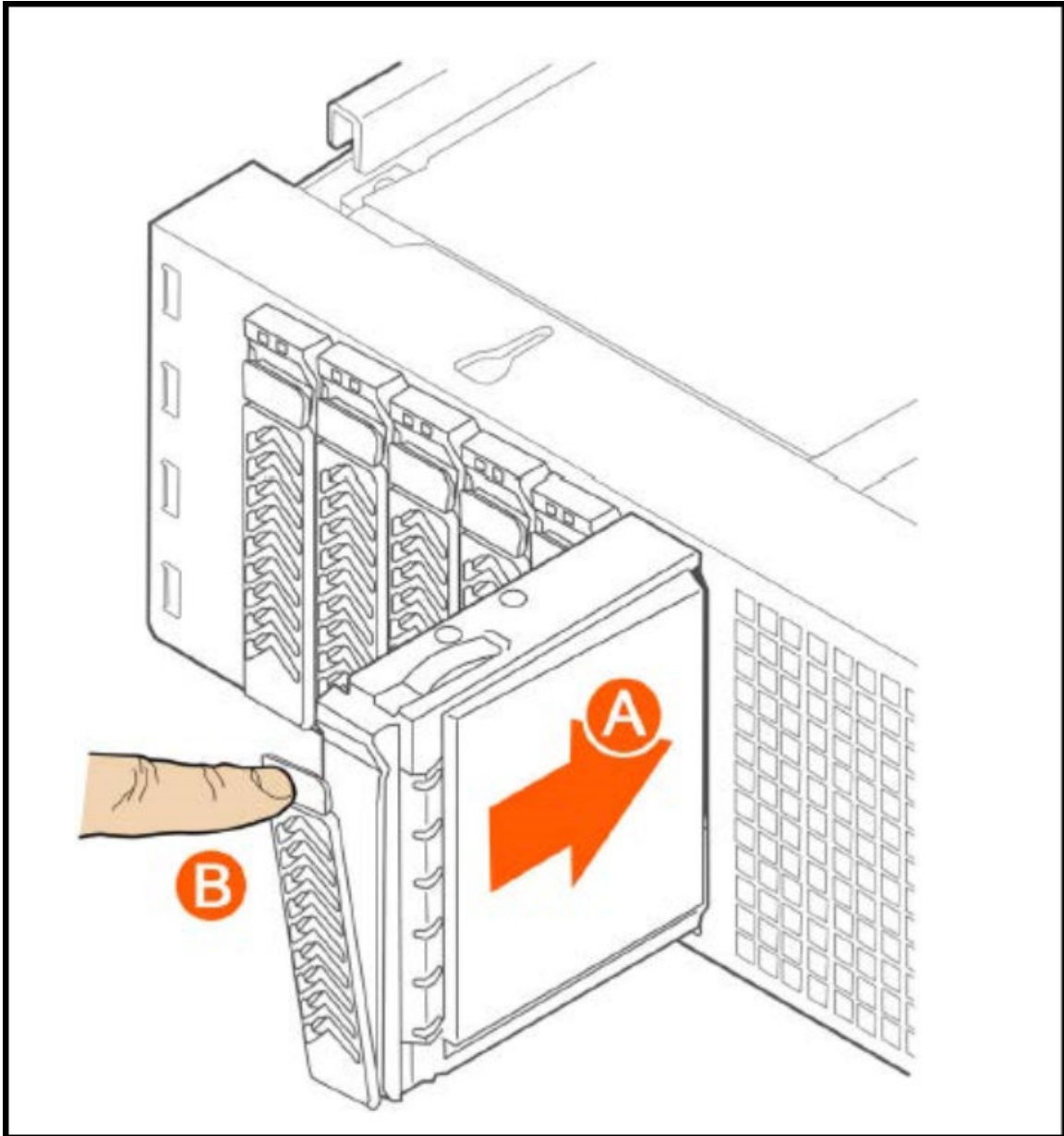
FIGURE 107 Installing the hard drive



Replacing Hardware Components
Installing or Replacing Hard Disk Drives

4. With the drive carrier locking lever fully open, push the hard drive carrier into the drive bay in the chassis until it stops (see A in [Figure 108](#)).

FIGURE 108 Inserting the carrier back into the chassis



5. Press the locking lever until it snaps shut and secures the drive in the bay.

You have completed installing or replacing the hard drive onto the controller.

NOTE

The new hard drive will synchronize automatically with the existing RAID array. During the synchronization process, the HDD LED on the controller will blink amber and green alternately. When the process is complete, the HDD LED will turn off.

Reinstalling the Front Bezel

Follow these steps to reinstall the front bezel on the controller.

1. Insert the tabs on the left side of the bezel into the slots on the front panel of the chassis.
2. Move the bezel toward the right of the front panel and align it on the front panel pins.
3. Snap the bezel into place and tighten the retention screw to secure it.

Replacing PSUs

The controller includes two redundant, hot-swappable power supply units (2 AC PSUs or 2 DC PSUs). No chassis components need to be removed to add or replace a PSU.

Follow these steps to remove and replace a PSU.

1. Identify the faulty PSU by looking at the PSU status LED (red indicates PSU failure, green indicates normal operation).
2. Press and hold the green safety lock downward while grasping the PSU handle.
3. Pull outward on the handle, sliding the PSU all the way out of the rear of the machine.
4. Insert the new PSU into the slot and, while holding the green safety lock, slide the PSU into the slot until it locks in place.

The PSU status LED turns green, indicating that the PSU is operating normally.

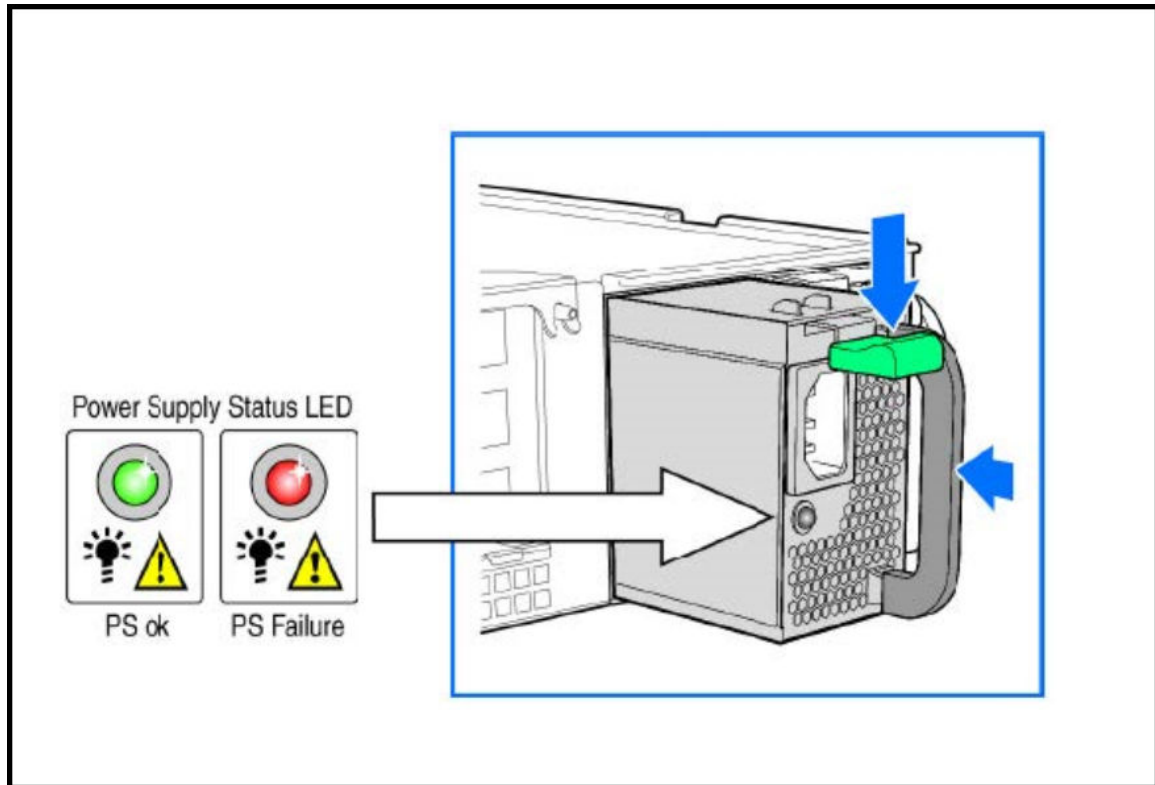
Replacing Hardware Components

Installing or Replacing Hard Disk Drives

NOTE

If you are installing a DC power supply, there are two threaded studs for chassis enclosure grounding. A 90" standard barrel, two-hole, compression terminal lug with 5/8-inch pitch suitable for a #14-10 AWG conductor must be used for proper safety grounding. A crimping tool may be needed to secure the terminal lug to the grounding cable.

FIGURE 109 Replacing a PSU



Replacing System Fans

The controller includes six redundant, hot-swappable system fans (four 80mm fans and two 60mm fans). There are also two fans located inside the power supply units. Redundancy for the two PSU fans is only achieved when both PSUs are installed.

If any of the system fans requires replacement, the replacement procedure is identical.

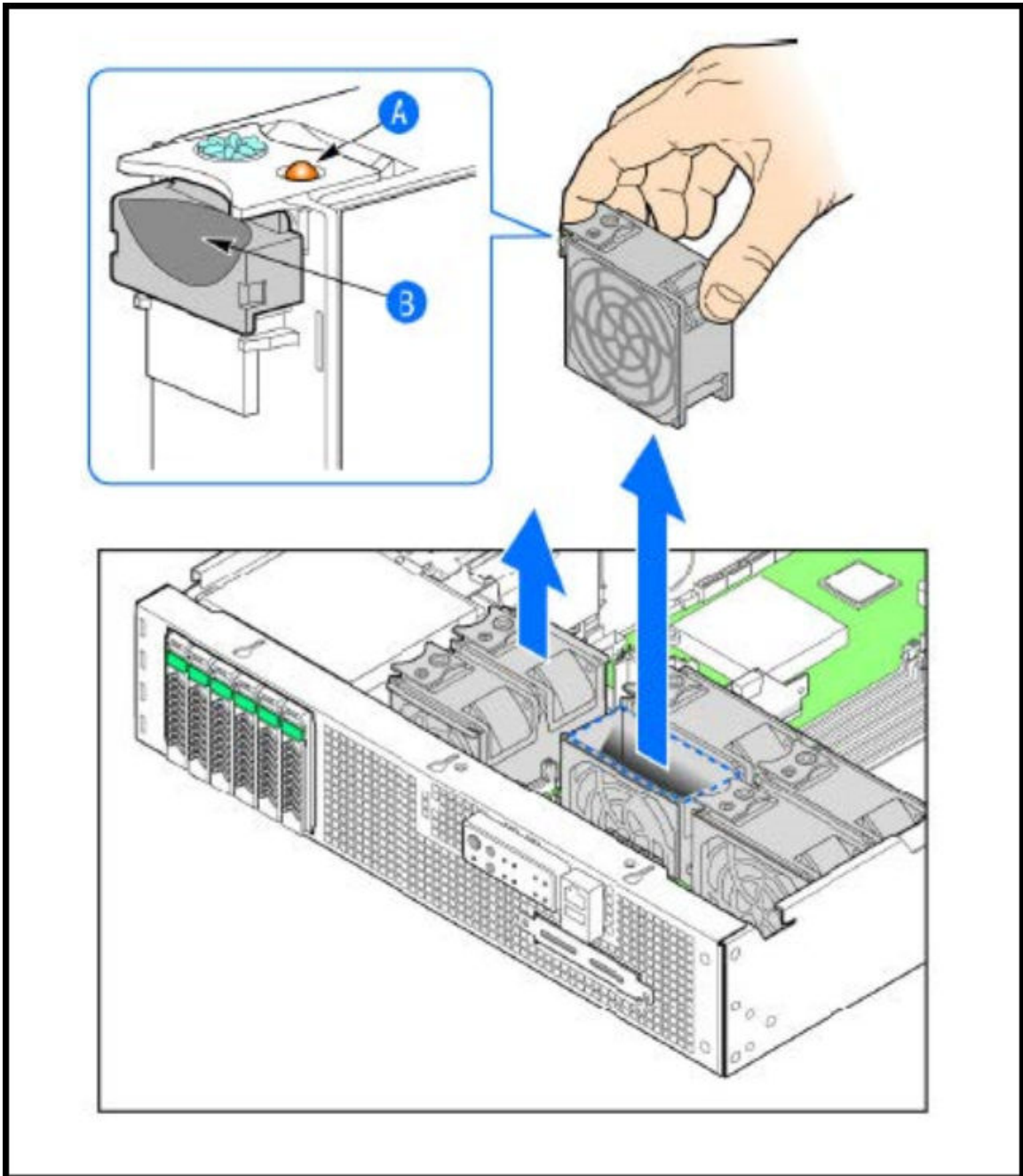
Electrostatic discharge (ESD) can damage internal components such as printed circuit boards and other parts. RUCKUS recommends that you only perform this procedure with adequate ESD protection. At a minimum, wear an anti-static wrist strap attached to the ESD ground strap attachment on the front panel of the chassis.

Follow these steps to replace a system fan.

1. Open the front chassis cover of the controller. It may be necessary to extend the controller into a maintenance position.
2. Identify the faulty fan. Each fan has a "service required" LED that turns amber when the fan is malfunctioning.
3. Remove the faulty fan by grasping both sides of the fan assembly, using the plastic finger guard on the left side and pulling the fan out of the metal fan enclosure.
4. Slide the replacement fan into the same metal fan enclosure. Use the edges of the metal enclosure to align the fan properly and ensure the power connector is seated properly in the header on the side of the enclosure.

5. Apply firm pressure to fully seat the fan.
6. Verify that the (service required) LED on the top of the fan is not lit.
7. Close the front chassis cover and return the controller to its normal position in the rack, if necessary.

FIGURE 110 Replacing a system fan



Upgrade

- [Upgrading the Controller.....](#) 165
- [Patch/Diagnostic Scripts.....](#) 168
- [Application Signature Packages.....](#) 169

Upgrading the Controller

RUCKUS may periodically release controller software updates that contain new features, enhancements, and fixes for known issues. These software updates may be made available on the RUCKUS support website or released through authorized channels.



CAUTION

Although the software upgrade process has been designed to preserve all controller settings, RUCKUS strongly recommends that you back up the controller cluster before performing an upgrade. Having a cluster backup will ensure that you can easily restore the controller system if the upgrade process fails for any reason.



CAUTION

RUCKUS strongly recommends that you ensure that all interface cables are intact during the upgrade procedure.



CAUTION

RUCKUS strongly recommends that you ensure that the power supply is not disrupted during the upgrade procedure.

Performing the Upgrade

RUCKUS strongly recommends backing up the controller cluster before performing the upgrade. If the system crashes for any reason, you can use the latest backup file to restore the controller cluster.

Always back up the controller before attempting a software upgrade. If you are managing a multi-node cluster, back up the entire cluster, and then verify that the backup process completes successfully.

If you have an FTP server, back up the entire cluster and upload the backup files from all the nodes in a cluster to a remote FTP server.

Before starting this procedure, you should have already obtained a valid controller software upgrade file from RUCKUS Support Team or an authorized reseller.

1. Copy the software upgrade file that you received from RUCKUS to the computer where you are accessing the controller web interface or to any location on the network that is accessible from the web interface.
2. Go to **Administration > Administration > Upgrade**.
3. Select the **Upgrade** tab.

In Current System Information, the controller version information is displayed.

NOTE

The **Upgrade History** tab displays information about previous cluster upgrades.

4. In Upload, select the **Run Pre-Upgrade Validations** check box to verify if the data migration was successful. This option allows you to verify data migration errors before performing the upgrade.
5. Click **Browse** to select the patch file.

Upgrade

Upgrading the Controller

6. Click **Upload** to upload the controller configuration to the one in the patch file.

The controller uploads the file to its database, and then performs file verification. After the file is verified, the **Patch for Pending Upgrade** section is populated with information about the upgrade file. If data migration was unsuccessful, the following error is displayed:

```
Exception occurred during the validation of data migration. Please apply the system configuration backup and contact system administrator.
```

7. Click **Backup & Upgrade** to perform the upgrade. The backup operation is done before the system upgrade flow starts. The backup file will be used to restore cluster automatically while the upgrade process fails. Refer to [Creating a Cluster Backup](#) on page 173 for more information.

When the forced backup-and-upgrade process is complete, the controller logs you off the web interface automatically. When the controller log on page appears again, you have completed upgrading the controller.

In the **Current System Information** section, check the value for controller version. If the firmware version is newer than the firmware version that controller was using before you started the upgrade process, then the upgrade process was completed successfully.

NOTE

APs periodically send scheduled configuration requests to the controller, including the firmware version. Therefore, when an AP joins a zone for the first time, the firmware version is verified by the controller. If the firmware version is different from that which is configured for the zone, the controller responds with a request to upgrade it, after which the AP initiates a request to upgrade the firmware using HTTP.

Verifying the Upgrade

You can verify that the controller upgrade was completed successfully.

1. Go to **Administration > Administration > Upgrade**.
2. In the **Current System Information** section, check the value for *Controller Version*. If the firmware version is newer than the firmware version that controller was using before you started the upgrade process, then the upgrade process was completed successfully.

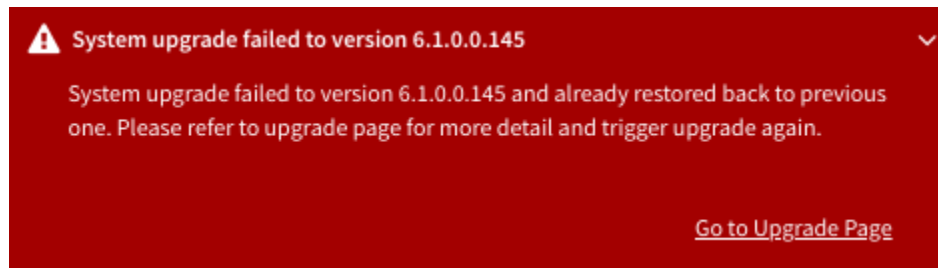
NOTE

APs periodically send scheduled configuration requests to the controller, including the firmware version. Therefore, when an AP joins a zone for the first time, the firmware version is verified by the controller. If the firmware version is different from that which is configured for the zone, the controller responds with a request to upgrade it, after which the AP initiates a request to upgrade the firmware using HTTP.

Verifying Upgrade Failure and Restoring Cluster

When the restore operation is complete and user log in the dashboard again, the following Global Warning message is displayed stating that the system upgrade failed and has been restored to the previous version.

FIGURE 111 Global Warning Message



NOTE

Click the **Go to Upgrade Page** link to initiate the **Backup & Upgrade** process again.

For more information on system restore:

1. Go to **Administration > Administration > Upgrade**.

The **Upgrade History** lists the information of upgrade success or upgrade failure with restore operation.

FIGURE 112 Upgrade History Table

Start Time	State	System Version	Control Plane Software Version	AP Firmware Version	Path File Name	Upgrade Elapsed
2021/03/22 16:14:16	Failed And Restored	6.0.0.0.1025->6.1.0.0.145	6.0.0.0.1025->6.1.0.0.126	6.0.0.0.1273->6.1.0.0.145	vscg-6.1.0.0.145.ximg	16m 56s
2021/03/22 15:23:33	Successful	6.0.0.0.1025	6.0.0.0.1025	6.0.0.0.1273	Fresh Installation	16m 6s

2. To avoid the global warning message to keep appearing on the window, click **Ignore**.

Rolling Back to a Previous Software Version

There are scenarios in which you may want to roll back the controller software to a previous version.

Here are two:

- You encounter issues during the software upgrade process and the controller cannot be upgraded successfully. In this scenario, you can only perform the software rollback from the CLI using the restore command. If you have a two nodes controller cluster, run the restore command on one of the nodes to restore them to the previous software before attempting to upgrade them again. The restore command will trigger restore action on all nodes of the cluster if all nodes could be connected to each other. Confirm if each node can be restored back to the previous version. If any node does not roll back to the previous version, execute the restore command again on the failure node.
- You prefer a previous software version to the newer version to which you have upgraded successfully. For example, you feel that the controller does not operate normally after you upgraded to the newer version and you want to restore the previous software version, which was more stable. In this scenario, you can perform the software rollback either from the web interface or the CLI. If you have a two-node controller cluster, you must have cluster backup on both of the nodes.

Upgrade

Patch/Diagnostic Scripts

To ensure that you will be able to roll back to a previous version, RUCKUS strongly recommends the following before attempting to upgrade the controller software:

- Always back up the controller before attempting a software upgrade. If you are managing a multi-node cluster, back up the entire cluster, and then verify that the backup process completes successfully. See [Creating a Cluster Backup](#) on page 173 for the local backup instructions. If you have a local backup and you want to roll back the controller to a previous software version, follow the same procedure described in [Creating a Cluster Backup](#) on page 173.
- If you have an FTP server, back up the entire cluster and upload the backup files from all the nodes in a cluster to a remote FTP server. See [Backing Up to an FTP Server](#) on page 177 for remote backup instructions and [Restoring from an FTP Server](#) on page 179 for remote restore instructions.

Cautions & Limitations of Administrating a Cluster

Wipeout Upgrade

Wipe-out upgrade can be done to a controller firmware running

- a version later than 5.1 to a version later than 5.1
- a version earlier than 5.1 by applying a KSP patch to make the wipe-out upgrade successful.

Contact Ruckus support to receive a KSP patch file to patch from CLI.

Cluster Upgrade

For issues during software upgrade, you can only perform the software rollback from the CLI using the restore command. If you have a two nodes controller cluster, run the restore command on one of the nodes to restore them to the previous software before attempting to upgrade them again. The restore command will trigger restore action on all nodes of the cluster if all nodes could be connected to each other. Confirm if each node could be restored back to the previous version. If any node does not roll back to previous version, execute the restore command again on the failure node. Refer [Rolling Back to a Previous Software Version](#) on page 167.

Patch/Diagnostic Scripts

RUCKUS Support can provide specific patch files to be applied to the controller, either for software bug fixes or diagnostic operations during troubleshooting. The Web UI provides a location to upload these files to the controller. Once the patch file is uploaded, it may need to be executed. For detailed guidance, consult directly with RUCKUS Support, as each specific patch or script may require specific operations.

Uploading Patch or Diagnostic Scripts

Complete the following steps to upload a script.

1. From the main menu, click **Monitor**.
2. Under **Troubleshooting & Diagnostics**, hover over the **Scripts**, and click **Patch/Diagnostic Scripts**.
3. Select the **Upload to current node** check box.
4. Click **Browse** to select a script that you want to upload to the controller.

5. Click **Upload**.

The script is listed in the **System Uploaded Scripts** area.

If you have uploaded a patch script, it is displayed in the **System Uploaded Patch Scripts** area with the following information:

- Name of the patch file
- Patch file description
- Supported AP firmware version
- AP model number

You can click **Delete** to delete scripts.

NOTE

Patch or Diagnostic scripts use the patch file type. Make sure this is the file type you are trying to upload or request the RUCKUS Support representative send the appropriate file type.

Applying Patch or Diagnostic Scripts

Each of the patch or diagnostic scripts is unique in its capabilities and depending on the issue that is to be addressed or the kind of diagnosing that will be performed, the patch can be applied directly using the Web UI in the controller or it should be executed to individual nodes using the CLI of the controller. Consult with RUCKUS Support for confirmation on the appropriate way to apply or execute the required script.

Complete the following steps to apply a patch/diagnostic script using the Web UI:

1. From the main menu, navigate to **Monitor > Troubleshooting & Diagnostics > Scripts > Patch/Diagnostic Scripts**.
2. Scroll down to **System Uploaded Scripts** or **Patch Scripts**.
3. Select the script to be applied and click **Apply Patch**.
4. A confirmation window will pop up. Click **Yes** to continue.
5. A message confirmation will appear. Click **OK** to finish.
6. Under **System Uploaded Scripts** or **Patch Scripts**, the **Applied On** column will confirm the patch has been recently applied.

NOTE

When the RUCKUS engineers are developing a new script, they will be required to know which scripts have already been applied to the controller, so they can consider these scripts when creating the new one. Make sure this information is shared with RUCKUS Support *before* the new patch/diagnostic script is created and applied.

Application Signature Packages

RUCKUS periodically releases and makes new application signature packages available for download.

The controller web user interface displays a notification on the **Dashboard**, when the latest signature application package is available for download.

Alternatively, application signature package updates or downloads can be scheduled from the RUCKUS download center.

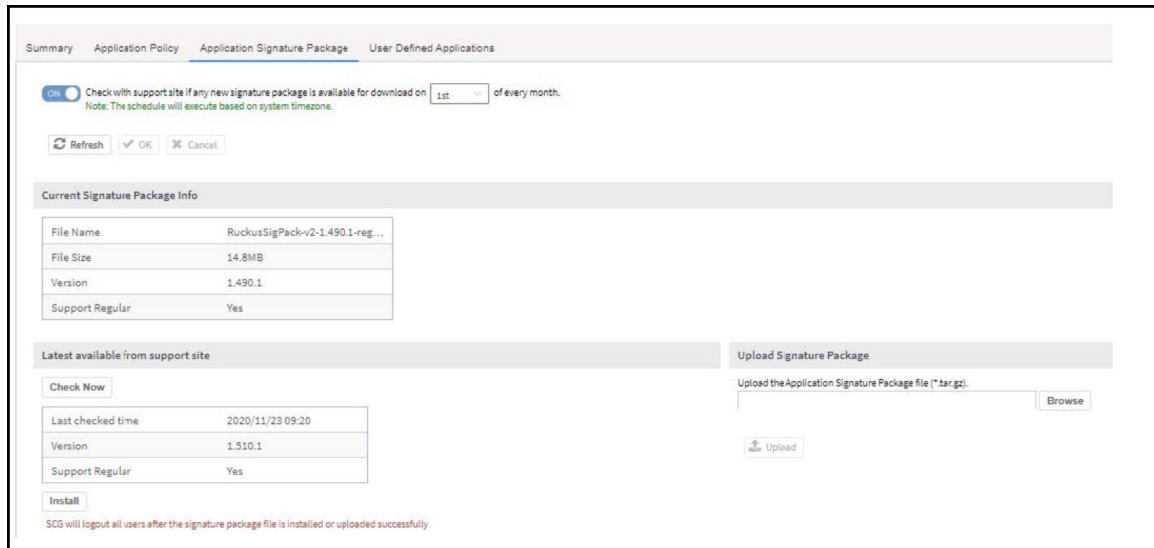
Refer to *RUCKUS SmartZone Controller Administration Guide* for detailed information related to the application signature packages.

Step 1: Uploading the Signature Package

Once you have downloaded a new signature package, you can import it into SmartZone using the following procedure:

1. Select **Security > Application Control > Application Signature Package**.

FIGURE 113 Viewing and Uploading Signature Package File Information



The **Current Signature Package Info** section displays the information about the file name, file size, version and type of the signature package. For information on the latest signature package, refer to *RUCKUS SmartZone Upgrade Guide*.

2. Select the tab.
3. Under **Upload Signature Package**, click **Browse** to select the signature package file.
4. Click **Upload** to upload the signature package file.

Once the import is complete, the list of system-defined applications is updated immediately.

Step 2: Validating the Signature Package

The application updates the latest signature package in all the connected APs. To validate the latest version follow the procedure:

1. In the Access Point, enter the Privileged EXEC mode using CLI.
2. Enter the following CLI command, which displays the latest version of the signature package.

```
get qmdpi-version : get qmdpi-version
                    == get version details of DPI

rkscli: get qmdpi-version
DPI Signature Version : RuckusSigPack-v2-1.430.1
DPI Engine Version   : 5.4.0-68.052 (build date Jun  3 2019)
DPI Bundle Version   : 1.430.0-20 (build date Apr 15 2019)
```

OK

Managing Signature Package Upgrading Conflicts

Upgrading a Signature package from lower version to a higher version fails when an Access Control Policy and an Application Control Policy already exists and the Application Signature in the AVC Policy of lower version conflicts with the one in higher version. In such a case, SZ displays an error message. Perform the following procedure to avoid this error.

To overcome Signature Package upgrade conflicts:

Step 1: Delete the L3 Access Control Policy:

1. Go to **Security > Access Control > L3 Access Control**.

NOTE

For SmartZone 5.2.1 or earlier releases, select **Firewall > L3 Access Control**

2. Take a note of the policy details that you want to delete; click **Configure** to get more details of the profile for future reference.
3. Select the profile and click **Delete**.

Step 2: Delete the Application Control Policy:

1. Go to **Security > Application Control > Application Policy**.

NOTE

For SmartZone 5.2.1 or earlier releases, select **Firewall > Application Control > Application Policy**

2. Take a note of the policy details that you want to delete; click **Configure** to get more details of the profile for future reference.
3. Select the policy and click **Delete**.

Step 3: Upgrade the Signature Package

1. Go to **Security > Application Control > Application Signature Package**.

NOTE

For SmartZone 5.2.1 or earlier releases, select **Firewall > Application Control > Signature Package**

2. Click **Browse**, and choose the Signature Package file.
3. Click **Upload**.

After the Signature Package is successfully applied the package file name, file size and the version will be visible in the UI.

Step 4: Create a new L3 Access Control Policy with the details of the policy deleted.

Step 5: Create a new Application Control Policy with the details of the policy deleted.

Backup and Restore

- Cluster Backup..... 173
- Configuration Backup..... 176

Cluster Backup

Disaster Recovery

Creating cluster backup and restoring cluster configurations periodically helps manage disaster recovery.

Creating a Cluster Backup

Backing up the cluster (includes OS, configuration, database and firmware) periodically enables you to restore it in the event of an emergency. RUCKUS also recommends that you back up the cluster before you upgrade the controller software.

1. Go to **Administration > Administration > Backup and Restore**.
2. Select the **Cluster** tab.
3. In Cluster Backup and Restore, click **Backup Entire Cluster** to backup both nodes in a cluster.
The following confirmation message is displayed: `Are you sure you want to back up the cluster?`
4. Click **Yes**.

The following message is displayed: `The cluster is in maintenance mode. Please wait a few minutes.`

When the cluster backup process is complete, a new entry is displayed in the **Cluster Backups History** section with a **Created On** value that is approximate to the time when you started the cluster backup process.

Restoring a Cluster Backup

You must be able to restore a cluster to its previous version in the case of a failure.

1. Go to **Monitor > Troubleshooting&Diagnostics > Application Logs**.
2. Select the **Cluster** tab.
3. In Cluster Backup History, select the cluster and click **Restore**.

The following confirmation message appears:

`Are you sure you want to restore the cluster?`

4. Click **Yes**.

The cluster restore process may take several minutes to complete. When the restore process is complete, the controller logs you off the web interface automatically.

ATTENTION

Do not refresh the controller web interface while the restore process is in progress. Wait for the restore process to complete successfully.

Backup and Restore

Cluster Backup

5. Log on to the controller web interface.

If the web interface displays the message `Cluster is out of service. Please try again in a few minutes` appears after you log on to the controller web interface, wait for about three minutes. The dashboard will appear shortly. The message appears because the controller is still initializing its processes.

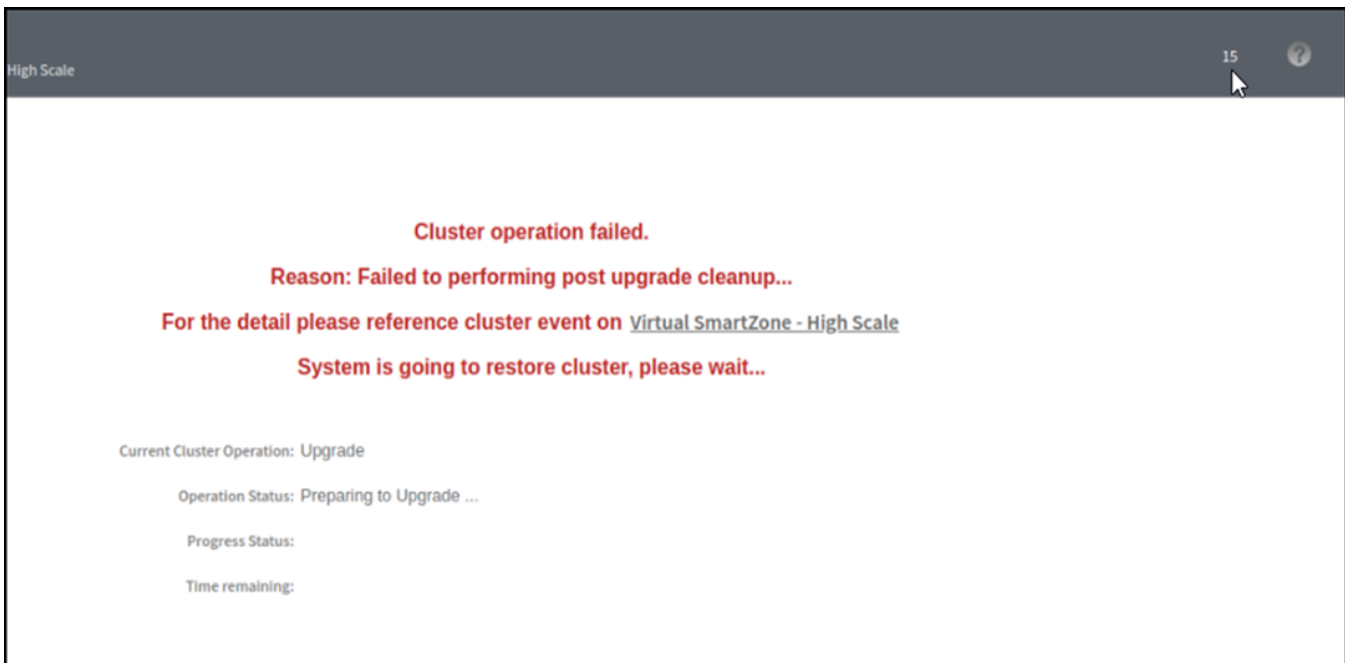
6. Go to **Administration > Upgrade**, and then check the **Current System Information** section and verify that all nodes in the cluster have been restored to the previous version and are all in service.
7. Go to **Diagnostics > Application Logs**, and then under **Application Logs & Status** check the **Health Status** column and verify that all of the controller processes are online.

Restoring a Cluster Automatically on Upgrade Failure

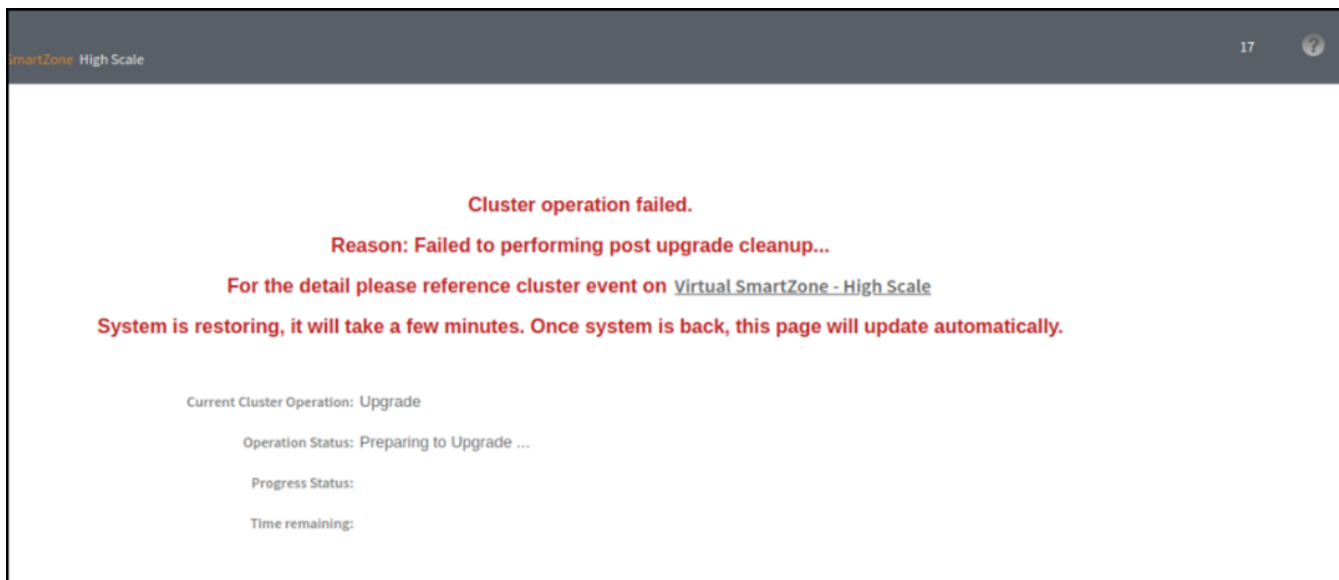
When cluster upgrade fails in the middle, the system will automatically restore the cluster with the backup file prepared in the beginning of the upgrade process and goes back to previous version of the image. The user does not need to manually restore the cluster.

When the cluster fails to upgrade and a restore action is triggered, the system performs the following process:

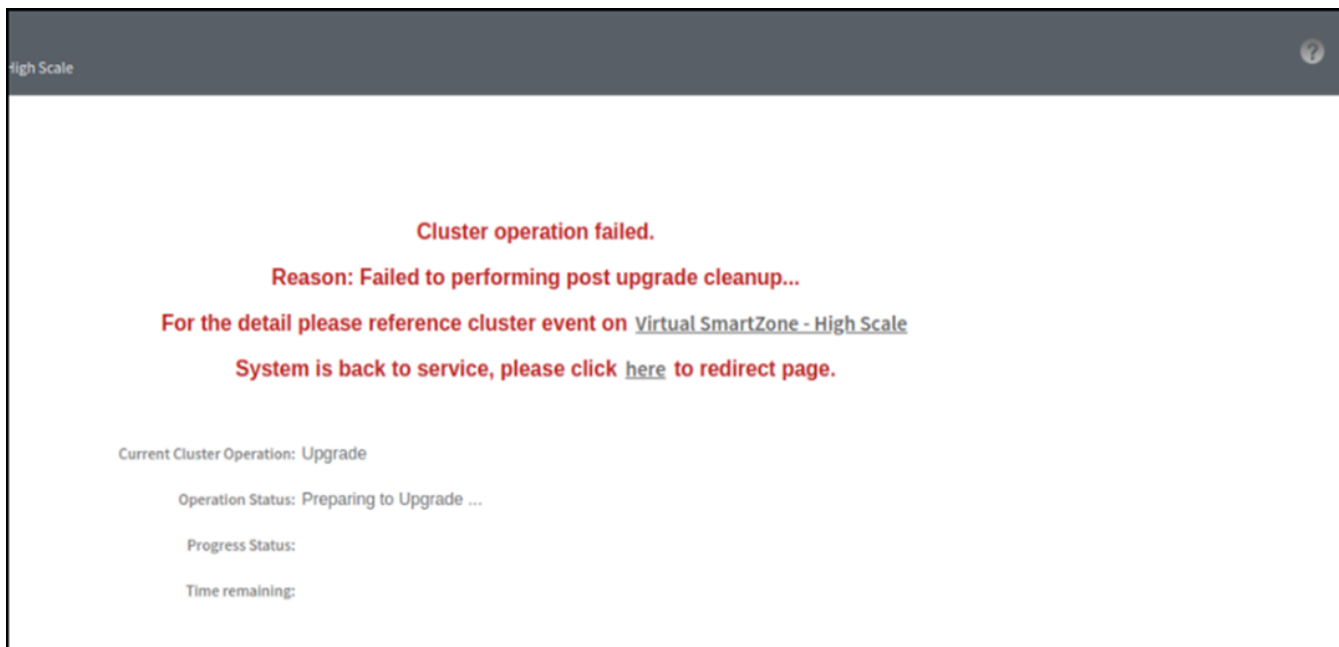
Starting a restore process



Restoring cluster



Cluster back to service



Configuration Backup

Backing up Cluster Configuration

RUCKUS strongly recommends that you back up the controller database periodically. This will help ensure that you can restore the system configuration settings easily if the database becomes corrupted for any reason.

The following are backed up in the system configuration backup file:

TABLE 17 Contents of a cluster configuration backup file

Configuration Data	Administration Data	Report Data	Identity Data
AP zones	Cluster backup	Saved reports	Created profiles
Third-party AP zones	System configuration backups	Historical client statistics	Generated guest passes
Services and profiles	Upgrade settings and history	Network tunnel statistics	
Packages	Uploaded system diagnostic scripts		
System settings	Installed licenses		
Management domains			
Administrator accounts			
MVNO accounts			

A system configuration backup does not include control plane settings, data plane settings, and user-defined interface settings.

1. Go to **Administration > Administration > Backup and Restore**.
2. Select the **Configuration** tab.
3. In System Configuration Backup History, click **Backup**.

The following confirmation message appears: Are you sure you want to back up the controller's configuration?

4. Click **Yes**.

A progress bar appears as the controller creates a backup of the its database. When the backup process is complete, the progress bar disappears, and the backup file appears under the **System Configuration Backup History** section.

NOTE

The system will limit the configuration backup to 5 scheduled and 50 Manual backup files.

Scheduling a Configuration Backup

You also have the option to configure the controller to backup its configuration automatically based on a schedule you specify.

1. Go to **Administration > Administration > Backup and Restore**.
2. Select the **Configuration** tab.

3. In Schedule Backup, you can configure the controller to backup its configuration automatically based on a schedule you specify.
 - a. In Schedule Backup, click **Enable**.
 - b. In Interval, set the schedule when the controller will automatically create a backup of its configuration. Options include: Daily, Weekly and Monthly.
 - c. Hour: Select the hour of the day when the controller must generate the backup.
 - d. Minute: Select the minute of the hour.
 - e. Click **OK**.

Backing Up to an FTP Server

Follow these steps to back up the controller network configuration to an FTP server.

1. Log on to the controller from the controller's command line interface (CLI). For more information, see the corresponding *Command Line Interface Reference Guide* for your controller platform.
2. At the prompt, enter **en** to enable privileged mode.

FIGURE 114 Enable privileged mode

```
dean300-1> en
Password: *****
```

3. Enter **-** to display the statuses of the node and the cluster.
Before continuing to the next step, verify that both the node and the cluster are in service.

FIGURE 115 Verify that both the node and the cluster are in service

```
dean300-1# show cluster-state
Current Management Service Status : In service
Current Node Status : In service
Cluster Status : In service
Cluster Operation : None
System Mode : None
```

4. Enter backup network to back up the controller network configuration, including the control plane and data plane information.
The controller creates a backup of its network configuration on its database.

FIGURE 116 Run backup network

```
login as: admin
#####
#      Welcome to SmartZone 300      #
#####
admin@10.206.20.239's password: *****
Last successful login: 2019-12-31 01:14:43
Last successful login from: 10.206.6.196
Failed login attempts since last successful login: 0
Account privilege changes: No
Please wait. CLI initializing...

Welcome to the Ruckus SmartZone 300 Command Line Interface
Version: 5.2.0.0.649

dean300-1> en
Password: *****

dean300-1# backup network
Do you want to backup network configurations (or input 'no' to cancel)? [yes/no] yes
Starting to backup network configurations...
Successful operation
```

5. Enter show backup-network to view a list of backup files that have been created.
Verify that the **Created On** column displays an entry that has a time stamp that is approximate to the time you started the backup.

FIGURE 117 Enter the show backup-network command

```
dean300-1# show backup-network
  No.   Created on                Patch Version                File Size
-----
  1     2019-12-31 01:15:30 GMT    5.2.0.0.649                 3.9KB
```

6. Enter **copy backup-network {ftp-url}**, where {ftp-url} (remove the braces) is the URL or IP address of the FTP server to which you want to back up the cluster configuration.
The CLI prompts you to choose the number that corresponds to the backup file that you want to export to the FTP server.

- Enter the number of the backup file that you want to export to the FTP server.

The controller encrypts the backup file, and then exports it to the FTP server. When the export process is complete, the following message appears on the CLI:

```
Succeed to copy to remote FTP server
Successful operation indicates that you have exported the backup file to the FTP server
successfully
```

FIGURE 118 Succeed to copy to remote FTP server

```
dean300-1# copy backup-network ftp://test:test@192.168.10.83
No.      Created on          Patch Version      File Size
-----
1        2019-12-31 01:15:30 GMT    5.2.0.0.649      3.9KB

Please choose a backup to send to remote FTP server or 'No' to cancel: 1
Starting to copy the chosen backup to remote FTP server...
Starting to encrypt backup file...
Starting to generate checksum for backup file...
Succeed to copy to remote FTP server
Successful operation
```

- Using an FTP client, log on to the FTP server, and then verify that the backup file exists.

The file format of the backup file is `network_<YYYYMMDDHHmmss>_<controller-version>.bak`.

For example, if you created the backup file on October 24th 2013 at 02:40:22 and the controller version is 2.5.0.0.402, you should see a file named `network_20131024024022_2.5.0.0.402.bak` on the FTP server.

Restoring from an FTP Server

Before you continue, take note of the following limitations with restoring a backup file of the controller network configuration from an FTP server:

- Only release 2.1 and later support restoring from an FTP server.
- In this current release, restoring the entire cluster from an FTP server is unsupported. The restore process must be performed on one node at a time.
- Restoring from an FTP server can only be performed using the CLI.



CAUTION

Restoring a backup file to the controller requires restarting all of the controller services.

Follow these steps to restore a backup file of the controller's network configuration that you previously uploaded to an FTP back to the controller.

- Log on to the controller from the CLI. For more information, see the corresponding *Command Line Interface Reference Guide* for your controller platform.
- At the prompt, enter `en` to enable privileged mode.

FIGURE 119 Enable privileged mode

```
dean300-1> en
Password: *****
```

3. Enter `show cluster-state` to display the statuses of the node and the cluster.
Before continuing to the next step, verify that both the node and the cluster are in service.

FIGURE 120 Verify that both the node and the cluster are in service

```
dean300-1# show cluster-state
Current Management Service Status : In service
Current Node Status : In service
Cluster Status : In service
Cluster Operation : None
System Mode : None
```

4. Enter the following command to log on to the FTP server and check for available backup files that can be copied to the controller:
`copy <ftp-url> backup-network`
5. If multiple backup files exist on the FTP server, the CLI prompts you to select the number that corresponds to the file that you want to copy back to the controller.

If a single backup file exists, the CLI prompts you to confirm that you want to copy the existing backup file to the controller.

When the controller finishes copying the selected backup file from the FTP server back to the controller, the following message appears:

```
Succeed to copy the chosen file from the remote FTP server
```

6. Enter `show backup-network` to verify that the backup file was copied back to the controller successfully.

FIGURE 121 Verify that the backup file was copied to the controller successfully

```
dean300-1# copy ftp://test:test@192.168.10.83 backup-network
Only one NetworkBackup file (network_20191231011530_5.2.0.0.649.bak) is found. Do you want to copy (or input 'no' to cancel)? [yes/no] yes
Starting to copy the chosen NetworkBackup file (network_20191231011530_5.2.0.0.649.bak) from remote FTP server...
Succeed to copy the chosen file from remote FTP server

dean300-1# show backup-network
```

No.	Created on	Patch Version	File Size
1	2019-12-31 01:15:30 GMT	5.2.0.0.649	3.9KB

7. Run `restore network` to start restoring the contents of the backup file to the current controller.

The CLI displays a list of backup files, and then prompts you to select the backup file that you want to restore to the controller.

8. Enter the number that corresponds to the backup file that you want to restore.

FIGURE 122 Enter the number that corresponds to the backup file that you want to restore

```
dean300-1# restore network
No.      Created on                Patch Version      File Size
-----
1        2019-12-31 01:15:30 GMT     5.2.0.0.649      3.9KB

Please choose a backup to restore or 'No' to cancel: 1
The matched network setting for current system serial number is found from the chosen backup as below:

[Control Plane Interfaces]
Interface  IP Mode  IP Address      Subnet Mask      Gateway
-----
Cluster   DHCP
Control   DHCP
Management Static   10.206.20.239   255.255.252.0    10.206.23.254

Access & Core Separation : Disabled
Default Gateway Interface : Management
Primary DNS Server       : 10.10.10.10
Secondary DNS Server      : 10.10.10.106
Internal Subnet Prefix    : 10.254.1.0/24
Control NAT IP           :

[IPv6 Control Plane Interfaces]
Interface  IP Mode  IP Address      Gateway
-----
Control    Static   2001:b030:2516:110::3012/64  2001:b030:2516:110::1
Management Static   2005:b030:2516:110::3012/64  2005:b030:2516:110::1

Please confirm this network setting, and this action will restart all services (or input 'no' to cancel)? [yes/no] yes
Process had been started before and running...
Starting to stop all SmartZone services..
```

The CLI displays the network configuration that the selected backup file contains.

If the serial number of the current controller matches the serial number contained in one of the backup files, the CLI automatically selects the backup file to restore and displays the network configuration that it contains.

9. Type **yes** to confirm that you want to restore the selected backup file. The controller starts the restore process and performs the following steps:

- a) Stop all services.
- b) Back up the current network configuration.

This will enable the controller to roll back to the current configuration, in case there is an issue with the restore process.

- c) Clean up the current network configuration.

The controller deletes its previous network configuration, including static routes, name server, user defined interfaces, etc.

10. Restore the network configuration contained in the selected backup file.

Backup and Restore

Configuration Backup

11. Restart all services.

When the restore process is complete, the following message appears on the CLI: All services are up!

FIGURE 123 The controller performs several steps to restore the backup file

```
Please confirm this network setting, and this action will restart all services (or input 'no' to cancel)? [yes/no] yes
Process had been started before and running...
Starting to stop all SmartZone services...
Process had been started before and running...
Stop service configurer done!
Wait for (Cassandra,Communicator,EAut,ElasticSearch,EventReader,Greyhound,LogMgr,MdProxy,Mosquitto,MsgDist,NgInX,Northbound,Observer,RabbitMQ,Radi
usProxy,ScgUniversalExporter,Scheduler,SessMgr,StatsHandler,SubscriberManagement,SubscriberPortal,Switchm,Web) down.
Wait for (Cassandra,Communicator,SubscriberManagement) down.
Wait for (Cassandra,SubscriberManagement) down.
Wait for (Cassandra,SubscriberManagement) down.
Wait for (Cassandra,SubscriberManagement) down.
Wait for (Cassandra) down.
Wait for (Cassandra) down.
Wait for (Cassandra) down.
All services are down.
Starting to restore current system network setting...
Starting to start all SmartZone services...
All interfaces get the IP.

=====
Controller IP : IPv4:192.168.10.166 IPv6:2001:b030:2516:110::3012/64
Cluster IP   : 192.168.30.92
Management IP : IPv4:10.206.20.239 IPv6:2005:b030:2516:110::3012/64
=====

/opt/ruckuswireless/wsg/cli/bin/configurer.py(#494): libcommon.SystemTools.runCmd(sCmd, return_message=False): execute CMD [[/opt/ruckuswireless/
sg/auto_scaling/auto_scaling start]]
      total      used      free   shared  buff/cache   available
Mem:   198053980  37314052  150314740  188024   10425188  159439640
Swap:      0           0           0

Wait for (Cassandra,Communicator,EAut,ElasticSearch,EventReader,Greyhound,LogMgr,MdProxy,Mosquitto,MsgDist,NgInX,Northbound,Observer,RabbitMQ,Radi
usProxy,ScgUniversalExporter,Scheduler,SessMgr,StatsHandler,SubscriberManagement,SubscriberPortal,Switchm,Web) up.
Wait for (Cassandra,Communicator,EAut,ElasticSearch,EventReader,Greyhound,LogMgr,MdProxy,Mosquitto,MsgDist,NgInX,Northbound,Observer,RabbitMQ,Radi
usProxy,ScgUniversalExporter,Scheduler,SessMgr,StatsHandler,SubscriberManagement,SubscriberPortal,Switchm,Web) up.
Wait for (Communicator,EAut,EventReader,Greyhound,LogMgr,MdProxy,Mosquitto,MsgDist,NgInX,Northbound,Observer,RabbitMQ,RadiusProxy,ScgUniversalExp
orter,Scheduler,SessMgr,StatsHandler,SubscriberManagement,SubscriberPortal,Switchm,Web) up.
Wait for (Communicator,EAut,EventReader,Greyhound,LogMgr,Mosquitto,NgInX,Northbound,Observer,RabbitMQ,RadiusProxy,ScgUniversalExporter,Scheduler,S
atsHandler,SubscriberManagement,SubscriberPortal,Switchm,Web) up.
Wait for (Communicator,EAut,EventReader,Greyhound,LogMgr,Mosquitto,NgInX,Northbound,Observer,RadiusProxy,ScgUniversalExporter,Scheduler,SessMgr,S
atsHandler,SubscriberManagement,SubscriberPortal,Switchm,Web) up.
Wait for (Communicator,EAut,EventReader,Greyhound,LogMgr,Mosquitto,NgInX,Northbound,Observer,RadiusProxy,ScgUniversalExporter,Scheduler,SessMgr,S
atsHandler,SubscriberManagement,SubscriberPortal,Switchm,Web) up.
Wait for (EAut,RadiusProxy,ScgUniversalExporter,Switchm) up.
Wait for (EAut,RadiusProxy,ScgUniversalExporter,Switchm) up.
Wait for (ScgUniversalExporter,Switchm) up.
Wait for (ScgUniversalExporter,Switchm) up.
Wait for (ScgUniversalExporter,Switchm) up.
All services are up.
Successful operation
```

12. Do the following to verify that the restore process was completed successfully:
 - a) Run show cluster-state to verify that the node and the cluster are back in service.
 - b) Run show interface to verify that all of the network configuration settings have been restored.

FIGURE 124 Verify that the node and cluster are back in service and that the network configuration has been restored successfully

```
dean300-1# show cluster-state
Current Management Service Status : In service
Current Node Status : In service
Cluster Status : In service
Cluster Operation : None
System Mode : None

Cluster Node Information
-----
No.   Name                Role
-----
1     dean300-1-C         LEADER

dean300-1# show interface
Interfaces
-----
Interface      : Control
IP Mode        : DHCP
IP Address     : 192.168.10.166
Subnet Mask    : 255.255.255.0
Gateway        :

Interface      : Cluster
IP Mode        : DHCP
IP Address     : 192.168.30.92
Subnet Mask    : 255.255.255.0
Gateway        :

Interface      : Management
IP Mode        : Static
IP Address     : 10.206.20.239
Subnet Mask    : 255.255.252.0
Gateway        : 10.206.23.254

Access & Core Separation : Disabled
Default Gateway Interface : Management
Primary DNS Server       : 10.10.10.10
Secondary DNS Server     : 10.10.10.106

User Defined Interfaces
-----
```

You have completed importing and applying the network configuration backup from the FTP server to the controller.

Exporting the Configuration Backup to an FTP Server Automatically

In addition to backing up the configuration file manually, you can configure the controller to export the configuration file to an FTP server automatically whenever you click **Backup**.

Follow these steps to back up the configuration file to an FTP server automatically.

1. Go to **Administration > Administration > Backup and Restore**.
2. Select the **Configuration** tab.
3. In Auto Export Backup, you can configure the controller to export the configuration file to an FTP server automatically whenever you back up the configuration file.
 - a. In Auto Export Backup, click **Enable**. In the **Name prefix** field, type the prefix name of the backup file. The maximum length of the prefix name must not be more than 32 characters.
 - b. **FTP Server**: Select the FTP server to which you want to export the backup file.
 - c. Click **Test**. The controller attempts to establish connection to the FTP server using the user name and password that you supplied. If the connection attempt is successful, a success message is displayed. If the connection attempt is unsuccessful, verify that the FTP server details (including the user name and password) are correct, and then click **Test** again.
 - d. Click **OK**.
4. After you verify the controller is able to connect to the FTP server successfully, click **OK** to save the FTP server settings.

Downloading a Copy of the Configuration Backup

After you create a configuration backup, you have the option to download the backup file from the **System Configuration Backups History** section.

1. Go to **Administration > Administration > Backup and Restore**.
2. Select the **Configuration** tab.
3. Locate the entry for the backup file that you want to download. If multiple backup files appear on the list, use the date when you created the backup to find the backup entry that you want.
4. Click **Download**.

Your web browser downloads the backup file to its default download folder. NOTE: When your web browser completes downloading the backup file, you may see a notification at the bottom of the page.

5. Check the default download folder for your web browser and look for a file that resembles the following naming convention: **[Name prefix]_Configuration_[datetime]_[Version].bak**

The controller will combine the prefix name with the date and time stamp to generate the filename for automatic backup. For example, RUCKUS_Configuration_20200902071625GMT_6.0.0.0.817.bak.

Restoring a System Configuration Backup

In the event of a failure or emergency where you may need to go back to the previous version of a cluster, you will have to restore your system configuration backup and restart the cluster.

1. Go to **Administration > Administration > Backup and Restore**.
2. Select the **Configuration** tab.

Backup and Restore

Configuration Backup

3. Once you locate the backup file, click **Restore** that is in the same row as the backup file. A confirmation message appears.

NOTE

Take note of the backup version that you are using. At the end of this procedure, you will use the backup version to verify that the restore process was completed successfully.

4. Click **Yes**. The following message appears: `System is restoring. Please wait...` When the restore process is complete, the controller logs you off the web interface automatically.
5. Log on to the controller web interface.
Check the web interface pages and verify that the setting and data contained in the backup file have been restored successfully to the controller.

Backed Up Configuration Information

The following list show which configuration information will be backing up.

- AP zones
- AP zone global configuration
- Zone templates
- WLAN templates
- AP registration rules
- Access point information
- General system settings
- Web certificate
- SNMP agent
- Alarm to SNMP agent
- Cluster planes
- Management interface ACL
- Domain information
- User credentials and information
- Mobile Virtual Network Operators (MVNO) information

Backing Up and Restoring Configuration

Configuration backup creates a backup of all existing configuration information on the controller. In addition to backing up a different set of information, configuration backup is different from cluster backup in a few ways:

- The configuration backup file is smaller, compared to the cluster backup file.
- The controller can be configured to back up its configuration to an external FTP server automatically.
- Configuration backup does not back up any statistical files or general system configuration.



© 2024 CommScope, Inc. All rights reserved.
350 West Java Dr., Sunnyvale, CA 94089 USA
<https://www.commscope.com>