CONFIGURATION GUIDE

RUCKUS SmartZone 300 and Virtual SmartZone-High Scale Administrator Guide, 6.1.0

Supporting SmartZone Release 6.1.0

Part Number: 800-72934-001 Rev K
Publication Date: November 2024

© 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
New In This Document....11

Monitor....13
Dashboard....13
Navigating the Dashboard....13
Wireless....26
Wired....47
Monitoring Access Points....47
Clients....67
Working with Wireless Clients....67
Working with Wired Clients....69
Switch Clients....70
Troubleshooting and Diagnostics....70
Troubleshooting....70
Support Bundle....75
Scripts....77
Application Logs....82
Radius Proxy....84
Reports....85
Report Generation....85
Rogue Devices....87
Historical AP Client Stats....88
Ruckus AP Tunnel Stats....89
Core Network Tunnel Stats....92
Events and Alarms....94
Events....94
Alarms....101

Network....103
Working with Wireless Network....103
Working With Access Points....103
Working with WLANs and WLAN Groups....182
Configuring AP Settings....217
Working with Maps....228
Working with Switches....235

Managing ICX Switches from SmartZone 235
SmartZone Switch Management 244
Troubleshooting Switch Issues 333
Viewing Switches on the Dashboard 342
Working with Data and Control Plane 346
Viewing the System Cluster Overview 346
Control Planes and Data Planes 347
Interface and Routing 347
Displaying the Chassis View of Cluster Nodes 348
Cluster Redundancy 348
Configuring the Control Plane 358
Configuring the Data Plane 362
Monitoring Cluster Settings 365
Creating a DP Group 366
Enabling Flexi VPN 370
Enabling L3 Roaming Criteria for DP 370
Powering Cluster Back 371

Security 373
Application Control 373
Viewing Application Control Summary 373
Creating an Application Control Policy 373
Working with Application Signature Package 376
Creating an User Defined Application 377
Access Control 378
Managing a Firewall Profile 378
Create an L3 Access Control Policy 380
Creating an L2 Access Control Service 382
URL Filtering 384
Creating a Device Policy 390
VLAN 393
Users and Roles 397
Guests 401
Dynamic PSK 412
Creating a User Traffic Profile 414
Restricted Access 414
Creating Blocked Clients 420
Creating a Client Isolation Whitelist 421
Creating Time Based Access Table 422
Creating a Traffic Class Profile 423
Classifying Rogue Policy 426
Authentication 427
Creating Non-Proxy Authentication AAA Server 427
Creating Proxy Authentication AAA Servers 429
Authentication Support Matrix 434
Non-Proxy (Social Login) 438
Creating Realm Based Authentication Profile 439
Fast Initial Link Setup (FILS) 440
Accounting 441
Creating Non-Proxy Accounting AAA Servers 441
Creating Proxy Accounting AAA Servers 443

Creating Realm Based Proxy....444

Services....447

Working with Hotspots and Portals....447

Creating a Guest Access Portal....447

Working with Hotspot (WISPr) Services....450

Working with Hotspot 2.0 Services....453

Creating a Web Authentication Portal....461

Creating a UA Blacklist Profile....463

Creating a Portal Detection and Suppression Profile....464

Creating a WeChat Portal....466

Creating Network Segmentation Profile on the vSZ Controller....468

Working with Tunnels and Ports....472

Creating a Ruckus GRE Profile....472

Creating a Soft GRE Profile....474

Creating an IPsec Profile....476

Creating an Ethernet Port Profile....479

Creating a Tunnel DiffServ Profile....483

Communications Assistance for Law Enforcement Act (CALEA)....485

Enabling Tunnel Encryption....485

Forwarding Multicast Packets....486

Split Tunnel Profile....486

Creating a Bond Port Profile....488

Managing Core Network Tunnels....489

SoftGRE Support....492

Working with DHCP....496

DHCP/NAT....496

Network Topology....497

Hierarchical Network Topology....499

Configuring AP-based DHCP Service Settings....499

Creating an AP DHCP Pool....505

Creating Profile-based DHCP....506

Creating Profile-based NAT....508

Configuring DHCP/NAT with Mesh Options....510

Working with Other SmartZone Services....511

Understanding WiFi Calling....511

Bonjour....515

3rd Party Service....522

Vendor-Specific Attribute (VSA) Profile....522

Creating a DNS Spoofing Profile....526

Enabling Global SNMP Notifications....527

AP SNMP Agent Profile....529

Creating an External Syslog Server Profile....532

Administration....535

System....535

System Info....535

Time....545

Syslog....550

Certificates....552

Templates....561

DNS Servers 569
External Services 572
Ruckus Services 572
Northbound Data Streaming 580
WISPr Northbound Interface 583
SNMP Agent 583
FTP 585
SMTP 585
SMS 586
Administration 587
Admins and Roles 587
Backup and Restore 617
Upgrade 637
MVNO 648
Licenses 649
ZD Migration 655
Admin Activities 656
Help 657
Rest API 657
Ports to open for AP-Controller Communication 657
Replacing Hardware Components 664
vSZ-H SSID Syntax 673
Web Server Support 676

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	`device(config)# interface ethernet 1/1/6`
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**.
italics	Publication titles	Refer to the *RUCKUS Small Cell Release Notes* 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.
italic text	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, *member*[*member*...].
\	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

- New In This Document..... 11

New In This Document

TABLE 2 Key Features and Enhancements in SmartZone 6.1.0

Feature	Description	Reference
Doc-defect SCG-161149	The controller does not support built-in QR code feature.	The "Viewing Generated DPSKs" topic is removed.

Monitor

- Dashboard..... 13
- Clients..... 67
- Troubleshooting and Diagnostics..... 70
- Reports..... 85
- Events and Alarms..... 94

Dashboard

Navigating the Dashboard

Setting Up the Controller for the First Time

The controller must first be set up on the network.

> **NOTE**
> Setting up the controller is described in the Getting Started Guide or Quick Setup Guide for your controller platform.

For information on how to set up the controller for the first time, including instructions for running and completing the controller's *Setup Wizard*, see the *Getting Started Guide* or *Quick Setup Guide* for your controller platform.

> **NOTE**
> While deploying vSZ, iSCSI must be used for block storage and make the hosts see everything as Direct-attached storage (DAS) for real-time database access/synchronisation as it requires lower latency and a high number of r/w transactions. Due to higher r/w latency, SAN and NAS might not be suitable for vSZ deployment.

You can deploy vSZ and vSZ-D via vCenter 6.7 on ESXi. Some of the new features (for example, location based services, rogue AP detection, force DHCP, and others) that this guide describes may not be visible on the controller web interface if the AP firmware deployed to the zone you are configuring is earlier than this release. To ensure that you can view and configure all new features that are available in this release, RUCKUS recommends upgrading the AP firmware to the latest version.

Logging On to the Web Interface

Before you can log on 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 web interface on any computer that can reach the Management (Web) interface on the IP network.

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

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

   Supported web browsers include:

   - Google Chrome
   - Safari
   - Mozilla Firefox

- Internet Explorer
- Microsoft Edge

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

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

   > **NOTE**
   > The controller web interface requires an **HTTPS** connection. You must append https (not **http**) to the Management interface IP address to connect to the web interface. If a browser security warning appears, this is 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.

   The controller web interface logon page appears.

3. Log on to the controller web interface using the following logon details:
   - **User Name**: **admin**
   - **Password**: {**the password that you set when you ran the Setup Wizard**}
4. Click **Log On**.

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

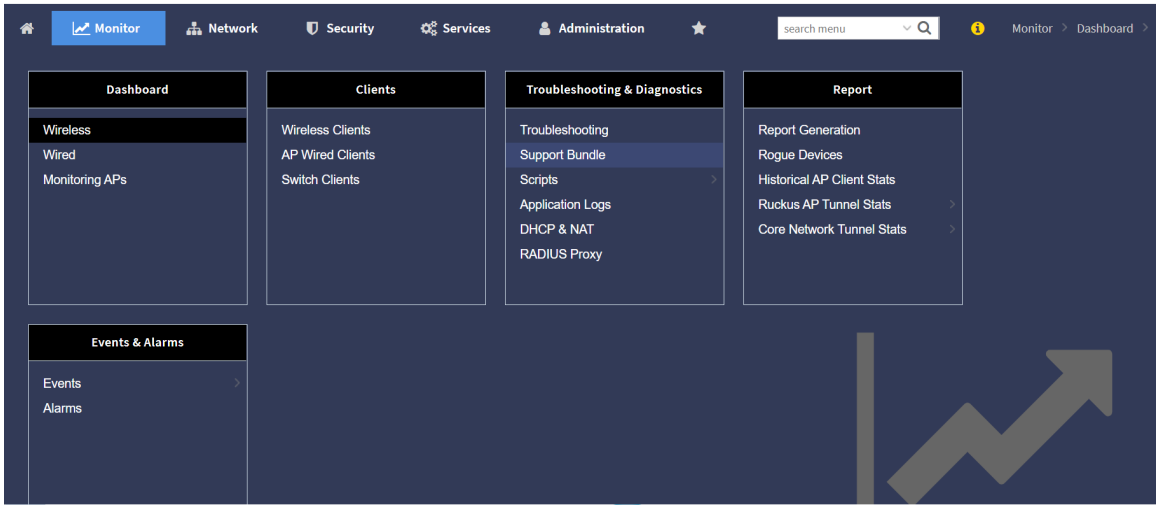
Web Interface Features

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

You can use it to:

- 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 back-up and restoring system configuration, upgrading the cluster, downloading support, performing system diagnostic tests, viewing the status of controller processes, and uploading additional licenses (among others).

FIGURE 1 Controller Web Interface Features



The following table describes the web interface features.

TABLE 3 Controller Web Interface Features

Feature	Description	Action
Main Menu	Lists the menus for administrative task.	Select the required menu and sub-menu.
Tab Page	Displays the options specific to the selected menu.	Select the required tab page.
Content Area	Displays tables, forms, and information specific to the selected menu and tab page.	View the tables, forms and information specific to the selected menu, sub-menu and tab page. Double-click an object or profile in a table, for example: a WLAN, to edit the settings.
Header Bar	Displays information specific to the web interface.	Select the required option (from left to right): • Warning—Lists the critical issues to be resolved. • System Date and time—Displays the current system date and time. • Refresh—Refreshes the web page. • Global filter—Allows you to set the preferred system filter. • My Account link—Allows you to: – Change password – Set session preference – View account activities such as login information and privilege changes – Log off • Online Help—Allows access to web help.

You can also use the  icon to expand and shrink the main menu. Shrinking the main menu increases the size of the content area for better readability and viewing.

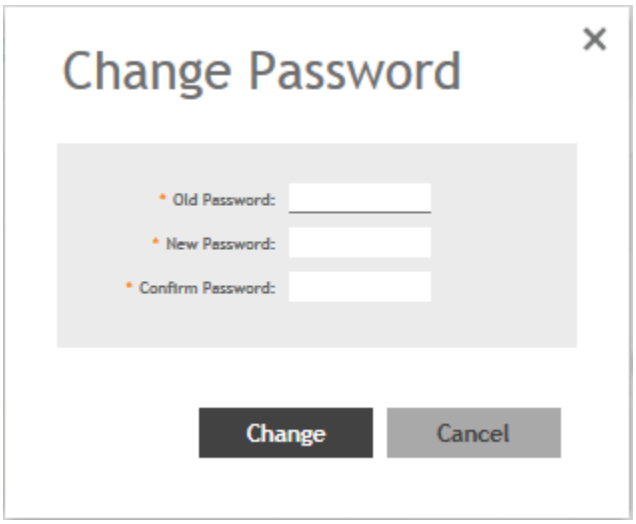
Changing the Administrator Password

Follow these steps to change the administrator password.

1. On the controller web interface, select **Change Password** from the **default** list.

The following window appears.

FIGURE 2 Change Password Form



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.

Setting User Preferences

You can configure the language in which the user interface must appear, and also customize the session tie for the interface.

1. On the controller web interface, select **Preferences** from the **default** list.

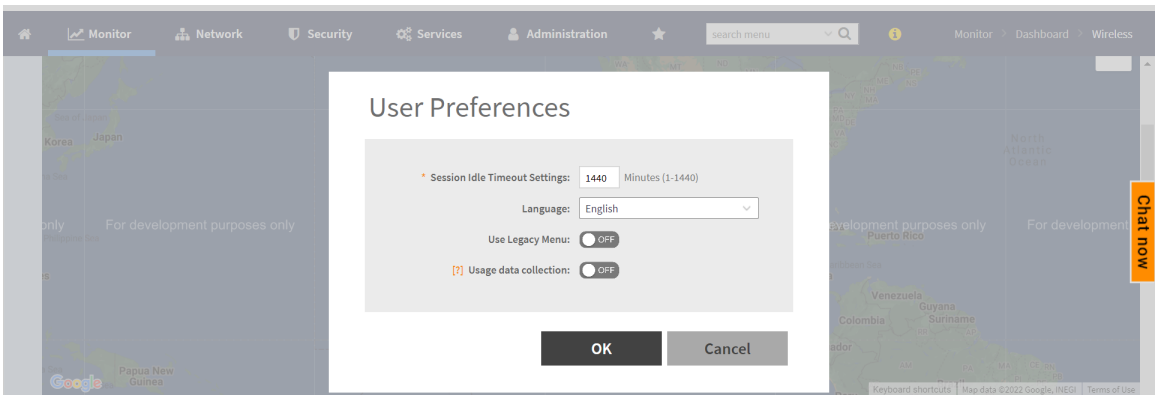
   The **User Preferences** page is displayed.
2. In Session Timeout Setting, enter the duration the web interface session must last for, in minutes.

3. In Language, select the language that you want to view the web interface in.

   The following languages are supported:

   - Spanish
   - Brazilian Portugese
   - French
   - German
   - Italian
   - Russian
   - Simplified Chinese
   - Traditional Chinese
   - Korean
   - Japanese

   FIGURE 3 User Preferences



Logging Off the Controller

You must be aware of how to log off the controller using the web interface and the CLI.

1. On the controller web interface, select **Log off** from the **default** list.

   The following message appears: `Are you sure you want to log off?`

2. Click **Yes**.

The controller logs you off the web interface and the logon page appears.

You have completed logging off the web interface.

You can also use CLI commands to shutdown the controller.

To shutdown the controller, use the following command: **shutdown** and specify the number of seconds before controller is shutdown.

To shutdown the controller immediately, use the following command: **shutdown now**. The controller will shutdown in 30 seconds.

Configuring Global Filters

The Global filter setting allows you to set your preferred system filter.

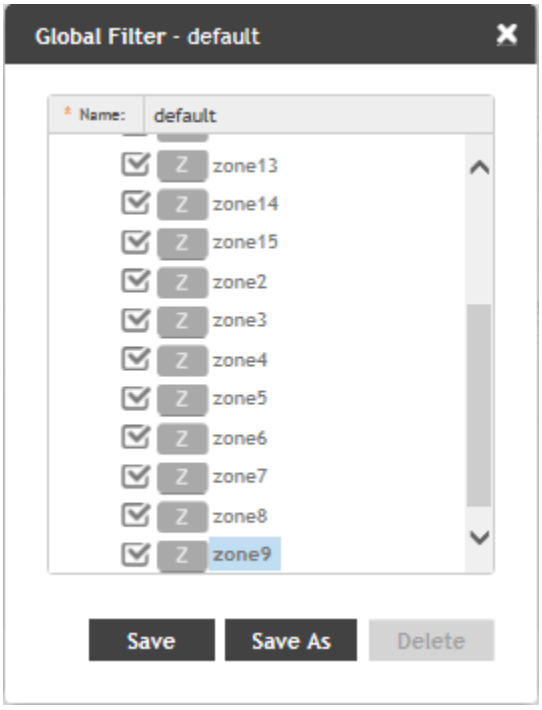
Global filters allow the administrator to define a system scope or system context that applies to all pages of the system as they navigate to different menus. For example, if your system includes 5 zones, but you want to view Zone1 and Zone2 only, you can create and apply such a filter. As you navigate throughout the system, the view will be restricted to show only the data, objects, and profiles contained within Zones 1 and 2.

To set the global filter:

1. On the controller web interface, click . The **Global Filter - default** page is displayed.

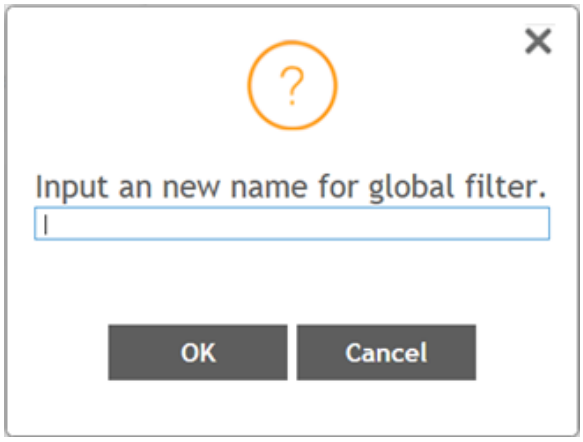
   The below figure appears.

   FIGURE 4 Global Filter Form



2. Select or clear the required system filters and click
   - **Save**—To save the filter settings with the default group.
   - **Save As**—To save the filter settings as a new group. The below figure appears. Enter a new name for the group and click **OK**.

FIGURE 5 New Name Form



NOTE

You can delete the filter setting. To do so, click the Filter setting button. The Global Filter form appears, click **Delete**.

Warnings and Notifications

This section explains about warnings and notifications.

Warnings

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

FIGURE 6 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

Setting 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 the “Managing Alarms and Events” chapter.

Alarm severity are of three types:

- Minor
- Major
- Critical

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

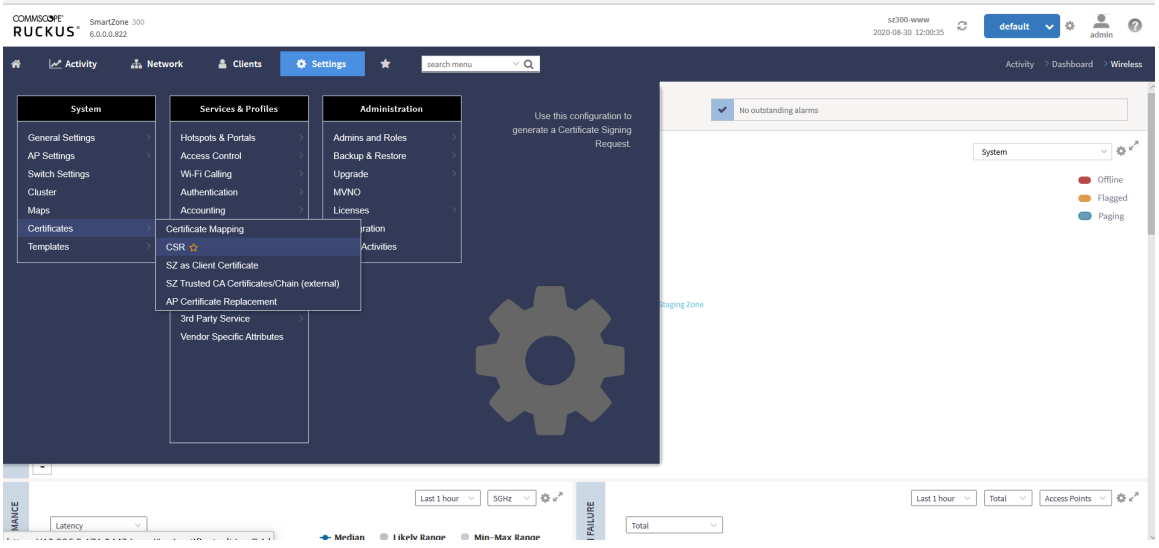
1. From the Notifications area, Click the Setting button. The Settings - Global Notification form appears.
2. From the **Lowest alarm severity** drop-down, select the required severity level.
3. Click **OK**. Notifications corresponding to the selected alarm severity and severity above it are displayed in the Notification area of the Dashboard.

GUI Usability Enhancement

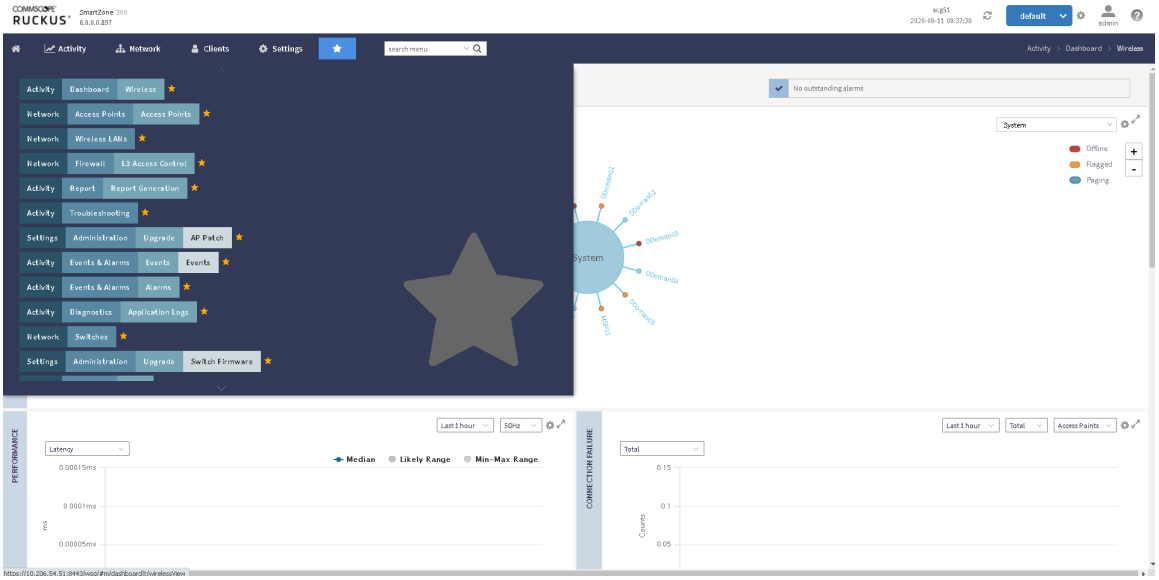
The dashboard outlook has been changed in 6.0 release.

In 6.0 the description is displayed on the right hand side for each menu available on the left hand side.

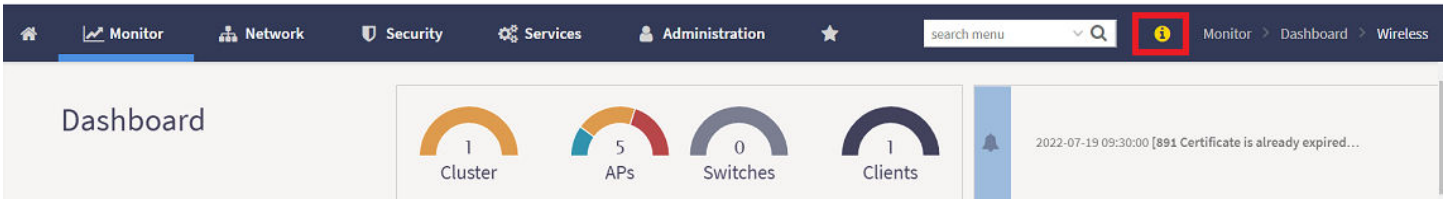
You can enter a search string in the Search Menu field in the menu bar to be directed to requested option.



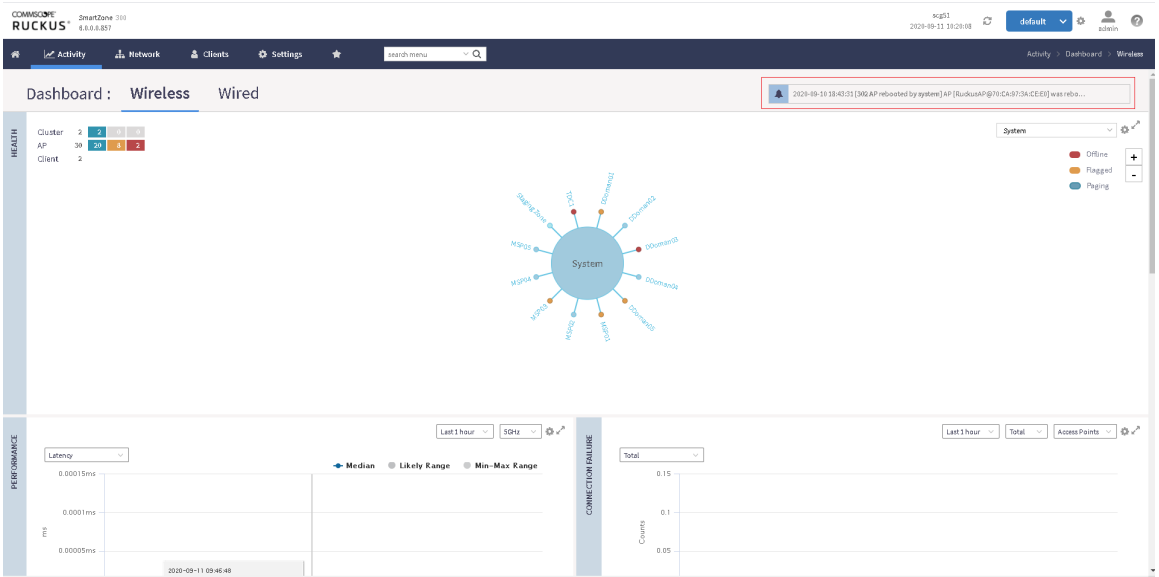
You can click the star icon to access the Favorites list.:

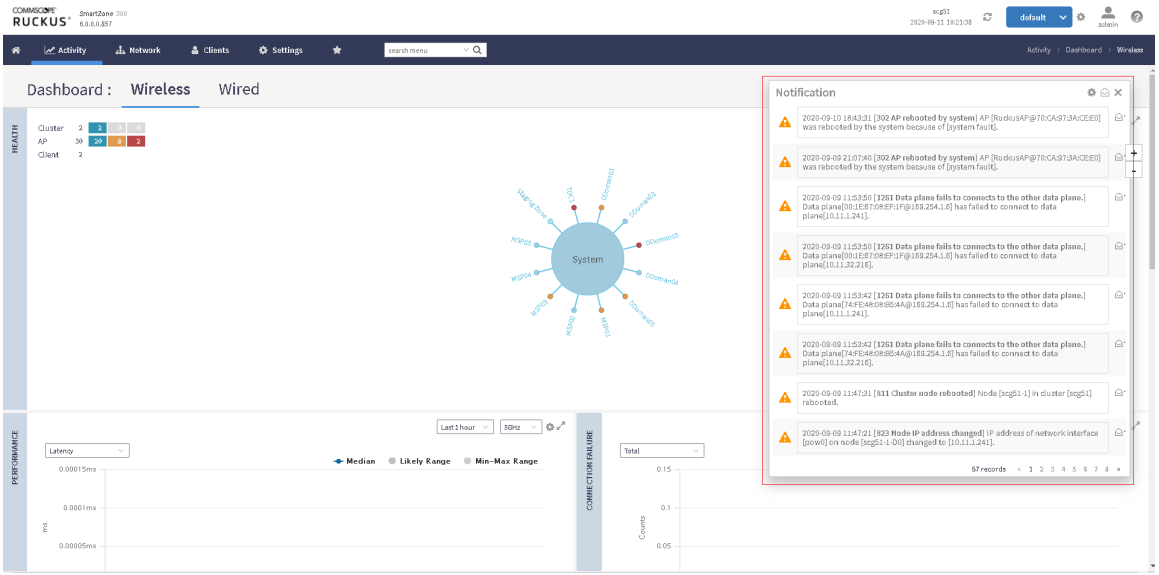


Click **i** icon to access the RUCKUS Analytics Free Trial offer.

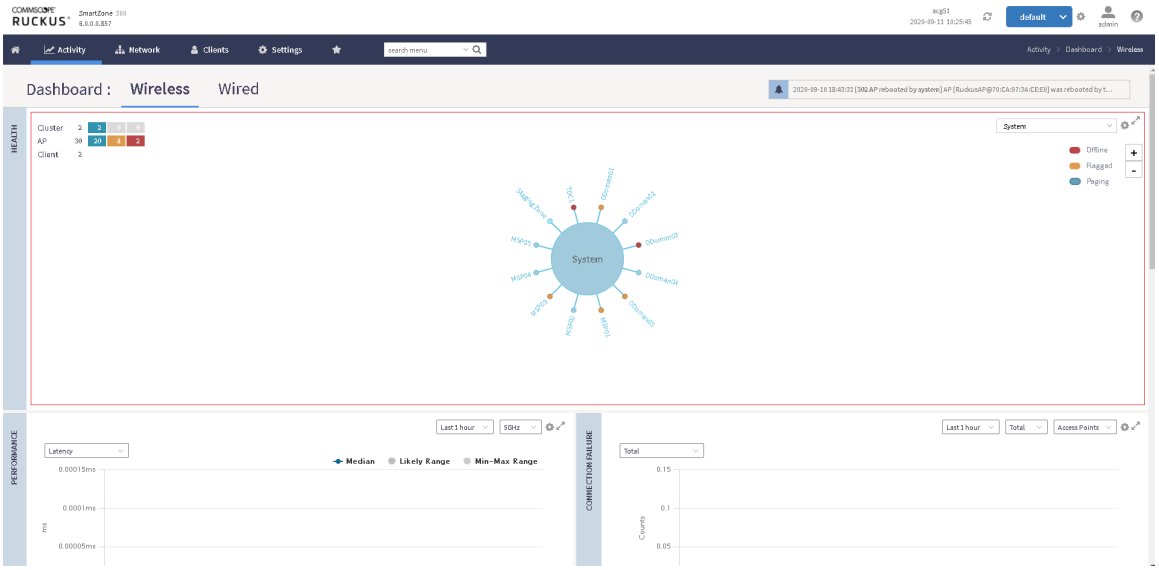


Following are the new UI styles for notification:

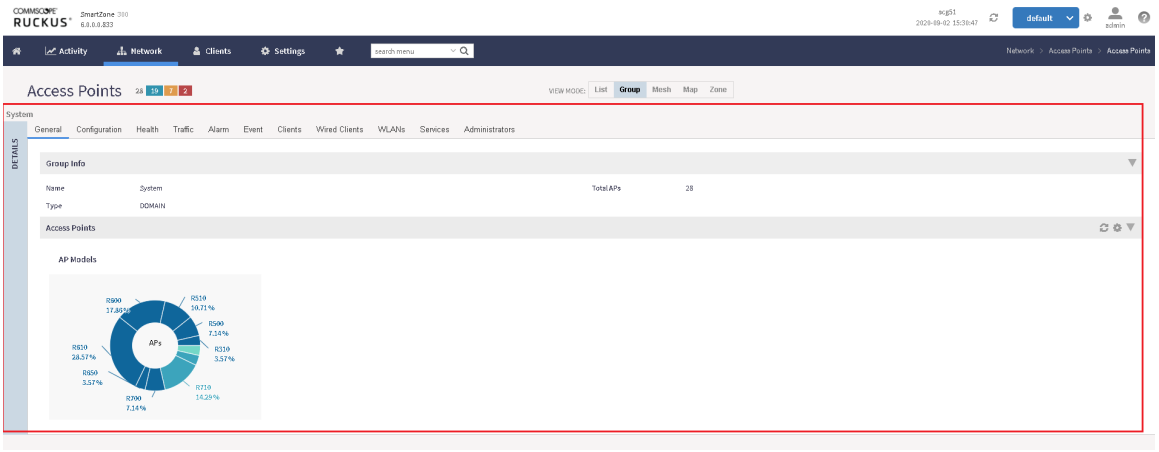




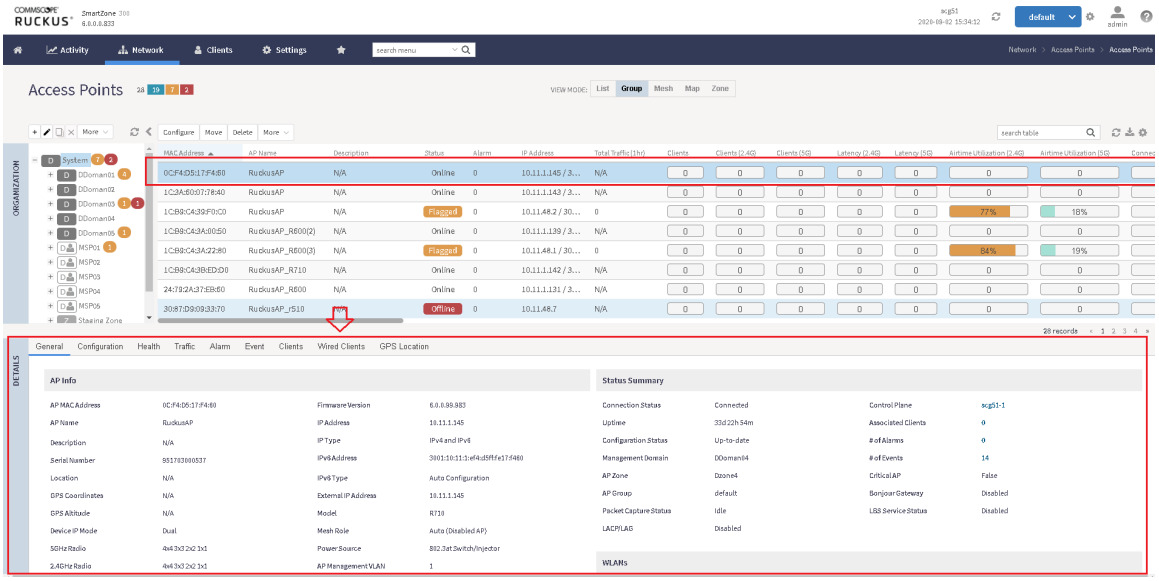
New group topology chart and new style for indicators(Online/Flagged/Offline).



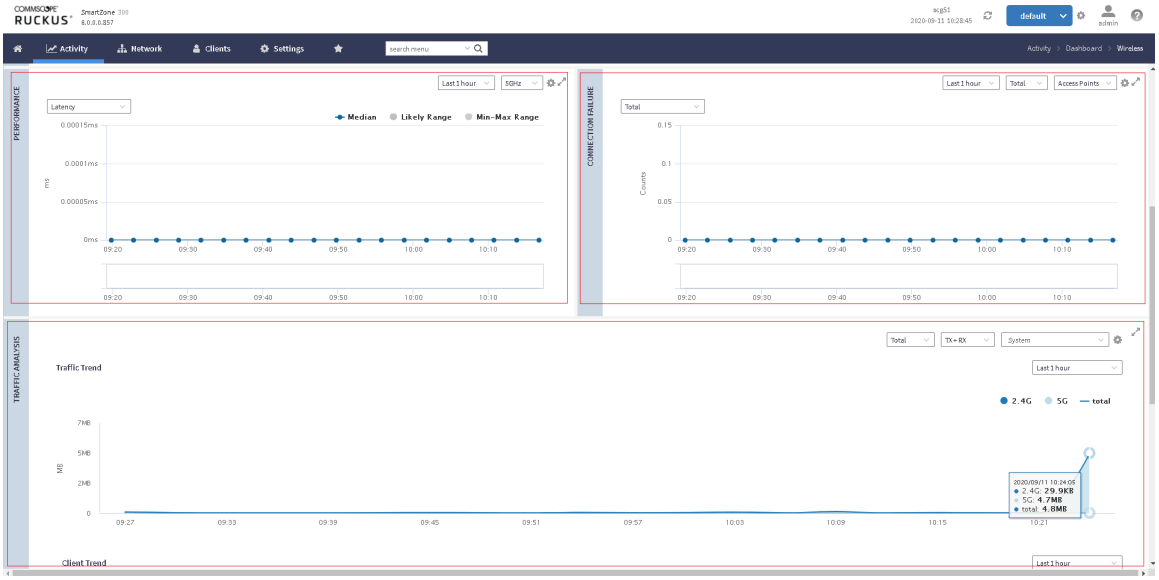
In APs/WLANs/Switches/Wireless Clients page, it can enlarge the detail section.

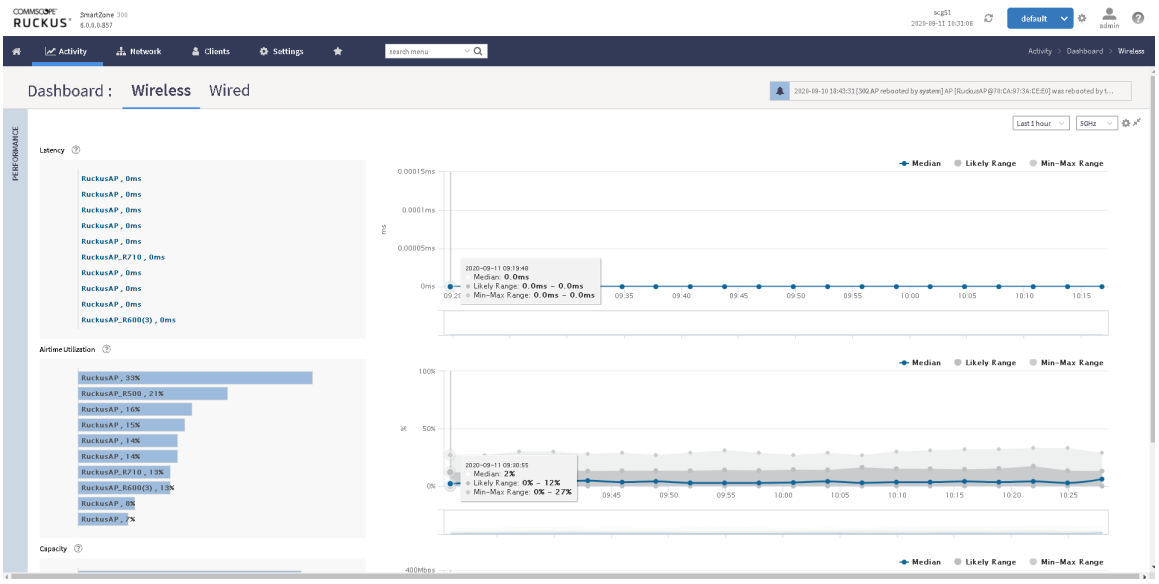


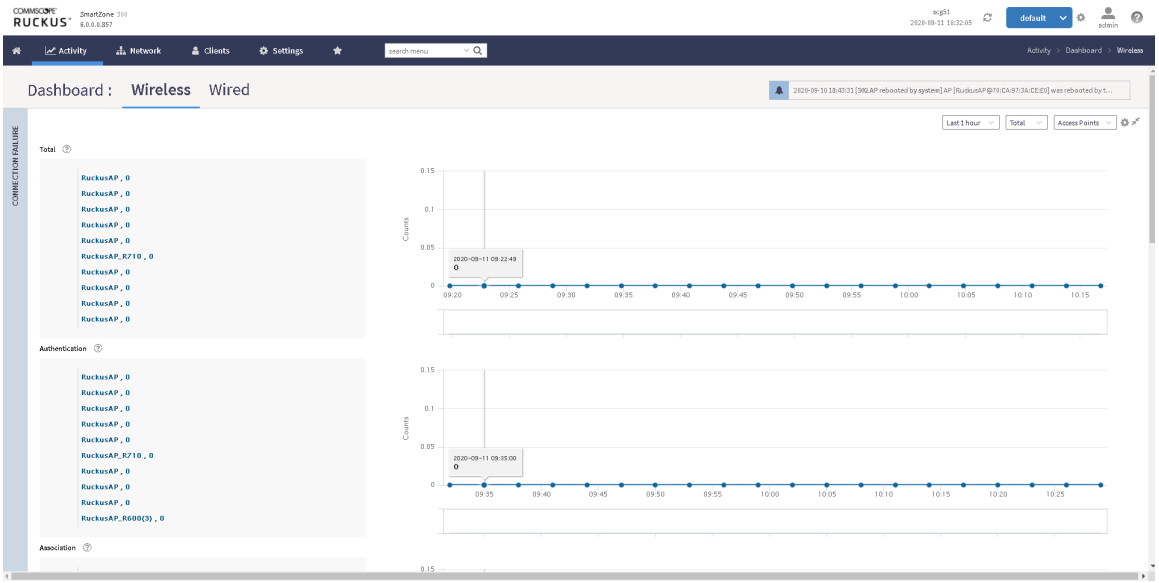
Click AP to see ap detail information, this is new layout for two columns display.

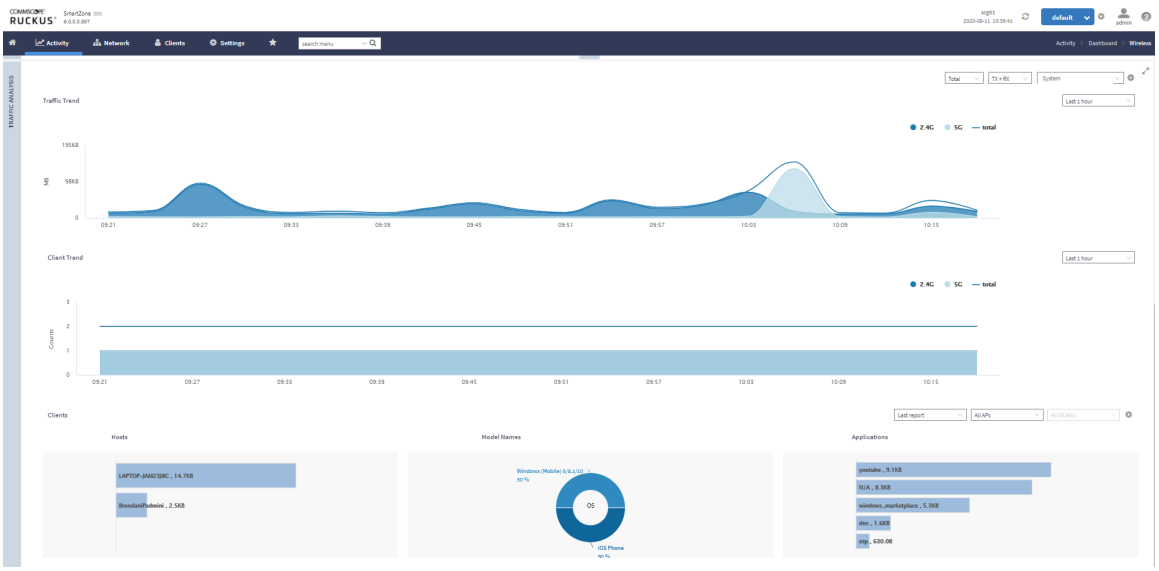


Enable the preview with Performance, Connection Failure and Traffic analysis is a new feature added to the GUI.


RUCKUS
Activity
Network
Clients
Settings
PERFORMANCE
Latency
Median
Likely Range
Min-Max Range
CONNECTION FAILURE
Total
Access Points
TRAFFIC ANALYSIS
Traffic Trend
2.4G
5G
total
Client Trend


RUCKUS
Activity
Network
Clients
Settings
Dashboard : Wireless Wired
PERFORMANCE
Latency
Median
Likely Range
Min-Max Range
Airtime Utilization
Capacity





UI Performance Tuning

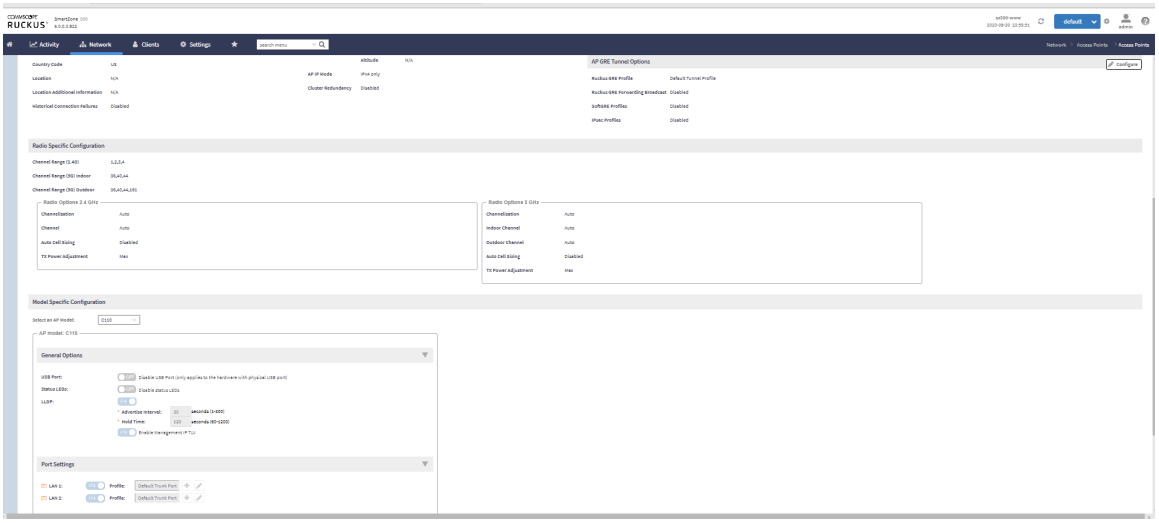
Navigate between the tabs: In 6.0 the user response is first and rendering the page last.

Compared to the previous version, we are directly guided to the page required without the time delay. So navigation is faster.

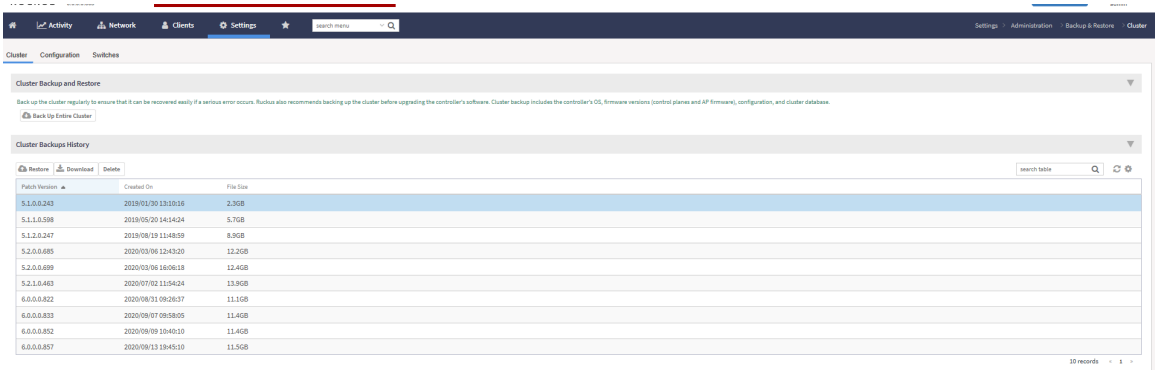
The height of the bar is adjusted dynamically for the display items as minimum 25 px height.

Click the panel headers to enlarge the preview section.

In the Network>Access point>Configuration , a floating Configure button is provided , to facilitate configuration at any moment while we are in the page.



In the GUI settings>Backup and Restore>Configuration a new download tab has been introduced.



Consistency in enable/disable, on/off elements

The checkboxes is "Allow Band Balancing" and enabled by default.

"Collect statistics from unauthorized clients" and enabled by default

"Broadcast SSID" and enabled by default.

Wireless

Viewing Information about a Wireless Client

You can view more information about a wireless client, including its IP address, MAC address, operating system, and even recent events that have occurred on it.

Follow these steps to view information about a wireless client.

1. Go to **Monitor** > **Clients** > **Wireless Clients**.
2. From the list of wireless clients, locate the client whose details you want to view.

3. Under the **MAC Address** column, click the MAC address of the wireless client.

   The **Associated Client** page appears and displays general information about the wireless client.

   - General: Displays general client information.
   - Health: Displays information about the real-time health of the client. It displays graphical trends based on the signal-to-noise ratio (SNR) and data rate. You can use the **Start** and **Stop** option to review client health at real time.
   - Traffic: Displays historical and real-time traffic information.
   - Event: Displays information about events associated with the client.

Viewing a Summary of Wireless Clients

You can view a summary of wireless clients that are currently associated with all of your managed APs.

You can view a summary of wireless clients associated with all of your managed APs. From the dashboard, go to **Monitor** > **Clients** > **Wireless Clients.**

The **Wireless Clients** tab displays a table that lists all clients currently associated with your managed APs.

> **NOTE**
> To view wireless clients that belong to a particular zone, click the zone name in the zone tree. The table refreshes, displaying only the clients that belong to the zone you selected.

The following table lists details for the wireless client.

> **NOTE**
> Not all the columns listed in the following table are displayed by default. To display columns that are currently hidden, click the gear icon in the upper-right corner of the table, and select the check boxes for the columns that you want to display.

Click the  icon to export the data into a CSV file.

> **NOTE**
> For 802.1X (WPA2, WPA3) and MAC-auth, WLAN Advanced Option has the Session Timeout configuration. If the Access-Accept of AAA does not include the session timeout, the Session Timeout configuration value is used as the default value. The range is from 120 to 864000 seconds (10 days.) The default value is 172800 seconds (2 days).

TABLE 4 Wireless Client Details

Column Name	Description
Hostname	Displays the hostname of the wireless client
OS Type	Displays the operating system that the wireless client is using
IP Address	Displays the IP address assigned to the wireless client
MAC Address	Displays the MAC address of the wireless client
WLAN	Displays the name of the WLAN with which the client is associated
AP Name	Displays the name assigned to the access point
AP MAC	Displays the MAC address of the access point
Traffic (Session)	Displays the total traffic (in KB, MB, GB, or TB) for this client in this session
Traffic (Uplink)	Displays the total uplink traffic (in KB, MB, GB, or TB) for this client in this session
Traffic (Downlink)	Displays the total downlink traffic (in KB, MB, GB, or TB) for this client in this session

TABLE 4 Wireless Client Details (continued)

Column Name	Description
RSSI	Displays the Received Signal Strength Indicator (RSSI), which indicates how well a wireless client can receive a signal from an AP. The RSSI value is shown in decibels (dB) and displayed as either the real-time value or the average value over the past 90 seconds.
SNR	Displays the Signal-to-Noise Ratio (SNR), which indicates the signal strength relative to background noise. The SNR value is shown in decibels (dB) and displayed as either the real-time value or the average value over the past 90 seconds.
Radio Type	Displays the type of wireless radio that the client supports. Possible values include 11b, 11g, 11g/n, 11a, 11a/g/n,11ac, and 11ax.
VLAN	Displays the VLAN ID assigned to the wireless client
Channel	Displays the wireless channel (and channel width) that the wireless client is using
CPE MAC	Displays the WLAN MAC address of the customer premises equipment
User Name	Displays the name of the user logged in to the wireless client
MCS Rate (Tx) (Rx)	Displays the median Tx and Rx Modulation and Coding Scheme rates for both client and APs on their respective pages. These values are updated every 180 seconds (High Scale) and 90 seconds (Essentials).
Effective Data Rate	Displays the real traffic transmit rate of the wireless client
Auth Method	Displays the authentication method used by the AP to authenticate the wireless client
Auth Status	Indicates whether the wireless client is authorized to access the WLAN service
Encryption	Displays the encryption method used by the access point
Control Plane	Displays the name of the SmartZone node to which the AP's control plane is connected
Packets to	Displays the downlink packet count for this session
Packets from	Displays the uplink packet count for this session
Packets dropped	Displays the downlink packet count that has been dropped for this client
Session start time	Indicates the session creation time

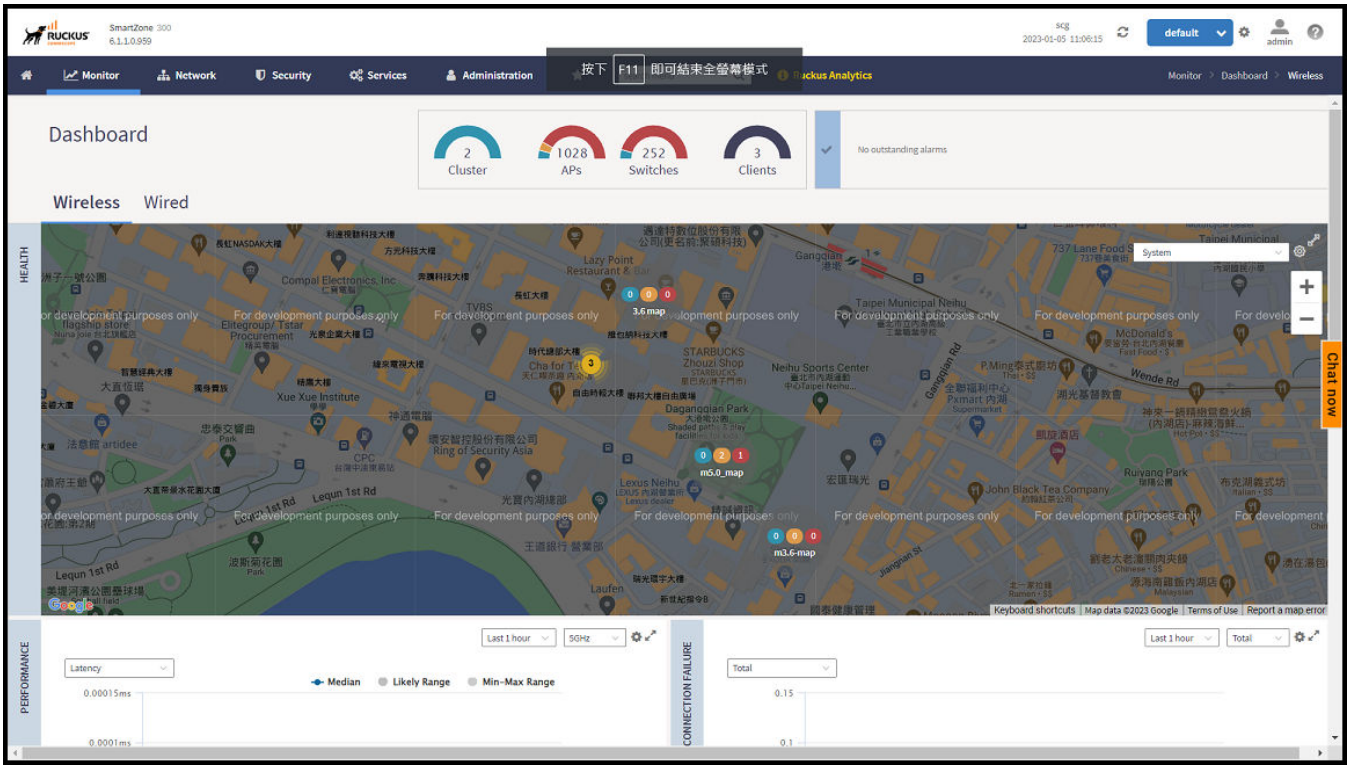
Health and Maps

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.

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 7 Health Workspace area



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

For more information on customizing the information displayed on the Health dashboard, see the “Customizing Health Status Thresholds” section.

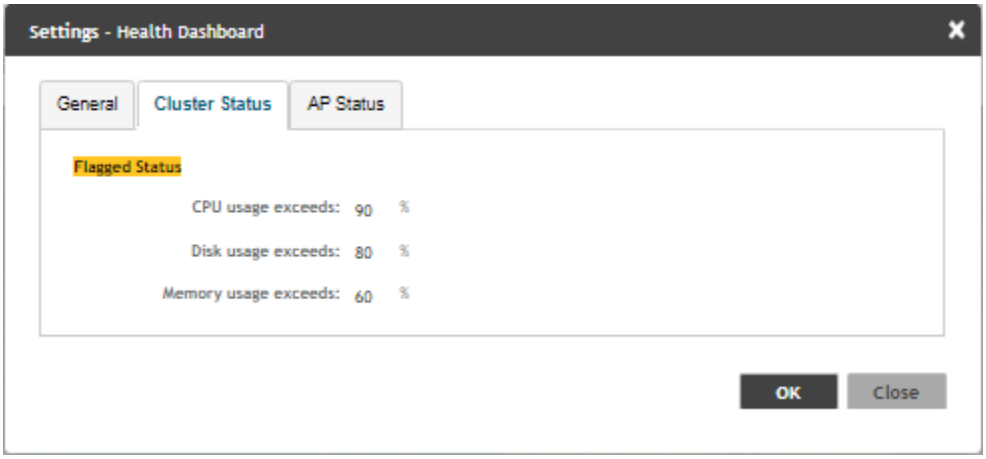
Customizing Health Status Thresholds

You can customize the way SmartZone 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** form, 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. For more information, see the “Customizing AP Flagged Status Thresholds” section.

FIGURE 8 Setting Cluster Health Status Thresholds



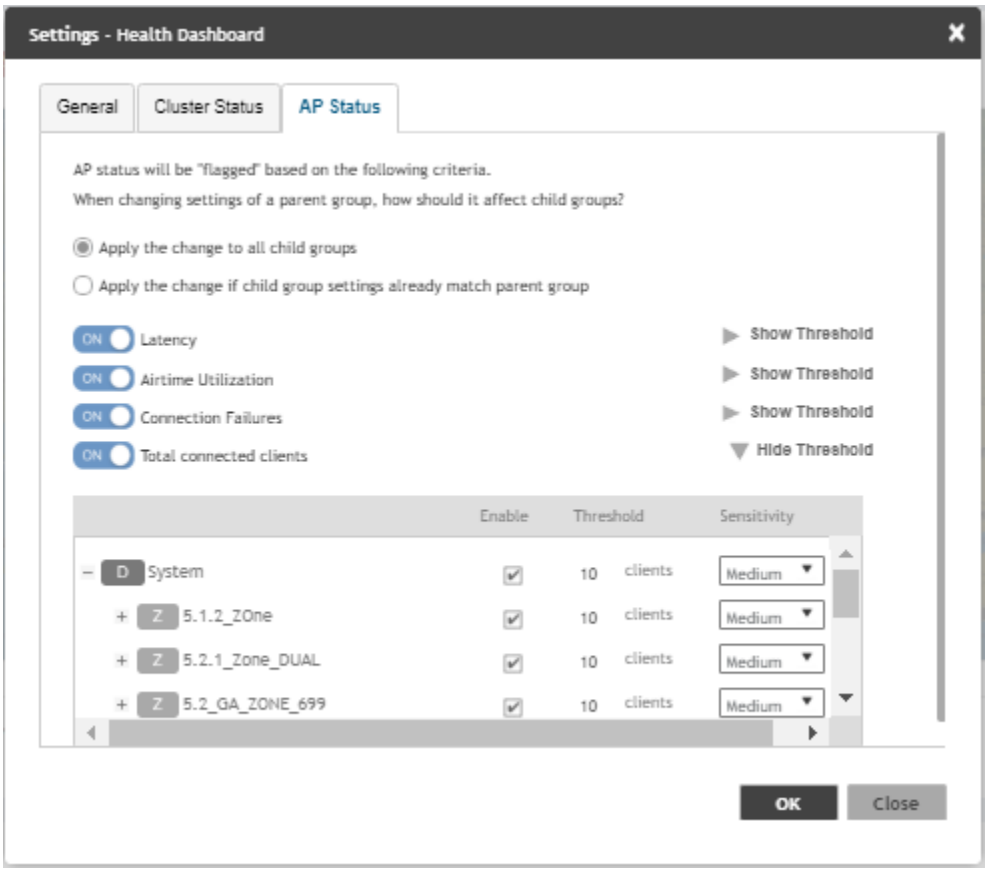
Customizing AP Flagged Status Thresholds

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** form 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 / 5 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 9 Configuring AP Flagged Status Thresholds



SCI Thresholds for each AP

The following are the thresholds from SCI for each AP.

The below thresholds provided is based on per AP model.

TABLE 5 SCI Thresholds

Resource	Low Threshold	Normal Threshold Range	High Threshold Range
CPU	Less than 25%	Between 25% to 75%	Greater than 75%
Memory	Less than 2GB	Between 2GB to 8GB	Higher than 8GB
Hard Disk	Less than 50GB	Between 50GB to 100GB	Higher than 100GB

Using the Health Dashboard Map

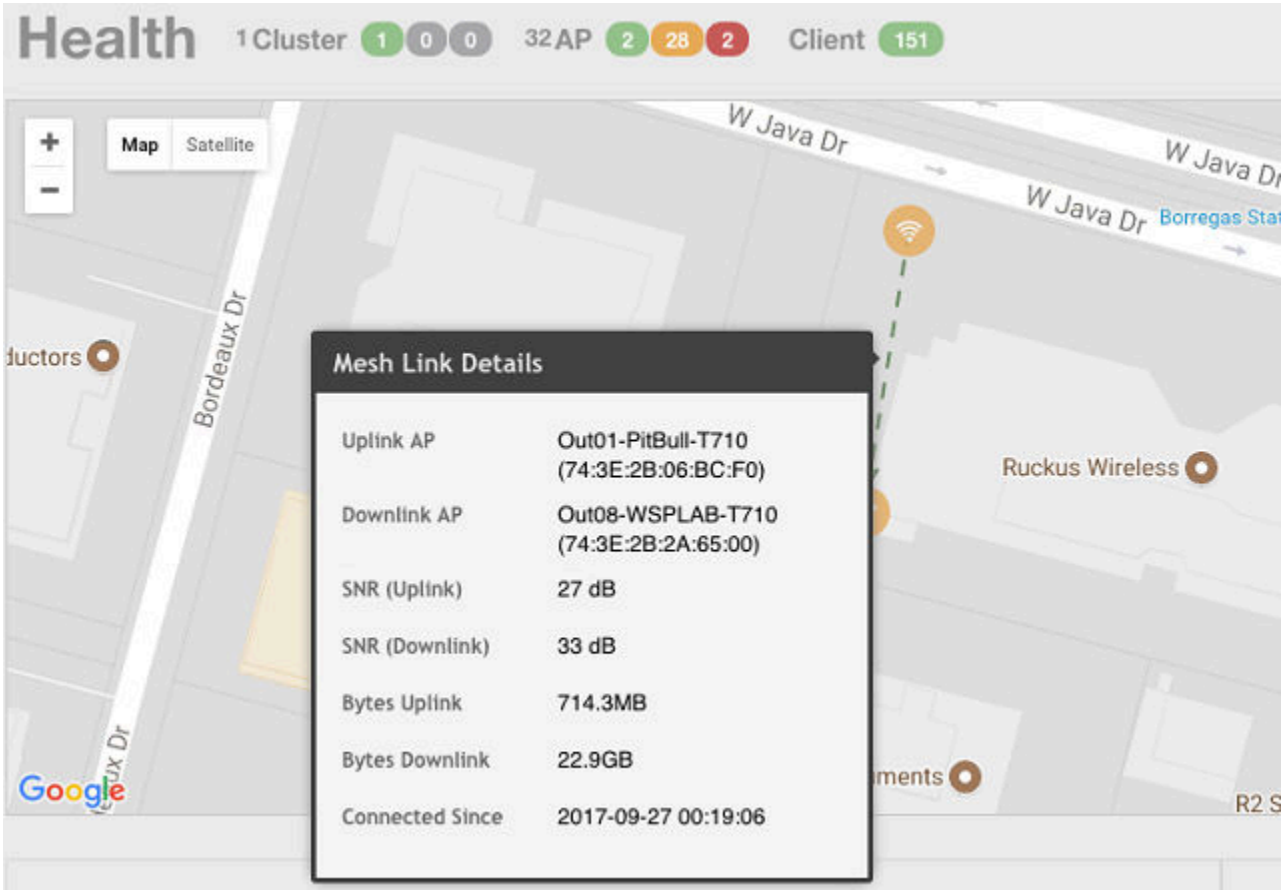
Use the Google Maps view just as you would normally use Google Maps - including zoom, satellite view, rotate and even street view icons. You can customize the AP icon information displayed on the map using the tools in the upper-right hand corner.

Use the **Settings** (gear) 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 check-box 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.

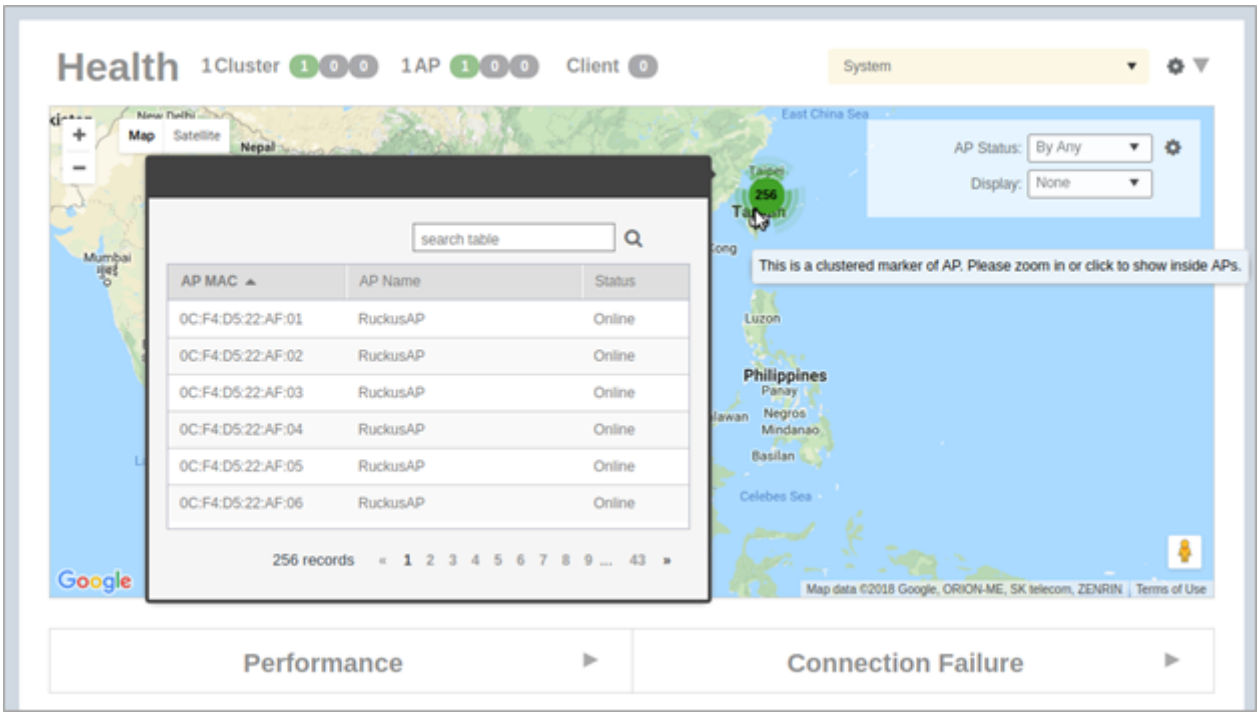
FIGURE 10 Mesh Link Details



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:

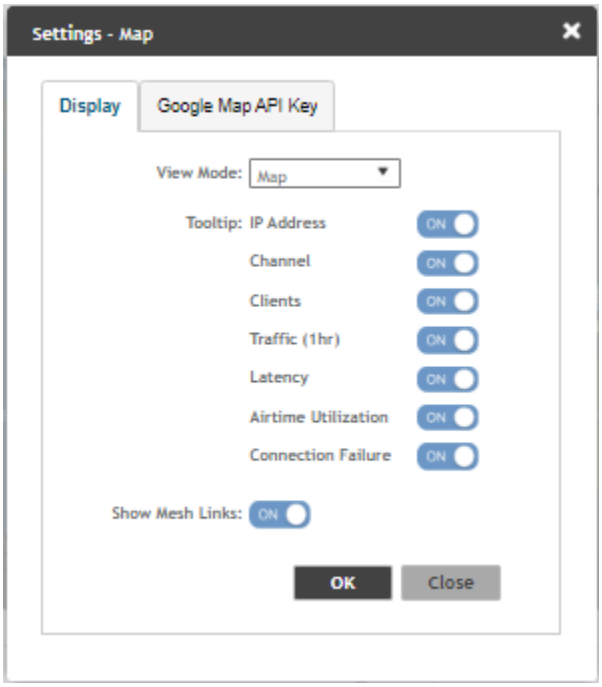
- AP MAC: Displays the MAC address of the AP
- AP Name: Displays the name assigned to the access point
- Status: Displays the status of the AP such as Online or Offline

FIGURE 11 AP Details



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

FIGURE 12 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

The Google Maps feature in the controller application works based on API interaction between the application and the Maps service hosted by Google. By default, these APIs are commonly available without the need for an API key but sometimes, you might have to generate a key.

If Google Maps do not display properly in the absence of an API key, or when the API usage exceeds the daily limit, then an API key needs to be generated to ensure the map displays all the elements properly.

You would also have to generate an API key if you encounter errors such as

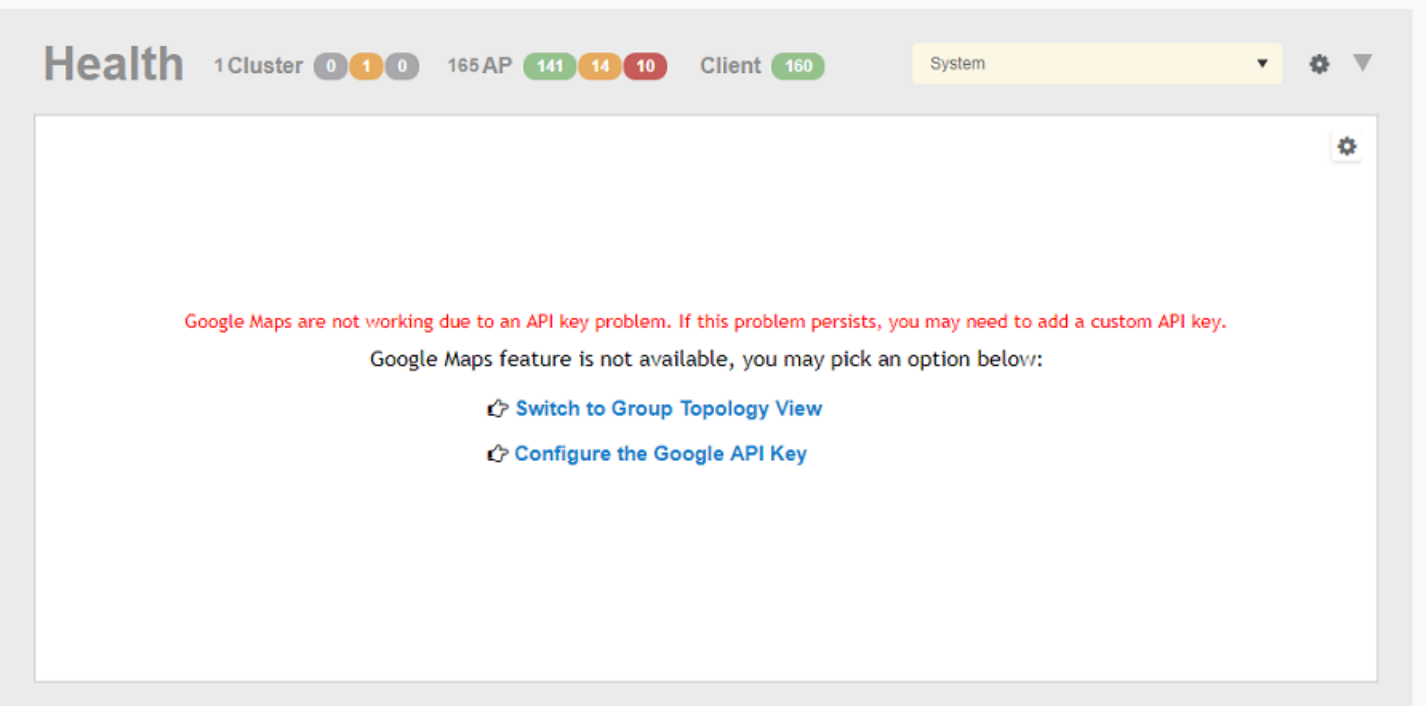
```
MissingKeyMapError
```

or

```
NoApiKeys
```

.

FIGURE 13 Health dashboard view when API key is not available



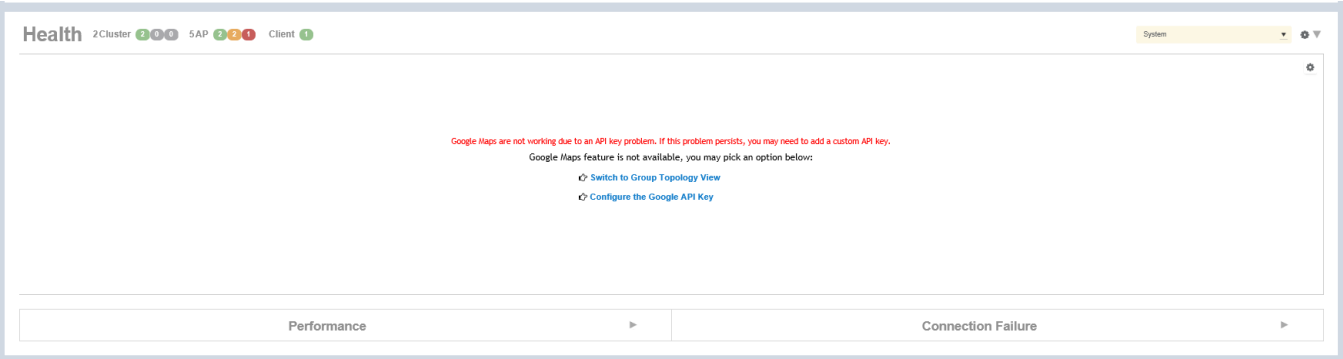
Clicking **Configure the Google API Key** directs you to the **Google Map API Key** tab, where you can manage the Google Map API Key behavior.

All administrators of the system can use the same API key, or apply a unique API key per administrator. Allowing an API key per administrator enables more flexibility when API usage is high, or in circumstances when each tenant must use their own API key.

Follow these steps to configure the Google Map API Key behavior.

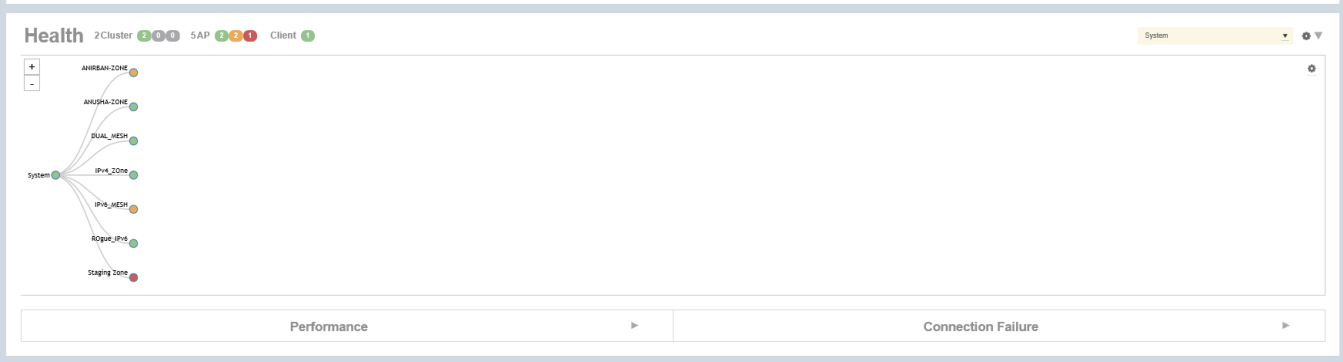
Launching the application displays the **Dashboard** menu, by default.
In **Health**, the map view appears if you are connected to a network. If you are not, then you might see the following screen and would have to view your network deployment as a topology diagram.

FIGURE 14 No Map View



If you click the **Switch to Group Topology View**, a topology diagram similar to the following figure is displayed.

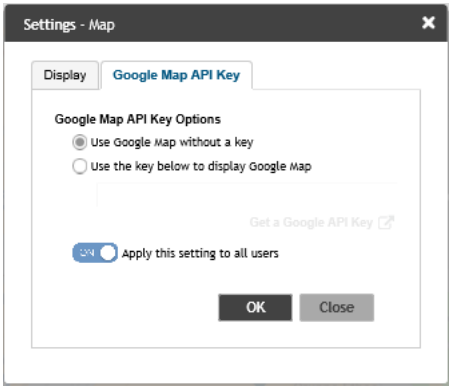
FIGURE 15 Topology View



1. From the map view in **Health**, click the **Settings** (gear-shaped) icon.

   The **Settings-Map** page appears.

   FIGURE 16 Google Map API Key Options



   From the **Display** tab, you can choose the mode in which you want to view your network deployment.

2. Click the **Google Map API Key** tab.
3. From the **Google Map API Key Options**, select one of the following:

Option	Description
Use Google Map without a key	Allows you to use the Google map feature without an API key.
Use the key below to display Google Map	Allows you to enter an API key which you already have to use the Google map feature. If you do not have a pre-existing API key, you can generate one by following the instructions in the **Get a Google API Key** link.

   NOTE
   The Google API Console is a platform on which you can build, test, and deploy applications. To use Google Maps API, you must register your application on the Google API Console and generate a Google API key which you can add to the application. For more information, see https://developers.google.com/maps/documentation/javascript/tutorial

   If you already have a Google API Map Key, type the key to establish a connection with Google Maps.

4. Select Apply this setting to all users to apply the configuration settings to all users in the network deployment.
5. Click **OK**.

You have successfully configured the Google Map API Key options for your network deployment.

Viewing AP Performance

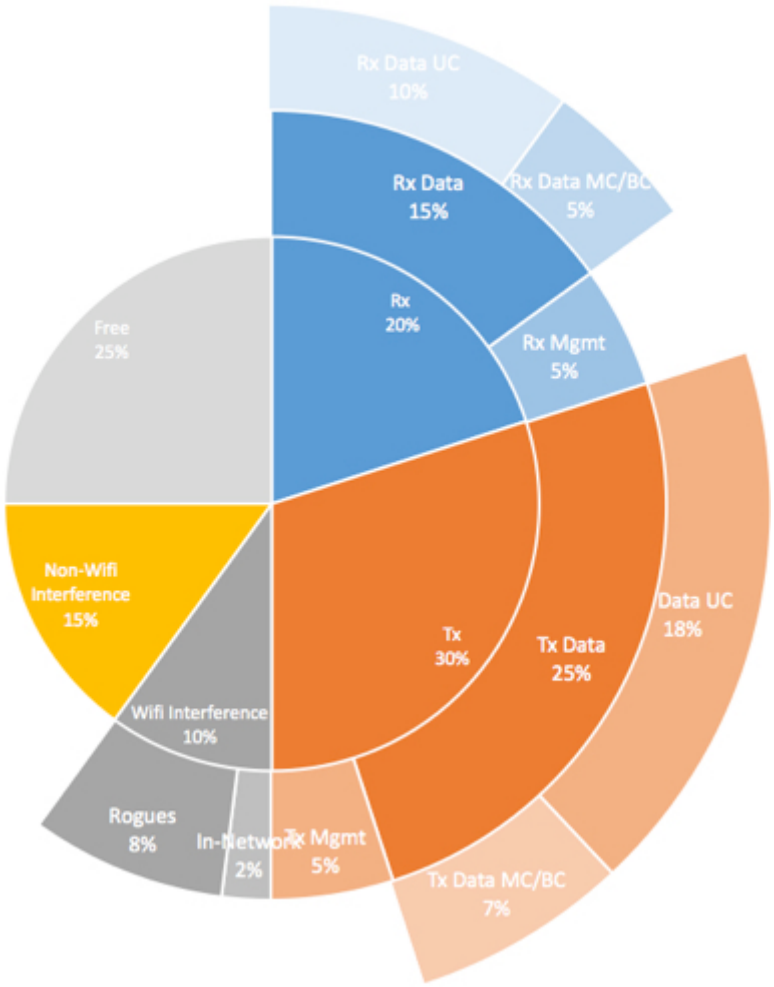
Click the Performance tab to analyze the following parameters:

- Latency - Average time delay between an AP and connected clients.
- Airtime Utilization - Percent of airtime utilized, by radio. Clicking **Airtime Detail** displays a pie chart that depicts a detailed breakup of the reception and transmission percentages (Rx and Tx) against parameters such as Data, Management, Unicast, Multicast, Interference and Network Load. Following are the statistics that are evaluated:

TABLE 6 Airtime Utilization Statistics

Total	Total Airtime under observation
RxLoad	Airtime spent in receiving frames destined to AP in Micro seconds
RxInt	Airtime spent in receiving frames NOT destined to AP in Micro seconds
TxSuccess	Airtime spent in transmitting frames successfully in Micro seconds
TxFailed	Airtime spent in transmit failed in Micro seconds
NonWifi	Airtime where CCA is busy in Micro seconds
RxTotal	Same as RxLoad or sum of Rx (Mgmt Unicast + Mgmt Bcast + Data Unicast + Data Bcast)
RxMgmtU	Airtime spent in receiving Management Unicast frames in Micro seconds
RxMgmtB	Airtime spent in receiving Management Broadcast frames in Micro seconds
RxDataU	Airtime spent in receiving Data Unicast frames in Micro seconds
RxDataB	Airtime spent in receiving Data Broadcast frames in Micro seconds
TxTotal	Same as TxSuccess or sum of Tx (Mgmt Unicast + Mgmt Bcast + Data Unicast + Data Bcast)
TxMgmtU	Airtime spent in transmitting Management Unicast frames in Micro seconds
TxMgmtB	Airtime spent in transmitting Management Broadcast frames in Micro seconds

FIGURE 17 Sample Airtime Utilization Pie Chart



- Capacity - Measurement of potential data throughput based on the recent air-time efficiency and the performance potential of the AP and its currently connected clients.

You can view the parameters based on specific:

- Duration: 1 hour, 24 hours, 7 days, and 14 days
- Radio: 2.4 GHz, 5GHz

The parameters are displayed as Graphs and Bar Charts. When you hover over the graph you can view the Date and Time, Median, Likely Range, Min-Max Range of the parameters. To view specific information on the graph, click and drag the portion. The selected portion would zoom in. To restore to normal view, click the **Reset zoom** button.

To display specific information, click the settings button. The Settings - Performance window pops up. In **Show top**, enter the number of APs to be analysed and choose the AP identity display.

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:

-  (Green): Online
-  (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 "flagged" state using the **Settings** (gear) icon in the status bar. For more information, see Customizing Health Status Thresholds on page 29.

Viewing AP Connection Failures

Click the Connection Failure tab to analyze the following parameters

- Total - Measurement of unsuccessful connectivity attempts by clients
- Authentication - Measurement of client connection attempts that failed at the 802.11 open authentication stage
- Association - Measurement of client connection attempts that failed at the 802.11 association stage
- EAP - Measurement of client connection attempts that failed during and EAP exchange
- RADIUS - Measurement of RADIUS exchanges that failed due to AAA client/server communication issues or errors
- DHCP - Measurement of failed IP address assignment to client devices

You can view the parameters based on specific:

- Duration: 1 hour and 24 hours
- Radio: Total, 2.4 GHz, 5GH

The parameters are displayed as Graphs and Bar Charts. When you hover over the graph you can view the Date and Time, Median, Likely Range, Min-Max Range of the parameters. To view specific information on the graph, click and drag the portion. The selected portion would zoom in. To restore to normal view, click the **Reset zoom** button.

To display specific information, click the Settings button. The Settings - Performance window pops up. In **Show top**, enter the number of APs to be analysed and choose the AP identity display.

Viewing Switches on the Dashboard

The wired dashboard displays detailed information about the health of the switch and displays charts illustrating traffic trends.

1. From the SmartZone interface, click **Monitor** > **Dashboard.**

   The **Dashboard** page is displayed.
2. Click **Wired**.

   The **Wired** page is displayed.
3. Click the Gear icon on the **Health** dashboard.

   The **Settings-Health Dashboard** page is displayed.
4. Click the **Display** tab.

5. From the **View Mode** , select either **Topology** or **Port** view to be displayed on the dashboard.

FIGURE 18 Showing Wired Devices Using Port View Mode

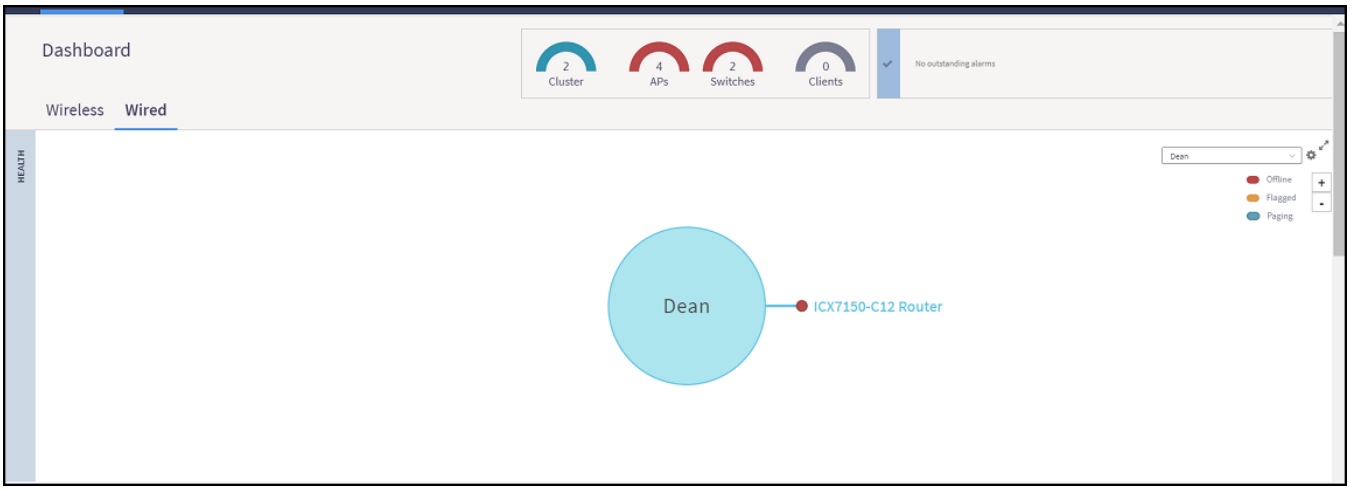
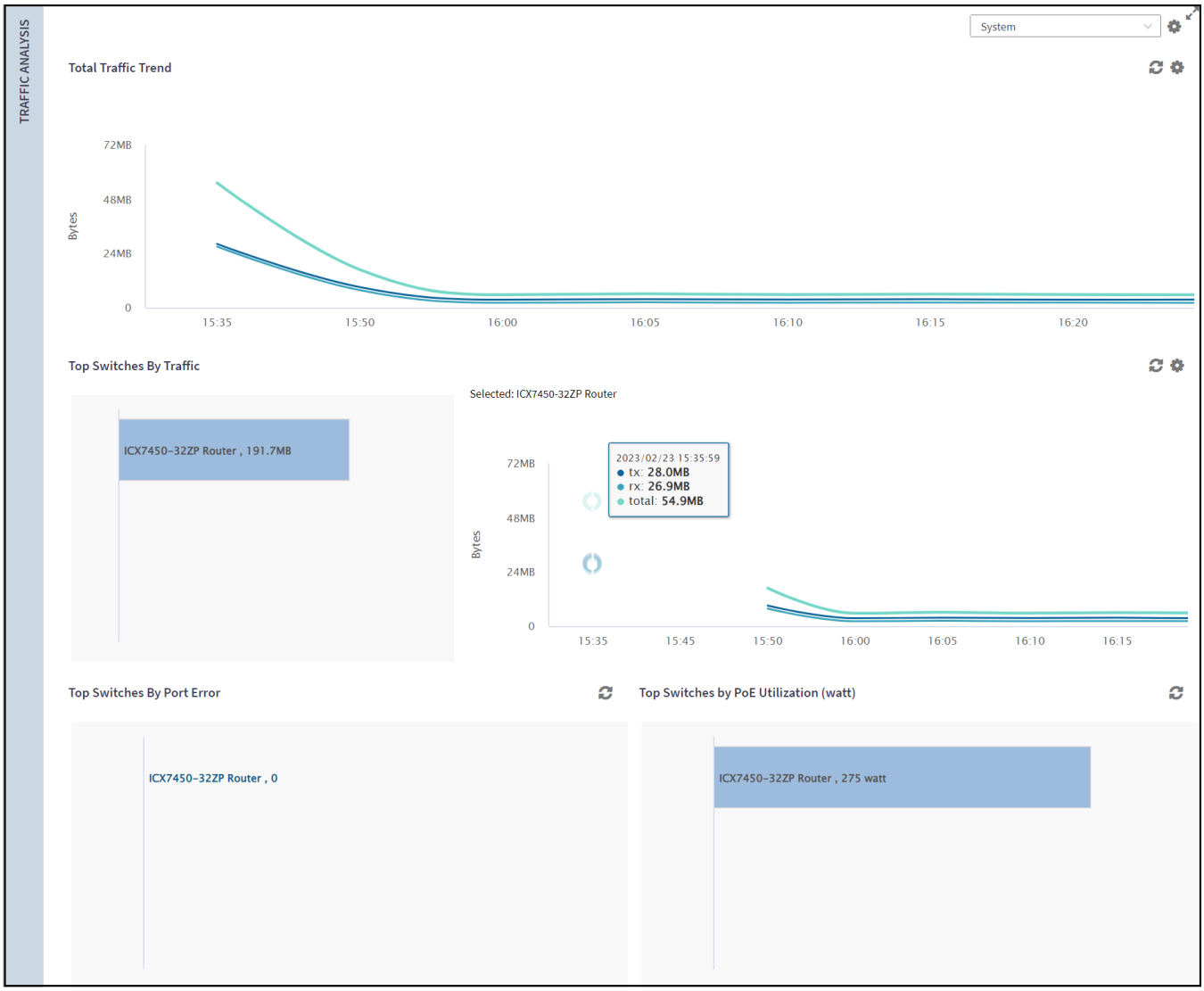


FIGURE 19 Viewing Traffic Analysis



In the port view mode, the **Health** pane displays the number of switches that are online, offline, and flagged.

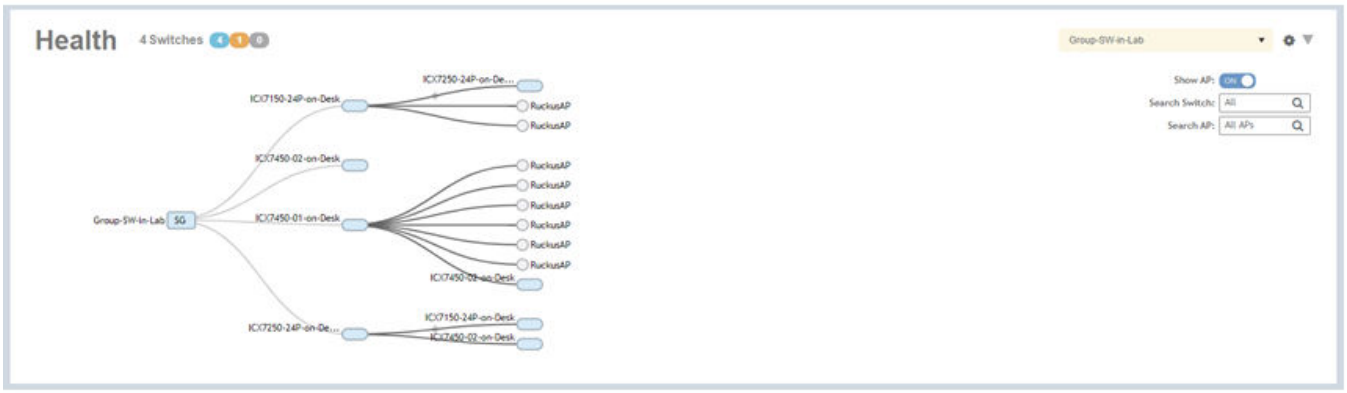
The **Health** pane also displays the number of ports for each port speed (1 Gbps, 2.5 Gbps, 10 Gbps, and so on) or all the ports, and indicates the status of the ports (Up, Down, Down by Admin, Down Total, and Up Total).

The **Traffic Analysis** pane displays the following information:

- Total Traffic Trend
- Top Switches By Traffic
- Top Switches By Port Error

- Top Switches by PoE Utilization (watt)

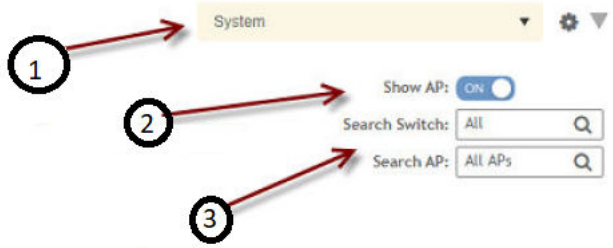
FIGURE 20 Showing Wired Devices Using Topology View Mode



In the topology view mode, the **Health** pane consists of a filter combo box to display domain, sub-domain and switch group in the topology view. The **Show AP** button can be turned on or off to view either the switch or a combination of switch and AP, and **Search** box to search AP or switch based on the device name and MAC address. If you pause the pointer on a link in the topology view, the highlighted link shows the port and LAG information. If you pause the pointer on a device, the highlighted device shows device information such as name, model, MAC address, and IP address (for the switch only).

NOTE
The **Health** dashboard refreshes automatically every 15 minutes to show the latest topology view.

FIGURE 21 Showing Elements on the Health Dashboard



1 - Filter

2 - Topology Type Switch Button

3 - Search Bar

Traffic Analysis

Traffic Analysis provides network traffic information for APs, WLANs and clients.

To view information of the network traffic, select a **Zone** > **WLAN** and click **Configure**. This displays **Edit WLAN Configuration** of the selected WLAN.

Scroll down to **Firewall Options** category and enable **Application Recognition and Control** toggle button to **On**.

Use below filters to view information of the selected WLAN and different applications connnected.

- **Channel Range**
  - **Total**
  - **2.4GHz**
  - **5GHz**
- **Throughput**
  - **TX+RX**—Number of bytes sent and received
  - **TX**—Number of bytes sent
  - **RX**—Number of bytes received
- **Group**

The parameters are displayed as Graphs and Bar Charts. When you hover over the graph you can view the Date and Time, Median, Likely Range, Min-Max Range of the parameters. To view specific information on the graph, click and drag the portion. The selected portion would zoom in. To restore to normal view, click the **Reset zoom** button.

Configuring Traffic Analysis Display for APs

Using traffic analysis you can measure the total volume of traffic sent or received by an Access Point (AP).

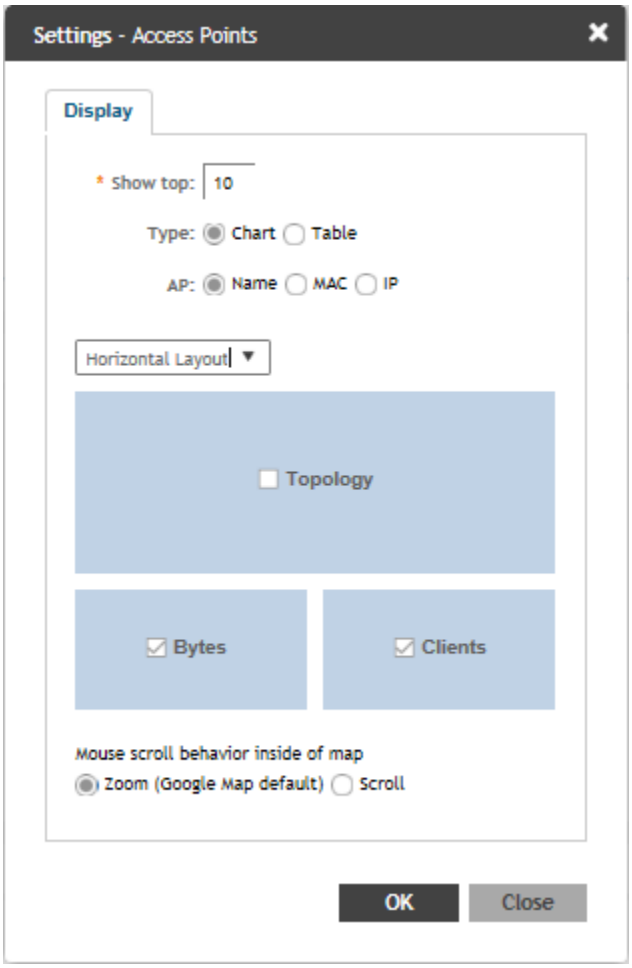
You can view historical and real-time data of the AP. Throughput and the number of clients connected to the AP are displayed in a bar chart. You can view the count of AP model details supported on the system in a pie chart. You must configure the AP settings to view its traffic analysis.

To configure the AP settings:

1. From the Access Points area, click settings .

   The AP setting form displays.

   FIGURE 22 AP Settings Form



2. In the **Show top** box, enter the number of APs for which the traffic must be analyzed. Range: 5 through 20.
3. Select the **Type** radio button for the type of display you want to view. The choices are **Chart** or **Table**.
4. Select the **AP** identification option to be displayed. The choices are **Name**, **MAC**, or **IP**.
5. From the drop-down, select the required display layout. The choices are **Horizontal Layout** or **Vertical Layout**.
6. Select or clear the required options that must be displayed in the Content area.
   a) **Topology**—To view the location map.
   b) **Bytes**—To view the location map.
   c) **Clients**—To view the location map.
   d) **AP Models**—To view the location map.

7. Select the following mouse-scroll behavior when you point the mouse over a map.
   a) **Zoom**
   b) **Scroll**
8. Click **OK**.

Configuring Traffic Analysis Display for WLANs

Using traffic analysis you can measure the total volume of traffic sent or received by WLANs.

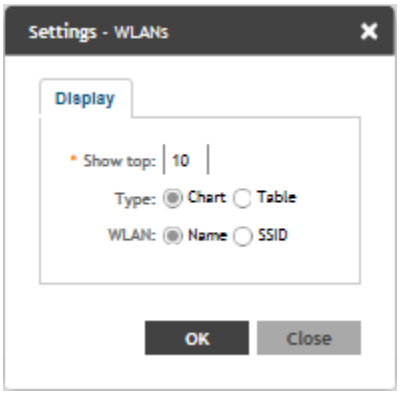
You can view historical and real-time data of the WLANs. Throughput and the number of clients connected to the WLANs are displayed in a bar chart. You must configure the WLAN settings to view its traffic analysis.

To configure the WLAN settings:

1. From the WLAN area, click settings .

   The WLAN settings form displays.

   FIGURE 23 WLAN Settings Form



2. In the **Show top** box, enter the number of WLANs for which the traffic must be analyzed. Range: 5 through 20.
3. Select the **Type** radio button for the type of display you want to view. The choices are **Chart** or **Table**.
4. Select the **WLAN** identification option to be displayed. The choices are **Name** or **SSID**.
5. Click **OK**.

Configuring Traffic Analysis Display for Top Clients

Using traffic analysis you can measure the total volume of traffic sent or received by clients.

Using traffic analysis you can measure the total volume of traffic sent or received by Clients. You must configure the Client settings to view the traffic analysis. You can view historical and real-time data of the Clients. The chart displays:

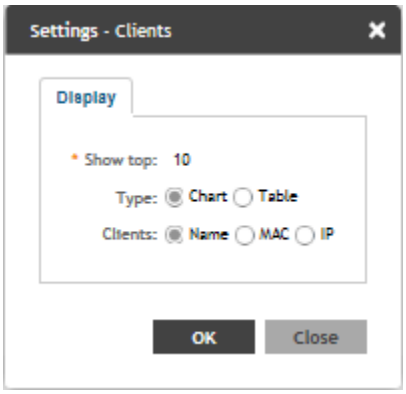
- Bytes—Frequency and number of clients connected to the AP
- OS Type—Types of OS the associated clients are using
- Application—Throughput the applications use

To configure the Client settings:

1. From the WLAN area, click settings .

   The Client settings form displays.

   FIGURE 24 Client Setting Form



2. In the **Show top** box, enter the number of Clients for which the traffic must be analyzed. Range: 5 through 20.
3. Select the **Type** radio button for the type of display you want to view. The choices are **Chart** or **Table**.
4. Select the **WLAN** identification option to be displayed. The choices are **Name**, **MAC**, or **IP**.
5. Click **OK**.

SmartCell Insight Report on Actual Traffic Rate for APs and Client

SmartZone (SZ) reports the total traffic statistics at an interval of every three minutes or 15 minutes to SmartCell Insight (SCI).

For traffic rate calculation, SCI divides the total traffic by time. But, this is not sufficient to accurately calculate airtime efficiency, as APs may not be sending or receiving the traffic all the time in the 15 minute interval. In other words, the SCI reporting of *traffic rate* needs to be across two dimensions:

1. **Traffic Over Time:** This is the current metric, and effectively captures how much traffic was sent or received over a period of time. The goal of this metric is to capture traffic, so that network operators can identify how much the network is being used in a time period.
2. **Traffic Efficiency:** This is the new metric, and effectively captures how much airtime was required to send receive traffic over time. The goal of this metric is to capture traffic efficiency, so that network operators can identify network performance in a time period.

To accomplish the efficiency calculation, information about both traffic and airtime usage (Tx,Rx, and busy), are measured as counters in a reporting interval. For SCI to do this, SZ will send the following information to SCI at the AP level.

- **Total traffic** Uplink and downlink time
- **Total Tx Time**: How much time did the AP spend transmitting traffic
- **Total Rx Time**: How much time did the AP spend receiving traffic for the AP's basic service set identifier (BSSIDs)
- **Other Rx Time**: How much time did the AP spend receiving broadcast traffic and traffic for other BSSIDs

  NOTE
  The reason for this metric is to distinguish between AP traffic and environmental traffic, where environmental traffic does affect airtime availability, but is not incorporated into the traffic efficiency calculation.

- **Total Tx/Rx Time**: How much time did the AP spend receiving and sending traffic in total for its BSSIDs
- **Idle Time**: How much time did the AP spend idle

SZ will send the following information to SCI at the Client level.

- **Total traffic** Uplink and downlink time
- **Total Tx Time**: How much time did the client spend transmitting traffic
- **Total Rx Time**: How much time did the client spend receiving traffic for the AP's basic service set identifier (BSSIDs)
- **Total Tx/Rx Time**: How much time did the client spend receiving and sending traffic in total for its BSSIDs

Wired

Viewing a Summary of Wired Clients

View a summary of wired clients that are currently associated with all of your managed access points.

Go to **Monitor** > **Clients** > **AP Wired Clients.**

The **AP Wired Clients** page appears and displays a table that lists all clients that are currently associated with your managed access points.

To view only wired clients that belong to a particular zone, click the zone name in the zone tree. The table refreshes and displays only the clients that belong to the zone you selected.

The following table lists the wired client details.

TABLE 7 Wired client details

Column Name	Description
MAC Addres	Displays the MAC address of the wired client
Username	Displays the name of the user logged on to the wire client
IP Address	Displays the IP address assigned to the wired client
AP MAC	Displays the MAC address of the AP
AP Name	Displays the name assigned to the access point
LAN	Displays the LAN ID assigned to the wired client
VLAN	Displays the VLAN ID assigned to the wired client
Auth Status	Indicates whether the wired client is authorized or unauthorized to access the WLAN service

To know more about how the 802.1X configuration works for the port refer Creating an Ethernet Port Profile on page 479.

Monitoring Access Points

When you select an AP from the list, contextual tabs appear at the bottom of the page.

The following table helps you to understand the real-time information about the AP.

TABLE 8 Access Point Monitoring Tabs

Tabs	Description
General	Displays group information
Configuration	Displays group configuration information.
Health	Displays historical health information.

TABLE 8 Access Point Monitoring Tabs (continued)

Tabs	Description
Traffic	Displays historical traffic information.
Alarm	Displays alarm information.
Event	Displays event information.
Clients	Displays client information.
Pool Stats	Displays DHCP pool data.
Stats Counter	Displays AP statistics that can be exported to CSV format.
GPS Location	Displays AP Historical GPS location information on a map **NOTE** For M510 AP, GPS location probe interval must be set to 5.

Additionally, you can select an AP and click **More** to perform the following operations as required:

- **Select ALL** - Selects all the APs in the list.
- **Deselect All**- Clears all selection from the list.
- **Troubleshooting > Client Connection** - Connects to client devices and analyze network connection issues in real-time. See, Troubleshooting Client Connections on page 70
- **Troubleshooting > Spectrum Analysis** - Troubleshoots issues remotely, identify sources of interferences within the network and allow administrators access to the RF health of the network environment. See, Troubleshooting through Spectrum Analysis on page 72
- **Restart** - Restarts an access point remotely from the web interface.
- **Lock** - Disables all WLAN services on the AP and disconnect all wireless users associated with those WLAN services temporarily.
- **Unlock** - Makes all WLAN services available.
- **Import Batch Provisioning APs** - Import the provisioning file. See, Options for Provisioning and Swapping APs on page 162
- **Import Swapping APs** - Manually trigger the swapping of two APs by clicking the swap action in the row. See, Options for Provisioning and Swapping APs on page 162
- **Export All Batch Provisioning APs** Downloads a CSV file that lists all APs that have been provisioned.. See, Options for Provisioning and Swapping APs on page 162
- **Export All Swapping APs** - Downloads a CSV file that lists all APs that have been swapped. See, Options for Provisioning and Swapping APs on page 162
- **Download Support Log** - Downloads support log.
- **Trigger AP Binary Log** - Triggers binary log for the selected AP.
- **Trigger Preferred Node** - Triggers an AP that belongs to the current zone to connect to the preferred node. See Triggering a Preferred Node on page 140.
- **Download CM Support Log** - Downloads Cable Momdem support log.
- **Restart Cable Modem** - Restarts the cable modem. The AP will disconnect from the network for a short period. The AP will disconnect from the network for a short period.
- **Reset Cable Modem** - Resets the cable modem.
- **Reset Cable Modem to Factory Default** - Resets the cable modem to factory default settings.
- **Untag Critical APs** - Stating APs as non-critical. See, Tagging Critical APs on page 54.
- **Swap** - Swaps current AP to swap-in AP. See, Editing Swap Configuration on page 163
- **Switch Over Clusters** - Moves APs between clusters. See Configuring AP Switchover on page 65.

- **Approve** - Approves AP and completes registering. See, Working with AP Registration Rules on page 53.

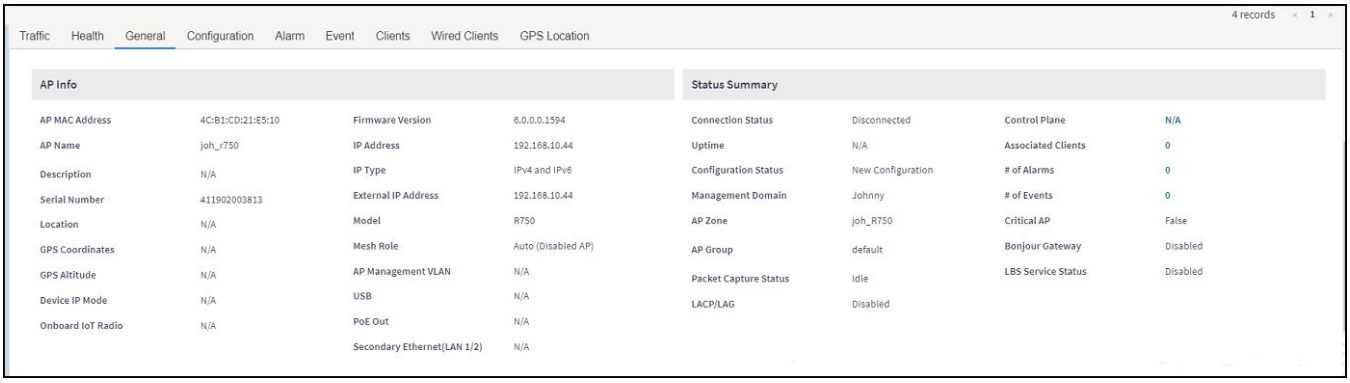
Viewing General AP Information

Complete the following steps to view general AP information.

1. From the **Network** > **Wireless** > **Access Points** page, select an AP.
2. In the **General** tab, scroll to the **AP Info** information.

   You can view information specific to the selected AP.

   FIGURE 25 General AP Information



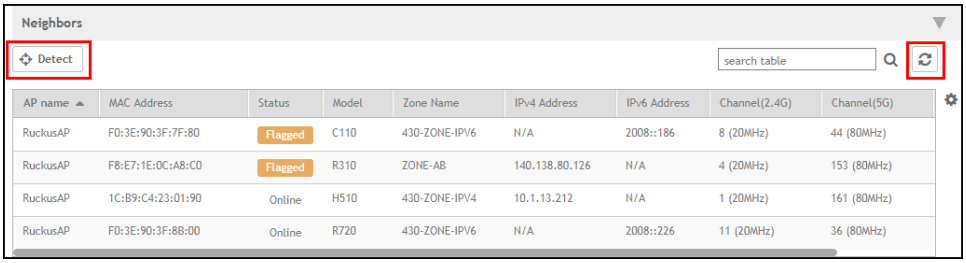
Viewing Neighbor APs in a Non-Mesh Zone

To view neighbor APs in a Non-Mesh zone:

1. From the **Network** > **Wireless** > **Wireless LANs** page, select an AP.
2. Scroll down to the bottom of the page. In the Neighbors area, click **Detect**.

   The list of neighboring APs are displayed in the table.

   FIGURE 26 Neighbor APs for a Non-Mesh Zone



3. To refresh the list, click the Refresh button.

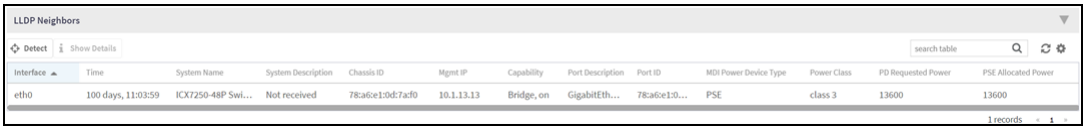
Viewing LLDP Neighbors

You can view basic information, and detailed information about the LLDP neighbor of an AP form the controller interface.

1. From the **Access Points** page, select an AP from the list.
2. Scroll down to the bottom of the page. In the **LLDP Neighbors** area, click **Detect**.

   The list of neighboring LLDP APs are displayed in the table.

   FIGURE 27 Neighbor LLDP APs for a Non-Mesh Zone

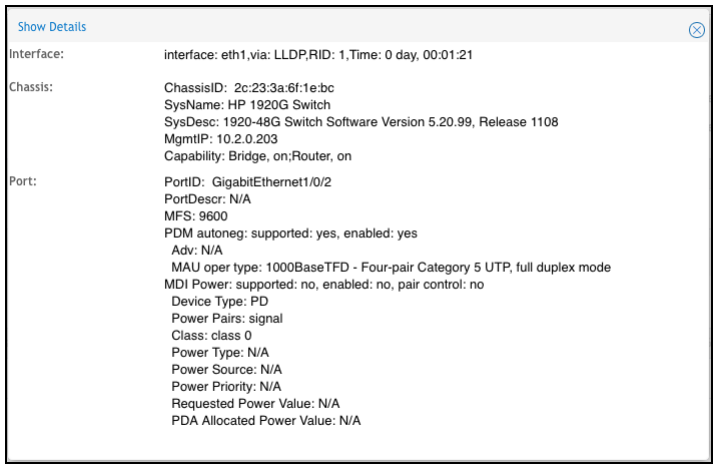


   You can view basic information about the LLDP AP neighbor such as:

   - Interface: displays the interface on the AP from which the LLDP neighbor is detected
   - Time: displays the matching time output in current LLDP command
   - System Name: displays the name of the system such as a switch or router
   - System Description: displays a short description about the system
   - Chassis ID: displays the chassis ID of the system
   - Mgmt IP: displays the management IP address of the LLDP neighbor
   - Capability: displays the capability of the LLDP neighbor such as Bridging or Routing capabilities
   - Port Description: displays the port type and capacity such as Gigabit Ethernet port
   - Port ID: displays the port ID
   - MDI Power Device Type: indicates whether the device is a power sourcing equipment (PSE) or a powered device (PD). PSE is the source of the power, or the device that integrates the power onto the network. PD is the Ethernet device that requires power and is situated on the other end of the cable connected to the PSE.
   - Power Class: displays the power-class of the device ranging from 0 to 4 (IEEE 802.3at power-classes).
   - PD Requested Power: displays power (in watts) requested by the Powered Device
   - PSE Allocated Power: displays power (in watts) allocated by the Power Sourcing Equipment to the Powered Device

3. Click **Show Details** to view detailed information about the LLDP AP neighbor such as the interface, chassis and ports.

   FIGURE 28 Additional LLDP AP Neighbor Details



4. To refresh the list, click the Refresh button.

Viewing AP Health Indicators

You can monitor the performance and connection failures of an AP from the Health tab page.

Performance

- Latency - It is the measurement of average delay required t successfuly deliver a Wi-Fi frame.
- Airtime Utilization - It is a measurement of airtime usage on the channel measuring the total percentage of airtime usage on the channel.
- Capacity - It is a measuement of potential data throughput based on recent airtime efficiency and the performacne potential of the AP and its currently connected clients.

Connection Failure

- Total - It is a measurement of unsuccessful connectivity attempts by clients.
- Authentication - It's a measurement of client connection attempts that failed at the 802.11 open authentication stage.
- Association - It is a measurement of client connection attempts that failed at the 802.11 association stage, which happens before user/device authentication.
- EAP - It is a measuremmetn of client connection attempts that failed during an EAP exchange.
- RADIUS - It's a measurement of RADIUS exchange failures due to AAA client /server communication.
- DHCP - It's a measurement of failed IP address assignment to client devices.

To customize Health Performance settings:

1. From the Access Points page, select the required AP from the list.
2. Scroll Down and select the **Health** tab.

3. On the **Performance** bar, select the Setting icon. The **Settings - Performance** pop-up appears. Customize the following:
   - **Show top**: Enter the number of performance failures to be displayed.
   - **Display Channel Change**: Select the required options. For example: **2.4G**, **5G**.
   - **AP**: Choose how the AP details must be displayed. For example: **Name**, **MAC**, **IP**.
4. Click **OK**.

   Performance details of the AP are listed according to the settings.

Viewing AP Traffic Indicators

You can monitor the performance and connection failures of an AP from the Traffic tab page.

You can view:

- Historical or Real Time traffic
- WLAN traffic

Traffic indicators can be filtered based on the following parameters:

- Rate, Packets, Rate
- Total, Downlink-From AP to client, Uplink-From client to AP

To customize Traffic settings:

1. From the Access Points page, select the required AP from the list.
2. Scroll Down and select the **Traffic** tab.
3. On the respective section bar, select the Settings icon. The **Settings - Clients** pop-up appears. Customize the following:
   - **Type**: Choose the Display format. For example: **Chart**, **Table**.
   - **Display Channel Change**: Select the required options. For example: **2.4G**, **5G**.

     NOTE
     This field is available only for the Clients Tab when you select the Display Type as Chart.

   - **AP**: Choose the AP display format. For example: **Name**, **MAC**, **IP**.
4. Click **OK**.

   Performance details of the AP are listed according to the settings.

Configuring AP Settings

Approving Access Points

Access Points (APs) must be approved to join the system. The APs can be approved either automatically or manually.

Approving Access Points Manually

To approve an AP manually, perform the following -

1. Go to **Network Wireless Access Points**.
2. On the left hand side, under **System** tree, scroll down and click on the **Staging Zone**.This displays all APs in the queue for approval.

3. Clear the **Automatically approve all join requests** from APs check box.
4. Click **Ok**.

Approving Access Points Automatically

To approve an AP automatically, perform the following -

1. Go to **Network Wireless Access Points**.
2. On the left hand side, under **System** tree, scroll down and click on the **Staging Zone**.

   This displays all APs in the queue for approval.
3. Select the **Automatically approve all join requests** from APs check box.
4. Click **Ok**.

Working with AP Registration Rules

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

> **NOTE**
> A registration rule is only applied to an AP the first time it joins the controller. If an AP's MAC address already exists on the controller database (whether it is in connected on disconnected state and whether it belongs to the Staging Zone or any other zone), the controller will assign the AP to its last known AP zone.

Creating an AP Registration Rule

You must create rules to register an AP.

To create an AP registration rule:

1. Go to **Network** > **Wireless** > **AP Settings** > **AP Registration**.

   > **NOTE**
   > For SmartZone 5.2.1 or earlier releases, select **System** > **AP Settings**>**AP Registration**.

2. Click **Create**, the AP Registration Rule form appears.
3. Enter a **Rule Description**.
4. Select the **Zone Name** to which this rule applies.
5. In **Rule Type**, click the basis upon which you want to create the rule. Options include:

   > **NOTE**
   > The format of the IP address or addresses that you need to enter here depends on the AP IP mode that you selected when you created the AP zone to which this rule will be assigned. If you selected IPv4 Only, enter an IPv4 address. If you selected IPv6 Only, enter an IPv6 address.

   - **IP Address Range**: If you select this option, enter the From (starting) and To (ending) IP address that you want to use.
   - **Subnet**: If you select this option, enter the IP address and subnet mask pair to use for matching.
   - **GPS Coordinates**: If you select this option, type the GPS coordinates to use for matching. Access points that have been assigned the same GPS coordinates will be automatically assigned to the AP zone that you will choose in the next step.

     You can choose the Rule Type as GPS coordinates, wherein you must provide information about the latitude, longitude and distance to determine if the AP is within the defined area.

- **Provision Tag**: If the access points that are joining the controller have been configured with provision tags, click the Provision Tag option, and then type a tag name in the Provision Tag box. Access points with matching tags will be automatically assigned to the AP zone that you will choose in the next step.

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

6. Click **OK**.

   When the process is complete, the page refreshes, and then registration rule that you created appears on the AP Registration Rules page.

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

   NOTE
   You can also edit, delete or clone an AP registration rule. To do so, select the rule profile from the list and click **Configure**, **Delete** or **Clone** respectively.

Configuring Registration Rule Priorities

The controller applies registration rules in the same order as they appear in the AP Registration Rules table (highest to lowest priority).

If you want a particular registration rule to have higher priority, you must move it up the table. Once an AP matches a registration rule, the controller assigns the AP to the zone specified in the rule and stops processing the remaining rules.

Follow these steps to configure the registration rule priorities.

1. Go to **Network** > **Wireless** > **AP Settings** > **AP Registration** .
2. Select the rule from the list and click.
   - **Up**—To give a rule higher priority, move it up the table
   - **Down**—To give a rule lower priority, move it down the table
3. Click **Update Priorities** to save your changes.

Tagging Critical APs

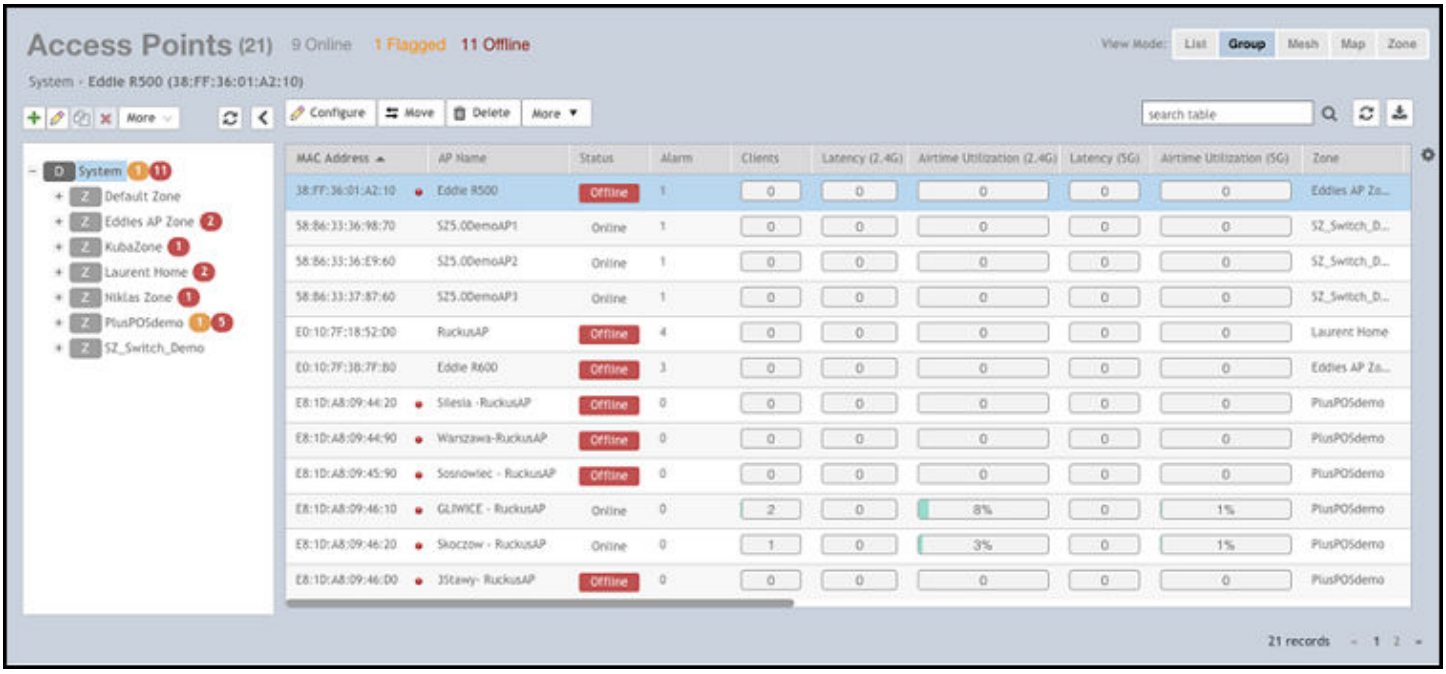
A critical AP is an AP that exceeds the daily traffic threshold (sum of uplink and downlink) data bytes configured on the controller web interface.

Follow these steps to tag critical APs (APs that exceed the data traffic threshold you have defined) automatically:

1. Go to **Network** > **Wireless** > **AP Settings** > **Critical AP Tagging**.
2. Select the **Enable Auto Tagging Critical APs** check box.
3. For **Auto Tagging Rules**, select **Daily Traffic Bytes Exceeds Threshold**.
4. For **Rule Threshold**:
   - In the first box, enter the value that you want to set as the traffic threshold. This value will be applied in conjunction with the data unit that you select in the second box.
   - In the second box, select the data unit for the threshold—**MB** for megabytes or **GB** for gigabytes.
5. Click **OK**.

Critical APs are marked with red dots next to its MAC Address for attention (refer the following image). APs that exceed the daily traffic threshold that you specified will appear highlighted on the Access Points page and the Access Point details page. Additionally, the controller will send an SNMP trap to alert you that an AP has been disconnected.

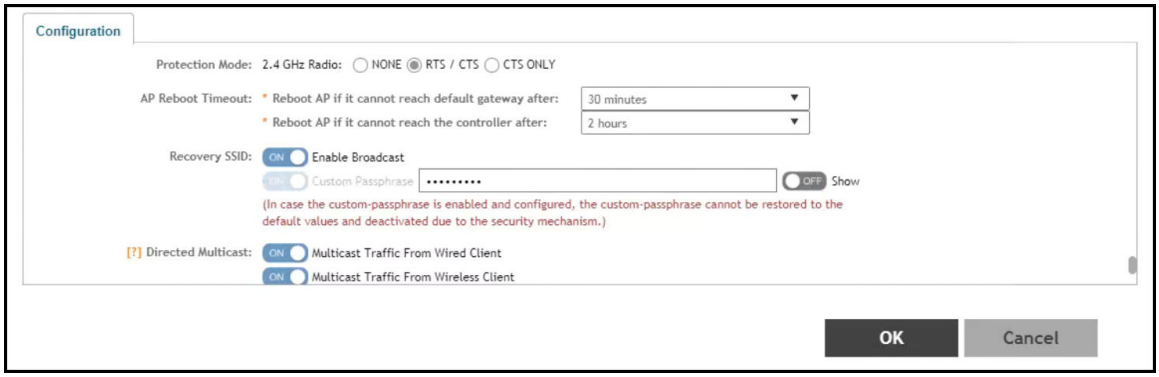
FIGURE 29 APs Tagged as Critical



AP Admin Password and Recovery SSID

This topic describes the mitigation of security enhancement of the AP admin password management.

Consider the following scenario while generating the configuration:



- Initial Installation: AP admin password need to be hashed in SHA-256 algorithm, stored in database and in configuration.

User can specify the Recovery SSID key in the Configuration Tab:

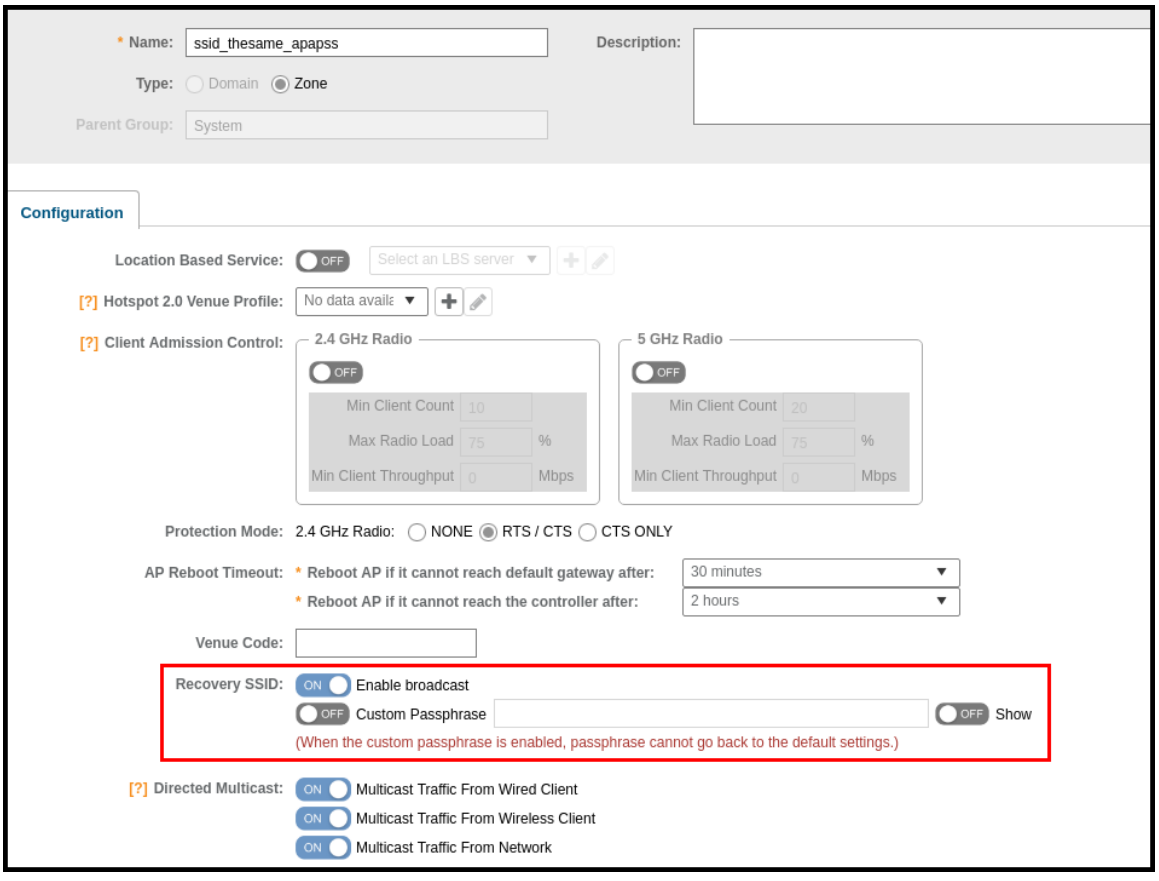
- The default of this Recovery SSID feature is enabled. The default passphrase is AP admin password in clear text format.
- If the user wants to change it, input the passphrase while enabling.
- The validation of passphrase, apply the same rule of WLAN passphrase.
- The passphrase can be clear text stored in the database and delivered to the AP in the GPB configuration by the way of secure channel (SSH channel).

The recovery SSID passphrase(key) will be delivered in GPB configuration as below:

- ccm_zone.proto
- message CcmCommon {
- /** recovery ssid
- */
- optional bool recovery_ssid_enabled = 26
- optional string recovery_ssid_psk_key = 27
- optional int32 server_loss_timeout = 28

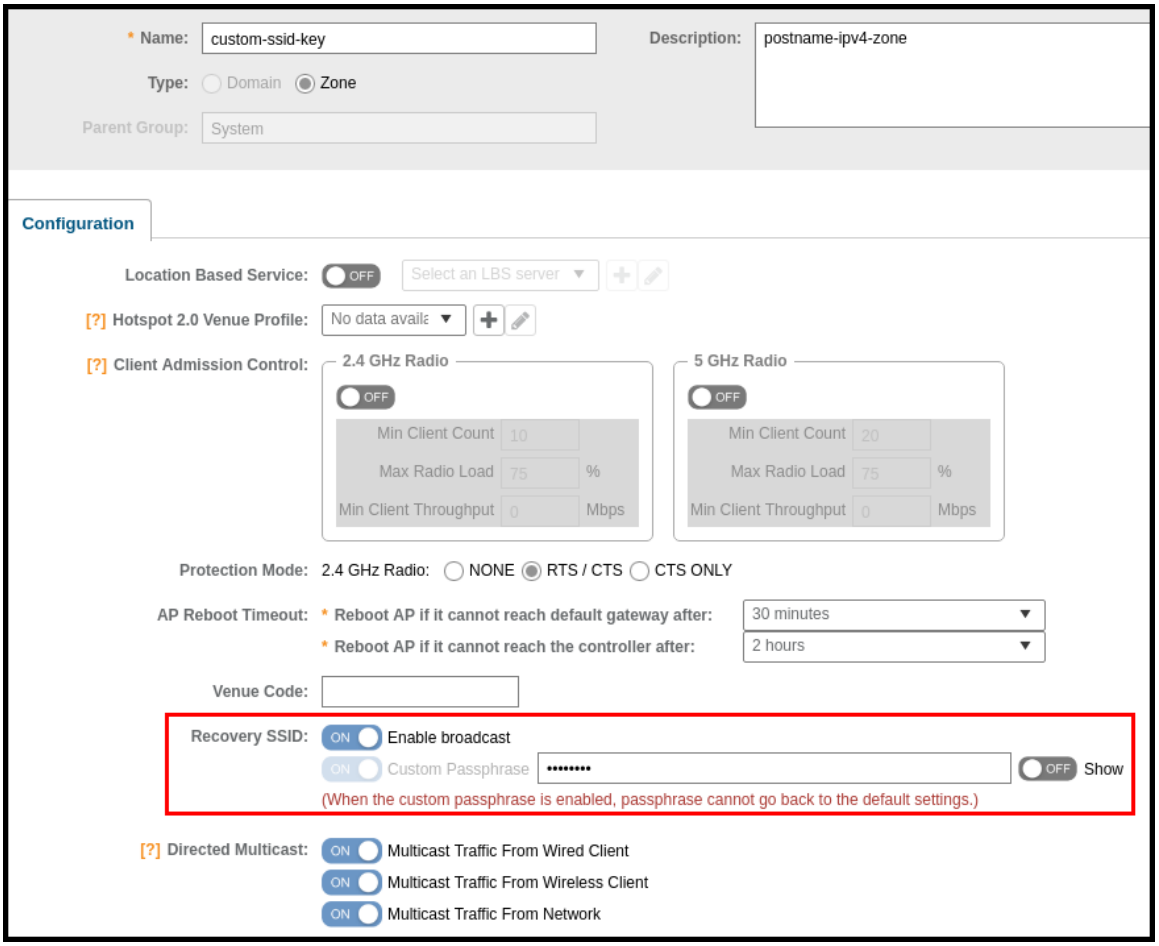
When the Custom passphrase is disabled, the Custom passphrase filed is empty.

FIGURE 30 Custom Passphrase Disabled



When the Custom passphrase is enabled, the Custom passphrase field is mandatory and should enter a passphrase.

FIGURE 31 Custom Passphrase Enabled



Power Source in AP Configuration

The table below displays the PoE mode as per industry standards.

The currently used APs have AF, AT, AT+ convention modes. The standardization applies when the AP is forced to certain PoE power mode. If the AP is set to AUTO PoE mode, feedback displays PoE mode of the AP is currently configured.

The PoE mode as per the industry standards:

TABLE 9 Industry Standard PoE Modes

Selection	Power@PSE	Power@AP (100M Cable)
802.3af	15.4W	12.95W
802.3at	30W	25.5W
802.3bt/Class 5	45W	40W→35W
802.3bt/Class 6	60W	51W
802.3bt/Class 7	75W	62W
802.3bt/Class 8	90W	71.3W

TABLE 10 Non-Standard High Power Solution Summary

	Customers	Maximum Power Sourced
UPoE	Enterprise Switch	60W
PoH	Consumer Customers, for example, audio systems)	95W

The SZ-GUI power mode drop-down has the following set of PoE mode configurations:

TABLE 11 PoE Mode Settings

Name	Value
Auto	0
802.3af	1
802.3at	2
802.3bt/Class 5	3
802.3bt/Class 6	4
802.3bt/Class 7	5

NOTE
The 802.3bt/Class5 is chosen for AP's with older software which advertise AT+.

NOTE
The below tables are applicable for stand alone APs as well. However, the IOT functionality is not available.

POE tables for different 11 AC AccessPoint

TABLE 12 R710

	LLDP Power Ask	2.4G tx/rx	5G tx/rx	1Gbps eth	USB	IOT
DC	N/A	4/4	4/4	Enabled	Enabled	Enabled
AF	N/A	2/4	4/4	Enabled	Disabled	Disabled
AT	25W	4/4	4/4	Enabled	Enabled	Enabled
Injector (Model 480125A)	N/A	4/4	4/4	Enabled	Enabled	Enabled

TABLE 13 R610

	LLDP Power Ask	2.4G tx/rx	5G tx/rx	1Gbps eth	USB	IOT
DC	N/A	4/4	4/4	Enabled	Enabled	Enabled
AF	N/A	2/4	4/4	Enabled	Disabled	Disabled
AT	24W	4/4	4/4	Enabled	Enabled	Enabled
Injector (Model 480125A)	N/A	4/4	4/4	Enabled	Enabled	Enabled

TABLE 14 R720

	LLDP Power Ask	2.4G tx/rx	5G tx/rx	1Gbps eth	USB	IOT	Comments
DC	N/A	4/4	4/4	Enabled	Enabled	Enabled	No comments
AF	N/A	1/4	1/4	Enabled	Disabled	Disabled	No comments
AT	25W	4/4	4/4	Enabled	Disabled	Disabled	No comments
3bt/class5	35W	4/4	4/4	Enabled	Enabled	Enabled	No comments

TABLE 14 R720 (continued)

POE Injector (Model 480125A) 60W	N/A	4/4	4/4	Enabled	Enabled	Enabled	Force to 802.3bt/ class5 from SZ GUI

TABLE 15 M510

	LLDP Power Ask	2.4G tx/rx	5G tx/rx	1Gbps eth	USB	IOT
DC	N/A	2/2	2/2	Enabled	Enabled	Enabled
AF	N/A	2/2	2/2	Enabled	Disabled	Disabled
AT	25W	2/2	2/2	Enabled	Enabled	Enabled
Injector (Model 480125A)	N/A	2/2	2/2	Enabled	Enabled	Enabled

TABLE 16 T610

	LLDP Power Ask	2.4G tx/rx	5G tx/rx	1Gbps eth	USB	IOT
DC	N/A	3/3	3/3	Enabled	Enabled	Enabled (0.5W)
AF	N/A	2/3	3/3	Enabled	Disabled	Disabled
AT	25W	3/3	3/3	Enabled	Enabled	Enabled (0.5W)
Injector (Model 480125A)	N/A	3/3	3/3	Enabled	Enabled	Enabled (0.5W)

POE tables for different 11 AX AccessPoint

TABLE 17 R730

	LLDP	2.4G tx/rx	5G tx/rx	5Gbps eth	1Gbps eth	USB	IOT	Comments
DC	N/A	4/4	8/8	Enabled	Enabled	Enabled	Enabled	No comments
AF	N/A	1/4	1/8	Enabled	Disabled	Disabled	N/ADisabled	Not supported via SZ-GUI, but we can AF mode via rkscli.
AT Mode = 0	25W	4/4	4/8	Enabled	Enabled	Enabled (0.5W)	Enabled	By default AT - mode = 0
AT Mode = 1	25W	4/4	8/8	Enabled	Disabled	Disabled	Disabled	Set AT - mode = 1 via Rkscli
802.3bt/class 5	35W	4/4	8/8	Enabled	Enabled	Enabled	Enabled	No comments
POE Injector (Model 480125A) 60W	N/A	4/4	4/8	Enabled	Enabled	Enabled	N/A	Force to 802.3bt/class5 from SZ GUI

TABLE 18 R850

	LLDP Power Ask	2.4G tx/rx	5G tx/rx	5Gbps eth	1Gbps eth	USB	IOT	Comment
DC	N/A	4/4	8/8	Enabled	Enabled	Enabled	Enabled	No comments
AF	N/A	1/4	1/8	Enabled	Disabled	Disabled	Disabled	Not supported via SZ-GUI, but we can AF mode via rkscli.
AT (Mode=0)	25W	4/4	4/8	Enabled	Enabled	Enabled (0.5W)	Enabled	By default at-mode=0

TABLE 18 R850 (continued)

	LLDP Power Ask	2.4G tx/rx	5G tx/rx	5Gbps eth	1Gbps eth	USB	IOT	Comment
AT (Mode=1)	25W	4/4	8/8	Enabled	Disabled	Disabled	Disabled	Set at-mode=1 via Rkscli
802.3bt/class5	35W	4/4	8/8	Enabled	Enabled	Enabled	Enabled	No comments
POE Injector (Model 480125A) 60W	N/A	4/4	4/8	Enabled	Enabled	Enabled	Enabled	Force to 802.3bt/ class5 from SZ GUI

TABLE 19 R750

	LLDP Power Ask	2.4G tx/rx	5G tx/rx	2.5Gbps eth	1Gbps eth	USB	IOT
DC	N/A	4/4	4/4	Enabled	Enabled	Enabled	Enabled
AF	N/A	2/4	2/4	Enabled	Disabled	Disabled	Disabled
AT	25W	4/4	4/4	Enabled	Enabled	Enabled	Enabled
POE Injector (Model 480125A) 60W	N/A	4/4	4/4	Enabled (1Gbps speed)	Enabled	Enabled	Enabled

TABLE 20 T750

	LLDP Power Ask	**2.4G tx/rx**	**5G tx/rx**	**2.5Gbps eth**	**1Gbps eth**	**USB**	**IOT**	**PSE**	**Comment**
DC	N/A	4/4	4/4	Enabled	Enabled	Enabled	Enabled	Enabled	No comments
AF	N/A	1/4	1/4	Enabled	Disabled	Disabled	Disabled	Disabled	Not supported operation mode
AT w/o USB	25W	4/4	4/4	Enabled	Enabled	Disabled	Enabled	Disabled	No comments
AT with USB	25W	2/4	4/4	Enabled	Disabled	Enabled	Enabled	Disabled	Set AT - mode = 1 via Rkscli
802.3bt/ class5	35W	4/4	4/4	Enabled	Enabled	Enabled	Enabled	Disabled	No comments
803.3bt/ class6	N/A	4/4	4/4	Enabled	Enabled	Enabled	Enabled	Disabled	51W by H/W negotiation
802.3bt/ class7	N/A	4/4	4/4	Enabled	Enabled	Enabled	Enabled	Enabled	62W by H/W negotiation
POE 60W Injector (Model 480125A)	N/A	4/4	4/4	Enabled (1Gbps speed)	Enabled	Enabled	Enabled	Disabled	Force to 802.3bt/ class5
POE 90W Injector	N/A	4/4	4/4	Enabled	Enabled	Enabled	Enabled	Enabled	Force to 802.3bt/ class7

TABLE 21 R650

	LLDP Power Ask	**2.4G tx/rx**	**5G tx/rx**	**2.5Gbps eth**	**1Gbps eth**	**USB**	**IOT**
DC	N/A	2/2	4/4	Enabled	Enabled	Enabled	Enabled
AF	N/A	2/2	2/4	Enabled	Disabled	Disabled	Disabled
AT	25W	2/2	4/4	Enabled	Enabled	Enabled	Enabled

TABLE 21 R650 (continued)

POE Injector (Model 480125A)	N/A	2/2	4/4	Enabled (1Gbps speed)	Enabled	Enabled	Enabled

TABLE 22 R550

	LLDP Power Ask	2.4G tx/rx	5G tx/rx	2.5Gbps eth	1Gbps eth	USB	IOT
DC	N/A	2/2	2/2	Enabled	Enabled	Enabled	Enabled
AF	N/A	2/2	2/2	Enabled	Disabled	Disabled	Disabled
AT	25W	2/2	2/2	Enabled	Enabled	Enabled	Enabled
POE Injector (Model 480125A)	N/A	2/2	2/2	Enabled	Enabled	Enabled	Enabled

Configuring the Tunnel UDP Port

The tunnel UDP port is used by all GRE+UDP type tunnels.

To configuring the tunnel UDP port:

1. Go to **Network** > **Wireless** > **AP Settings** > **Tunnel UDP Port**.
2. Enter the **Tunnel UDP Port** number.
3. Click **OK**.

Setting the Country Code

Different countries follow different regulations for radio channel usage.

To ensure that the APs use authorized radio channels:

1. Go to **Network** > **Wireless** > **AP Settings** .
2. Select the **Country Code** for your location from the drop-down.
3. Click **OK**.

Limiting the Number of APs in a Domain or Zone

You can limit the number of APs in a Partner-Managed Domain or a Zone. An MSP may have multiple customers each with their own zone and a number of APs. This feature ensures that their customers do not over-subscribe the licenses that they are entitled. MVNO domains do not have this option. When an AP joins a zone, where an AP number limitation has been applied to that zone, the controller checks the current capacity based on zone's limitation and:

- allows the new AP joining if the number of APs connected do not exceed the limit
- denies the new AP joining if there is no capacity in the domain or zone.

A scheduler task in the background periodically checks the AP number limitation against the number of APs connected. To avoid occupying the license capacity, the APs will be rejected in the following situations:

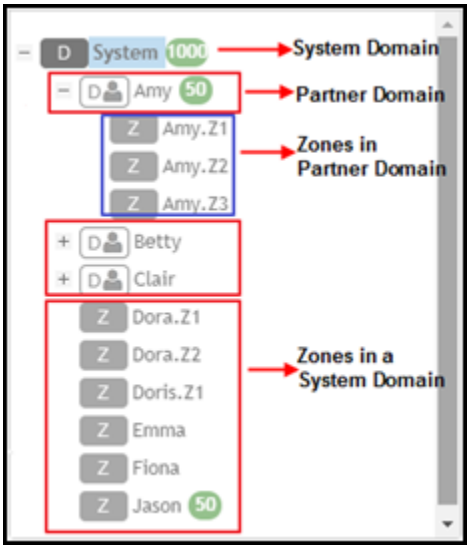
- If the AP number limitation of a Domain or a Zone is increased or reduced.
- If the license capacity is changed.

The following image gives a clarity on:

- System domain

- Partner domain
- Zones in a System domain
- Zones in a Partner domain

FIGURE 32 System Hierarchy



Limiting the AP count for a Partner Domain or a System Zone

Only super admin of the system domain is privileged to limit the number of APs in a partner domain or a system zone.

To limit the number of AP count for a partner domain or a system zone:

1. Log on to the controller web interface using super admin credentials of the system domain.
2. Follow the procedure to limit the number of APs in the partner domain or a zone in system domain:
   a) Go to **Network** > **Wireless** > **AP Settings** > **AP Number Allocation**.
   a) For **Enable AP Number Allocation**, select the **Enabled** check box and click **OK**. The Settings bar appears.
   b) From the left pane, in the system tree hierarchy, select the partner-managed Domain or Zone for which you want to set the AP number limit.
   c) On the right pane, select **Share Mode** or enter the **Number Limit**.
   d) Click **OK**. You have set the AP number limit for the selected Domain or Zone.

Limiting the AP count for a Zone in a Partner Domain

To limit the number of AP count for a zone in a partner domain:

1. Create a super admin account for the partner domain. See the Administrating the Controller chapter.
2. **NOTE**
   While creating user groups, in step 4 (I) c, for **Permission**, select Super Admin from the drop-down.

   Create a user group and configure the access permissions, resources and administrator account. Refer Creating User Groups on page 587.

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

     ```
     Account Name@Domain
     ```

     The Account Name that you set when you created the Administrator Account and the Domain for which you created the Administrator Account. For example: If the partner domain is *TestDomain* and the Account Name is *User*, then the User Name is

     ```
     User@TestDomain
     ```

   - **Password** : The password that you set when you created the Administrator Account.
4. Follow the procedure to limit the number of APs for a zone in a partner-domain:
   a) Go to **Network** > **Wireless** > **AP Settings** > **AP Number Allocation**.
   a) Select the **Enable AP Number Allocation** check box and click **OK**. The Settings bar appears.
   b) From the left pane, in the system tree hierarchy, select the partner-managed zone for which you want to set the AP number limit.
   c) On the right pane, perform one of the following procedure:
      - Select **Share Mode**
      - Enter **Number Limit**
   d) Click **OK**.

   You have set the AP number limit for the selected partner-domain Zone.

Creating an AP MAC OUI Address

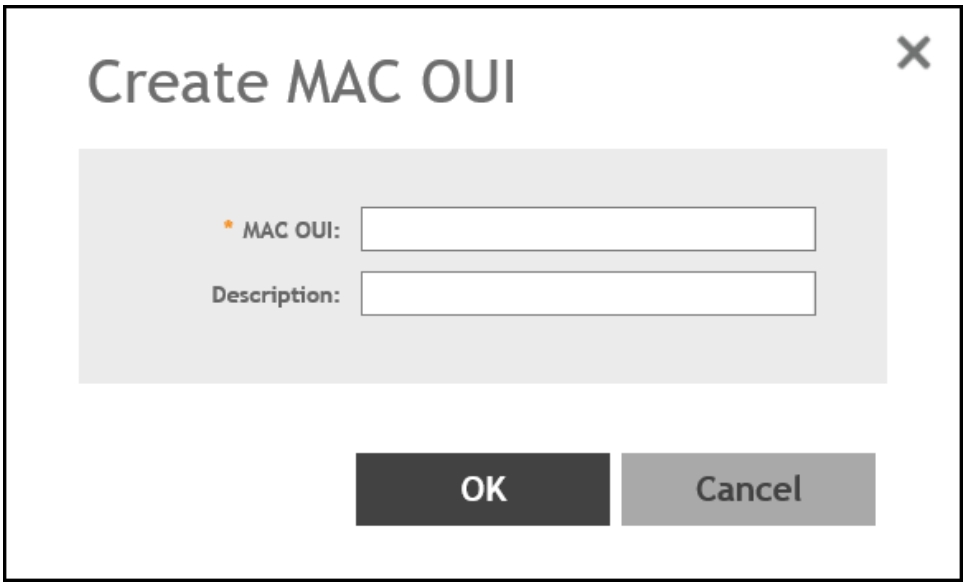
You must enable the AP MAC OUI validation for an AP with a specific organizationally unique identifier (OUI) to be allowed to connect to SZ. If the AP that is not in the OUI list connects to the SZ, then the AP is rejected and event code 186 is generated.

Perform the following procedure to create the MAC OUI address for an AP.

1. Go to **Network** > **Wireless** > **AP Settings** > **AP MAC OUI Validation**.
2. Select **Enable AP MAC OUI Validation**.

3. Click **Create** to create the MAC OUI settings for an AP.

   FIGURE 33 Creating an AP MAC OUI Address



4. Enter the MAC OUI.
5. Click **OK**.

Configuring Packet Capture for APs

User can enable packet streaming feature on both wired and wireless interfaces on specified APs using web UI. You must enable this feature on a per-AP basis. It allows multiple users to execute AP packet capturing, but only a single AP can execute one capturing task at a time. For a single user can capture tasks in multiple APs, but batch operation is not allowed. Only users with full access permission can execute AP packet capturing.

To configure Packet Capture:

1. From the **Network** > **Wireless** > **Wireless LANs** page, select an AP.
2. Click **More** and select **Packet Capture**.

   The **Packet Capture** dialog box appears.

3. Configure the **Capture Mode**:
   - **Stream to Wireshark**
     - **Capture Interface** Select the required wireless or wired interface
       - For 2.4 GHz/5 GHz, update the following details:

         Wireshark station IP: Enter the IP address.

         MAC Address Filter: Enter the MAC address.

         Frame Type Filter: Click the required options from Management, Control, and Data.
       - For Wired Interface, update the following details:

         Wireshark station IP: Enter the IP address.

         LAN Port: Choose the LAN port.
   - **Save to file**
     - **Capture Interface** Select the required wireless or wired interface
       - For 2.4 GHz/5 GHz, update the following details:

         MAC Address Filter: Enter the MAC address.

         Frame Type Filter: Click the required options from Management, Control, and Data.
       - For Wired Interface, update the following details:

         MAC Address Filter: Enter the MAC address.

         LAN Port: Choose the LAN port.
4. Click **Start**.

Configuring AP Switchover

AP switchover is the moving of APs between clusters, and is not confined to clusters that enable cluster redundancy. For normal clusters, you can switchover APs with firmware later or equal to R5.0, regardless of whether it is in the Staging or Non-staging Zone in High-scale platform and Default or Non-default Zone in the Essentials platform. But for a standby cluster in cluster redundancy, APs in the Staging or Default Zone can only be moved to another cluster by switchover.

The following task configures APs to swtichover clusters:

1. From the **Network** > **Wireless** > **Wireless LANs** page, select an AP.
2. Click **More** and select **Switch Over Clusters**.

   The specify **Destination Cluster** dialog box appears.
3. Enter **Control IP** or **FQDN**
4. Click **OK**. A confirmation dialog to trigger the AP switchover appears.
5. Click **Yes**.

   You have configured AP switchover.

Running a Speed Test

You can run a speed test to measure the uplink or downlink performance between the controller or wireless device and an AP in a specific environment.

> **NOTE**
> The speed test traffic between the controller and an AP is not treated as data traffic. Hence, the traffic goes through the Linux Kernel NIC interface of the Controller where the interface is capped to 1 Gbps. Even when the AP's ethernet speed exceeds 1 Gbps, the speed test performance result still shows the upper threshold of 1Gbps.

To run a speed test from a wireless client to an AP, the RUCKUS SpeedFlex application must be installed on the wireless client. The application can be downloaded from Google Play store for Android devices or the Apple App Store for iPhones. The following fields must be configured before performing a run test:

- Destination Address
- Source Address
- Link
- Protocol
- Test Duration

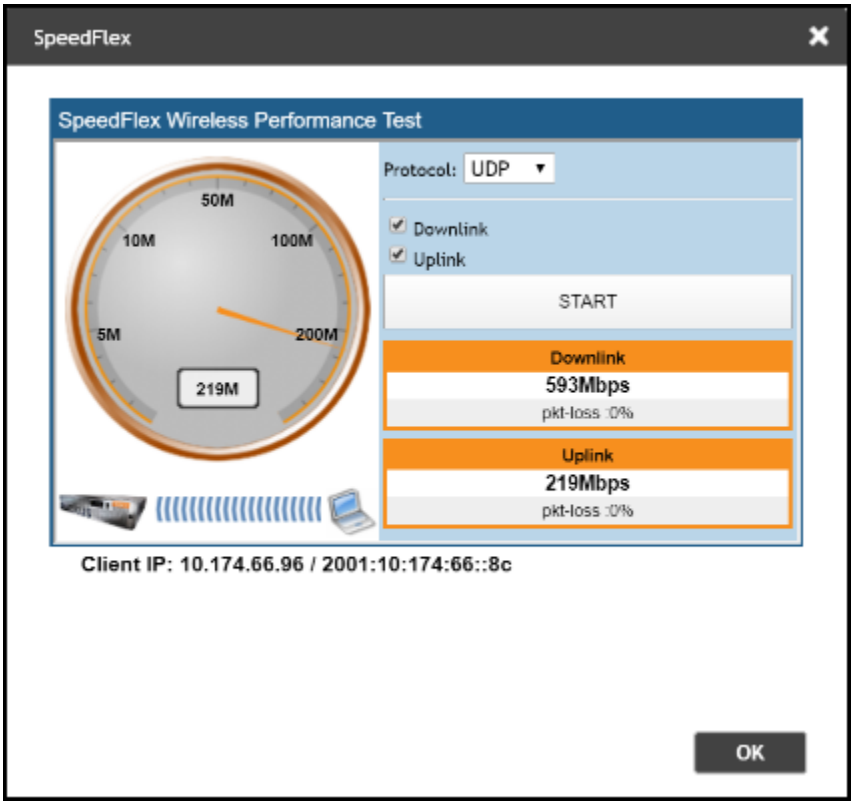
To run a speed test between an AP and the controller, perform the following steps.

1. From the main menu, go to **Network** > **Wireless**, select **Access Points**.
   The **Access Points** page is displayed.
2. Select an AP from the list and then select the **Health** tab.
3. Click **Test Speed**.
   The **SpeedFlex** page is displayed.

4. Click **Start** to test the speed of UDP.

   When the test is complete, the downlink and uplink results are displayed, along with packet loss percentages.

   FIGURE 34 SpeedFlex Test Result



Clients

Working with Wireless Clients

Wireless clients are client devices that are connected to the wireless network services that your managed APs provide. Wireless clients can include smart phones, tablets, and notebook computers equipped with wireless network adapters.

Deauthorizing a Wireless Client

If you want to force wireless clients that joined the wireless network through an authentication portal (for example, a hotspot, guest access or web authentication portal) to reauthenticate themselves, you can deauthorize them. Deauthorized wireless clients remain connected to the wireless network, but these clients will be redirected to the authentication portal whenever they attempt to access network resources.

Follow these steps to deauthorize a wireless client.

1. On the menu, click **Monitor** > **Wireless Clients** > **Clients** > **Deauthorize.**

2. From the list wireless clients, locate the client that you want to deauthorize. If you have a large number of wireless clients and you know the MAC address of the client, enter the MAC address in the search box, and then press Enter to search for the client.
3. When you have located the client, select it, and then click the **Deauthorize** button above the table.

   The table refreshes, and then the client that you deauthorized disappears from the list.

Blocking a Wireless Client

When a user associates a wireless client device with an AP that the controller is managing, the client device is recorded and tracked. If, for any reason, you need to block a client device from accessing the network, you can do so from the web interface.

A few reasons why you might consider blocking a wireless client device include:

- Network abuse
- Violation of acceptable use policy
- Theft
- Security compromise

Follow these steps to block a wireless client from accessing the SmartZone network.

1. On the menu, click **Monitor** > **Clients** > **Wireless Clients**.
2. From the list wireless clients, locate the client that you want to block. If you have a large number of wireless clients and you know the MAC address of the client, enter the MAC address in the search box, and then press <Enter> to search for the client.
3. When you have located the client, select it, and then click the **Block** button above the table.

You have completed blocking a wireless client.

Unblocking a Wireless Client

If you want to allow a client that you previously blocked to access the SmartZone network, you can unblock it.

Follow these steps to unblock a wireless client.

1. On the menu, click **Monitor** > **Clients** > **Wireless Clients**.
2. Click the **Blocked Client** tab.
3. From the list of blocked clients, locate the client that you want to unblock. If you have a large number of blocked clients and you know the MAC address of the client, enter the MAC address in the search box, and then press **<Enter>** to search for the client.
4. When you have located the client, select it, and then click the **Delete** button above the table.

   The table refreshes, and then the client that you want to unblock disappears from the list.

You have completed unblocking a wireless client.

Disconnecting a Wireless Client

If you need to temporarily disconnect a wireless client from the wireless network, you can do so from the web interface. For example, if you are troubleshooting problematic network connections, you might have to manually disconnect wireless clients as part of the troubleshooting process.

Follow these steps to disconnect a wireless client from the WLAN to which it is connected.

1. On the menu, click **Monitor** > **Clients** > **Wireless Clients.**
2. From the list wireless clients, locate the client that you want to disconnect. If you have a large number of wireless clients and you know the MAC address of the client, enter the MAC address in the search box, and then press <Enter> to search for the client.

3. When you have located the client, select it, and then click the **Disconnect** button above the table.

   The table refreshes, and then the client that you disconnected disappears from the list.

Working with Wired Clients

Wired clients are client devices that are connected to the Ethernet ports of APs managed by the controllers, and thereby are connected to the wired network services that your managed APs provide.

Viewing a Summary of Wired Clients

View a summary of wired clients that are currently associated with all of your managed access points.

Go to **Monitor** > **Clients** > **AP Wired Clients.**

The **AP Wired Clients** page appears and displays a table that lists all clients that are currently associated with your managed access points.

To view only wired clients that belong to a particular zone, click the zone name in the zone tree. The table refreshes and displays only the clients that belong to the zone you selected.

The following table lists the wired client details.

TABLE 23 Wired client details

Column Name	Description
MAC Addres	Displays the MAC address of the wired client
Username	Displays the name of the user logged on to the wire client
IP Address	Displays the IP address assigned to the wired client
AP MAC	Displays the MAC address of the AP
AP Name	Displays the name assigned to the access point
LAN	Displays the LAN ID assigned to the wired client
VLAN	Displays the VLAN ID assigned to the wired client
Auth Status	Indicates whether the wired client is authorized or unauthorized to access the WLAN service

To know more about how the 802.1X configuration works for the port refer Creating an Ethernet Port Profile on page 479.

Deauthorizing a Wired Client

If you want to force wired clients that joined the wired network through an authentication portal to reauthenticate themselves, you can deauthorize them. Deauthorized wired clients remain connected to the wired network, but these clients will be redirected to the authentication portal whenever they attempt to access network resources.

Follow these steps to deauthorize a wired client.

1. Go to **Monitor** > **Clients** > **AP Wired Clients.**
2. From the list wired clients, locate the client that you want to deauthorize. If you have a large number of wired clients and you know the MAC address of the client, enter the MAC address in the search box, and then press **Enter** to search for the client.
3. When you have located the client, select it, and then click the **Deauthorize** button above the table.

   The table refreshes, and then the client that you deauthorized disappears from the list.

Switch Clients

The Switch Clients tab displays the information of wireless and wired clients.

The user can view summary of wireless and wired clients associated with Access Points.

Go to **Monitor** > **Clients** > **Switch Clients.**

To view clients associated to a particular zone, select **Zone Name** in the zone tree. This displays only clients associated to the selected zone.

TABLE 24 Switch Client

Column Name	Description
Status	Indicates whether the client is online or offline.
Device MAC	Displays the MAC address of the device.
Device Type	Displays the type of device used by the client.
Last Seen	Displays the last login information.
Authentication Type	Displays the authentication flow used by the client.
User	Displays the user details.
Port	Displays the port number.
Switch	Displays the switch details.
VLAN	Displays the assigned VLAN ID.
Description	Displays the description of the client.
Past 24 Hour Auth	Displays if the client was authorized in the last 24 hours.

Troubleshooting and Diagnostics

Troubleshooting

Troubleshooting Client Connections

Network administrators can connect to client devices and analyze network connection issues in real time.

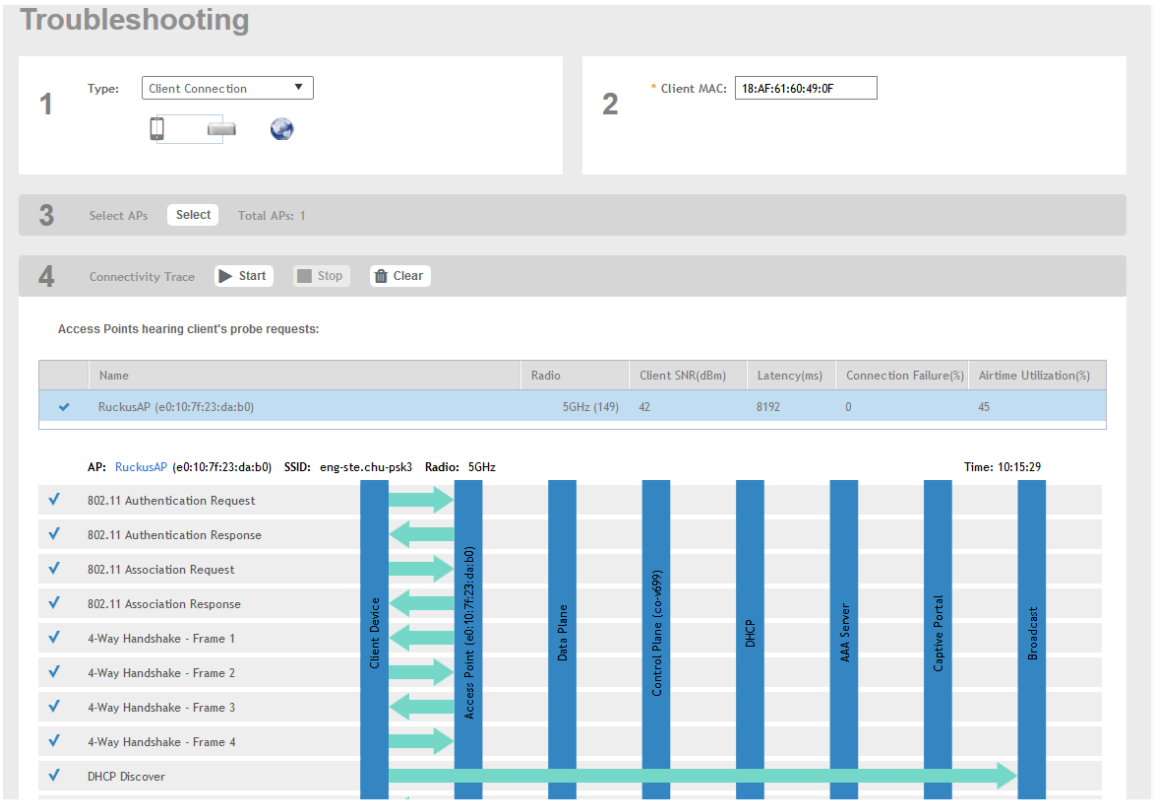
The network administrator types the MAC address of the client device and starts services to identify the connectivity issue. The APs assigned to the client device relay data frames from the device to the controller. The administrator can analyze these frames to determine which stage of the connection is causing problems.

Perform the following steps to troubleshoot client connections.

1. In the main menu, click **Monitor**. Select **Troubleshooting** from **Troubleshooting & Diagnostics** menu.

   This displays **Troubleshooting** window as shown in the below example.

FIGURE 35 Troubleshooting - Client Connections



2. In Type, select **Client Connection** from the drop-down menu.
3. In **Client MAC**, click settings, and choose **Historical Client** or **Connected Client** to view the client list.
4. Enter the MAC address of the client device with connectivity issues, or select the client device from the drop-down, which lists the **MAC Address**, **Hostname**, and **OS Type**.

   You can search or sort the drop-down list by Client MAC, Hostname, or OS Type.
5. In Select APs, click **Select**.

   The **Select APs** page is displayed.
6. Select an AP to communicate between the client and the controller, and then click **OK**.

7. In Connectivity Trace, click **Start**.

   The controller configures the APs to receive data frames from the target client and relay frames to the controller based on the client filter.

   The APs that receive probe requests from the target client are listed in a table, along with the AP's operating channel and the RSSI at which the client's frames were received. This stage of the connection identifies whether there are acceptable APs for the client to connect to.
   The following items are displayed:

   - AP Name and MAC Address
   - Radio: The 2.4 or 5 GHz radio of the AP and the channel number the radio is operating on
   - Client SNR: The signal-to-noise ratio received, in dB
   - Latency: Time delay in connecting the AP to the client
   - Connection Failures: The percentage of AP-client connection attempts that failed
   - Airtime Utilization: The percentage of air time that was used by the client to transfer data

   At this stage, the tool displays the statuses `Client is in a discovery state and not currently connected` (when the tool starts or when the client is already connected to an AP) and `Client is attempting a new connection` (when the target client sends an 802.11 authentication request frame to an AP to initiate a connection).

   Use the list of APs that communicated with the client to determine whether the client chose the best AP based on signal quality and other health metrics.

   When the client sends an 802.11 authentication request frame, a flow diagram depicting different stages of the AP-client connection is initiated. This sends a trigger frame to the AP, and it is highlighted from the list for reporting APs.

   The Flow ladder in the diagram shows the step-by-step exchange of information between devices during the connection process. As the steps are completed, colored arrows are displayed when the step depicts a warnings (yellow) or event (for example, red for failure). Typical warning scenarios include time delays or a failed negotiation for an unsupported EAP type. Failure conditions are also highlighted as red arrows, typically when the connection itself fails.

   NOTE
   The following authentication types are supported:

   - Open
   - PSK (WPA2-Personal)
   - 802.1X (PEAP, TTLS, TLS, SIM)
   - WISPr

8. Click **Stop** to terminate the connection between the AP and the client.

VIDEO
Client Connection Troubleshooting Demo. Overview of how to use the Client Connection tool.
Click to play video in full screen mode.

Troubleshooting through Spectrum Analysis

Interference between wireless devices is seen to increase dramatically due to the increase in the number of device used, and the availability of only three non-interfering channels in 802.11. This reduces the performance of the wireless network, therefore, it is important to monitor the spectrum usage in a particular area and efficiently allocate the spectrum as needed to wireless devices.

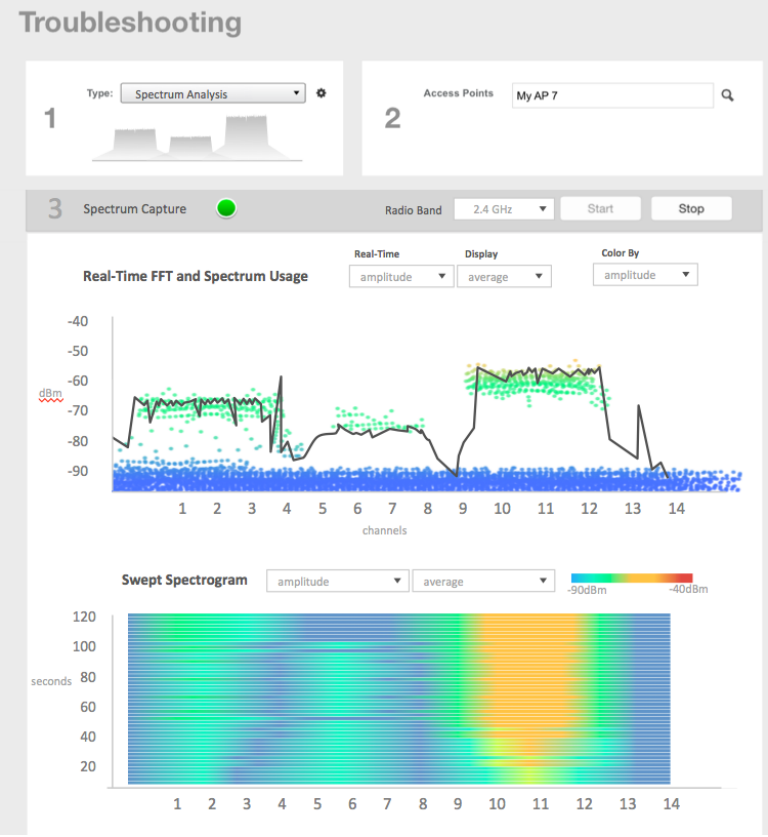
In addition, spectrum analysis provides the flexibility to troubleshoot issues remotely, identify sources of interferences within the network and allow administrators access to the RF health of the network environment.

APs which are put in spectrum-mode transmit data to the controller, which in turn displays the data in specturm-mode for analysis.

1. In the main menu, click **Monitor**. Select **Troubleshooting** from **Troubleshooting & Diagnostics** menu.

   This displays **Troubleshooting** window as shown in the below example.

FIGURE 36 Troubleshooting - Spectrum Analysis



2. In Type, select **Spectrum Analysis** from the drop-down menu.
3. In AP MAC Address, select the AP that needs to be in the spectrum analysis-mode.

4. In Spectrum Capture, select the radio frequency values (2.4GHz or 5GHz) for the analysis from the **Radio** option.

   The 2.4GHz band spans from 2400 - 2480 GHz and 5GHz band spans from 5.15 - 5.875 GHz.

   You can select and view the spectrum analysis trends in these graphs:

   - Spectrum Usage: This chart uses a color-based view to show collections of data points over time. As more data samples are measured at a specific frequency and amplitude coordinate, the color shown at that coordinate will change. If you choose to view colors by amplitude, the warm colors depict higher amplitude and cool colors lower amplitudes. If you view the colors by density, the warm colors depict a high number of samples at a given coordinate and cool colors show low number of samples at a given coordinate.
   - Real-Time FFT : This chart is a second-by-second (2sec) update of measured data across the band. If you view by Amplitude (signal strength), then the chart displays both average and maximum amplitudes of energy measured across the band for that sample period. If you view by Utilization (duty cycle), then the chart displays the percentage (%) of time at which the frequency is utilized at an amplitude above N. The amplitude threshold is configurable but the default is -85dBm.
   - Swept Spectrogram: This chart displays a waterfall of color over time, where each horizontal line in the waterfall represents one sample period (e.g. 2 seconds), and the full waterfall display spans 2 minutes of time (60 sample bins of 2sec each). There are two display options for the spectrogram chart:
     - Amplitude: Shows both average and maximum amplitude of energy measured across the band for that sample period.
     - Utilization: Shows the percentage of time at which the frequency is utilized at an amplitude above N. The amplitude threshold is configurable but the default is -85dBm.

5. After you select the parameters that you want to use to view the graphs, click **Start**.
6. Click **Stop** to terminate viewing spectrum analysis trends.

Support Bundle

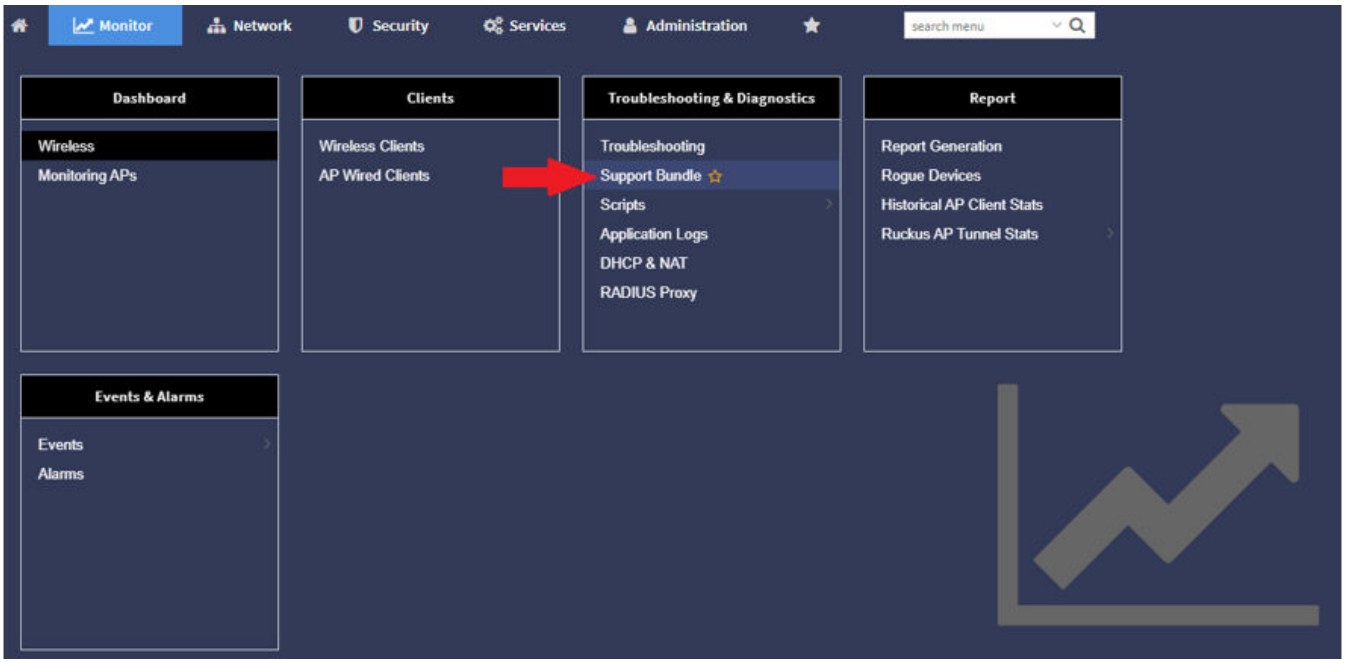
Support Bundle allows you to gather the bundle log files from the controller and APs.

Complete the following steps to enable Support Bundle.

1. From the controller web interface, go to **Monitor** > **Troubleshooting & Diagnostics** > **Support Bundle**.

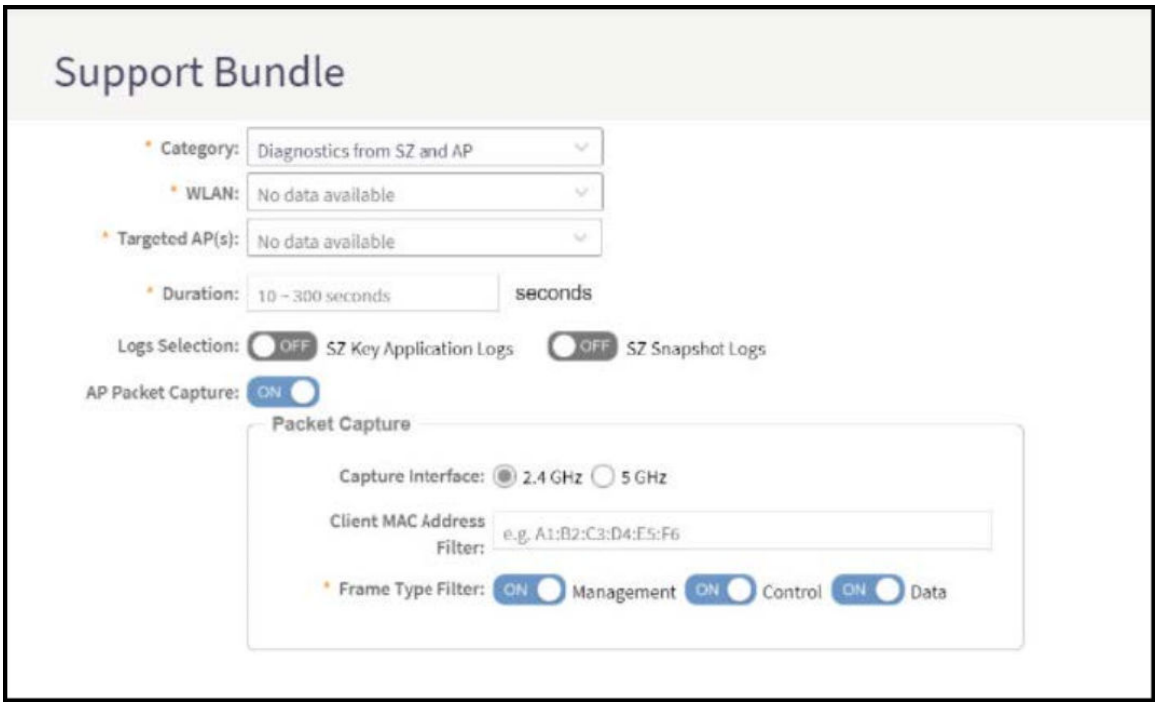
   The **Support Bundle** dialog box is displayed.

   FIGURE 37 Accessing the Support Bundle



2. Configure the following options:

FIGURE 38 Support Bundle Dialog Box



- **Category**: Select the type of support bundle from the list.
- **WLAN**: Select the WLAN on which the log collection will be performed from the list.
- **Targeted AP(s)**: Select the APs from the list. The list contains the APs that have served the selected WLAN and are limited to the same zone.

  NOTE
  Any APs with a firmware version earlier than SmartZone 6.1 are disabled. A maximum of three APs can be displayed for the selected WLAN.

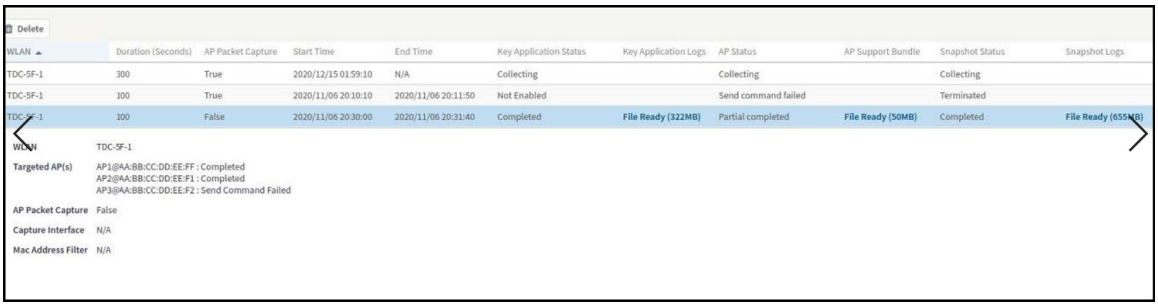
  - The disconnected APs cannot be selected by the user.
  - When the support bundle process is running, user cannot change the **Application Log**.

- **Duration**: Enter the time period for log selection (in seconds). The minimum value is 10 seconds, and the maximum value is 300 seconds.
- **Logs Selection**: Set **SZ Key Application Logs** or **SZ Snapshot Logs** to **ON**, this allows the application to collect different types of logs. If you use **SZ Key Application Logs**, a message is displayed to indicate that the application log level changes and this affect the application performance.
- **AP Packet Capture**: Set **AP Packet Capture** to **ON**, and complete the following options:
  - **Capture Interface**: Select **2.4. GHz** or **5 GHz** for the wireless interface.
  - **Client MAC Address Filter**: Enter the MAC address.
  - **Frame Type Filter**: Set the required options (**Management**, **Control**, and **Data**) to **ON**.

3. Click **OK**.

4. To download Support Bundle output files, click **File Ready** in the **Key Application Logs** or **AP Support Bundle** columns.

   FIGURE 39 Support Bundle Download Options



Scripts

Applying Scripts

New AP models and firmware updates are supported without the need to upgrade the controller image by using AP patch files and diagnostic scripts.

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

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

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

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

   Click **Delete** to delete scripts.
5. Click **Apply Patch** to apply the patch file to the AP model or firmware as appropriate.

You have successfully applied scripts to the controller AP.

Uploading AP CLI Scripts

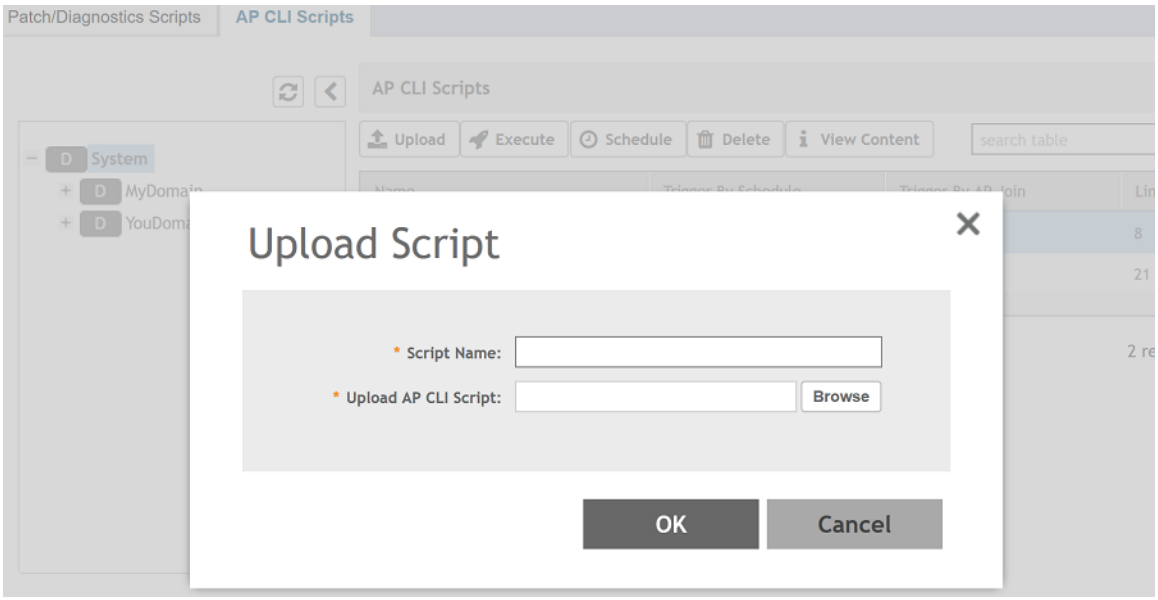
You can upload AP CLI scripts to the controller which make the controller compatible with new AP models and new firmware without the need to upgrade the controller image.

1. In the main menu, click **Monitor**, under **Troubleshooting & Diagnostics** menu, hover the mouse over **Scripts** and click **Patch/Diagnostic Scripts** .
2. Select the **AP CLI Scripts** tab.
3. From the domain tree, choose the AP zone for which you want to apply the script.

4. Click **Upload**.

   The Upload page appears.

   FIGURE 40 Uploading scripts



5. In **Script Name**, enter the name of the script you want to upload.
6. Click **Browse** to select an AP CLI script that you want to upload.
7. Click **OK** to apply the AP CLI script file to the AP zone.

You have successfully uploaded AP CLI scripts to the controller AP.

Executing AP CLI Scripts

You can upload AP CLI Scripts to be run on APs within selected zones, and execute them immediately or on-demand.

1. In the main menu, click **Monitor**, under **Troubleshooting & Diagnostics** menu, hover the mouse over **Scripts** and click **Patch/Diagnostic Scripts** .
2. Select the **AP CLI Scripts** tab.
3. From the domain tree, choose the domain in which the AP is present.
4. Select the script from the list of scripts in the **AP CLI Scripts** table.

5. Click **Execute**.

   The **Execute Script** page appears.

   FIGURE 41 Executing script



6. Select one or more zones from the domain tree.
7. Click **OK** to run the AP CLI script on the AP zone.

The controller runs the selected script on the specified zone.

Scheduling AP CLI Scripts

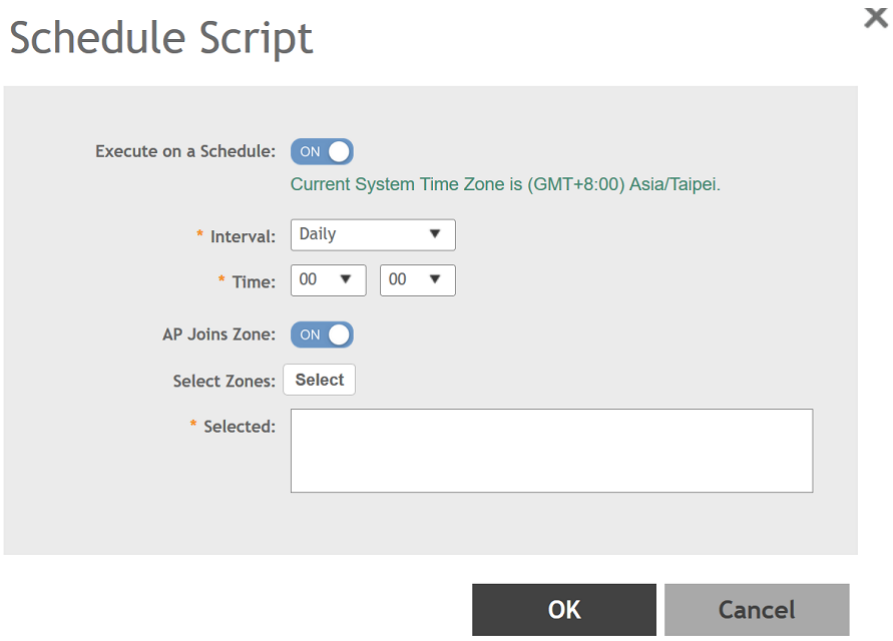
You can upload AP CLI Scripts to be run on APs within selected zones. You can also schedule the script to be run on the APs at a particular time or when the AP joins the zone.

1. In the main menu, click **Monitor**, under **Troubleshooting & Diagnostics** menu, hover the mouse over **Scripts** and click **Patch/Diagnostic Scripts** .
2. Select the **AP CLI Scripts** tab.
3. From the domain tree, choose the domain in which the AP is present.
4. Select the script from the list of scripts in the **AP CLI Scripts** table.

5. Click **Schedule**.

   The **Schedule Script** page appears.

   FIGURE 42 Scheduling scripts



6. Configure the following:
   - Execute on a Schedule: Enable this option to execute the script based on the current system time which is displayed.
   - Interval: select the time interval within which you want to schedule the execution. Options include Daily, Weekly and Monthly.
   - Time: from the drop-down menu, select te hours and minute when the script must be executed
   - AP Joins the Zone: enabling this will ensure the script is run on the AP when it joins a particular zone.
7. To select the zone, click **Select**.

   The **Select Zone** page appears. Identify and select the zone. The selected zone is populated in the **Selected** area.
8. Click **OK**.

The schedule is configured and the script will run on the AP as planned.

Viewing Scripts

You can open the AP CLI script and view the script details.

1. From the main menu, click **Monitor**.
2. Under **Troubleshooting & Diagnostics**, hover over the **Scripts**, and click **Patch/Diagnostic Scripts**.
3. Select the **AP CLI Scripts** tab.
4. From the domain tree, choose the domain in which the AP is present.

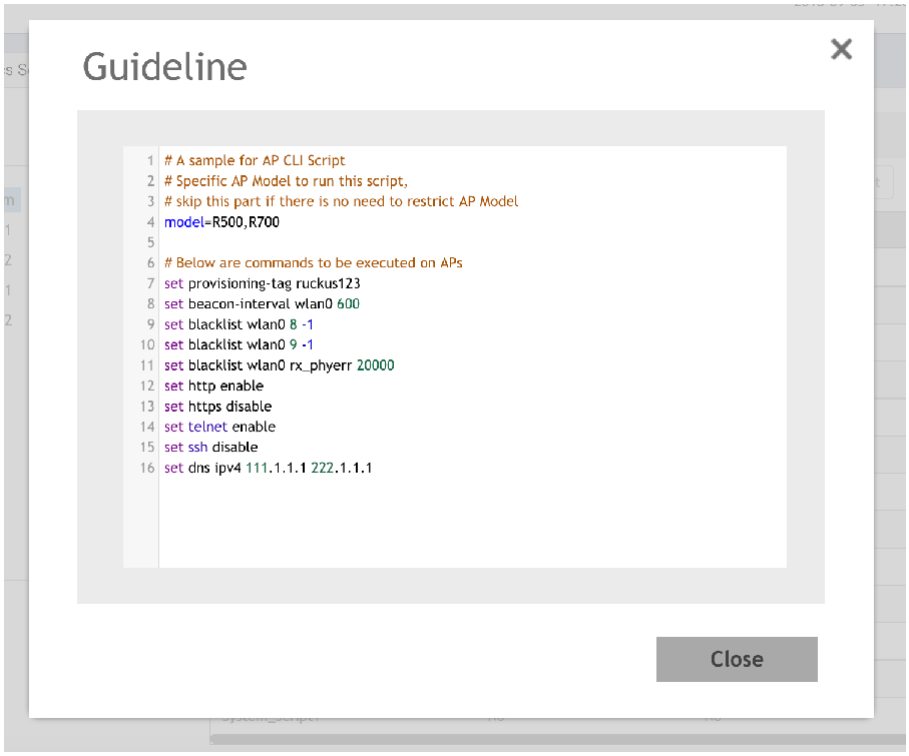
5. From the **AP CLI Scripts** tab, select the script from the list of scripts.

   NOTE
   For more information on the AP CLI Commands, use the help command on the AP console.

6. Click **View Content**.

   The **Guideline** dialog box is displayed.

   FIGURE 43 Viewing Script Details



7. Click **Close**.

Viewing Script Execution Summary

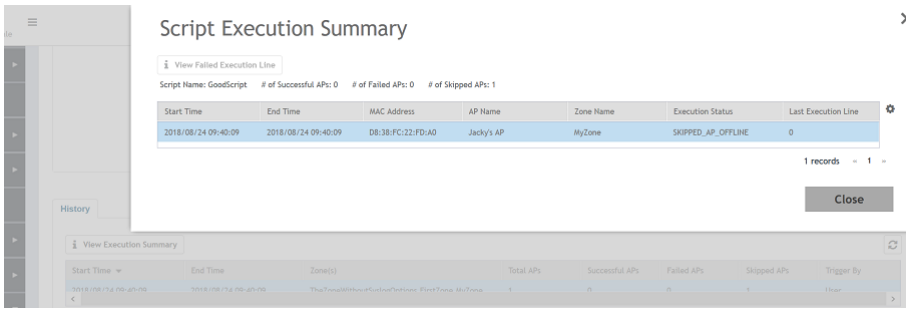
After an AP CLI script is executed on-demand or as per schedule, you can view details of the execution from the **History** tab.

1. In the main menu, click **Monitor**, under **Troubleshooting & Diagnostics** menu, hover the mouse over **Scripts** and click **Patch/Diagnostic Scripts** .
2. Select the **AP CLI Scripts** tab.
3. From the domain tree, choose the domain in which the AP is present.
4. Select the script from the list of scripts in the **AP CLI Scripts** table.
5. In the History tab below, you will see the list of scripts that were executed.

6. To view the execution summary of a script, select a script from this list and click **View Execution Summary**.

   You will be able to view information such as the script name, number of execution attempts that were successful, failed and skipped, start and end time of the execution process, MAC address of the AP, AP and zone names, execution status and last line of the execution.

   FIGURE 44 Script execution summary



7. Click **Close**.

Application Logs

Viewing and Downloading Logs

The controller generates logs for all the applications that are running on the server.

1. In the main menu, click **Monitor**, under **Troubleshooting & Diagnostics** menu, click **Application Logs** . This displays **Application Logs** screen.
2. Click the drop-down list from **Select the Control Plane** to download logs.
3. Select the **Upload to current node** check-box.
4. Choose the type of logs and click to download. The options are:

Option	
Download Logs	To download all logs for the selected application.
Download All Logs	To download all available logs from the controller. Go to your web browsers default download location and verify that the TGZ file was downloaded successfully. You must use your preferred compression/decompression program to extract the log files from the TGZ file. When the log files are extracted (for example, `adminweb.log`, `cassandra.log`, `communicator.log`, etc.), use a text editor to open and view the log contents.
Download Snapshot Logs	To download snapshot logs that contain system and configuration information, such as the AP list, configurations settings, event list, communicator logs, SSH tunnel lists, etc. If you triggered the controller to generate a snapshot from the CLI, you have the option to download snapshot logs from the web interface. Go to your browser's default download folder, and then verify that the snapshot log file or files have been downloaded successfully. Extract the contents of the tar file.

You have successfully completed downloading log files/snapshot logs from the controller.

Available System Logs for platforms

The controller generates logs for all the applications that are running on the server.

The following table lists the controller applications that are running.

TABLE 25 Controller applications and log types for vSZ-H and SZ300

Application	Description
Cassandra	The controller's database server that stores most of the run-time information and statistical data
Communicator	Communicates with access points and retrieves statuses, statistics, and configuration updates
Configurer	Performs configuration synchronization and cluster operations (for example, join, remove, upgrade, backup, and restore)
Diagnostics	An interface that can be use to upload RUCKUS scripts (.ksp files) for troubleshooting or applying software patches. This interface displays the diagnostic scripts and system patch scripts that are uploaded to a node.
EventReader	Receives event messages from access points and saves the information into the database
LogMgr	Organizes the Application Logs into a common format, segregates them, and copies them into the respective Application log file
MdProxy	MdProxy on AP and controller connect to AP-MD and controller-MD respectively. MdProxy on controller receives messages and retrieves the message header. It also forwards the response to controller-MD. This message is sent to the MdProxy on AP through AP-MD. MdProxy on the AP removes the MSL header and responds to the connection on which the request was received.
Memcached	The controller's memory cache that stores client authentication information for fast authentication or roaming
MemProxy	Replicates MemCached entries to other cluster nodes
Mosquitto	A lightweight method used to carry out messaging between LBS and APs
MsgDist	The Message distributor (MD) maintains a list of communication points for both local applications and remote MDs to perform local and remote routing
NginX	Is a web server that is used as a reserve proxy server or a HTTP cache
Northbound	As an interface between SP and AAA, it performs UE authentication and handles approval or denial of UEs to AP.
RadiusProxy	Sets the RADIUS dispatch rules and synchronizes configuration to each cluster node
Scheduler	Performs task scheduling and aggregates statistical data
SNMP	Provides a framework for the monitoring devices on a network. The SNMP manager is the system is used to control and monitor the activities of network hosts using SNMP. As an agent that responds to queries from the SNMP Manager, SNMP Traps with relevant details are sent to the SNMP Manager when configured.
SubscriberManagement	Maintains local user credentials for WISPr authentication.
SubscriberPortal	Internal portal page for WISPr (hotspot)
System	Collects and sends log information from all processes
Web	Runs the controller management web server

DHCP & NAT

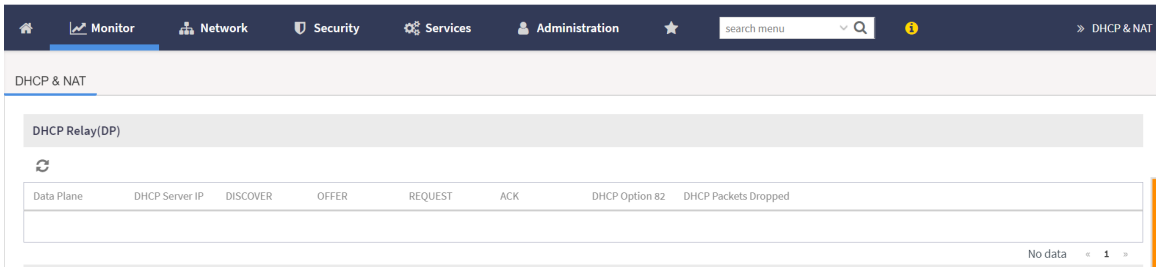
Viewing DHCP and NAT Information

You must be aware of the DHCP and NAT information of the controller to monitor the health of the controller.

1. Go to **Monitor** > **Troubleshooting&Diagnostics** > **DHCP & NAT** .

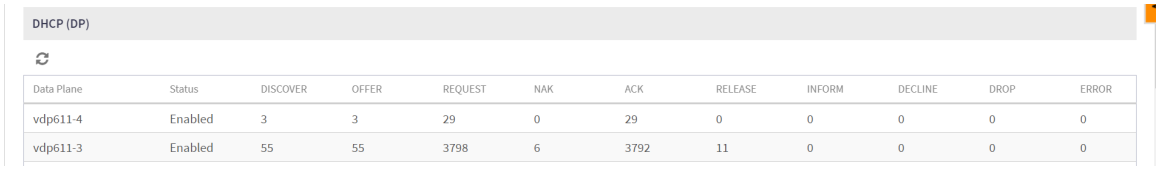
2. Select the following tabs to monitor:
   - **DHCP Relay (DP)**: To monitor the DHCP relay information of the Data Planes. Displays information the of DHCP relay packets when DHCP relay is enabled in **Core Network Tunnel** > **Bridge or L2oGRE**.

     FIGURE 45 Diagnostics - DHCP Relay



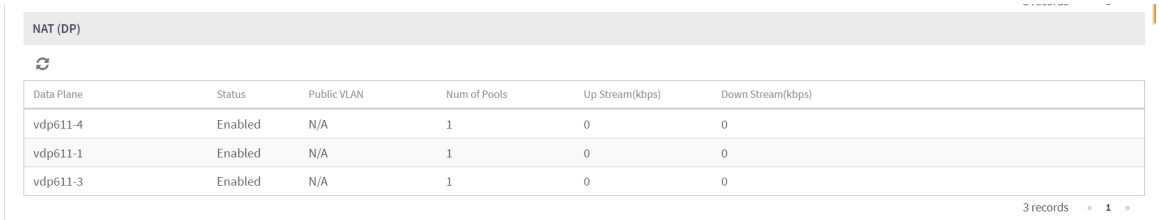
   - **DHCP (DP)**: To monitor the DHCP DP information of the Data Planes. Display information of the DP DHCP server packets and the number of IPs assigned .

     FIGURE 46 Diagnostics - DHCP DP



   - **NAT (DP)**: To monitor the NAT DP information of the Data Planes. Displays information of the DP NAT server packets and the number of used ports.

     FIGURE 47 Diagnostics - NAT DP



Radius Proxy

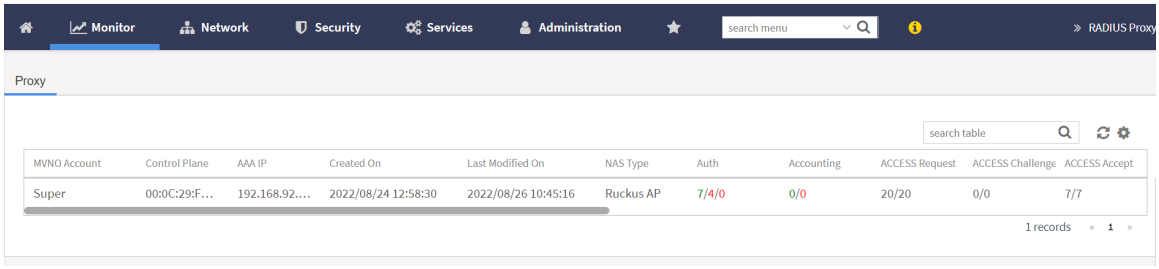
Viewing RADIUS Proxy Settings

You must be aware of the RADIUS Proxy settings on the controller to monitor the health of the controller.

Go to **Monitor** > **Troubleshooting and Diagnostics** > **RADIUS Proxy**.

The **Proxy** page appears displaying the RADIUS settings.

FIGURE 48 Diagnostics - RADIUS Proxy



Reports

Report Generation

Creating Reports

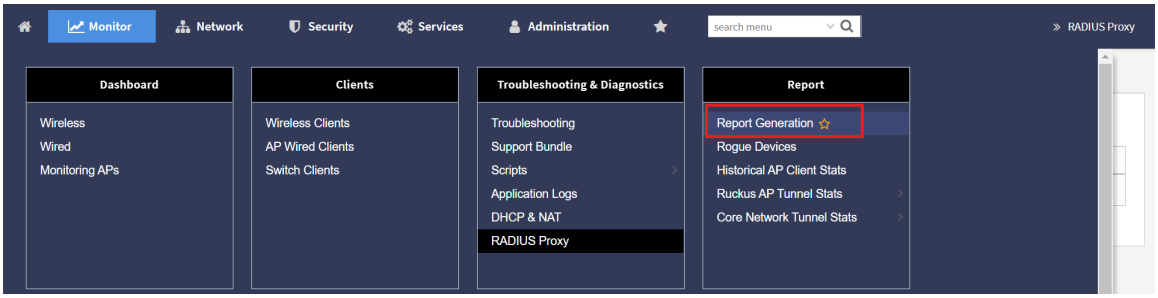
You can create reports to obtain a historical view of the maximum and minimum number of clients connect to the system, to view client number at different time intervals and to view the traffic statistics of switches.

To create a new report:

1. In the main menu, click **Monitor**>**Report** >**Report Generation**.

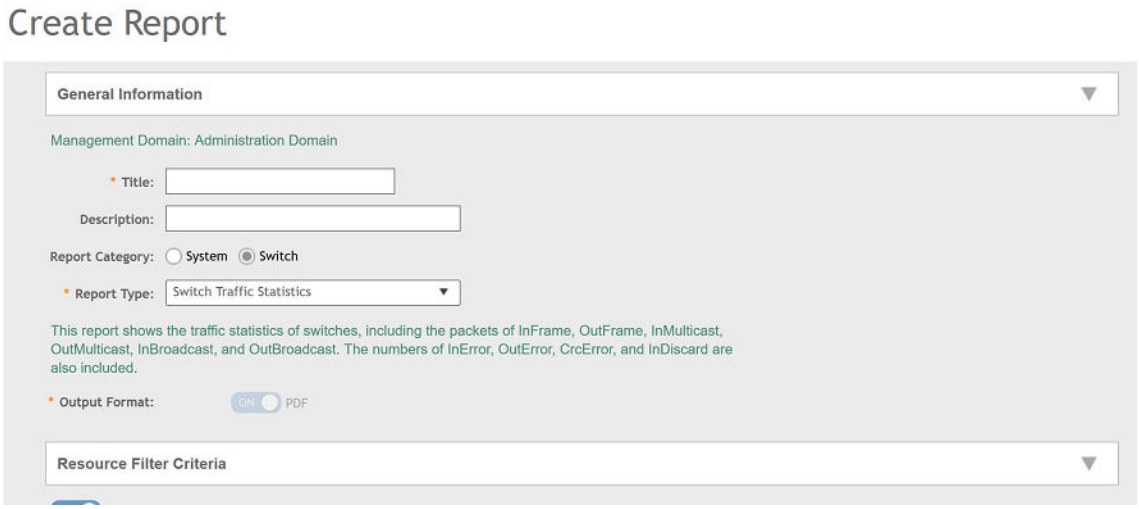
   This displays the **Report Generation** screen.

   FIGURE 49 Report Generation Screen



2. Click **Create**, Figure 50 appears.

FIGURE 50 Create Reports Screen



3. Enter the required parameters as explained in Table 26.
4. Click **OK**.

TABLE 26 Report Parameters

Field	Description	Your Action
General Information		
Title	Indicates the report name.	Enter a title for the report.
Description	Describes the report type.	Enter a short description.
Report Category	Provides an option to generate reports for System or Switch devices in the network.	Select System or Switch as appropriate.
Report Type	Specifies the report type	Select the required report.
Output Format	Specifies the report output format.	Select the required report output format.
Resource Filter Criteria		
Device	Indicates the level of resource filtering for which you want to generate the report. For example: Management Domains, AP Zone or Access Point (if you select System option) and Switch.	Enter the device/switch name or select the device/ switch from the list and choose the option.
SSID	Indicates the SSID for which you want to generate the report.	Select the check box and choose the SSID for which you want the report. You can select **All SSIDs** to generate reports for all the SSIDs available. This option is convenient as you do not have to update the resource filter criteria periodically.
Radio	Indicates the frequency for which you want to generate the report.	Select the check box and choose the required frequency: • **2.4G** • **5G**
Time Filter		
Time Interval	Defines the time interval at which to generate the report.	Select the required time interval.
Time Filter	Defines the time duration for which to generate the report.	Select the required time filter.
Schedules		

TABLE 26 Report Parameters (continued)

Field	Description	Your Action
Enable/Disable	Specifies the scheduled time when a report must be generated. By default, the current system time zone is also displayed.	By default the option is disabled. Select **Enable** and select the **Interval**, **Hour** and **Minute**. You can add multiple schedules. You can also click **Add New** to include more schedules.
Email Notification		
Enable/Disable	Triggers an email notification when the report is generated.	By default the option is disabled. Select **Enable** and click the **Add New** and enter the email address. You can add multiple email addresses.
Export Report Results		
Export Report Results, Enable/Disable	Uploads the report results to an FTP server.	By default the option is disabled. Select **Enable** and select the **FTP Server**. Click **Test** to ping the FTP server and test if you are able to establish a connection.

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

Generating Reports

To generate a report:

1. Go to **Monitor** > **Report** > **Report Generation** . Figure 49 on page 85 appears.
2. Select the required report from the list and click **Generate**. The Report Generated form appears.
3. Click **OK**, the report will be generated and listed in the Report Results area.
4. Select the required format from the **Result Links** column and click **Open**.

Rogue Devices

Viewing Rogue Devices

To view the rogue APs or rogue clients, select **Access Point** or **Client** from the **Device Type** list.

If you enabled rogue AP or rogue client detection when you configured the common AP settings (refer to Configuring APs), click **Monitor** > **Report** > **Rogue Devices**. Under **Device Type**, select **Access Point** or **Client**. The **Rogue Devices** page displays all the rogue APs or rogue clients that the controller has detected on the network, including the following information:

- **Rogue MAC**: The MAC address of the rogue AP.
- **Type**: The client has a different set of rogue types (for example, rogue, normal rogue AP, not yet categorized as malicious or non-malicious).
- **Classification Policy**: The rogue classification policy associated with the rogue AP.
- **Channel**: The radio channel used by the rogue AP.
- **Radio**: The WLAN standards with which the rogue AP complies.
- **SSID**: The WLAN name that the rogue AP is broadcasting.
- **Detecting AP Name**: The name of the AP.
- **Zone**: The zone to which the AP belongs.
- **RSSI**: The radio signal strength.

- **Encryption**: Indicates whether the wireless signal is encrypted.
- **Detected Time**: The date and time that the rogue AP was last detected by the controller.

Marking Rogue Access Points

To mark a rogue (or unauthorized) Access Point as known.

In the list of discovered rogue access points, administrator cannot classify the rogue type. However, administrator can manually override the discovered rogue AP as Known or Malicious the AP.

To mark a rogue AP as known or malicious, perform the following:

1. From the left pane, click **Report** > **Rogue Devices**. This displays the **Rogue Devices** page.
2. Select the rogue AP from the list and select **Mark as Known or Malicious or Ignore** from the drop-down list. The classification **Type** of the rogue AP changes as per the selection. You can also select the rogue AP from the list and click **Unmark** to change the classification.

Locating a Rogue Device

You can identify the estimated location area of a rogue AP or rogue client on a map. Managed APs that detect the rogue APs and rogue clients are also visible on the map.

Perform the following procedure to locate a rogue AP or rogue client.

1. From the left pane, select **Monitor** > **Report** > **Rogue Devices**.
2. In the **Rogue Devices** page, select **Rogue AP** or **Client** from the **Device** list.
3. Click **Locate Rogue**.

   The **Rogue AP Location** page appears locating the rogue AP or rogue client. You can select from the following options:

   - **Map**: View the location in street view.
   - **Satellite**: View the location as satellite imagery.
   - **+**: Zoom in on the location.
   - **-**: Zoom out of the location.

   You can find the following information about rogue and detecting APs:

   - Rogue APs: MAC address, type, and SSID
   - Detecting APs: MAC address, name, and RSSI
4. Click **OK**.

Historical AP Client Stats

Viewing AP Client Statistics

AP Client Statistics is a cumulative value per session and one entry is created per session. Data is reported every 60 seconds and is not bin data. The user interface displays the table and its corresponding graph chart. The two representations are synchronized and controlled by the search criteria. For performance reasons, the total counters per DP or per GGSN IP for each bin is precalculated.

To view AP Client Statistics:

1. From the left pane, select **Monitor**>**Report** > **Historical Client Stats**. The Ruckus AP Client page appears.
2. Update the parameters as explained in Table 27.

3. Click:
   - **Load Data**— To view the report in the workspace.
   - **Export CSV**—To open or save the report in CSV file format.

TABLE 27 AP Client Statistics Report Parameters

Field	Description	Your Action
Time Period	Indicate the time period for which you want to view the report.	Move the slider to set the duration.
Zone Name	Specifies the zone for which you want to view the report.	Enter the zone name or choose the zone from the list.
Client MAC	Specifies the MAC.	Enter the client MAC.
Client IP	Indicates the client IP.	Enter the client IP address.
MVNO Name	Indicates the mobile virtual network operator name.	Choose the MVNO.

Table 28 contains historical client statistics report based on the UE session statistics.

TABLE 28 AP Client Statistics Report Attributes

Attribute	Type	Description
Start	Long	Indicates the session creation time.
End	Long	Indicates the session end time.
Client MAC	String	Indicates the Mac address of the client.
Client IP Address	String	Indicates the IP address of the client.
Core Type	String	Indicates the core network tunnel type.
MVNO Name	String	Indicates the mobile virtual network operator name.
AP MAC	String	Indicates the Client AP MAC.
SSID	String	Indicates the SSID
Bytes from Client	Long	Indicates the number of bytes received from the client.
Bytes to Client	Long	Indicates the number of bytes sent to the client.
Packets from Client	Long	Indicates the number of packets received from the client.
Packets to Client	Long	Indicates the number of packets sent to the client.
Dropped Packets from Client	Long	Indicates the number of packets dropped from the client.
Dropped Packets to Client	Long	Indicates the number of packets dropped to the client.

Ruckus AP Tunnel Stats

Viewing Statistics for Ruckus GRE Tunnels

The web interface displays the table and its corresponding graph chart. The two representations are synchronized and controlled by the search criteria. For performance reasons, the total counters per DP or per AP for each bin may be pre-calculated.

To view the Ruckus GRE Tunnel Statistics:

1. Select **Monitor** > **Report** > **Rogue Devices** > **Ruckus AP Tunnel Stats**. The Ruckus GRE tab appears by default.

2. Update the parameters as explained in Table 29.
3. Click:
   - **Load Data**— To view the report in the workspace.
   - **Export CSV**—To open or save the report in CSV file format.

TABLE 29 Ruckus GRE Report Parameters

Field	Description	Your Action
Time Period	Indicate the time period for which you want to view the report.	Move the slider to set the duration.
Data Plane	Indicates the Data Plane.	Select the Data Plane.
AP MAC or IP Address	Indicates the MAC of the Access Point or IP Address.	Enter the AP MAC or IP address.
Zone Name	Specifies the zone for which you want to view the report.	Enter the zone name or select the zone from the list.

Table 30 contains the report based on the statistics for Ruckus GRE. Each entry contains the 15 minutes cumulative data.

TABLE 30 Ruckus GRE report attributes

Attribute	Type	Description
Time	Long	Bin ID, which is stamped at a 15 minute interval. For example, 10:00, 10:15.
TXBytes	Long	Indicates the number of bytes sent.
RXBytes	Long	Indicates the number of bytes received.
TXPkts	Long	Indicates the number of packets sent.
RXPkts	Long	Indicates the number of packets received.
Dropped Packets	Long	Indicates the number of packets dropped.

Viewing Statistics for SoftGRE Tunnels

The web interface displays the table and its corresponding graph chart. The two representations are synchronized and controlled by the search criteria. For performance reasons, the total counters per DP or per AP for each bin may be pre-calculated. The tunneled flows are offloaded by default for 11ax and cypress profiles.

To view the SoftGRE Tunnel statistics:

1. Select **Monitor** > **Report** > **Rogue Devices** > **Ruckus AP Tunnel Stats**. The Ruckus GRE tab appears by default.
2. Select **SoftGRE**. Update the parameters as explained in Table 31.
3. Click:
   - **Load Data**— To view the report in the workspace.
   - **Export CSV**—To open or save the report in CSV file format.

TABLE 31 SoftGRE Report Parameters

Field	Description	Your Action
Time Period	Indicate the time period for which you want to view the report.	Move the slider to set the duration.
Zone Name	Specifies the zone for which you want to view the report.	Select the required zone.
Gateway Address	Specifies the gateway address	Enter the gateway address.

TABLE 31 SoftGRE Report Parameters (continued)

Field	Description	Your Action
AP MAC or IP Address	Indicates the MAC of the Access Point or IP Address.	Enter the AP MAC or IP address.

Table 32 contains the report based on the statistics for SoftGRE. Each entry contains the 15 minutes cumulative data.

TABLE 32 SoftGRE Report Attributes

Attribute	Type	Description
Time	Long	Bin ID, which is stamped at a 15 minute interval. For example, 10:00, 10:15.
TXBytes	Long	Indicates the number of bytes sent.
RXBytes	Long	Indicates the number of bytes received.
TXPkts	Long	Indicates the number of packets sent.
RXPkts	Long	Indicates the number of packets received.
RX Dropped Packets	Long	Indicates the number of packets dropped.
TX Dropped Packets	Long	Indicates the number of packets dropped.
TX Error Packets	Long	Indicates the number of packets with a header error.
RX Error Packets	Long	Indicates the number of packets with a header error.

Viewing Statistics for SoftGRE IPsec Tunnels

The web interface displays the table and its corresponding graph chart. The two representations are synchronized and controlled by the search criteria. For performance reasons, total counters per DP or per AP for each bin may be pre-calculated.

To view the SoftGRE IPsec Tunnel Statistics:

1. elect **Monitor** > **Report** > **Rogue Devices** > **Ruckus AP Tunnel Stats**. The Ruckus GRE tab appears by default.
2. Select **SoftGRE + IPsec**. Update the parameters as explained in Table 33.
3. Click:
   - **Load Data**— To view the report in the workspace.
   - **Export CSV**—To open or save the report in CSV file format.

TABLE 33 SoftGRE + IPsec Report Parameters

Field	Description	Your Action
Time Period	Indicate the time period for which you want to view the report.	Move the slider to set the duration.
Zone Name	Specifies the zone for which you want to view the report.	Select the required zone.
Gateway Address	Specifies the gateway address	Enter the gateway address.
AP MAC or IP Address	Indicates the MAC of the Access Point or IP Address.	Enter the AP MAC or IP address.

Table 34 contains the report based on the statistics for access point IPsec. Each entry contains the 15 minutes cumulative data.

TABLE 34 SoftGRE + IPsecReport Attributes

Attribute	Type	Description
Time	Long	Bin ID, which is stamped at a 15 minute interval. For example, 10:00, 10:15.

TABLE 34 SoftGRE + IPsecReport Attributes (continued)

Attribute	Type	Description
TXBytes	Long	Indicates the number of bytes sent.
RXBytes	Long	Indicates the number of bytes received.
TXPkts	Long	Indicates the number of packets sent.
RXPkts	Long	Indicates the number of packets received.
TX Dropped Packets	Long	Indicates the number of packets dropped.
RX Dropped Packets	Long	Indicates the number of packets dropped.

Core Network Tunnel Stats

Viewing Statistics for L2oGRE Core Network Tunnel

To view Stats for L2oGRE Core Network Tunnel:

1. Select **Monitor** > **Report** > **Rogue Devices** > **Core Network Tunnel Stats**. The L2oGRE page appears.
2. Update the parameters as explained in Table 35.
3. Click:
   - **Load Data**— To view the report in the workspace.
   - **Export CSV**—To open or save the report in CSV file format.

TABLE 35 L2oGRE Core Network Tunnel Parameters

Field	Description	Your Action
Time Period	Indicate the time period for which you want to view the report.	Move the slider to set the duration.
Data Plane	Indicates the Data Plane.	Select the Data Plane.
Gateway IP Address	Indicates the gateway IP Address.	Enter the gateway IP address.
MVNO Name	Indicates teh mobile virtual network operator name.	Choose the MVNO name.

Table 36 contains the report based on the statistics for L2oGRE core network tunnel.

TABLE 36 L2oGRE Core Network Tunnel Attributes

Attribute	Type	Description
Time	Long	Bin ID, which is stamped at a 15 minute interval. For example, 10:00, 10:15.
TX Bytes	Long	Indicates the number of bytes sent.
RX Bytes	Long	Indicates the number of bytes received.
TX Packets	Long	Indicates the number of packets sent.
RX Packets	Long	Indicates the number of packets received.
Dropped Packets	Long	Indicates the number of packets dropped.

Viewing Statistics for GTP Core Network Tunnel

You can view historical traffic statistics and trends of th core GTP tunnels.

GPRS Tunneling Protocol (GTP) transmits user data packets and signaling between controller and GGSN. GTP encapsulates traffic and creates GTP tunnels, which act as virtual data channels for transmission of packet data between the controller and GGSN. A GTP tunnel is established between the controller and GGSN for a data session initiated from UE.

To view Stats for GTP Core Network Tunnel:

1. Select **Monitor** > **Report** > **Rogue Devices** > **Core Network Tunnel Stats**. The SoftGRE page appears.
2. Select **GTP** and update the parameters as explained in Table 37.
3. Click:
   - **Load Data**— To view the report in the workspace.
   - **Export CSV**—To open or save the report in CSV file format.

TABLE 37 GTP Core Network Tunnel Parameters

Field	Description	Your Action
Time Period	Indicate the time period for which you want to view the report.	Move the slider to set the duration.
Zone Name	Indicates the zone.	Select the Zone name.
Gateway Address	Indicates the gateway address.	Enter the gateway address.
AP MAC or IP Address	Indicates the MAC of the Access Point or IP Address.	Enter the AP MAC or the IP address.

Table 38 contains the report based on the statistics for GTP. Each entry contains the 15 minutes cumulative data.

TABLE 38 GTP Report Attributes

Field	Type	Description
Time	Long	Bin ID, which is stamped at a 15 minute interval. For example, 10:00, 10:15.
TX Bytes	Long	Indicates the number of bytes sent.
RX Bytes	Long	Indicates the number of bytes received.
TX Packets	Long	Indicates the number of packets sent.
RX Packets	Long	Indicates the number of packets received.
Tx Dropped Packets	Long	Indicates the number of packets dropped while sending.
Rx Dropped Packets	Long	Indicates the number of packets dropped while receiving.
Bad GTPU	Long	Indicates a tunneling mechanism that provides a service for carrying user data packets dropped.
RX TEID Invalid	Long	Indicates the number of invalid packets received by Tunnel End Point Identifiers.
TX TEID Invalid	Long	Indicates the number of invalid packets sent by Tunnel End Point Identifiers.
Echo RX	Long	Indicates the echo message received.
Last Echo RX Time	Long	Indicates the time when the last echo message was received.

Events and Alarms

Events

Event

Viewing Events

An event is an occurrence or the detection of certain conditions in and around the network. An AP being rebooted, an AP changing its IP address, and a user updating an AP's configuration are all examples of events.

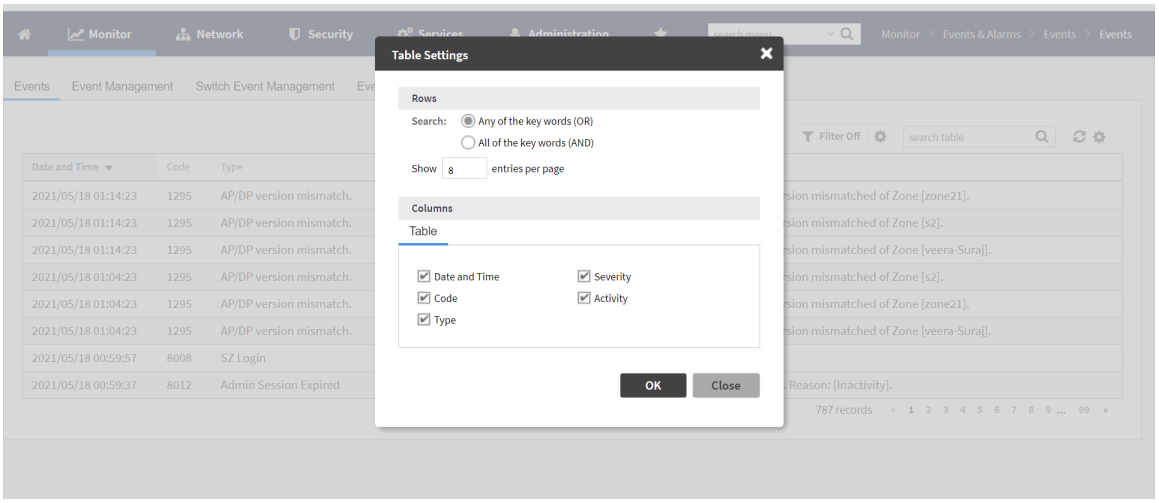
In the main menu, click **Monitor** and hover the mouse on **Events** from the **Events & Alarms** menu. From the **Events** drop-down list select **Events**

This displays **Events** page. The **Events** page displays the below information.

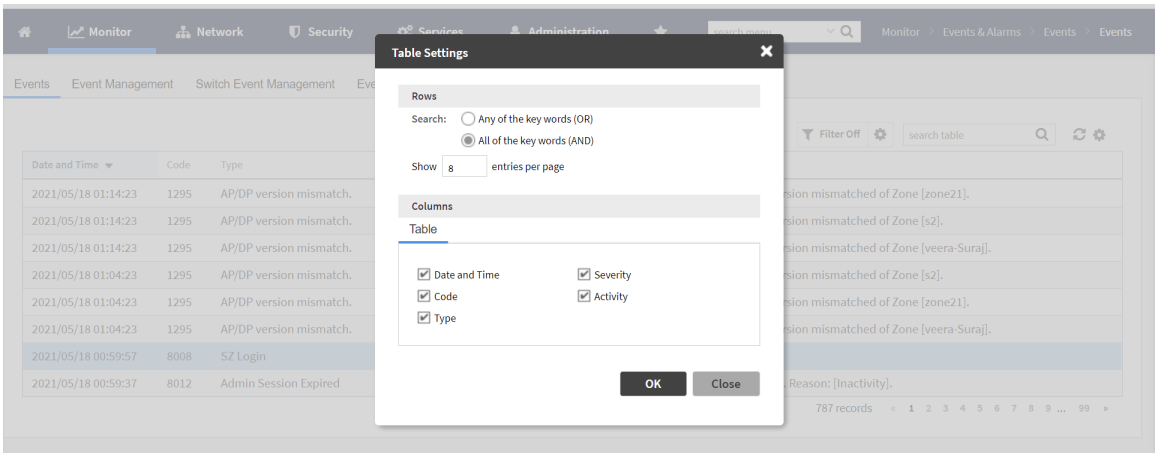
You can also click the  icon to apply filters, to display events based on time and severity.

Events can be searched with "OR" or "AND" options as displayed in the below images.

Search Events with OR Option



Search Events with AND Option



- Date and Time: Displays the date and time when the event occurred
- Code: Displays the event code (see the Alarm and Event Reference Guide for your controller platform more information).
- Type: Displays the type of event that occurred (for example, AP configuration updated).
- Severity: Displays the severity level assigned to the events such as Critical, Debug, Informational, Warning, Major etc.
- Activity: Displays additional details about the event, including (if available) the specific access point, control plane, or data plane that triggered the event.

Switch Event Management

Sending SNMP Traps and Email Notifications for Switch Events

You can configure the controller to send SNMP traps and email notifications by System Domain, Partner Domain, Domain (under System Domain), and Switch Group (level 1 group) for switch events.

You must verify that global SNMP traps are enabled to ensure that the controller can send SNMP traps for alarms:

- System domain:
  - For viewing system domain event notification settings and email notification setting, *SZ* permission and *Read* or higher (*Modify* or *FULL_ACCESS*) access level is required.
  - For editing system domain event notification settings and email notification setting, *SZ* permission and *Modify* or *FULL_ACCESS* access level is required.
- Partner domain and domain (under system domain):
  - For editing event notification settings and email notification setting, *Admin* permission and *Modify* or *FULL_ACCESS* access level permission is required.
  - For editing switch group event notification settings and email notification setting, *ICX Switch* permission and *Modify* or *FULL_ACCESS* access level permission is required.
  - To view switch group event notification settings and email notification setting, *ICX Switch* permission and *Read* access level permission is required.
  - The events grid shows only Switch events that fall under event category "Switch" or "Switch Custom Event".
  - For Highscale deployments, the staging group is not configureable.
  - For Enterprise deployments, only the level-one switch group is configurable.
  - The cache data for event notification is kept for five minutes after which the cache will be cleaned. If the notification is changed within five minutes, the user needs to wait for five minutes for setting the update.

To configure switch event management:

In the main menu, click **Monitor** and hover mouse on **Events** from the **Events & Alarms** menu. In the **Events** drop-down list select **Switch Event Management**.

This displays **Switch Event Management** page. The **Switch Event Management** page displays the below information.

- Email Notification: Select the **Enable** check box, and then type an email address or email addresses in the **Mail To** box. If you want to send notifications to multiple recipients, use a comma to separate the email addresses. Then, click **OK**.
- Events: View the table and select the events for which you want to send traps or email notifications (or both). Select the **Enable** or **Disable** options from the drop-down menu, and configure the following:

  System Domain: Displays global setting for Switch event.

  - Enable SNMP Notification: Select to enable SNMP trap notifications for all selected events.
  - Enable Email: Select to enable email notifications for all selected events.
  - Enable DB Persistence: Select to enable saving of all selected events to the controller database. If an event is already currently enabled, it will stay enabled after you click this link.

  Partner Domain: Displays notification setting for the partner domain.

  - Enable Override: Select the option to enable override settings as follows:
    - Partner domain or domain under system domain setting overrides the system domain setting.
    - Switch group setting overrides the partner domain, the domain under system domain, and the system domain setting.
  - Enable Email: Select to enable email notifications for all the selected events.

NOTE
To select or clear all events, click **More** and select **Select All** or **Deselect All** respectively.

There are twenty seven events. Following information related to the event are displayed:

- Code: displays the event code.
- Severity: displays the severity of the event such as Information, Minor and so on.
- Category: displays the category under which the event falls under, such as AP communication.
- Type: displays the event type such as AP managed, AP rejected and so on.
- Override (Partner domain, domain under system domain and level-one switch group): display the override system domain settings.
- SNMP Notification (Specific to system domain): displays SNMP trap notifications for all selected events.
- Email (System domain, partner domain, domain under system domain and level-one switch group): displays email notifications for all selected events.
- DB persistance (Specific to system domain): displays DB persistance for all selected events.
- OID (Specific to system domain): Displays OID for events.
- Description: displays a short note on the events.

Event Management

Sending SNMP Traps and Email Notifications for Events

By default, the controller saves a record of all events that occur to its database. You can configure the controller to also send SNMP traps and email notifications for specific events whenever they occur.

Verify that global SNMP traps are enabled to ensure that the controller can send SNMP traps for alarms.

You can also manage notifications of the event for each zone by clicking the zones displayed in the tree structure. Event configuration for each zone is independent including:

- Enabling or disabling E-mail notification settings
- Recipient E-mail address
- Enabling or disabling DB persistence settings
- Enabling or disabling SNMP trap settings

You can also manually trigger SNMP traps without generating events using CLI. You can use the **#trigger-trap <event code>** command to trigger traps for respective events with their default attributes.

You can acquire the status of a specific client MAC address by using the query RUCKUS-CTRL-MIB. For more information, see the *SmartZone SNMP MIB Reference Guide*.

In the main menu, click **Monitor** and hover mouse on **Events** from the **Events & Alarms** menu. In the **Events** drop-down list select **Event Management**.

This displays **Event Management** page. The **Events** page displays the below information.

- Email Notification: Select the **Enable** check box, and then type an email address or email addresses in the **Mail To** box. If you want to send notifications to multiple recipients, use a comma to separate the email addresses. Then, click **OK**.
- Events: View the table and select the events for which you want to send traps or email notifications (or both). Select the **Enable** or **Disable** options from the drop-down menu, and configure the following:
  - Enable SNMP Notification: Click this link to enable SNMP trap notifications for all selected events.
  - Enable Email: Click this link to enable email notifications for all selected events.

- Enable DB Persistence: Click this link to enable saving of all selected events to the controller database. If an event is already currently enabled, it will stay enabled after you click this link.

Following information related to the event are displayed:

- Code: displays the event code.
- Severity: displays the severity of the event such as Information, Minor and so on.
- Category: displays the category under which the event falls under, such as AP communication.
- Type: displays the event type such as AP managed, Ap rejected and so on.
- Zone Override: display the override status of the zone.

Event Threshold

Configuring Event Threshold

An event threshold defines a set of conditions related to the controller hardware that need to be met before the controller triggers an event. You can accept the default threshold values or you can update the threshold values to make them more suitable to your deployment or controller environment.

1. In the main menu, click **Monitor** and hover mouse on **Events** from the **Events & Alarms** menu. In the **Events** drop-down list select **Event Threshold**.

   This page displays the list of events with configurable thresholds including the event code, severity level, default value and accepted range, and unit of measurement for each event.
2. Identify the event threshold that you want to configure.
3. Click the event name under the **Name** column.

   The threshold value for the event becomes editable. Next to the threshold value, the acceptable range is displayed.
4. Edit the threshold value.

   For **Client Count**, you can also edit the **Trigger Criterion** value between the range 1000-999999. When the client count exceeds 1000 users and when the client count drop percentage is more than 50% within an hour, the **Threshold Value** range of 50%-95% is breeched. This generates event 956 and alarm 956 which are displayed in the **Events** and **Alarms** dashboard.
5. Click **OK**.

Switch Custom Events

Creating Custom Events for ICX Switches

You can create custom events by specifying that a particular switch status, for example a particular CPU utilization, memory utilization, or text pattern, generates an alarm or an event. Therefore, there are 3 types of custom events - CPU, Memory and TextPattern.

Because the polling interval between the switch and the controller is 5 minutes, the switch status cannot be obtained in real time. However, you can monitor memory and CPU utilization by creating an event or alarm that is triggered when a particular threshold is reached. You can also create a custom event to monitor for switch events based on text patterns.

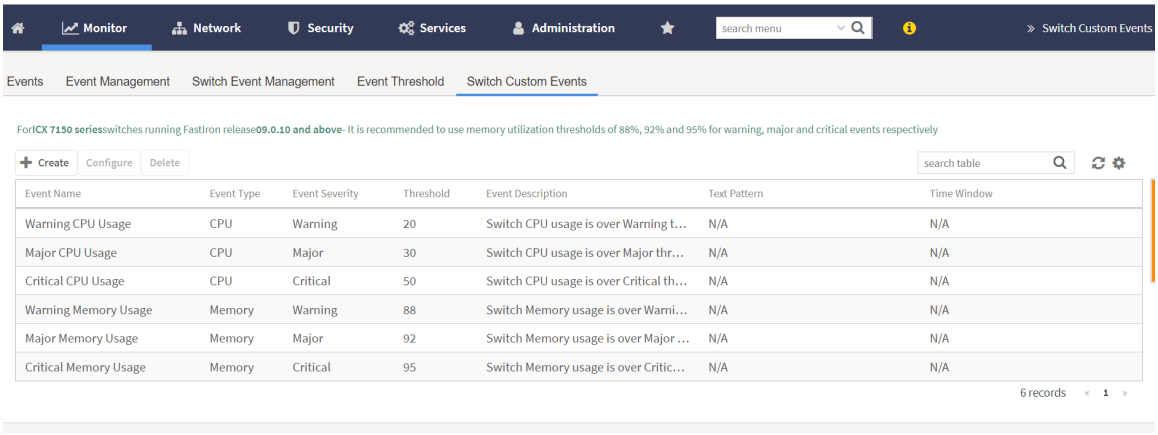
To create a customer event, perform the following steps.

NOTE
DB Persistence must be enabled to generate custom events.

1. In the main menu, click **Monitor** and hover mouse on **Events** from the **Events & Alarms** menu. In the **Events** drop-down list select **Switch Custom Events**.

   This displays **Switch Custom Events** page.

FIGURE 51 Types of custom events available

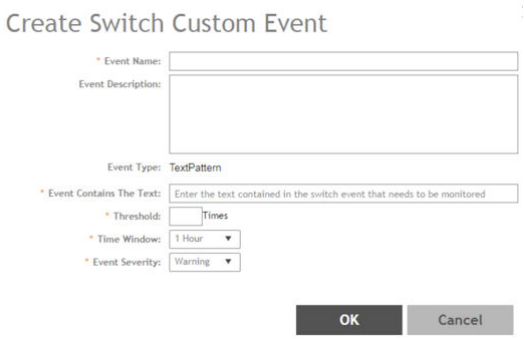


2. Click **Create**.

The **Create Switch Custom Events** page is displayed as shown in the following example.

NOTE
You can only create new TextPattern custom events. Custom events of CPU or Memory type can only be edited or configured, and cannot be created.

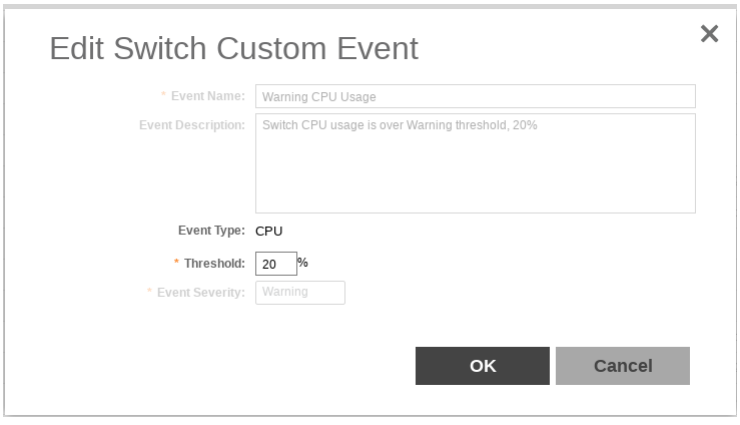
FIGURE 52 Creating custom events for switches - TextPattern type



Configure the following:

- Event Name: Enter the name of the event. For example, you can provide a name to identify the text pattern to be displayed in the event description.
- Event Description: Enter a detailed description of the event.
- Event Type: Displays the type of event. Here, Text Pattern.
- Event Contains The Text: Enter the text used in the event to be monitored.
- Threshold: Enter the number of times the user-defined status is achieved.
- Time Window: Select the time frame within which the threshold is achieved. You can select from a few hours to two days.
- Event Severity: Select the severity level of the custom event. Options include Warning, MAJOR, Critical.

FIGURE 53 Editing custom events for switches - CPU/Memory type



Configure the following:

- Event Name: Displays the name of the event.

- Event Description: Displays a detailed description of the event.
- Event Type: Displays te type of event. Here, CPU.
- Threshold: Enter the percentage of times the user-defined status is achieved.
- Event Severity: Displays the severity level of the custom event. Options include Warning, Major, and Critical.

3. Click **OK**.

Alarms

Configuring Alarms

Alarms are a type of event that typically warrants your attention. Alarms are generated by managed access points and the controller system (control plane and data plane).

In the main menu, click **Monitor** and hover mouse on Events from the **Events & Alarms** menu. Click **Alarms**. This displays the **Alarms** page with the following information

- Date and Time: Displays the date and time when the alarm was triggered.
- Code: Displays the alarm code (see the Alarm and Reference Guide for your controller platform for more information).
- Alarm Type: Displays the type of alarm event that occurred (for example, AP reset to factory settings).
- Severity: Displays the severity level assigned to the events such as Critical, Major, Minor and Warning.
- Status: Indicates whether the alarm has already been cleared or still outstanding.
- Activity: Displays additional details about the alarm, including (if available) the specific access point, control plane, or data plane that triggered the alarm.
- Acknowledged On: Displays the date and time when the administrator acknowledge the alarm.
- Cleared By: Displays information about who cleared the alarm.
- Cleared On: Displays the date and time when the alarm was cleared.
- Comments: Displays administrator notes recorded during alarm management.

NOTE

Click  to export the alarms details to a CSV file. Check the default download folder of your web browser and look for a file named *alarms.csv* and view it using a spreadsheet application (for example, Microsoft Excel®).

Clearing Alarms

Clearing an alarm removes the alarm from the list but keeps it on the controller's database.

To clear an alarm:

1. Select the alarm form the list and click **Clear Alarm**. The **Clear Alarm** page appears.
2. Type your comments and select **Apply**.

Acknowledging Alarms

Acknowledging an alarm lets other administrators know that you have examined the alarm. After you acknowledge an alarm, it will remain on the list of alarms and will show the date and time that you acknowledged it.

To acknowledge an alarm:

1. Select the alarm from the list and click **Acknowledge Alarm**.

   This message appears:

   ```
   Are you sure you want to acknowledge the selected alarms?
   ```

   .
2. Select **Yes**.

Applying Filters

You can view a list of alarms by date, time, severity and status.

1. Click the  icon.

   The **Apply Filters** page appears. Configure the following:

   a. Severity: Select the severity level by which you want to filter the list of alarms.

   b. Status: Select the status by which you want to filter the list of alarms.

   c. Date and Time: Select the alarms by their start and end dates.
2. Click **OK**.

   All the alarms that meet the filter criteria are displayed on the **Alarms** page and the display changes to **Filter On**.

   You can export the alarms into a CSV file by clicking the  icon.

Network

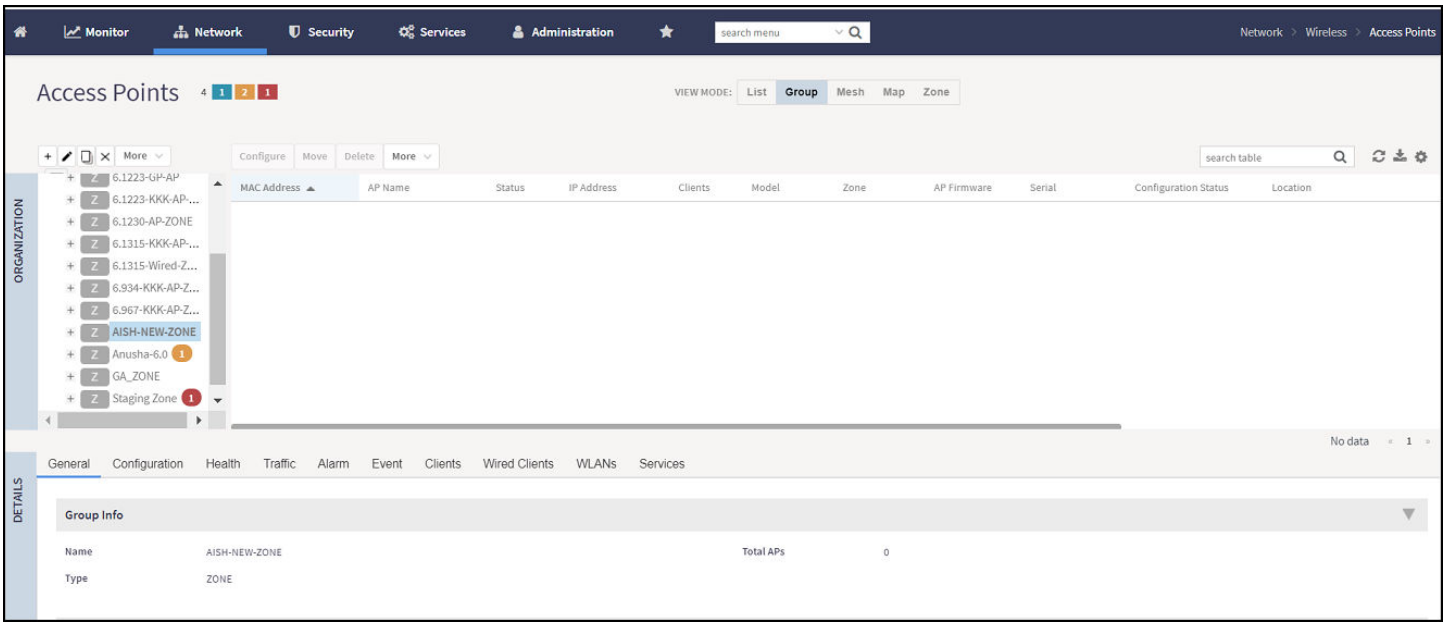
- Working with Wireless Network.....103
- Working with Switches.....235
- Working with Data and Control Plane.....346

Working with Wireless Network

Working With Access Points

The following image gives you an understanding of the Acces Point home page.

FIGURE 54 Working with Access Points



Understanding WLAN Services

Hierarchy Overview

The hierarchy helps in specifying which AP groups or APs provide which WLAN services.

You can virtually split them using the following hierarchy:

- System—Highest order that comprises of multiple zones
- Domains—Broad classification that comprises of multiple Zones.
- Zones—Comprises of multiple AP groups
- AP groups—Comprises of multiple APs

- APs—Individual access points.

Creating an AP Domain

To create an AP domain:

1. From the System tree hierarchy, select the location where you want to create the domain.
2. Click the **Create** button, the Create Group form appears.
3. Configure the following details:
   a. Enter a **Name** for the domain.
   b. Enter a **Description** about the domain.
   c. By default, the **Type** selected is **Domain**.
   d. The **Parent Group** displays the group to which this domain will be tagged.
   e. If you want to create a domain to manage MSP-related settings within that domain, in the **Managed by Partner** field, select the **Enable** check box.
4. Click **OK**.

NOTE

You can also edit, clone and delete an AP Domain by selecting the options Configure, Clone or Delete respectively, from the Access Points page.

Working with AP Zones

An AP zone functions as a way of grouping RUCKUS APs and applying a particular set of settings (including WLANs and their settings) to thise group of RUCKUS APs. Each AP zone can include up to 2048 WLAN services.

By default, an AP zone named Staging Zone exists in the SZ300/vSZH platforms and Default Zone in the SZ100/vSZE plaftorms. Any AP that registers with the controller that is not assigned a specific zone is automatically assigned to the Staging or Default Zone. This section describes how to use AP zones to manage devices.

NOTE
When an AP is assigned or moved to the Staging or Default Zone, the cluster name becomes its user name and password after the AP shows up-to-date state. If you need to log on to the AP, use the cluster name for the user name and password.

Before creating an AP zone, RUCKUS recommends that you first set the default system time zone on the General Settings page. This will help ensure that each new AP zone will use the correct country. For information on how to set the default system time zone, see Configuring System Time on page 545.

Working with AP Groups

AP (access point) groups can be used to define configuration options and apply them to groups of APs at once, without having to individually modify each AP's settings.

For each group, administrators can create a configuration profile that defines the channels, radio settings, Ethernet ports and other configurable fields for all members of the group or for all APs of a specific model in the group. AP groups are similar to WLAN groups (see Working with WLAN Groups for more information). While WLAN groups can be used to specify which WLAN services are served by which APs, AP groups are used for more specific fine-tuning of how the APs themselves behave.

NOTE
AP group configuration settings can be overridden by individual AP settings. For example, if you want to set the transmit power to a lower setting for only a few specific APs, leave the Tx Power Adjustment at **Auto** in the AP group configuration page, then go to the individual AP configuration page (**Access Points** > **Access Points** > **Edit [AP MAC address]**) and set the **Tx Power Adjustment** to a lower setting.

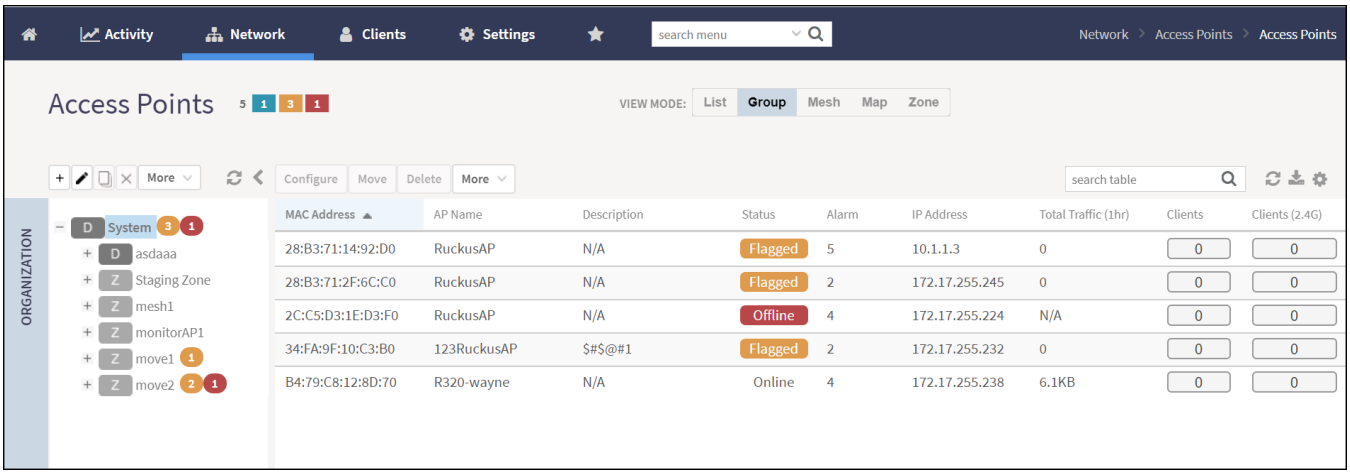
Creating an AP Zone

An AP zone functions as a way of grouping RUCKUS Wireless APs and applying settings including WLANs to these groups of RUCKUS Wireless APs. Each AP zone can include up to six WLAN services.

To create an AP zone, complete the following steps.

1. On the menu, click **Network** > **Wireless** > **Access Point**.

FIGURE 55 Access Points Page



2. From the **System** tree hierarchy, select the location where you want to create the zone (for example, System or Domain), and click .

FIGURE 56 Create Domain Page



3. Configure the zone by completing the settings listed in the following table:

TABLE 39 AP Zone Details

Field	Description	Your Action
Name	Indicates the name of the zone or an AP group.	Enter a name.
Description	Indicates the short description assigned to the zone or AP group.	Enter a brief description
Type	Indicates if you are creating a domain, zone, or an AP group.	Appears by default. You can also choose the option.
Parent Group	Indicates the parent AP group.	Appears by default.
Link Switch Group	Allows to create a link between the switch group and an AP.	You can enable or disable the option. When the link state is enabled, you can modify the name and description of the switch group, the AP zone will change accordingly. When the link is disabled, the AP zone and switch group no longer share same name and description, but the link between them still exists. To delete the link, modify the name of AP zone or switch group. After successful deletion of the link, the **Link AP Zone** option is unavailable.
Configuration > General Options		
AP Firmware	Indicates the firmware to which it applies.	Select the firmware.
Country Code	Indicates the country code. Using the correct country code helps ensure that APs use only authorized radio channels.	Select the country code.
Location	Indicates the generic location of the zone.	Enter the location.
Location Additional Information	Indicates detailed location.	Enter additional location information.
GPS Coordinates	Indicates the geographical location.	Enter the following coordinates: • **Longitude** • **Latitude** • **Altitude**
AP Admin Logon	Indicates the administrator logon credentials.	Enter the **Logon ID** and **Password**.
AP Time Zone	Indicates the time zone that applies.	Select a time zone, and enter the details as required.
AP IP Mode	Indicates the IP version that applies.	Select the IP version. IPv6, IPv4, and dual addressing modes are supported.
Historical Connection Failures	Allows the zone APs to report client connection failures so that the administrator can view past connection problems from the Troubleshooting menu. **NOTE** For enterprise profile (vSZ-E) is 5 days, for carrier profile (vSZ-H) is 3 days.	Click the button.
DP Group	Specifies the group for the zone. **NOTE** This option is supported only on vSZ-H.	Select the DP group from the list.
SSH Tunnel Encryption	Specifies the encryption that reduces the load on controller control of SSH traffic.	Select the required option: • **AES 128** • **AES 256**

TABLE 39 AP Zone Details (continued)

Field	Description	Your Action
Cluster Redundancy	Provides cluster redundancy option for the zone. **NOTE** Cluster redundancy is supported only on SZ300 and vSZ-H.	Select the required option: • **Zone Enable** • **Zone Disable**
Configuration > Mesh Options		
Enable mesh networking in this zone	Enables managed APs to automatically form a wireless mesh network, in which participant nodes (APs) cooperate to route packets. Dual-band APs can only mesh with other dual-band APs, while single-band APs can only mesh with other single-band APs.	Click the button.
Zero Touch Mesh	Enables a new AP to join the network using wireless connection.	Click the button.
Mesh Name (ESSID)	Indicates the mesh name.	Enter a name for the mesh network. Alternatively, do nothing to accept the default mesh name that the controller has generated.
Mesh Passphrase	Indicates the passphrase used by the controller to secure the traffic between Mesh APs.	Enter a passphrase that contains at least 12 characters. Alternatively, click **Generate** to generate a random passphrase with 32 characters or more.
Mesh Radio Option	Indicates the channel range configured.	Select the channel option: 2.4 GHz or 5 GHz.
Configuration > Radio Options		
Dual-5G Mode	Enables third radio operator in 2.4 GHz, Lower 5 GHz, and Upper 5 GHz. By default, the **Dual-5G Mode** is enabled. In the enabled mode, radio-0 will be on 2.4GHz band, radio-1 will be on 5G Lower band and radio-2 will be on 5G Upper band. • 5G Lower BAND : UNII-1, UNII-2A • 5G Upper BAND : UNII-2C, UNII-3 In the disabled mode, the radio-0 will be on 2.4GHz band, radio-1 will be on 5G band and radio-2 will be on 6G band. This also depends on the country code.	Select or keep the default **Dual-5G Mode** option.
Configuration > Band/Spectrum Configuration > 2.4 GHz		
Channelization	Indicates the channel width.	Set the channel width used during transmission to either 20 or 40 (MHz), or select Auto to set it automatically.
Channel	Indicates the channel to use.	Select one of the options: Auto, 1, 6 or 11.
Auto Cell Sizing	Enables the AP to share information on interference seen by each other and dynamically adjust their radio Tx power and Rx parameters to minimize interference. Enabling this option disables the TX Power Adjustment configuration. **NOTE** Ensure that Background Scan is enabled.	Select the option.

TABLE 39 AP Zone Details (continued)

Field	Description	Your Action
TX Power Adjustment	Allows to manually configure the transmit power on the 2.4 GHz radio. By default, the TX power is set to Full on the 2.4 GHz radio. **NOTE** If you choose Min, the transmit power is set to 0dBm (1mW) per chain for 11n APs, and 2dBm per chain for 11ac APs. If you choose Max, the transmit power is set to the maximum allowable value according to the AP's capability and the operating country's regulations.	Select the preferred TX power.
Protection Mode	Indicates the mechanism to reduce frame collision.	Choose one of the following options: • None • RTS/CTS • CTS Only
Background Scan	Allows the AP radio to scan other channels in the band for accessing channel health and capacity, detecting rogue devices, optimizing and mainting mesh links and to discover AP neighbors.	Enter the duration in seconds. Range: 1 through 65535.
Auto Channel Selection	Automatically adjusts the channel using the ChannelFly option.	Select the required option. For **ChannelFly**, set the **Channel Change Frequency** and **Full Optimization Period**.
Configuration > **Band/Spectrum Configuration** > **5 GHz**		
Channelization	Indicates the channel width.	Set the channel width used during transmission: Auto, 20, 40, 80 and 160.
Channel	Indicates the channel to use.	Select the required options for the Indoor and Outdoor APs.
Secondary Channel	Indicates the secondary channel to used.	By default, the Indoor and Outdoor option is set to Auto.
Allow DFS Channels	Allows ZoneFlex APs to use DFS channels.	Click to enable the option.
Allow Channel 144	Provides channel 140 and 144 support for 11ac and 11ax APs. Enabling this option supports 20 MHz, 40 MHz, or 80 MHz channel modes. The 160 MHz mode is supported if the AP supports this mode. Disabling this option provides Channel 140 support only to 20 MHz mode. **NOTE** This option is available for selection only if you enable the **DFS Channels** option. **NOTE** This feature is currently supported only in the United States.	Click to enable the option.
Allow Indoor Channels	Allows outdoor APs to use channels regulated as for indoor use only.	Click to enable the option.

TABLE 39 AP Zone Details (continued)

Field	Description	Your Action
Auto Cell Sizing	Enables the AP to share information on interference seen by each other and dynamically adjust their radio Tx power and Rx parameters to minimize interference. Enabling this option disables the TX Power Adjustment configuration. **NOTE** Ensure that Background Scan is enabled.	Select the option.
TX Power Adjustment	Allows to manually configure the transmit power on the 5 GHz radio. By default, the TX power is set to Full on the 5 GHz radio. **NOTE** If you choose Min, the transmit power is set to 0dBm (1mW) per chain for 11n APs, and 2dBm per chain for 11ac APs. If you choose Max, the transmit power is set to the maximum allowable value according to the AP's capability and the operating country's regulations.	Select the preferred TX power.
Background Scan	Allows the AP radio to scan other channels in the band for accessing channel health and capacity, detecting rogue devices, optimizing and mainting mesh links and to discover AP neighbors.	Enter the duration in seconds. Range: 1 through 65535.
Auto Channel Selection	Automatically adjusts the channel using the ChannelFly option.	Select the required option. For **ChannelFly**, set the **Channel Change Frequency** and **Full Optimization Period**.
Configuration > **Band/Spectrum Configuration** > **6 GHz** **NOTE** This tab is available only if the **Tri-band Dual-5G Mode** option is not enabled.		
Channelization	Indicates the channel width.	Set the channel width used during transmission: Auto, 20, 40, 80 and 160.
Channel	Indicates the channel to use.	Select the required options for the Indoor and Outdoor APs.
Auto Cell Sizing	Enables the AP to share information on interference seen by each other and dynamically adjust their radio Tx power and Rx parameters to minimize interference. Enabling this option disables the TX Power Adjustment configuration. **NOTE** Ensure that Background Scan is enabled.	Select the option.

TABLE 39 AP Zone Details (continued)

Field	Description	Your Action
TX Power Adjustment	Allows to manually configure the transmit power on the 6 GHz radio. By default, the TX power is set to Full on the 6 GHz radio. **NOTE** If you choose Min, the transmit power is set to 0dBm (1mW) per chain for 11n APs, and 2dBm per chain for 11ac APs. If you choose Max, the transmit power is set to the maximum allowable value according to the AP's capability and the operating country's regulations.	Select the preferred TX power.
LPI (Low Power Indoor) mode:	Allows the use of a 4 U-NII bands U-NII-5 to U-NII-8 indoors at a reduced Tx power level.	Enable the option.
Background Scan	Allows the AP radio to scan other channels in the band for accessing channel health and capacity, detecting rogue devices, optimizing and mainting mesh links and to discover AP neighbors.	Enter the duration in seconds. Range: 1 through 65535.
Auto Channel Selection	Automatically adjusts the channel using the ChannelFly option.	For **ChannelFly**, set the **Channel Change Frequency** and **Full Optimization Period**.
Configuration > **Band/Spectrum Configuration** > **Lower 5 GHz**		
Channelization	Indicates the channel width.	Set the channel width used during transmission: Auto, 20, 40, 80 and 160.
Channel	Indicates the channel to use.	Select the required options for the Indoor and Outdoor APs.
Allow DFS Channels	Allows ZoneFlex APs to use DFS channels.	Click to enable the option.
Allow Indoor Channels	Allows outdoor APs to use channels regulated as for indoor use only.	Click to enable the option.
Auto Cell Sizing	Enables the AP to share information on interference seen by each other and dynamically adjust their radio Tx power and Rx parameters to minimize interference. Enabling this option disables the TX Power Adjustment configuration. **NOTE** Ensure that Background Scan is enabled.	Select the option.
TX Power Adjustment	Allows to manually configure the transmit power on the Lower 5 GHz radio. By default, the TX power is set to Full on the Lower 5 GHz radio. **NOTE** If you choose Min, the transmit power is set to 0dBm (1mW) per chain for 11n APs, and 2dBm per chain for 11ac APs. If you choose Max, the transmit power is set to the maximum allowable value according to the AP's capability and the operating country's regulations.	Select the preferred TX power.

TABLE 39 AP Zone Details (continued)

Field	Description	Your Action
Background Scan	Allows the AP radio to scan other channels in the band for accessing channel health and capacity, detecting rogue devices, optimizing and mainting mesh links and to discover AP neighbors.	Enter the duration in seconds. Range: 1 through 65535.
Auto Channel Selection	Automatically adjusts the channel using the ChannelFly option.	Select the required option. For **ChannelFly**, set the **Channel Change Frequency** and **Full Optimization Period**.
Configuration > **Band/Spectrum Configuration** > **Upper 5 GHz**		
Channelization	Indicates the channel width.	Set the channel width used during transmission: Auto, 20, 40, 80 and 160.
Channel	Indicates the channel to use.	Select the required options for the Indoor and Outdoor APs.
Allow DFS Channels	Allows ZoneFlex APs to use DFS channels.	Click to enable the option.
Allow Channel 144	Provides channel 140 and 144 support for 11ac and 11ax APs. Enabling this option supports 20 MHz, 40 MHz, or 80 MHz channel modes. The 160 MHz mode is supported if the AP supports this mode. Disabling this option provides Channel 140 support only to 20 MHz mode. **NOTE** This option is available for selection only if you enable the **DFS Channels** option. **NOTE** This feature is currently supported only in the United States.	Click to enable the option.
Auto Cell Sizing	Enables the AP to share information on interference seen by each other and dynamically adjust their radio Tx power and Rx parameters to minimize interference. Enabling this option disables the TX Power Adjustment configuration. **NOTE** Ensure that Background Scan is enabled.	Select the option.
TX Power Adjustment	Allows to manually configure the transmit power on the Upper 5 GHz radio. By default, the TX power is set to Full on the Upper 5 GHz radio. **NOTE** If you choose Min, the transmit power is set to 0dBm (1mW) per chain for 11n APs, and 2dBm per chain for 11ac APs. If you choose Max, the transmit power is set to the maximum allowable value according to the AP's capability and the operating country's regulations.	Select the preferred TX power.
Background Scan	Allows the AP radio to scan other channels in the band for accessing channel health and capacity, detecting rogue devices, optimizing and mainting mesh links and to discover AP neighbors.	Enter the duration in seconds. Range: 1 through 65535.

TABLE 39 AP Zone Details (continued)

Field	Description	Your Action
Auto Channel Selection	Automatically adjusts the channel using the ChannelFly option.	Select the required option. For **ChannelFly**, set the **Channel Change Frequency** and **Full Optimization Period**.
Configuration > **AP GRE Tunnel Options**		
Ruckus GRE Profile	Indicates the GRE tunnel profile.	Choose the GRE tunnel profile from the list.
Ruckus GRE Forwarding Broadcast	Forwards the broadcast traffic from network to tunnel.	Click the option to enable forwarding broadcast.
Soft GRE Profiles	Indicates the SoftGRE profiles that you want to apply to the zone.	a. Click the **Select** check box, a form is displayed. b. From the **Available Profiles**, select the profile and click the -> icon to choose it. You can also click the + icon to create a new SoftGRE profile. c. Click **OK**.
IPsec Tunnel Mode	Indicated the tunnel mode for the Ruckus GRE and SoftGRE profile.	Select an option: • Disable • SoftGRE • Ruckus GRE
IPsec Tunnel Profile	Indicates the tunnel profile for SoftGRE. **NOTE** Select the same tunnel type for IPsec tunnel profile in WLAN configuration.	Choose the option from the drop-down.
Configuration > **Syslog Options**		
Enable external syslog server for APs	Enables the controller to send syslog data to the syslog server on the network.	Select the option.

TABLE 39 AP Zone Details (continued)

Field	Description	Your Action
Config Type	Allows to customize or select an external syslog server profile.	Select the option: • Custom: Configure the details for the AP to send syslog messages to syslog server. **NOTE** The IP address format that you enter here will depend on the AP IP mode that you selected earlier in this procedure. If you selected IPv4 Only, enter an IPv4 address. If you selected IPv6 Only, enter an IPv6 address. – **Primary Server Address**: If the primary server goes to send syslog messages. › **Port**: enter the syslog port number on the respective servers. › **Portocol**: select between UDP and TCP protocols. – **Secondary Server Address**: If the primary server goes down, the AP sends syslog messages to the secondary server as backup. › **Port**: Enter the syslog port number on the respective servers. › **Portocol**: Select between UDP and TCP protocols. – **Event Facility**: Select the facility level that will be used by the syslog message. Options include: Keep Original, Local0 (default), Local1, Local2, Local3, Local4, Local5, Local6, and Local7. – **Priority**: Select the lowest priority level for which events will be sent to the syslog server. For example, to only receive syslog messages for events with the warning (and higher) priority, select **Warning**. To receive syslog messages for all events, select **All**. – **Send Logs**: Select the type of messages to be sent to the syslog server. For example, General Logs, Client Logs or All Logs. • AP External Syslog Profile: Select the profile from the drop-down or click Add to create a new profile. Refer to Creating an External Syslog Server Profile on page 532 for more information.
Configuration > AP SNMP Options		
Enable AP SNMP	Indicates if the AP SNMP option is enabled.	Select the check box.
Config Type	Enables custom or AP SNMP Profile Agent.	Select the check box. • Custom: Select this option to create customized SNMPv2 and SNMPv3 profile agents. • AP SNMP Profile Agent: Select this option to create AP SNMPv2 and SNMPv3 profile agents directly.

TABLE 39 AP Zone Details (continued)

Field	Description	Your Action
SNMPv2 Agent	Indicates if the SNMPv2 agent is enabled.	If the SNMPv2 agent is enabled, configure the community settings. a. Click **Create** and enter **Community**. b. Select the required **Privilege**. If you select **Notification**, enter the **Target IP**. c. Click **OK**.
SNMPv3 Agent	Indicates the SNMPv3 Agent is applied.	If the SNMPv3 agent is enabled, configure the community settings. a. Click **Create** and enter **User**. b. Select the required **Authentication**. c. Enter the **Auth Pass Phrase**. d. Select the **Privacy** option. e. Select the required **Privilege**. If you select **Notification**, select the option **Trap** or **Inform** and enter the **Target IP** and **Target Port**. f. Click **OK**.
Configuration > **Cellular Options**		
LTE Band Lock	Displays the list of LTE bands (4G/3G) and allows you to lock one or more bands from the list. Once a lock is enabled, the connection is established only to the specified bands. **NOTE** The list of bands is only applicable to: • **Domain** • **USA** • **Canada** • **Japan**	Select the check box and choose the band from: • **Primary Sim** • **Secondary Sim**
Configuration > **Advanced Options**		
Restricted AP Access Profile **NOTE** This feature is available from 5.2 release and onwards.	Restricted AP Access blocks access to the AP's standard well know open ports to protect the APs and enhance their security.	Select the Restricted AP Access profile from the drop-down. You can also create a new profile by clicking **+** icon. **NOTE** By default this feature is disabled. **NOTE** You can add maximum five Restricted AP Access profiles for a zone.
Channel Mode	Indicates if location-based service is enabled. If you want to allow indoor APs that belong to this zone to use wireless channels that are Channel Mode regulated as indoor-use only.	Select the **Allow indoor channels** check box.
Smart Monitor	Indicates AP interval check and retry threshold settings.	Select the check box and enter the interval and threshold.
AP Ping Latency Interval	Measures the latency between the controller and AP periodically, and sends this data to SCI.	Enable by moving the button to ON to measure latency.

TABLE 39 AP Zone Details (continued)

Field	Description	Your Action
AP Management VLAN	Indicates the AP management VLAN settings.	Choose the option. Click **VLAN ID**, and then type the VLAN ID that you want to assign (valid range is from 1 to 4094). To keep the same management VLAN ID that has been configured on the AP, click Keep AP's settings. **ATTENTION** For standalone APs, set the AP Ethernet port to trunk before changing the AP Management VLAN settings.
Rogue AP Detection	Indicates rogue AP settings. **NOTE** Rogue detection AP in active-active mode cluster redundancy environment is restricted from storing its own BSSIDs to avoid considering its own APs as rogues attacking.	Enable the option.
Rogue Classification Policy	Indicates the parameters used to classify rogue APs. This option is available only if you enable the **Rogue AP Detection** option.	Select the options for rogue classification policy: • – **Enable events and alarms for all rogue devices** – **Enable events and alarms for malicious rogues only** • **Report RSSI Threshold**: Enter the threshold. Range: **0** through **100**. • **Protect the network from malicious rogue access points**: Enable the option and choose one of the following: – **Aggressive** – **Auto** – **Conservative** • **Radio Jamming Detection**: Enable the option and enter the **Jamming Threshold** in percentage.
DoS Protection	Indicates settings for blocking a client.	Select the check box and enter the duration in seconds.
Load Balancing	Balances the number of clients or the available capacity across APs.	Select the required option: • Based on Client Count • Based on Capacity • Disabled
Band Balancing	Balances the client distribution across frequency bands.	Enter the 2.4G client percentage to control the 2.4G clients limit and to enforce band balance.

TABLE 39 AP Zone Details (continued)

Field	Description	Your Action
Steering Mode	Controls the APs' steering behavior for load balancing and band balancing.	Select the option and use the slider to actively control associated stations to meet the distribution requirements allowing band balancing and load balancing: • Basic (default): During heavy load conditions, this option withholds probe and authentication responses in order to achieve load balance. • Proactive: This is a dynamic form of band balancing where some selected associated clients are rebalanced on the AP or across APs utilizing the 802.11v BTM. The AP sends a BTM message to the client to roam and it is left to the client's discretion to make its roaming decision. • Strict: This is an aggressive form of balancing where some selected associated clients are forced to rebalance utilizing the 802.11v BTM. The AP sends a BTM message to the client to roam. If the client does not roam, the client is forced to disconnect after 10 seconds. Additionally, some selected non-802.11v clients are forcefully disconnected directly to force them to roam. **NOTE** The band change is applicable only for those connected clients that support the 802.11v standard. Enter the percentage of client load on the 2.4 GHz band.
Location Based Service	Indicates that the location-based service is enabled.	• Select the check box and choose the options. • Click **Create**, In the Create LBS Server form: a. Enter the **Venue Name**. b. Enter the **Server Address**. c. Enter the **Port number**. d. Enter the **Password**.
Client Admission Control	Indicates the load thresholds on the AP at which it will stop accepting new clients.	Select the check box and update the following settings: • **Min Client Count** • **Max Radio Load** • **Min Client Throughput**
AP Reboot Timeout	Indicates the AP reboot settings.	Choose the required option: • **Reboot AP if it cannot reach default gateway after** • **Reboot AP if it cannot reach the controller after**
Recovery SSID	Allows you to enable or disable the Recovery (Island) SSID broadcast on the controller.	Enable **Recovery SSID Broadcast**.
My.Ruckus support for Tunnel-WLAN/ VLAN	By default, support for LBO, tunneled-WLAN, and non-default management VLAN is disabled because it adds an ACL which affects the LBO and tunneled-WLAN performance. Enabling this support may have a 10 percent impact on the Wi-Fi performance.	Enable the option for support.

4. Click **OK**.

For SZ300 and vSZ-H, you can also migrate the Zone configuration from a regular Domain to a Partner Domain. For more information, see https://support.ruckuswireless.com/answers/000006414

NOTE

You can also edit, clone or delete an AP Zone by selecting the options Configure , Clone or Delete respectively, from the Access Points page.

Auto Cell Sizing

NOTE

Before enabling auto cell sizing, you must enable **Background Scan**.

When Wi-Fi is deployed in a high-density environment, despite the use of auto-channel selection, multiple APs operating on the same channel face a significant overlap of coverage regions. This could happen more so in a 2.4 GHz band where there is limited number of available channels and band path loss is lower than 5 GHz band. In such circumstances, the performance could be affected by AP to AP co-channel interference. To overcome this circumstance, the Auto Cell Sizing feature uses AP to AP communication to share information on the degree of interference seen by each other. Based on this information, the APs dynamically adjust their radio Tx power and Rx parameters (or cell size) to mitigate interference. Enabling the Auto Cell Sizing option, disables the TX Power Adjustment configuration.
ChannelFly and Background Scanning

The controller offers the ChannelFly and Background Scanning automatic channel selection methods for spectrum utilization and performance optimization.

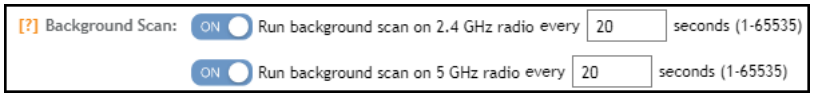
ChannelFly has undergone significant changes in SmartZone 5.2.1 release, combining the benefits of the Background Scanning method and the original Legacy ChannelFly. ChannelFly is the recommended method for all deployments.

TABLE 40

Channel Selection Method	When to Use
ChannelFly	Recommended method for most deployments.
Background Scanning	For existing deployments that currently use Background Scanning
Legacy ChannelFly (Accessible only from AP CLI)	When Background Scan is not allowed – Legacy ChannelFly excels at avoiding excessive interference without the need of *Background Scan*

NOTE

Both channel selection methods require *Background Scan*, ideally with the default 20 second scan interval.
Background Scan is accessible from the zone configuration, advanced settings.



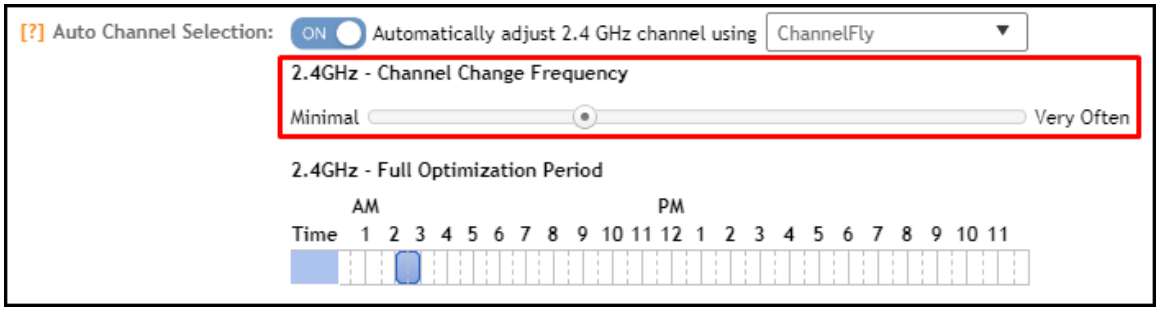
ChannelFly

ChannelFly uses Background Scan to collect information on the presence of neighboring APs and to assess how busy the channel is. The algorithm focuses on placing neighboring APs on different channels and avoiding busy channels. A Background Scan interval of 20 seconds is recommended for most deployments. In deployments where a larger interval is necessary, ChannelFly will still work but will take longer to settle upon a channel plan and may be less responsive to interference.

ChannelFly uses 802.11h channel change announcements to minimize the impact of channel changes on the wireless client. Despite 802.11h, channel changes still run the risk of disrupting wireless clients, and ChannelFly takes into the account the impact on associated clients.

The *Channel Change Frequency* (CCF) configuration allows the user to specify the responsive of ChannelFly to interference with consideration for the impact on associated clients. ChannelFly will avoid performing channel changes when a certain number of clients are associated to the AP on a

per-radio basis. This threshold is defined by the CCF. **With the default CCF of 33, channel changes may occur only when there are 3 or fewer associated clients**. The CCF also affects the probability that a channel change occurs when a better channel is found. However, a channel change will only occur when the number of associate clients is below the client threshold as defined in Table 41.



The following table details the threshold for each CCF. It provides the number of associated clients that would bar ChannelFly from performing a channel change.

TABLE 41 Client Threshold Table

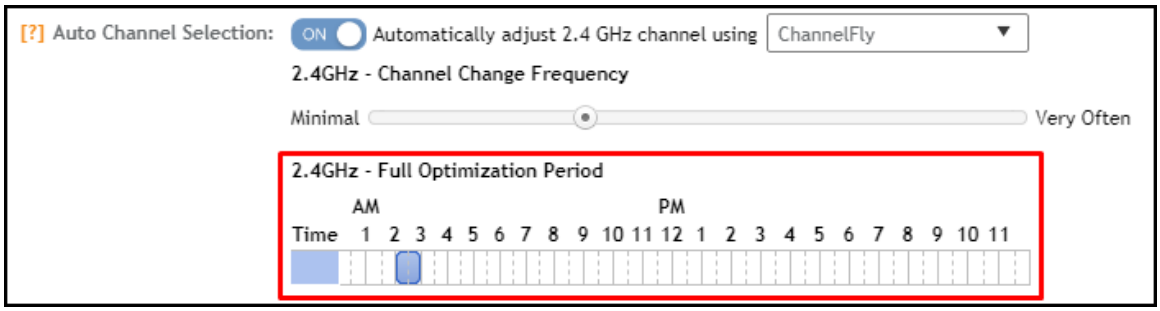
CCF	100	90	80	70	60	50	40	30	20	10	1
Client Threshold	10	9	8	7	6	5	4	3	2	1	0

For deployments where impact on the clients is less of a consideration and avoiding interference is paramount, higher values of CCF are recommended.

For deployments with low client counts, two or fewer associated clients per AP on average, a CCF of 10 or 20 is recommended. For deployments where channel changes are not allowed to impact any associate client, a CCF of 0 is recommended.

The *Full Optimization Period* configuration specifies a period of time where ChannelFly is allowed to ignore the impact of channel changes on associated clients. During this time, preferably when the wireless network is not expected to be actively servicing clients such as the middle of the night, ChannelFly will be free to full optimize the channel plan. A higher number of channel changes may be observed during this time.

The *Full Optimization Period* can be specified by clicking specific hours or by clicking-and-dragging across the time bar to affect multiple hours. The time periods can be non-contiguous, and the period can be disabled entirely by clicking the blue box under *Time*.



For the first hour following the reboot of an AP, ChannelFly may perform up to six channel changes in order to quickly settle upon a channel plan. During this period, ChannelFly will ignore the impact of channel changes on associated clients.

The table below summarizes the channel change behavior for each of the ChannelFly states.

TABLE 42 ChannelFly State and its Behavior

State	Behavior
AP reboot	Channel changes may occur at higher frequency for the first hour

TABLE 42 ChannelFly State and its Behavior (continued)

State	Behavior
Normal operation	Channel changes may occur only when the number of associated clients is lower than the client threshold based on the *Channel Change Frequency*
Full Optimization Period	Channel changes may occur at higher frequency

ChannelFly can be enabled/disabled per band. If there are 2.4 GHz clients do not support 802.11h on the wireless network, RUCKUS recommends disabling ChannelFly for 2.4 GHz but leaving it enabled for the 5 GHz band.

To revert to Legacy ChannelFly, first select ChannelFly from the controller, then from AP CLI:

```
rkscli: set channselectmode wifi<0/1> <mode>
   wifi0 - 2.4 GHz
   wifi1 - 5 GHz
  <mode> - 1: ChannelFly
           0: Legacy ChannelFly
```

Background Scanning

Background Scanning is a channel selection method, and *Background Scan* is the AP functionality where the AP briefly leaves the home channel to scan another channel.

Background Scanning uses Background Scan to collect information on the presence of neighboring APs. Background Scanning focuses on finding a channel with the fewest number of neighbors.

When the AP is rebooted, Background Scanning will enter a training period where the number of channel changes may be elevated in the first hour.

Background Scan is required, with the recommended default scan interval of 20 seconds. In situations where a larger scan interval is necessary, Background Scan will require a longer training period.

NOTE
In order to detect rogue APs on the network, you must enable Background Scan on the controller.

VIDEO
ChannelFly Overview. This video provides a brief overview of ChannelFly.
Click to play video in full screen mode.

VLAN Pooling

When Wi-Fi is deployed in a high density environment (such as a stadium) or on a university campus to provide access for students, the number of IP addresses required for client devices can easily run into several thousands.

Allocating a single large subnet results in a high probability of degraded performance due to factors like broadcast/multicast traffic.

To address this problem, VLAN pooling provides a method by which administrators can deploy pools of multiple VLANs from which clients are assigned, thereby automatically segmenting large groups of clients into smaller subgroups, even when connected to the same SSID.

As the client device joins the Wi-Fi network, the VLAN is assigned based on a hash of the client's MAC address (by default).

Creating an AP Group

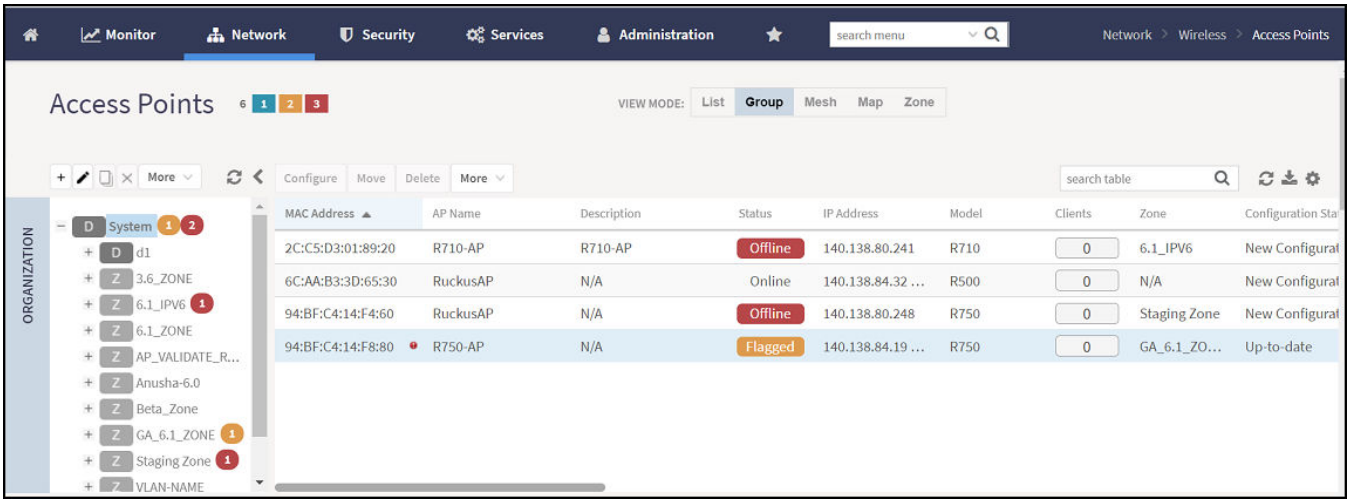
Creating an AP group means creating a configuration profile that defines the channels, radio settings, Ethernet ports and other configurable fields for all members of the group or for all APs of a specific model in the group.

Follow these steps to create an AP group.

1. On the main menu, click **Network** > **Access Point**

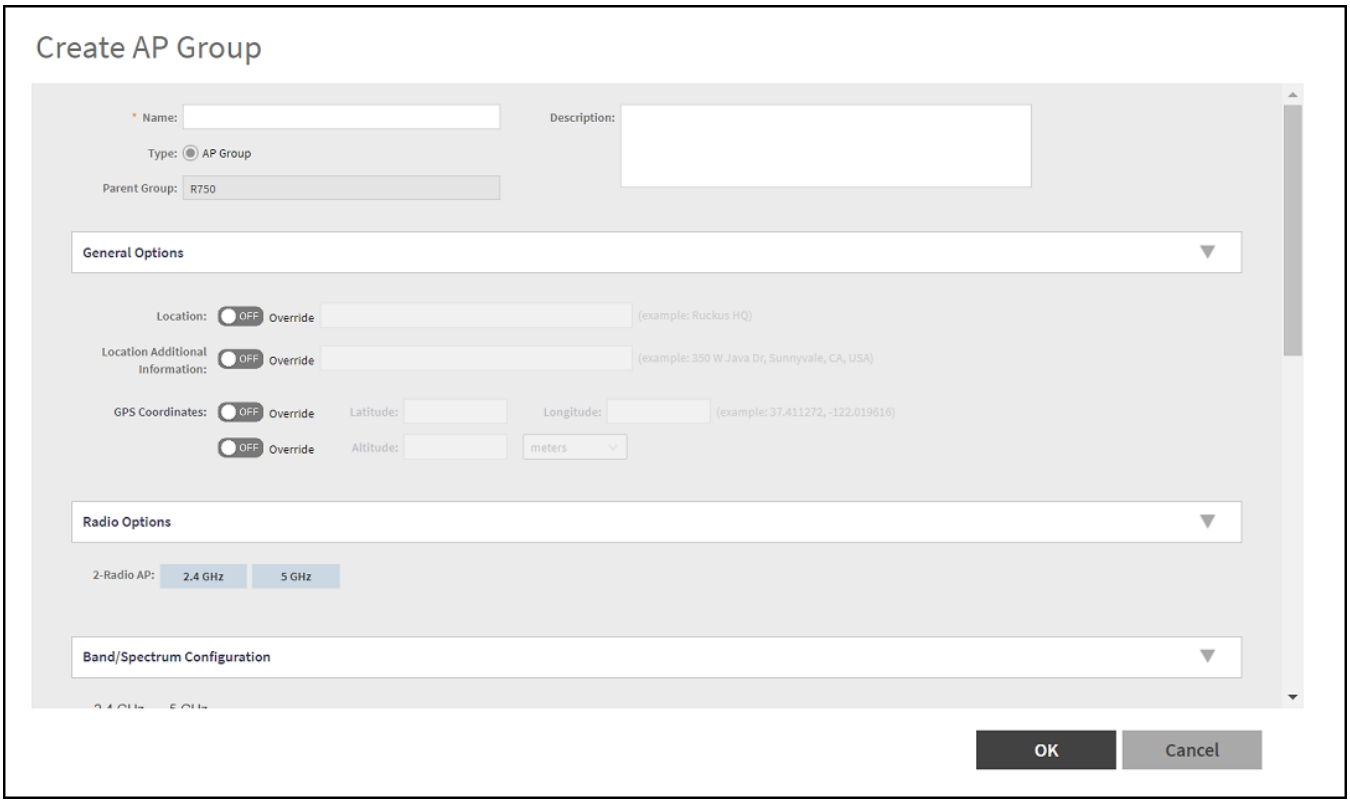
   The **Access Point** page is displayed.

FIGURE 57 Access Point Page



2. From the System tree hierarchy, select the location (for example: System, Domain, Zone) and click . The following figure appears.

FIGURE 58 Create an AP Group



3. Enter the details as explained in the following table.

NOTE

You can also edit the configuration of default APs by selecting the AP and clicking the  icon.

4. Click **OK**.

TABLE 43 AP Group Details

Field	Description	Your Action
Name	Indicates a name for the Zone/AP group.	Enter a name.
Description	Indicates a short description.	Enter a brief description
Type	Indicates if you are creating a domain, zone or an AP group.	Appears by default. You can also choose the option.
Parent Group	Indicates the parent group that this AP group belongs.	Appears by default.
Configuration > General Options		
Location	Indicates generic location.	Enter the location.
Location Additional Information	Indicates detailed location.	Enter additional location information.
GPS Coordinates	Indicates the geographical location.	Enter the following coordinates in meters or floor: • **Longitude** • **Latitude** • **Altitude**
Configuration > Group Members		
Members	Displays the list of APs that belong to the group.	Select the members from the list and click **Move to** to assign them to the required group.
Access Points	Displays the list of APs that belong to the zone.	Select the **Access Points** from the list and click **Add to Group**.
Configuration > Radio Options		
Dual-5G Mode	Enables third radio operator in 2.4 GHz, Lower 5 GHz, and Upper 5 GHz. By default, the **Dual-5G Mode** is enabled. In the enabled mode, radio-0 will be on 2.4GHz band, radio-1 will be on 5G Lower band and radio-2 will be on 5G Upper band. • 5G Lower BAND : UNII-1, UNII-2A • 5G Upper BAND : UNII-2C, UNII-3 In the disabled mode, the radio-0 will be on 2.4GHz band, radio-1 will be on 5G band and radio-2 will be on 6G band. This also depends on the country code.	Select or keep the default **Dual-5G Mode** option.
Configuration > Band/Spectrum Configuration > 2.4 GHz		
Channelization	Indicates the channel width.	Set the channel width used during transmission to either 20 or 40 (MHz), or select Auto to set it automatically.
Channel	Indicates the channel to use.	Select one of the options: Auto, 1, 6 or 11.
Auto Cell Sizing	Enables the AP to share information on interference seen by each other and dynamically adjust their radio Tx power and Rx parameters to minimize interference. Enabling this option disables the TX Power Adjustment configuration. **NOTE** Ensure that Background Scan is enabled.	Select the option.

TABLE 43 AP Group Details (continued)

Field	Description	Your Action
TX Power Adjustment	Allows to manually configure the transmit power on the 2.4 GHz radio. By default, the TX power is set to Full on the 2.4 GHz radio. **NOTE** If you choose Min, the transmit power is set to 0dBm (1mW) per chain for 11n APs, and 2dBm per chain for 11ac APs. If you choose Max, the transmit power is set to the maximum allowable value according to the AP's capability and the operating country's regulations.	Select the preferred TX power.
Protection Mode	Indicates the mechanism to reduce frame collision.	Choose one of the following options: • None • RTS/CTS • CTS Only
Background Scan	Allows the AP radio to scan other channels in the band for accessing channel health and capacity, detecting rogue devices, optimizing and mainting mesh links and to discover AP neighbors.	Enter the duration in seconds. Range: 1 through 65535.
Auto Channel Selection	Automatically adjusts the channel using the ChannelFly option.	Select the required option. For **ChannelFly**, set the **Channel Change Frequency** and **Full Optimization Period**.
Configuration > Band/Spectrum Configuration > 5 GHz		
Channelization	Indicates the channel width.	Set the channel width used during transmission: Auto, 20, 40, 80 and 160.
Channel	Indicates the channel to use.	Select the required options for the Indoor and Outdoor APs.
Secondary Channel	Indicates the secondary channel to used.	By default, the Indoor and Outdoor option is set to Auto.
Allow DFS Channels	Allows ZoneFlex APs to use DFS channels.	Click to enable the option.
Allow Channel 144	Provides channel 140 and 144 support for 11ac and 11ax APs. Enabling this option supports 20 MHz, 40 MHz, or 80 MHz channel modes. The 160 MHz mode is supported if the AP supports this mode. Disabling this option provides Channel 140 support only to 20 MHz mode. **NOTE** This option is available for selection only if you enable the **DFS Channels** option. **NOTE** This feature is currently supported only in the United States.	Click to enable the option.
Allow Indoor Channels	Allows outdoor APs to use channels regulated as for indoor use only.	Click to enable the option.

TABLE 43 AP Group Details (continued)

Field	Description	Your Action
Auto Cell Sizing	Enables the AP to share information on interference seen by each other and dynamically adjust their radio Tx power and Rx parameters to minimize interference. Enabling this option disables the TX Power Adjustment configuration. **NOTE** Ensure that Background Scan is enabled.	Select the option.
TX Power Adjustment	Allows to manually configure the transmit power on the 5 GHz radio. By default, the TX power is set to Full on the 5 GHz radio. **NOTE** If you choose Min, the transmit power is set to 0dBm (1mW) per chain for 11n APs, and 2dBm per chain for 11ac APs. If you choose Max, the transmit power is set to the maximum allowable value according to the AP's capability and the operating country's regulations.	Select the preferred TX power.
Background Scan	Allows the AP radio to scan other channels in the band for accessing channel health and capacity, detecting rogue devices, optimizing and mainting mesh links and to discover AP neighbors.	Enter the duration in seconds. Range: 1 through 65535.
Auto Channel Selection	Automatically adjusts the channel using the ChannelFly option.	Select the required option. For **ChannelFly**, set the **Channel Change Frequency** and **Full Optimization Period**.
Configuration > **Band/Spectrum Configuration** > **6 GHz** **NOTE** This tab is available only if the **Tri-band Dual-5G Mode** option is not enabled.		
Channelization	Indicates the channel width.	Set the channel width used during transmission: Auto, 20, 40, 80 and 160.
Channel	Indicates the channel to use.	Select the required options for the Indoor and Outdoor APs.
Auto Cell Sizing	Enables the AP to share information on interference seen by each other and dynamically adjust their radio Tx power and Rx parameters to minimize interference. Enabling this option disables the TX Power Adjustment configuration. **NOTE** Ensure that Background Scan is enabled.	Select the option.

TABLE 43 AP Group Details (continued)

Field	Description	Your Action
TX Power Adjustment	Allows to manually configure the transmit power on the 6 GHz radio. By default, the TX power is set to Full on the 6 GHz radio. **NOTE** If you choose Min, the transmit power is set to 0dBm (1mW) per chain for 11n APs, and 2dBm per chain for 11ac APs. If you choose Max, the transmit power is set to the maximum allowable value according to the AP's capability and the operating country's regulations.	Select the preferred TX power.
LPI (Low Power Indoor) mode:	Allows the use of a 4 U-NII bands U-NII-5 to U-NII-8 indoors at a reduced Tx power level.	Enable the option.
Background Scan	Allows the AP radio to scan other channels in the band for accessing channel health and capacity, detecting rogue devices, optimizing and mainting mesh links and to discover AP neighbors.	Enter the duration in seconds. Range: 1 through 65535.
Auto Channel Selection	Automatically adjusts the channel using the ChannelFly option.	For **ChannelFly**, set the **Channel Change Frequency** and **Full Optimization Period**.
Configuration > **Band/Spectrum Configuration** > **Lower 5 GHz**		
Channelization	Indicates the channel width.	Set the channel width used during transmission: Auto, 20, 40, 80 and 160.
Channel	Indicates the channel to use.	Select the required options for the Indoor and Outdoor APs.
Allow DFS Channels	Allows ZoneFlex APs to use DFS channels.	Click to enable the option.
Allow Indoor Channels	Allows outdoor APs to use channels regulated as for indoor use only.	Click to enable the option.
Auto Cell Sizing	Enables the AP to share information on interference seen by each other and dynamically adjust their radio Tx power and Rx parameters to minimize interference. Enabling this option disables the TX Power Adjustment configuration. **NOTE** Ensure that Background Scan is enabled.	Select the option.
TX Power Adjustment	Allows to manually configure the transmit power on the Lower 5 GHz radio. By default, the TX power is set to Full on the Lower 5 GHz radio. **NOTE** If you choose Min, the transmit power is set to 0dBm (1mW) per chain for 11n APs, and 2dBm per chain for 11ac APs. If you choose Max, the transmit power is set to the maximum allowable value according to the AP's capability and the operating country's regulations.	Select the preferred TX power.
Background Scan	Allows the AP radio to scan other channels in the band for accessing channel health and capacity, detecting rogue devices, optimizing and mainting mesh links and to discover AP neighbors.	Enter the duration in seconds. Range: 1 through 65535.

TABLE 43 AP Group Details (continued)

Field	Description	Your Action
Auto Channel Selection	Automatically adjusts the channel using the ChannelFly option.	Select the required option. For **ChannelFly**, set the **Channel Change Frequency** and **Full Optimization Period**.
Configuration > **Band/Spectrum Configuration** > **Upper 5 GHz**		
Channelization	Indicates the channel width.	Set the channel width used during transmission: Auto, 20, 40, 80 and 160.
Channel	Indicates the channel to use.	Select the required options for the Indoor and Outdoor APs.
Allow DFS Channels	Allows ZoneFlex APs to use DFS channels.	Click to enable the option.
Allow Channel 144	Provides channel 140 and 144 support for 11ac and 11ax APs. Enabling this option supports 20 MHz, 40 MHz, or 80 MHz channel modes. The 160 MHz mode is supported if the AP supports this mode. Disabling this option provides Channel 140 support only to 20 MHz mode. **NOTE** This option is available for selection only if you enable the **DFS Channels** option. **NOTE** This feature is currently supported only in the United States.	Click to enable the option.
Auto Cell Sizing	Enables the AP to share information on interference seen by each other and dynamically adjust their radio Tx power and Rx parameters to minimize interference. Enabling this option disables the TX Power Adjustment configuration. **NOTE** Ensure that Background Scan is enabled.	Select the option.
TX Power Adjustment	Allows to manually configure the transmit power on the Upper 5 GHz radio. By default, the TX power is set to Full on the Upper 5 GHz radio. **NOTE** If you choose Min, the transmit power is set to 0dBm (1mW) per chain for 11n APs, and 2dBm per chain for 11ac APs. If you choose Max, the transmit power is set to the maximum allowable value according to the AP's capability and the operating country's regulations.	Select the preferred TX power.
Background Scan	Allows the AP radio to scan other channels in the band for accessing channel health and capacity, detecting rogue devices, optimizing and mainting mesh links and to discover AP neighbors.	Enter the duration in seconds. Range: 1 through 65535.
Auto Channel Selection	Automatically adjusts the channel using the ChannelFly option.	Select the required option. For **ChannelFly**, set the **Channel Change Frequency** and **Full Optimization Period**.
Configuration > AP GRE Tunnel Options		

TABLE 43 AP Group Details (continued)

Field	Description	Your Action
Ruckus GRE Forwarding Broadcast	Forwards broadcast traffic from network to tunnel. **NOTE** ARP and DHCP traffic are allowed even if this option disabled	Click **Override** to enable the Ruckus GRE broadcast forwarding option. Click the **Enable Forwarding Broadcast** option to forward the broadcast traffic.
Configuration > AP SNMP Options		
Override zone configuration	Indicates that the AP Group configuration overrides the zone configuration.	Select the check box.
Enable AP SNMP	Indicates if the AP SNMP option is enabled.	Select the check box.
SNMPv2 Agent	Indicates SNMPv2 Agent is applied.	1. Click **Create** and enter **Community**. 2. Select the required **Privilege**. If you select **Notification** enter the **Target IP**. 3. Click **OK**.
SNMPv3 Agent	Indicates SNMPv3 Agent is applied.	1. Click **Create** and enter **User**. 2. Select the required **Authentication**. 3. Enter the **Auth Pass Phrase**. 4. Select the **Privacy** option. 5. Select the required **Privilege**. If you select **Notification** select the option **Trap** or **Inform** and enter the **Target IP** and **Target Port**. 6. Click **OK**.
Configuration > Model Specific Options **NOTE** Select the **Override** check box for that setting, and then configure the setting.		
AP Model	Indicate the AP model for which you are configuring.	Select the option.
Status LEDs	Disable the status LED on the selected AP model.	Select the option.
LLDP	Enables the Link Layer Discovery Protocol (LLDP) on the selected AP model.	Select the option and enter the following details: • **Advertise Interval**—Enter the duration in seconds. • **Hold Time**—Enter the duration in seconds. • **Enable Management IP TLV**—Select the check box.
External Antenna (2.4 GHz)	Enables the external 2.4 GHz antenna on the selected AP model.	Select the **Enable external antenna** check box, and then set the gain value (between 0 and 90dBi) in the box provided.
External Antenna (5 GHz)	Enables the external 5 GHz antenna on the selected AP model.	Select the **Enable external antenna** check box, and then set the gain value (between 0 and 90dBi) in the box provided.
Port Settings	Indicates the port settings.	Select the option and choose the required LAN option.
PoE out port	Enables PoE out mode.	Select the Enable PoE out ports (specific ZoneFlex AP models only) check box.

TABLE 43 AP Group Details (continued)

Field	Description	Your Action
PoE Operating Mode	Indicates the PoE operating mode of the selected AP model. **NOTE** You can set the PoE operating mode from the **AP Configuration** tab on the controller or using the **get power-mode** CLI command. • R550 • R610 • R650 • R710 • R720 • R730 • R750 • R850 • M510 • H550 • T610 • T610S • T750 • T750SE	Choose the option. **NOTE** When this option is selected, some AP features are disabled to reduce power consumption, such as the USB port and one of the Ethernet ports.
Internal Heater	Enables the heater that is built into the selected AP model	Select the Enable internal heaters (specific AP models only) check box.
USB Port	Disables the USB port. USB ports are enabled by default.	Select the Disable USB port check box.
Configuration > Cellular Options		
LTE Band Lock	Displays the list of LTE bands (4G/3G) and allows you to lock one or more bands from the list. Once a lock is enabled, the connection will be established only to the specified bands. The LTE band lock function is disabled by default. **NOTE** The list of bands is only applicable to: • **Domain** • **USA** • **Canada** • **Japan**	Select **Override zone configuration** to enable and choose the band from the following: • **Primary Sim** • **Secondary Sim**
Configuration > Advanced Options		
Location Based Service	Enables location-based service for the AP group.	• Select the **Override zone configuration** check box. • Select the **Enable LBS Service** check box. • **Select an LBS Server** from the drop-down.

TABLE 43 AP Group Details (continued)

Field	Description	Your Action
Hotspot 2.0 Venue Profile	Indicates the hotspot profile that you want to assign to the group.	Select the required option or click **Create** and update the following details: • Enter the **Name**. • Enter the **Description**. • Enter the **Venue Names**. • Select the **Venue Category**. • Select the **Type**. • Enter the **WLAN Metrics**.
AP Management VLAN	Indicates the AP management VLAN settings.	Choose the option. Click **VLAN ID**, and then type the VLAN ID that you want to assign (valid range is from 1 to 4094). To keep the same management VLAN ID that has been configured on the AP, click **Keep AP's settings**. **ATTENTION** For standalone APs, set the AP ethernet port to trunk before changing the AP Management VLAN settings.
Client Admission Control	Indicates the load thresholds on the AP at which it will stop accepting new clients.	Select the **Override** check box respective to **2.4 GHz Radio** or **5 GHz Radio** and update the following details: • **Enable** **NOTE** Client load balancing and band balancing will be disabled for this AP group. • **Min Client Count** • **Max Radio Load** • **Min Client Throughput**
Rogue Classification Policy	Indicates the parameters used to classify rogue APs. This option is available only if you enable the **Rogue AP Detection**option.	Select the options for rogue classification policy: • Enable the **Override** option and select the rogue classification policy from the list to override for this group. • Enable the **Override** option and enter the **Report RSSI Threshold**. Range: **0** through **100**. • Enable the **Overide** option to override the aggressiveness of protecting the network and choose one of the following: – **Aggressive** – **Auto** – **Conservative** • Enable the **Override** option and enter the **Jamming Threshold** in percentage.
Recovery SSID	Allows you to enable or disable the Recovery(Island) SSID broadcast on the controller.	Enable **Recovery SSID Broadcast**
Direct Multicast	Indicates whether multicast traffic is sent from a wired device, wireless device or from the network.	Select one or more of the following: • **Multicast Traffic from Wired Client** • **Multicast Traffic from Wireless Client** • **Multicast Traffic from Network**
VxLAN Network Identifier (VNI)	Used to uniquely identify VxLAN	Enter single value or range. Range is 1- 16777215

NOTE

You can also edit, clone or delete an AP Group by selecting the options Configure , Clone  or Delete  respectively, from the Access Points page.

Configuring Model-Based Settings

You can apply a set of settings to all APs of a particular model, use the **Model Specific Options** section.

Complete the following steps to configure model based settings.

1. Click **Network** > **Wireless** > **Access Points**.
2. From the list, select AP for which you want to apply model-based settings and click **Configure**. This displays **Edit AP**.
3. Scroll down to **Model Specific Options** section, expand the section.
4. In **Model Specific Control**, select **Override zone config** check box. The settings available for the AP model are displayed.
5. In the **General Options** section, configure the following settings.

NOTE
The options that appear in the **Model Specific Options** section depend on the AP model that you select. Not all the options described in the following table are displayed for every AP model.

TABLE 44 Configuring the Model Specific Options

Option	Description
USB Port	To disable the USB port on the selected AP model, select the **Disable USB port** check box. USB ports are enabled by default.
Status LEDs	To disable the status LED on the selected AP model, select the **Disable Status LEDs** check box.
LLDP	To enable Link Layer Discovery Protocol (LLDP) on the selected AP model, select the **Enable Link Layer Discovery Protocol** check box. • Enter the **Advertise Interval** duration in seconds. • Enter the **Hold Time** duration in seconds. • Select the **Enable Management IP TLV** check box.
PoE Operating Mode	Click the drop-down to view the available options. Options are: • Auto (default) • 802.3at • 802.3af • 802.3bt/Class 5 • 802.3bt/Class 6 • 802.3bt/Class 7 **NOTE** If **802.3af PoE Operating Mode** PoE is selected, this AP model will operate in 802.3af mode and will consume less power than in 802.3at mode. However, when this option is selected, some AP features, such as the USB port and one of the Ethernet ports, are disabled to reduce power consumption. For AP model R640, if **802.3at PoE Operating Mode** PoE is selected and the **USB Port** option is enabled, the second Ethernet port and any devices running on that port will be disabled.

TABLE 44 Configuring the Model Specific Options (continued)

Option	Description
PoE out port	To enable the PoE out port on the selected AP model, select the **Enable PoE out ports (specific ZoneFlex AP models only)** . **NOTE** If the controller country code is set to United Kingdom, an additional **Enable 5.8 GHz Channels** option will be available for outdoor 11n and 11ac APs. Enabling this option allows the use of restricted C-band channels. These channels are disabled by default and should only be enabled by customers with a valid license to operate on these restricted channels.
Internal Heater	To enable the heater that is built into the selected AP model, select the **Enable internal heaters (specific AP models only)** check box.
External Antenna (2.4 GHz)	To enable the external 2.4-GHz antenna on the selected AP model, select the **Enable external antenna** check box, and then set the gain value (between 0 and 90dBi) in the field provided.
External Antenna (5 GHz)	To enable the external 5-GHz antenna on the selected AP model, select the **Enable external antenna** check box, and then set the gain value (between 0 and 90dBi) in the field provided.

NOTE
For H series AP models such as H500 and H510, you can disable LAN5.

6. In the **Port Settings** section, configure the following options for each LAN port.

NOTE
The number of LAN ports that appear in this section correspond to the physical LAN ports that exist on the selected AP model.

NOTE
When trunk port limitation is enabled, the controller does not validate the port settings configured in the AP or the AP group with no members.

TABLE 45 Configuring the Options for LAN Port

Option	Description
Enable	Use this option to enable and disable this LAN port on the selected AP model. By default, this check box is selected. To disable this LAN port, clear this check box.
Profile	Use this option to select the Ethernet port profile that you want this LAN port to use. Two default Ethernet port profiles exist: **Default Trunk Port** (selected by default) and **Default Access Port**. If you created Ethernet port profiles (see *Creating an Ethernet Port Profile*), these profiles will also appear on the drop-down list. **NOTE** If you recently created an Ethernet port profile and it does not appear on the drop-down menu, click **Reload** on the drop-down menu to refresh the Ethernet port profile list.
Overwriter VLAN	Select the **Overwriter VLAN** check box and enter: • **Untag ID**—Default: 1 • **Members**—Range: 1 through 4094.

7. Click **OK**.

Supported LLDP Attributes

The Link Layer Discovery Protocol (LLDP) is a vendor-neutral Layer 2 protocol that allows a network device (for example, a RUCKUS AP) to advertise its identity and capabilities on the local network.

LLDP information is sent by devices from each of their interfaces at a fixed interval (default is 30 seconds), in the form of an Ethernet frame. Each LLDP Ethernet frame contains a sequence of type-length-value (TLV) structures starting with Chassis ID, Port ID and Time to Live (TTL) TLV. The follwoing table lists the LLDP attributes supported by the controller.

TABLE 46 LLDP Attributes

Attribute (TLV)	Description
Chassis ID	Indicates the MAC address of the AP's br0 interface
Port ID	Identifies the port from which the LLDP packet was sent
Time to Live	Same as LLDP Hold Time. Indicates the length of time (in seconds) that a receiving device will hold the LLDP information sent by the selected AP model before discarding it. The default value is 120 seconds.
System Name	Indicates the name assigned to the AP. The default name of RUCKUS APs is RuckusAP.
System Description	Indicates the AP model plus software version
System Capabilities	Indicates the AP's capabilities (Bridge, WLAN AP, Router, Docsis), and which capabilities are enabled
Management Address	Indicates the management IP address of the AP
Port Description	Indicates the description of the port in alphanumeric format

Configuring the Port Settings of a Particular AP Model

Use Port Settings in the AP Model-Specific Configuration section to configure the Ethernet ports of a particular AP model.

Follow these steps to configure the port settings of a certain AP model.

1. All ports are enabled by default (the Enable check boxes are all selected). To disable a particular port entirely, clear the Enable check box next to the port name (LAN1, LAN2, etc.)
2. For any enabled ports, you can choose whether the port will be used as a Trunk Port, Access Port, or General Port.

   The following restrictions apply:

   - All APs must be configured with at least one Trunk Port.

     NOTE
     You cannot move an AP model to an AP group and configure the AP model to use a trunk port at the same time, if general ports are enabled when trunk port limitation is disabled. You must configure the selected AP model to use at least one trunk port, and then move the AP model to the AP group.

   - For single port APs, the single LAN port must be a trunk port and is therefore not configurable.
   - For ZoneFlex 7025/7055, the LAN5/Uplink port on the rear of the AP is defined as a Trunk Port and is not configurable. The four front-facing LAN ports are configurable.
   - For all other APs, you can configure each port individually as either a Trunk Port, Access Port, or General Port. For more information, refer the *Designating an Ethernet Port Type*.

Creating a Monitoring AP Group

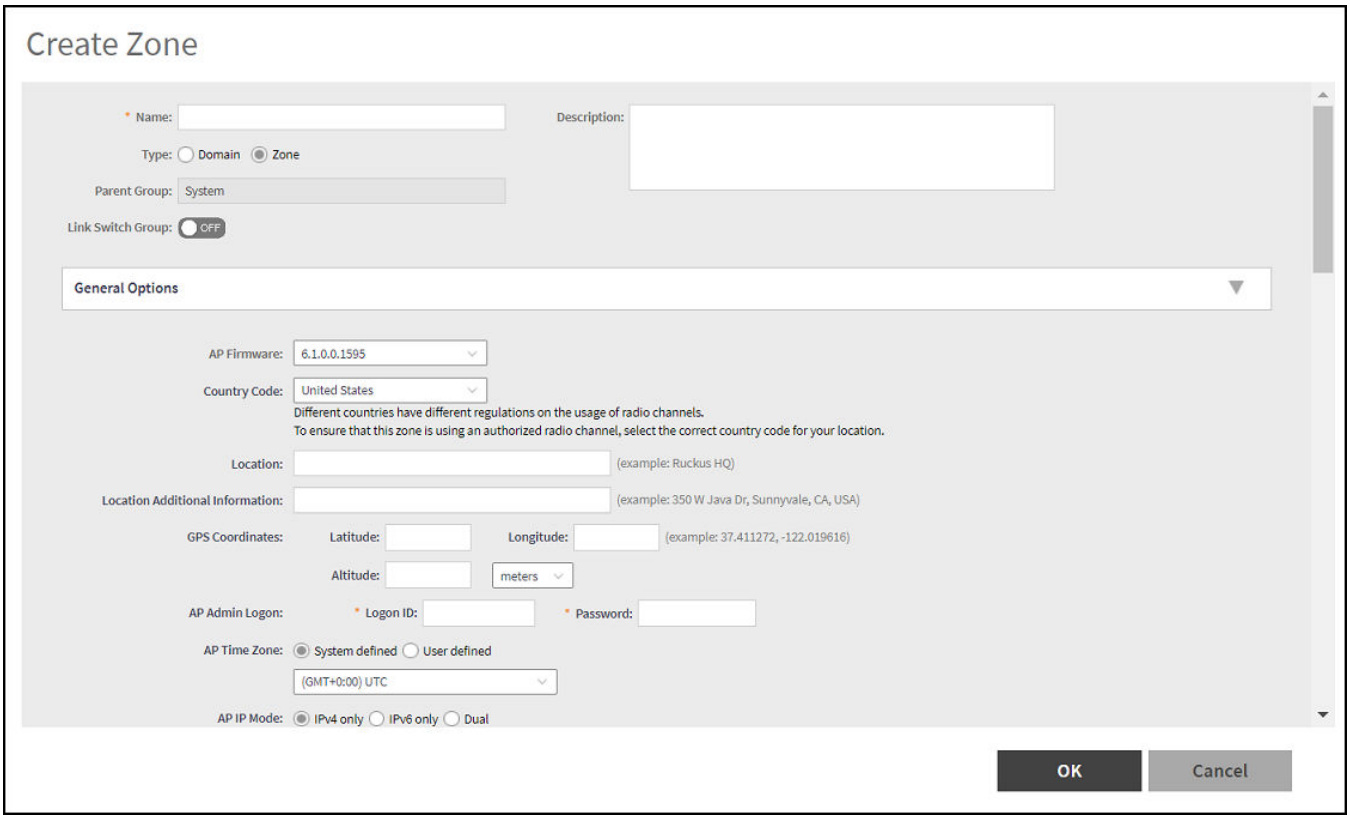
As a prerequisite, the monitoring AP must be connected to the controller.

Perform the following procedure to create a monitoring AP group.

1. From the main menu, click **Monitor** > **Monitoring APs**.

2. Select **System** and click **+** to create a zone.

FIGURE 59 Creating a Zone



3. For **Type**, select **Zone**.
4. Select **General Options** > **AP Admin Logon**, enter the user name and password, and click **OK**.
5. Under **Advanced Options**, enable **Rogue AP Detection**.
6. For **Rogue Classification Policy**, configure the following options:
   a) In the **Report RSSI Threshold** field, enter the threshold (the threshold ranges from 0 through 100).
   b) Enabling the option **Protect the network from malicious rogue access points** has no effect as an AP in monitoring mode is a passive listener.

      NOTE
      An AP in a monitoring group cannot be used for prevention services. The monitoring AP will work only in passive mode.

   c) Enable **Radio Jamming Session** and enter the jamming threshold as a percentage.
   d) Click **OK**.

7. On the **Monitoring APs** page, select the AP Zone you just created and click **+** to create the AP Monitoring Group.

FIGURE 60 Creating an AP Monitoring Group

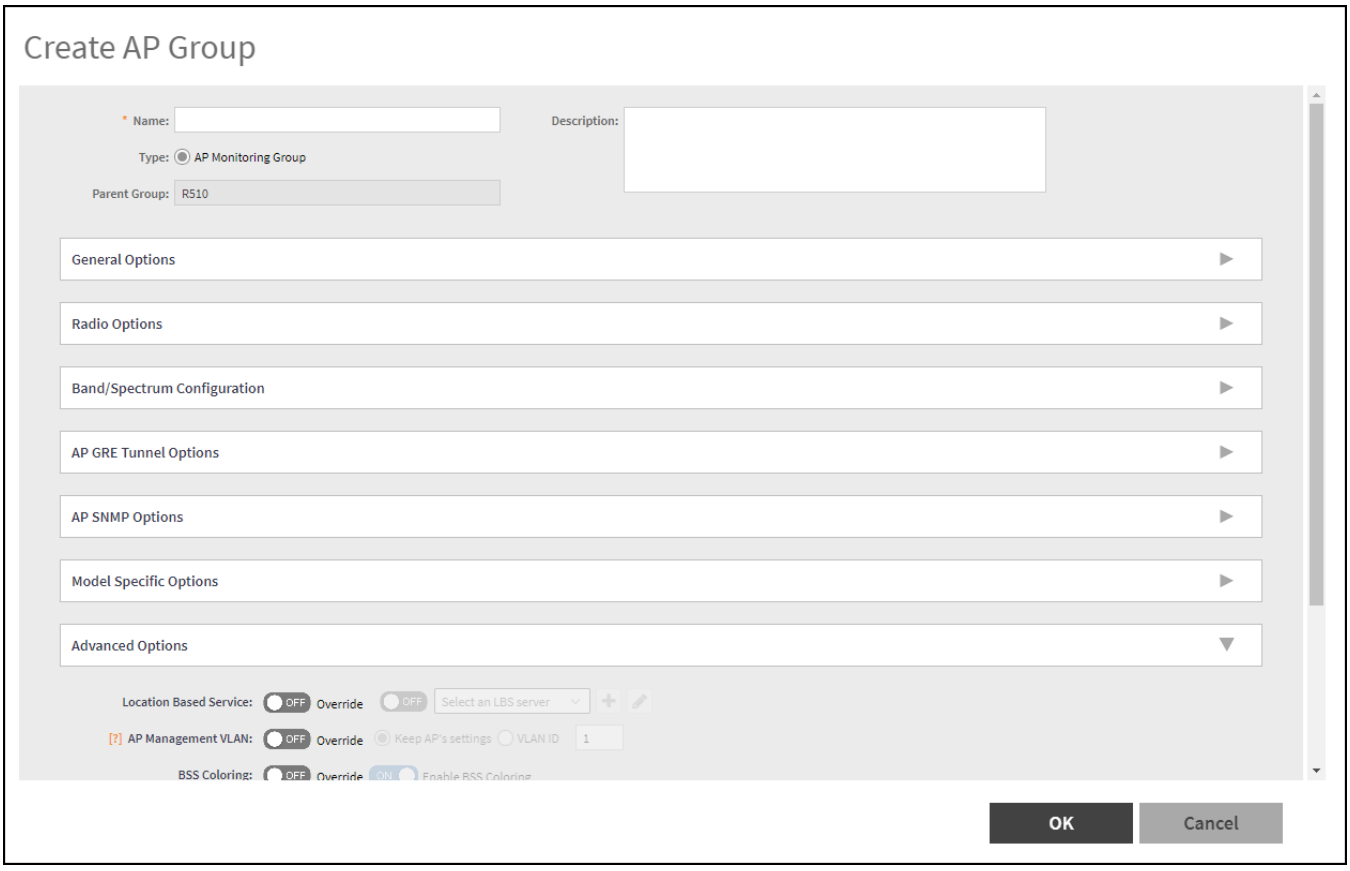
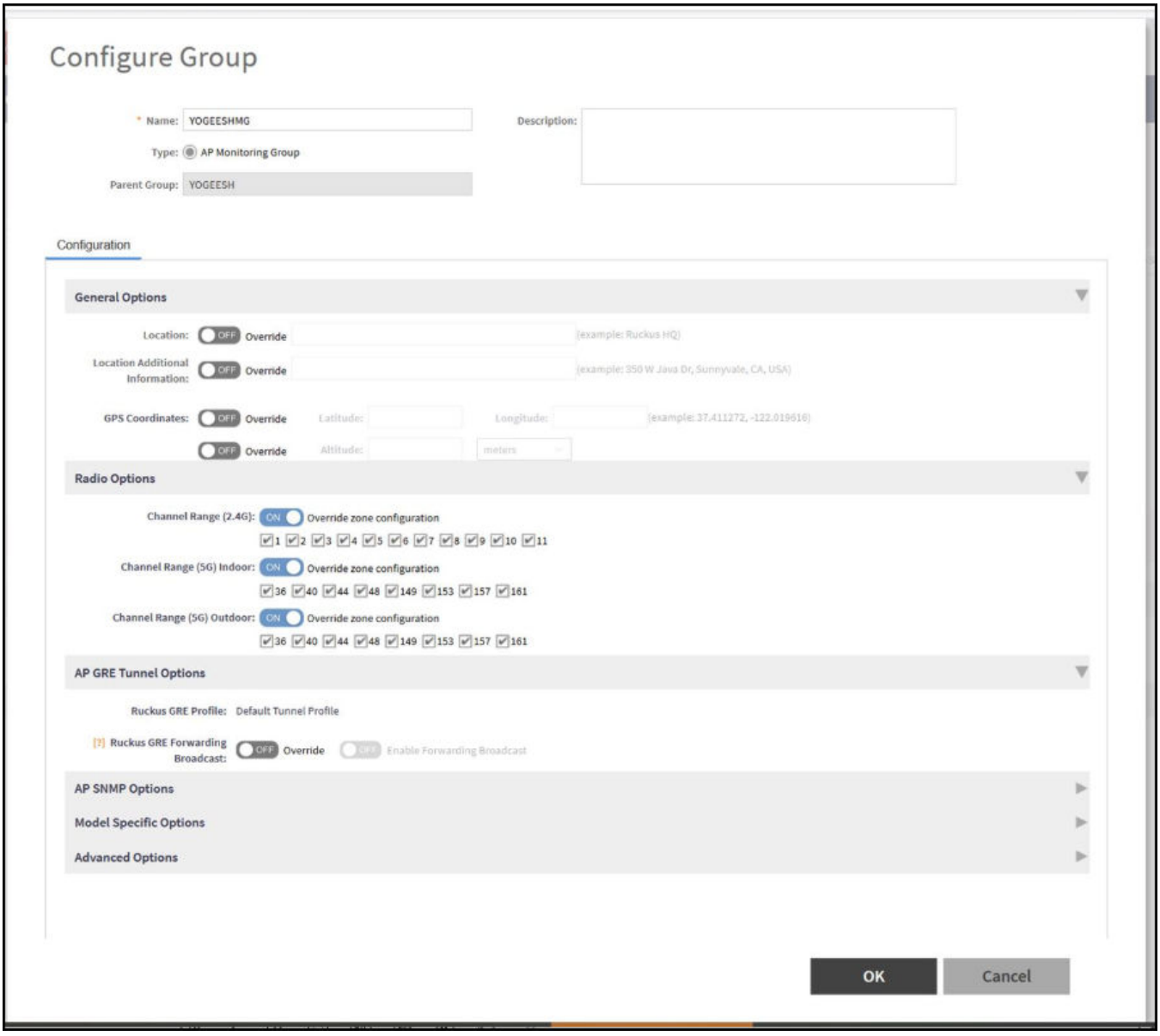


FIGURE 61 Configuring Group



8. Enter the group name.
9. Under **Radio Options**, you can select the bandwidth over the **2.4G**, **(5G) Indoor** and **(5G) Outdoor** channel range.

10. Under **Advanced Options**, configure the following options:
    a) Enable **Rogue Classification Policy** and select a rogue classification policy from the list.

    NOTE
    You can click **+** to create a rogue classification policy. To create a rogue classification policy, refer to the **Classifying a Rogue Policy** section in the *SmartZone 6.1.x (LT-GA) Security Guide (SZ300/vSZ-H) Configuration Guide*.

    NOTE
    Rogue detection AP in active-active mode cluster redundancy environment is restricted from storing its own BSSIDs to avoid considering its own APs as rougues attacking.

    b) In the **Report RSSI Threshold** field, enter the threshold (the threshold ranges from 0 through 100).
    c) Enable **Radio Jamming Session** and enter the jamming threshold as a percentage.
    d) Select the frequency for scanning to detect rogue devices:
    - **Low** (20 seconds)
    - **Medium** (60 seconds)
    - **High** (120 seconds)

    NOTE
    You can configure **Jamming Threshold** and **Report RSSI Threshold** for individual APs.

11. To move the AP group to the **Monitoring APs** page, complete the following steps:
    a) In the **Access Points** page, select the AP from the **Default Zone** and click **Move**.
    b) In the **Select Destination Management Domain** page, select the AP monitoring group to where the selected AP must be moved and click **OK**.

    Viewing Associated Events

    a. From the left pane, select **Monitoring APs**.
    b. Select the zone and the corresponding monitoring AP group and AP, and click **Event**.

    The event table lists the rogue APs that are detected by the monitoring AP. Likewise, the rogue APs that are detected by the monitoring AP are listed on the **Rogue Devices** page.

Designating an Ethernet Port Type

Ethernet ports can be configured as access ports, trunk ports, or general ports.

Trunk links are required to pass VLAN information between switches. Access ports provide access to the network and can be configured as members of specific VLANs, thereby separating the traffic on these ports from traffic on other VLANs. General ports are user-defined ports that can have any combination of up to 20 VLAN IDs assigned.

For most ZoneFlex APs, you can set ports to be Access, Trunk and General Ports from the controller web interface, as long as at least one port on each AP is designated as a Trunk Port.

By default, all ports are enabled as Trunk Ports with Untag VLAN set as 1 (except for ZoneFlex 7025, in which front ports are enabled as Access Ports by default). If configured as an Access Port, all untagged ingress traffic is the configured Untag VLAN, and all egress traffic is untagged. If configured as a Trunk Port, all untagged ingress traffic is configured Untag VLAN (by default, 1), and all VLAN-tagged traffic on VLANs 1-4094 will be seen when present on the network.

The default Untag VLAN for each port is VLAN 1. Change the Untag VLAN to:

- Segment all ingress traffic on this Access Port to a specific VLAN.

- Redefine the native VLAN on this Trunk Port to match your network configuration.

When trunk port limitation is disabled using the **eth-port-validate-one-trunk disable** command, validation checks are not performed for the VLAN members and the AP Management VLAN. If the AP configuration for general ports and access ports do not include a member of an AP management VLAN, or the VLAN of a WAN interface configured through CLI, the AP will disconnect and the Ethernet port stops transmitting data. Make sure that you configure the correct VLAN member in the ports (general/access) and the AP management VLAN.

NOTE
Ensure that at least one of the general port VLANs is the same as a Management VLAN of the AP.

Access Ports

Access ports provide access to the network and can be configured as members of a specific VLAN, thereby separating the traffic on these ports from traffic on other VLANs.

NOTE
This feature is applicable only for SZ300 and vSZ-H platforms.

All Access Ports are set to Untag (native) VLAN 1 by default. This means that all Access Ports belong to the native VLAN and are all part of a single broadcast domain. When untagged frames from a client arrive at an AP's Access Port, they are given an 802.1Q VLAN header with 1 as their VLAN ID before being passed onto the wired network.

When VLAN 1 traffic arrives destined for the client, the VLAN tag is removed and it is sent as untagged 802.11 traffic. When any tagged traffic other than VLAN 1 traffic arrives at the same Access Port, it is dropped rather than being forwarded to the client.

To remove ports from the native VLAN and assign them to specific VLANs, select the Access Port and enter any valid VLAN ID in the VLAN ID field (valid VLAN IDs are 2-4094).

The following table describes the behavior of incoming and outgoing traffic for Access Ports with VLANs configured.

TABLE 47 Access Ports with VLANs Configured

VLAN Settings	Incoming Traffic (from Client)	Outgoing Traffic (to Client)
Access Port, Untag VLAN 1	All incoming traffic is native VLAN (VLAN 1).	All outgoing traffic on the port is sent untagged.
Access Port, Untag VLAN [2-4094]	All incoming traffic is sent to the VLANs specified.	Only traffic belonging to the specified VLAN is forwarded. All other VLAN traffic is dropped.

Trunk Ports

Trunk links are required to pass VLAN information between switches. Trunking is a function that must be enabled on both sides of a link.

NOTE
This feature is applicable only for SZ300 and vSZ-H platforms.

If two switches are connected together, both switch ports must be configured as trunk ports.

The trunk port is a member of all the VLANs that exist on the AP/switch and carries traffic for all VLANs between switches.

For a trunk port, the VLAN Untag ID field is used to define the native VLAN - the VLAN into which untagged ingress packets are placed upon arrival. If your network uses a different VLAN as the native VLAN, configure the AP trunk port's VLAN Untag ID with the native VLAN used throughout your network.

General Ports

General ports are user-specified ports that can be assigned a combination of up to 20 VLAN IDs.

NOTE
This feature is applicable only for SZ300 and vSZ-H platforms.

General ports function similarly to Trunk ports, except that where Trunk ports pass all VLAN traffic, General ports pass only the VLAN traffic that is defined by the user.

To configure an AP Ethernet port as a General port, select General Port and enter multiple valid VLAN IDs separated by commas or a range separated by a hyphen.

> **NOTE**
> You must also include the Untag VLAN ID in the Members field when defining the VLANs that a General port will pass. For example, if you enter 1 as the Untag VLAN ID and want the port to pass traffic on VLANs 200 and 300, you would enter: 1,200,300.

Configuring Client Admission Control

As an administrator, you can help maintain a positive user experience for wireless users on the network by configuring the following client admission control settings:

- Minimum client count
- Maximum radio load
- Minimum client throughput

Client admission control is implemented on a per radio basis and is supported on 802.11n and 802.11ac APs.

Monitoring WLAN Services

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 table lists the tabs that appear for System, Domain, Zone, and AP Group.

TABLE 48 System, Domain, Zone, and AP Groups Monitoring Tabs

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**

Moving an AP Zone Location

Follow these steps to move an AP zone to a different location:

1. From the Access Points page, locate the AP zone that you want to move to a different location.
2. Click **Move**, the **Select Destination Management Domain** dialog box appears.
3. Select the destination and click **OK**, a confirmation dialog box appears.
4. Click **Yes**, the page refreshes and AP zone is moved to the selected destination.

Creating a New Zone using a Zone Template

Follow these steps to create a new zone using a template:

1. From the Access Points page, locate the zone from where you want to create a new zone.
2. Click **More** and select **Create New Zone from Template**, a dialog box appears.
3. In **Zone Name**, enter a name for the new AP zone.
4. Select the required template from the **Template Name** drop-down.
5. Click **OK**. The page refreshes and and the new zone is created.

Extracting a Zone Template

You can extract the current configuration of a zone and save it as a zone template.

Follow these steps to extract the configuration of a zone to a zone template:

1. From the Access Points page, locate the zone from where you want to extract the WLAN template.
2. Click **More** and select **Extract Zone Template**, the **Extract Zone Template** dialog box appears.
3. In **Zone Template Name**, enter a name for the Template.
4. Click **OK**, a message appears stating that the zone template was extracted successfully.
5. Click **OK**. You have completed extracting a zone template.

   The extracted Zone template can be viewed under **System** > **Templates** > **Zone Templates**.

Applying a Zone Template

You can apply an AP zone configuration template to a zone.

Follow these steps to apply a zone template:

1. From the Access Points page, locate the zone where you want to apply the zone template.
2. Click **More** and select **Apply Zone Template**, the **Import Zone Template** dialog box appears.

3. From the **Select a Zone template** drop-down, select the template.
4. Click **OK**, a confirmation message appears asking to apply the zone template to the AP zone.
5. Click **Yes**. The zone template was applied successfully.

   You have completed applying zone template to the AP zone.

Changing the AP Firmware Version of the Zone

The controller supports multiple firmware versions. You can manually upgrade or downgrade the AP firmware version of the zone.

Complete the following steps to change the AP firmware version of the zone.

1. From the **Access Point** page, locate a zone for which you want to upgrade the AP firmware version.

   NOTE
   To upgrade multiple zones, click the **Zone** view mode and select the zones by holding down the Ctrl key and clicking each of the zones.

2. Click **More** and select **Change AP Firmware**. The **Change AP Firmware** dialog box displays the current AP firmware version.
3. Select the firmware version you need. If you upgrade to a new firmware version, a backup configuration file will be created. You can use this backup file to downgrade to the original firmware version.

   NOTE
   If the multiple zones do not have the same supported firmware version, the dialog box displays the following message:`These Zones do not have same supported AP firmware available for upgrade/downgrade.`

4. Click **Yes**, and a confirmation message is displayed stating that the firmware version was updated successfully.

   NOTE
   If any zone fails to upgrade, a dialog box displays to download an error CSV list.

5. Click **OK**. You have completed changing the AP firmware version of the zone.

Switch Over Managed APs and External DPs

Switchover helps move APs / external DPs between clusters that are not confined to cluster, which enable cluster redundancy. For normal clusters you can switchover APs regardless of staging zone with firmware version 5.0 or later and external DPs with version 5.1 or later. For a standby cluster in cluster redundancy, APs in Staging Zone can only be moved to another cluster by switchover. You can switch over per AP or APs per Zone. However, you can switch over only per data plane.
Switch Over APs (per Zone)

To switch over APs per zone:

1. From the Access Points page, select the Zone.
2. Click **More** and select **Switch Over Clusters** . The **Switchover Cluster** dialog appears.
3. Choose the Target Cluster:
   - Predefined Destination: Available only when "Active-Active" mode cluster redundancy is enabled. Choose the **Cluster Name** of the switchover target from the list of target active clusters. The Control IPv4 List and Control IPv6 List is displayed.
   - Custom Destination: Enter the **Control IP/FQDN** of the switchover target cluster .
4. To delete the AP record after triggering a switchover, enable the **Delete selected Access Point after switchover** option.

5. Click **OK**, you have set all APs to disconnect from current cluster then connect to target cluster.

Switch Over APs (per AP)

To switch over per AP:

1. From the Access Points page, navigate the Zone and select the AP from the list.
2. Click **More** and select **Switch Over Clusters** . The **Specify Destination cluster** dialog appears.
3. Enter the **Control IP/FQDN** of the switchover target cluster.
4. Click **OK**, a confirmation dialog appears.
5. Click **OK** to confirm. You have set the AP to disconnect from current cluster then connect to target cluster.

Switch Over Data Planes (per data plane)

You can switch over external data planes.

To switch over external data planes:

1. Go to **System** > **Cluster**. From the Data Plane section, select the vSZ-D from the list.
2. Click **More** and select **Switch Over Clusters** . The **Switchover Cluster** dialog appears.
3. Choose the Target Cluster:
   - Predefined Destination: Available only when "Active-Active" mode cluster redundancy is enabled. Choose the **Cluster Name** of the switchover target from the list of target active clusters. The Control IPv4 List and Control IPv6 List is displayed.
   - Custom Destination: Enter the **Control IP/FQDN** of the switchover target cluster .
4. To delete the external data planes record after triggering a switchover, enable the **Delete selected Data Plane after switchover** option.
5. Click **OK**, you have set the external data plane to disconnect from current cluster then connect to target cluster.

Triggering a Preferred Node

You can trigger an AP that belongs to the current zone force go to their preferred node. For this, you must enable Node affinity, which gives AP the priority of preferred nodes.

Follow these steps to trigger a node:

> **NOTE**
> You must enable node affinity before triggering nodes.

1. From the Access Points page, locate the zone.
2. Click **More** and select **Trigger Preferred Node**, a confirmation stating that the node has been triggered appears.
3. Click **OK**. You have triggered the preferred node for the AP.

Rehoming Managed APs and Data Planes

Rehoming is the process of returning the APs and external data planes that have failed over to the standby cluster back to their original cluster (once it becomes available). Rehoming must be done manually. APs and external data planes that have failed over will continue to be managed by the failover cluster until you rehome them.

> **NOTE**
> You can rehome managed APs and external data planes, only in a cluster redundancy environment. When APs or external data planes of a certain active cluster failover to a standby cluster, you must manually restore them to the original cluster, once the active cluster is fixed and back to service.

Rehoming APs or external data planes must be done on a per-cluster basis. Follow these steps to rehome managed APs to the original cluster:

1. From the **Access Points** page, select the **System** to activate rehome operation.
2. Click **More** and select **Rehome Active Clusters**.

   A confirmation dialog box appears.
3. Click Yes, you have set all APs in the standby cluster to rehome to the active cluster to which they were previously. connected

Viewing Modes

You can view System, Zone, and AP Group-level information by selecting one of the following **View Mode** options:

- **List**—Displays the list of all APs irrespective of the Zone or Group they belong.
- **Group**—Displays the list of APs in a hiearchy format. The is the default viewing mode.
- **Mesh**—Lists AP details.
- **Map**—Displays the location map of the APs.
- **Zone**—Lists zone details. There will be 10,000 zones in a system.

  NOTE

  You can also edit, clone or delete a zone by selecting the options Configure , Clone  or Delete  respectively from the Access Points page.

AP Status

The real-time status of the Access Points are classified as follows:

The status of Access Points can be one of the following:

-  **Online**—Number of Access Points that are online.
-  **Flagged**—Number of Access Points that are flagged.
-  **Offline**—Number of Access Points that are offline.

  NOTE
  APs that exceed their health threshold and that require your attention are flagged. See Understanding Cluster and AP Health Icons on page 39.

Configuring Access Points

Once you have created registration rules and the AP zones to which joining access points can be assigned automatically, access points will be able to join or register with the controller automatically.

After an access point registers successfully with the controller, you can update its configuration by completing the following steps.

1. From the list, select the AP that you want to configure and click **Configure**. The **Edit AP** page is displayed.
2. Edit the parameters as explained in Table 49.
3. Click **OK**.

NOTE
Select the **Override** check box if you want to configure new settings.

TABLE 49 Access Point Edit Parameters

Field	Description	Your Action
AP Configuration > General Options		
AP Name	Indicates the name of the AP.	Enter a name.
Description	Gives a short description of the AP.	Enter a short description.
Location	Indicates a generic location.	Select the check box and enter the location.
Location Additional Information	Indicates a specific location.	Select the check box and enter the location.
GPS Coordinates	Indicates the geographical location.	Select the option. For the Manual option, enter the following details: • **Latitude** • **Longitude** • **Altitude**
User Location Information	Indicates the demographic information.	Enter the **Area Code** and **Cell Identifier**.
AP Admin Logon	Indicates the administrator logon credentials.	Select the check box and enter the **Logon ID** and **Password**.
AP Configuration > Radio Options		
Dual-5G Mode	Enables third radio operator in 2.4 GHz, Lower 5 GHz, and Upper 5 GHz. By default, the **Dual-5G Mode** is enabled. In the enabled mode, radio-0 will be on 2.4GHz band, radio-1 will be on 5G Lower band and radio-2 will be on 5G Upper band. • 5G Lower BAND : UNII-1, UNII-2A • 5G Upper BAND : UNII-2C, UNII-3 In the disabled mode, the radio-0 will be on 2.4GHz band, radio-1 will be on 5G band and radio-2 will be on 6G band. This also depends on the country code.	Select or keep the default **Dual-5G Mode** option.
AP Configuration > Band/Spectrum Configuration > 2.4 GHz		
Channelization	Indicates the channel width.	Set the channel width used during transmission to either 20 or 40 (MHz), or select Auto to set it automatically.
Channel	Indicates the channel to use.	Select one of the options: Auto, 1, 6 or 11.
Auto Cell Sizing	Enables the AP to share information on interference seen by each other and dynamically adjust their radio Tx power and Rx parameters to minimize interference. Enabling this option disables the TX Power Adjustment configuration. **NOTE** Ensure that Background Scan is enabled.	Select the option.

TABLE 49 Access Point Edit Parameters (continued)

Field	Description	Your Action
TX Power Adjustment	Allows to manually configure the transmit power on the 2.4 GHz radio. By default, the TX power is set to Full on the 2.4 GHz radio. **NOTE** If you choose Min, the transmit power is set to 0dBm (1mW) per chain for 11n APs, and 2dBm per chain for 11ac APs. If you choose Max, the transmit power is set to the maximum allowable value according to the AP's capability and the operating country's regulations.	Select the preferred TX power.
Background Scan	Allows the AP radio to scan other channels in the band for accessing channel health and capacity, detecting rogue devices, optimizing and mainting mesh links and to discover AP neighbors.	Enter the duration in seconds. Range: 1 through 65535.
Auto Channel Selection	Automatically adjusts the channel using the ChannelFly option.	Select the required option. For **ChannelFly**, set the **Channel Change Frequency** and **Full Optimization Period**.
AP Configuration > **Band/Spectrum Configuration** > **5 GHz**		
Channelization	Indicates the channel width.	Set the channel width used during transmission: Auto, 20, 40, 80 and 160.
Channel	Indicates the channel to use.	Select the required options for the Indoor and Outdoor APs.
Secondary Channel	Indicates the secondary channel to used.	By default, the Indoor and Outdoor option is set to Auto.
Allow DFS Channels	Allows ZoneFlex APs to use DFS channels.	Click to enable the option.
Allow Channel 144	Provides channel 140 and 144 support for 11ac and 11ax APs. Enabling this option supports 20 MHz, 40 MHz, or 80 MHz channel modes. The 160 MHz mode is supported if the AP supports this mode. Disabling this option provides Channel 140 support only to 20 MHz mode. **NOTE** This option is available for selection only if you enable the **DFS Channels** option. **NOTE** This feature is currently supported only in the United States.	Click to enable the option.
Allow Indoor Channels	Allows outdoor APs to use channels regulated as for indoor use only.	Click to enable the option.
Auto Cell Sizing	Enables the AP to share information on interference seen by each other and dynamically adjust their radio Tx power and Rx parameters to minimize interference. Enabling this option disables the TX Power Adjustment configuration. **NOTE** Ensure that Background Scan is enabled.	Select the option.

TABLE 49 Access Point Edit Parameters (continued)

Field	Description	Your Action
TX Power Adjustment	Allows to manually configure the transmit power on the 5 GHz radio. By default, the TX power is set to Full on the 5 GHz radio. **NOTE** If you choose Min, the transmit power is set to 0dBm (1mW) per chain for 11n APs, and 2dBm per chain for 11ac APs. If you choose Max, the transmit power is set to the maximum allowable value according to the AP's capability and the operating country's regulations.	Select the preferred TX power.
Background Scan	Allows the AP radio to scan other channels in the band for accessing channel health and capacity, detecting rogue devices, optimizing and mainting mesh links and to discover AP neighbors.	Enter the duration in seconds. Range: 1 through 65535.
Auto Channel Selection	Automatically adjusts the channel using the ChannelFly option.	Select the required option. For **ChannelFly**, set the **Channel Change Frequency** and **Full Optimization Period**.
AP Configuration > **Band/Spectrum Configuration** > **6 GHz** **NOTE** This tab is available only if the **Tri-band Dual-5G Mode** option is not enabled.		
Channelization	Indicates the channel width.	Set the channel width used during transmission: Auto, 20, 40, 80 and 160.
Channel	Indicates the channel to use.	Select the required options for the Indoor and Outdoor APs.
Auto Cell Sizing	Enables the AP to share information on interference seen by each other and dynamically adjust their radio Tx power and Rx parameters to minimize interference. Enabling this option disables the TX Power Adjustment configuration. **NOTE** Ensure that Background Scan is enabled.	Select the option.
TX Power Adjustment	Allows to manually configure the transmit power on the 6 GHz radio. By default, the TX power is set to Full on the 6 GHz radio. **NOTE** If you choose Min, the transmit power is set to 0dBm (1mW) per chain for 11n APs, and 2dBm per chain for 11ac APs. If you choose Max, the transmit power is set to the maximum allowable value according to the AP's capability and the operating country's regulations.	Select the preferred TX power.
LPI (Low Power Indoor) mode:	Allows the use of a 4 U-NII bands U-NII-5 to U-NII-8 indoors at a reduced Tx power level.	Enable the option.
Background Scan	Allows the AP radio to scan other channels in the band for accessing channel health and capacity, detecting rogue devices, optimizing and mainting mesh links and to discover AP neighbors.	Enter the duration in seconds. Range: 1 through 65535.

TABLE 49 Access Point Edit Parameters (continued)

Field	Description	Your Action
Auto Channel Selection	Automatically adjusts the channel using the ChannelFly option.	For **ChannelFly**, set the **Channel Change Frequency** and **Full Optimization Period**.
AP Configuration > **Band/Spectrum Configuration** > **Lower 5 GHz**		
Channelization	Indicates the channel width.	Set the channel width used during transmission: Auto, 20, 40, 80 and 160.
Channel	Indicates the channel to use.	Select the required options for the Indoor and Outdoor APs.
Allow DFS Channels	Allows ZoneFlex APs to use DFS channels.	Click to enable the option.
Allow Indoor Channels	Allows outdoor APs to use channels regulated as for indoor use only.	Click to enable the option.
Auto Cell Sizing	Enables the AP to share information on interference seen by each other and dynamically adjust their radio Tx power and Rx parameters to minimize interference. Enabling this option disables the TX Power Adjustment configuration. **NOTE** Ensure that Background Scan is enabled.	Select the option.
TX Power Adjustment	Allows to manually configure the transmit power on the Lower 5 GHz radio. By default, the TX power is set to Full on the Lower 5 GHz radio. **NOTE** If you choose Min, the transmit power is set to 0dBm (1mW) per chain for 11n APs, and 2dBm per chain for 11ac APs. If you choose Max, the transmit power is set to the maximum allowable value according to the AP's capability and the operating country's regulations.	Select the preferred TX power.
Background Scan	Allows the AP radio to scan other channels in the band for accessing channel health and capacity, detecting rogue devices, optimizing and mainting mesh links and to discover AP neighbors.	Enter the duration in seconds. Range: 1 through 65535.
Auto Channel Selection	Automatically adjusts the channel using the ChannelFly option.	Select the required option. For **ChannelFly**, set the **Channel Change Frequency** and **Full Optimization Period**.
AP Configuration > **Band/Spectrum Configuration** > **Upper 5 GHz**		
Channelization	Indicates the channel width.	Set the channel width used during transmission: Auto, 20, 40, 80 and 160.
Channel	Indicates the channel to use.	Select the required options for the Indoor and Outdoor APs.
Allow DFS Channels	Allows ZoneFlex APs to use DFS channels.	Click to enable the option.

TABLE 49 Access Point Edit Parameters (continued)

Field	Description	Your Action
Allow Channel 144	Provides channel 140 and 144 support for 11ac and 11ax APs. Enabling this option supports 20 MHz, 40 MHz, or 80 MHz channel modes. The 160 MHz mode is supported if the AP supports this mode. Disabling this option provides Channel 140 support only to 20 MHz mode. **NOTE** This option is available for selection only if you enable the **DFS Channels** option. **NOTE** This feature is currently supported only in the United States.	Click to enable the option.
Auto Cell Sizing	Enables the AP to share information on interference seen by each other and dynamically adjust their radio Tx power and Rx parameters to minimize interference. Enabling this option disables the TX Power Adjustment configuration. **NOTE** Ensure that Background Scan is enabled.	Select the option.
TX Power Adjustment	Allows to manually configure the transmit power on the Upper 5 GHz radio. By default, the TX power is set to Full on the Upper 5 GHz radio. **NOTE** If you choose Min, the transmit power is set to 0dBm (1mW) per chain for 11n APs, and 2dBm per chain for 11ac APs. If you choose Max, the transmit power is set to the maximum allowable value according to the AP's capability and the operating country's regulations.	Select the preferred TX power.
Background Scan	Allows the AP radio to scan other channels in the band for accessing channel health and capacity, detecting rogue devices, optimizing and mainting mesh links and to discover AP neighbors.	Enter the duration in seconds. Range: 1 through 65535.
Auto Channel Selection	Automatically adjusts the channel using the ChannelFly option.	Select the required option. For **ChannelFly**, set the **Channel Change Frequency** and **Full Optimization Period**.
Configuration > AP GRE Tunnel Options		
Ruckus GRE Forwarding Broadcast	Forwards broadcast traffic from network to tunnel. **NOTE** ARP and DHCP traffic are allowed even if this option disabled	Click **Override** to enable the Ruckus GRE broadcast forwarding option. Click the **Enable Forwarding Broadcast** option to forward the broadcast traffic.
AP Configuration > AP SNMP Options		
Override zone configuration	Allows you to override the existing zone configuration	Select the check box
Enable AP SNMP	Enables you to configure SNMP settings.	Select the check box

TABLE 49 Access Point Edit Parameters (continued)

Field	Description	Your Action
SNMPv2 Agent	Allows you to add users to SNMPv2 Agent.	1. Click **Create** and enter **Community**. 2. Select the required **Privilege**. If you select **Notification** enter the **Target IP**. 3. Click **OK**.
SNMPv3 Agent	Allows you to add users to SNMPv3 Agent.	1. Click **Create** and enter **User**. 2. Select the required **Authentication**. 3. Enter the **Auth Pass Phrase**. 4. Select the **Privacy** option. 5. Select the required **Privilege**. If you select **Notification** select the option **Trap** or **Inform** and enter the **Target IP**. 6. Click **OK**.
AP Configuration > Model Specific Options		
Model Specific Control	Indicates that the model overides the AP settings.	Select the check box.
USB Port	Disables the USB port on the selected AP model.	Select the option. USB ports are enabled by default.
Status LEDs	Disable the status LED on the selected AP model.	Select the option.
LLDP	Enables the Link Layer Discovery Protocol (LLDP) on the selected AP model.	Select the option and enter the following details: • **Advertise Interval**—Enter the duration in seconds. • **Hold Time**—Enter the duration in seconds. • **Enable Management IP TLV**—Select the check box.
PoE Operating Mode	Allows you to operate using PoE mode. For optimal LAG performance, a power mode higher than 802.3at is recommended.	Select the option.
LACP/LAG	Aggregates multiple network interfaces into a single logical or bonded interface. LACP can be enabled only on two-port 11ac wave2 and 11ax APs. A minimum of two ports must be active on AP and switch for LACP/LAG configuration. Enabled on switch ports where the APs ethernet cables are connected increases the bandwidth between the AP and the switch.	Choose the option: • Keep the AP's settings: Retains the current AP settings. • Disabled: Disables bond configuration. • Enabled: Enables bond configuration. Select the **Bond Port Profile** from the drop-down. Refer to Creating a Bond Port Profile on page 488 for more information.
Port Settings	Indicates the port settings. This feature is not available if the LACP/LAG feature is selected.	Select the option and choose the required LAN option.
AP Configuration > Advanced Options		
Network Settings	Determines the network settings.	Select the IPv4 Settings from the following: • **Static**-Enter the **IP Address**, **Network Mask**, **Gateway**, **Primary DNS**, **Secondary DNS**. • **Dynamic** • **Keep the AP's Setting**
Smart Monitor	Indicates AP interval check and retry threshold settings.	Select the required check boxes.
Syslog Options		

TABLE 49 Access Point Edit Parameters (continued)

Field	Description	Your Action
Override zone configuration	Cancels the AP zone configuration that was set previously. **NOTE** The **Enable External syslog server** field will be available for configuration only if this option is selected.	Select the option.
Enable External syslog server	Enables the controller to send syslog data to the syslog server on the network.	Select the option.

TABLE 49 Access Point Edit Parameters (continued)

Field	Description	Your Action
Config Type	Allows to customize or select an external syslog server profile.	Select the option: • Custom: Configure the details for the AP to send syslog messages to syslog server. **NOTE** The IP address format that you enter here will depend on the AP IP mode that you selected earlier in this procedure. If you selected IPv4 Only, enter an IPv4 address. If you selected IPv6 Only, enter an IPv6 address. – **Primary Server Address**: If the primary server goes to sends syslog messages. › **Port**: enter the syslog port number on the respective servers. › **Portocol**: select between UDP and TCP protocols – **Secondary Server Address**: If the primary server goes down, the AP sends syslog messages to the secondary server as backup. › **Port**: enter the syslog port number on the respective servers. › **Portocol**: select between UDP and TCP protocols – **Event Facility**: Select the facility level that will be used by the syslog message. Options include: Keep Original, Local0 (default), Local1, Local2, Local3, Local4, Local5, Local6, and Local7. – **Priority**: Select the lowest priority level for which events will be sent to the syslog server. For example, to only receive syslog messages for events with the warning (and higher) priority, select **Warning**. To receive syslog messages for all events, select **All**. – **Send Logs**: Select the type of messages to be sent to the syslog server. For example, General Logs, Client Logs or All Logs. • AP External Syslog Profile: Select the profile from the drop-down or click Add to create a new profile. Refer to Creating an External Syslog Server Profile on page 532 for more information.

TABLE 49 Access Point Edit Parameters (continued)

Field	Description	Your Action
Hotspot 2.0 version Profile	Indicates the hotspot profile that you want to assign to the group.	Select the required option or click **Create** and update the following details: • Enter the **Name**. • Enter the **Description**. • Enter the **Venue Names**. • Select the **Venue Category**. • Select the **Type**. • Enter the **WLAN Metrics**.
AP Management VLAN	Indicates the AP management VLAN settings.	Select the check box and choose the option. **ATTENTION** For standalone APs, set the AP ethernet port to trunk before changing the AP Management VLAN settings.
Client Admission Control	Indicates the load thresholds on the AP at which it will stop accepting new clients.	Select the check boxes and update the following details: • **Min Client Count** • **Max Radio Load** • **Min Client Throughput**
Rogue Classification Policy	Indicates the parameters used to classify rogue APs. This option is available only if you enable the **Rogue AP Detection**option.	Select the options for rogue classification policy: • Enable the **Override** option and enter the **Report RSSI Threshold**. Range: **0** through **100**. • Enable the **Overide** option to override the aggressiveness of protecting the network and choose one of the following: – **Aggressive** – **Auto** – **Conservative** • Enable the **Override** option and enter the **Jamming Threshold** in percentage.
Recovery SSID	Allows you to enable or disable the Recovery(Island) SSID broadcast on the controller.	Enable **Recovery SSID Broadcast**
Direct Multicast	Indicates whether multicast traffic is sent from a wired device, wireless device or from the network.	Select one or more of the following: • **Multicast Traffic from Wired Client** • **Multicast Traffic from Wireless Client** • **Multicast Traffic from Network**
Test Speed	Measures the connection performance of the AP. The option must be enabled to run the SpeedFlex traffic test between wireless clients and the AP.	Enable the option.
Swap Configuration		
Add Swap-In AP	Allows to swap APs.	Select the check box and enter the **Swap-in AP MAC** details.

NOTE

- You can also move the location of an AP or delete an AP. To do so, select the AP from the list and click **Move** or **Delete** as required.
- A maximum of 50 APs in a specific group can be moved from one zone to another by using an API command. APs that fail to move return and error code indicating the failure and the AP count. Select **Adminstration** > **Help** > **REST API** to refer to the API command. In the *SmartZone 300 Public API Reference Guide*, refer to **Access Point Configuration** > **Move multiple APs**.

Configuring the M510 AP

The M510 Access Point (AP) is an 802.11ac Wave 2 access point with LTE backhaul.

SmartZone supports the M510 AP with cellular backhaul connections. Model-specific configurations including settings for cellular radio allow you to configure the AP behavior.

1. From the list, select the M510 AP and click **Configure**. The **Edit AP** is displayed.
2. Edit the parameters as explained in the following table.

TABLE 50 Access Point Edit Parameters

Field	Description	Your Action
AP Configuration > **General Options**		
AP Name	Indicates the name of the AP.	Enter a name.
Description	Gives a short description of the AP.	Enter a short description.
Location	Indicates a generic location.	Select the check box and enter the location.
Location Additional Information	Indicates a specific location.	Select the check box and enter the location.
GPS Coordinates	Indicates the geographical location.	Select the option. For the Manual option, enter the following details: • **Latitude** • **Longitude** • **Altitude**
User Location Information	Indicates the demographic information.	Enter the **Area Code** and **Cell Identifier**.
AP Admin Logon	Indicates the administrator logon credentials. For the default zone, the SZ cluster name is used as the default logon ID and password.	Select the check box and enter the **Logon ID** and **Password**.
AP Configuration > **Radio Options**		
Channel Range (2.4G)	Overrides the 2.4 GHz channel range that has been configured for the zone to which this AP group belongs.	Select the **Select Channel Range (2.4G)** check boxes for the channels on which you want the 2.4 GHz radios of managed APs to operate. Channel options include channels 1 through 11. By default, all channels are selected.
Channel Range (5G)	Overrides the 5 GHz channel range that has been configured for the zone to which this AP group belongs.	Select the **Select Channel Range (5G)** check boxes for the channels on which you want the 5 GHz radios of managed APs to operate.

TABLE 50 Access Point Edit Parameters (continued)

Field	Description	Your Action
Radio Options b/g/n (2.4 GHz)	Indicates the 2.4 GHz radio option.	Select the following options: • **Channelization**: Set the channel width used during transmission to either **20** or **40** (MHz), or select **Auto** to set it automatically. • **Channel**: Select the channel to use for the b/g/n (2.4 GHz) radio, or select **Auto** to set it automatically. • **Auto cell sizing**: Select this option to enable APs to share information on interference seen by each other and dynamically adjust their radio Tx power and Rx parameters to minimize interference. Selecting the **Enable** option disables the **TX Power Adjustment** configuration. • **TX Power Adjustment**: Select the required option. **NOTE** If you choose **Min**, the transmit power is set to 0 dBm (1 mW) per chain for 11n APs, and 2 dBm per chain for 11ac APs. If you choose **Max**, the transmit power is set to the maximum allowable value according to the capability of the AP and the regulations of the operating country.. • **WLAN Group**: Select the WLAN group to which this AP belongs. • **WLAN Services**: Select the check box to enable WLAN services in this radio.

TABLE 50 Access Point Edit Parameters (continued)

Field	Description	Your Action
Radio Options a/n/ac (5 GHz)	Indicates the radio option 5 GHz configurations.	Select the following options: • **Channelization**: Set the channel width used during transmission to **20**, **40**, or **80** (MHz), or select **Auto** to set it automatically. • **Channel**: Select the channel to use for the a/n/c (5 GHz) radio, or select **Auto** to set it automatically. • **Auto cell sizing**: Select this option to enable APs to share information on interference seen by each other and dynamically adjust their radio Tx power and Rx parameters to minimize interference. Selecting the **Enable** option disables the **TX Power Adjustment** configuration. • **TX Power Adjustment**: Select the required option. **NOTE** If you choose **Min**, the transmit power is set to 0 dBm (1 mW) per chain for 11n APs, and 2 dBm per chain for 11ac APs. If you choose **Max**, the transmit power is set to the maximum allowable value according to the capability of the AP and the regulations of the operation country. • **WLAN Group**: Select the WLAN group to which this AP belongs. • **WLAN Services**: Select the check box to enable WLAN services in this radio.
AP Configuration > AP SNMP Options		
Override zone configuration	Overrides the existing zone configuration	Select the check box.
Enable AP SNMP	Configures SNMP settings.	Select the check box.
SNMPv2 Agent	Adds users to the SNMPv2 Agent.	Click **Create** and enter **Community**. a. Select the required **Privilege**. If you select **Notification**, enter the **Target IP**. b. Click **OK**.
SNMPv3 Agent	Adds users to the SNMPv3 Agent.	Click **Create** and enter **User**. a. Select the required **Authentication**. b. Enter the **Auth Pass Phrase**. c. Select the **Privacy** option. d. Select the required **Privilege**. If you select **Notification**, select the option **Trap** or **Inform** and enter the **Target IP**. e. Click **OK**.
AP Configuration > Model Specific Options		
Model Specific Control	Indicates that the model overides the AP settings.	Select the check box.

TABLE 50 Access Point Edit Parameters (continued)

Field	Description	Your Action
USB Port	Disables the USB port on the selected AP model.	Select the option. USB ports are enabled by default.
Status LEDs	Disables the status LED on the selected AP model.	Select the option.
LLDP	Enables the Link Layer Discovery Protocol (LLDP) on the selected AP model.	Select the option and enter the following details: • **Advertise Interval**: Enter the duration in seconds. • **Hold Time**: Enter the duration in seconds. • **Enable Management IP TLV**: Select the check box.
Cellular Radio Settings	Indicates the settings you can configure for the cellular connection.	Select the following options: • **APN for Primary SIM**: Enter the APN name for the primary SIM. If you choose to keep it blank, the controller sets NULL for APN. If you are not sure about the APN name, enter **defaultapn**. **NOTE** For defaultapn, the AP internally searches for an appropriate apn name and sets it in the rpm key through the LTE chipset. • **APN for Secondary SIM**: Enter the APN name for the secondary SIM. If you choose to keep it blank, the controller sets NULL for APN. If you are not sure about the APN name, then enter **defaultapn**. **NOTE** For defaultapn, the AP internally searches for an appropriate apn name and sets it in the rpm key through the LTE chipset. • **SIM Card Usage**: Select one or both SIM cards to prioritize SIM card usage. • **3G/4G Selection**: Select either 3G or 4G internet speed. • **Data Roaming**: Enable or disable data roaming. • **WAN connection**: The AP can be connected to the WAN either through the Ethernet or cellular data, and only from the primary SIM card. The following options are available: – Ethernet primary with cellular failover (the AP is connected to the Ethernet if LTE fails) – Cellular primary with Ethernet failover (the AP is connected to LTE if the Ethernet connection fails) – Ethernet only – Cellular only

TABLE 50 Access Point Edit Parameters (continued)

Field	Description	Your Action
PoE Operating Mode	Allows you to operate using PoE mode.	Select the option.
Port Settings	Indicates the port settings.	Select the option and choose the required LAN option.
AP Configuration > Advanced Options		
Network Settings	Determines the network settings.	Select the IPv4 settings from the following options: • **Static**: Enter the **IP Address**, **Network Mask**, **Gateway**, **Primary DNS**, and **Secondary DNS**. • **Dynamic** • **Keep the AP's Setting**
Smart Monitor	Indicates the AP interval check and retry threshold settings.	Select the required check boxes.
Syslog Options	Determines if external syslog server settings are applicable.	Select the required check boxes. For the **Enable external syslog server** option, update the following information: • **Server Address** • **Port** • **Facility for Event** • **Priority**
Hotspot 2.0 version Profile	Indicates the hotspot profile that you want to assign to the group.	Select the required option or click **Create** and update the following details: • Enter the **Name**. • Enter the **Description**. • Enter the **Venue Names**. • Select the **Venue Category**. • Select the **Type**. • Enter the **WLAN Metrics**.
AP Management VLAN	Indicates the AP management VLAN settings.	Select the check box and choose the option. **ATTENTION** For standalone APs, set the AP Ethernet port to trunk before changing the AP management VLAN settings.
Auto Channel Selection	Indicates auto-channel settings.	Select the check box and choose the option.
Client Admission Control	Indicates the load thresholds on the AP at which it will stop accepting new clients.	Select the check boxes and update the following details: • **Min Client Count** • **Max Radio Load** • **Min Client Throughput**

TABLE 50 Access Point Edit Parameters (continued)

Field	Description	Your Action
Protection Mode	Indicates the protection mode settings for the AP.	You can override the protection mode settings at 2.4 GHz, and select one of the following options: • **None** • **RTS/CTS (Request to Send/Clear to Send flow control mechanism that allows receiver and the transmitter to alert each other to their state)** • **CTS Only**
Venue Code	Indicates the venue code.	You can choose to override this setting and enter the code in the field provided.
Recovery SSID	Indicates the recovery SSID.	Select the **Enable Recovery SSID Broadcast** option for the AP to broadcast the SSID so it can be visible during discovery.
Direct Multicast	Indicates the direction in which multicast traffic can be sent.	Configure the AP to multicast traffic from wired clients, wireless clients, and from the network.
Swap Configuration		
Add Swap-In AP	Allows swapping of APs.	Select the check box and enter the **Swap-in AP MAC** details.

3. Click **OK**.

NOTE
You can also move the location of an AP or delete an AP. To do so, select the AP from the list and click **Move** or **Delete** as required.

NOTE
Select the **Override** check box if you want to configure new settings.

Managing Access Points

Overview of Access Point Configuration

Once you have created registration rules and the AP zones to which joining access points can be assigned automatically, access points will be able to join or register with the controller automatically.

Whenever a new AP connects to the controller and before it gets approval, the AP registration is moved to "Pending" state determining there is communication between the AP and controller. Every time an unapproved AP attempts to register, a "AP reject" event is generated and can be exported to syslog server if there is one configured.

NOTE
AP reject event is generated only once since subsequent events are suppressed to reduce resource usage.

After an access point registers successfully with the controller, you can update its configuration by following the steps described in this section.

Viewing Managed Access Points

After an access point registers successfully with the controller, it appears on the Access Points page, along with other managed access points.

Follow these steps to view a list of managed access points.

1. Click **Access Points**, a list of access points that are being managed by the controller appears on the Access Points page. These are all the access points that belong to all management domains.

   The list of managed access points displays details about each access point, including its:

   - AP MAC address
   - AP name
   - Zone (AP zone)
   - Model (AP model)
   - AP firmware
   - IP address (internal IP address)
   - External IP address
   - Provision Method
   - Provision State
   - Administrative Status
   - Status
   - Configuration Status
   - Registered On (date the access point joined the controller network)
   - Registration Details
   - Registration State
   - Actions (actions that you can perform)

     NOTE
     By default, the Access Points page displays 20 access points per page (although you have the option to display up to 250 access points per page). If the controller is managing more than 20 access points, the pagination links at the bottom of the page are active. Click these pagination links to view the succeeding pages on which the remaining access points are listed.

2. To view access points that belong to a particular administration domain, click the name of the administration domain in the domain tree (on the sidebar).

   The page refreshes, and then displays all access points that belong to that management domain.

BSS Coloring

Configuring BSS Coloring for a Zone

BSS Coloring intelligently color-codes (or marks) shared frequencies with a number that is included within the PHY header that is passed between the device and the network. These color codes allow access points to decide if the simultaneous use of spectrum is permissible because the channel is only busy and unavailable to use when the same color is detected. This helps mitigate overlapping Basic Service Set (OBSS) issues. In turn, this enables a network to more effectively and concurrently transmit data to multiple devices in congested areas.

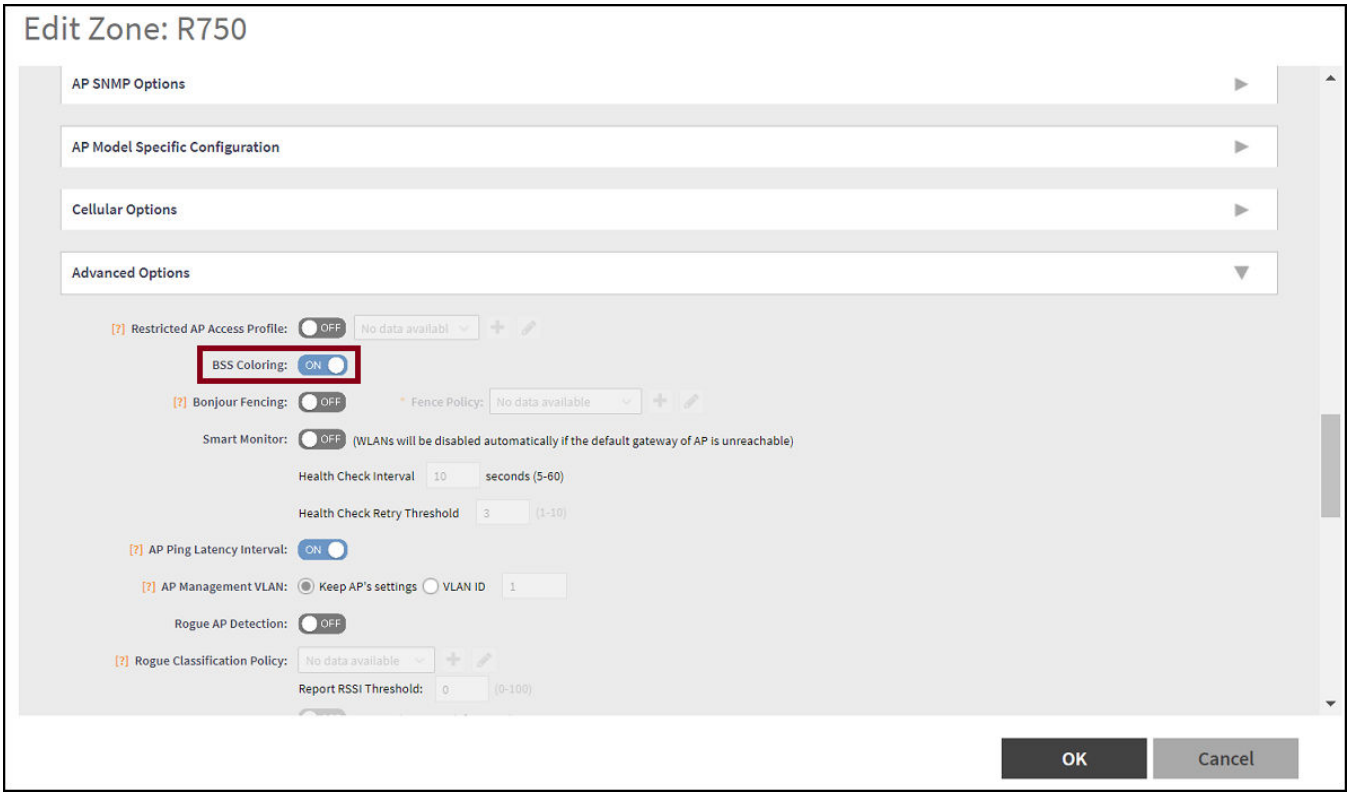
Complete the following steps to configure BSS Coloring for a zone.

1. Go to **Network** > **Access Points**.

2. Select a **zone**, and click the **Edit** option.

   The **Configure Zone** page is displayed.

   FIGURE 62 Configuring BSS Coloring in Zone Configuration



3. For **BSS Coloring**, enable BSS Coloring by setting the switch to ON.

   NOTE
   The BSS color value is automatically selected.

4. Click **OK** to complete the configuration.

Configuring BSS Coloring for an Individual Access Point

Complete the following steps to configure BSS Coloring for individual access points.

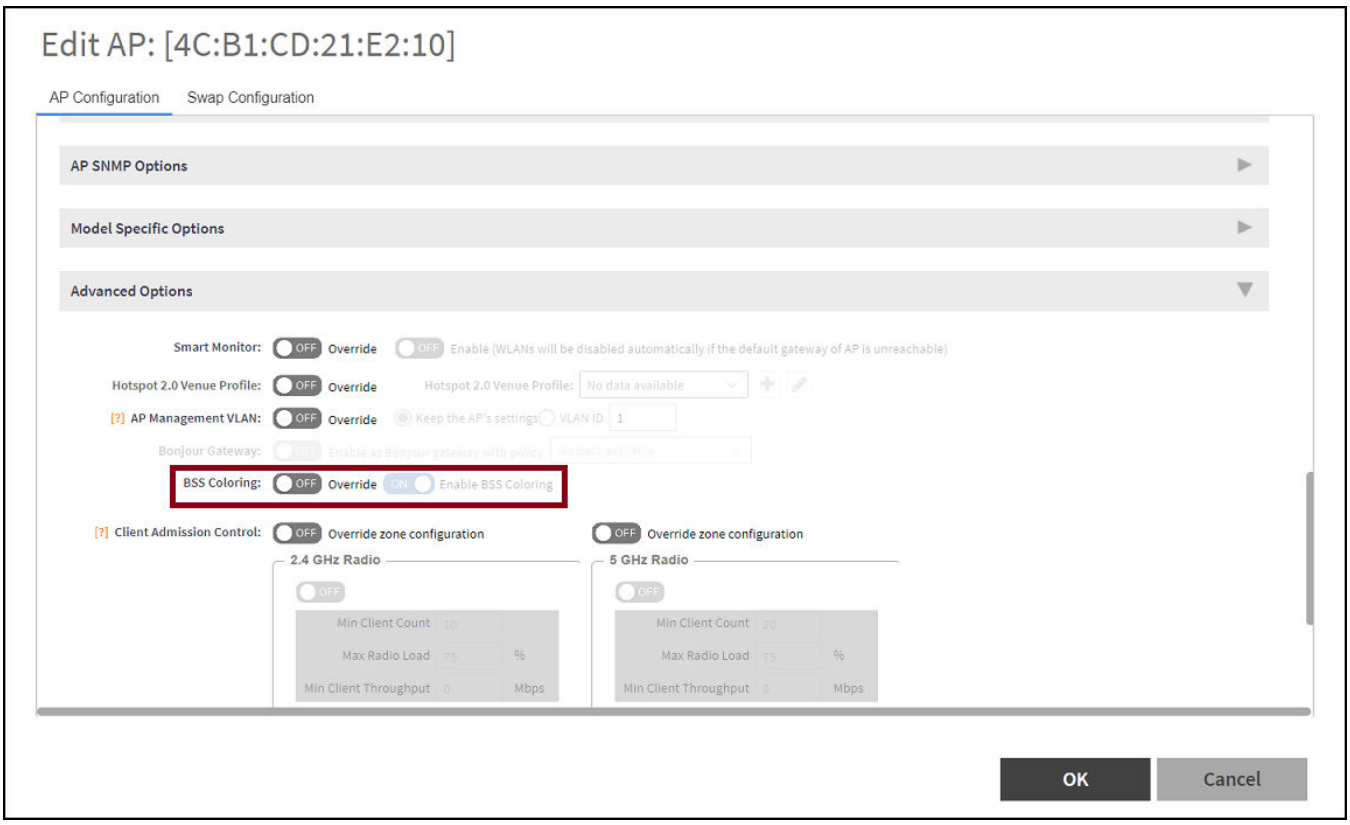
NOTE
BSS Coloring for individual access points is available for 802.11ax APs only.

1. Go to **Network** > **Access Points**.
2. Expand the **zone**, and select the intended access point.

3. Click **Configure**.

   The **AP Configuration** page is displayed.

FIGURE 63 Configuring BSS Coloring for an Individual Access Point Configuration



4. For **BSS Coloring**, enable BSS Coloring by setting the switch to ON.

   NOTE
   If the **Override** option is set to ON, the AP uses BSS Coloring configuration and ignores the zone or AP group configuration. If it is set to OFF, BSS Coloring uses the zone or AP group configuration.

5. Click **OK** to complete the configuration.

Configuring BSS Coloring within an AP Group

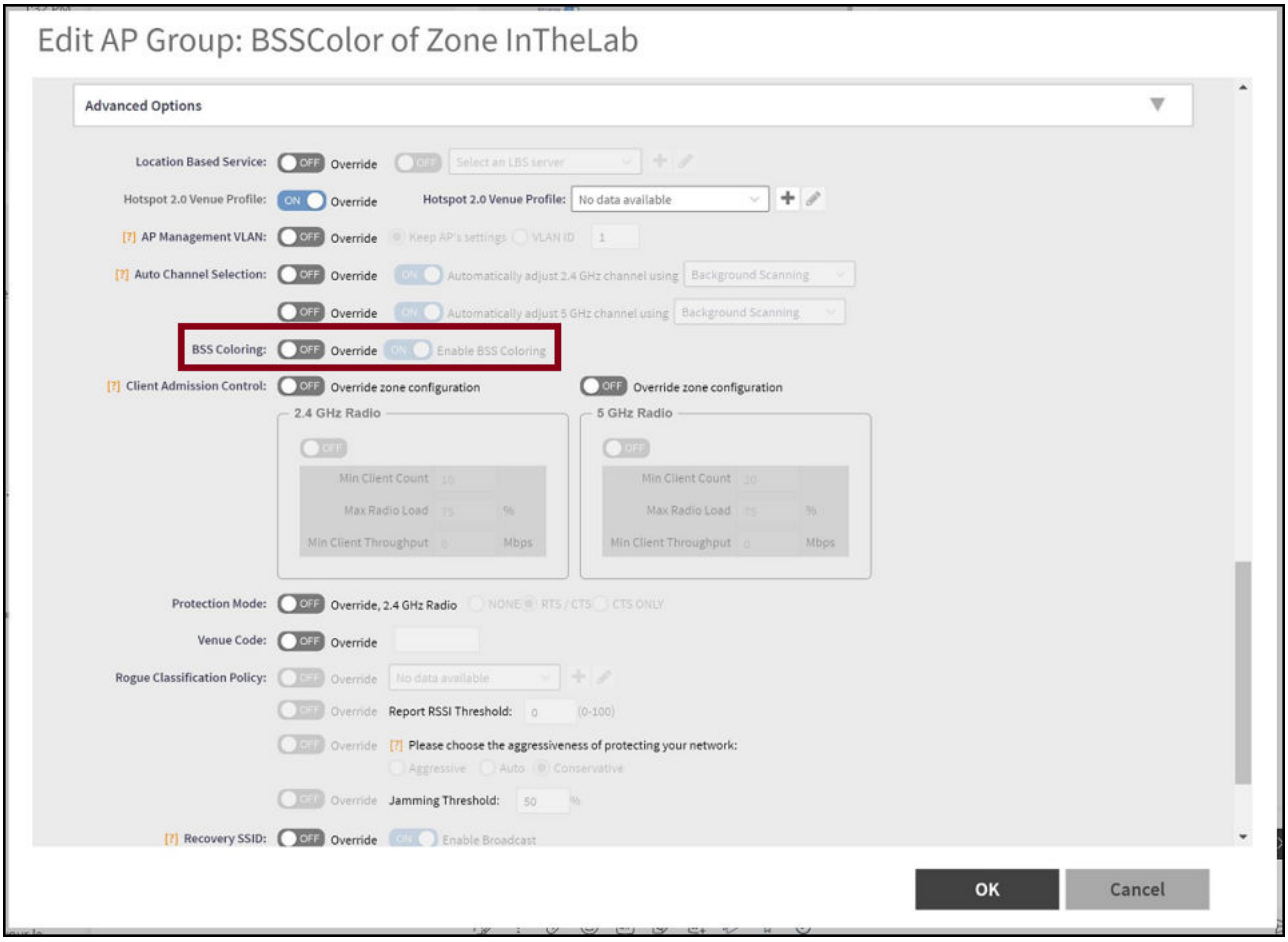
Complete the followings steps to configure the BSS Coloring within an AP group.

1. Go to **Network** > **Access Points**.

2. Expand the zone, select the AP group, and click the Edit option.

   The **AP Group Configure** page is displayed.

   FIGURE 64 Configuring BSS Coloring within an AP Group



3. For **BSS Coloring**, enable BSS Coloring by setting the switch to ON.

   NOTE
   If the **Override** option is set to ON, the AP group configuration of BSS Coloring takes precedence over zone configuration. If it is set to OFF, BSS Coloring uses the zone.

Downloading the Support Log from an Access Point

If you are experiencing issues with an access point, RUCKUS Support Team may request you to download the support log from the access point.

The support log contains important technical information that may be help RUCKUS Support Team troubleshoot the issue with the access point. Follow these steps to download the support log from an access point.

To download a support log from an AP:

- Select the AP and click **More** > **Download Support Log**. The following message appears: Do you want to open or save **SupportLog_{random-string}.log**.

Save the file and use a text editor (for example, Notepad) to view the contents of the text file. Send the support log file to RUCKUS Support Team, along with your support request.

Debugging an AP Failure

When an AP fails and reboots, himem logs pertaining to the failure are saved in the AP. These logs can be retrieved from the AP and the controller. From the AP support log, the **Himem Ring Buffer 0** section contains the himem rb0 logs. Log files can be exported to an external server for troubleshooting and debugging issues.

Complete the following steps to retrieve the himem logs from the controller.

1. From the main menu, go to **Network**, and click **Access Point**.

   The **Access Points** page is displayed.
2. Select an AP from the list.
3. Click **More** and select **Trigger AP binary log**.
4. When the **Trigger AP binary log successfully** dialog box is displayed, click **OK**.
5. From the left pane, select **Diagnostics** > **Application Logs**.

   The **Application Logs** page is displayed.
6. From the **# of Logs** column, select the log corresponding to **AP Diagnostic Information** from the **Application Name** column.
7. Select the ap-dump-xxxxx.tar file to download it
8. Extract the file to get the himem rb0 logs .gz files.

NOTE
The most recent five himem log files can be viewed.

Provisioning and Swapping Access Points

The controller supports the provisioning and swapping of access points.

As an administrator you can:

- Upload a file containing list of AP and the pre-provisioned configuration data for each AP. The controller processes the file and provides details on regarding the import results (including a list of failed APs and failure reasons).
- Modify or delete pre-provisioning data if AP does not connect to the controller
- Monitor the status and stage of the pre-provisioned APs
- Manually lock or unlock APs
- Upload a file containing list of AP pairs for swapping. The controller processes the file and provide the detailed import result (including a list of failed APs and failure reasons).
- Manually enter the AP swap pair
- Delete the swap configuration if AP fails to contact the controller
- Monitor the status and stage of the swapping AP pairs
- Manually swap the APs

Options for Provisioning and Swapping APs

The controller supports the provisioning and swapping of access points.

Use the following buttons on the AP List page to perform the AP provisioning and swapping.

- **Import Batch Provisioning APs**: Select this option to import the provisioning file. The controller displays the import results. Any errors that occur during the import process will be listed by the controller.
- **Export All Batch Provisioning APs**: Select this option to download a CSV file that lists all APs that have been provisioned. The exported CSV contains the following information:
  - AP MAC Address
  - Zone Name
  - Model
  - AP Name
  - Description
  - Location
  - GPS Coordinates
  - Logon ID
  - Password
  - Administrative State
  - IP Address
  - Network Mask
  - Gateway
  - Primary DNS
  - Secondary DNS
  - Serial Number
  - IPv6 Address
  - IPv6 Gateway
  - IPv6 Primary DNS
  - IPv6 Secondary DNS

    NOTE
    The exported CSV file for all batch provisioned APs only contains pre-provisioned APs. It does not contain swapping APs or auto discovered APs.
    If no APs have been pre-provisioned, you will still be able to export the CSV file but it will be empty (except for the column titles).

- **Import Swapping APs**: Manually trigger the swapping of two APs by clicking the swap action in the row. You can also edit the pre-provision configuration only if the AP does not connect to the controller. Click the AP MAC address to bring up the configuration edit form, and then select Pre-provision Configuration.
- **Export All Batch Swapping APs**: Select this option to download a CSV file that lists all APs that have been swapped. The exported CSV contains the following information:
  - Swap In AP MAC
  - Swap In AP Model
  - Swap Out AP MAC

    NOTE
    The exported CSV file for batch swapping APs only contains swapping APs. It does not contain pre-provisioned APs or auto discovered APs.

Understanding How Swapping Works

The following table lists how the controller handles swapping by detailing each stage. For example, you have entered swap configuration as Swap In: A and Swap out: B.

TABLE 51 AP swapping stages

Stage	State A	Stage A	State B	Stage B
1. Enter data	Swapping	Not Registered	Approved	Waiting for swap in AP registration
2. AP register	Swapping	Waiting for swapping in	Approved	Waiting for swapping out
3. User swap	Approved	Swapped in	Swapping	Swapped out
4. Second swap	Swapping	Swapped out and waiting for swapping in	Approved	Swapped in and waiting for swapping out

Editing Swap Configuration

The controller supports the swapping or replacement of a managed AP with a new AP of the same model. This feature is useful when you want to avoid service interruption because you need to replace an AP in the field.

By configuring the swap settings, you can easily and automatically export and apply the settings of the old AP to the new AP.

Follow these steps to configure the swap settings of an AP.

1. On the Access Points page, locate the access point whose swap configuration you want to update.
2. Click **Configure**, the Edit AP page appears.
3. Click the **Swap Configuration** tab.
4. Select the **Add Swap-In AP** check box.
5. Enter the **Swap-In AP MAC** address.
6. Click **OK**.

You have completed editing the swap configuration.

Approving Mesh APs

You can approve mesh APs that join the network using wireless connection.

To approve mesh APs:

1. Go to the Access Points page. On the upper-right corner of the page, select the **Mesh** option from **View Mode**.

   The mesh APs are listed. The **Mesh Role** field, displays the status of the APs.

   NOTE
   To view the list of APs pending for approval, click the **Unapproved APs** below the left pane.

2. From the list, select the AP which is not assigned to a Staging or Default Zone and click **Approve**.

   The **Approve Mesh AP** form appears.

3. From the **AP Zone** drop-down, select the zone.
4. In **Last 4 digit of AP S/N**, enter the last four digit serial number of the AP.
5. Click **Approve**, to manually approve the APs that join the network using Zero Touch Mesh (ZTM).

   After approval, Zero Touch Mesh (ZTM) AP changes mesh role to “approved”, and the AP will show up in AP list for waiting AP join.

Monitoring Access Points

When you select an AP from the list, contextual tabs appear at the bottom of the page.

The following table helps you to understand the real-time information about the AP.

TABLE 52 Access Point Monitoring Tabs

Tabs	Description
General	Displays group information
Configuration	Displays group configuration information.
Health	Displays historical health information.
Traffic	Displays historical traffic information.
Alarm	Displays alarm information.
Event	Displays event information.
Clients	Displays client information.
Pool Stats	Displays DHCP pool data.
Stats Counter	Displays AP statistics that can be exported to CSV format.
GPS Location	Displays AP Historical GPS location information on a map **NOTE** For M510 AP, GPS location probe interval must be set to 5.

Additionally, you can select an AP and click **More** to perform the following operations as required:

- **Select ALL** - Selects all the APs in the list.
- **Deselect All**- Clears all selection from the list.
- **Troubleshooting > Client Connection** - Connects to client devices and analyze network connection issues in real-time. See, Troubleshooting Client Connections on page 70
- **Troubleshooting > Spectrum Analysis** - Troubleshoots issues remotely, identify sources of interferences within the network and allow administrators access to the RF health of the network environment. See, Troubleshooting through Spectrum Analysis on page 72
- **Restart** - Restarts an access point remotely from the web interface.
- **Lock** - Disables all WLAN services on the AP and disconnect all wireless users associated with those WLAN services temporarily.
- **Unlock** - Makes all WLAN services available.
- **Import Batch Provisioning APs** - Import the provisioning file. See, Options for Provisioning and Swapping APs on page 162
- **Import Swapping APs** - Manually trigger the swapping of two APs by clicking the swap action in the row. See, Options for Provisioning and Swapping APs on page 162
- **Export All Batch Provisioning APs** Downloads a CSV file that lists all APs that have been provisioned.. See, Options for Provisioning and Swapping APs on page 162
- **Export All Swapping APs** - Downloads a CSV file that lists all APs that have been swapped. See, Options for Provisioning and Swapping APs on page 162
- **Download Support Log** - Downloads support log.
- **Trigger AP Binary Log** - Triggers binary log for the selected AP.
- **Trigger Preferred Node** - Triggers an AP that belongs to the current zone to connect to the preferred node. See Triggering a Preferred Node on page 140.
- **Download CM Support Log** - Downloads Cable Momdem support log.

- **Restart Cable Modem** - Restarts the cable modem. The AP will disconnect from the network for a short period. The AP will disconnect from the network for a short period.
- **Reset Cable Modem** - Resets the cable modem.
- **Reset Cable Modem to Factory Default** - Resets the cable modem to factory default settings.
- **Untag Critical APs** - Stating APs as non-critical. See, Tagging Critical APs on page 54.
- **Swap** - Swaps current AP to swap-in AP. See, Editing Swap Configuration on page 163
- **Switch Over Clusters** - Moves APs between clusters. See Configuring AP Switchover on page 65.
- **Approve** - Approves AP and completes registering. See, Working with AP Registration Rules on page 53.

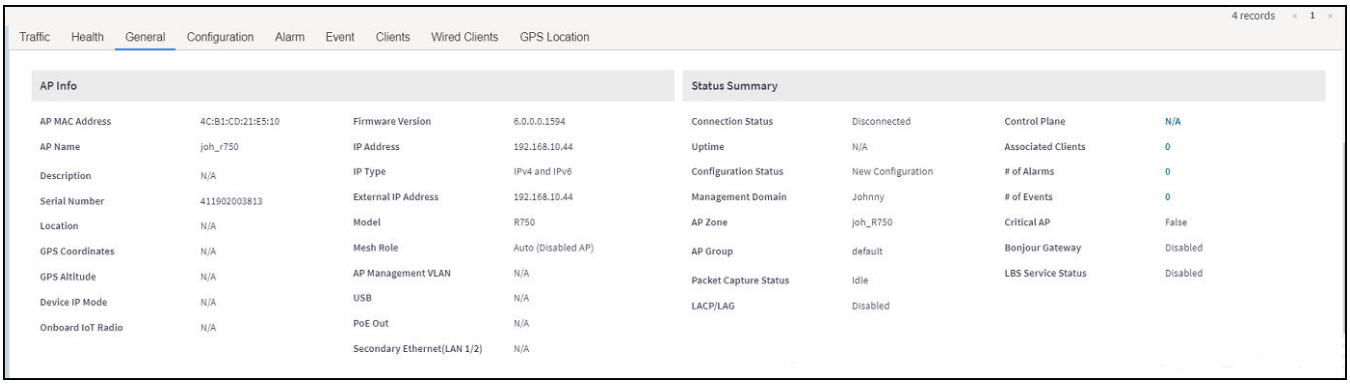
Viewing General AP Information

Complete the following steps to view general AP information.

1. From the **Network** > **Wireless** > **Access Points** page, select an AP.
2. In the **General** tab, scroll to the **AP Info** information.

   You can view information specific to the selected AP.

   FIGURE 65 General AP Information



Viewing Neighbor APs in a Non-Mesh Zone

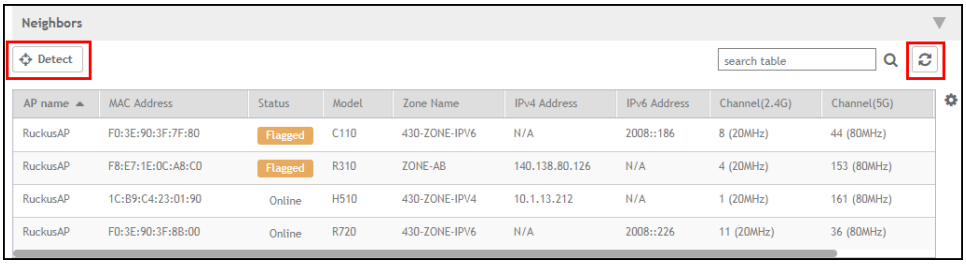
To view neighbor APs in a Non-Mesh zone:

1. From the **Network** > **Wireless** > **Wireless LANs** page, select an AP.

2. Scroll down to the bottom of the page. In the Neighbors area, click **Detect**.

   The list of neighboring APs are displayed in the table.

   FIGURE 66 Neighbor APs for a Non-Mesh Zone



3. To refresh the list, click the Refresh button.

Viewing LLDP Neighbors

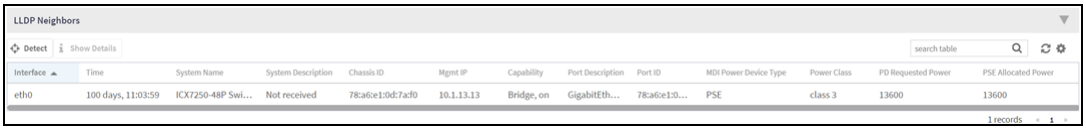
You can view basic information, and detailed information about the LLDP neighbor of an AP form the controller interface.

1. From the **Access Points** page, select an AP from the list.

2. Scroll down to the bottom of the page. In the **LLDP Neighbors** area, click **Detect**.

   The list of neighboring LLDP APs are displayed in the table.

   FIGURE 67 Neighbor LLDP APs for a Non-Mesh Zone

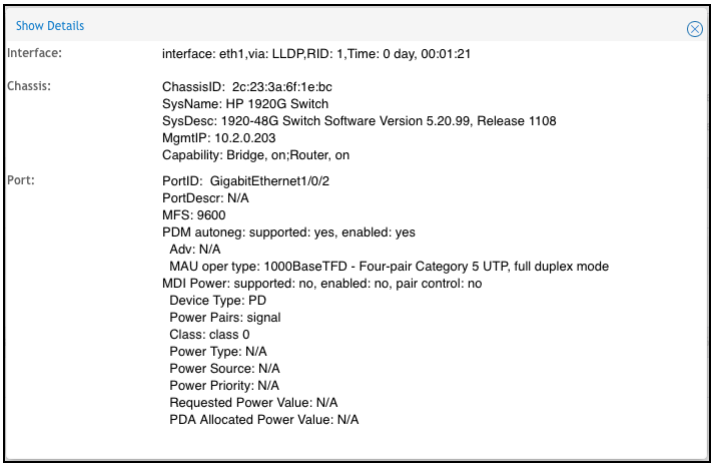


   You can view basic information about the LLDP AP neighbor such as:

   - Interface: displays the interface on the AP from which the LLDP neighbor is detected
   - Time: displays the matching time output in current LLDP command
   - System Name: displays the name of the system such as a switch or router
   - System Description: displays a short description about the system
   - Chassis ID: displays the chassis ID of the system
   - Mgmt IP: displays the management IP address of the LLDP neighbor
   - Capability: displays the capability of the LLDP neighbor such as Bridging or Routing capabilities
   - Port Description: displays the port type and capacity such as Gigabit Ethernet port
   - Port ID: displays the port ID
   - MDI Power Device Type: indicates whether the device is a power sourcing equipment (PSE) or a powered device (PD). PSE is the source of the power, or the device that integrates the power onto the network. PD is the Ethernet device that requires power and is situated on the other end of the cable connected to the PSE.
   - Power Class: displays the power-class of the device ranging from 0 to 4 (IEEE 802.3at power-classes).
   - PD Requested Power: displays power (in watts) requested by the Powered Device
   - PSE Allocated Power: displays power (in watts) allocated by the Power Sourcing Equipment to the Powered Device

3. Click **Show Details** to view detailed information about the LLDP AP neighbor such as the interface, chassis and ports.

   FIGURE 68 Additional LLDP AP Neighbor Details



4. To refresh the list, click the Refresh  button.

Viewing AP Health Indicators

You can monitor the performance and connection failures of an AP from the Health tab page.

Performance

- Latency - It is the measurement of average delay required t successfuly deliver a Wi-Fi frame.
- Airtime Utilization - It is a measurement of airtime usage on the channel measuring the total percentage of airtime usage on the channel.
- Capacity - It is a measuement of potential data throughput based on recent airtime efficiency and the performacne potential of the AP and its currently connected clients.

Connection Failure

- Total - It is a measurement of unsuccessful connectivity attempts by clients.
- Authentication - It's a measurement of client connection attempts that failed at the 802.11 open authentication stage.
- Association - It is a measurement of client connection attempts that failed at the 802.11 association stage, which happens before user/device authentication.
- EAP - It is a measuremmetn of client connection attempts that failed during an EAP exchange.
- RADIUS - It's a measurement of RADIUS exchange failures due to AAA client /server communication.
- DHCP - It's a measurement of failed IP address assignment to client devices.

To customize Health Performance settings:

1. From the Access Points page, select the required AP from the list.
2. Scroll Down and select the **Health** tab.
3. On the **Performance** bar, select the Setting  icon. The **Settings - Performance** pop-up appears. Customize the following:
   - **Show top**: Enter the number of performance failures to be displayed.
   - **Display Channel Change**: Select the required options. For example: **2.4G**, **5G**.
   - **AP**: Choose how the AP details must be displayed. For example: **Name**, **MAC**, **IP**.
4. Click **OK**.

   Performance details of the AP are listed according to the settings.

Viewing AP Traffic Indicators

You can monitor the performance and connection failures of an AP from the Traffic tab page.

You can view:

- Historical or Real Time traffic
- WLAN traffic

Traffic indicators can be filtered based on the following parameters:

- Rate, Packets, Rate
- Total, Downlink-From AP to client, Uplink-From client to AP

To customize Traffic settings:

1. From the Access Points page, select the required AP from the list.

2. Scroll Down and select the **Traffic** tab.
3. On the respective section bar, select the Settings icon. The **Settings - Clients** pop-up appears. Customize the following:
   - **Type**: Choose the Display format. For example: **Chart**, **Table**.
   - **Display Channel Change**: Select the required options. For example: **2.4G**, **5G**.

     NOTE
     This field is available only for the Clients Tab when you select the Display Type as Chart.

   - **AP**: Choose the AP display format. For example: **Name**, **MAC**, **IP**.
4. Click **OK**.

   Performance details of the AP are listed according to the settings.

Configuring AP Switchover

AP switchover is the moving of APs between clusters, and is not confined to clusters that enable cluster redundancy. For normal clusters, you can switchover APs with firmware later or equal to R5.0, regardless of whether it is in the Staging or Non-staging Zone in High-scale platform and Default or Non-default Zone in the Essentials platform. But for a standby cluster in cluster redundancy, APs in the Staging or Default Zone can only be moved to another cluster by switchover.

The following task configures APs to swtichover clusters:

1. From the **Network** > **Wireless** > **Wireless LANs** page, select an AP.
2. Click **More** and select **Switch Over Clusters**.

   The specify **Destination Cluster** dialog box appears.
3. Enter **Control IP** or **FQDN**
4. Click **OK**. A confirmation dialog to trigger the AP switchover appears.
5. Click **Yes**.

   You have configured AP switchover.

Configuring Packet Capture for APs

User can enable packet streaming feature on both wired and wireless interfaces on specified APs using web UI. You must enable this feature on a per-AP basis. It allows multiple users to execute AP packet capturing, but only a single AP can execute one capturing task at a time. For a single user can capture tasks in multiple APs, but batch operation is not allowed. Only users with full access permission can execute AP packet capturing.

To configure Packet Capture:

1. From the **Network** > **Wireless** > **Wireless LANs** page, select an AP.
2. Click **More** and select **Packet Capture**.

   The **Packet Capture** dialog box appears.

3. Configure the **Capture Mode**:
   - **Stream to Wireshark**
     - **Capture Interface** Select the required wireless or wired interface
       - For 2.4 GHz/5 GHz, update the following details:

         Wireshark station IP: Enter the IP address.

         MAC Address Filter: Enter the MAC address.

         Frame Type Filter: Click the required options from Management, Control, and Data.
       - For Wired Interface, update the following details:

         Wireshark station IP: Enter the IP address.

         LAN Port: Choose the LAN port.
   - **Save to file**
     - **Capture Interface** Select the required wireless or wired interface
       - For 2.4 GHz/5 GHz, update the following details:

         MAC Address Filter: Enter the MAC address.

         Frame Type Filter: Click the required options from Management, Control, and Data.
       - For Wired Interface, update the following details:

         MAC Address Filter: Enter the MAC address.

         LAN Port: Choose the LAN port.
4. Click **Start**.

Running a Speed Test

You can run a speed test to measure the uplink or downlink performance between the controller or wireless device and an AP in a specific environment.

> **NOTE**
> The speed test traffic between the controller and an AP is not treated as data traffic. Hence, the traffic goes through the Linux Kernel NIC interface of the Controller where the interface is capped to 1 Gbps. Even when the AP's ethernet speed exceeds 1 Gbps, the speed test performance result still shows the upper threshold of 1Gbps.

To run a speed test from a wireless client to an AP, the RUCKUS SpeedFlex application must be installed on the wireless client. The application can be downloaded from Google Play store for Android devices or the Apple App Store for iPhones. The following fields must be configured before performing a run test:

- Destination Address
- Source Address
- Link
- Protocol
- Test Duration

To run a speed test between an AP and the controller, perform the following steps.

1. From the main menu, go to **Network** > **Wireless**, select **Access Points**.

   The **Access Points** page is displayed.
2. Select an AP from the list and then select the **Health** tab.

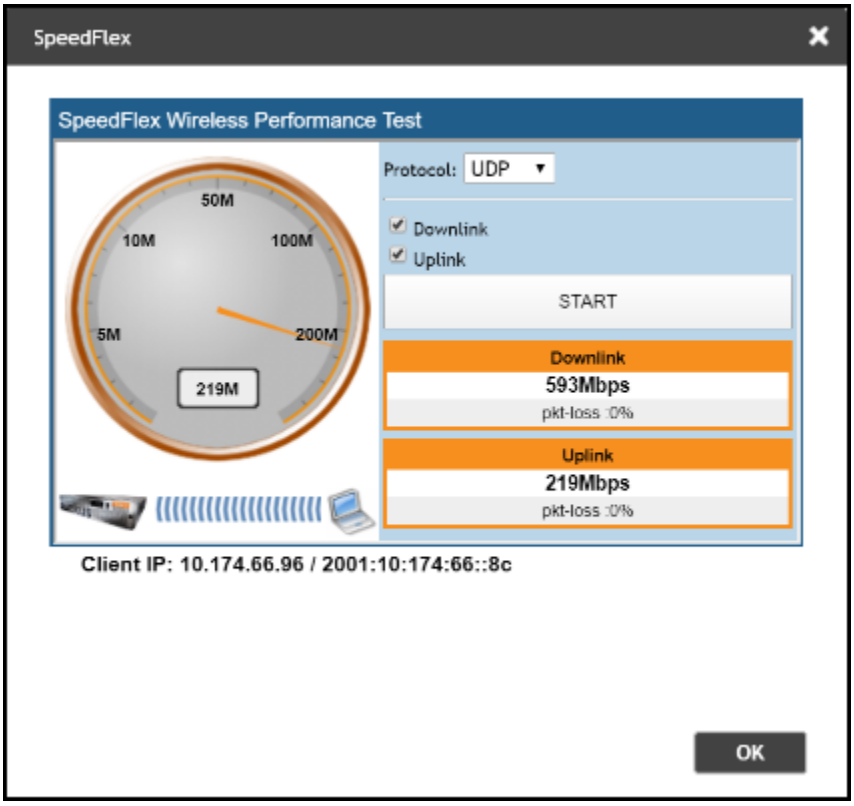
3. Click **Test Speed**.

   The **SpeedFlex** page is displayed.

4. Click **Start** to test the speed of UDP.

   When the test is complete, the downlink and uplink results are displayed, along with packet loss percentages.

FIGURE 69 SpeedFlex Test Result



Multi-Tunnel Support for Access Points

In prior RUCKUS solutions, APs could only support a single tunnel to a data plane, as well as a local break out. In this release, we're adding support for RUCKUS APs to provide multiple simultaneous tunnels to different data planes.

For 5.0, the AP will support a single RUCKUS GRE tunnel (with our without encryption) while supporting up to three SoftGRE (without encryption) tunnels, in addition to local breakout option. The tunneling will be based on SSID configurations on the AP.

This feature is designed to help in common MSP (Managed Service Provider) use cases, where each of the MSP's customer will have the possibility to get its own tunnel directly to the data center.

Before configuring multiple tunnels, consider the following configuration prerequisites:

- Ensure that there is a reachable SoftGRE gateway and also verify that there is network connectivity.
- Ensure that the zone is configured with correct SoftGRE gateway information.
- Verify that the SSID to SoftGRE tunnel mapping is correct.

- Verify the SoftGRE tunnel configuration and run time status using the command **get softgre***tunnel-index*. The tunnel index can be 1, 2, or 3.

Configuring Multiple Tunnels for Zone Templates

Multiple tunnels can be configured for a zone template.

Perform the following steps to select a tunnel profile for a zone template.

1. From the main menu, go to **Administration** > **System** > **Template** > **Zone Templates**.
2. Click **Create**.

   The **Create Zone Template** form appears.

   FIGURE 70 Configuring a RUCKUS GRE Profile



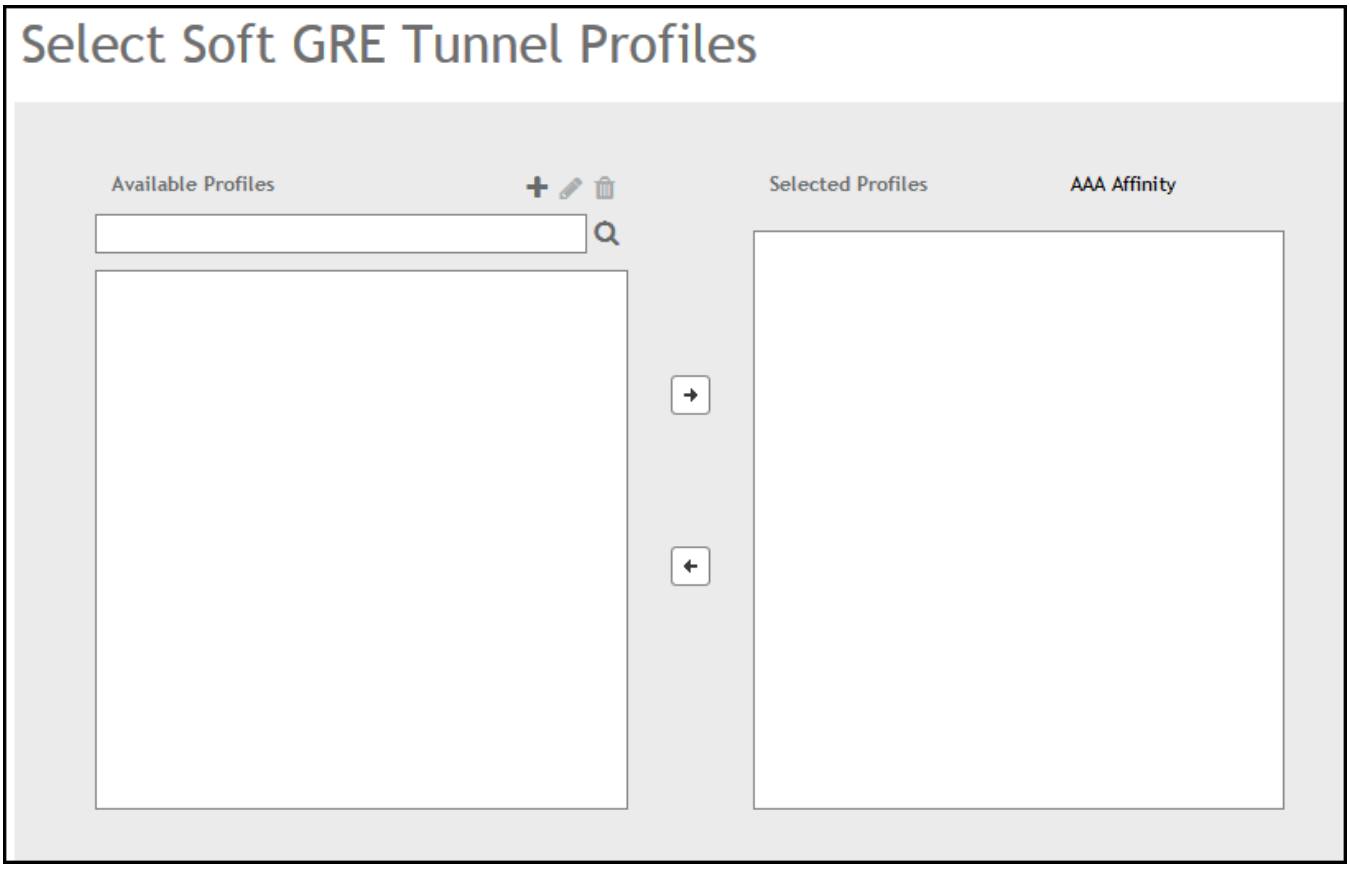
3. Navigate to the **AP GRE Tunnel Options** section.
4. For the **Ruckus GRE Profile** select a profile from the drop-down menu.

   Click the **+** icon to create a new Ruckus GRE profile.

5. Click the **Select** checkbox above the SoftGRE Profiles box.

   A form appears from which you can select the SoftGRE profiles that you want to apply to the zone. The profiles you can select are displayed under **Available Profiles**. Select the profile and click the **->** icon to choose it. The profile is now listed under the **Selected Profiles** area.

   FIGURE 71 SoftGRE Profiles Form



   You can also click the **+** icon to create a new SoftGRE profile.

   If you wish to deselect a profile, select it and click the **<-** icon. The profile will be moved back to the **Available Profiles** area and will not be applied to that zone.

6. Click **OK**.

   Your multiple tunnel configuration for the zone template is saved.

Configuring Multiple Tunnels for Zone

Multiple tunnels can be configured for a zone.

To configure the tunnel types for an AP zone, perform the following steps.

1. From the main menu, go to **Network** > **Wireless**, select **Access Points**, the **Access Point** page is displayed, select the AP from the list.
2. From the System tree, select the location where you want to create the zone. For example, System or Domain. Click **+** icon.

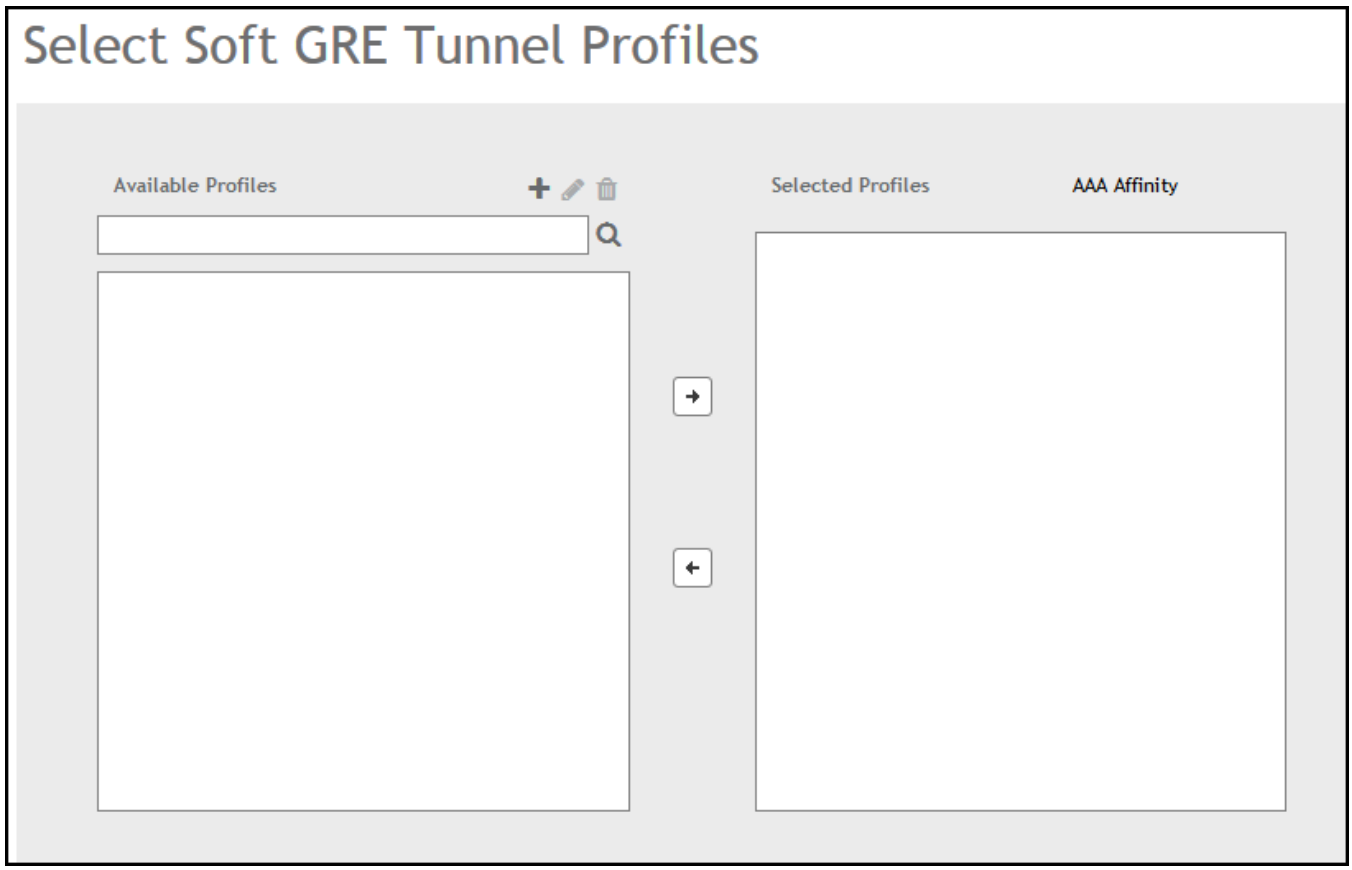
   The **Create Group** page appears.

3. Under **Type**, select **Zone**.
4. Navigate to the **AP GRE Tunnel** section.
5. For the **Ruckus GRE Profile** select a profile from the drop-down menu.

   Click the **+** icon to create a new Ruckus GRE profile.
6. Click the **Select** checkbox above the SoftGRE Profiles box.

   A form appears from which you can select the SoftGRE profiles that you want to apply to the zone. The profiles you can select are displayed under **Available Profiles**. Select the profile and click the **->** icon to choose it. The profile is now listed under the **Selected Profiles** area.

   FIGURE 72 SoftGRE Profiles Form



   You can also click the **+** icon to create a new SoftGRE profile.

   If you wish to deselect a profile, select it and click the **<-** icon. The profile will be moved back to the **Available Profiles** area and will not be applied to that zone.
7. Click **OK**.

   Your multiple tunnel configuration for the zone is saved.

Configuring Multiple Tunnels in WLANs

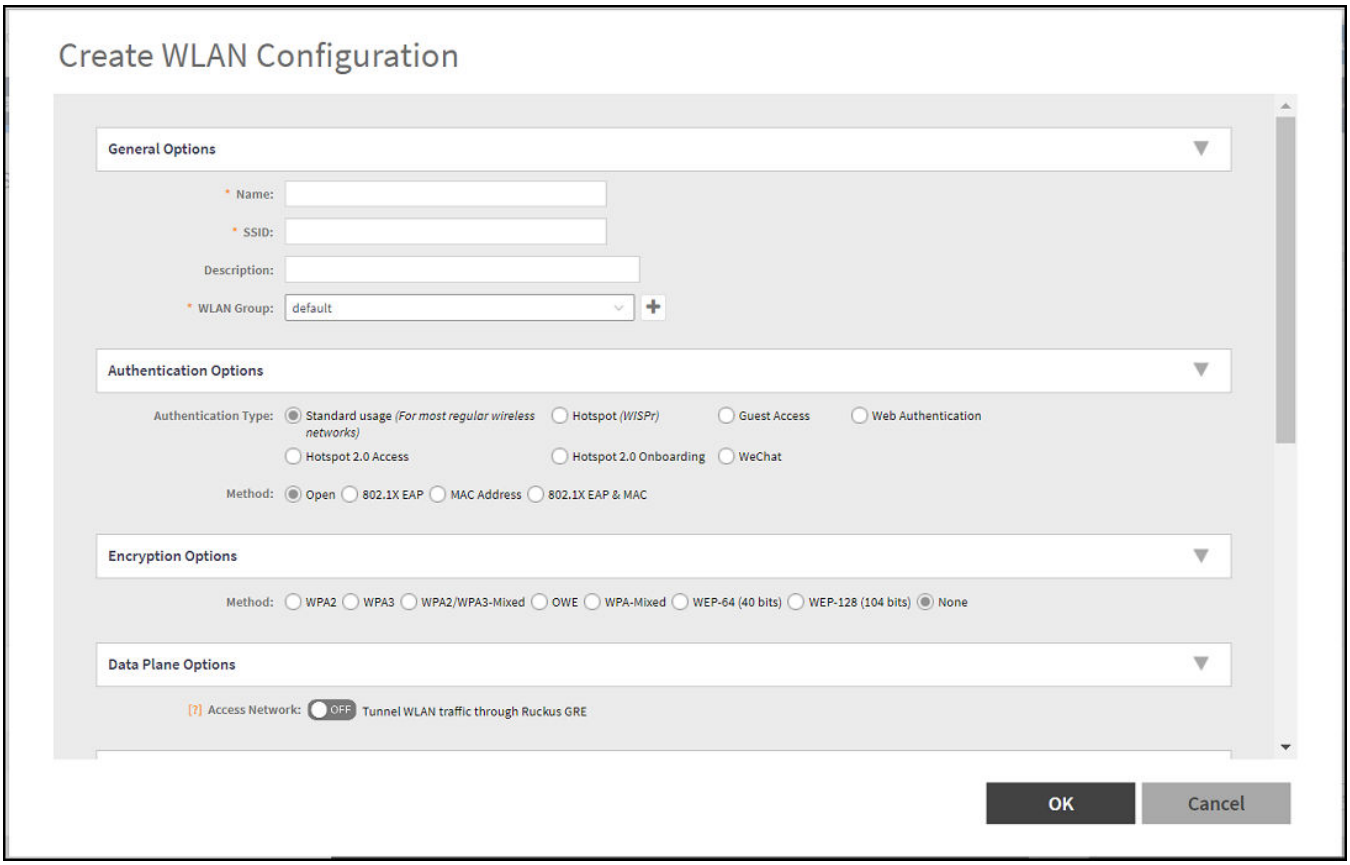
In WLANs where there is an option to tunnel the traffic, you can choose the tunneling profile the WLAN can use.

Perform the following steps to enable tunneling in WLANs.

1. Go to **Network** > **Wireless** > **Wireless LANs**, from the **System tree hierarchy**, select the **Zone** where you want to create a WLAN.
2. Click **Create**.

   The **Create WLAN Configuration** page appears.

   FIGURE 73 Tunneling Options while Creating a WLAN Configuration



3. In the section **Data Plane Options** , enable the **Tunnel WLAN traffic through Ruckus GRE** switch.

You have successfully configured the tunneling option to forward traffic in a WLAN.

Link Aggregation Control Protocol (LACP) support for R720 AP

The R720 AP is a four-stream 802.11ac Wave 2 access point. The AP can transmit to multiple Wave 2 clients in parallel, improving the RF efficiency in addition to faster connectivity and reliable network performance.

NOTE
LACP or Bonding feature is configurable using AP RKS CLI mode though the web user interface configuration option is limited to APs R720, R710 and R610.

NOTE
LACP or Bonding feature option enable or disable is a service-affecting feature configuration. This feature can be used during setup or maintenance mode only when there are no active downlink (DL) or uplink (UL) traffic in progress.

NOTE
To support LACP or Link Aggregation Group (LAG) feature on RUCKUS APs, the administrator needs to ensure correct PoE power modes to Bring-Up LAN1 and 2 ports. For example, PoE-at+ for R720, PoE-at for R710, and so on. Refer to the respective AP product guides for details. LACP/LAG UL throughput is limited to around 1 Gbps.

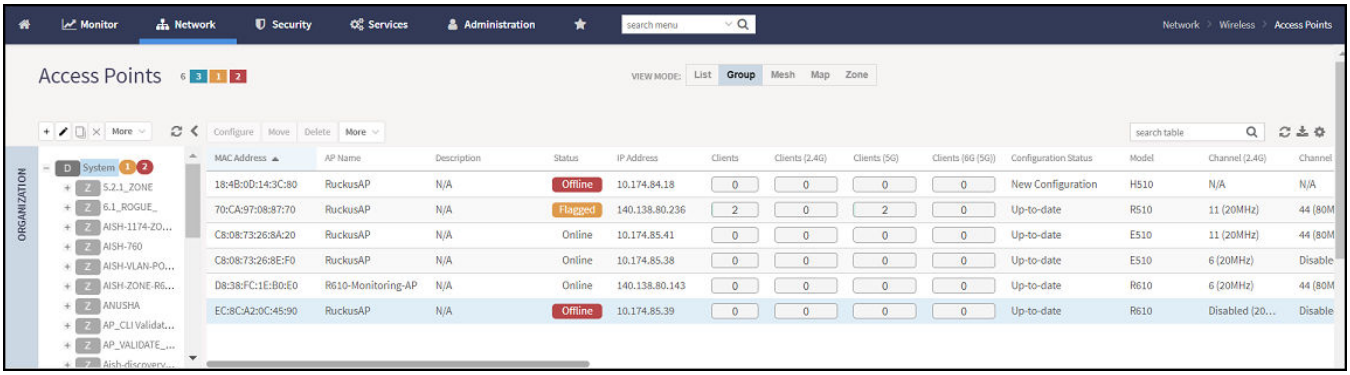
Enabling the LACP Support for a Zone

Perform the following procedure to enable the LACP support for a zone.

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

   The **Access Points** page is displayed.

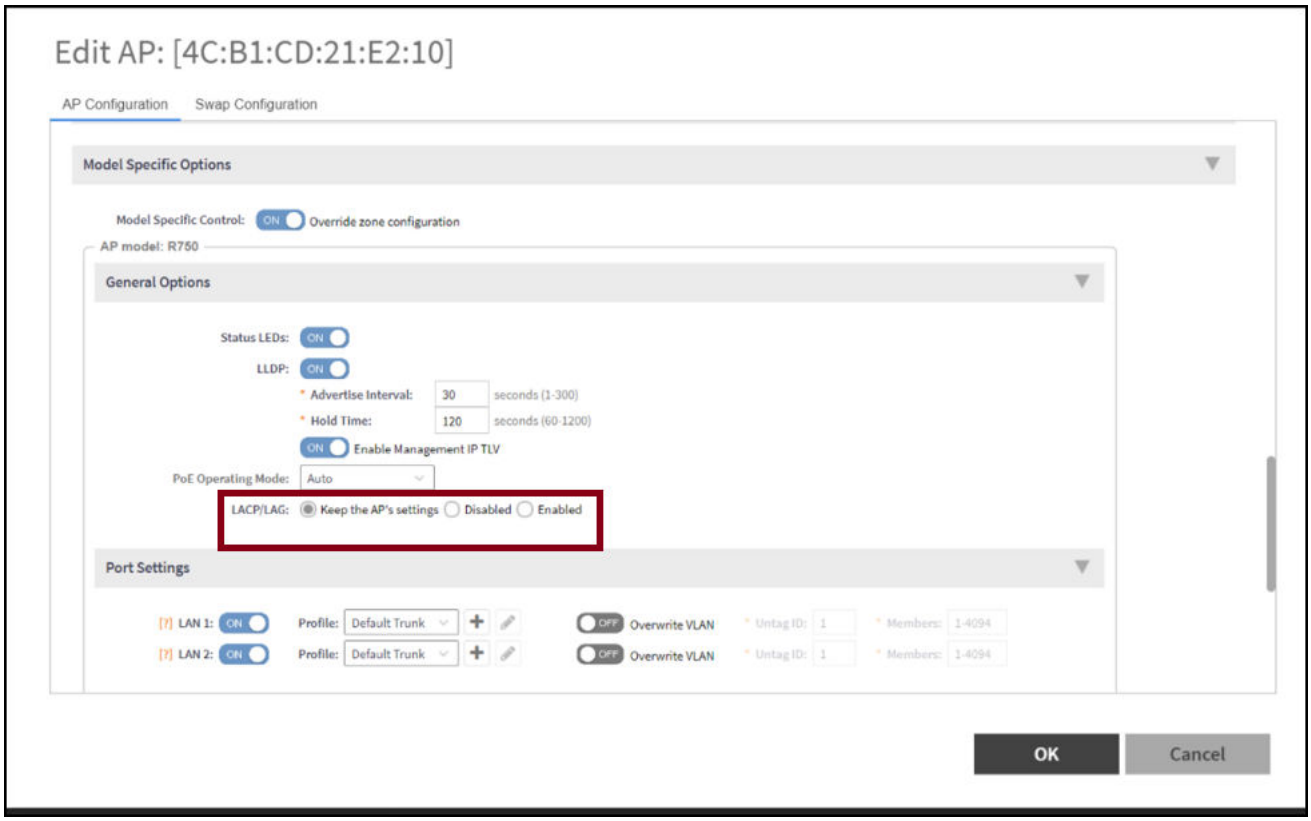
   FIGURE 74 Viewing the Access Points



2. Select a zone and click .

   The **Configure Group** page is displayed.

   FIGURE 75 Enabling LACP Support for a Zone



3. Enter the zone name.
4. Under **Configuration**, select **R720** from the **Select an AP Model** list.
5. Under **General Options**, enable **LACP**.

   NOTE
   By default, LACP is disabled.

   NOTE
   To support the LACP and LAG feature on RUCKUS APs, ensure that the correct PoE mode is selected to bring up LAN1,2 ports. For example, PoE-at+ for R720, PoE-at for R710. The LACP and LAG UL throughput is limited to around 1Gbps.

6. Click **OK**.

Enabling LACP Support for an AP Group

Perform the following procedure to enable the LACP support for an AP group.

1. From the main menu, go to **Network** > **Wireless**, select **Access Points**.

2. Select an AP group from the zone and click .
3. In the **Configure** page, enter the name of the AP group.
4. Under **Configuration**, select **R720** from the **Select an AP Model** list.
5. Under **General Options**, enable **LACP**.

   NOTE
   By default, LACP is disabled. To enable LACP, both **LACP** and **Override** must be enabled.

   NOTE
   To support the LACP and LAG feature on RUCKUS APs, ensure that the correct PoE mode is selected to bring up LAN1,2 ports. For example, PoE-at+ for R720, PoE-at for R710. The LACP and LAG UL throughput is limited to around 1Gbps.

6. Click **OK**.

Enabling LACP Support for an AP

Perform the following procedure to enable the LACP support for an AP.

1. From the main menu, go to **Network** > **Wireless**, select **Access Points**. The Access Point page is displayed.
2. Select an AP group from the zone.
3. Select an AP and click .
4. In the **Edit AP** page, enter the AP name.
5. Under **Configuration**, select **R720** from the **Select an AP Model** list.
6. Under **General Options**, enable **LACP**.

   NOTE
   By default, LACP is disabled.

   NOTE
   To support the LACP and LAG feature on RUCKUS APs, ensure that the correct PoE mode is selected to bring up LAN1,2 ports. For example, PoE-at+ for R720, PoE-at for R710. The LACP and LAG UL throughput is limited to around 1Gbps.

7. Click **OK**.

   NOTE
   When you enable or disable LACP, the corresponding status is updated in the **General** tab of the **Access Points** page.

Power Source in AP Configuration

The table below displays the PoE mode as per industry standards.

The currently used APs have AF, AT, AT+ convention modes. The standardization applies when the AP is forced to certain PoE power mode. If the AP is set to AUTO PoE mode, feedback displays PoE mode of the AP is currently configured.

The PoE mode as per the industry standards:

TABLE 53 Industry Standard PoE Modes

Selection	Power@PSE	Power@AP (100M Cable)
802.3af	15.4W	12.95W
802.3at	30W	25.5W
802.3bt/Class 5	45W	40W→35W
802.3bt/Class 6	60W	51W
802.3bt/Class 7	75W	62W
802.3bt/Class 8	90W	71.3W

TABLE 54 Non-Standard High Power Solution Summary

	Customers	Maximum Power Sourced
UPoE	Enterprise Switch	60W
PoH	Consumer Customers, for example, audio systems)	95W

The SZ-GUI power mode drop-down has the following set of PoE mode configurations:

TABLE 55 PoE Mode Settings

Name	Value
Auto	0
802.3af	1
802.3at	2
802.3bt/Class 5	3
802.3bt/Class 6	4
802.3bt/Class 7	5

NOTE
The 802.3bt/Class5 is chosen for AP's with older software which advertise AT+.

NOTE
The below tables are applicable for stand alone APs as well. However, the IOT functionality is not available.

POE tables for different 11 AC AccessPoint

TABLE 56 R710

	LLDP Power Ask	**2.4G tx/rx**	**5G tx/rx**	**1Gbps eth**	**USB**	**IOT**
DC	N/A	4/4	4/4	Enabled	Enabled	Enabled
AF	N/A	2/4	4/4	Enabled	Disabled	Disabled
AT	25W	4/4	4/4	Enabled	Enabled	Enabled
Injector (Model 480125A)	N/A	4/4	4/4	Enabled	Enabled	Enabled

TABLE 57 R610

	LLDP Power Ask	**2.4G tx/rx**	**5G tx/rx**	**1Gbps eth**	**USB**	**IOT**
DC	N/A	4/4	4/4	Enabled	Enabled	Enabled
AF	N/A	2/4	4/4	Enabled	Disabled	Disabled

TABLE 57 R610 (continued)

AT	24W	4/4	4/4	Enabled	Enabled	Enabled
Injector (Model 480125A)	N/A	4/4	4/4	Enabled	Enabled	Enabled

TABLE 58 R720

	LLDP Power Ask	2.4G tx/rx	5G tx/rx	1Gbps eth	USB	IOT	Comments
DC	N/A	4/4	4/4	Enabled	Enabled	Enabled	No comments
AF	N/A	1/4	1/4	Enabled	Disabled	Disabled	No comments
AT	25W	4/4	4/4	Enabled	Disabled	Disabled	No comments
3bt/class5	35W	4/4	4/4	Enabled	Enabled	Enabled	No comments
POE Injector (Model 480125A) 60W	N/A	4/4	4/4	Enabled	Enabled	Enabled	Force to 802.3bt/ class5 from SZ GUI

TABLE 59 M510

	LLDP Power Ask	2.4G tx/rx	5G tx/rx	1Gbps eth	USB	IOT
DC	N/A	2/2	2/2	Enabled	Enabled	Enabled
AF	N/A	2/2	2/2	Enabled	Disabled	Disabled
AT	25W	2/2	2/2	Enabled	Enabled	Enabled
Injector (Model 480125A)	N/A	2/2	2/2	Enabled	Enabled	Enabled

TABLE 60 T610

	LLDP Power Ask	2.4G tx/rx	5G tx/rx	1Gbps eth	USB	IOT
DC	N/A	3/3	3/3	Enabled	Enabled	Enabled (0.5W)
AF	N/A	2/3	3/3	Enabled	Disabled	Disabled
AT	25W	3/3	3/3	Enabled	Enabled	Enabled (0.5W)
Injector (Model 480125A)	N/A	3/3	3/3	Enabled	Enabled	Enabled (0.5W)

POE tables for different 11 AX AccessPoint

TABLE 61 R730

	LLDP	2.4G tx/rx	5G tx/rx	5Gbps eth	1Gbps eth	USB	IOT	Comments
DC	N/A	4/4	8/8	Enabled	Enabled	Enabled	Enabled	No comments
AF	N/A	1/4	1/8	Enabled	Disabled	Disabled	N/ADisabled	Not supported via SZ-GUI, but we can AF mode via rkscli.
AT Mode = 0	25W	4/4	4/8	Enabled	Enabled	Enabled (0.5W)	Enabled	By default AT - mode = 0
AT Mode = 1	25W	4/4	8/8	Enabled	Disabled	Disabled	Disabled	Set AT - mode = 1 via Rkscli
802.3bt/class 5	35W	4/4	8/8	Enabled	Enabled	Enabled	Enabled	No comments

TABLE 61 R730 (continued)

POE Injector (Model 480125A) 60W	N/A	4/4	4/8	Enabled	Enabled	Enabled	N/A	Force to 802.3bt/class5 from SZ GUI

TABLE 62 R850

	LLDP Power Ask	2.4G tx/rx	5G tx/rx	5Gbps eth	1Gbps eth	USB	IOT	Comment
DC	N/A	4/4	8/8	Enabled	Enabled	Enabled	Enabled	No comments
AF	N/A	1/4	1/8	Enabled	Disabled	Disabled	Disabled	Not supported via SZ-GUI, but we can AF mode via rkscli.
AT (Mode=0)	25W	4/4	4/8	Enabled	Enabled	Enabled (0.5W)	Enabled	By default at-mode=0
AT (Mode=1)	25W	4/4	8/8	Enabled	Disabled	Disabled	Disabled	Set at-mode=1 via Rkscli
802.3bt/class5	35W	4/4	8/8	Enabled	Enabled	Enabled	Enabled	No comments
POE Injector (Model 480125A) 60W	N/A	4/4	4/8	Enabled	Enabled	Enabled	Enabled	Force to 802.3bt/class5 from SZ GUI

TABLE 63 R750

	LLDP Power Ask	2.4G tx/rx	5G tx/rx	2.5Gbps eth	1Gbps eth	USB	IOT
DC	N/A	4/4	4/4	Enabled	Enabled	Enabled	Enabled
AF	N/A	2/4	2/4	Enabled	Disabled	Disabled	Disabled
AT	25W	4/4	4/4	Enabled	Enabled	Enabled	Enabled
POE Injector (Model 480125A) 60W	N/A	4/4	4/4	Enabled (1Gbps speed)	Enabled	Enabled	Enabled

TABLE 64 T750

	LLDP Power Ask	**2.4G tx/rx**	**5G tx/rx**	**2.5Gbps eth**	**1Gbps eth**	**USB**	**IOT**	**PSE**	**Comment**
DC	N/A	4/4	4/4	Enabled	Enabled	Enabled	Enabled	Enabled	No comments
AF	N/A	1/4	1/4	Enabled	Disabled	Disabled	Disabled	Disabled	Not supported operation mode
AT w/o USB	25W	4/4	4/4	Enabled	Enabled	Disabled	Enabled	Disabled	No comments
AT with USB	25W	2/4	4/4	Enabled	Disabled	Enabled	Enabled	Disabled	Set AT - mode = 1 via Rkscli
802.3bt/class5	35W	4/4	4/4	Enabled	Enabled	Enabled	Enabled	Disabled	No comments
803.3bt/class6	N/A	4/4	4/4	Enabled	Enabled	Enabled	Enabled	Disabled	51W by H/W negotiation
802.3bt/class7	N/A	4/4	4/4	Enabled	Enabled	Enabled	Enabled	Enabled	62W by H/W negotiation

TABLE 64 T750 (continued)

POE 60W Injector (Model 480125A)	N/A	4/4	4/4	Enabled (1Gbps speed)	Enabled	Enabled	Enabled	Disabled	Force to 802.3bt/ class5
POE 90W Injector	N/A	4/4	4/4	Enabled	Enabled	Enabled	Enabled	Enabled	Force to 802.3bt/ class7

TABLE 65 R650

	LLDP Power Ask	**2.4G tx/rx**	**5G tx/rx**	**2.5Gbps eth**	**1Gbps eth**	**USB**	**IOT**
DC	N/A	2/2	4/4	Enabled	Enabled	Enabled	Enabled
AF	N/A	2/2	2/4	Enabled	Disabled	Disabled	Disabled
AT	25W	2/2	4/4	Enabled	Enabled	Enabled	Enabled
POE Injector (Model 480125A)	N/A	2/2	4/4	Enabled (1Gbps speed)	Enabled	Enabled	Enabled

TABLE 66 R550

	LLDP Power Ask	2.4G tx/rx	5G tx/rx	2.5Gbps eth	1Gbps eth	USB	IOT
DC	N/A	2/2	2/2	Enabled	Enabled	Enabled	Enabled
AF	N/A	2/2	2/2	Enabled	Disabled	Disabled	Disabled
AT	25W	2/2	2/2	Enabled	Enabled	Enabled	Enabled
POE Injector (Model 480125A)	N/A	2/2	2/2	Enabled	Enabled	Enabled	Enabled

Working with WLANs and WLAN Groups

Domains, Zones, WLAN Groups, and WLANs

If your wireless network covers a large physical environment (for example, a multi-floor building or multi-building office) and you want to manage and provide different WLAN services to different areas of your environment, you can virtually split them using the following hierarchy:

- Domains: Geographical grouping for regulatory operation
- Zones: Consists of multiple WLAN groups
- WLAN Groups: Consists of multiple WLANs
- WLANs: Provides wireless network service

Viewing Modes

The **View Mode** on the upper-right corner of the page provides two options to view the WLANs available in the system:

- **List**—Displays the list of all WLANs irrespective of the Zone or Group they belong.
- **Group**—Displays the list of WLANs that belong to a specific Zone or Group.

The following WLAN details can be viewed regardless of the mode selected:

- **Name**
- **Alert**
- **SSID**

- **Auth Method**
- **Encryption Method**
- **Clients**
- **Traffic**
- **VLAN**
- **Application Recognition**
- **Tunneled**

Creating a WLAN Domain for an MSP

A Managed Services Provider (MSP) manages and assumes a defined set of responsibility. You can create an MSP managed domain, to manage all their settings within that domain.

> **NOTE**
> This feature is applicable only for SZ300 and vSZ-H platforms.

Complete the following steps to create a WLAN Domain for an MSP:

1. From the **Network** > **Wireless** > **Wireless LANs** , select **System** from the tree hierarchy.
2. Click the **Create** button, the Create Group form appears.
3. Configure the following details:
   a. Enter a **Name** for the domain.
   b. Enter a **Description** about the domain.
   c. By default, the **Type** selected is **Domain**.
   d. The **Parent Group** displays the group to which this domain will be tagged.
   e. In **Managed by Partner**, select the **Enable** check box.
4. Click **OK**. You have created a new WLAN domain. In the left pane, the new MSP domain appears.

WLAN Groups

WLAN groups are configured at the zone level. A default WLAN group (called "default") exists, and the first 27 WLANs that you create are automatically assigned to this default WLAN group. A WLAN group can include a maximum of 27 member WLANs. For dual or tri-band radio APs, each radio can be assigned to only one WLAN group (single radio APs can be assigned to only one WLAN group).

Creating WLAN groups is optional. If you do not need to provide different WLAN services to different areas in your environment, you do not need to create a WLAN group.

A WLAN group is a way of specifying which APs or AP groups provide which WLAN services. For example, if your wireless network covers three floors of a building and you want to provide wireless access to visitors only on the first floor, take the following action.

1. Create a WLAN service (for example, Guest Only Service) that provides guest-level access only.
2. Create a WLAN group (for example, Guest Only Group).
3. Assign Guest Only Service (WLAN service) to Guest Only Group (WLAN group).
4. Assign APs on the first floor (where visitors need wireless access) to your Guest Only Group.

Any wireless client that associates with APs assigned to the Guest Only Group will get the guest-level access privileges defined in your Guest Only Service. APs on the second and third floors can remain assigned to the default WLAN group and provide normal-level access.

Creating a WLAN Group

If your wireless network covers a large physical environment and you want to provide different WLAN services to different areas, you may want to create WLAN groups.

1. From the main menu, go to **Network** > **Wireless** > **Wireless LANs** .
2. From the **System** tree hierarchy, select the zone where you want to create a WLAN group.
3. Click the add button . The **Create WLAN Group** dialog box is displayed.
4. In the **Name** field, enter a name for the WLAN group.
5. In the **Description** field, enter a brief description of the WLAN group.
6. From the **Available WLANs** list, perform one of the following option:
   - Select the required WLAN and click **Move**. The WLAN will move to the **Selected WLANs** list.
   - Click the add button to create a new WLAN service. Create WLAN Configuration dialog box is displayed.. Refer Creating a WLAN Configuration on page 184.

     NOTE
     To edit or delete a WLAN configuration, select the WLAN from the **Available WLANs** list and click the **Configure** or **Delete** options respectively.

7. Click **Next**. The C**reate WLAN Group** dialog box is displayed.
8. Click **OK**.

NOTE
You can also edit, clone, and delete a WLAN group by selecting the options **Configure**, **Clone**, and **Delete** options respectively, from the **Wireless LANs** page.

Creating a WLAN Configuration

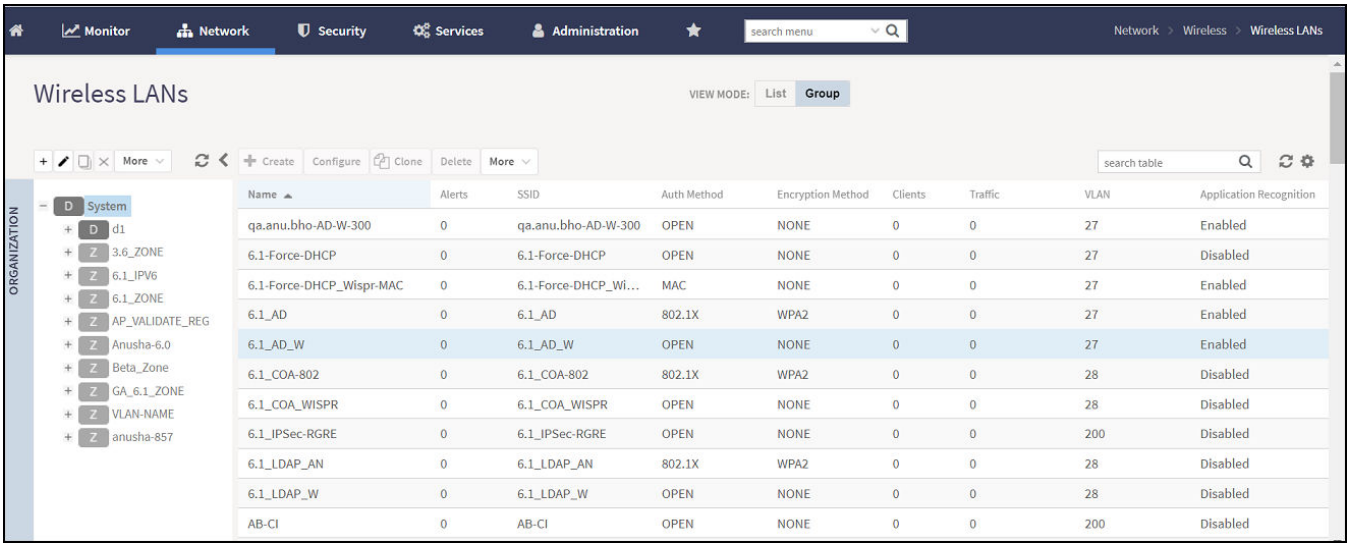
An AP zone functions as a way of grouping RUCKUS APs and applying settings including WLANs to these groups of RUCKUS APs.

Complete the following steps to create a WLAN configuration for an AP zone.

1. Go to **Network** > **Wireless** > **Wireless LANs** page, from the **System** tree hierarchy, select the **Zone** where you want to create a WLAN.

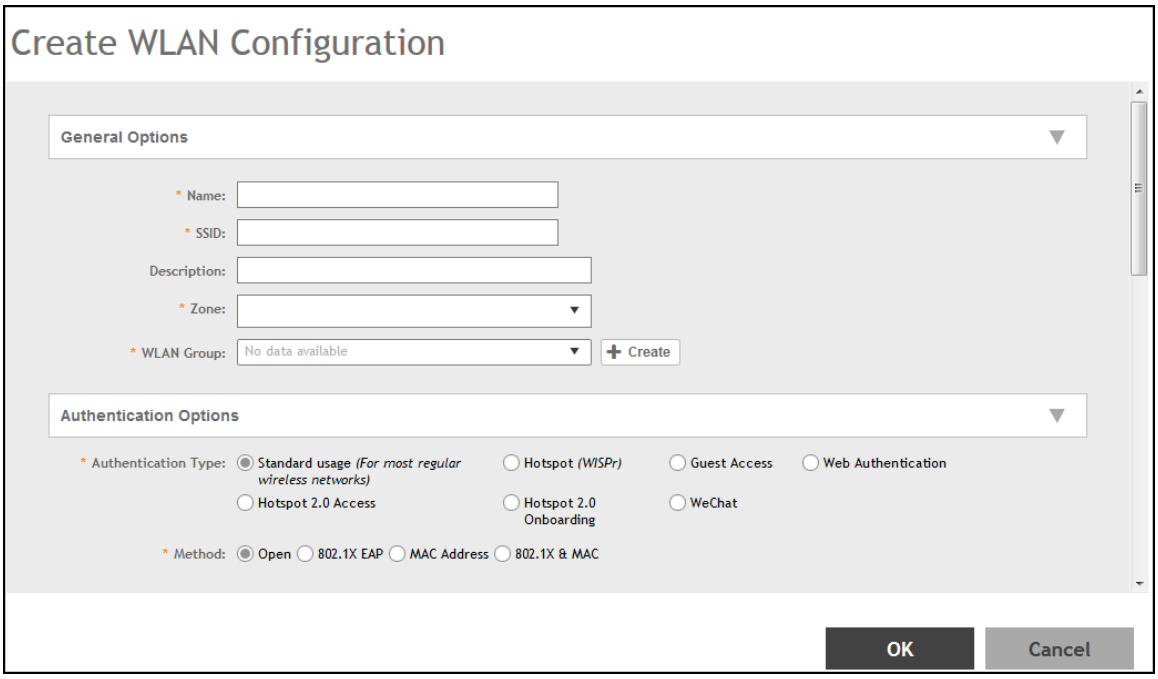
   NOTE
   For SmartZone 5.2.1 or earlier releases, in the **Wireless LANs** page, from the **System** tree hierarchy, select the **Zone** where you want to create a WLAN.

FIGURE 76 Wireless LANs Page



2. Click **Create** and the **Create WLAN Configuration** page is displayed.

FIGURE 77 Create WLAN Configuration Page



3. Set the required configurations as explained in the following table.

TABLE 67 WLAN Configurations

Field	Description	Your Action
General Options		

TABLE 67 WLAN Configurations (continued)

Field	Description	Your Action
Name	Indicates the user-friendly administrative name for the WLAN.	Enter a name.
SSID	Indicates the SSID for the WLAN.	Enter the SSID.
Description	Indicates a user-friendly description of the WLAN's settings or function.	Enter a short description.
Zone	Indicates the zone to which the WLAN configuration applies.	Select the zone to which the WLAN settings apply.
WLAN Groups	Indicates the WLAN groups to which the WLAN applies.	Select the WLAN groups to which the WLAN configuration applies.
Authentication Options		
Authentication Type	Defines the type of authentication flow for the WLAN. **NOTE** Authentication types such as WeChat, Web Authentication, and Guest Access are not supported by APs in IPv6 mode.	Select the required option: • **Standard Usage**—This is a regular WLAN suitable for most wireless networks. • **Hotspot (WISPr)**—Click this option if want to use a hotspot service (use this type for external captive portal workflows) or WISPr. **NOTE** Hotspot (WISPr) applies to WLAN traffic that is tunneled and not tunneled. • **Guest Access**—Click this option if you want guest users to use this WLAN. After you complete creating this WLAN for guest access, you can start generating guest passes. For more information about Hotspot 2.0 online signup, see the Hotspot 2.0 Reference Guide for this release. • **Web Authentication**—Click this option if you want to require all WLAN users to complete a web-based logon to this network every time they attempt to connect. • **Hotspot 2.0 Access**—Click this option if you want a Hotspot 2.0 operator profile that you previously created to use this WLAN. See the Hotspot 2.0 Reference Guide for this release. **NOTE** You can select 8021.X EAP + "WPA3" or "WPA2/WPA3-Mixed" for HS2.0 access wlan to add more security. • **Hotspot 2.0 Onboarding**—Click this option if you want to use this WLAN for Hotspot 2.0 onboarding. See the Hotspot 2.0 Reference Guide for this release for more information. Hotspot 2.0 onboarding allows for Open and 802.1x EAP authentication methods. **NOTE** This authentication type cannot be reconfigured to use a different authentication type due to differences in how Authentication and Accounting profiles are stored and subsequently mapped to WLAN configurations. • **WeChat**—Click this option if you want the WLAN usage through WeChat.
Authentication Options		

TABLE 67 WLAN Configurations (continued)

Field	Description	Your Action
Method	Specifies the authentication mechanism.	Select the following option: • **Open** (Default)—No authentication mechanism is applied to connections. If WPA or WPA2 encryption is used, this implies WPA-PSK authentication. If you clicked **Web Authentication** in **Authentication Type**, **Open** is the only available authentication option, even though PSK-based encryption can be supported. • **802.1X EAP**—A very secure authentication/encryption method that requires a back-end authentication server, such as a RADIUS server. Your choice mostly depends on the types of authentication the client devices support and your local network authentication environment. If you select **Enable RFC Location Delivery Support** for **Authentication & Accounting Server**, enter the **Operator Realm**. Selecting the authentication method as Hotspot (WISPr) allows you to select 802.1x EAP as an authentication option. This enables a two-step authentication method when shared and pre-authenticated devices are used, or when user equipment is shared among multiple users. The device access is successful when both authentication processes are completed successfully: 802.1x EAP authentication first, followed by Hotspot (WISPr) authentication. Selecting the authentication method as Hotspot 2.0 Access with support of WPA3 allows you to select 802.1x EAP as an authentication option. • **MAC Address**—Authenticate clients by MAC address. – **MAC Authentication**—Requires a RADIUS server and uses the MAC address as the user logon name and password. › Select **Use user defined text as authentication password** (default is device MAC address) and enter the format. – **MAC Address Format**—Choose the MAC address format from the drop-down menu. • **802.1X EAP & MAC**—Selecting this option indicates that the 802.1x EAP and MAC address authentication methods must both pass for a user to successfully authenticate. First, MAC address authentication is verified; if that passess, 802.1x EAP authentication is processed. After the two authentication methods succeed, the user equipment gains access to the WLAN. Authentication is handled by a back-end RADIUS server. When this authentication method is selected, the MAC Authentication and MAC Address Format fields will be shown within the Authentication Options section.
Encryption Options		

TABLE 67 WLAN Configurations (continued)

Field	Description	Your Action
Method	Specifies the encryption method. WPA and WPA2 are both encryption methods certified by the Wi-Fi Alliance; WPA2 with AES is the recommended encryption method. The Wi-Fi Alliance will be mandating the removal of WEP due to its security vulnerabilities, and RUCKUS recommends against using WEP, if possible.	Select the option: • **WPA2**—Enhanced WPA encryption using AES encryption algorithm. a. Choose **Algorithm**: – **AES**: 1. Enter **Passphrase**. 2. Select or clear **Show**. 3. Select › the **Enable 802.11 Fast BSS Transition** check box and enter the **Mobility Domain ID**. › the required **802.11w MFP** option. 4. **Dynamic PSK** › **Disable** › **Internal** a. Enter **DPSK Length** b. Choose **DPSK Type** c. Select **DPSK Expiration** › **External**—Enables **Authentication Service** – **AUTO**: 1. Enter **Passphrase**. 2. Select or clear **Show**. • **WPA3**—Enhanced WPA3 encryption using AES encryption algorithm. Enable this option for 6G radio. a. Choose **Algorithm**: – **AES**: 1. Enter **Passphrase**. 2. Select or clear **Show**. 3. In the **802.11w MFP** field, " Required" is the default selected option. – **AES-GCMP-256**: › **NOTE** WPA3-Enterprise cannot be supported by the 802.11ac Wave-1 AP models. • **WPA2/WPA3-Mixed** Encryption - Allows mixed networks of WPA2- and WPA3-compliant devices using AES algorithm. a. 1. Choose **Algorithm**: – **AES**: a. Enter **Passphrase**. b. Enter **SAE Passphrase** c. Select or clear **Show**. d. In the **802.11w MFP** field, " Capable" is the default selected option b. Choose **Algorithm**: – **AES**: 1. Enter **Passphrase**. 2. Enter **SAE Passphrase** 3. Select or clear **Show**. • **Opportunistic Wireless Encryption (OWE)** - Allows the encryption without the manual input the passphrase using AES algorithm. Enable this option for 6G radio.

TABLE 67 WLAN Configurations (continued)

Field	Description	Your Action
Data Plane Options		
Access Network	Defines the data plane tunneling behavior.	Enable **Tunnel WLAN traffic through Ruckus GRE**. Configure the following options as appropriate: • **GRE Tunnel Profile:** Manages AP traffic. Select the profile from the list. • **Split Tunnel Profile:** Enables split tunneling to manage user traffic between corporate and local traffic. Enable the profile from the list. Click  to create a new profile or click  to edit a profile. By default, the option is disabled.
Core Network	Defines the network mode.	Select the option: • **Bridge** • **L2oGRE**
vSZ-D DHCP/NAT	Enables tunneling option for DHCP/NAT.	Select the required check boxes: • **Enable Tunnel NAT** • **Enable Tunnel DHCP**
RADIUS based DHCP/NAT	Enables RADIUS-based DHCP/NAT settings. The DHCP server authorizes remote clients and allocates addresses based on replies from a RADIUS server.	Select the required check boxes: • **Enable RADIUS based NAT** • **Enable RADIUS based DHCP**
Flexi-VPN Profile	Enables forwarding of tunneled traffic to another remote DP instance through inter-DP RuckusGRE Tunnel (Flexi). **NOTE** If there are more than 40 DPs been approved, SZ limit user to use Flexi-VPN feature.	Select the profile from the list.
Authentication & Accounting Server (for WLAN **Authentication Type**: **Standard usage**)		
Authentication Server	Specifies the server used for authentication on this network. By enabling Proxy, authentication requests will flow through the controller. In a non-proxy mode, the AP will communicate directly with the authentication server without going through the controller.	a. Select the **Use controller as proxy** check box. b. Select the server from the menu. c. Select **Enable RFC Location Delivery Support**.
Accounting Server	Specifies the server used for accounting messages. By enabling Proxy, accounting messages are sent by the controller. In a non-proxy mode, the AP will communicate accounting messages directly.	a. Select the **Use controller as proxy** check box. b. Select the server from the menu.
Hotspot Portal (for WLAN **Authentication Type**: **Hotspot (WisPr)**)		
Hotspot (WISPr) Portal	Defines hotspot behavior such as redirects, session timers, and location information among others.	Select the hotspot portal profile that you want this WLAN to use.
Bypass CNA	Bypasses the Apple CNA feature on iOS and OS X devices that connect to this WLAN.	Select the **Enable** check box.

TABLE 67 WLAN Configurations (continued)

Field	Description	Your Action
Portal Detection and Suppression	Designed to allow the operator to set some policy rules that would trigger based on http User-Agent data.	Select the portal detection profile from the list, or click **+** to create a new profile.
Authentication Service	Indicates the authentication server that you want to use for this WLAN.	Choose the option. Options include **Local DB**, **Always Accept**, and any AAA servers that you previously added. Select: • **Use Controller as Proxy** for the controller to proxy authentication messages to the AAA server • **Use Realm-based profile** to list contents the realm-based profile When the SSH tunnel between the AP and the controller is down, you can enable **Backup Authentication Service** to back up the AP's authentication services to a secondary device. **NOTE** The customer portal must use AP WISPr ZD-Style API/ Backup AAA to continue to provide the WISPr service for WISPr survivability.
Accounting Service	Indicates the RADIUS Accounting server that you want to use for this WLAN.	Choose the option. You must have added a RADIUS Accounting server previously. Additionally, if you want the controller to proxy accounting messages to the AAA server, select the **Use the Controller as Proxy** check box. Select: • **Use Controller as Proxy** for the controller to proxy authentication messages to the AAA server • **Use Realm-based profile** to list contents the realm-based profile When the SSH tunnel between the AP and the controller is down, you can enable **Backup Accounting Service** to back up the AP's accounting services to a secondary device. **NOTE** The customer portal must use AP WISPr ZD-Style API/ Backup AAA to continue to provide the WISPr service for WISPr survivability.
Guest Access Portal (for WLAN **Authentication Type**: **Guest Access**)		
Guest Access Service	Indicates the guest access portal to be used on this WLAN.	Choose the guest portal service.
Bypass CNA	Bypasses the Apple CNA feature on iOS and OS X devices that connect to this WLAN.	Select the **Enable** check box.
Portal Detection and Suppression	Designed to allow the operator to set some policy rules that would trigger based on http User-Agent data.	Select the portal detection profile from the list, or click **+** to create a new profile.
Guest Authentication	Manages guest authentication.	Select: • **Guest** to require users to enter their guest pass credentials. Guest passes are managed directly on the controller. • **Always Accept** to allow users without guest credentials to receive authentication.
Guest Accounting	Indicates the RADIUS Accounting server that you want to use for this WLAN.	Choose the server. You must have added a RADIUS Accounting server previously. Additionally, if you want the controller to proxy accounting messages to the AAA server, select the **Use the Controller as Proxy** check box.

TABLE 67 WLAN Configurations (continued)

Field	Description	Your Action
Authentication & Accounting Service (for WLAN **Authentication Type**: **Web Authentication**)		
Web Authentication Portal	Indicates the web authentication portal to use for this WLAN.	Choose the web authentication portal from the list.
Bypass CNA	Bypasses the Apple CNA feature on iOS and OS X devices that connect to this WLAN.	Select the **Enable** check box.
Authentication Service	Indicates the authentication server that you want to use for this WLAN.	Choose the option. Options include **Local DB**, **Always Accept**, and any AAA servers that you previously added. Additionally, if you want the controller to proxy authentication messages to the AAA server, select the **Use the Controller as Proxy** check box.
Accounting Service	Indicates the RADIUS Accounting server that you want to use for this WLAN.	Choose the server. You must have added a RADIUS Accounting server previously. Additionally, if you want the controller to proxy accounting messages to the AAA server, select the **Use the Controller as Proxy** check box.
Hotspot 2.0 Profile (for WLAN **Authentication Type**: **Hotspot 2.0 Access**)		
Hotspot 2.0 Profile	Indicates the profile, which includes the operator and identifies provider profiles.	Choose the profile.
Accounting Service (RFC 5580)	Supports RFC 5580 location delivery on the WLAN, which carries location information in RADIUS exchanges.	Select the check box.
Accounting Service (Updates)	Indicates the frequency to send interim updates. Configures the account update interval for accounting servers defined in the Hotspot 2.0 Identity Provider profile.	Enter the duration in minutes. Range: 0 through 1440.
WeChat Portal (for WLAN **Authentication Type**: **WeChat**)		
WeChat Portal	Defines the WeChat authentication URL, DNAT destination, and other information.	Select a WeChat portal service.
Accounting Server	Indicates the RADIUS Accounting server that you want to use for this WLAN.	Choose the server. You must have added a RADIUS Accounting server previously. Additionally, if you want the controller to proxy accounting messages to the AAA server, select the **Use the Controller as Proxy** check box.
Forwarding Profile (for **WLAN Usage** > **Access Network**)		
Forwarding Policy	Defines special data packet handling to be taken by the data plane when the traffic is tunneled.	**Forwarding Profile** is **Factory Default**. It is disabled.
Options		
Wireless Client Isolation	Prevents wireless clients from communicating with each other.	Enable **Isolate wireless client traffic from all hosts on the same VLAN/subnet**. Enable the following required options as appropriate: • **Isolate unicast packets:** Isolates only unicast packets between a client isolation-enabled client and other clients of the AP. By default, the option is enabled. • **Isolate multicast/broadcast packets:** Isolates only multicast packets between a client isolation-enabled client and other clients of the AP. By default, the option is disabled. • **Automatic support for VRRP:** Isolates packets in VRRP deployment. By default, the option is disabled indicating that the AP is not in a VRRP deployment.

TABLE 67 WLAN Configurations (continued)

Field	Description	Your Action
Isolation Whitelist	Defines wired destinations on the local subnet that can be reached, even if client isolation is enabled. This option is available only if you enable **Wireless Client Isolation**.	Select the option. **NOTE** Isolation Whitelist is not applicable for tunneled WLANs except in the vSZ-D platform.
Priority	Determines high versus low transmit preference of one WLAN compared to another. Traffic for high priority WLANs is always sent before low priority WLANs in the same QoS category (background, best effort, video, voice).	Choose the priority: • **High** • **Low**
RADIUS Option		
NAS ID	Defines the ID sent to the RADIUS server, which will identify the AP.	Choose the option: • **WLAN BSSID** • **AP MAC** • **User-defined**
Delimiter	Delimiter is the way to show MAC format.	Choose the option • **Dash** • **Colon**
NAS Request Timeout	Indicates the duration after which an expected RADIUS response message is considered to have failed.	Enter the timeout period (in seconds). **NOTE** It is recommended to configure the same values for **NAS Request Timeout**, **NAS Max Number of Retries**, and **NAS Reconnect Primary**.
NAS Max Number of Retries	Indicates the maximum number of failed connection attempts after which the controller will fail over to the backup RADIUS server.	Enter the maximum number of failed connection attempts. **NOTE** It is recommended to configure the same values for **NAS Request Timeout**, **NAS Max Number of Retries**, and **NAS Reconnect Primary**.
NAS Reconnect Primary	Indicates the time interval after which the controller will recheck if the primary RADIUS server is available when the controller has failed over to the backup RADIUS server.	Enter the duration in minutes. Range: 1 through 60 minutes. The default interval is 5 minutes. **NOTE** It is recommended to configure the same values for **NAS Request Timeout**, **NAS Max Number of Retries**, and **NAS Reconnect Primary**.
Called Station ID	Indicates the format for the called station ID, which is sent to the RADIUS server as an attribute, and can be used in policy decisions.	Select a format: • **WLAN BSSID** • **AP MAC** • **AP GROUP** • **AP NAME** **NOTE** This field is displayed only for vSZ-H controllers. • **NONE**

TABLE 67 WLAN Configurations (continued)

Field	Description	Your Action
Single Session ID Accounting	Allows the APs to maintain one accounting session for a client roaming between APs. If the client roams from one AP to another, the accounting session ID and statistics will be carried while roaming from one AP to the other. If the feature is not enabled, the accounting session ID is regenerated and the statistics are also reset, essentially resetting the accounting session.	Select the **Enable** check box.
NAS IP	Indicates the NAS IP address.	Select the option: • **Disabled** • **SZ Control IP** • **SZ Management IP** • **User-defined**
Vendor Specific Attribute Profile	Indicates the VSA profile	Select from the following options: • **VSA profiles** **NOTE** VSA profiles are configured at the zone level. • **Disabled** (default) **NOTE** Click  to edit the VSA profile.
Firewall Options		
Firewall Profile	Indicates the zone for which the firewall profile applies.	Select the option.
Enable WLAN specific	Applies the firewall profile to the WLAN.	Select the option and update the following: a. In the **Rate Limiting** field, select the **Uplink** and **Downlink** option to specify and apply rate limit values for the device policy to control the data rate. b. Select the **L3 Access Control Policy** from the drop-down list or click  to create a new policy. Refer Create an L3 Access Control Policy on page 380 for more information. c. Select the **L2 Access Control Policy** from the drop-down list or click  to create a new policy. Refer Creating an L2 Access Control Service on page 382 for more information. d. Select the **Application Policy** from the drop-down list or click  to create a new policy. Refer Creating an Application Control Policy on page 373 for more information. e. Select the **URL Filtering Profile** from the drop-down list or click  to create a new profile. Refer Creating a URL Filtering Policy on page 385 for more information. f. Select the **Device Policy** from the drop-down list or click  to create a new policy. Refer Creating a Device Policy on page 390 for more information.

TABLE 67 WLAN Configurations (continued)

Field	Description	Your Action
Application Recognition and Control	Enables DPI-based Layer 7 application recognition, and if enabled, an application control policy. Recognition and control are performed on the AP.	Select the option.
Client Virtual ID Extraction	Extracts the Virtual IDs of the users who login into the social media , public email such as wechat, whatsapp, hotmail, and cloud disk, and send these virtual ids to the auditing system.	**NOTE** To enable the Client Virtual ID Extraction, enable Application Recognition Control, and ensure that Sigpack contains regular version.
URL Filtering	Enables URL filtering on the WLAN controller to block or allow access to specific websites or web pages.	Select the option.
Advanced Options		
Client Fingerprinting	Enables the AP to attempt to utilize DHCP fingerprinting to identify client devices by their operating system, device type, and host name.	Select the check box.
Wi-Fi Calling	When Wi-Fi calling is enabled by the mobile carrier, an IPSec tunnel is established between the phone and the mobile network through which calls are routed.	Click **Select**, and choose the WiFi calling profile that you want to apply to WLAN.
Access VLAN	Tags the WLAN traffic with a VLAN ID from 2 through 4094. By default, all client traffic will be assigned to the native (untagged) VLAN on the AP's Ethernet port, which is represented as VLAN ID 1.	Select the check box and enter the **VLAN ID**. Enable **Enable VLAN Pooling** to assign the VLAN pooling profile to a specific WLAN or override the VLAN settings of a WLAN group. Select the VLAN pooling profile from the list or create a new profile by clicking "+". Select **Enable Dynamic VLAN** if you want the controller to assign VLAN IDs on a per-user basis.
Hotspot 2.0 Onboarding	Allows devices to connect to a Wi-Fi network automatically, wherein the service providers engage in roaming partnerships to provide seamless access to Wi-Fi networks. The devices are authenticated using credentials or certificates.	Select the check box to allow Hotspot 2.0 Onboaring for the WISPr WLAN.
Hide SSID	Removes the SSID from beacon frames. By removing the SSID, in most cases, clients will not show this SSID in their scan list unless the device is already configured to connect. This can simplify the network decision for an end user.	Select the check box.
Client Load Balancing	Disables client load balancing on this WLAN if the option is selected.	Select the check box to disable client load balancing on this WLAN.
Proxy ARP	Enables proxy ARP. When proxy ARP is enabled on a WLAN, the AP provides ARP response service for stations. When the AP receives an ARP request for a known host, it replies with an ARP response on behalf of the host. If the AP receives a request for an unknown host, it forwards the request.	Select the check box.

TABLE 67 WLAN Configurations (continued)

Field	Description	Your Action
DGAF	Disables AP from forwarding downstream group-addressed frames. This option is available only when proxy ARP is enabled.	Select the option.
ND Proxy	Enables Neighbor Discovery proxy. When ND proxy is enabled on a WLAN, the AP provides Neighbor Advertisement service for stations. When the AP receives a Neighbor solicitation request for a known host, it replies with a Neighbor Advertisement on behalf of the host. If the AP receives a request for an unknown host, it forwards the request. **NOTE** This feature is available only on IPv6 and Dual zone and is enabled by default.	Enable the option.
Suppress NS	Suppress Network Solicitation (NS) on a wireless medium when there is no Station entry available in the cache. This feature can be configured only when the **ND Proxy** option is enabled. **NOTE** This feature is available only on IPv6 and Dual zone and is disabled by default.	Enable the option.
RA Proxy	Enables Router Advertisement proxy. When RA proxy is enabled on a WLAN, the AP provides Router Advertisement service for wireless stations. When the AP receives a Router solicitation request on a WLAN, it replies with a Router Advertisement on behalf of the routers available on the network learned by the AP. If the router entries are not found in the cache, the AP forwards the request. **NOTE** This feature is available only on IPv6 and Dual zone and is enabled by default.	Enable the option.
RS/RA Guard	Prevents Router Solicitation (RS) from the wired side of the network to a wireless side. Also prevents Router Advertisement (RA) from a wireless side of the network to the wired side. This feature can be configured only when the **RA Proxy** option is enabled. **NOTE** This feature is available only on IPv6 and Dual zone and is disabled by default.	Enable the option.

TABLE 67 WLAN Configurations (continued)

Field	Description	Your Action
RA Throttling	Regulates the multicast Router Advertisement (RA) from a wired medium to a wireless medium based on the configured **Max Allowed RA** and **Interval**. This feature can be configured only when **RA Proxy** is enabled. **NOTE** This feature is available only on IPv6 and Dual zone and is disabled by default.	• **Max Allowed RA**: Enter the maximum number of Router Advertisements (RAs) allowed per minute. Range: 1 through 1440, default 10 • **Interval**: Enter the regulating frequency in minutes. Range: 1 through 256, default 10
MAX Clients	Limits the number of clients that can associate with this WLAN per AP radio (default is 100). Every connection attempt after this maximum value will not be permitted to connect.	Enter the number of clients allowed.
802.11d	Adds additional regulatory information to AP beacons and probe responses. This compliance information provides country-specific guidance such as permitted channels and transmit power, to ensure that the devices operate within the legal boundaries of the country. 11d is helpful for many devices that cannot independently determine their operating country.	Enable the option.
802.11k Neighbor Report	Enhances roaming by providing a list of neighbor APs to the client device. APs build a neighbor AP list via background scanning, and when the client plans to roam, it will request this list from the AP. This list is then used to perform efficient scanning to find a roaming candidate.	Enable the option.

TABLE 67 WLAN Configurations (continued)

Field	Description	Your Action
Anti-spoofing	Prevents attacks on genuine clients from rogue clients that could lead to service disruption, data loss, and so on. This is achieved by matching the MAC address or IP address (IPv4) of the client with the address in the Ruckus database. If the addresses do not match, the packet is dropped. These checks are also performed on ingress data packets to catch spoofed data packets early.	Enable the option. By default, the following options are also enabled: • ARP request rate limit: Enter the packets to be reviewed for Address Resolution Protocol (ARP) attacks, per minute. In ARP attacks a rouge client sends messages to a genuine client to establish connection over the network. • DHCP request rate limit: Enter the packets to be reviewed for DHCP pool exhaustion per minute. When rouge clients send a DHCP request with a spoofed address, an IP address from the DHCP pool is assigned to it. If this happens repeatedly, the IP addresses in the DHCP pool are exhausted, and genuine clients may miss out on obtaining the IP addresses. **NOTE** When you enable anti-spoofing, an ARP request and DHCP request rate limiter is automatically enabled with default values (in packets per minute, or ppm) which are applied per client; implying that each client connected to an interface enabled with anti-spoofing is allowed to send a maximum of "X" ARP/DHCP request ppm. The value "X" is configured on the interface that the client is connected. **NOTE** The Force-DHCP option will be enabled by default when anti-spoofing is enabled, and it cannot be changed after anti-spoofing is enabled.
Force DHCP	Requires the clients to obtain a valid IP address from DHCP within the specified number of seconds. This prevents clients configured with a static IP address from connecting to the WLAN. Additionally, if a client performs Layer 3 roaming between different subnets, in some cases the client sticks to the former IP address. This mechanism optimizes the roaming experience by forcing clients to request a new IP address.	Select the check box.
DHCP Option 82	Enables an AP to encapsulate additional information (such as VLAN ID, AP name, SSID, and MAC address) into DHCP request packets before forwarding them to the DHCP server. The DHCP server uses this information to allocate an IP address to the client from a particular DHCP pool based on these parameters.	Enable the **On/Off** button. **NOTE** The options are displayed only if the **On** is enabled.

TABLE 67 WLAN Configurations (continued)

Field	Description	Your Action
DHCP Option 82 Format	Enables an AP to encapsulate additional information into DHCP request packets before forwarding them to the DHCP server. The DHCP server uses this information to allocate an IP address to the client from a particular DHCP pool based on these parameters.	Enable the required format: • **Subopt-1 with format** and select the option. The options are : – **IF-Name:VLAN-ID:ESSID:AP-Model:AP-Name:AP-MAC:Location** – **IF-Name:VLAN-ID:ESSID:AP-Model:AP-Name:AP-MAC** – **AP-MAC;ESSID;PRIVACY-TYPE** – **AP-MAC-hex** – **AP-MAC-hex ESSID** – **ESSID** – **AP-MAC** – **AP-MAC ESSID** – **AP-NAME ESSID** • **Subopt-2 with format** and select the option. The options are: – **Client-MAC** – **Client-MAC-hex** – **Client-MAC-hex ESSID** – **AP-MAC** – **AP-MAC-hex** – **AP-MAC-hex ESSID** – **AP-MAC ESSID** – **AP-NAME** • **Subopt-150 with VLAN-ID**. • **Subopt-151 with format** and select the option. • **Mac format delimiter**, choose the MAC format from the drop-down list.
DTIM Interval	Indicates the frequency at which the Delivery Traffic Indication Message (DTIM) will be included in Beacon frames.	Enter the frequency number. Range: 1 through 255.

TABLE 67 WLAN Configurations (continued)

Field	Description	Your Action
Directed MC/BC Threshold	Defines the per-radio-client count at which an AP stops converting group-addressed data traffic to unicast. However, the Directed Threshold logic is only one part of the access points' multicast handling logic, which means there may be other factors that determine whether a frame is transmitted as unicast or multicast. APs support a feature called Directed Multicast (configurable only on AP CLI, enabled by default), which adds additional logic to the multicast flow. If Directed Multicast is disabled, the AP uses the Directed Threshold as the only criteria to determine whether to transmit a multicast packet as unicast. However, when Directed Multicast is enabled, the flow is changed. Directed Multicast is a feature that checks to see if a multicast packet is well-known or not. For well-known multicast packets, for example, Bonjour, uPNP, most IPv6 link- and node-local, and Spectralink, the AP still applies the Directed Threshold logic to determine conversion to unicast. For non well-known types, the AP monitors and maintains a database of client subscriptions using IGMP and MLD. If associated clients are subscribed to the multicast stream, then the AP always converts these packets to unicast, regardless of the Directed Threshold configuration. If there are no clients subscribed to the multicast stream, the AP drops these packets. It is important to be aware of this behavior when validating multicast operation in a deployment.	Enter the client count number. Range: 0 through 128.
Client Tx/Rx Statistics	Stops the controller from monitoring traffic statistics for unauthorized clients.	Select the check box.
User Session Timeout	Indicates the duration after which idle clients will be disconnected. **NOTE** Before getting disconnected the client can be either in an idle state or connected to the WLAN (SSID).	Enter the duration. Range: 120 to 864000 seconds (10 days). Default Value: 172800 seconds (2 days). **NOTE** This default value will remain effected only when the session timeout is not applied from the Radius server. **NOTE** The user session timeout is displayed only for those WLANs in which 802.1X or MAC authentication is enabled.

TABLE 67 WLAN Configurations (continued)

Field	Description	Your Action
User Session Timeout	Indicates the duration after which the client gets disconnected. **NOTE** Before getting disconnected the client can be either in an idle state or connected to the WLAN.	Enter the duration. Range: 120 to 864000 seconds (10 days). Default Value: 172800 seconds (2 days). **NOTE** This default value will remain effected only when the session timeout is not applied from the Radius server.
WiFi 6	Allows legacy Wi-Fi 5 clients with outdated drivers to interoperate with a Wi-Fi 6 AP. Use this option to disable Wi-Fi 6 if the client drivers on the network are not the latest or are free of bugs. Wi-Fi 6 clients connecting to a WLAN with Wi-Fi 6 disabled on a Wi-Fi 6 AP will not be able to use Wi-Fi 6 features such as the OFDMA and TWT. **NOTE** Wifi 6 feature is supported for the firmware release 5.2.1 and above.	Select the option.
OFDM Only	Disconnects 802.11b devices from the WLAN and all devices are forced to use higher data rates for more efficient airtime usage. This setting only affects the 2.4-GHz radio. OFDM is used by 802.11a, g, n, and ac, but is not supported by 802.11b.	Select the check box.
BSS Min Rate	Forces client devices to be both closer to the AP and to use higher, more efficient rates when you increase the BSS minimum rate above the default (all rates) setting. The BSS minimum rate is the lowest data rate supported on the WLAN. When OFDM-only is enabled, it takes higher priority than BSS minimum rate settings.	Select the option.
Mgmt Tx Rate	Sets the transmit rate for management frame types such as beacon and probes.	Select the value.
6G BSS Min Rate	Forces client devices to both be closer to the AP and to use higher, more efficient rates when you increase the BSS minimum rate above the default (all rates) setting. The BSS minimum rate is the lowest data rate supported on the WLAN. When OFDM-only is enabled, it takes higher priority than BSS minimum rate settings.	Select one of the following option: • 6 mbps • 9 mbps • 12 mbps • 18 mbps • 24 mbps

TABLE 67 WLAN Configurations (continued)

Field	Description	Your Action
6G Mgmt Tx Rate	Sets the transmit rate for management frame types such as beacon and probes.	Select one of the following option: • 6 mbps • 9 mbps • 12 mbps • 18 mbps • 24 mbps
Service Schedule	Controls when the WLAN service is active. The purpose of this setting is to automatically enable or disable a WLAN based on a predetermined schedule. By default, the service is **Always On**. **Always Off** can be selected in order to create a WLAN and apply it, but prevent it from advertising until ready. The **Specific** setting allows a configurable schedule based on time of day and days of the week. **NOTE** When a service schedule is created, it is saved by the SZ and AP using the time zone of the browser. When it is enforced by the AP, the AP will enforce it according to the time zone of the browser when it was configured.	Choose the option: • **Always On** • **Always Off** • **Specific** and select a schedule profile from the drop-down list.
Band Balancing	Disables band balancing only for this WLAN, if you select the check box.	Select the **Disable band balancing for this WLAN service** check box.
Qos Map Set	Reprioritizes downlink packets based on the configured mappings. When an AP receives a downlink packet, it checks the existing DSCP (Layer 3 QoS) marking, compares it to this map set, and then changes the user priority (Layer 2 QoS) values for transmission by the AP. To configure this feature, select the User Priority (UP) from the table (0-7) and configure the DSCP (0-64) range that will be mapped to this UP. Exceptions can also be added such that the original DSCP and UP tagging are preserved and honored by the AP.	To configure this feature, select the User Priority (UP) from the table (0-7) and configure the DSCP (0-64) range that will be mapped to this UP. Select **Enable QOS Map Set**.
Multicast Filter	Drops the broadcast and multicast from the associated wireless clients.	Click to enable this option.
SSID Rate Limiting	Enforces an aggregate rate limit for all users of the WLAN. The purpose of this feature is to prevent the combined throughput from all users of an SSID from exceeding this threshold. This feature is different from per-user rate limiting, which enforces the same rate limit for each individual device.	Select the **Uplink** and **Downlink** check boxes and enter the limiting rates in mbps, respectively. Range: 1 through 200 Mbps.

TABLE 67 WLAN Configurations (continued)

Field	Description	Your Action
Multicast Rate Limiting	Multicast rate limit can be configured at WLAN level. The **UplinkDownlink** values are displayed only if the multicast rate limit is enabled. The **Downlink** traffic is limited to 50% of the configured multicast rate limiting. For example, if multicast rate limiting downlink traffic is set to 6Mbps, only ~50%, .i.e. 3.00Mbps to 4.00Mbps max per second traffic passes. This limit is only for downlink and shall not be affected by BSS Min Rate setting. **NOTE** SSID Rate Limit always take precedence, if, Mutlicast Rate Limit is also configured.	Select the **Uplink** and **Downlink** check boxes and enter the limiting rates in Mbps, respectively. Range: 1 through 100 Mbps. **NOTE** Multicast Rate Limit value cannot exceed SSID Rate Limit values for respective **Uplink** and **Downlink** direction.
DNS Server Profile	Allows the AP to inspect DHCP messages and overwrite the DNS servers with the DNS server configured in this profile. This allows for policy-based DNS application in which unique users/roles should use a different DNS server than others.	Select a profile from the menu. Select **Disable** from the menu if you want to disable the DNS Server profile for the WLAN service. Click  to add a new profile or click  to edit a profile.
DNS Spoofing Profile	When an AP receives a DNS packet, all the fields in the packet are validated. **NOTE** Only A/AAA server DNS query packets are considered. When same domain name is present in both DNS spoofing profile and walled garden table in the WISPr WLAN, then the AP DNS cache is updated with the IP address present in the DNS spoofing profile. If DNS spoofing and URL filtering with safe search is enabled, URLfiltering (safe search) takes precedence for the Google, YouTube, and Bing domain names. If safe search is not enabled, DNS spoofing takes the precedence. If safe search is not enabled and URL filtering is enabled also DNS-Spoof takes the precedence.	Select a profile from the menu. Select **Disable** from the menu if you want to disable the DNS Spoofing profile for the WLAN service. Click  to add a new profile or click  to edit a profile

TABLE 67 WLAN Configurations (continued)

Field	Description	Your Action
Precedence Profile	Defines the relative policy assignment priority for some specific settings. For example, if a WLAN is configured to use VLAN 10, and an AAA/role policy is configured for VLAN 20, and a device OS policy is configured for VLAN 30, and a user/device connects to the WLAN matching all of these policies, which VLAN should be assigned. The precedence policy determines which setting takes priority.	Select the option. Click  to add a new profile or click  to edit a profile.
CALEA (This feature is supported only for SZ300 controllers.)	Intercepts traffic, a requirement enforced on some networks by government agencies. To utilize CALEA, you must support a vSZ-D and configure the CALEA settings in the **Services & Profiles** > **Tunnels & Ports** menu.	Select the check box. **NOTE** If there are more than 40 DPs been approved, SZ limit user to use CALEA feature.
Venue Code(This field is displayed only for vSZ-H controllers.)	Indicates venue code.	Select check box to log the client-flow data to the external syslog server. Then enable AP syslog functionality from the zone settings.
Client Flow Data Logging	Sends a log message with the source MAC address, destination MAC address, source IP address, destination IP address, source port, destination port, Layer 4 protocol, and AP MAC address of each packet session to the external syslog server. This function is provided by the AP syslog client (not the SZ syslog client), which must be enabled at the zone level in order to support this client flow logging.	Select the check box to log the client-flow data to the external syslog server. Then enable AP syslog functionality from the Zone settings.
Airtime Decongestion	Mitigates airtime congestion caused by management frames in high-density deployments.	Select the check box.
Join RSSI threshold	Indicates the signal threshold that could connect to the Wi-Fi. If **Airtime Decongestion** is enabled, **Join RSSI threshold** is automatically disabled.	Enter the Client RSSI threshold to allow joining. Range: -60 through -90 dBm.
Transient Client Management	Discourages transient clients from joining the network.	Select enable **Transient Client Management** and set the following parameters: • **Join wait time**—Enter the wait time before a client can be permitted to join. Range: 1 through 60 secs. • **Join expire time**—Enter the time during which a rejoin request is accepted without delay. Range: 1 through 300 secs. • **Join wait threshold**—Enter the number of join attempts after which a client is permitted to join even before the join wait time expires.
Optimized Connectivity Experience (OCE)	OCE enables probe response suppression and prevents devices with marginal connectivity from joining the network. Optimizes the connectivity experience for OCE-enabled APs and stations.	Select **Optimized Connectivity Experience (OCE)** and set the following parameters: • **Broadcast Probe Response Delay**: Indicates the time delay to transmit probe response frames in milliseconds. • **RSSI-based Association Rejection Threshold**: Indicates the minimum threshold value to connect to the network (in dBm). If the value entered is less than the minimum threshold value, then any RSSI-based association is rejected.

4. Click **OK**.

For SZ300 and vSZ-H, you can also migrate the WLAN configuration from a regular Domain to a Partner Domain. For more information, see https://support.ruckuswireless.com/answers/000006414.

NOTE
You can edit, clone, and delete WLANs by selecting the options **Configure**, **Clone**, and **Delete** respectively, from the **Wireless LANs** page.

NOTE
From the **Wireless LANs** page, you can also select **More** and perform the following operations:

- **Select All**: Select all WLANs in the list.
- **Deselect All**: Clear all WLAN selections from the list.
- **Enable**: Enable a WLAN from the list.
- **Disable**: Disable a WLAN from the list.

In the WLAN list, the **Status** column indicates whether the WLAN configuration is active or inactive. Though a WLAN is disabled by a time schedule, its configuration will remain active.

802.11r Fast BSS Transition

802.11r Fast BSS Transition is a fast roaming protocol that reduces the number of frame exchanges required for roaming and allows the clients and APs to reuse the master keys obtained during a prior authentication exchange. 802.11r is most helpful for 802.1X networks. Client support is required for 802.11r to work.

A Mobility Domain ID is used by 802.11r to define a scope of the network in which fast roaming is supported. Master keys are shared within the Mobility Domain, allowing clients to support fast roaming.

802.11w Management Frame Protection

802.11w Management Frame Protection (MFP) provides additional security measures for management frames. Not all client devices support 802.11w.

Check your client devices before enabling 11watts. If “Required” is selected, client device must support 11watts in order to connect. If “Capable” is selected, client device with or without 11watts should be able to connect. However, note that some client devices with poor driver software may have connection issues even if 11watts is set to "Capable".

Airtime Decongestion

NOTE
Ensure that **Background Scan** is enabled.

The Airtime Decongestion feature optimized the Wi-Fi management traffic in a network where the amount of management traffic can potentially consume a significant portion of airtime thereby reducing the amount of time available for traffic. This feature controls the RSSI threshold setting for Transient Client Management. Enabling this feature disables the **RSSI threshold** configuration in **Transient Client Management**.

Band Balancing

Band balancing balances the client load on radios by distributing clients between the 2.4-GHz and 5-GHz radios.

Band balancing is enabled by default and set to a target of 25 percent of clients connecting to the 2.4-GHz band. You must enable this setting in the advanced option that comes under zone configuration. To balance the load on a radio, the AP encourages dual-band clients to connect to the 5-GHz band when the configured percentage threshold is reached. To turn-off the band balancing, go to the advanced option in WLAN configuration.

FIGURE 78 Load Balancing

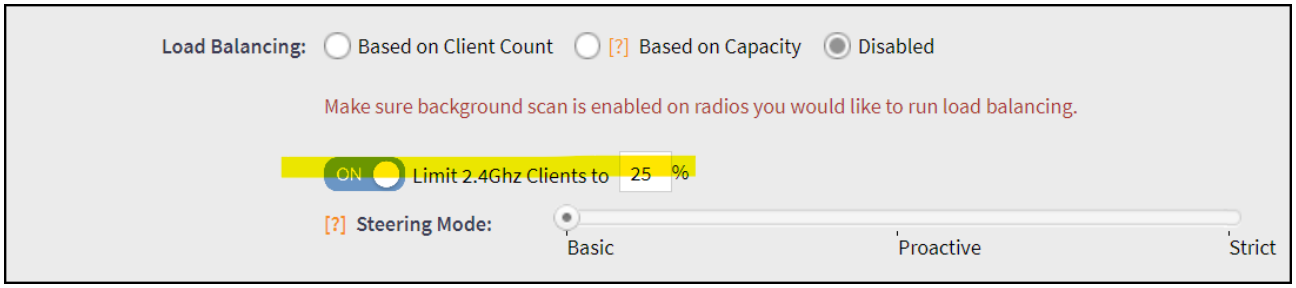
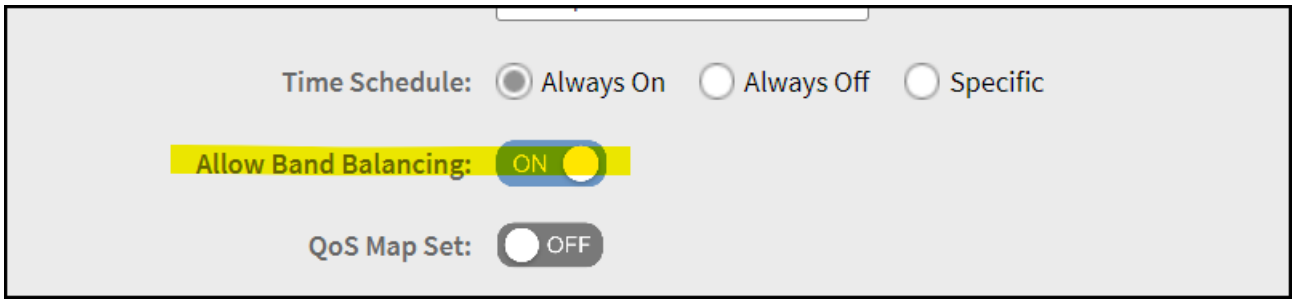


FIGURE 79 Band Balancing



Bypassing Apple CNA

Some Apple iOS and OS X clients include Captive Network Assistant (CNA), which allows clients to connect to an open captive portal WLAN without displaying the login page.

When a client connects to a wireless network, the CNA launches a pre-browser login utility and it sends a request to a success page on the Apple® website. If the success page is returned, the device assumes it has network connectivity and no action is taken. However, this login utility is not a fully functional browser, and does not support HTML, HTML5, PHP, or other embedded video. In some situations, the ability to skip the login page for open WLANs is a benefit. However, for other guest or public access designs, the lack of ability to control the entire web authentication process is not desirable.

The controller provides an option to work around Apple CNA if it is not desirable for your specific deployment. With CNA bypass enabled, captive portal (web-based authentication) login must be performed by opening a browser to any unauthenticated page (HTTP) to get redirected to the login page.

Band or Spectrum Configuration

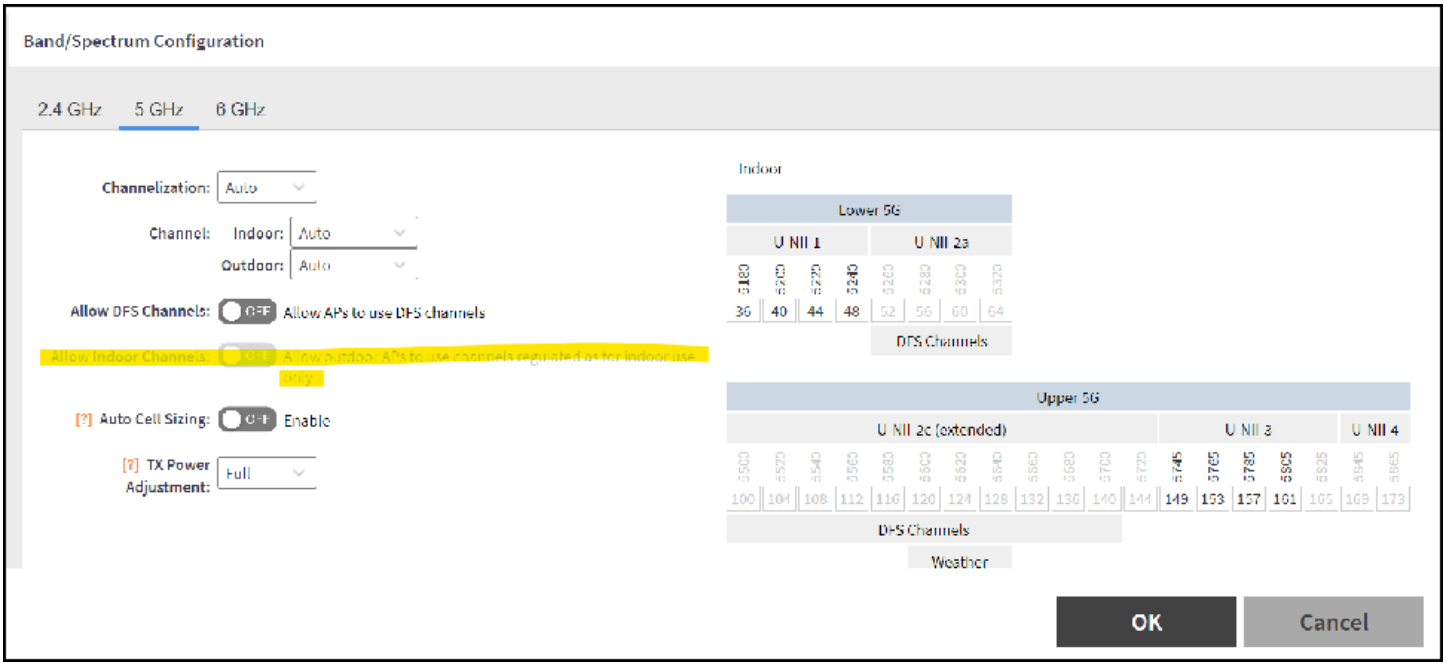
Band or spectrum configuration is a method of statistically picking the most potent channel for an AP.

NOTE
This feature is applicable only for SZ300 and vSZ-H platforms.

Some countries restrict certain 5-GHz channels to indoor use only. For instance, Germany restricts channels in the 5.15-GHz to 5.25-GHz band to indoor use. When ZoneFlex Outdoor APs and Bridges with 5-GHz radios (ZoneFlex 7762, 7762-S, 7762-T, 7761-CM, and 7731) are set to a country code where these restrictions apply, the AP or Bridge can no longer be set to an indoor-only channel and will no longer select from amongst a channel set that includes these indoor-only channels when SmartSelect or Auto Channel selection is used, unless the administrator configures the AP to allow use of these channels.

For instance, if the AP is installed in a challenging indoor environment (such as a warehouse), the administrator may want to allow the AP to use an indoor-only channel. These channels can be enabled for use through the AP CLI or the controller web interface.

FIGURE 80 Band or Spectrum Configuration



Client Admission Control

Client admission control allows APs to adaptively allow or deny the association of clients based on the potential throughput of the currently associated clients. This helps prevent APs from becoming overloaded with clients and improves user experience for wireless users.

As an administrator, you can help maintain a positive user experience for wireless users on the network by configuring the following client admission control settings:

- Minimum client count - 0 - 100. To set minimum client control to 0, select Client Admission Control threshold.
- Maximum radio load (%) - 50 - 100
- Minimum client throughput (Mbps) - 0 -100

Client admission control is implemented on a per radio basis and is supported on 802.11n and 802.11ac APs.

NOTE
Client admission control cannot be enabled if client load balancing/band balancing (or both) is enabled.

NOTE
If you are trying to steer clients to the appropriate band (band steering), please refer Band Balancing on page 204 section.

Client Load Balancing

Enabling load balancing can improve WLAN performance by helping to spread the wireless client load between nearby access points, so that one AP does not get overloaded while another sits idle.

Load balancing can be controlled from within the controller web interface to balance the number of clients per radio on adjacent APs.

Adjacent APs are determined by the controller at startup by measuring the RSSI during channel scans. After startup, the controller uses subsequent scans to update the list of adjacent APs periodically and when a new AP sends its first scan report. When an AP leaves, the controller immediately updates the list of adjacent APs and refreshes the client limits at each affected AP.

Once the controller is aware of which APs are adjacent to each other, it begins managing the client load by sending the configured client limits to the APs. These limits are soft values that can be exceeded in several scenarios, including:

- When a client signal is so weak that it may not be able to support a link with another AP
- When a client signal is so strong that it really belongs on this AP.

The APs maintain these configured client limits and enforce them once they reach the limits by withholding probe responses and authentication responses on any radio that has reached its limit.

> **NOTE**
> Adaptive Client Load Balancing (ACLB) is not supported on AP R730 in SmartZone 5.1.1 release. The R730 AP supports only legacy client load balancing (CLB). The R730 AP is supported only in SZ6.1.0 firmware zone. ACLB is disabled by default if capacity mode is configured on the controller. If station mode is configured, ACLB acts as legacy CLB on the AP.

Client Load Balancing Considerations

Before you enable load balancing, keep the following considerations in mind:

- The load balancing rules apply only to client devices; the AP always responds to another AP that is attempting to set up or maintain a mesh network.
- Load balancing does not disassociate clients already connected.
- Load balancing takes action before a client association request, reducing the chance of client misbehavior.
- Load balancing does not require any time-critical interaction between APs and the controller.
- Provides control of adjacent AP distance with safeguards against abandoning clients.
- Load balancing can be disabled on a per-WLAN basis. For instance, on a voice WLAN, load balancing may not be desired due to voice roaming considerations.
- Background scanning must be enabled on the WLAN for load balancing to work.

Mobility Domain ID

A Mobility Domain ID is used by 802.11r to define a scope of the network in which an 11r fast roaming is supported. Master keys are shared within the Mobility Domain, allowing clients to support fast roaming.

Portal-Based WLANs

There are many types of portal-based WLANs and they can be distinguished based on where the user credentials are stored, and where the portal page is hosted.

TABLE 68 Portal-based WLANs

WLAN Type	User Credential	Portal on Which WLAN is Hosted
Guest	Guest passes on the controller	AP
Hotspot (WISPr)	RADIUS server; LDAP/Active Directory from SmartZone 3.2 and later	External portal server or internal portal on the controller
WebAuth	RADIUS/LDAP/Active Directory	AP

Guest and WebAuth WLAN portals are hosted on the controller AP with limited customization.

WISPr WLANs are usually hosted on external portal servers providing the flexibility to customize. WISPr WLANs allow for sophisticated customization such as providing a customized login page which could include locale information, advertisements and so on.

WISPr WLANs can also be configured to bypass the authentication portal so that if the MAC address of an end user device (used as a credential) is stored on a RADIUS server, there is no need to redirect the end user to the portal server for authentication.

Portal-Based WLANs Characteristics

Portal-based WLANs have the following characteristics:

WebAuth WLANs have the following characteristics:

- Does not provide an option to modify the portal (WYSIWYG)
- Handles user authentication by the RADIUS server, LDAP, and Active Directory
- Allows redirecting of user web pages

Guest WLANs have the following characteristics:

- Provides an option to modify the portal elements such as the logo, Terms and Conditions, title, and so on
- Handles user authentication by using guest passphrases (or selecting the **Always Accepted**option)
- Allows redirecting of user web pages
- Does not possess a local database, LDAP, Active Directory, or RADIUS server

Hotspot (WISPr) WLANs (Internal Portal) have the following characteristics:

- Internal Portal
  - Provides an option to modify the portal elements such as the logo, Terms and Conditions, title, and so on
  - Handles user authentication by the local database, LDAP, Active Directory, RADIUS server (or selecting the **Always Accepted** option)
  - Allows redirecting user web pages
  - Supports the Walled Garden approach to allow user access to specific areas within the network
- Hotspot (WISPr) WLANs (External Portal) have the following characteristics:
  - Allows customization of the portal pages through external services
  - Supports Northbound Portal Interface for authentication
  - Handles user authentication by the local database, LDAP, Active Directory, RADIUS server (or selecting the **Always Accepted** option)
  - Allows redirecting of user web pages
  - Supports the Walled Garden approach to allow user access to specific areas within the network

Multicast Rate Filter

All the controller managed APs support this feature. The GUI for rate limit control is designed as:

- **FIGURE 81** Multicast Rate Limiting



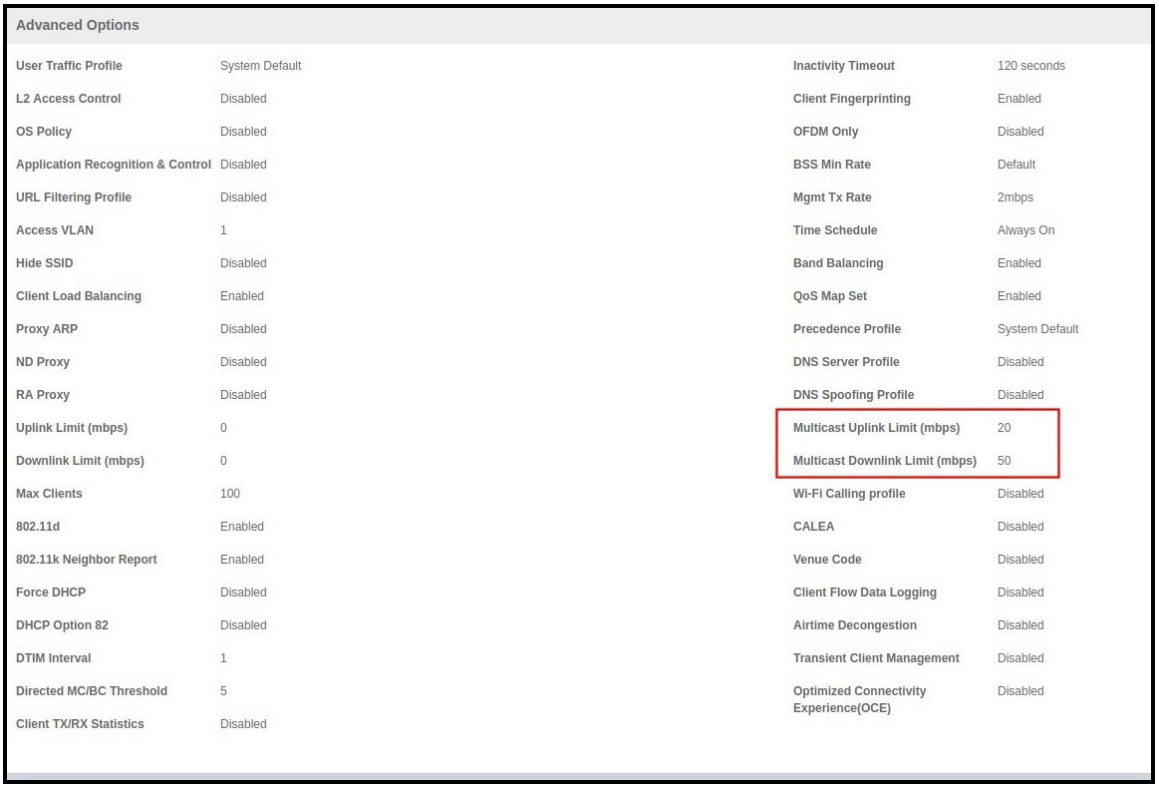
Configuring the Multicast rate limit

- Multicast Downlink/Uplink Rate Limit should be configured at WLAN level.
- Multicast Rate Limit and Drop Multicast/Broadcast Traffic from Associated Wireless Clients are mutually exclusive feature.
- Mutlicast UL/DL values should be shown only if Mutlicast Rate limit is enabled.

- Downlink value default is u to 6 mbps. The range of multicast values depends on the BSS minimum rate selection in the wlan and a maximum of half of the BSS minimum rate.
- SSID Rate Limit will always take precedence if Mutlicast Rate Limit is also configured.

Add Multicast Rate Limiting Uplink and Downlink Fields in Advanced Option of WLAN

FIGURE 82 Configuring the Multicast Rate Limit



User can check multicast uplink and downlink fields in WLAN preview.

FIGURE 83 WLAN Preview



Rate Limiting Ranges for Policies

You can define and apply rate limit values for user devices to control the data rate and types of network traffic the device transmits.

NOTE
For SmartZone release 3.4 and 3.2.x, the APs support the following rate limiting values:

- 0.10Mbps
- 0.25Mbps - 20.00Mbps (increments by 0.25Mbps)
- 21.00Mbps - 200.00Mbps (increments by1.00mpbs)

For example, typing 6.45 Mbps maps to the closest predefined rate value, so 6.45Mbps will be rendered as 6.50Mbps.

NOTE
For SmartZone release 3.1.x, the APs support the following rate limiting values:

- 0.10Mbps
- 0.25Mbps - 20.00Mbps (increments by 0.25Mbps)
- 30.00Mbps
- 40.00Mbps
- 50.00Mbps

For example, typing 31.50 Mbps maps to the closest predefined rate value, so 31.50 Mbps will be rendered as 40 Mbps. Any rate greater than 50.00Mbps would be mapped to the maximum rate which is 50.00Mbps.

TABLE 69 Rate Limiting ranges for different controller policies

Policy	Global or Zone	Rate limit range for zone running SmartZone 3.4	Rate limit range for zone running SmartZone 3.2.x	Rate limit range for zone running SmartZone 3.1.x
Device Policy	Zone	0.1 Mbps to 200 Mbps Support uni-direction (Uplink and Downlink need not be enabled or disabled at the same time)	0.1 Mbps to 200 Mbps No support for uni-direction (Uplink and Downlink need not be enabled or disabled at the same time)	0.1 Mbps to 200 Mbps. But any rate greater than 50Mbps will be mapped to 50 Mbps implicitly on the AP side when the rate is applied. No support for uni-direction
User Traffic Profile	Global	0.1 Mbps to 200 Mbps No support for uni-direction because this is Global profile that is used by 3.2.x and 3.1.x APs	0.1 Mbps to 200 Mbps No support for uni-direction	But any rate greater than 50Mbps will be mapped to 50 Mbps implicitly on the AP side when the rate is applied. No support for uni-direction

Transient Client Management

Transient Client Management allows only those clients that stay within the coverage region of the AP for a minimum period of time to associate with the AP and use the network service. For example, in a train station or downtown area, there may be passersby who do not intend to connect and utilize the network service. However, their Wi-Fi devices may conduct an active/passive scanning and may be roaming from cellular to Wi-Fi, from one Wi-Fi AP to another Wi-Fi AP, or from Wi-Fi to cellular, which could compromise the experience of users who are connected and using the network service. First-time client association may be delayed.

Transient Client Management uses statistical methods to delay the association of transient clients to an AP. Venue administrators will be able to tune configuration parameters based on typical observed dwell times and RSSI of transient clients. Transient Client Management delivers efficient airtime utilization and minimizes cellular-to-Wi-Fi handoffs and AP-to-AP roaming of transient clients.

Optimized Connectivity Experience

Optimized Connectivity Experience (OCE) delivers a better overall connectivity experience by enabling probe response suppression and by preventing devices with marginal connectivity to join the network.

When OCE is enabled, the affected APs and stations are excluded from Airtime Decongestion and Transient Client Management, resulting in reduction in probe response. Probe response suppression optimizes airtime for data traffic. OCE solves connectivity issues by rejecting any association with clients with poor signals.



VIDEO
Optimized Connectivity Experience. This video provides a brief overview of Optimized Connectivity Experience.
Click to play video in full screen mode.

Fast Initial Link Setup (FILS)

Enable Fast Initial Link Setup (FILS) for 802.1X EAP WLAN and select the realm-based AAA configuration and DHCP server IP address.

Combines the authentication, authorization, and DHCP to reduce EAP frames and skip EAPOL 4-way handshake when station reconnects or roams. It requires AAA to support Higher Layer Protocol (HLP) and EAP-RP. The DHCP server requires the Rapid commit. The following WLAN feature combinations are supported by FILS:

- 802.1x(FILS) + WISPr
- 802.1x(FILS) + MAC Auth
- 802.1x(FILS) + 802.11w
- 802.1x(FILS) + FT

NOTE
FILS provides MAC support. When FILS is enabled, the DHCP Rapid Commit Proxy is also enabled by default. However, it is hidden in the screen.

Create FILS Realm Profile

To create FILS Realm Profile, perform the following:

1. Go to **Security** > **Authentication** > **FILS Realm Proxy**.

   This displays **Create FILS Realm Profile** screen.
2. In the **Create FILS Realm Profile** screen, enter the following details:
   - Name: Enter name for the profile.
   - Description: Enter a short description for the profile.
   - Realms: Enter a Realm Name and click **Add**.

     The Realm Name is displayed below.
   - Click **Ok**.

   The new profile is displayed in the **FILS Realm Profile** screen.

NOTE
The **FILS Realm Profile** can be created from the **Fast Initial Link Setup** by clicking **+** corresponding to the **Realm Profile**.

Working with Time Schedule Profiles

A **Time Schedule** profile specifies the hours of the day or week during which a WLAN service is enabled or disabled.

For example, a WLAN for student use at a school can be configured to provide wireless access only during school hours. This example involves creating a time schedule profile, and when configuring a WLAN, selecting the schedule profile to enable or disable the WLAN service during those days and hours.

NOTE
Creating a Time Schedule profile will not work properly if the system does not have the correct time. To ensure that the system always maintains the correct time, configure an NTP server and point the system to the IP address of the NTP server.

NOTE
When configuring the WLAN time schedule, all times are based on the time zone setting of your browser. If your browser and the target AP and WLAN are in different time zones, configure the on and off times according to the desired schedule according to your local browser. For example, if you want a WLAN in Los Angeles to turn on at 9 AM and your browser is set to New York time, configure the WLAN time schedule to enable the WLAN at noon.

Creating a Time Schedule Profile

Complete the following steps to create a Time schedule profile.

1. From the main menu, go to **Network** > **Wireless** > **Wireless LANS**, and select a WLAN.
2. Click **Configure**. The **Edit WLAN Configuration** dialog box is displayed.
3. Go to **Advanced Options**.
4. For **Time Schedule**, select **Specific**.

NOTE
By default, **Always On** is selected.

5. Click **Create (+)**. The **Create Time Based Access Table** dialog box is displayed.
6. In the **General Options**, enter the schedule name and schedule description.
7. In the **Schedule Table**, create a WLAN schedule profile for the selected wireless LAN.
8. To create the time-based access table for a WLAN, perform the following actions:
   - To enable or disable the WLAN for an entire day, click the day of the week under the **Time** column.
   - To enable or disable the WLAN for specific housr of a specific day, select the squares in the table. A single square represents 30 minutes (two 15-minute blocks).

     Blue-colored cells indicate the hours when the WLAN is enabled. Clear (or white) cells indicate the hours when the WLAN is disabled.
9. Click Ok. The schedule is submitted and the schedule name is displayed.

Managing WLANs

When you select a system, domain, zone, or WLAN group from the hierarchy tree, respective contextual tabs appear at the bottom of the page.

TABLE 70 System, Domain, Zone, and WLAN Groups Monitoring Tabs

Tabs	Description	System	Domain	Zone	WLAN Groups
Configuration	Displays the respective configuration information.	Yes	Yes	Yes	Yes
Traffic	Displays the respective historical traffic information.	Yes	Yes	Yes	Yes
Alarm	Displays the respective alarms information.	Yes	Yes	Yes	Yes
Event	Displays the respective event information.	Yes	Yes	Yes	Yes
APs	Displays the respective AP information.	Yes	Yes	Yes	N/A
Clients	Displays the respective client information.	Yes	Yes	Yes	N/A
Services	Displays the respective services information.	Yes	Yes	Yes	N/A
Administrators	Displays the respective administrator account information.	Yes	N/A	N/A	N/A

When you can select a zone and click **More**, you can perform the following operations:

- Move a WLAN to a different zone
- Extract a WLAN Template
- Apply a WLAN Template
- Change the AP Firmware
- Switch over a Cluster
- **Trigger a preferred node**

NOTE
WLANs can be disabled or enabled at the AP. To disable or enable a WLAN, refer Configuring Access Points > Radio Options b/g/n (2.4GHz).

Moving a Single WLAN to a Different WLAN Zone

Complete the following steps to move a single WLAN from its current WLAN zone to a different one.

NOTE
The WLAN that you move will inherit the configuration of the new WLAN zone. This feature is applicable only for SZ300 and vSZ-H platforms.

1. From the main menu, go to **Network** > **Wireless** > **Wireless LANs**, and locate the WLAN zone that you want to move to a different WLAN zone.
2. Click **More** and select **Move**. The **Select Destination Management Domain** dialog box is displayed.
3. Select the destination WLAN zone.
4. Click **OK**. A confirmation message is displayed.
5. Click **Yes**. The WLAN is moved to the destination location.

Extracting a WLAN Template

You can extract only the WLAN-related configuration to a WLAN template.

Complete the following steps to extract a WLAN template.

1. From the main menu, go to **Network** > **Wireless** > **Wireless LANs**and locate the zone from where you want to extract the WLAN template.
2. Click **More** and select **Extract WLAN Template**. The **Extract WLAN Template**dialog box is displayed.
3. For **WLAN Template Name**, enter a name for the template.
4. Click **OK**. A message is displayed stating that the WLAN template was extracted successfully.
5. Click **OK**.

   The extracted WLAN template can be viewed at **System** > **Templates** > **WLAN Templates**.

Applying a WLAN Template

You can apply only the WLAN-related configuration to an AP zone using a WLAN template. You can apply the WLAN template to zones where the AP's firmware version is later than the Zone templates firmware version. An unsupported firmware version of the WLAN template is automatically upgraded to its next version before being upgraded to the current version.

Complete the following steps to apply a WLAN template.

1. From the main menu, go to **Network** > **Wireless** > **Wireless LANs** and locate the zone from where you want to extract the WLAN template.
2. Click **More** and select **Apply WLAN Template**, The **Apply WLAN Template** dialog box is displayed.
3. From the **Select a WLAN template** list, select the template.
4. Click **Next.** The **Apply WLAN template to selected zone** dialog box is displayed.
5. Complete the required options:
   - Create all WLANs and WLAN profiles from the template if they do not already exist in the target zones.
   - If the target zones have a WLAN or WLAN profile with the same name as the template, overwrite the current settings with settings from the template.
   - Click **OK**. A confirmation dialog box is displayed.
6. Click **OK**.

Triggering a Preferred Node

You can trigger an AP that belonging to its current zone to connect to the preferred node. First, you must enable Node Affinity, which gives the AP the priority of the preferred nodes.

> **NOTE**
> This feature is applicable only for SZ300 and vSZ-H platforms.

Complete the following steps to trigger a preferred node.

> **NOTE**
> You must enable the Node Affinity before triggering nodes.

1. Click **Network** > **Wireless** > **Wireless LANs** and select zone.
2. Click **More** and select **Trigger Preferred Node**. A confirmation dialog box is displayed.
3. Click **OK**.

How Dynamic VLAN Works

Dynamic VLAN can be used to automatically and dynamically assign wireless clients to different VLANs based on RADIUS attributes.

Dynamic VLAN Requirements:

- A RADIUS server must have already been added to the controller
- WLAN authentication method must be set to 802.1X, MAC address or 802.1X + MAC address

To enable Dynamic VLAN for a WLAN:

1. Go to **Network** > **Wireless** > **Wireless LANs**.
2. Click **Configure** for to the WLAN you want to configure.
3. In **Authentication Server**, select the AAA profile.
4. Expand the **Advanced Settings** section and click the**Enable Dynamic VLAN box** next to Access VLAN.

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

FIGURE 84 Enabling Dynamic VLAN



How It Works

- User associates with a WLAN on which Dynamic VLAN has been enabled.
- The AP requires the user to authenticate with the RADIUS server.
- When the user completes the authentication process, the AP will approve the user along with the VLAN ID that has been assigned to the user on the RADIUS server.
- User joins the AP and is segmented to the VLAN ID that has been assigned to him.

Required RADIUS Attributes

For dynamic VLAN to work, you must configure the following RADIUS attributes for each user:

- **Tunnel-Type**: Set this attribute to VLAN.
- **Tunnel-Medium-Type**: Set this attribute to IEEE-802.
- **Tunnel-Private-Group-ID**: Set this attribute to the VLAN ID to which you want to segment this user.

Depending on your RADIUS setup, you may also need to include the user name or the MAC address of the wireless device that the user will be using to associate with the AP. The following table lists the RADIUS user attributes related to dynamic VLAN.

TABLE 71 RADIUS user attributes related to dynamic VLAN

Attribute	Type ID	Expected Value (Numerical)
Tunnel-Type	64	VLAN (13)
Tunnel-Medium-Type	65	802 (6)
Tunnel-Private-Group-Id	81	VLAN ID

Here is an example of the required attributes for three users as defined on Free RADIUS:

```
0018ded90ef3
   User-Name = user1,
   Tunnel-Type = VLAN,
   Tunnel-Medium-Type = IEEE-802,
   Tunnel-Private-Group-ID = 0014
00242b752ec4
   User-Name = user2,
   Tunnel-Type = VLAN,
   Tunnel-Medium-Type = IEEE-802,
   Tunnel-Private-Group-ID = 0012
013469acee5
   User-Name = user3,
   Tunnel-Type = VLAN,
   Tunnel-Medium-Type = IEEE-802,
   Tunnel-Private-Group-ID = 0012
```

NOTE
The values in bold are the users' MAC addresses.

Configuring AP Settings

Working with AP Registration Rules

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

NOTE
A registration rule is only applied to an AP the first time it joins the controller. If an AP's MAC address already exists on the controller database (whether it is in connected on disconnected state and whether it belongs to the Staging Zone or any other zone), the controller will assign the AP to its last known AP zone.

Creating an AP Registration Rule

You must create rules to register an AP.

To create an AP registration rule:

1. Go to **Network** > **Wireless** > **AP Settings** > **AP Registration**.

   NOTE
   For SmartZone 5.2.1 or earlier releases, select **System** > **AP Settings**>**AP Registration**.

2. Click **Create**, the AP Registration Rule form appears.
3. Enter a **Rule Description**.
4. Select the **Zone Name** to which this rule applies.
5. In **Rule Type**, click the basis upon which you want to create the rule. Options include:

   NOTE
   The format of the IP address or addresses that you need to enter here depends on the AP IP mode that you selected when you created the AP zone to which this rule will be assigned. If you selected IPv4 Only, enter an IPv4 address. If you selected IPv6 Only, enter an IPv6 address.

   - **IP Address Range**: If you select this option, enter the From (starting) and To (ending) IP address that you want to use.
   - **Subnet**: If you select this option, enter the IP address and subnet mask pair to use for matching.

- **GPS Coordinates**: If you select this option, type the GPS coordinates to use for matching. Access points that have been assigned the same GPS coordinates will be automatically assigned to the AP zone that you will choose in the next step.

  You can choose the Rule Type as GPS coordinates, wherein you must provide information about the latitude, longitude and distance to determine if the AP is within the defined area.
- **Provision Tag**: If the access points that are joining the controller have been configured with provision tags, click the Provision Tag option, and then type a tag name in the Provision Tag box. Access points with matching tags will be automatically assigned to the AP zone that you will choose in the next step.

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

6. Click **OK**.

   When the process is complete, the page refreshes, and then registration rule that you created appears on the AP Registration Rules page.

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

   NOTE
   You can also edit, delete or clone an AP registration rule. To do so, select the rule profile from the list and click **Configure**, **Delete** or **Clone** respectively.

Configuring Registration Rule Priorities

The controller applies registration rules in the same order as they appear in the AP Registration Rules table (highest to lowest priority).

If you want a particular registration rule to have higher priority, you must move it up the table. Once an AP matches a registration rule, the controller assigns the AP to the zone specified in the rule and stops processing the remaining rules.

Follow these steps to configure the registration rule priorities.

1. Go to **Network** > **Wireless** > **AP Settings** > **AP Registration** .
2. Select the rule from the list and click.
   - **Up**—To give a rule higher priority, move it up the table
   - **Down**—To give a rule lower priority, move it down the table
3. Click **Update Priorities** to save your changes.

Tagging Critical APs

A critical AP is an AP that exceeds the daily traffic threshold (sum of uplink and downlink) data bytes configured on the controller web interface.

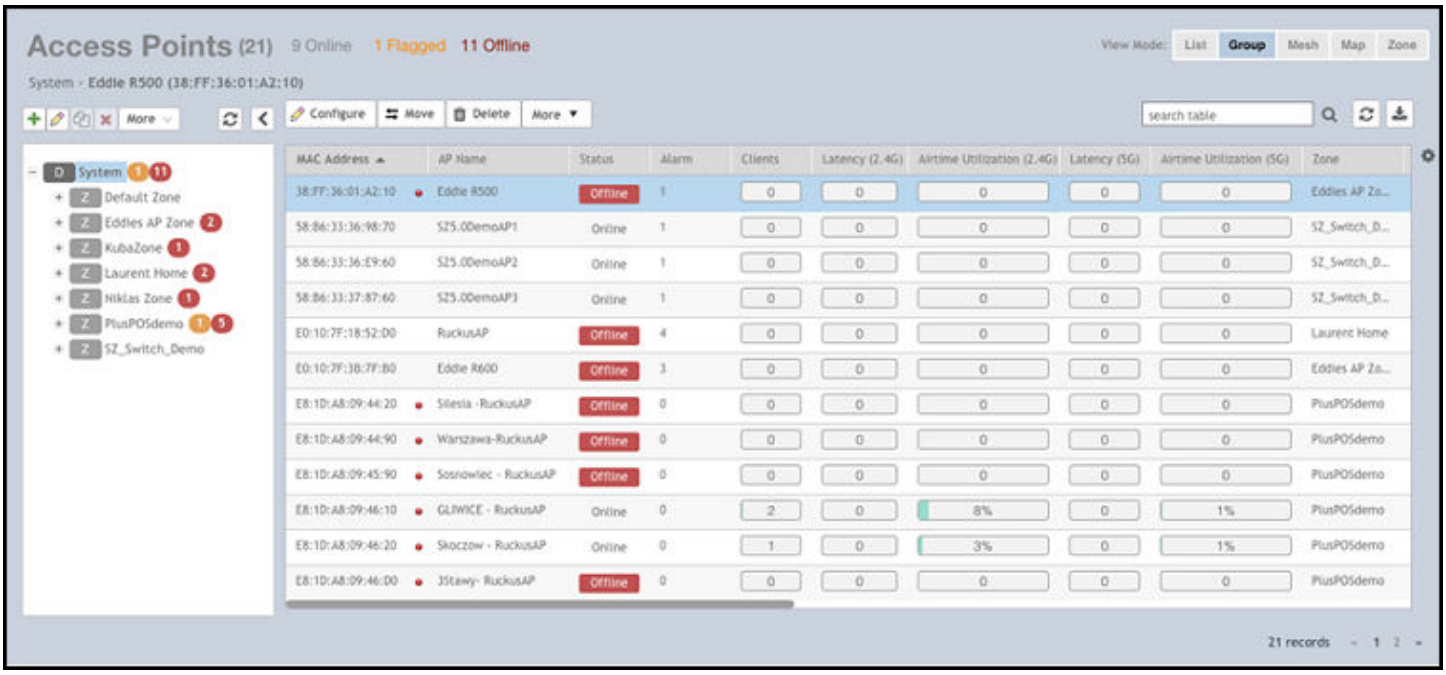
Follow these steps to tag critical APs (APs that exceed the data traffic threshold you have defined) automatically:

1. Go to **Network** > **Wireless** > **AP Settings** > **Critical AP Tagging**.
2. Select the **Enable Auto Tagging Critical APs** check box.
3. For **Auto Tagging Rules**, select **Daily Traffic Bytes Exceeds Threshold**.
4. For **Rule Threshold**:
   - In the first box, enter the value that you want to set as the traffic threshold. This value will be applied in conjunction with the data unit that you select in the second box.
   - In the second box, select the data unit for the threshold—**MB** for megabytes or **GB** for gigabytes.

5. Click **OK**.

Critical APs are marked with red dots next to its MAC Address for attention (refer the following image). APs that exceed the daily traffic threshold that you specified will appear highlighted on the Access Points page and the Access Point details page. Additionally, the controller will send an SNMP trap to alert you that an AP has been disconnected.

FIGURE 85 APs Tagged as Critical



Configuring the Tunnel UDP Port

The tunnel UDP port is used by all GRE+UDP type tunnels.

To configuring the tunnel UDP port:

1. Go to **Network** > **Wireless** > **AP Settings** > **Tunnel UDP Port**.
2. Enter the **Tunnel UDP Port** number.
3. Click **OK**.

Setting the Country Code

Different countries follow different regulations for radio channel usage.

To ensure that the APs use authorized radio channels:

1. Go to **Network** > **Wireless** > **AP Settings** .
2. Select the **Country Code** for your location from the drop-down.
3. Click **OK**.

Limiting the Number of APs in a Domain or Zone

You can limit the number of APs in a Partner-Managed Domain or a Zone. An MSP may have multiple customers each with their own zone and a number of APs. This feature ensures that their customers do not over-subscribe the licenses that they are entitled. MVNO domains do not have this option. When an AP joins a zone, where an AP number limitation has been applied to that zone, the controller checks the current capacity based on zone's limitation and:

- allows the new AP joining if the number of APs connected do not exceed the limit
- denies the new AP joining if there is no capacity in the domain or zone.

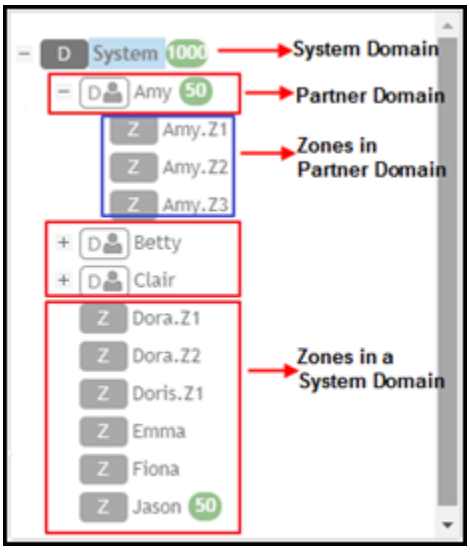
A scheduler task in the background periodically checks the AP number limitation against the number of APs connected. To avoid occupying the license capacity, the APs will be rejected in the following situations:

- If the AP number limitation of a Domain or a Zone is increased or reduced.
- If the license capacity is changed.

The following image gives a clarity on:

- System domain
- Partner domain
- Zones in a System domain
- Zones in a Partner domain

FIGURE 86 System Hierarchy



Limiting the AP count for a Partner Domain or a System Zone

Only super admin of the system domain is privileged to limit the number of APs in a partner domain or a system zone.

To limit the number of AP count for a partner domain or a system zone:

1. Log on to the controller web interface using super admin credentials of the system domain.

2. Follow the procedure to limit the number of APs in the partner domain or a zone in system domain:
   a) Go to **Network** > **Wireless** > **AP Settings** > **AP Number Allocation**.
   a) For **Enable AP Number Allocation**, select the **Enabled** check box and click **OK**. The Settings bar appears.
   b) From the left pane, in the system tree hierarchy, select the partner-managed Domain or Zone for which you want to set the AP number limit.
   c) On the right pane, select **Share Mode** or enter the **Number Limit**.
   d) Click **OK**. You have set the AP number limit for the selected Domain or Zone.

Limiting the AP count for a Zone in a Partner Domain

To limit the number of AP count for a zone in a partner domain:

1. Create a super admin account for the partner domain. See the Administrating the Controller chapter.
2. **NOTE**
   While creating user groups, in step 4 (I) c, for **Permission**, select Super Admin from the drop-down.

   Create a user group and configure the access permissions, resources and administrator account. Refer Creating User Groups on page 587.
3. Log on to the controller web interface using the following logon details:
   - **User Name**:

     ```
     Account Name@Domain
     ```

     The Account Name that you set when you created the Administrator Account and the Domain for which you created the Administrator Account. For example: If the partner domain is *TestDomain* and the Account Name is *User*, then the User Name is

     ```
     User@TestDomain
     ```

   - **Password** : The password that you set when you created the Administrator Account.
4. Follow the procedure to limit the number of APs for a zone in a partner-domain:
   a) Go to **Network** > **Wireless** > **AP Settings** > **AP Number Allocation**.
   a) Select the **Enable AP Number Allocation** check box and click **OK**. The Settings bar appears.
   b) From the left pane, in the system tree hierarchy, select the partner-managed zone for which you want to set the AP number limit.
   c) On the right pane, perform one of the following procedure:
      - Select **Share Mode**
      - Enter **Number Limit**
   d) Click **OK**.

   You have set the AP number limit for the selected partner-domain Zone.

Creating an AP MAC OUI Address

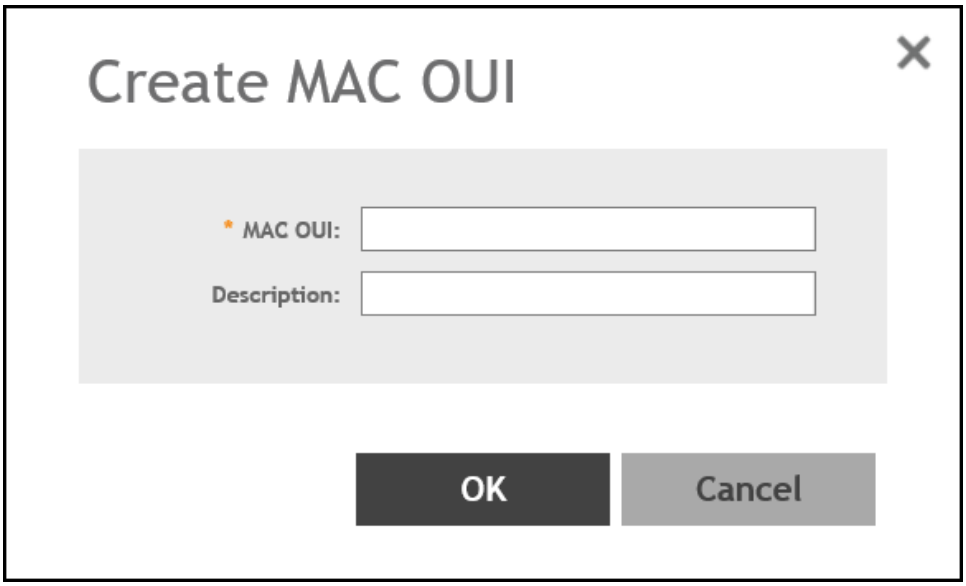
You must enable the AP MAC OUI validation for an AP with a specific organizationally unique identifier (OUI) to be allowed to connect to SZ. If the AP that is not in the OUI list connects to the SZ, then the AP is rejected and event code 186 is generated.

Perform the following procedure to create the MAC OUI address for an AP.

1. Go to **Network** > **Wireless** > **AP Settings** > **AP MAC OUI Validation**.
2. Select **Enable AP MAC OUI Validation**.

3. Click **Create** to create the MAC OUI settings for an AP.

FIGURE 87 Creating an AP MAC OUI Address

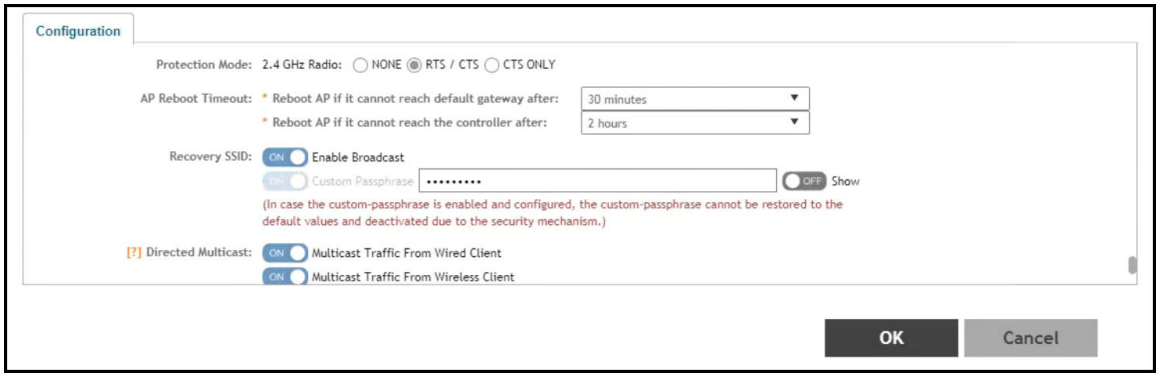


4. Enter the MAC OUI.
5. Click **OK**.

AP Admin Password and Recovery SSID

This topic describes the mitigation of security enhancement of the AP admin password management.

Consider the following scenario while generating the configuration:



- Initial Installation: AP admin password need to be hashed in SHA-256 algorithm, stored in database and in configuration.

User can specify the Recovery SSID key in the Configuration Tab:

- The default of this Recovery SSID feature is enabled. The default passphrase is AP admin password in clear text format.
- If the user wants to change it, input the passphrase while enabling.
- The validation of passphrase, apply the same rule of WLAN passphrase.

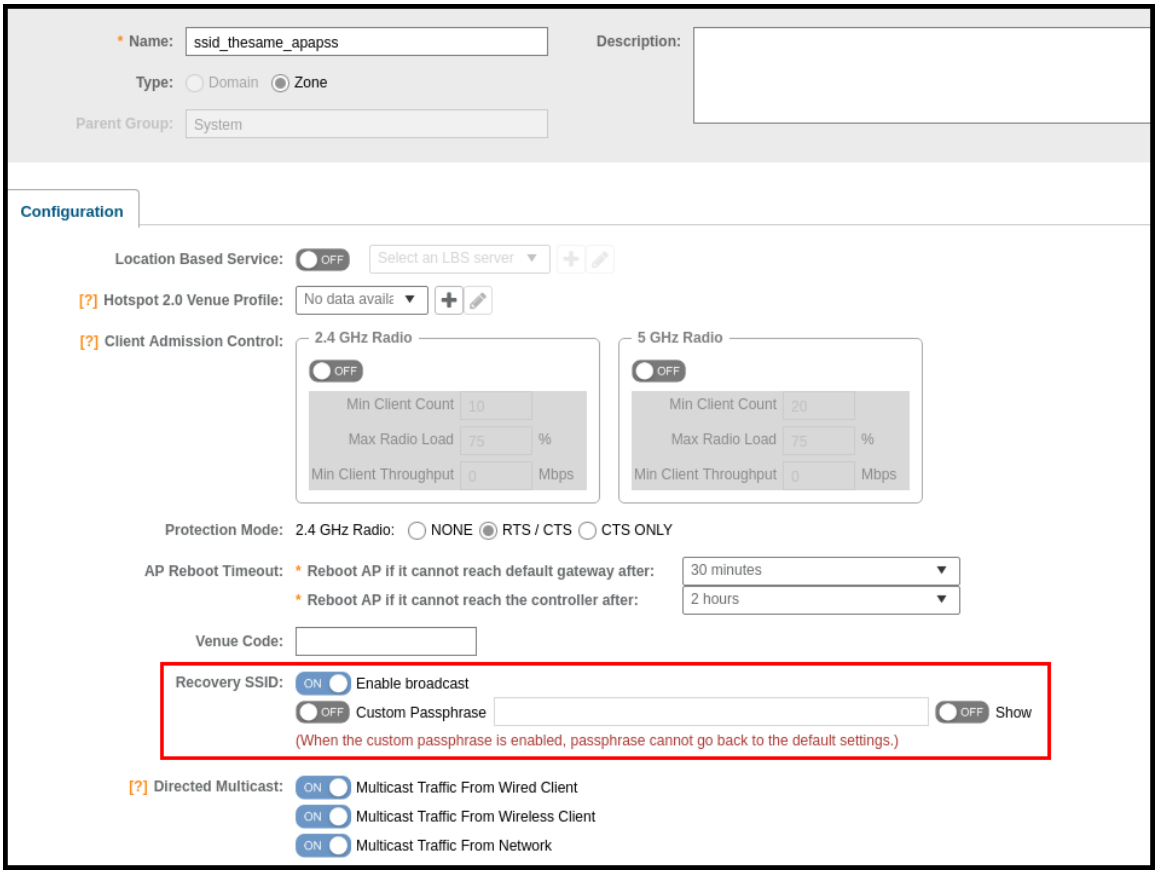
- The passphrase can be clear text stored in the database and delivered to the AP in the GPB configuration by the way of secure channel (SSH channel).

The recovery SSID passphrase(key) will be delivered in GPB configuration as below:

- ccm_zone.proto
- message CcmCommon {
- /** recovery ssid
- */
- optional bool recovery_ssid_enabled = 26
- optional string recovery_ssid_psk_key = 27
- optional int32 server_loss_timeout = 28

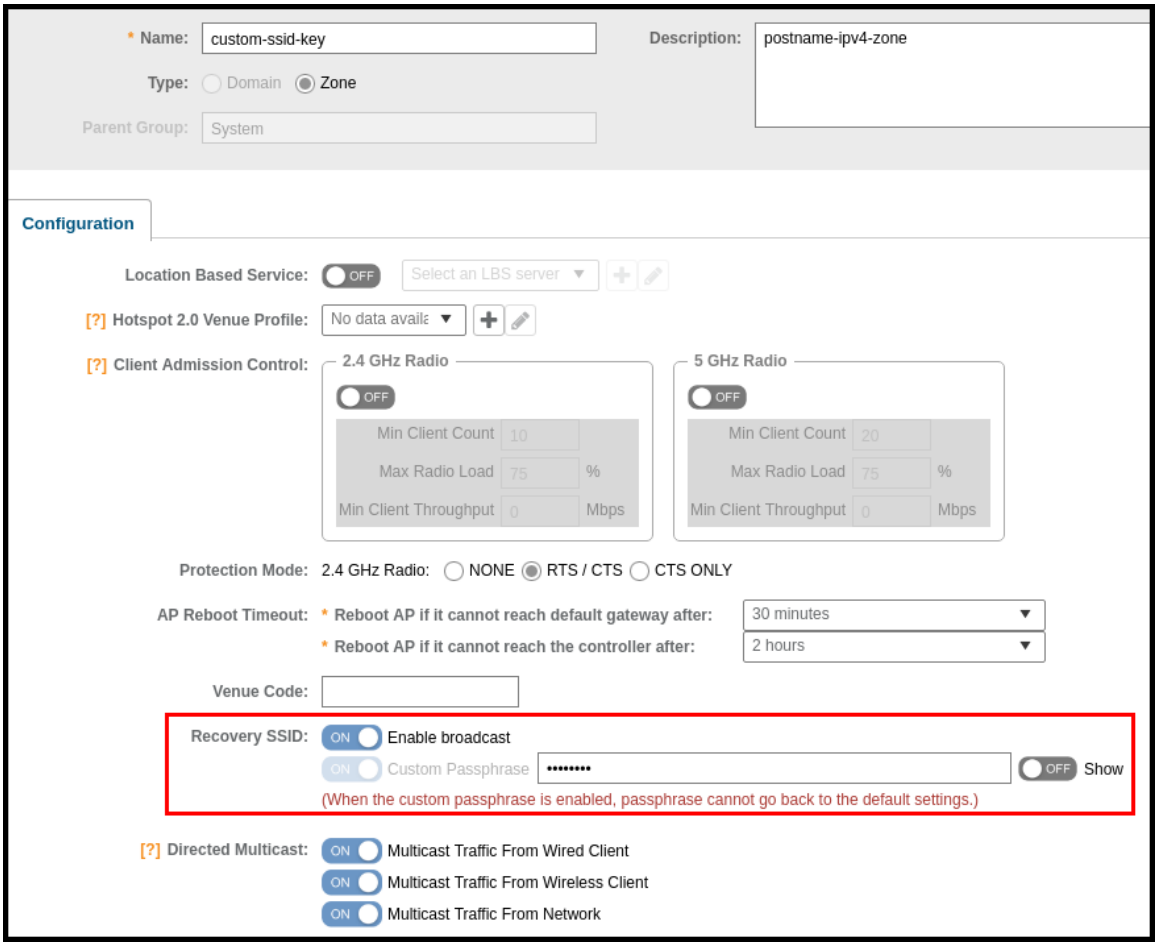
When the Custom passphrase is disabled, the Custom passphrase filed is empty.

FIGURE 88 Custom Passphrase Disabled



When the Custom passphrase is enabled, the Custom passphrase field is mandatory and should enter a passphrase.

FIGURE 89 Custom Passphrase Enabled



Power Source in AP Configuration

The table below displays the PoE mode as per industry standards.

The currently used APs have AF, AT, AT+ convention modes. The standardization applies when the AP is forced to certain PoE power mode. If the AP is set to AUTO PoE mode, feedback displays PoE mode of the AP is currently configured.

The PoE mode as per the industry standards:

TABLE 72 Industry Standard PoE Modes

Selection	Power@PSE	Power@AP (100M Cable)
802.3af	15.4W	12.95W
802.3at	30W	25.5W
802.3bt/Class 5	45W	40W→35W
802.3bt/Class 6	60W	51W
802.3bt/Class 7	75W	62W
802.3bt/Class 8	90W	71.3W

TABLE 73 Non-Standard High Power Solution Summary

	Customers	Maximum Power Sourced
UPoE	Enterprise Switch	60W
PoH	Consumer Customers, for example, audio systems)	95W

The SZ-GUI power mode drop-down has the following set of PoE mode configurations:

TABLE 74 PoE Mode Settings

Name	Value
Auto	0
802.3af	1
802.3at	2
802.3bt/Class 5	3
802.3bt/Class 6	4
802.3bt/Class 7	5

NOTE
The 802.3bt/Class5 is chosen for AP's with older software which advertise AT+.

NOTE
The below tables are applicable for stand alone APs as well. However, the IOT functionality is not available.

POE tables for different 11 AC AccessPoint

TABLE 75 R710

	LLDP Power Ask	2.4G tx/rx	5G tx/rx	1Gbps eth	USB	IOT
DC	N/A	4/4	4/4	Enabled	Enabled	Enabled
AF	N/A	2/4	4/4	Enabled	Disabled	Disabled
AT	25W	4/4	4/4	Enabled	Enabled	Enabled
Injector (Model 480125A)	N/A	4/4	4/4	Enabled	Enabled	Enabled

TABLE 76 R610

	LLDP Power Ask	2.4G tx/rx	5G tx/rx	1Gbps eth	USB	IOT
DC	N/A	4/4	4/4	Enabled	Enabled	Enabled
AF	N/A	2/4	4/4	Enabled	Disabled	Disabled
AT	24W	4/4	4/4	Enabled	Enabled	Enabled
Injector (Model 480125A)	N/A	4/4	4/4	Enabled	Enabled	Enabled

TABLE 77 R720

	LLDP Power Ask	2.4G tx/rx	5G tx/rx	1Gbps eth	USB	IOT	Comments
DC	N/A	4/4	4/4	Enabled	Enabled	Enabled	No comments
AF	N/A	1/4	1/4	Enabled	Disabled	Disabled	No comments
AT	25W	4/4	4/4	Enabled	Disabled	Disabled	No comments
3bt/class5	35W	4/4	4/4	Enabled	Enabled	Enabled	No comments

TABLE 77 R720 (continued)

POE Injector (Model 480125A) 60W	N/A	4/4	4/4	Enabled	Enabled	Enabled	Force to 802.3bt/ class5 from SZ GUI

TABLE 78 M510

	LLDP Power Ask	2.4G tx/rx	5G tx/rx	1Gbps eth	USB	IOT
DC	N/A	2/2	2/2	Enabled	Enabled	Enabled
AF	N/A	2/2	2/2	Enabled	Disabled	Disabled
AT	25W	2/2	2/2	Enabled	Enabled	Enabled
Injector (Model 480125A)	N/A	2/2	2/2	Enabled	Enabled	Enabled

TABLE 79 T610

	LLDP Power Ask	2.4G tx/rx	5G tx/rx	1Gbps eth	USB	IOT
DC	N/A	3/3	3/3	Enabled	Enabled	Enabled (0.5W)
AF	N/A	2/3	3/3	Enabled	Disabled	Disabled
AT	25W	3/3	3/3	Enabled	Enabled	Enabled (0.5W)
Injector (Model 480125A)	N/A	3/3	3/3	Enabled	Enabled	Enabled (0.5W)

POE tables for different 11 AX AccessPoint

TABLE 80 R730

	LLDP	2.4G tx/rx	5G tx/rx	5Gbps eth	1Gbps eth	USB	IOT	Comments
DC	N/A	4/4	8/8	Enabled	Enabled	Enabled	Enabled	No comments
AF	N/A	1/4	1/8	Enabled	Disabled	Disabled	N/ADisabled	Not supported via SZ-GUI, but we can AF mode via rkscli.
AT Mode = 0	25W	4/4	4/8	Enabled	Enabled	Enabled (0.5W)	Enabled	By default AT - mode = 0
AT Mode = 1	25W	4/4	8/8	Enabled	Disabled	Disabled	Disabled	Set AT - mode = 1 via Rkscli
802.3bt/class 5	35W	4/4	8/8	Enabled	Enabled	Enabled	Enabled	No comments
POE Injector (Model 480125A) 60W	N/A	4/4	4/8	Enabled	Enabled	Enabled	N/A	Force to 802.3bt/class5 from SZ GUI

TABLE 81 R850

	LLDP Power Ask	2.4G tx/rx	5G tx/rx	5Gbps eth	1Gbps eth	USB	IOT	Comment
DC	N/A	4/4	8/8	Enabled	Enabled	Enabled	Enabled	No comments
AF	N/A	1/4	1/8	Enabled	Disabled	Disabled	Disabled	Not supported via SZ-GUI, but we can AF mode via rkscli.
AT (Mode=0)	25W	4/4	4/8	Enabled	Enabled	Enabled (0.5W)	Enabled	By default at-mode=0

TABLE 81 R850 (continued)

	LLDP Power Ask	2.4G tx/rx	5G tx/rx	5Gbps eth	1Gbps eth	USB	IOT	Comment
AT (Mode=1)	25W	4/4	8/8	Enabled	Disabled	Disabled	Disabled	Set at-mode=1 via Rkscli
802.3bt/class5	35W	4/4	8/8	Enabled	Enabled	Enabled	Enabled	No comments
POE Injector (Model 480125A) 60W	N/A	4/4	4/8	Enabled	Enabled	Enabled	Enabled	Force to 802.3bt/ class5 from SZ GUI

TABLE 82 R750

	LLDP Power Ask	2.4G tx/rx	5G tx/rx	2.5Gbps eth	1Gbps eth	USB	IOT
DC	N/A	4/4	4/4	Enabled	Enabled	Enabled	Enabled
AF	N/A	2/4	2/4	Enabled	Disabled	Disabled	Disabled
AT	25W	4/4	4/4	Enabled	Enabled	Enabled	Enabled
POE Injector (Model 480125A) 60W	N/A	4/4	4/4	Enabled (1Gbps speed)	Enabled	Enabled	Enabled

TABLE 83 T750

	LLDP Power Ask	**2.4G tx/rx**	**5G tx/rx**	**2.5Gbps eth**	**1Gbps eth**	**USB**	**IOT**	**PSE**	**Comment**
DC	N/A	4/4	4/4	Enabled	Enabled	Enabled	Enabled	Enabled	No comments
AF	N/A	1/4	1/4	Enabled	Disabled	Disabled	Disabled	Disabled	Not supported operation mode
AT w/o USB	25W	4/4	4/4	Enabled	Enabled	Disabled	Enabled	Disabled	No comments
AT with USB	25W	2/4	4/4	Enabled	Disabled	Enabled	Enabled	Disabled	Set AT - mode = 1 via Rkscli
802.3bt/ class5	35W	4/4	4/4	Enabled	Enabled	Enabled	Enabled	Disabled	No comments
803.3bt/ class6	N/A	4/4	4/4	Enabled	Enabled	Enabled	Enabled	Disabled	51W by H/W negotiation
802.3bt/ class7	N/A	4/4	4/4	Enabled	Enabled	Enabled	Enabled	Enabled	62W by H/W negotiation
POE 60W Injector (Model 480125A)	N/A	4/4	4/4	Enabled (1Gbps speed)	Enabled	Enabled	Enabled	Disabled	Force to 802.3bt/ class5
POE 90W Injector	N/A	4/4	4/4	Enabled	Enabled	Enabled	Enabled	Enabled	Force to 802.3bt/ class7

TABLE 84 R650

	LLDP Power Ask	**2.4G tx/rx**	**5G tx/rx**	**2.5Gbps eth**	**1Gbps eth**	**USB**	**IOT**
DC	N/A	2/2	4/4	Enabled	Enabled	Enabled	Enabled
AF	N/A	2/2	2/4	Enabled	Disabled	Disabled	Disabled
AT	25W	2/2	4/4	Enabled	Enabled	Enabled	Enabled

TABLE 84 R650 (continued)

POE Injector (Model 480125A)	N/A	2/2	4/4	Enabled (1Gbps speed)	Enabled	Enabled	Enabled

TABLE 85 R550

	LLDP Power Ask	2.4G tx/rx	5G tx/rx	2.5Gbps eth	1Gbps eth	USB	IOT
DC	N/A	2/2	2/2	Enabled	Enabled	Enabled	Enabled
AF	N/A	2/2	2/2	Enabled	Disabled	Disabled	Disabled
AT	25W	2/2	2/2	Enabled	Enabled	Enabled	Enabled
POE Injector (Model 480125A)	N/A	2/2	2/2	Enabled	Enabled	Enabled	Enabled

Working with Maps

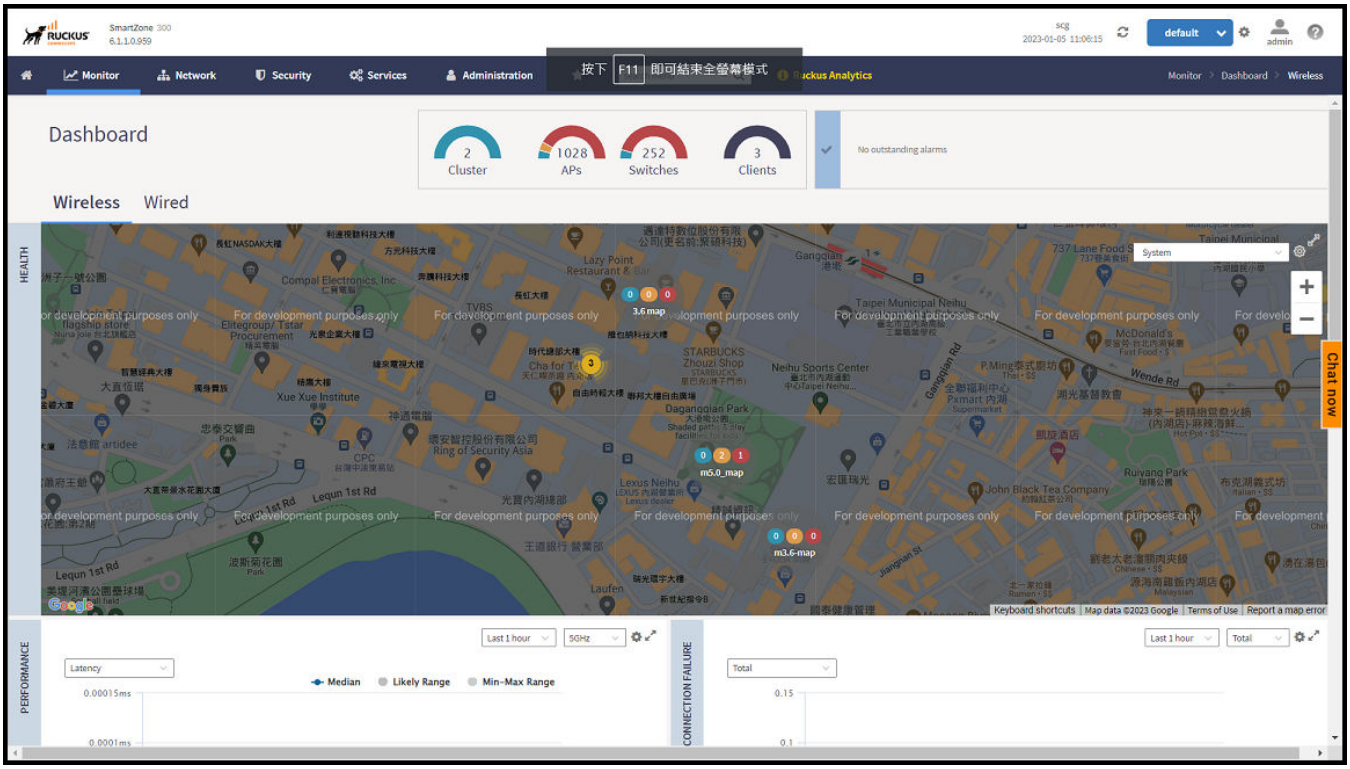
Importing floorplan maps into SmartZone allows you to further customize the information displayed on the Dashboard and Access Points pages, and monitor your APs, zones, groups, clients and traffic statistics all within the world map view on the Dashboard.

Additionally, you can use the maps to quickly locate more specific information on a venue or zone, and drag and drop APs onto the floor plan map to represent their locations in physical space in your venue.

Once a map is imported and GPS coordinates are entered, an icon representing the venue appears on the world map on the Dashboard. The icon displays the current number of APs (Online, Flagged and Offline). You can hover over the icon for more information.

Double-click the map icon or click **Zoom into this map** to view the imported map in the Dashboard.

FIGURE 90 Imported Maps on the Dashboard



Importing a Floorplan Map

The controller provides a user-friendly workflow for importing a map of your venue floorplan, placing APs in their respective physical locations on the map, and scaling the map to match the actual dimensions of your venue.

Floorplan maps allow you to view site/venue/floor-specific details such as:

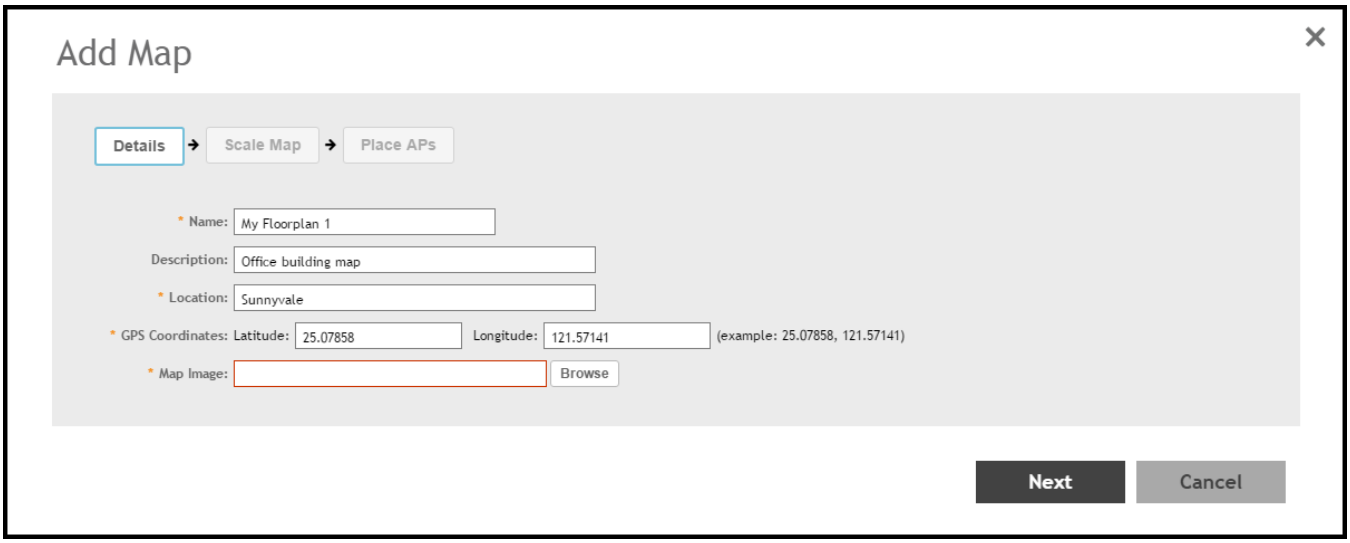
- AP status, performance, and health conditions
- Client connections to an AP
- Location-specific trouble spots related to AP or client connectivity

To import a floorplan map:

1. Go to **Network** > **Wireless** > **Maps**.
2. From the System tree hierarchy, select the location where you want to create a map and click the **Add** icon button. The **Add Map** form appears.
3. On the **Details** tab, enter a **Name** and optionally a **Description** to identify the map.
4. Enter a **Location** for the map. Alternatively, you can choose the location from the auto-completion options. After you select the location, the GPS Coordinates are automatically updated.

5. For **GPS Coordinates**, you can enter the **Latitude** and **Longitude** values.

FIGURE 91 Creating the Add Map form



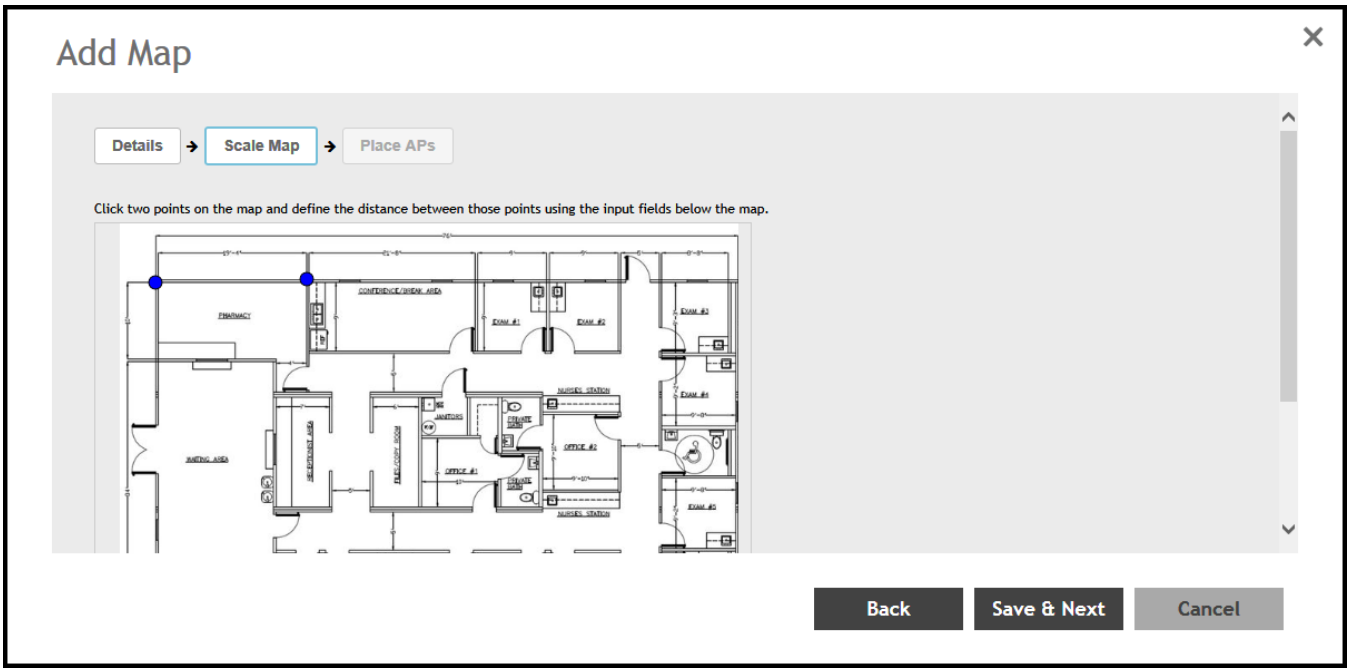
6. To add a **Map Image**, click **Browse** and select a site, venue, or floor map in jpg, jpeg, png, bmp or svg file formats.

NOTE
The maximum file size per indoor map is 5MB.

7. Click **Next**, the **Scale Map** tab is displayed.

8. Click two points on the map between which you know the distance. Blue dots appear to show the points you selected.

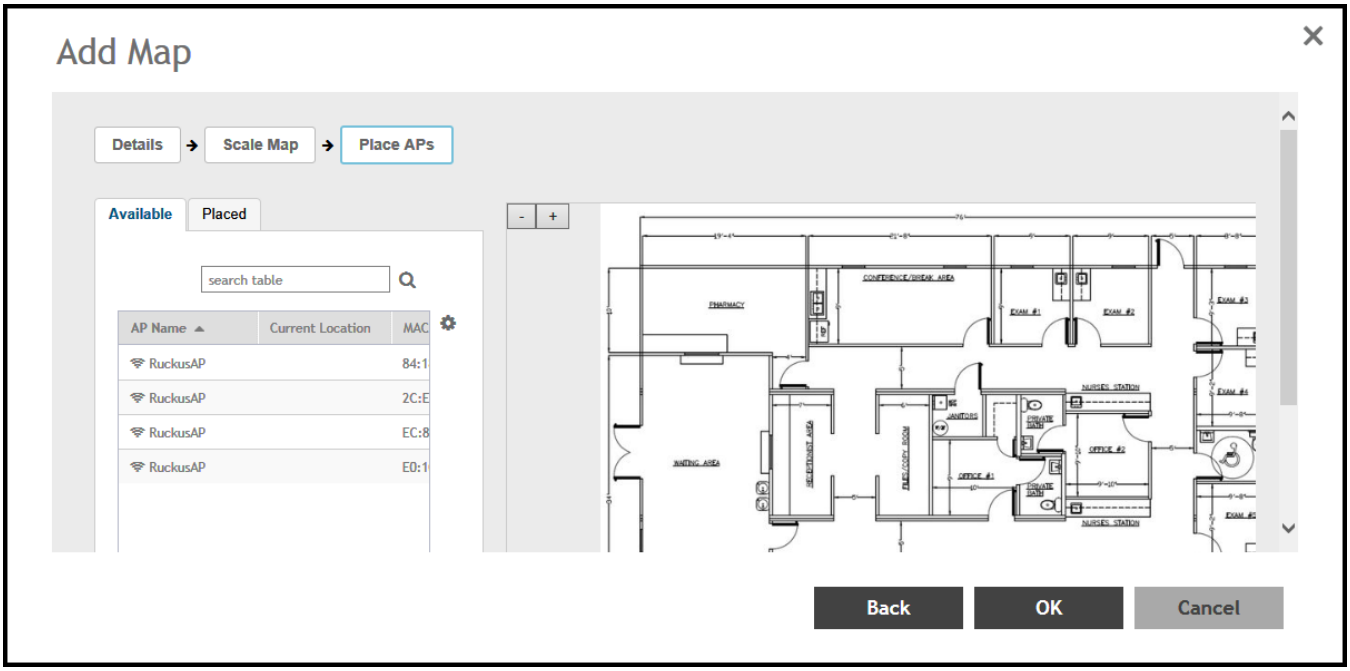
FIGURE 92 Indicating the Selected Points on the Map



9. Enter the **Physical Distance** between the two points and select the unit of measurement (mm, cm, m, ft, yard).
10. Click **Save & Next**. The **Place APs** tab appears.

11. From the **Available** list, drag the APs and place them in their physical locations on the map. Click the **Placed** tab to see the list of placed APs.

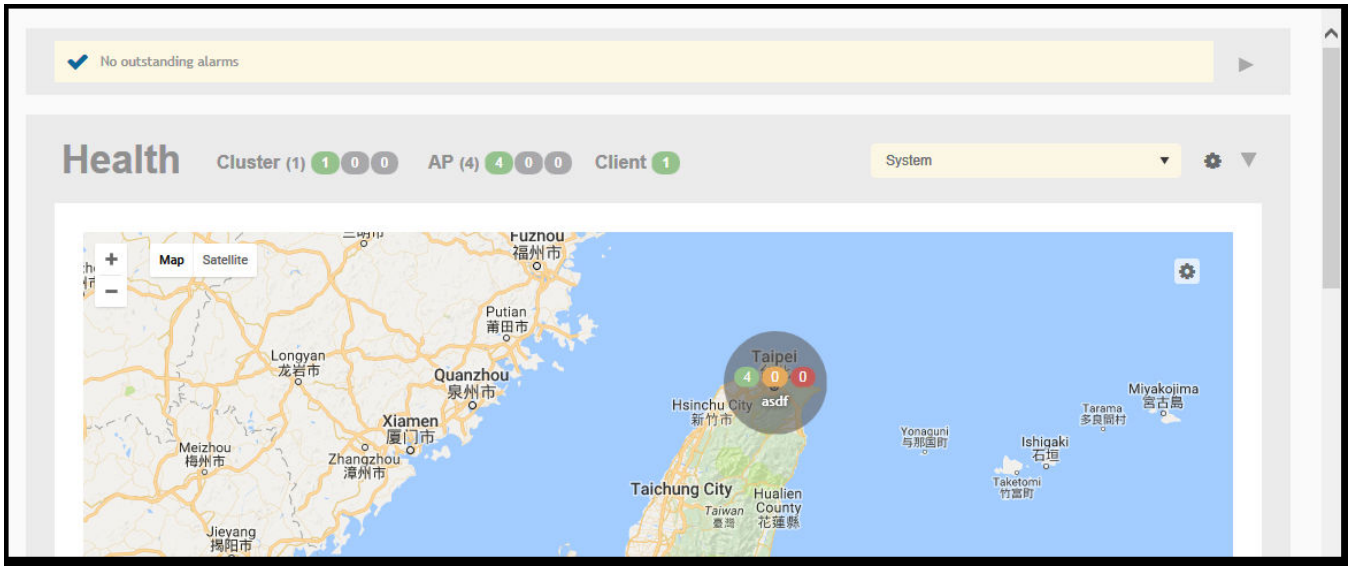
    FIGURE 93 Dragging and dripping to place APs on the Floorplan



12. Once you are happy with the placement of your APs on the map, click **OK** to save your map.

Your venue now appears as an icon on the world map on the Dashboard, located at your venue's actual physical location (if you entered the GPS coordinates correctly). The Dashboard icon that represents your venue provides an overview of the number of APs in the venue and their status. Hover over the icon to view more details, or click one of the links to zoom in to the venue floorplan map you imported.

FIGURE 94 Importing Venue Map Icon



NOTE
You can also edit or delete a map. To do so, select the map from the list and click the **Edit** or **Delete** icons respectively.

Viewing RF Signal Strength

Radio Frequency (RF) signal strength can be viewed using a heat map for a specific location.

The heat map helps us identify the RF signal strength in a specific location. It provides heat maps using actual path loss information from the environment. You can view an indoor floor plan map for an AP.

To view the RF signal strength:

1. Go to **Network** > **Wireless** > **Maps**.
2. From the System tree hierarchy, select the location of the map that you want to view.
3. Select the **Show Signal Coverage** check box and choose the required RF frequency. For example, 2.4 GHz or 5 GHz. The heat map is displayed with a color-gradient legend. High signal strength appears in red. The color changes as the signal strength reduces.

FIGURE 95 RF Coverage Heat Map

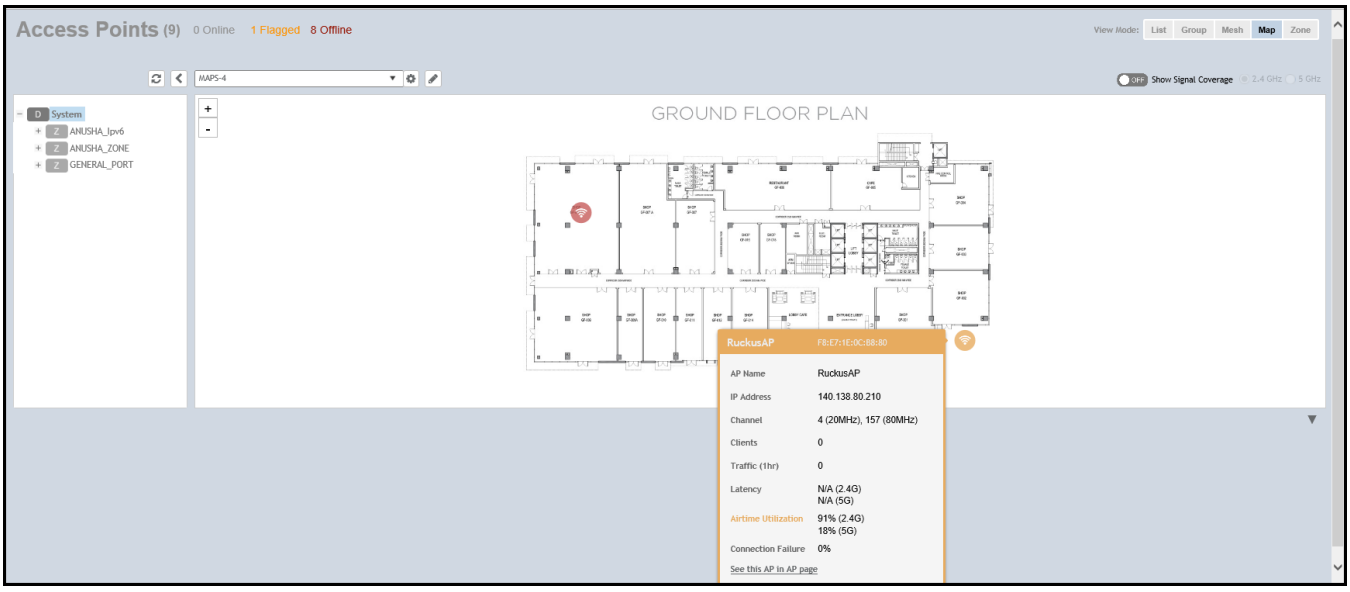


Monitoring APs Using the Map View

Use the Map view on the **Access Points** page to monitor APs in relation to your venue's floorplan.

1. Go to **Network** > **Wireless** > **Access Points**.
2. In **View Mode**, click the **Map** button. The map view is displayed with your placed APs.
3. Hover over an AP to view the following AP-specific details:
   - **AP Name**: The name of the AP, if configured. If not, the default AP name is "RuckusAP."
   - **IP Address**: The current IPv4 or IPv6 address assigned to the AP.
   - **Channel**: Displays the channel (2.4 GHz / 5 GHz) in use, along with the channel width in parentheses.
   - **Clients**: The number of currently connected wireless clients.
   - **Traffic**: The total traffic volume over the last 1 hour.
   - **Latency**: The average time delay between AP and connected clients.
   - **Airtime Utilization**: Percent of airtime utilized, by radio.
   - **Connection Failure**: Percent of client connection attempt failures.

   FIGURE 96 Hover to AP to view details



4. To view more specific details on the AP, click the **See this AP in AP page** link.
5. To view the RF signal strength, select the **Show Signal Coverage** check box and choose the required RF frequency. For example, 2.4 GHz or 5 GHz.

   The heat map is displayed with a color-gradient legend. High signal strength appears in red. The color changes as the signal strength reduces.

Working with Switches

Managing ICX Switches from SmartZone

Supported ICX Models

The following ICX switch models can be managed from SmartZone:

- ICX 7150
- ICX 7250
- ICX 7450
- ICX 7550
- ICX 7650
- ICX 7850

The following table defines ICX and SmartZone release compatibility.

NOTE
ICX switches must be running FastIron 08.0.80a at a minimum to connect to SmartZone.
An ICX switch running unsupported firmware can still connect to the SmartZone controller. After the switch is connected, you must upgrade it to a firmware version that is compatible with the SmartZone controller version. This can be achieved using the switch firmware upgrade option in the Switch Group or by selecting one or more switches and performing the upgrade.

NOTE
ICX switches with FIPS mode enabled do not support management by SmartZone.

NOTE
FastIron 09.0.10a and later releases support management by SmartZone 6.1 and above.

TABLE 86 ICX and SmartZone Release Compatibility Matrix

	SmartZone 5.0[1]	SmartZone 5.1[1]	SmartZone 5.1.1	SmartZone 5.1.2	SmartZone 5.2	SmartZone5.2.1	SmartZone 6.0	SmartZone 6.1
FastIron 08.0.80	Yes	Yes	Yes[1]	No	No	No	No	No
FastIron 08.0.90a	No	No	Yes	Yes	Yes	Yes	No	No
FastIron 08.0.91	No	No	Yes	Yes	Yes	No	No	No
FastIron 08.0.92	No	No	No	Yes	Yes	Yes	Yes	Yes
FastIron 08.0.95 and subsequent patches	No	No	No	No	No	No	Yes	Yes

[1] Does not support ICX configuration.

TABLE 86 ICX and SmartZone Release Compatibility Matrix (continued)

	SmartZone 5.0[1]	SmartZone 5.1[1]	SmartZone 5.1.1	SmartZone 5.1.2	SmartZone 5.2	SmartZone5.2.1	SmartZone 6.0	SmartZone 6.1
FastIron 09.0.10a	No	No	No	No	No	No	No	Yes

The following table provides details on switch management feature compatibility between ICX and SmartZone releases.

TABLE 87 Switch Management Feature Compatibility Matrix

Feature	SmartZone Release	ICX FastIron Release
Switch Registration	5.0 and later	08.0.80 and later
Switch Inventory	5.0 and later	08.0.80 and later
Switch Health and Performance Monitoring	5.0 and later	08.0.80 and later
Switch Firmware Upgrade	5.0 and later	08.0.80 and later
Switch Configuration File Backup and Restore	5.0 and later	08.0.80 and later
Client Troubleshooting: Search by Client MAC Address	5.1 and later	08.0.80 and later
Remote Ping and Traceroute	5.1 and later	08.0.80 and later
Switch Custom Events	5.1 and later	08.0.80 and later
Remote CLI Change	5.2.1 and later	08.0.90 and later
Switch Configuration: Zero-Touch Provisioning	5.1.1 and later	08.0.90a and later
Switch-specific Settings: Hostname, Jumbo Mode, IGMP Snooping, and DHCP Server	5.1.1 and later	08.0.90a and later
Switch Port Configuration	5.1.1 and later	08.0.90a and later
Switch AAA Configuration	5.1.1 and later	08.0.90a and later
Switch Client Visibility	5.1.2 and later	08.0.90a and later
Manage Switches from Default Group in SZ-100 / vSZ-E	5.1.2 and later	08.0.90a and later
DNS-based SmartZone Discovery	5.1.2 and later	08.0.95c and later
Download Syslogs for a Selected Switch[2]	5.2.1 and later	08.0.91 and later
Switch Topology	5.2 and later	08.0.92 and later
Designate a VLAN as Management VLAN	5.2.1 and later	08.0.92 through 09.0.10a and subsequent patches
Change Default VLAN	5.2.1 and later	08.0.95 and later
Configure the PoE Budget per Port on ICX through the Controller GUI with 1W Granularity	5.2.1 and later	08.0.95 and later
Configuring Protected Ports	5.2.1 and later	08.0.95 and later
Configuring QoS	5.2.1 and later	08.0.95 and later
Configuring Syslog	5.2.1 and later	08.0.95 and later
Geo Redundancy Active-Standby Mode	6.0 and later	08.0.95b and later
Generic CLI Configuration	6.0 and later	08.0.95b and later
Port-Level Override	6.0 and later	08.0.95b and later

[1] Does not support ICX configuration.
[2] To download system logs from SmartZone for a particular ICX switch, TFTP must be enabled.

TABLE 87 Switch Management Feature Compatibility Matrix (continued)

Feature	SmartZone Release	ICX FastIron Release
Port-Level Storm Control Configuration	6.1 and later	08.0.95 and later
IPv6 Support (connection through static configuration only)	6.1 and later	09.0.10a and later
Save Boot Preference	6.1 and later	09.0.10a and later
Virtual Cable Testing	6.1 and later	09.0.10a and later
Blink LEDs	6.1 and later	09.0.10a and later
Send Event Email Notifications at Tenant Level	6.1 and later	09.0.10a and later
Update the Status of a Switch	6.1 and later	09.0.10a and later
Convert Standalone Switch	6.1 and later	09.0.10a and later
Flexible Authentication Configuration	6.1 and later	09.0.10a and later

Overview of ICX Switch Management

Beginning with SmartZone 5.0, the SmartZone administrator can monitor and manage switches and routers in the ICX 7000 series. SmartZone 5.1.1 introduced the capability to configure switches.

SmartZone ICX-Management supports the following ICX switch activities:

- Registration and authentication
- Switch inventory (for example, model, firmware version, and last backup)
- Health and performance monitoring (for example, status, traffic statistics, errors, and clients) with alarms
- Zero-touch provisioning
- Configuration changes
- Port settings
- Configuration copy
- Configuration file backup and restore
- Firmware upgrade
- Client troubleshooting
- Remote Ping and Traceroute

NOTE
Refer to the Supported ICX Models on page 235 for more details.

Preparing ICX Devices to be Managed by SmartZone

NOTE
For more information on ICX device capabilities and configuration, refer to the RUCKUS FastIron documentation set available at the following URL:
https://support.ruckuswireless.com. On the site, select **Products > Ruckus ICX Switches > Technical Documents**, and choose the platform and document of interest.

ICX devices running either router or switch images can be managed by SmartZone. The following items are required to manage ICX devices:

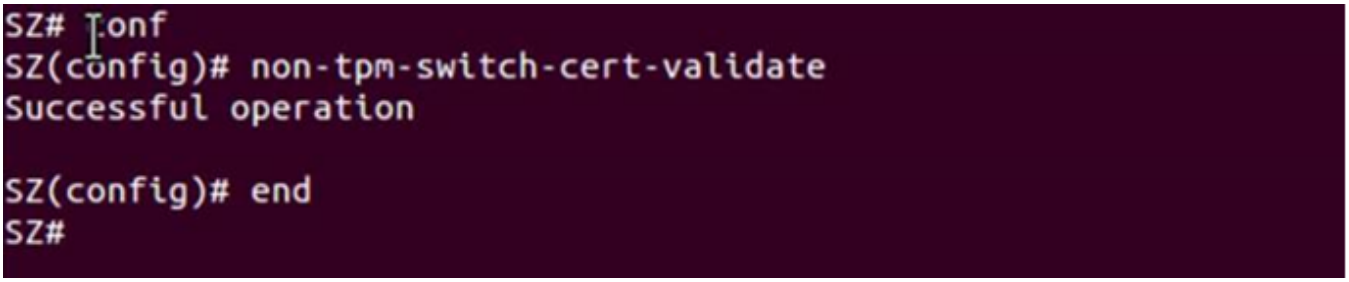
NOTE
Refer to the Supported ICX Models on page 235 for detailed information on software compatibility requirements and feature availability.

- The SmartZone IP address must be reachable by the ICX device through the Management interface or through switch or router interfaces.
- The ICX device must be made aware of the configured SmartZone IP address in one of the following ways:
  - Configure the DHCP server to use DHCP option 43.
  - Issue the following command at the global configuration level:

    ```
    ICX(conf)# manager active-list SmartZone_Control_IP_Address
    ```

  - Add an entry in the DNS server with the hostname ruckuscontroller or ruckuscontroller.*local domain* that points to the SmartZone IP address.
- On some ICX 7250 and ICX 7450 devices, self-signed certificates are used. SmartZone honors these certificates when the **non-tpm-switch-cert-validate** command is entered on the SmartZone console, as shown in the following example.

FIGURE 97 Command Required to Disable Certificate Check



NOTE
ICX 7150, ICX 7650, and ICX 7850 devices are shipped with embedded certificates that are used for authentication with SmartZone.

- When SmartZone or ICX devices are behind network address translation (NAT), be sure to forward TCP ports 443 and 22 through NAT.
- Virtual platform requirements for supporting ICX devices are listed in the following table.

NOTE
Each unit in a stack is considered a separate switch unit for capacity management purposes.

TABLE 88 Virtual Platform Requirements for Supporting ICX Devices

Platform	Maximum Number of Switches Per Node	RAM	vCPU	Disk Storage
vSZ-E	200	18 GB	4	100 GB
vSZ-H	2000	30 GB	12	300 GB

The scaling limits in the table apply to switch-only deployments. For a mix of APs and switches, the scaling limits vary accordingly. SmartZone supports a 5-to-1 AP-to-switch ratio.

vSZ-E Example: vSZ-E supports up to 1,000 APs on a single node. If 200 APs are currently managed by SmartZone, there is room for 800 more APs or 160 ICX switches (800 divided by 5).

vSZ-H Example: vSZ-H supports up to 2,000 ICX switches on a single node. If 500 switches are currently managed, there is room for 1,500 more switches, or 7,500 APs (1500 multiplied by 5).

VIDEO
Onboarding ICX Switches to SmartZone. Using CLI commands to establish and verify switch connectivity to SmartZone.
Click to play video in full screen mode.

ICX Switch Behavior with SmartZone

NOTE
The full range of ICX-Management capabilities (including configuration support in SmartZone 5.1.1 or later) is available only when ICX devices have been upgraded to FastIron 08.0.90a or later using a Unified Forwarding Image (UFI). Beginning with FastIron 08.0.90, RUCKUS ICX devices support unified images that require custom upgrades from prior releases. Any ICX switch that is running a FastIron 08.0.80 non-UFI image on the ICX switch must follow a two-step image upgrade process to FastIron 08.0.90a through SmartZone controller image updates. If an ICX switch from the factory has a FastIron 08.0.80 non-UFI image, it must first be upgraded with a FastIron 08.0.90 UFI, followed by a FastIron 08.0.90a UFI, to avoid any boot configuration issues. Refer to the *RUCKUS FastIron Software Upgrade Guide* for more information.

NOTE
Campus Fabric (SPX) is not compatible with SmartZone. When SPX is enabled using the **spx cb-enable** command, SmartZone is disabled automatically. The following messages and syslog entry are displayed.

```
Console message
===============
Disabling SZ since SPX is enabled...
SZ Disable Initiated...
SZ Connection would be disconnected now if connected...

Syslog
=======
Aug  4 00:57:14:W:SZ:Disabling SZ, because SZ is not supported in SPX
```

If SPX is enabled on an ICX device and you try to enable SmartZone using the **no manager disable** command, the following warning message is displayed.

```
ICX(config)# no manager disable
SZ configuration is not allowed in SPX enabled setup. Please disable SPX to enable SZ
When ICX is managed through SZ, if 'spx cb-enable' is configured, SZ will be disconnected from ICX.
```

When an ICX switch is managed by SmartZone, the following considerations apply:

- All local configuration methods continue to be available to the local administrator, which means the switch can be configured through the console, Telnet, SSH, SNMP, or the web.
- It is recommended that the ICX switch be configured with the same NTP server as SmartZone.
- In an ICX stack, if a stack switchover or failover occurs, the original connection to SmartZone is closed, and the new active switch initiates a connection with SmartZone.

Enabling an ICX Device to Be Managed by SmartZone

There are several ways to make an ICX device aware of the SmartZone IP address:

- Use switch registrar discovery.
- Use DHCP option 43.
- Configure the ICX device manually using FastIron commands.

All of these methods are supported for new ICX switches with no configuration as well as for ICX switches with existing configuration.

Configuring the ICX Source Address to Be Used by SmartZone

By default, the IP address of the management port is included in the manager query as the ICX source address for an ICX-Management connection. Use the **management source-interface protocol manager** command to specify a different ICX source address.

> **NOTE**
> Only ICX devices with a router image support the **management source-interface protocol manager** command.

The **management source-interface protocol manager** command can specify an Ethernet, LAG, loopback, or virtual Ethernet (VE) interface. The IP address with the lowest number for the specified interface is used for the connection.

The following example configures an Ethernet port as the ICX source address for an ICX-Management connection.

```
ICX# configure terminal
ICX(config)# management source-interface ethernet 1/1/3 protocol manager
```

Refer to the *RUCKUS FastIron Command Reference* for more information.

Setting Up Switch Registrar Discovery

The switch registrar is a RUCKUS-hosted cloud service that enables SmartZone discovery from ICX devices.

You can configure the ICX device to retrieve the correct SmartZone management IP address, IP address set, or fully qualified domain name (FQDN) from the switch registrar. The switch registrar must be set up in advance through Managed Service Provider (MSP) with SmartZone IP addresses or an FQDN and the ICX serial numbers they can manage.

> **NOTE**
> If SmartZone management is not enabled on the ICX device, switch registrar discovery does not occur.

How Switch Registrar Discovery Works

The ICX device sends an HTTP GET message to a default server host, sw-registrar.ruckuswireless.com, for the list of SmartZone management IP addresses or an FQDN, unless the system administrator configures an alternate host. The SmartZone IP address or FQDN obtained in response to the GET message is used to query the SmartZone device to set up a connection. If the ICX device receives a set of IP addresses from the switch registrar, it stores the information and tries the addresses in turn until a successful connection is established with the SmartZone device. The IP address, set of IP addresses, or FQDN obtained through the switch registrar is given priority above all other addresses in the list of SmartZone IP addresses, including addresses received from other sources such as the DHCP list, the active list, and the backup list. Once the ICX device has obtained a SmartZone IP address from the switch registrar, it no longer attempts switch registrar discovery.

This query is performed only for greenfield deployments and when the ICX device boots up with no startup configuration. ICX switches being upgraded from older releases that already have a configuration in place will not have the registrar-based SmartZone discovery turned on. The HTTPS session used for the database query uses the device certificate installed on the switch for SSL session establishment. For the initial release of the switch registrar, no server certificate validation will be performed.

Disabling or Enabling Switch Registrar Discovery

The system administrator can disable or enable switch registrar discovery from the command line.

> **NOTE**
> The registrar IP list is removed when you disable the switch registrar.

To disable switch registrar discovery, enter the **no manager registrar** command in global configuration mode, and use the **write memory** command to save the change, as shown in the following example.

```
ICX# configure terminal
ICX(config)# no manager registrar
ICX(config)# write memory
```

To restart the switch registrar discovery process, use one of the following commands at the privileged EXEC level:

- **manager registrar-query-restart**
- **manager reset**

To enable switch registrar discovery on an alternate registrar host server and save the entry to the startup configuration, enter the following commands.

```
ICX# configure terminal
ICX(config)# manager registrar sw-alternate.ruckuswireless.com
ICX(config)# write memory
```

NOTE
The **manager registrar** *hostname* command is for test purposes only. The **manager registrar-query-restart** command by itself is sufficient to initiate registrar-based SmartZone discovery.

Confirming Successful Switch Registrar Discovery

To display log entries specific to registrar queries, use the **show manager log** command.

When the switch registrar database has been successfully queried, a syslog message similar to the following is displayed.

```
Aug 8 21:47:17:I:MGMT Agent: SZ Switch Registrar Query to 54.186.143.194 Success
```

When the ICX device requires a restart to connect to the SmartZone address because a new registrar list has been received, a syslog message similar to the following is displayed.

```
Aug 8 21:47:17:I:MGMT Agent: Disconnect to SZ: 54.16.143.194, Got SZ ip via registrar
```

You can use the **show running-config** command to check for the name of the registrar host and the registrar list of SmartZone IP addresses.

The following example indicates that the ICX device uses the default switch registrar host and has obtained one SmartZone IP address (of a possible set of two addresses).

```
ICX# show running-config
!
!
manager registrar
manager registrar-list 23.251.150.119
!
!
```

You can also enter the **show manager status** command to obtain information on the switch registrar, as shown in the following example.

```
ICX# show manager status

============    MGMT Agent State Info     ===================

Config Status:Enabled Operation Status:Enabled
State:SSH CONNECTED  Prev State:SSH CONNECTING             Event:SZ_SSH_CONNECT_EVENT

SWR List                          : None
DNS List                :
Active List             : 10.176.160.116
Active List IPV6        : 2620:107:90d0:ab40::116
DHCP Option 43          : No
DHCP Opt 43 List        : None
```

```
Backup List             : None
Backup List IPV6        : None
Merged List             : 2620:107:90d0:ab40::116 10.176.160.116

SZ IP Used              : 2620:107:90d0:ab40::116
Port List               : 987
Server Port Used        : 443
Query Status            : APPROVED

SSH Tunnel Status -:
Tunnel Status           : Established
CLI IP/Port             : 127.255.255.253/59449
SNMP IP/Port            : 127.255.255.254/8253
Syslog IP/Port          : 127.0.0.1/20514
HTTP CLIENT IP/Port     : 127.0.0.1/5080
HTTP SERVER IP/Port     : 127.255.255.252/63098
Timer Status            : Not Running
```

Troubleshooting Switch Registrar Discovery

In the event that switch registrar discovery fails, check for the following conditions:

- The running configuration contains "manager disable".
- The switch registrar is not configured on the ICX device.
- The DNS configuration needed to resolve the switch registrar address is not present on the ICX device.
- The ICX device could not reach the switch registrar due to routing issues.

NOTE
If the switch registrar is enabled and you enter the **no manager disable** command, switch registrar discovery is still started when the registrar IP list is empty.

NOTE
The switch registrar discovery process continues to run until the configuration issues are fixed, a successful query result is obtained, or you enter a command to disable the switch registrar.

Preparing Stacking Devices to Connect to SmartZone

Consider the following guidelines when preparing ICX stacking devices to be discovered and managed by SmartZone:

- Define the stack configuration on the SmartZone device before connecting cables between the SmartZone and ICX devices.
- The devices to be managed in the stack must be part of a "firmware version" switch group configured on the SmartZone device.

If only the ICX device intended to be the stack active controller is an active switch under SmartZone control and is part of a configured "firmware version" switch group, perform the following steps to establish a stack:

- Connect all cables between ICX devices to form the desired stack configuration.
- On the active controller, enter the following commands in privileged EXEC mode:
  - **stack enable** (enables stacking on the active controller)
  - **stack zero-touch-enable** (triggers automatic discovery of the stack units and connections)
  - **write memory** (saves the running configuration to startup flash)

  No commands need to be entered on the other stack units in this case.

If all switches intended to be members of a stack have already joined and have been approved by SmartZone and are already part of a "firmware version" switch group, enter the following commands on the ICX devices to form a stack:

- On the active controller, enter the following commands in privileged EXEC mode:
  - **stack enable** (enables stacking on the active controller)

  - **stack zero-touch-enable** (triggers automatic discovery of the stack units and connections)
  - **write memory** (saves the running configuration to startup flash)
- On all other prospective stack members, configure the following commands in global configuration mode:
  - **stack suggested-id**
  - **stack ztp-force**
  - **write memory**

Configuring DHCP to Provide SmartZone IP Addresses to an ICX Switch

A DHCP server can be configured to send SmartZone IP addresses to ICX devices using DHCP Option 43.

Configure DHCP Option 43 on the DHCP server, using **RKUS.scg-address** to identify the SmartZone IP addresses.

A single SmartZone IP address or a comma-separated list can be configured. SmartZone IP addresses are sent with a sub-option value of 6. The ICX device ignores all other data in DHCP Option 43 if SmartZone IP addresses are present.

The following example shows a DHCP Option 43 configuration on a DHCP server. The IP addresses listed are examples only.

```
subnet 192.168.12.0 netmask 255.255.255.0 {
   range  192.168.12.100 192.168.12.199;
   option routers 192.168.12.1;
   option subnet-mask 255.255.255.0;
   option broadcast-address 192.168.12.255;
   option ntp-servers 192.168.11.22;
   class "Ruckus AP" {
      match if option vendor-class-identifier = "Ruckus CPE";
      option vendor-class-identifier "Ruckus CPE";
      default-lease-time 86400;
      vendor-option-space RKUS;
      option RKUS.scg-address "192.168.11.200, 192.168.11.201, 192.168.11.202";
   }
}
```

Manually Configuring the SmartZone IP Address on an ICX Switch

Complete the following steps to configure a list of SmartZone IP addresses on the ICX device.

1. Enter the **manager active-list** command followed by one or more priority IP addresses for the SmartZone device, as shown in the following example.

   The IP addresses listed are examples only.

   ```
   ICX# configure terminal
   ICX(config)# manager active-list 192.168.11.200 192.168.11.201 192.168.11.202
   ```

2. Use the **sz passive-list** *ip-address* command to configure the SmartZone IP addresses to be used for redundancy.

   ```
   ICX(config)# sz passive-list 10.176.160.118
   ```

Displaying the SmartZone Connection Status

Use the **show manager status** command to display the SmartZone IP address lists and information about the status of the connection.

```
ICX7450-24# show manager status

============    MGMT Agent State Info     ===================

Config Status:Enabled Operation Status:Enabled
State:SSH CONNECTED  Prev State:SSH CONNECTING             Event:SZ_SSH_CONNECT_EVENT
```

```
SWR List                              : None
DNS List                 :
Active List              : 10.176.160.116
Active List IPV6         : 2620:107:90d0:ab40::116
DHCP Option 43           : No
DHCP Opt 43 List         : None
Backup List              : None
Backup List IPV6         : None
Merged List              : 2620:107:90d0:ab40::116 10.176.160.116

SZ IP Used               : 2620:107:90d0:ab40::116
Port List                : 987
Server Port Used         : 443
Query Status             : APPROVED

SSH Tunnel Status -:
Tunnel Status            : Established
CLI IP/Port              : 127.255.255.253/59449
SNMP IP/Port             : 127.255.255.254/8253
Syslog IP/Port           : 127.0.0.1/20514
HTTP CLIENT IP/Port      : 127.0.0.1/5080
HTTP SERVER IP/Port      : 127.255.255.252/63098
Timer Status             : Not Running
```

Disconnecting the Switch Connection with SmartZone

The **manager disconnect** command can be used to disconnect the ICX switch from SmartZone and initiate a new connection based on the currently available list of SmartZone IP addresses.

Enter the **manager disconnect** command as shown.

This command can be executed on the local terminal.

```
ICX# manager disconnect
SZ Disconnect initiated...
```

Disabling SmartZone Management on the ICX Switch

When SmartZone management is disabled on the switch, the switch will not initiate a connection with SmartZone even if a SmartZone IP address is available.

Enter the **manager disable** command to disable SmartZone management on the ICX switch.

```
ICX(config)# manager disable
```

SmartZone Switch Management

Using Controller Settings to Manage Switch Groups

Controller allows you to create switch groups, similar to AP zones. Switches connecting to controller can be placed in one of these logical groups for better manageability. A Staging or Default Group is created by the controller automatically. All switches are placed in this group when they initially joining the controller. You have the option to create additional groups.

NOTE
In SZ300 and vSZ-H platforms, a warning message is displayed to move the switches from the Staging Group to another group for controller to monitor.

Using registration rules, you can specify which group the switch should be placed into. Refer to Creating Switch Groups on page 245 and Creating Switch Registration Rules on page 246 for additional information.

Creating Switch Groups

You can group switches based on your need, for example, you can group switches based on their size or their location.

You can only create a maximum of two levels within the group hierarchy. By default, all the switches are placed under the default switch group. You can create a group or sub-group and then move the switch under it. You can also modify or delete a group at any time.

After the switch is registered with the controller interface, you can monitor, view status or usage, and perform some basic management, including configuration backups and firmware management. However, you cannot configure the switch from the controller web user interface.

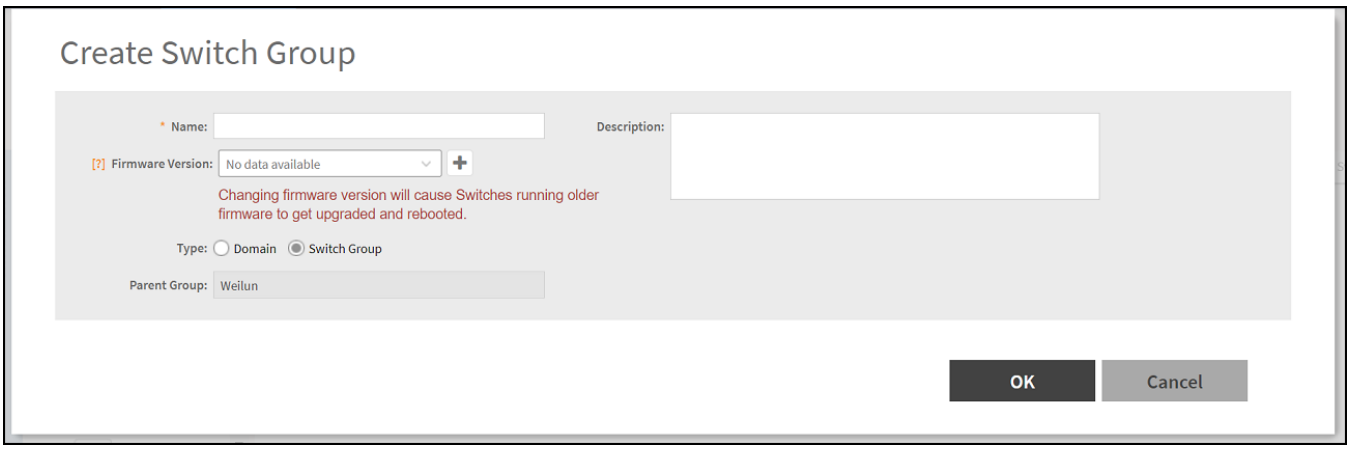
1. From the main menu, go to **Network** > **Wired** > **Switches**.

   The **Switches** page appears.

2. Click .

   The **Create Group** page appears.

   FIGURE 98 Creating switch groups

   Configure the following:

   - Name: Type the name of the switch group that you want to create
   - Description: Enter a brief description for the switch group
   - Type: Select **Switch Group**. For enterprise devices such as SZ-300 and vSZ-H, you also have the option to select **Domain**.
   - Parent Group: Displays the parent group under which the switch group resides
   - Firmware Version: Select the Firmware version (optional) which will automatically upgrade the switches (running an older version) joining the group.
   - Managed by Partner: This option is available if you select the group type as **Domain**. You can slide the radio button to ON or OFF to enable or disable partners from managing the switches.

3. Click **OK**.

   The switch group is created under the selected parent group.

Creating Switch Registration Rules

You can create registration rules for switch groups, which are identified and approved by the controller to establish connections. Typically, the switch is registered with the controller using an IP address, subnet, or model number.

Complete the following steps to create a registration rule.

1. From the main menu, go to **Network** > **Wired** > **Switch Registration**.

   The **Switch Registration** page is displayed.

2. Click **Create**.

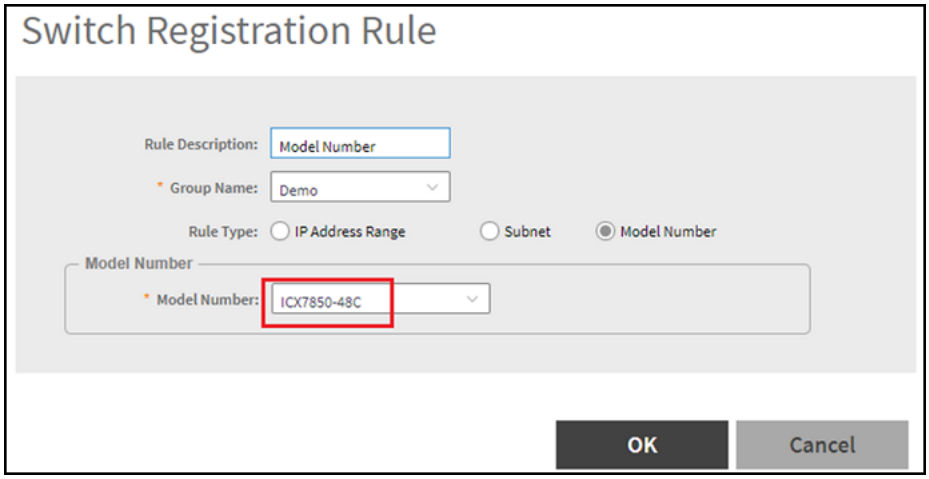
   The **Switch Registration Rule** dialog box is displayed.

   Enter the following details:

   - **Rule Description**: Provide a brief description of the registration rule you are creating to put the switches into specific groups.
   - **Group Name**: Select the switch group to which you want to apply this rule from the list.
   - **Rule Type**: Select **IP Address Range**, **Subnet**, or **Model Number** to apply the rule to the switch based on the rule type.

     If you select **IP Address Range**, you must provide the range of the IP addresses for which this rule will apply. If you select **Subnet**, you must provide the network address and subnet mask that will apply to the rule. If you select **Model Number**, you must provide the model number of the device.

   FIGURE 99 Creating Registration Rules



3. Click **OK**.

   You can edit, copy and delete the rule by selecting the rule and clicking **Configure**, **Clone**, and **Delete**, respectively.

   TAfter the registration rules are created, they can be rearranged using the **Up** and **Down** options. They can be arranged in an order of priority. After the order of priority for the list of rules is finalized, click **Update Priority** to confirm.

Approving Switches

The switch must be approved so that it can be discovered and monitored by the controller.

- Switches that do not match any registration rule are automatically in the default group.
- At this point, a switch is not managed and the status is shown as offline.

- To actively manage a switch in this predicament, you must move it from the staging group to any other switch group or domain in SZ300 and vSZ-H platforms. In SZ100 and vSZ-E platforms, the default group behavior is similar to any other group. Refer to Moving the Switches between Groups on page 247 for more information.

  NOTE
  A switch capacity license (CAPACITY-SWITCH-DEFAULT) is available for controllers and switches managed by the controllers. The license is activated for devices running SmartZone 5.1 or later. Upgrading to SmartZone 5.1 from an earlier version activates the license by default. A 90-day license version is then available for trial or purchase. The controller manages switches only as defined in the Switch Capacity license and rejects individual switches or stacks when license capacity is reached. Any switch that exceeds license limits is moved to the service group, where it cannot be configured. When license capacity is again available, the controller accepts the switch for management. For the controllers (SZ100 or SZ300), a trial license will allow adding the maximum number of switches supported. In the case of vSZ-E or vSZ-H, a trial license will allow the addition of 5 switches.

  NOTE
  Based on the switch capacity license (CAPACITY-SWITCH-HA), you can approve a failover switch on a standby cluster to switch over to the original cluster.

The recommendation is to always use switch registration rules so that the switches are placed in the correct switch group and avoid manual intervention.

Moving the Switches between Groups

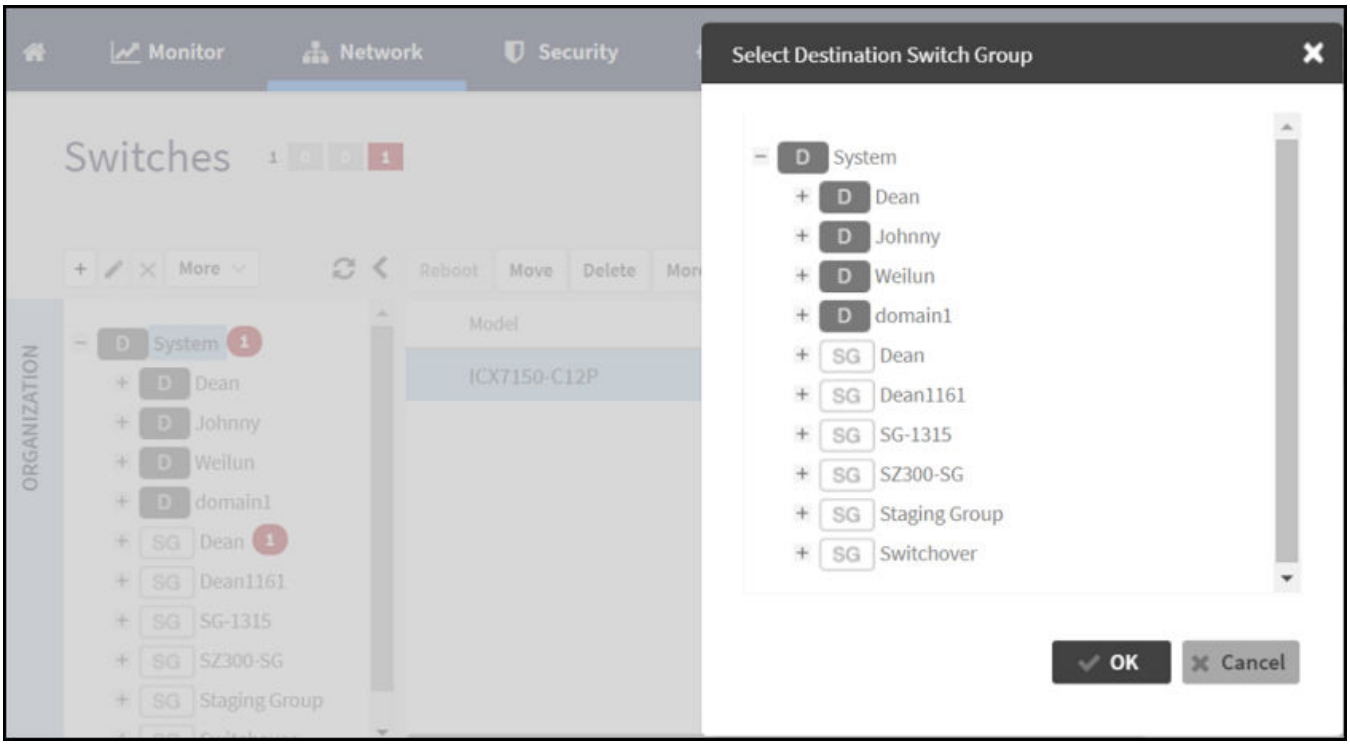
You can move the switches within any group or sub-group within the system hierarchy to manage it.

1. From the main menu, go to **Network** > **Wired** > **Switches**.

   The **Switches** page appears.

2. From the **Switches** page, select the switch that you want to move and click **Move**.

   FIGURE 100 Moving the switch



   The **Select Destination Switch Group** page appears. It displays the system hierarchy from which you can select the group under which you want to move the switch.

Deleting Switches

You can delete switches that you do not want the controller to manage anymore.

1. From the main menu, go to **Network** > **Wired** > **Switches**.

   The **Switches** page appears.

2. Select the switch you want to delete and click **Delete**.

   The selected switch is deleted, and it will not be managed by the controller interface.

Backing up and Restoring Switch Configuration

The controller can back up the switch's running configuration. By default, controller makes a backup of switch configuration on a daily basis. The configuration is only stored if there is a change between the last configuration backup and the current backup. Otherwise, it is discarded. Controller saves the last seven configuration backups. When needed, these backups can be restored to the switch. While performing network maintenance, you can initiate a backup without having to wait for the daily backup.

Perform the following steps to configure switch backups.

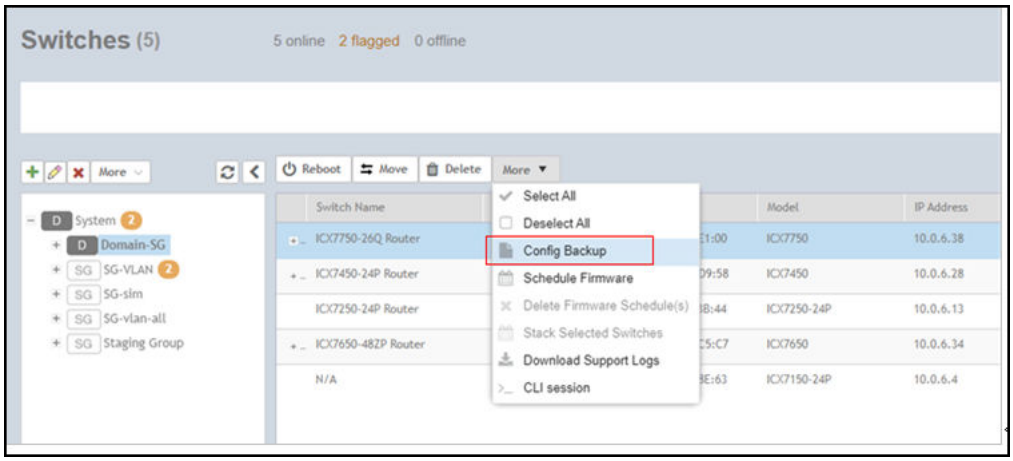
NOTE
Be sure to sync the controller to the NTP server during installation. You can do this by selecting **Administration** > **Time**.

1. From the main menu, go to **Network** > **Wired** > **Switches**.

   The **Switches** page is displayed.

2. From the **Switches** page, select the switch for which you want to backup the configuration and click **More**.

FIGURE 101 Configuring Backup



3. From the drop-down menu, select **Config Backup**.

   A confirmation message is displayed asking whether to continue with the backup.

4. Click **Yes**. A message is displayed confirming that the backup process has been initiated.

   After the backup is completed, the status is recorded in the **Backup & Restore** tab.

NOTE

- As soon as the switch connects to the controller, and when it is online, the controller retrieves all the information about the switch.
- The controller maintains seven of the latest configuration backups for each switch.
- The controller automatically backs up the configuration of each switch, once, every 24 hours.
- If a previous switch configuration matches the current configuration, the latest configuration is saved and the old configuration is removed.

You can restore an individual switch to its previous configuration by clicking **Config Restore**. A message is displayed stating the restore operation is initiated and that the system must be rebooted for the configuration changes to take effect.

For switches, you can click **Config Diff** to view differences in configuration details, click **Config View** to see the configuration details from the **Switch Config View** screen and click **Config Download** to download the copy of the configuration file.

You can delete a configuration file by selecting it and clicking **Delete**.

Rehoming Switches

Rehoming is the process of returning the switches that have failed over to the standby cluster back to their original cluster (once it becomes available). Rehoming must be done manually. Switches that have failed over continue to be managed by the failover cluster until you rehome them.

NOTE
You can rehome switches only in a cluster redundancy environment. When switches of a certain active cluster fail over to a standby cluster, you must manually restore them to the original cluster after the active cluster is fixed and back to service.

Complete the following steps on the standby cluster to rehome switches to the original cluster:.

1. Select **Network** > **Switches** > **Switches**.

   The **Switches** page is displayed.
2. From the list, select the switch to rehome.
3. From the system domain, click **More** and select **Rehome Active Cluster**.

   A confirmation dialog box is displayed.
4. Click **Yes**.

Switching Over Clusters

Switchover helps move individual switches or switches in a switch groups across clusters.

NOTE
Ensure that a switch registation rule is created on the target cluster before switching over to another cluster. For more information, refer to Creating Switch Registration Rules on page 246.

NOTE
Depending on the switch High Availability license on the standby cluster switches must be approved so that it can be discovered and monitored by the controller. For more information, refer to Approving Switches on page 246.

Complete the following steps to switch over from one cluster to another.

1. Select **Network** > **Switches** > **Switches**.

   The **Switches** page is displayed.
2. Select a switch group from the left pane or a switch from the right pane.
3. Click **More** on the respective pane and select **Switch Over Cluster**. The **Specify Destination cluster** dialog appears.
4. For **Control IP**, enter the control IP address of the switchover target cluster.
5. Click **OK**. A confirmation dialog box is displayed.
6. Click **OK** to confirm.

Scheduling a Firmware Upgrade for Switch Group

You can upgrade a switch group on a Level 1 group that has no default firmware setting. The forced upgrade allows the device to remain in the same firmware type (Layer 2 still Layer 2, Layer 3 still Layer 3) with only a change to the version type.

NOTE
If the switch group has a default firmware selected the **Firmware Upgrade** option is unavailable.

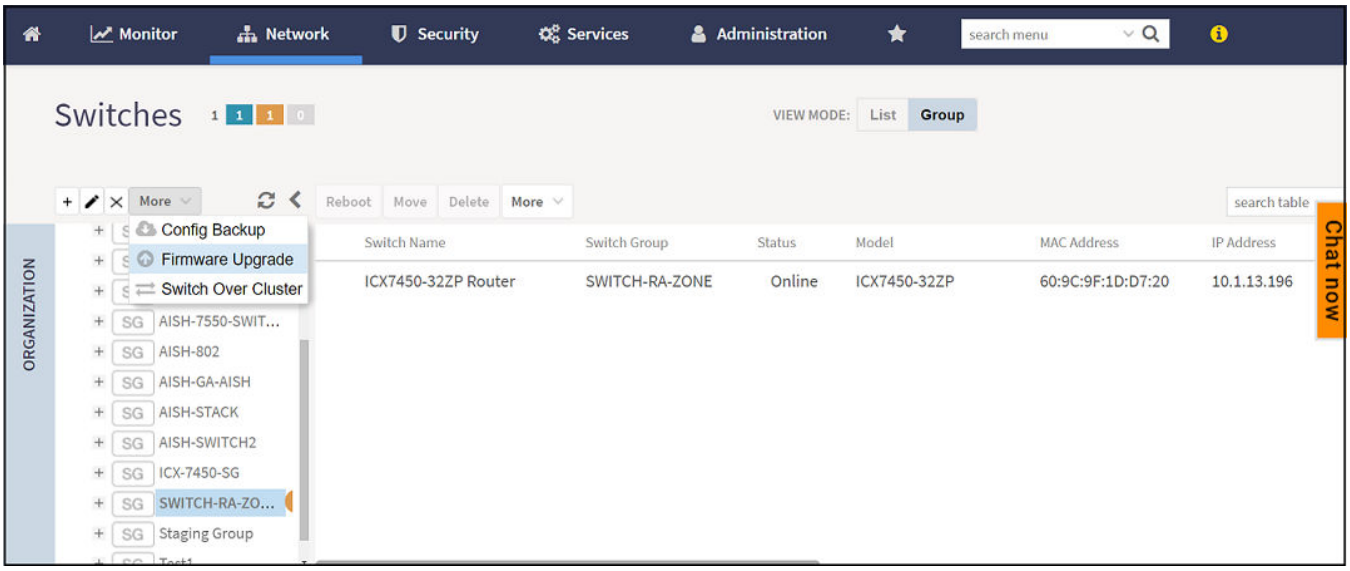
Complete the following steps to perform a firmware upgrade on the switch group.

1. From the main menu, go to **Network** > **Wired** > **Switches**.

   The **Switches** page is displayed.
2. From the **Switches** page, select the switch group.

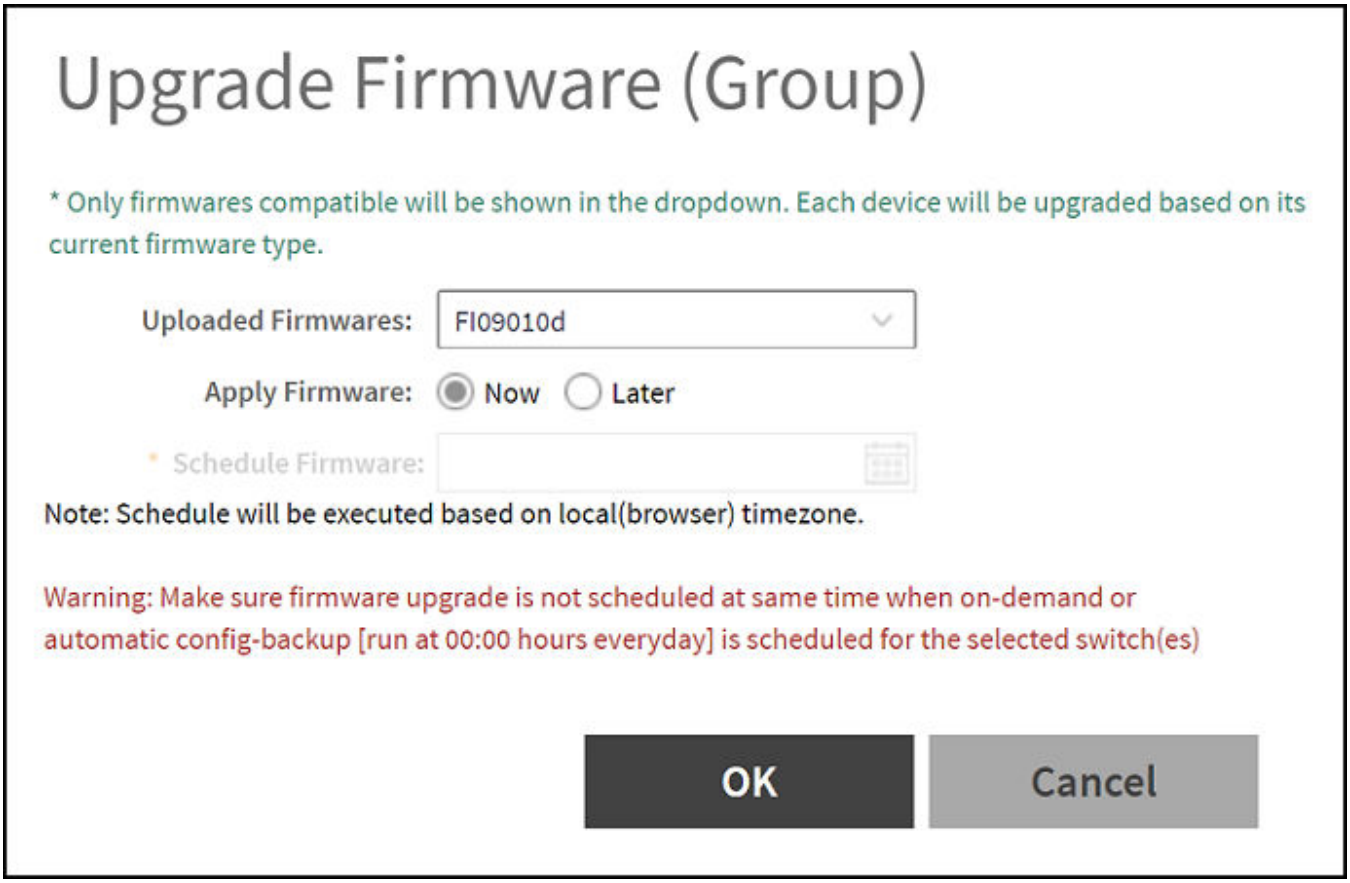
3. Click **More**, and select Firmware Upgrade.

FIGURE 102 Selecting Firmware Upgrade for a Switch Group



The **Upgrade Firmware (Group)** page is displayed.

FIGURE 103 Scheduling the Upgrade for a Switch Group



4. Configure the following options.
   a. **Uploaded Firmwares**: Select firmware from the list.
   b. **Apply Firmware**: Select Now or Later to set the new firmware version to the switch group.
   c. **Schedule Firmware**: If you select Later for **Apply Firmware**, you must select the date to schedule the upload.
5. Click **OK**.

Scheduling a Firmware Upgrade for Selected Switches

You can upgrade or downgrade the firmware version of a switch or multiple switches that you are monitoring. You can upgrade the firmware on demand or schedule a firmware update for a list of selected switches.

Upload a valid firmware which is greater than version 8.0.80 to the controller.

NOTE
Ensure you sync the controller to the NTP server during installation. You can also do this from, go to **Administration** > **System** > **Time** > **Switches**.

To upgrade the firmware for a group of switches, you must select multiple switches at the same time and perform steps 3 to 7. For more information on uploading the switch firmware, see Uploading the Switch Firmware to the Controller on page 642

NOTE
Only firmware versions later than ICX 8.0.80 are supported.

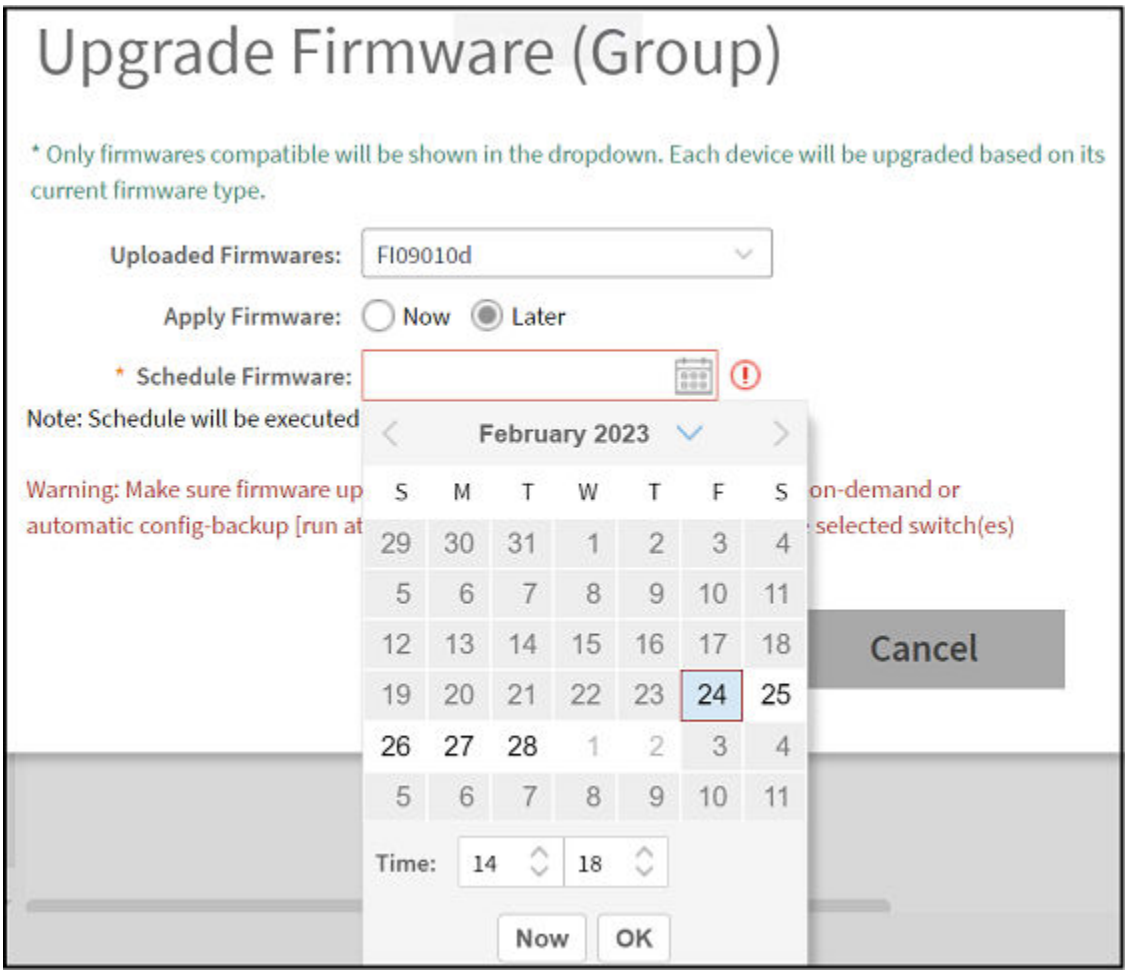
Scheduling Firmware Upgrade

1. From the main menu, go to **Network** > **Wired** > **Switches.**

   The **Switches** page appears.
2. From the **Switches** page, select the switch that you want to upgrade and click **More**.
3. From the drop-down menu, select **Schedule Firmware**.

   The **Upgrade Firmware** page appears.

FIGURE 104 Scheduling Firmware Upgrade



4. From **Uploaded Firmware**, select the firmware version that you want the switch to be upgraded to
5. In **Firmware Type**, select type of firmware you want to upload to the switch. Options include Switch and Router images.
6. In **Apply Firmware**, set when you want to apply the new firmware version to the switch. You can select Now or Later to schedule your upload. If you select Later, then you must select the date from the **Schedule Firmware** field.

7. Click **OK**.

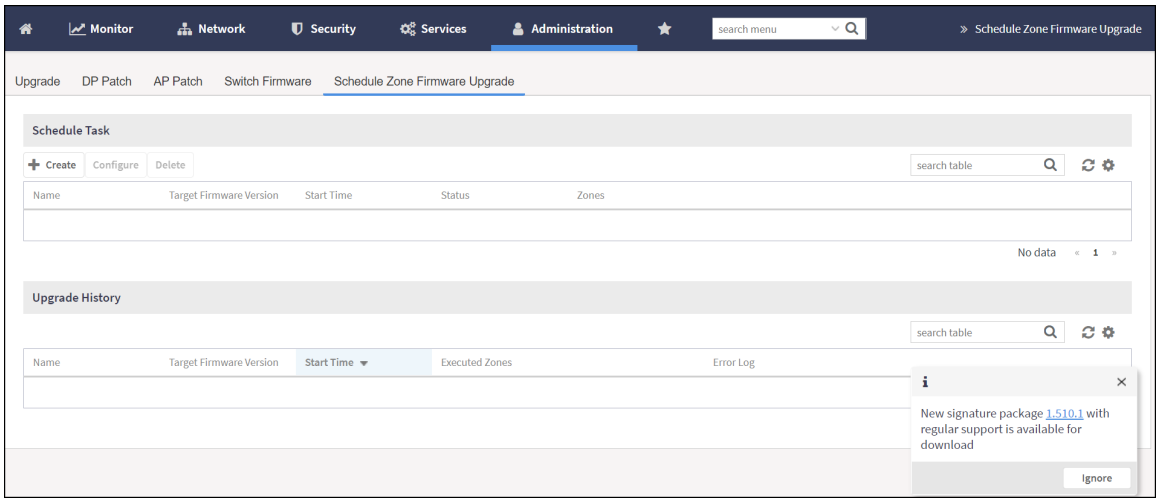
   If you want to delete the schedule you created; From **More**, click **Deleted Firmware Schedule(s)**.

   Schedule Zone Firmware Upgrade

   •Allow user setup a schedule time to upgrade/downgrade single or multiple zone firmware.

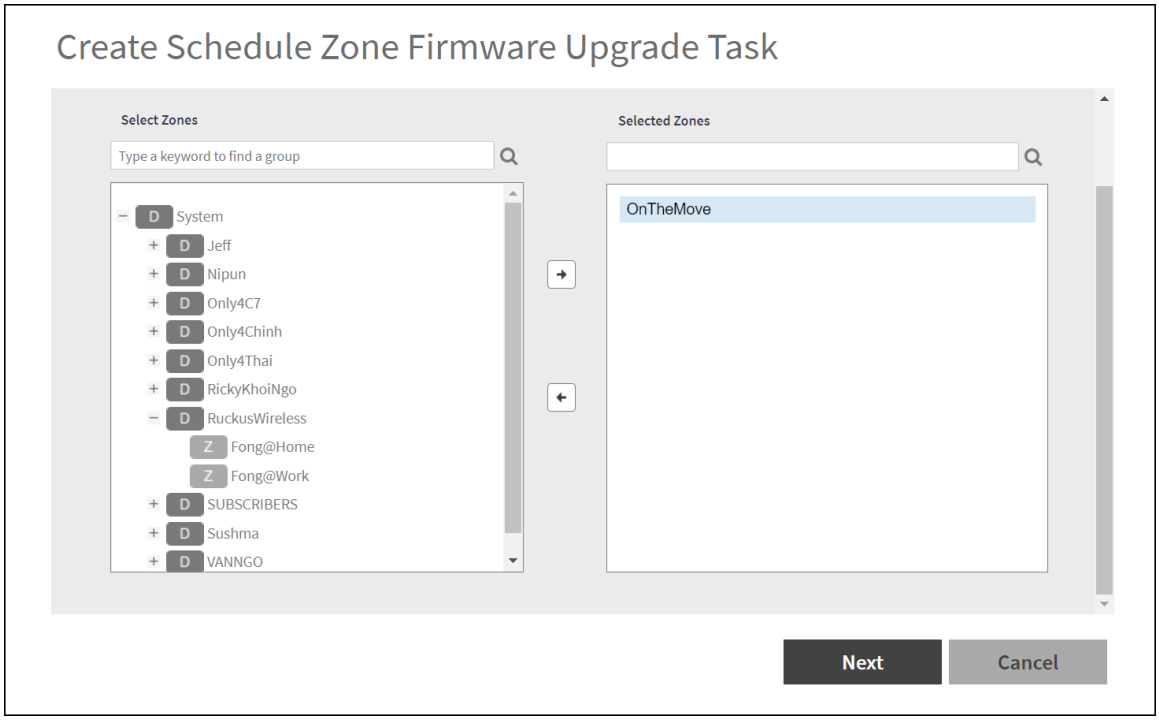
   •After a zone firmware upgrade/downgrade task is executed, user can see the zone firmware change history.

   a. From the main menu, go to **Administration** > **Upgrade** > **Schedule Zone Firmware Upgrade**.

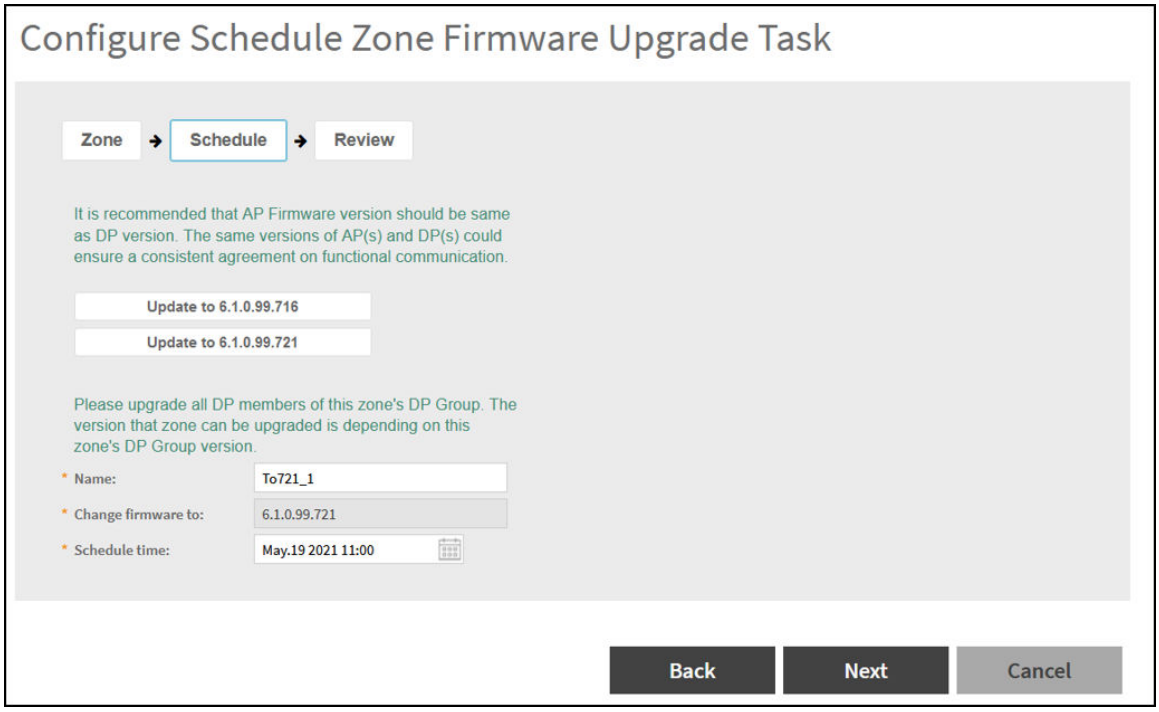


   b. Click "Create"

   c. Add the zone to schedule



d. Click "Next".



e. Enter the Name

f. Enter "Change Firmware to"

g. Enter the scheduled time of upgrade.

h. Click "next"

i. Review the task and click "Ok"

Viewing Switch Information

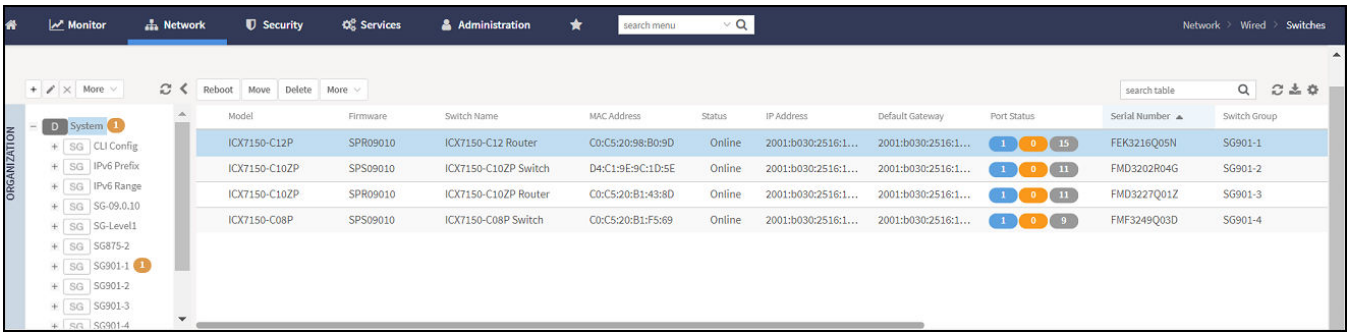
Details such as switch status, firmware version, and IP address are available for individual switches, stacks, and switch groups.

To view information on a switch, a stack, or a switch group, perform these steps.

1. From the main menu, go the **Network** > **Wired** > **Switches.**

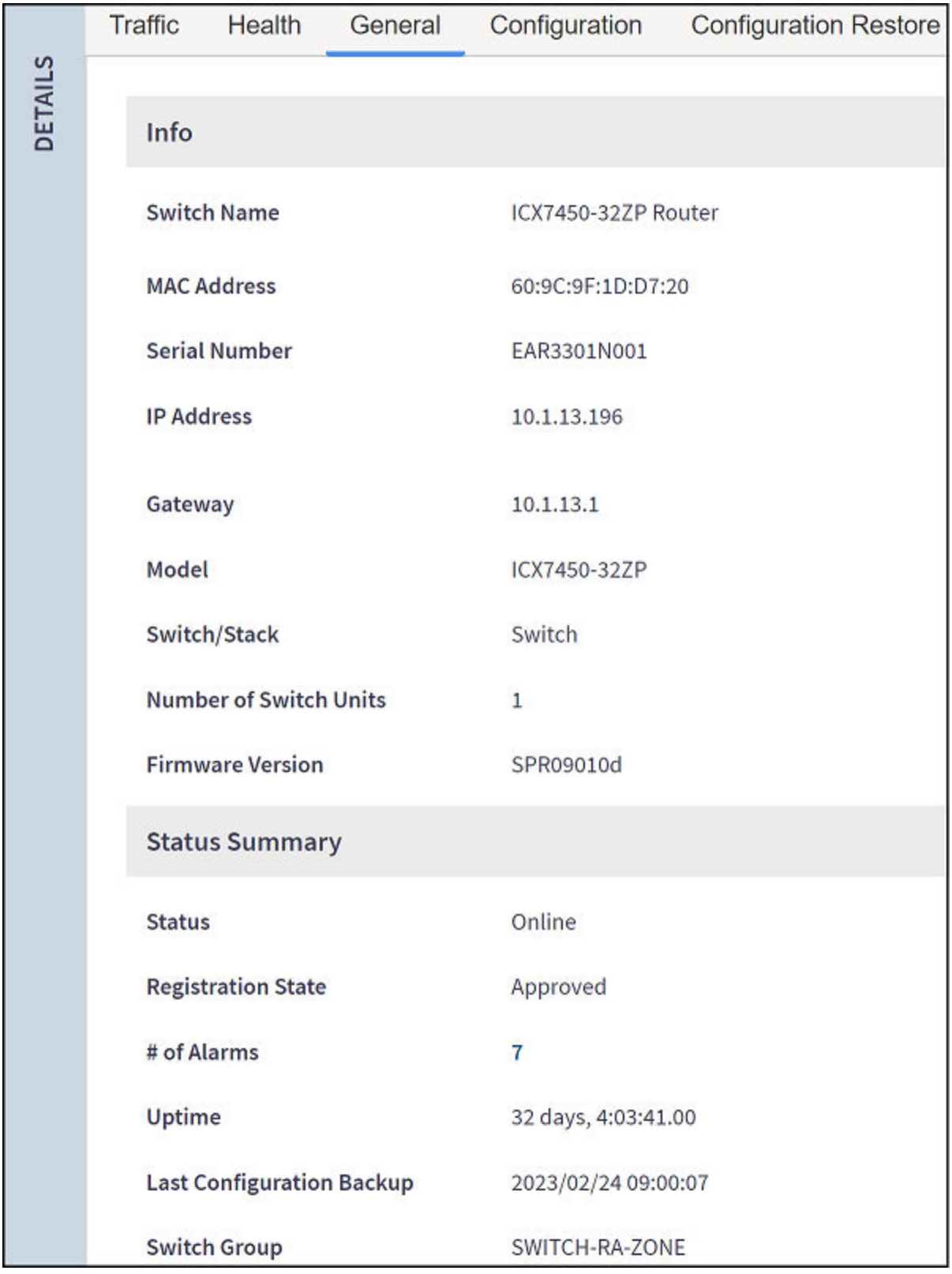
   The **Switches** page is displayed as shown in the following example.

   FIGURE 105 Switches Page



2. Select a switch to display information specific to it. Then select the **General** tab to display the information shown in the following example.

FIGURE 106 Switch Stack and General Information



The following information about the selected switch is displayed in the **General** tab:

- Switch Name: The name of the switch or group
- MAC Address: The MAC address of the switch
- Serial Number: The serial number assigned to the switch
- IP Address: The IP of the controller that monitors the switch
- Gateway: The gateway IP address through which the switch, group, or stack forwards data
- Model: The model number of the switch
- Switch/Stack: Whether the selected system is a standalone switch or a stack of switches
- Number of Switch Units: The number of switches in a group or stack
- Firmware Version: The firmware version uploaded to the selected switch
- Status: The status of the switch, such as Online, Offline, or Flagged

  NOTE
  Flagged status indicates that one or more switches have an outstanding alarms and/or Port errors are seen on the switch ports. Click **Flagged** to view the flagged switches.

- Registration State: The status of the switch, such as Approved, Offline, Online, or Flagged (when an event or alarm is triggered)
- Number of Alarms: The number of alarms generated for the selected switch or stack
- Uptime: The time that has elapsed since reboot
- Last Configuration Backup: The time the switch or stack configuration was last backed up
- Switch Group: The name of the group to which the switch belongs
- PoE Utilization (watts): The total switch PoE utilization. For example, if the total PoE allocation for the switch is 520 Watts, and 300 Watts are used, the column displays 300/520 W.

Configuring the Switch

SmartZone 5.1.1 introduces switch configuration capabilities. The following features are added:

- **Zero Touch Provisioning**: Greatly simplifies initial deployment of switches. Users can define switch configuration at a switch group level. Any new switch joining the group automatically gets provisioned.
- **Ongoing Configuration Changes**: Users can further modify the switch configuration as a part of network maintenance. This includes modifying switch group level settings, port settings, and routing interfaces.
- **Stack formation**: Users can configure individual switches to be formed into a stack directly from the controller.
- **Configuration copy**: Users can copy configuration from a working switch to one or multiple new switches seamlessly.

You can view and modify various configuration parameters of switches from the controller web interface. You can create switch configuration profiles at the group level, individual switch level and at the port level.

The **Configuration** page displays common configurations based on DNS, allows setting configuration values for a family of switches and also provides a summary of the switch configuration history.

You can update the configuration profile for new and existing switches, switches that join the controller after being offline, switches that may or may not have local feature changes via CLI/Telnet/SSH/other web interfaces.

After the switch configuration is updated successfully, you can continue to monitor the configuration deployed on the switch. If the switch configuration is not updated successfully, a message is displayed on the controller interface.

Zero Touch Provisioning using Group level Configuration

You can create and view configurations that are defined at the switch group level. Within the switch group, there is an option to define common configuration that is applicable to all the switch models in the group and another option to select configuration based on switch family, for example ICX 7150, ICX 7250, and so on. When a new switch without any existing configuration running FastIron version 8.0.90a or later version joins the controller, the group level configuration is automatically applied to the switch. This includes the global AAA settings, common configuration, and model-specific settings. If the switch joining the group already has an existing configuration, then the group level configuration is not applied during the initial join. Only the subsequent changes done at the group level are applied.

NOTE
ICX switches must run 08.0.90a or later version to take advantage of the switch configuration capabilities of the controller.

Creating Common Configuration

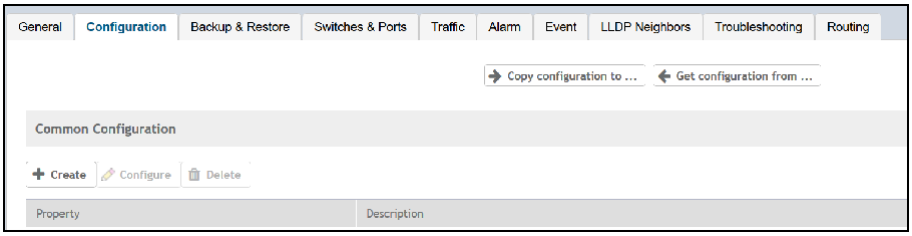
You can create, view, and edit the configuration settings for a group of switches.

1. Go to **Network** > **Wired** > **Switches.**

   The **Switches** page is displayed.

2. Select the switch and click the **Configuration** tab.

FIGURE 107 Switch Configuration Tab



3. Under **Common Configuration**, click **Create**.

   The **Common Configuration** page is displayed.

   NOTE
   In the following example, the Switch Group is the Default Group.

   a) Click the **DNS** tab.

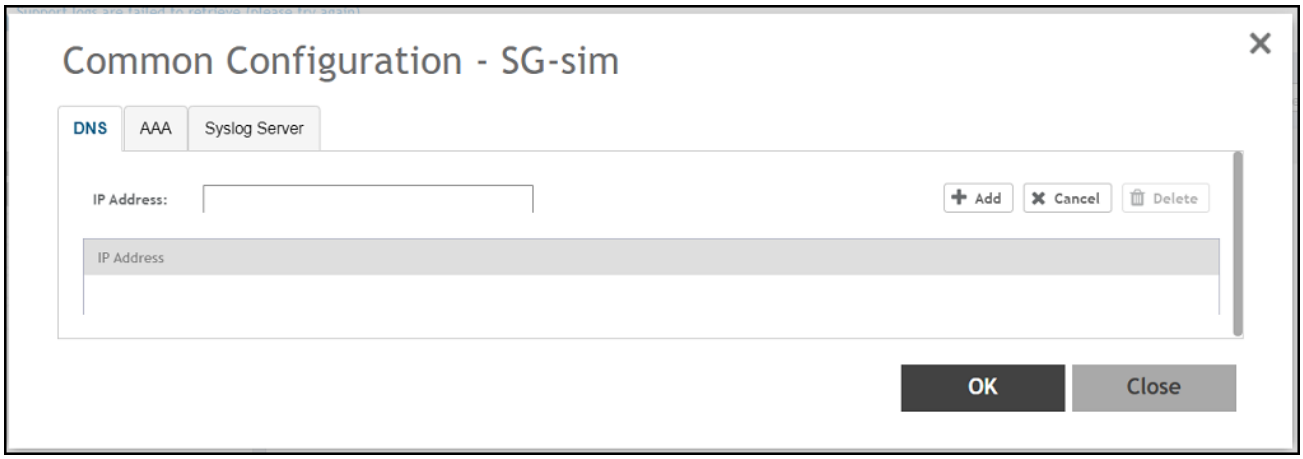
      The **DNS** tab is displayed.

   b) Enter the IP address and click **Add**.

   c) Click **OK**.

      The IP address is added to the **Common Configuration** page under **Property** and any new (factory default) switch joining this group will have the DNS configuration applied. If you want to edit the configuration, select it and click **Configure** to edit the settings.

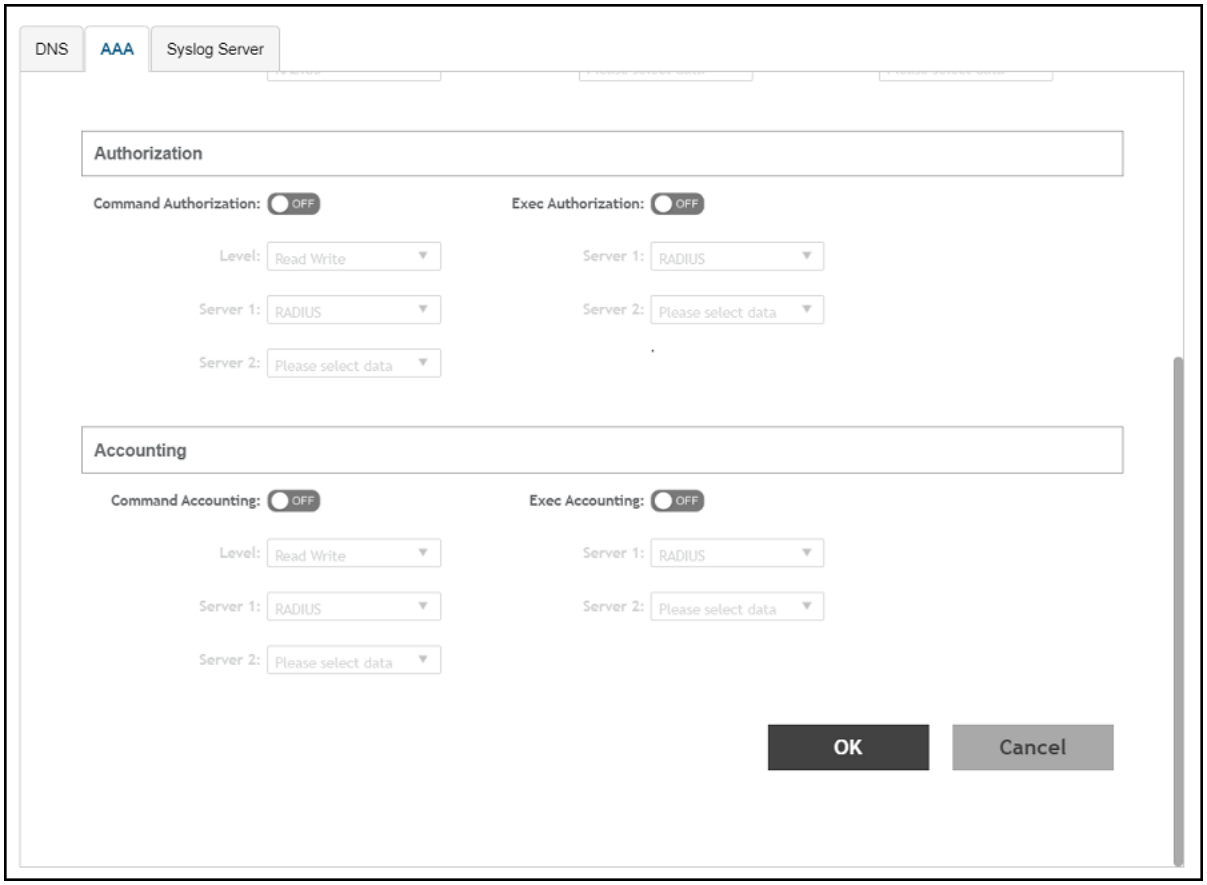
      FIGURE 108 DNS Settings



   d) Click **AAA** tab.

      The **AAA** page is displayed.

FIGURE 109 AAA Settings



e) Configure the AAA settings for the switches.

A Switch AAA server can be a RADIUS server, a TACACS+ server, or a local server with user name password. Switch AAA settings include enabling or disabling of SSH or Telnet Authentication, Authorization and Accounting, including selecting the order of preference for the AAA servers.

f) Click **OK**.

g) Click the **Syslog Server** tab.

FIGURE 110 Syslog Server Settings



NOTE
This feature is supported on the switch firmware version 08.0.95.

h) In the **IP Address** field, enter the IP address of the external syslog server. Click **Cancel** to erase the entry in the field.

i) Enter the port number in the **Ports** field.

NOTE
The default port is 514, but the user can change it as per the requirements.

j) Click **Add** to add the entries.

NOTE
The maximum of four IP addresses can be added.

k) Click **Delete** to delete the syslog server.

l) Click **OK**.

Creating Switch Model-Based Configurations

You can create and edit ACL, Layer 2, and Layer 3 configuration settings for a family of switches. You can also create or update the ACL to configure QoS profiles that prioritize VOIP and VIDEO VLAN traffic.

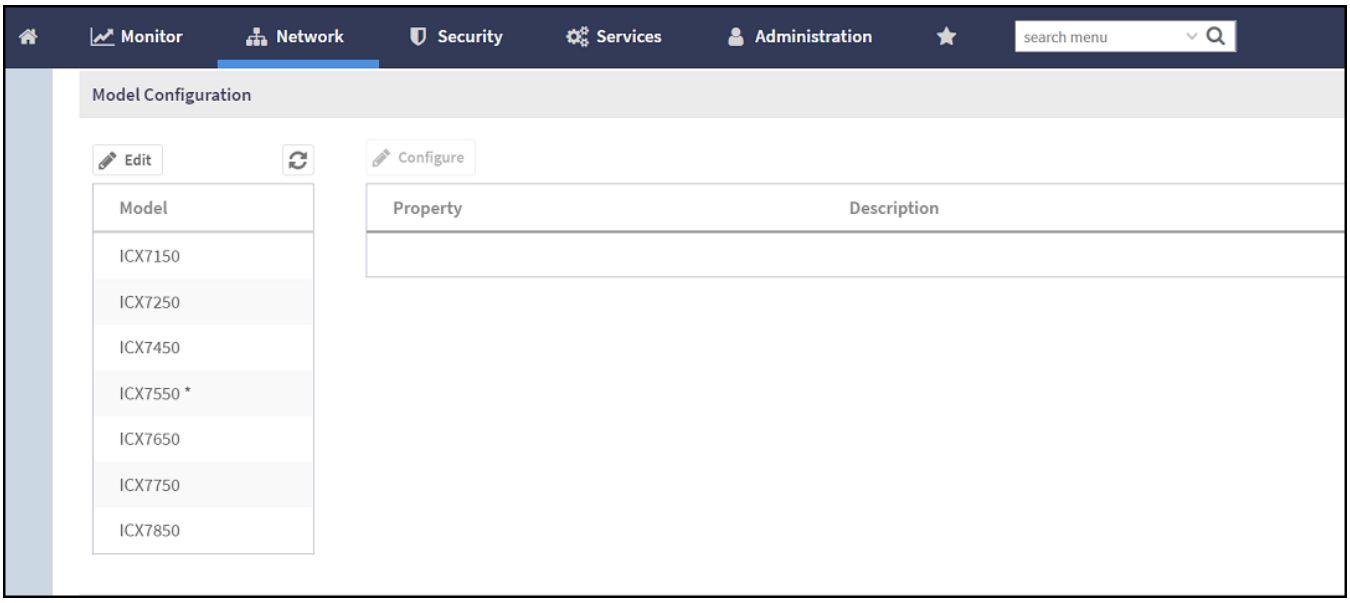
NOTE
Configuring the QoS Profiles requires ICX Firmware version 08.0.95.

1. Go to **Network** > **Wired** > **Switches.**

   The **Switches** page is displayed.

2. Select the switch group and click the **Configuration** tab.

FIGURE 111 Switch Configuration Tab



3. In **Model Configuration**, select the switch model from the list and click **Configure**.

   The **Feature Configuration** page displays details about the ACL, VLAN, and static route. You can create, edit, and delete these configurations as necessary.

   FIGURE 112 ACL Configuration

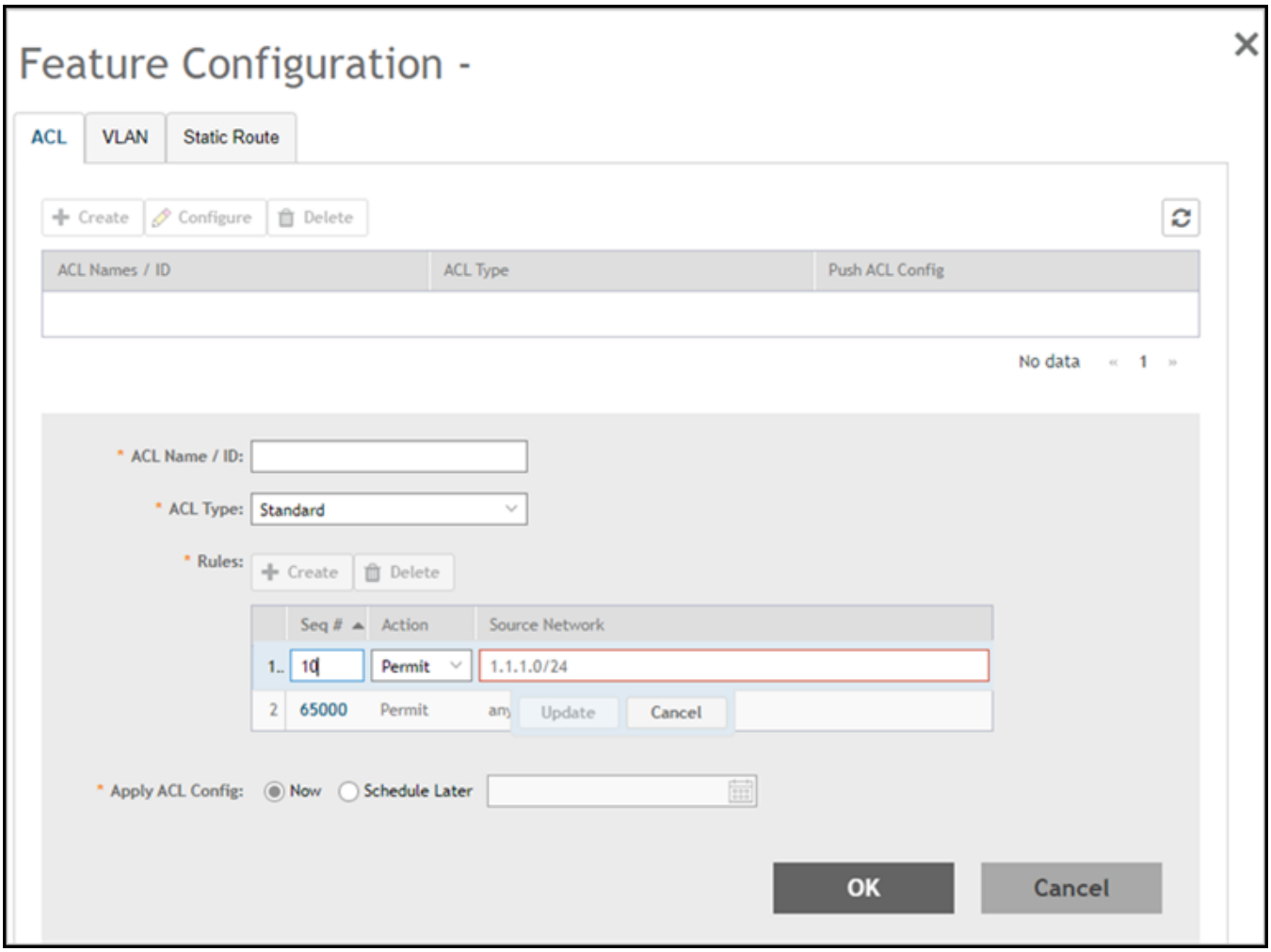
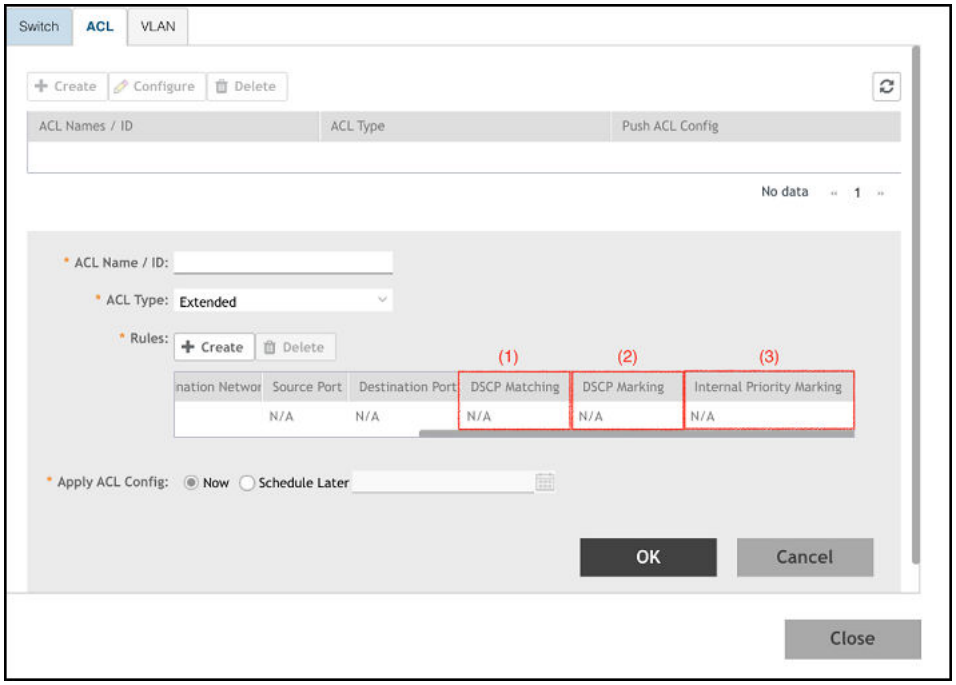


FIGURE 113 ACL Configuration with ICX Firmware version 08.0.95



Configure the following ACL details:

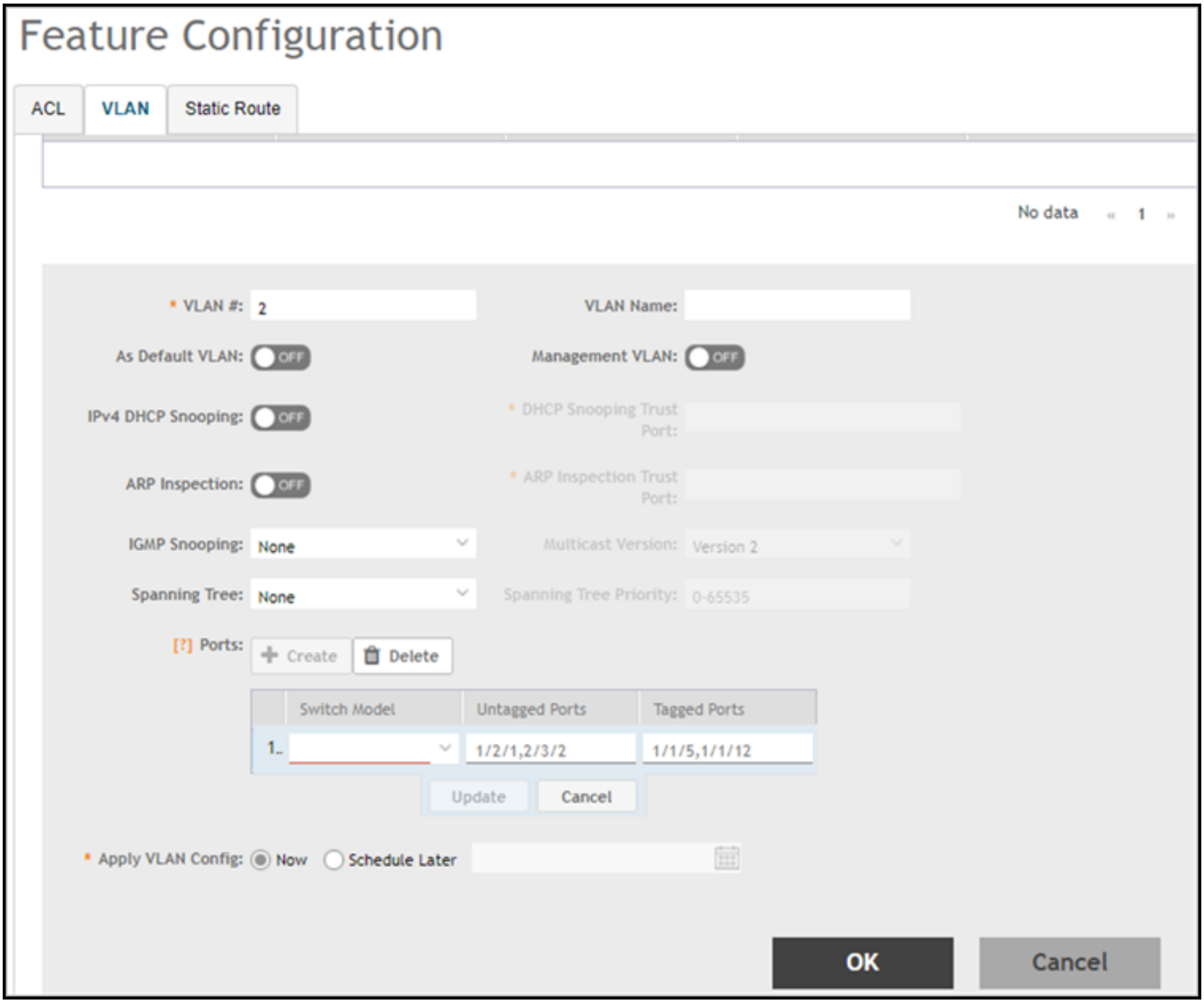
- **ACL Name/ID**: Enter the name of the access control list or provide the list identifier.
- **ACL Type**: Select Standard and Extended from the list.
- **Rules**: Click **Create** to create an ACL rule. You must provide the list sequence (**Seq#**), **Action** (Permit or Deny) and **Source Network** information to create the rule.

  NOTE
  Controller supports the "equal to" operator only.

  NOTE
  The Controller release 5.2.1 adds three new fields adds three fields (**DSCP Matching**, **DSCP Marking** and **Internal Priority Marking**) to configure QoS. After creating or updating the three fields, apply the ACL on a port or a VE to prioritize/de-prioritize traffic.

- From **Apply ACL Config**, you can either select Now or Schedule Later. If you choose to schedule the configuration deployment later, provide the time and date.
- Click **OK** to add the newly created ACL configuration to the **ACL** page. You can edit the configuration by selecting **Configure**.

FIGURE 114 VLAN Configuration

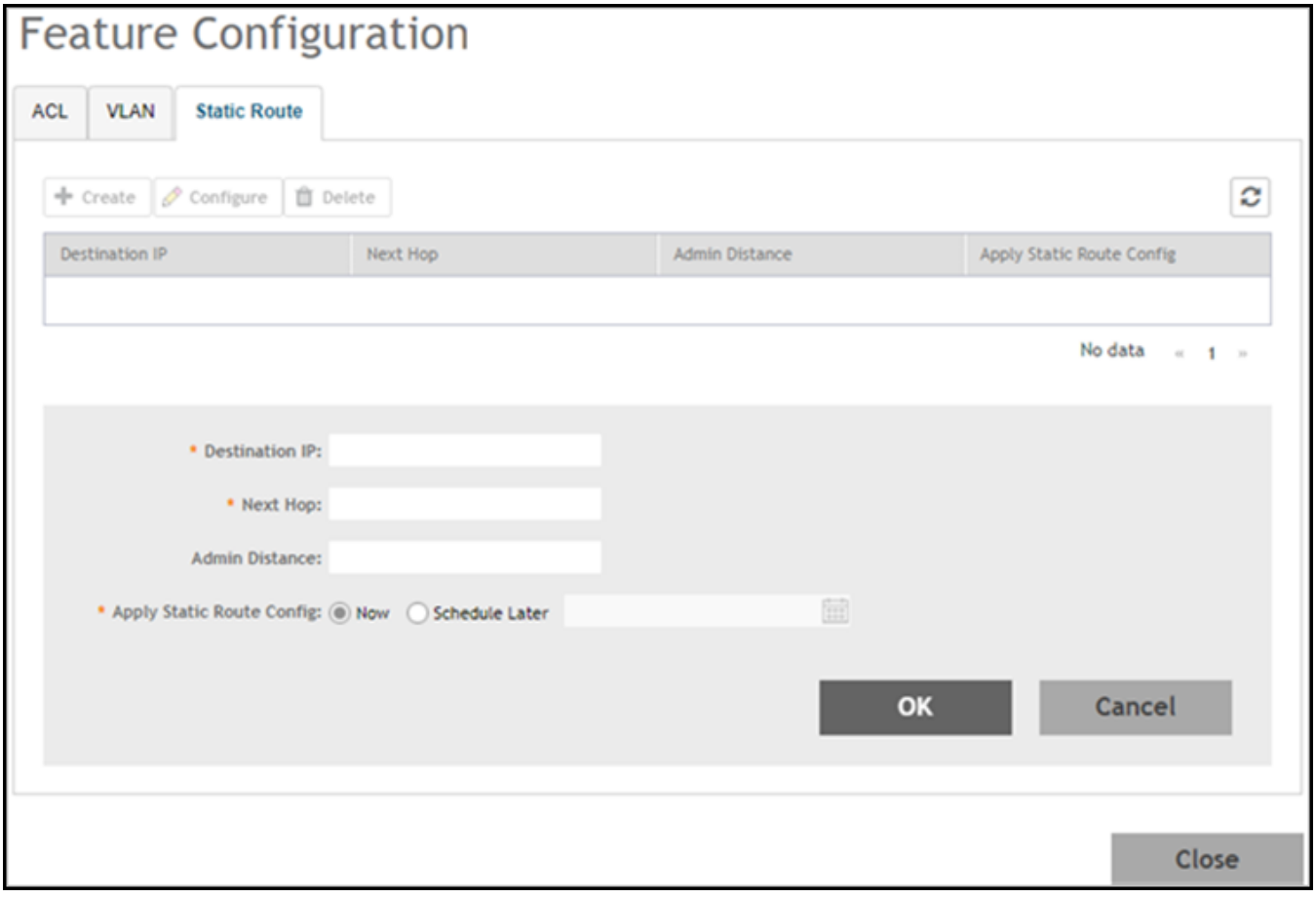


Configure the following VLAN details:

- **VLAN #**: Enter the number of the VLAN.
- **VLAN Name**: Enter the name of the Layer 2 VLAN.
- **As Default VLAN**: If you enable the **As Default VLAN** the **VLAN Name** is changed to **DEFAULT-VLAN** and the Management settings correspond to the previous VLAN settings.
- **Management VLAN**: By enabling this, you can configure Management VLAN for the switches or switch groups. To configure Managemnt VLAN for switches or switch groups refer the topic Creating Switch Level Configuration on page 272.
- **IPv4 DHCP Snooping**: Enable or disable IPv4 DHCP Snooping. Enabling this option allows the controller to send the ACL-per-port-per-VLAN message to the switch to reboot it. If you enable IPv4 DHCP Snooping, you must provide the trusted port for this option in the **DHCP Snooping Trust Port** field.

- **APR Inspection**: enable or disable ARP Inspection. Enabling this option allows the controller to send the ACL-per-port-per-VLAN message to the switch to reboot it. If you enable IPv4 DHCP Snooping, you must provide the trusted port for this option in the **ARP Inspection Trust Port** field.
- **IGMP Snooping**: Select **None**, **Active**, or **Passive** from the list. The Internet Group Management Protocol (IGMP) allows the switch to track the communication between hosts and routers based on which the switch maintains a map of which links need which IP multicast streams. If you select **Active** or **Passive**, you are required to select the **Multicast Version** as well.
- **Spanning Tree**: Select **None**, **STP (802.1d)**, or **RSTP (802.1w)** from the list. Both Spanning Tree Protocol (STP) and Rapid Spanning Tree Protocol (RSTP) prevent creation of bridge loops when you have redundant paths in your network, and the broadcast radiation that results from them. If you select **STP 802.1d** or **RSTP 802.1w**, you are required to select the **Spanning Tree Priority** as well.
- **Ports**: Click **Create** to assign the ports to the switch model. For desired switch models, enter values for **Untagged Ports**, and **Tagged Ports** and click **Update**. Different set of ports can be entered for each switch model.
- **Apply VLAN Config**: Select Now or Schedule Later. If you choose to schedule the configuration deployment for later, provide the time and date.
- Click **OK** to add the newly created VLAN configuration to the **VLAN** page. You can edit the configuration by selecting **Configure**.

FIGURE 115 Static Route Configuration



Configure the following static route details:

- **Destination IP**: Enter the destination IP address.

- **Next Hop**: Enter the next-hop IP address. Multicast and broadcast IP addresses are not allowed.
- **Admin Distance**: Enter a value from 1 through 255.
- **Apply Static Route Config**: Select Now or Schedule Later. If you choose to schedule the configuration deployment for later, provide the time and date.
- Click **OK** to add the newly created static route configuration to the **Static Route** page. You can edit the configuration by selecting **Configure**.

4. Click **Close**.

   The IP address is added to the **Model Configuration** page under **Property**. If you want to edit the configuration, select it and click **Edit** to edit the settings.

   NOTE
   Any changes made to the group level configuration including common configuration and switch model-based configuration will be applied to all the switches belonging to the group.

   Configuration defined at group level can be chosen to be applied instantaneously by selecting the **Now** option or schedule for a later time using **Schedule later** option. The scheduling option is only applicable if you are trying to make changes to existing switches in the group. For any new switches that are joining the group, this configuration gets applied instantaneously.

Copying Switch Group Configuration

You can copy the configuration settings from a working switch to one or multiple new switches.

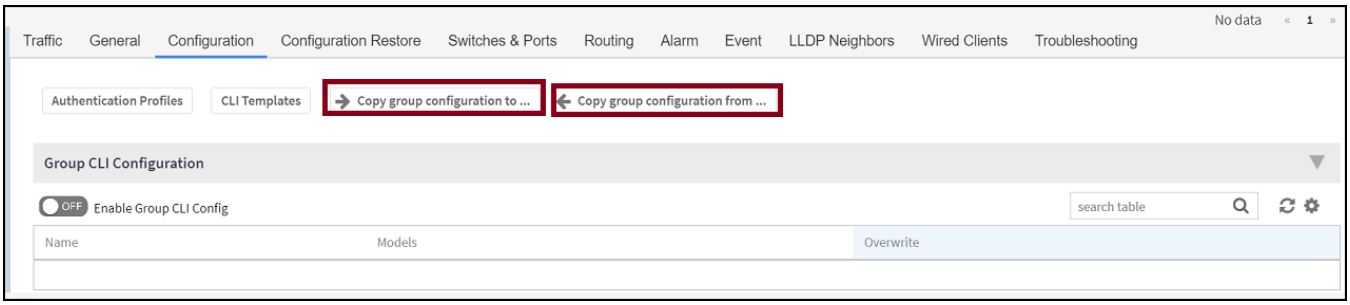
NOTE
It is recommended to exercise caution when using the copy configuration option as it replaces the entire configuration of the destination switch.

1. From the main menu, go to **Network** > **Wired** > **Switches.**

   The **Switches** page appears.

2. Select the switch group and then the **Configuration** tab.

FIGURE 116 Switch Group Configuration Tab



3. Click **Copy Configuration To** and select the switch or group to which you want to copy the configuration profile, and click **OK**.
4. Click **Copy Configuration From** and select the switch or group from which you want to get the configuration profile, and click **OK**.

Accessing AAA Settings for Switch Configuration

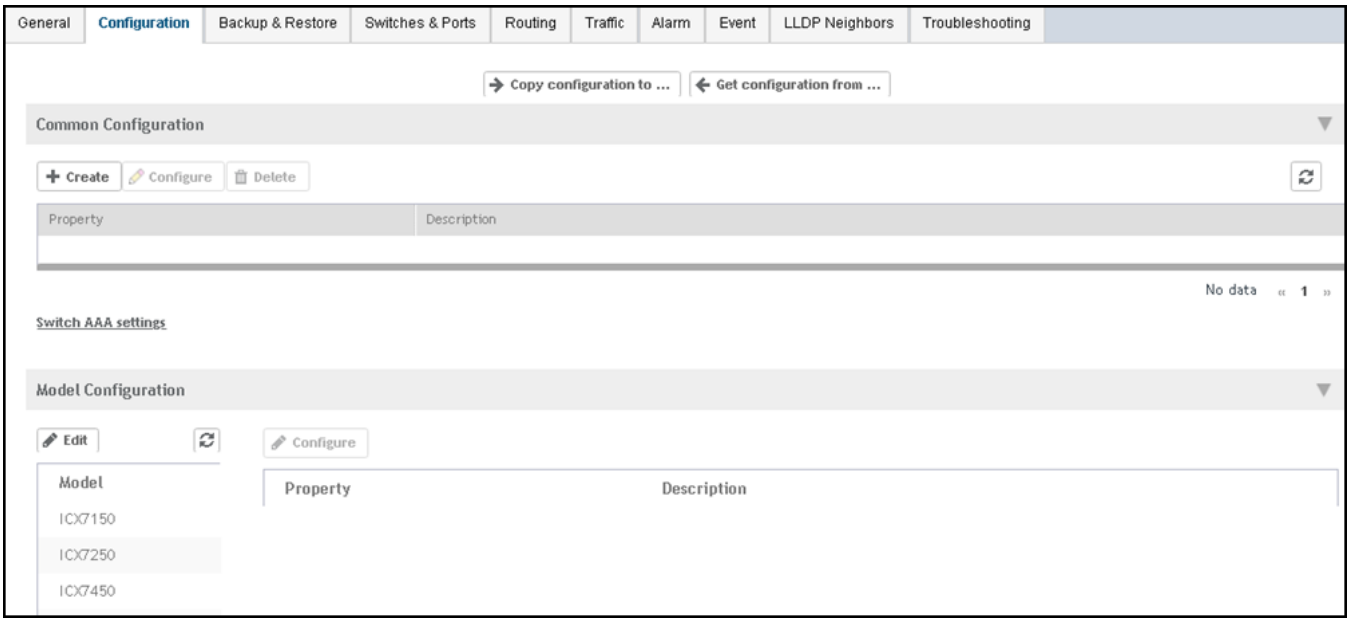
You can create, view, and edit the configuration settings for a group of switches.

1. From the main menu, go to **Network** > **Wired** > **Switches**.

   The **Switches** page is displayed.

2. Select the switch and click the **Configuration** tab.

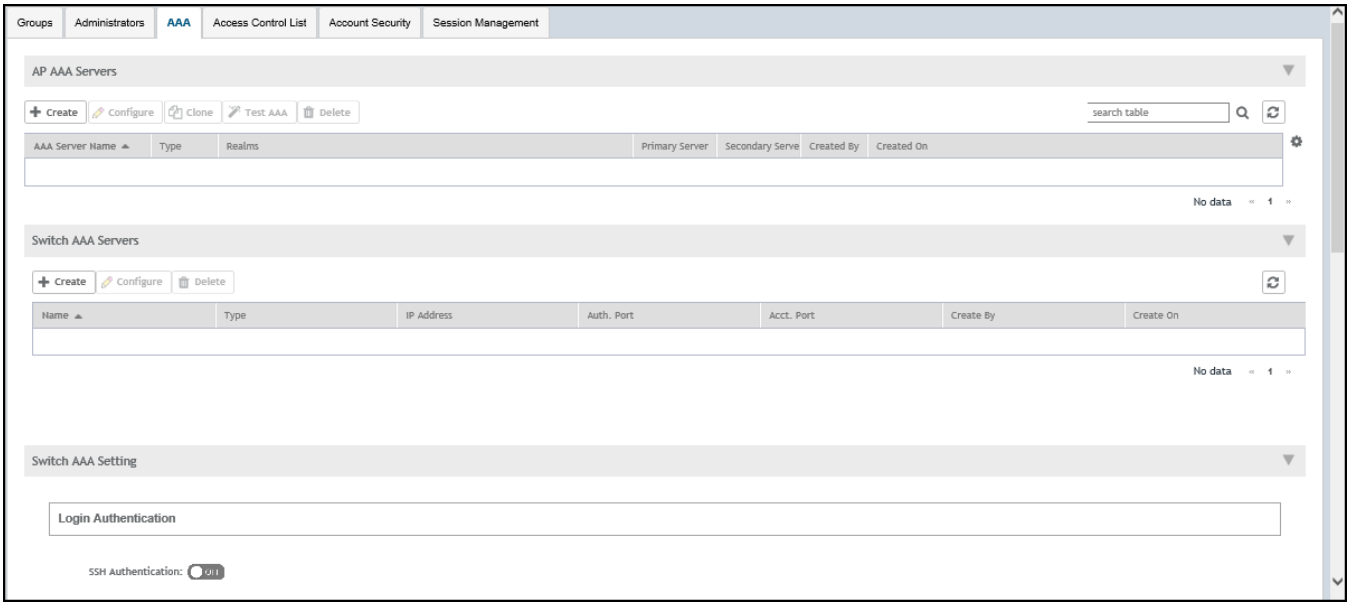
   FIGURE 117 Switch Configuration Tab



3. Click **Switch AAA settings** to access the global AAA configuration settings for switches.

   The **AAA** page appears.

   FIGURE 118 AAA Page



   You can configure the AAA settings for the switches.

   Switch AAA servers can be a RADIUS server, TACACS+, or a local username password. Switch AAA settings include enabling or disabling SSH or Telnet Authentication, Authorization, and Accounting including selecting the order of preference for the AAA servers.

Viewing the Configuration History of Switches

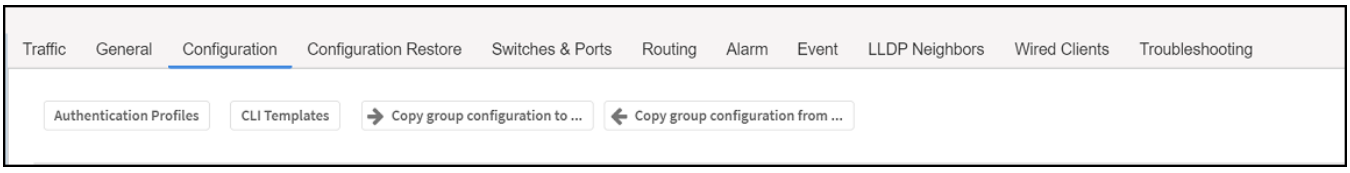
You can view the configuration details of switches from the **Configuration History** tab.

1. From the main menu, go to **Network** > **Wired** > **Switches**.

   The **Switches** page appears.

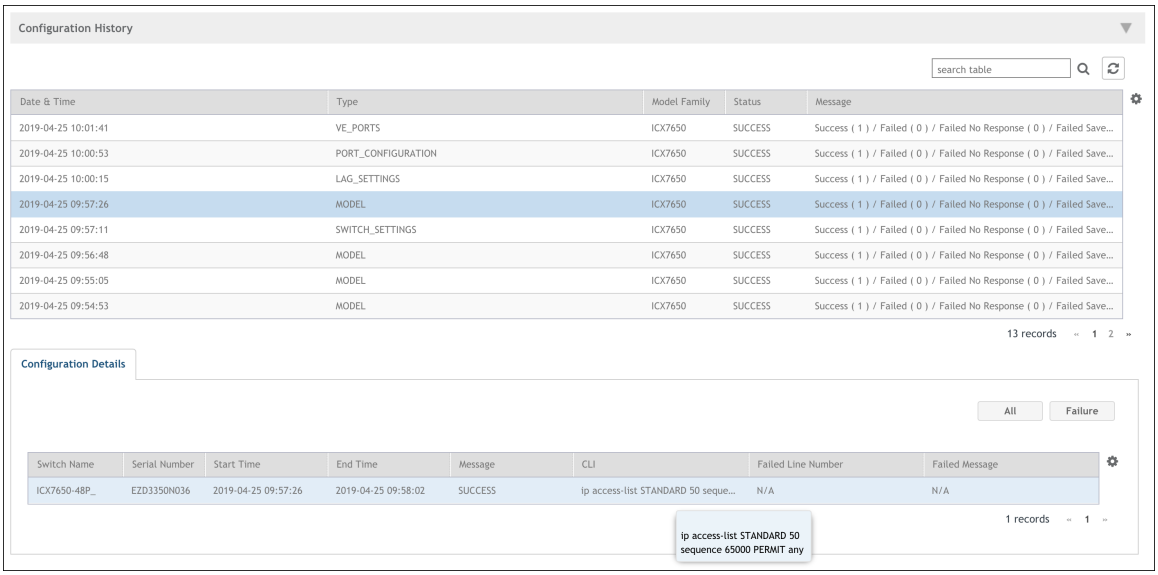
2. Select the switch and then click the **Configuration** tab.

   FIGURE 119 Switch Configuration Tab



3. You can view the following configuration information:

   FIGURE 120 Configuration history



   Information about the date and time at which the configuration profile was created, type of configuration, switch model or switch family that its created for, configuration status and a message confirming the configuration implementation on the switch/switch group is displayed.

   Clicking the switch displays more information about the **Configuration Details** as shown.

Switch Level Configuration

In addition to the group level configuration, individual switch-level configuration can be edited by selecting the switch from the Switch table.

Switch-specific settings include **Hostname**, **Jumbo Mode**, **IGMP Snooping**, and **DHCP Server**. In addition, the switch configuration defined at the group level is available for editing at the switch level.

Creating Switch Level Configuration

You can configure switch, ACL, VLAN, and static route settings for each switch.

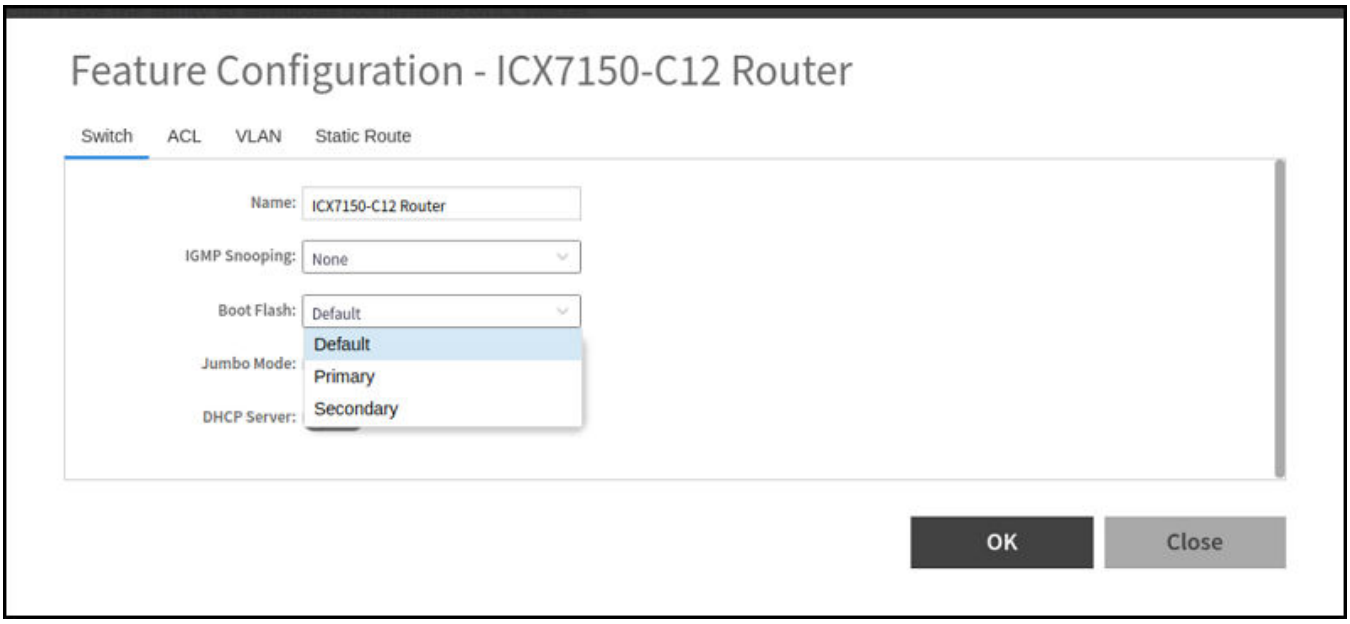
1. From the main menu, go to **Network** > **Wired** > **Switches.**

   The **Switches** page is displayed.

2. Select a switch and click the **Configuration** tab.

3. Click **Configure** and select the **Switch** tab.

FIGURE 121 Switch Configuration



4. Configure the following switch details:
   - **Name**: Enter the name of the switch.
   - **IGMP Snooping**: Select the profile from the list.
   - **Boot Flash**: Select the **Default**, **Primary** or **Secondary** option to configure boot preference.
   - **Jumbo Mode**: Enable this option to reboot the switch.
   - **DHCP Server:** Enable this option and click **Create** to configure the following DHCP server settings:

     NOTE
     You must disable the DHCP client before enabling the DHCP server.

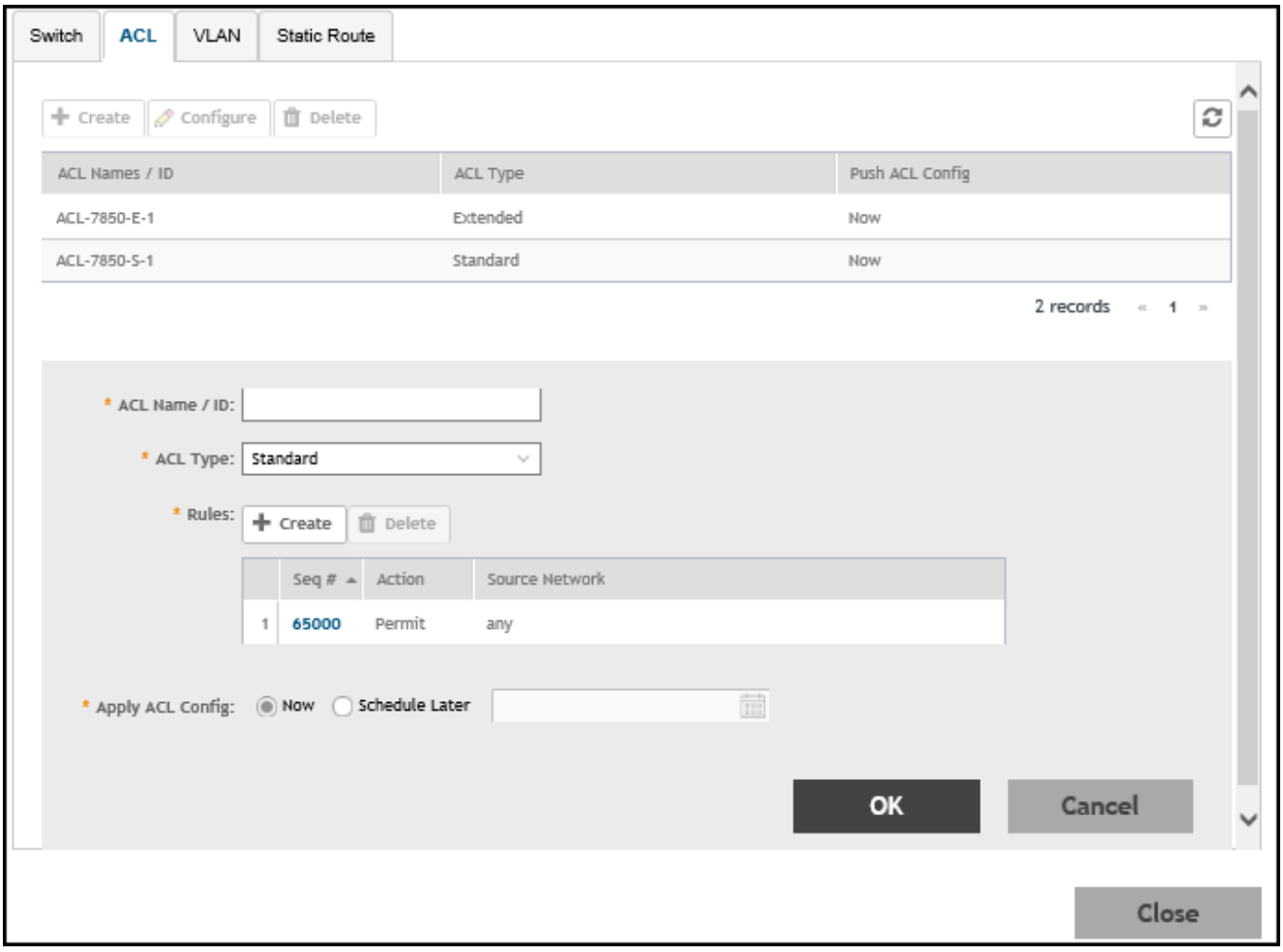
     - **Pool Name:** Enter a name.
     - **Network/Mask**: Enter the network address and network mask.
     - **Excluded Range**: Enter the network range to be excluded.
     - **Lease Time**: Enter the lease time duration.
     - **Default Router IP**: Enter the default router IP address.
     - **Options**: Click **Create** and enter the option number, , select a type, and enter a value for the option.

     Click **Update** to apply the option.

   Click **OK** to add the newly created switch configuration to the **Switch** tab page. You can edit or delete the configuration by selecting **Edit** or **Delete**, respectively.

5. Select the **ACL** tab.

FIGURE 122 ACL Configuration



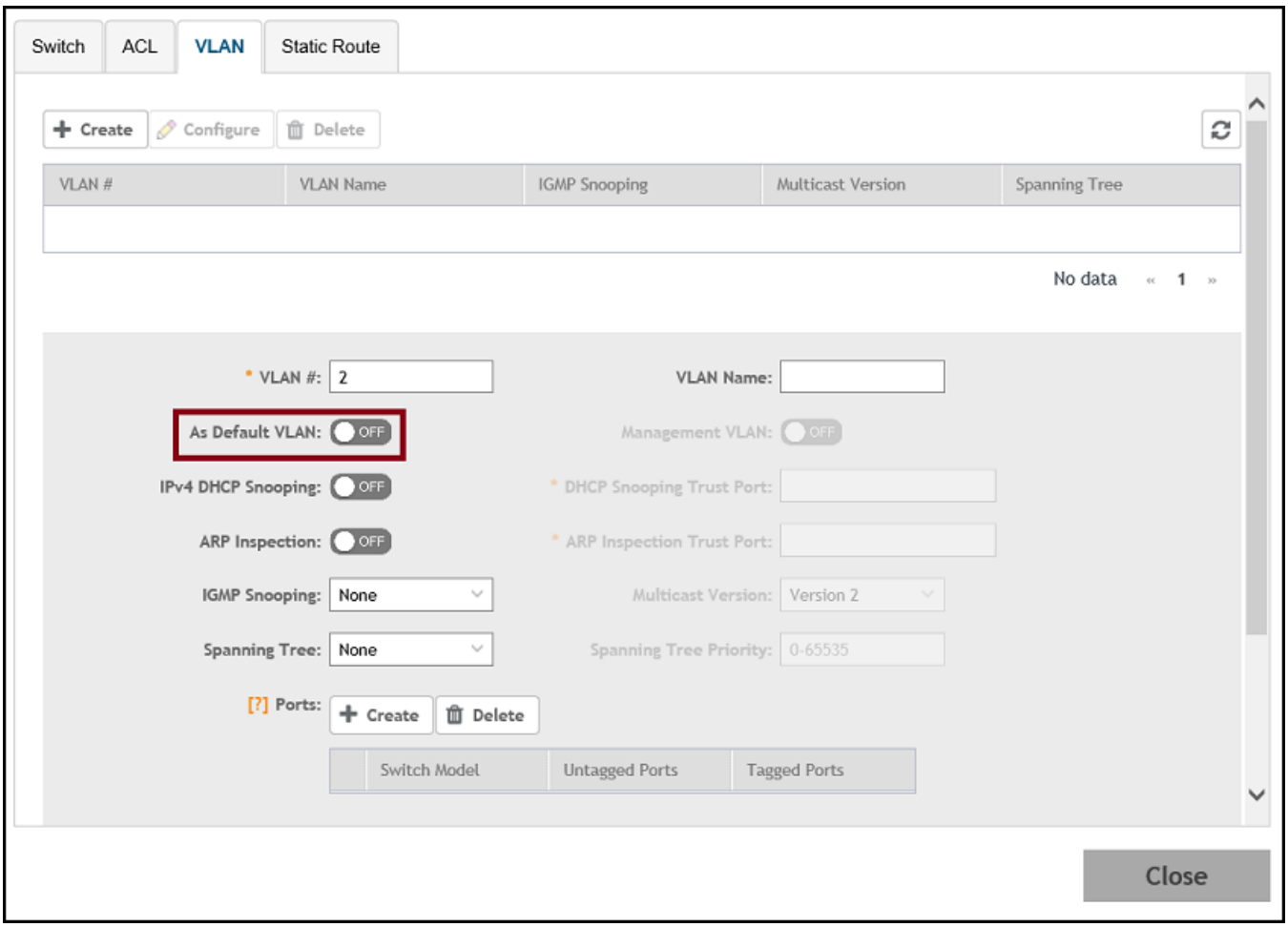
6. Click **Create** and configure the following ACL details:
   - **ACL Name/ID**: Enter the name of the access control list or provide the ACL ID.
   - **ACL Type**: Select **Standard** or **Extended** from the list.
   - **Rules**: Click **Create** to create an ACL rule. You must provide the list sequence number, action (Permit or Deny), and **Source Network** information to create the rule.
   - **Apply ACL Config**: Select **Now** or **Schedule Later**. If you choose to schedule the configuration deployment for later, provide the time and date.

   Click **OK** to add the newly created ACL configuration to the **ACL** page. You can edit or delete the configuration by selecting **Configure** or **Delete**, respectively.

7. Select the **VLAN** tab.

   You can create a new VLAN and set it as the default VLAN.

FIGURE 123 VLAN Configuration

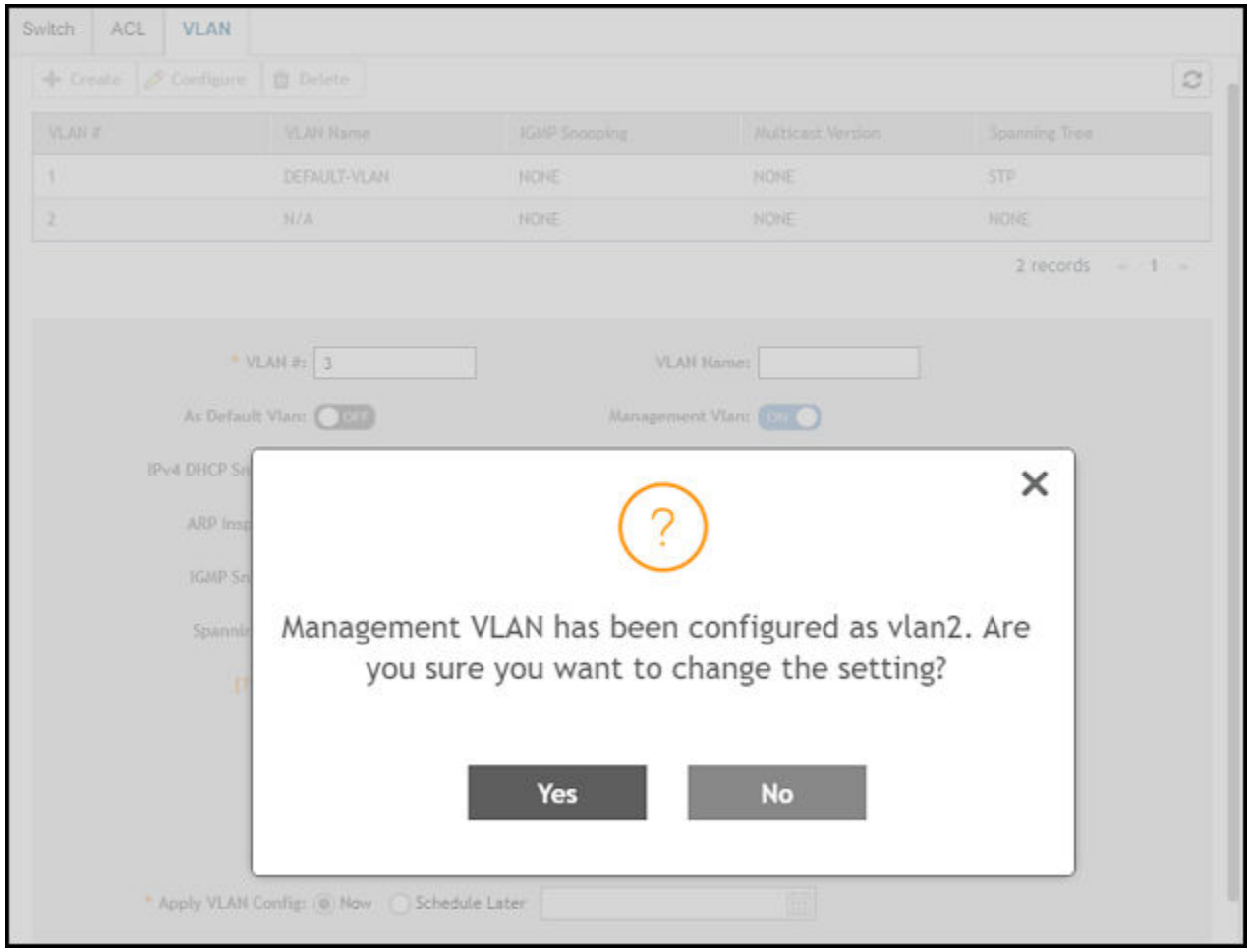


8. Click **Create** and configure the following VLAN details:
   - **VLAN #**: Enter a unique number for VLAN.
   - **VLAN Name**: Enter the name of the Layer 2 VLAN.

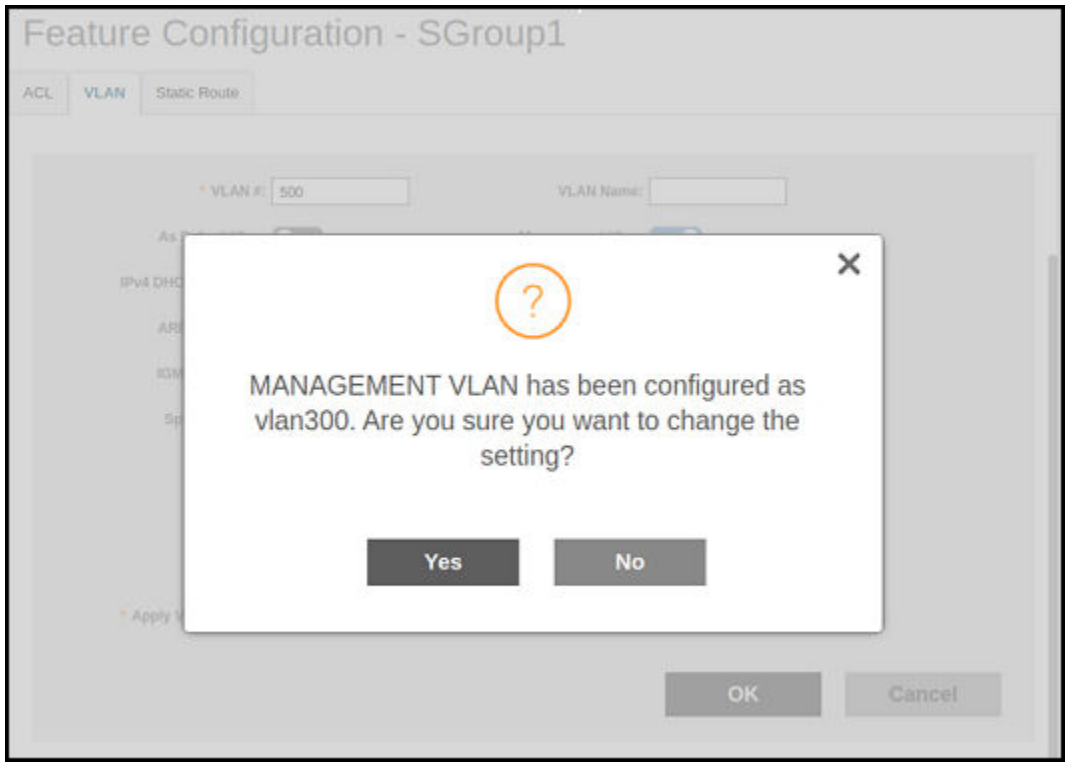
     NOTE
     If you enable the **As Default VLAN**, the **VLAN Name** is changed to **DEFAULT-VLAN** and the Management settings correspond to the previous VLAN settings.

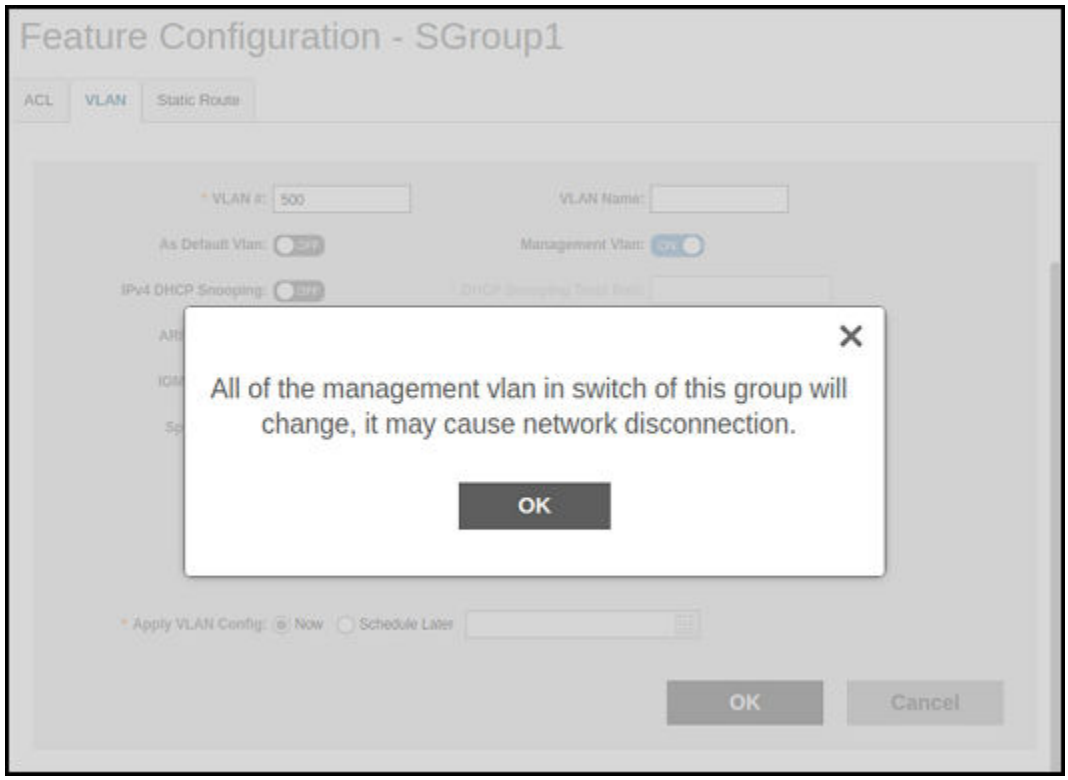
   - **Management VLAN**: You can configure the Management VLAN for the switches or switch groups in the following ways:
     - Enable **Management VLAN**, and click **OK**.

       If the VLAN is configured as the default VLAN, enable or disable **Management VLAN** on the default VLAN, and click **OK**. A dialogue box is displayed, as shown in the following.

       If **Management VLAN** is enabled on a VLAN and you try to enable it on another VLAN, the controller displays a dialogue box showing the VLAN ID that has been configured as the Management VLAN. If you click **Yes**, the controller overwrites the settings.
     - For a switch group, the controller displays a dialogue box, as shown in the following figure.





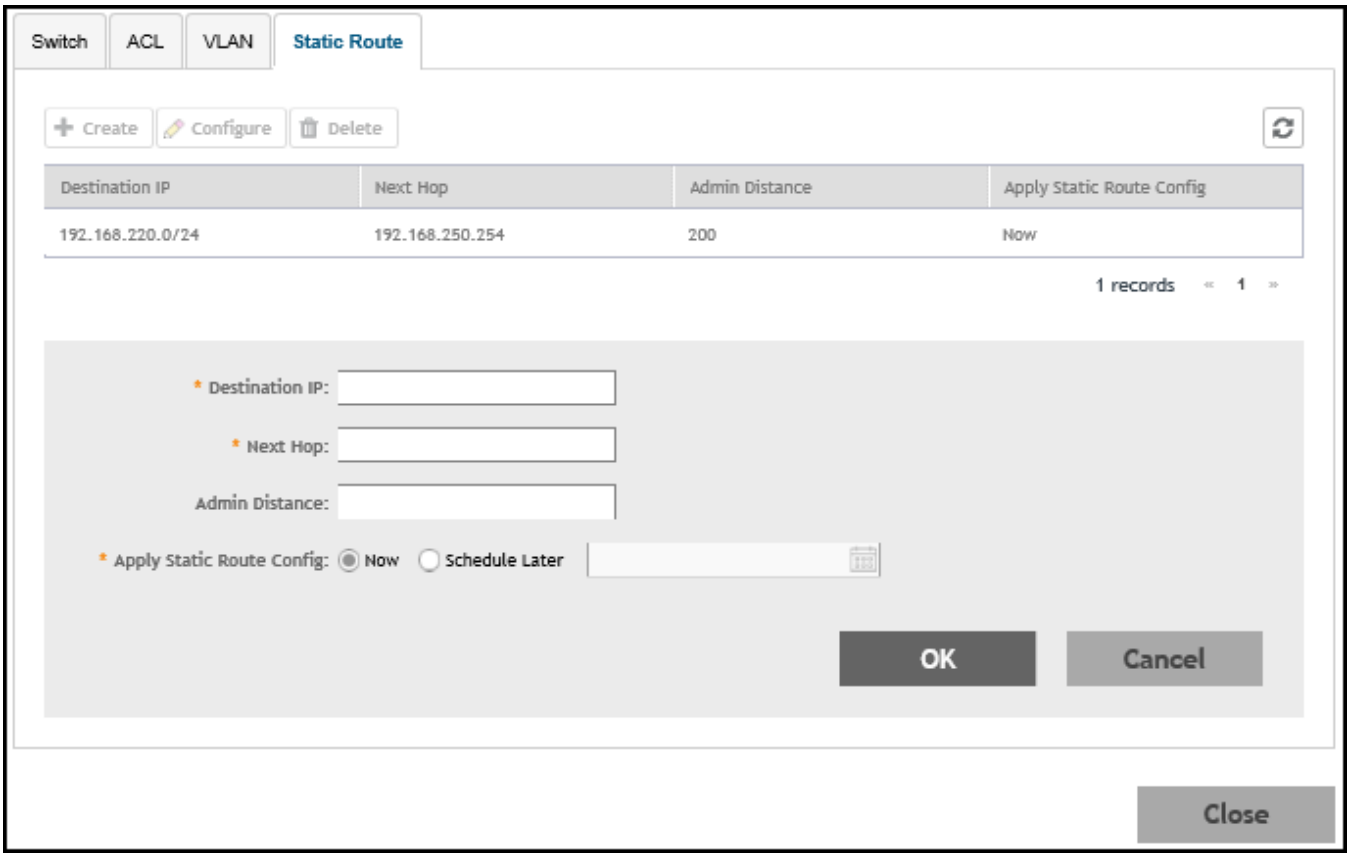
- **IPv4 DHCP Snooping**: Enable or disable IPv4 DHCP Snooping. Enabling this option allows the controller to send the ACL-per-port-per-VLAN message to the switch to reboot it. If you enable IPv4 DHCP Snooping, you must provide the trusted port for this option in the **DHCP Snooping Trust Port** field.

- **APR Inspection**: enable or disable ARP Inspection. Enabling this option allows the controller to send the ACL-per-port-per-vlan message to the switch to reboot it. If you enable IPv4 DHCP Snooping, you must provide the trusted port for this option in the **ARP Inspection Trust Port** field.
- **IGMP Snooping**: Select **None**, **Active**, or **Passive** from the list. The Internet Group Management Protocol (IGMP) allows the switch to track the communication between hosts and routers based on which the switch maintains a map of which links need which IP multicast streams. If you select **Active** or **Passive**, you are required to select the **Multicast Version** as well.
- **Spanning Tree**: Select **None**, **STP (802.1d)**, or **RSTP (802.1w)** from the list. Both Spanning Tree Protocol (STP) and Rapid Spanning Tree Protocol (RSTP) prevent creation of bridge loops when you have redundant paths in your network, and the broadcast radiation that results from them. If you select **STP** or **RSTP**, you are required to select the **Spanning Tree Priority** as well.
- **Ports**: Click **Create** to assign the ports to the switch model. Enter values for **Switch Model**, **Untagged Ports**, and **Tagged Ports** and click **Update**.
- **Apply VLAN Config**: Select **Now** or **Schedule Later**. If you choose to schedule the configuration deployment for later, provide the time and date.

Click **OK** to add the newly created VLAN configuration to the **VLAN** tab. You can edit or delete the configuration by selecting **Configure** or **Delete**, respectively.

9. Select the **Static Route** tab.

FIGURE 124 Static Route Configuration



Click **Create** and configure the following static route details:

- **Destination IP**: Enter the destination IP address.
- **Next Hop**: Enter the next hop IP address. Multicast and broadcast IP addresses are not allowed.
- **Admin Distance**: Enter a value from 1 through 255.
- **Apply Static Route Config**: Select **Now** or **Schedule Later** . If you choose to schedule the configuration deployment for later, provide the time and date.

Click **OK** to add the newly created static route configuration to the **Static Route** tab. You can edit or delete the configuration by selecting **Configure** or **Delete**, respectively

10. Click **Close**.

The configurations are updated under **Property**. If you want to edit the configuration, select it and click **Edit** to edit the settings.

NOTE
Use the switch-level option to add additional ACLs, VLANs, or static routes other than those already defined at the switch group level. Use the group-level configuration to make changes to existing settings at the group level.

Copying Configuration

If you already have a switch with the desired set of features configured, controller provides an option to load the current configuration of the switch, remove unique settings like hostname, IP addresses, and so on, and copy it to one or more target switches. This procedure is applicable only if the target switches have no existing configuration.

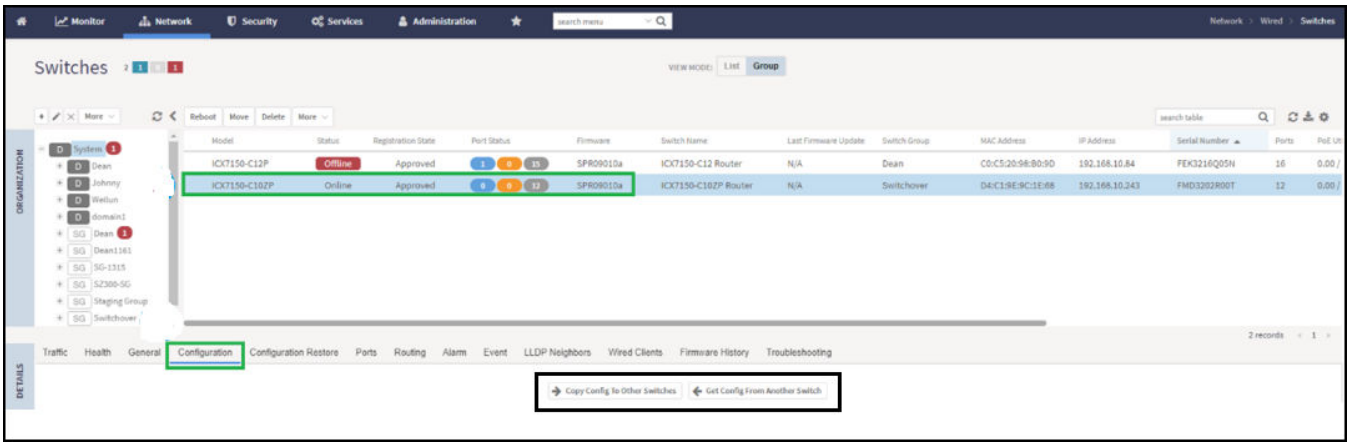
Complete the following steps to copy configuration to one or more target switches.

1. From the main menu, go to **Network** > **Wired** > **Switches.**

   The **Switches** page appears.

2. Select the switch and then the **Configuration** tab.

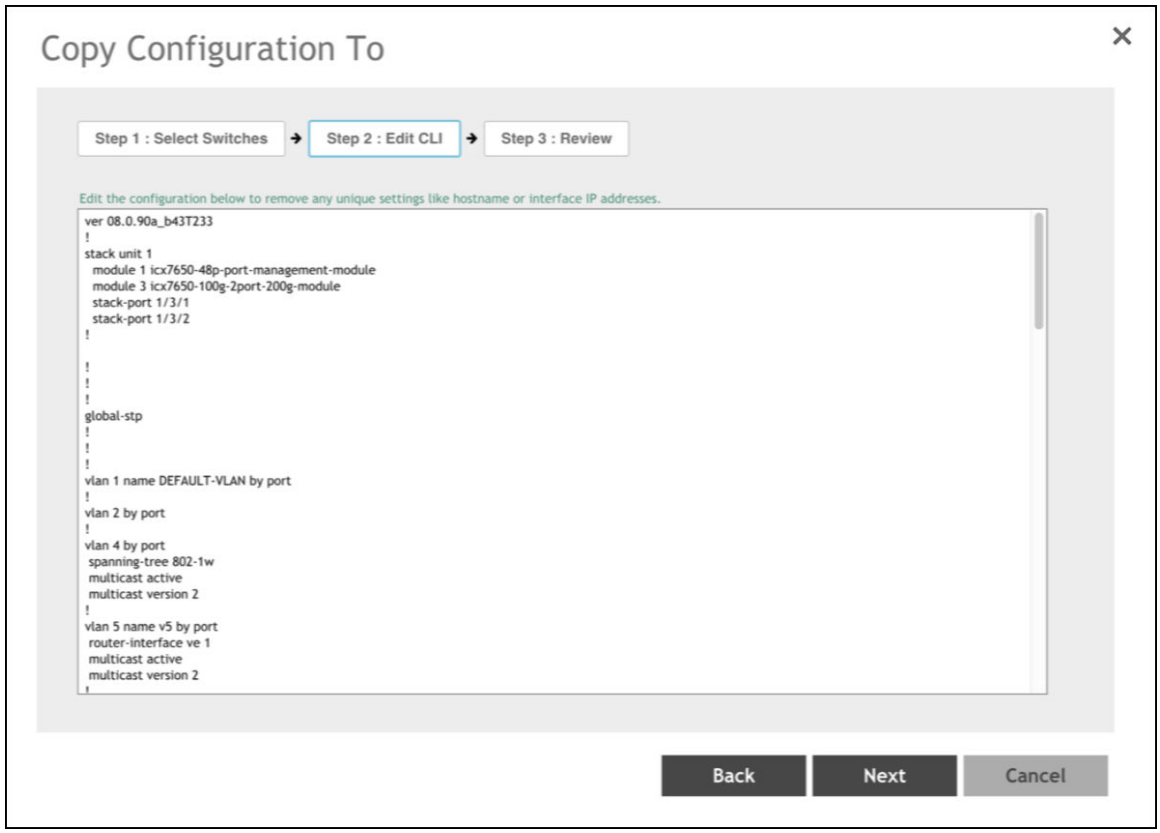
   FIGURE 125 Switch Group Configuration Tab



3. Click **Copy Configuration To**. This option lets you replace the entire configuration (startup-config) of the selected switch with that of a source switch.
4. Click **Get Configuration From** and select the switch or group from which you want to get the configuration profile, and click **OK**. This option lets you replace the entire configuration of destination switches (one or more) with the configuration of the selected switch.

5. Edit the CLI commands to remove unique settings like IP settings and hostname and click **Next**.

FIGURE 126 Copy Configuration To - Edit CLI Page



6. Review CLI config and click **OK**.

Generic CLI Configuration

SmartZone 6.0 introduces capability to provision switches using predefined CLI configuration making it easy for users to deploy any feature that ICX supports.

Group Level CLI Configuration

Users can pre-define CLI configuration for one or more switch models. When switches join this switch group, the CLI configuration gets applied to the startup-config and the switches are rebooted for the configuration to take effect.

Users can pre-define CLI configuration for one or more switch models. When switches join this switch group, the CLI configuration gets applied to the startup-config and the switches are rebooted for the configuration to take effect.

- After selecting the Group CLI configuration option, the existing GUI options at the switch group level are disabled, including common settings, model family based configurations, the **Copy configuration** to, and **Get configuration** from functions.
- If the Group CLI configuration is selected, only those switches joining the switch group after that point will inherit the configuration.
- Switch-level UI configuration options and routing must be read-only. However, ports and LAG settings can still be configured from the ports table.

- You cannot return to GUI mode to define the Switch group configuration unless the switch group is deleted and re-created.

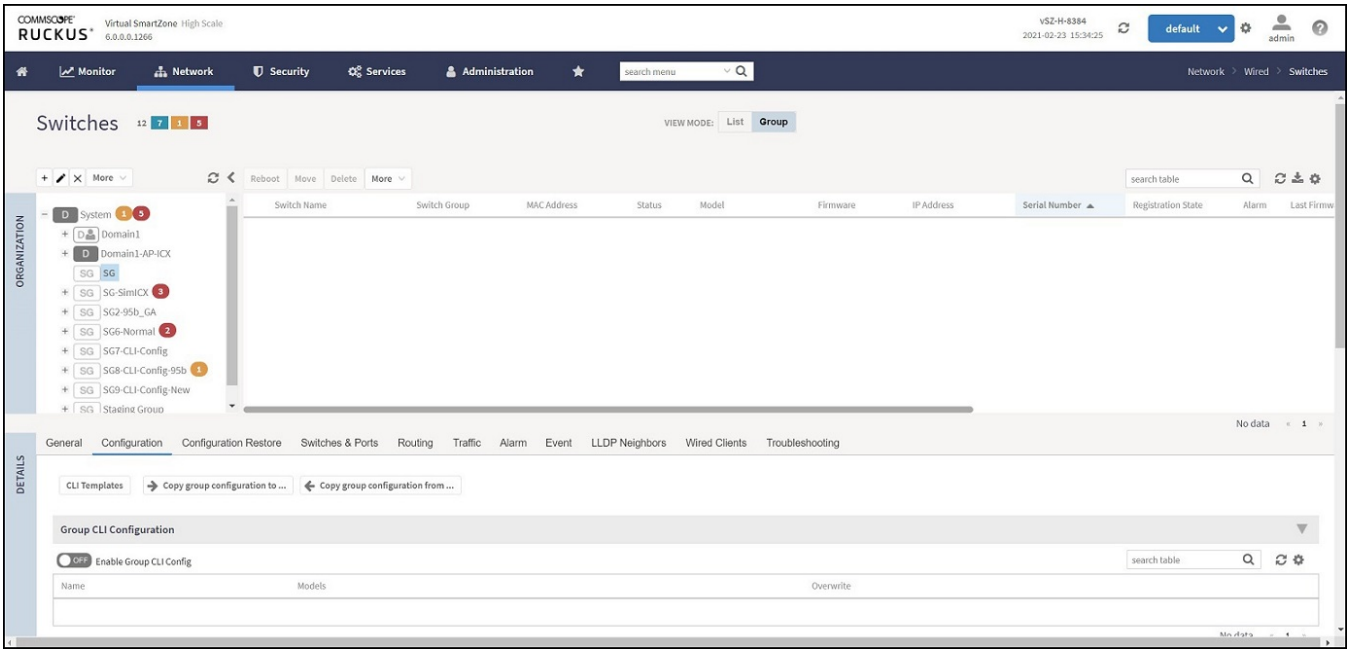
Enabling the Group CLI Configuration

An administrator can create a new template or modify an existing Group CLI configuration for the switch group before enabling the template.

1. From the main menu, go to **Network** > **Wired** > **Switches.**

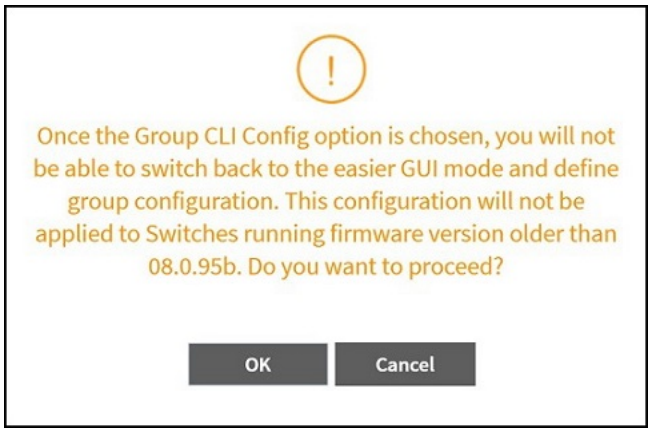
   The **Switches** page is displayed.
2. From the **Switches** group, select **Switches**.
3. Click the **Configuration** tab.

FIGURE 127 Enabling Group CLI Config setup



4. A dialog box is displayed confirming the Group CLI Configuration Setup. Click **OK**.

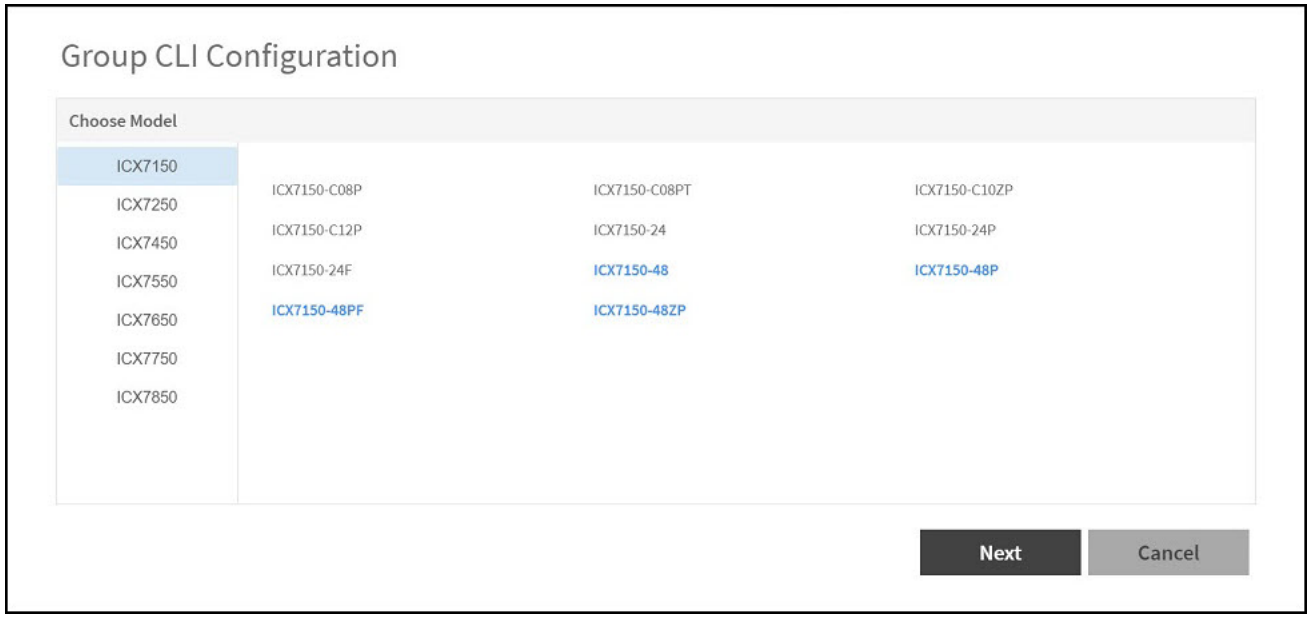
FIGURE 128 Confirming Group CLI Configuration Setup



5. Under **Choose Model**, select one or more ICX models to create a new Group CLI Configuration template and click **Next**. You can also select an existing ICX model and click **Next** to modify the Group CLI configuration.

NOTE
Any ICX models that have already been selected in the Group CLI configuration will be unavailable and you cannot select them.

FIGURE 129 Choosing ICX Models



The **Group CLI Configuration** page is displayed.

6. Enter the name of the Group CLI Configuration in the **Name** field. Insert the command lines in the space provided. Users can choose the CLI commands under the 'Examples' pane to build configuration. Alternatively, CLI commands can be typed directly or copied from a notepad and pasted into the 'CLI Configuration' box.

   NOTE
   It is recommended that users get familiarized with FastIorn commands and their ordering to avoid any issues with applying the configuration.

FIGURE 130 Entering the Name in the new Group CLI Configuration

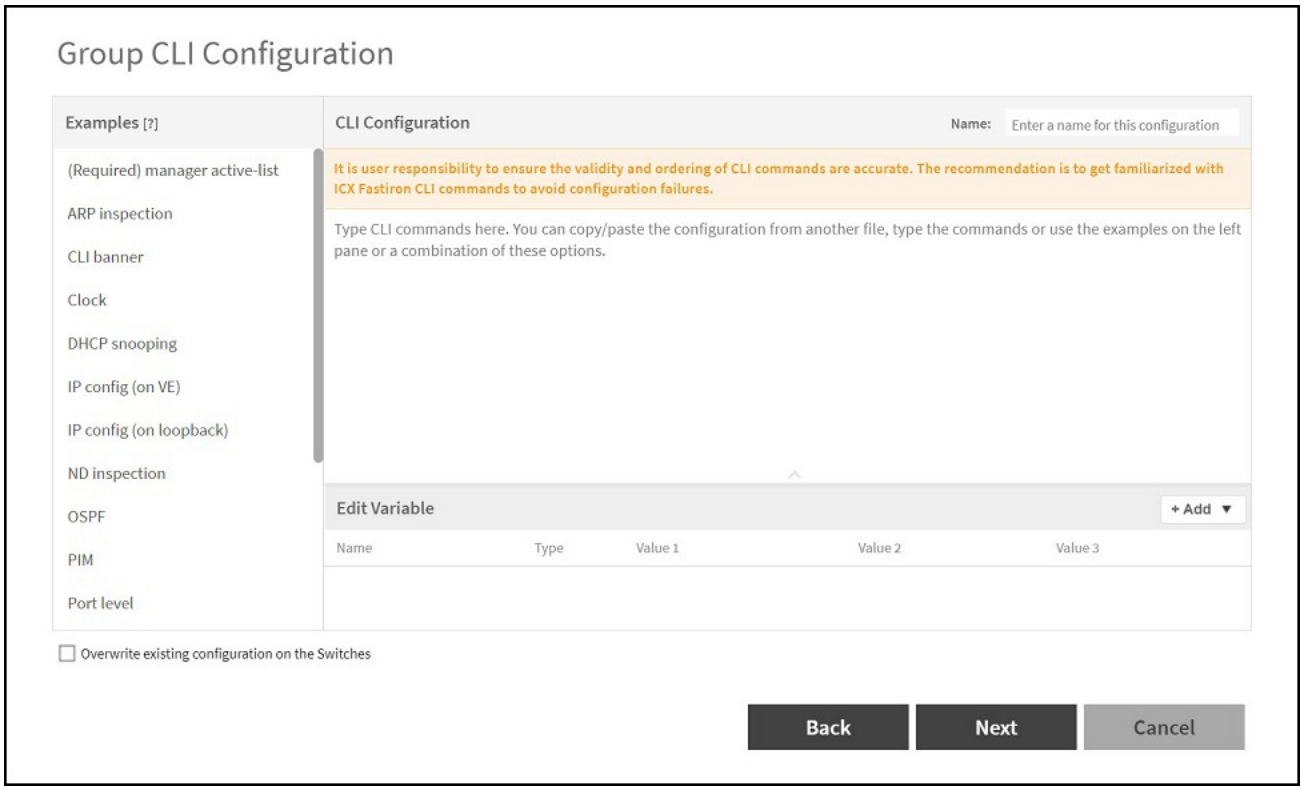


FIGURE 131 Inserting Command Lines in the new Group CLI Configuration

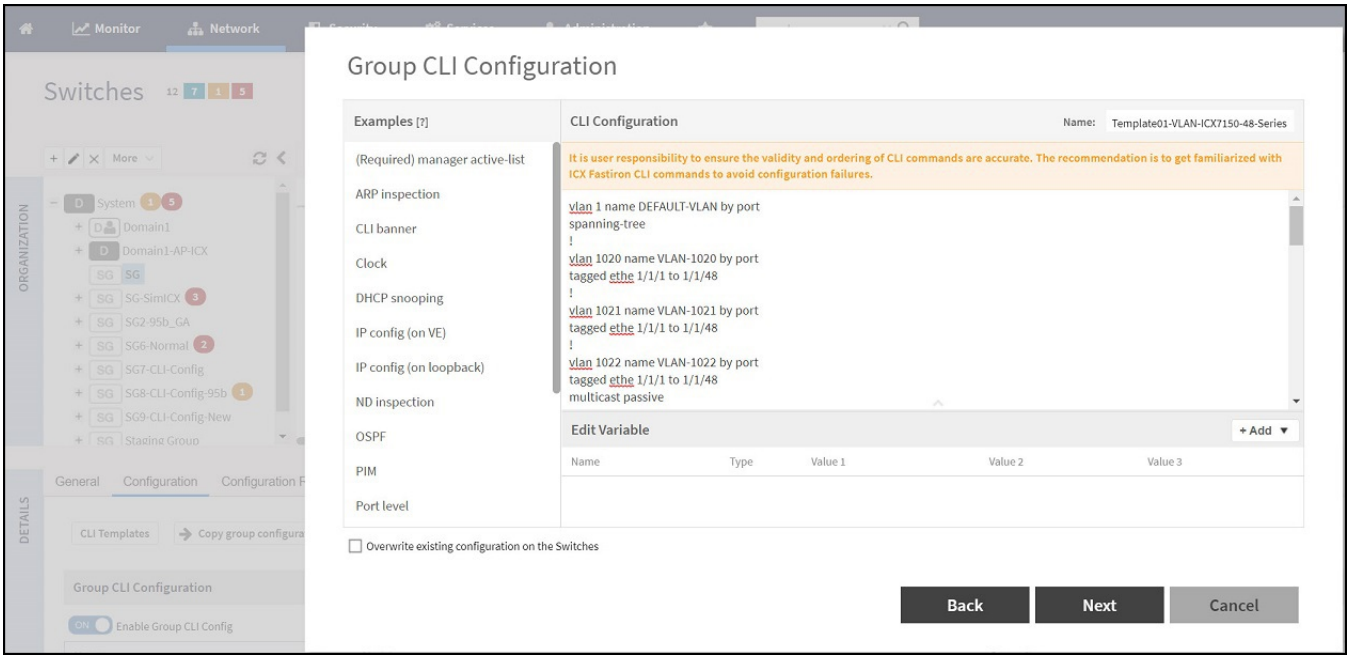


FIGURE 132 Support for space in variable string

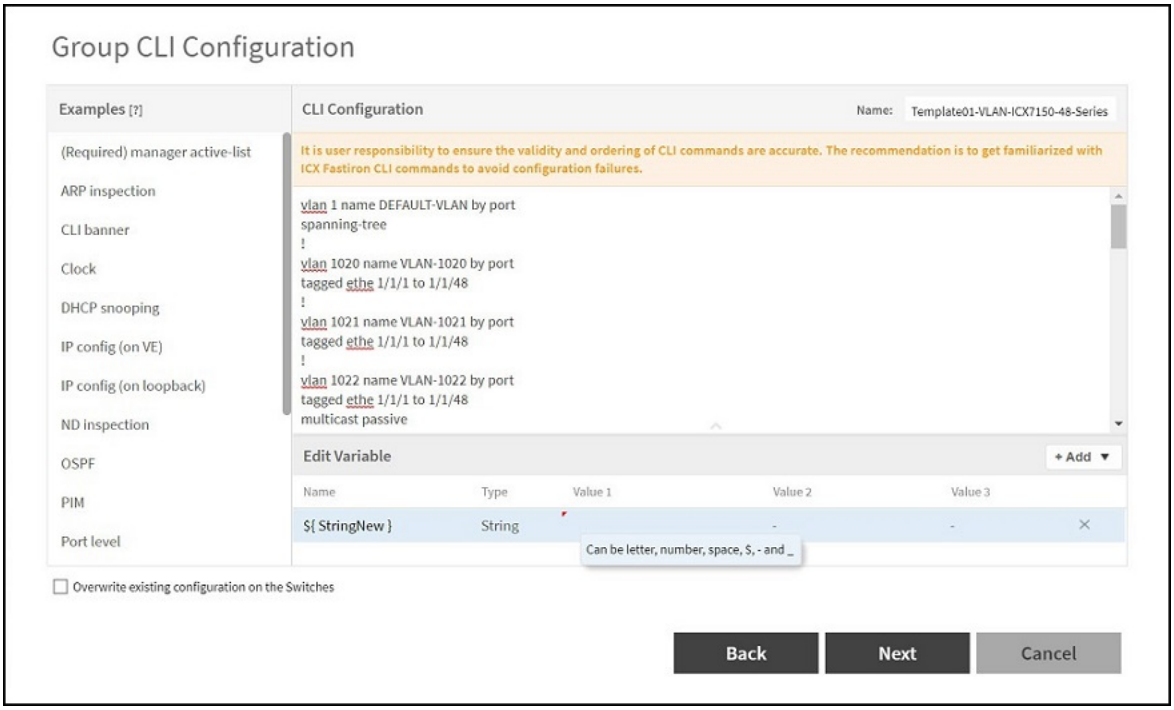


FIGURE 133 Support for dollar sign in varibale string

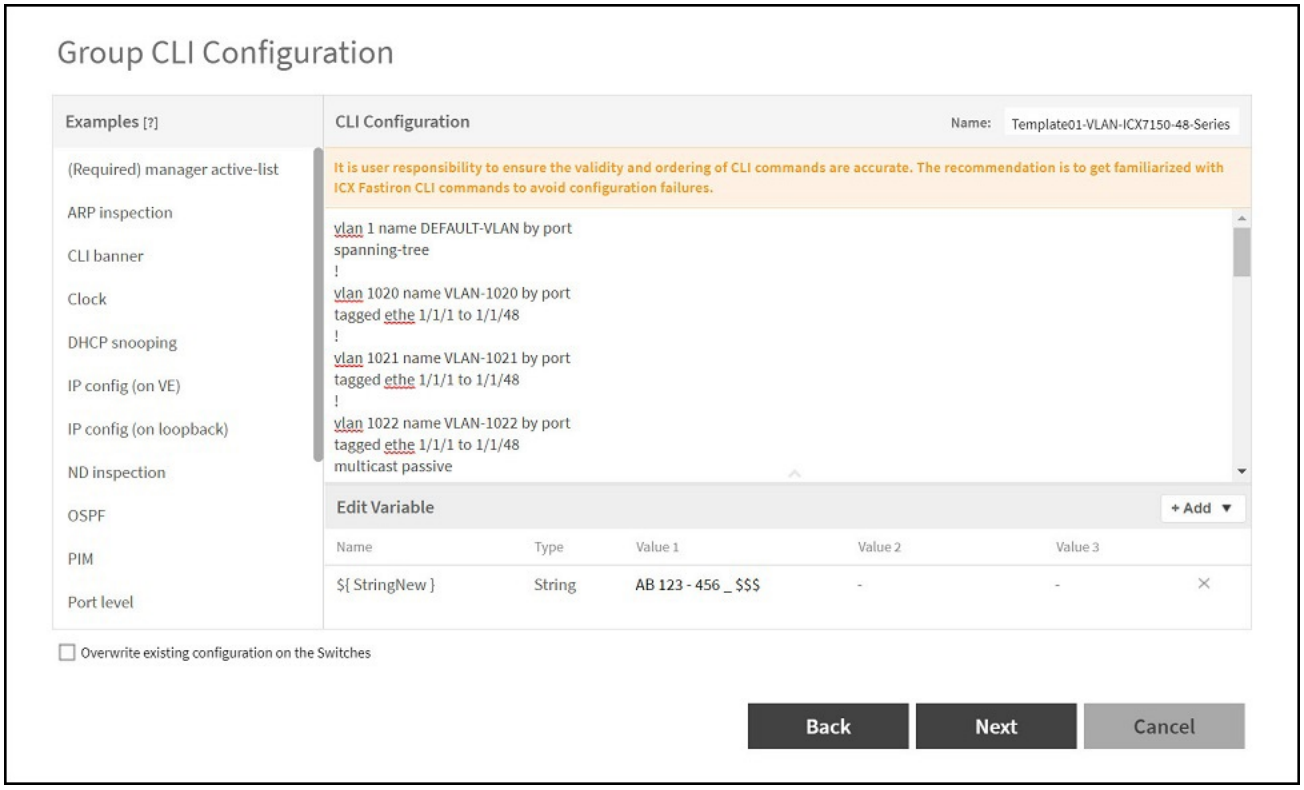


FIGURE 134 Example Template

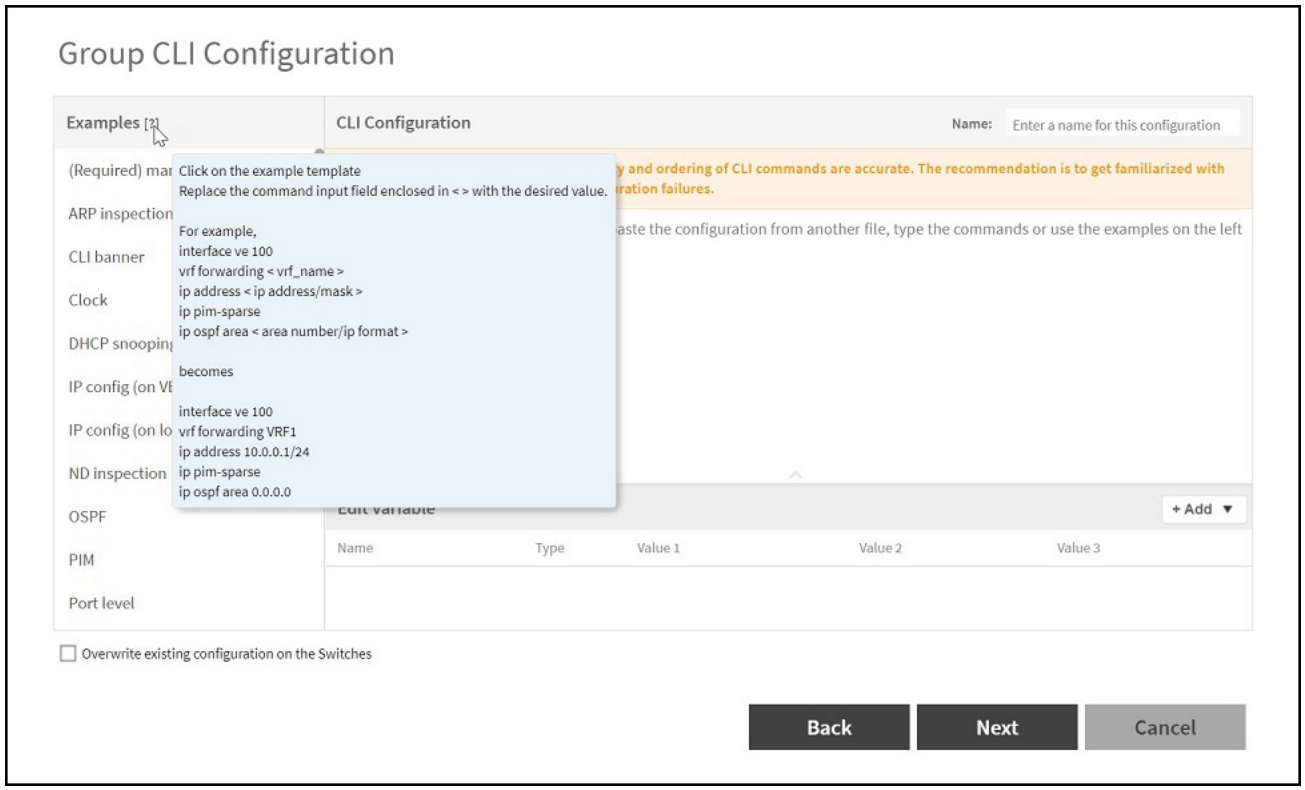


FIGURE 135 Support for IP address in variable

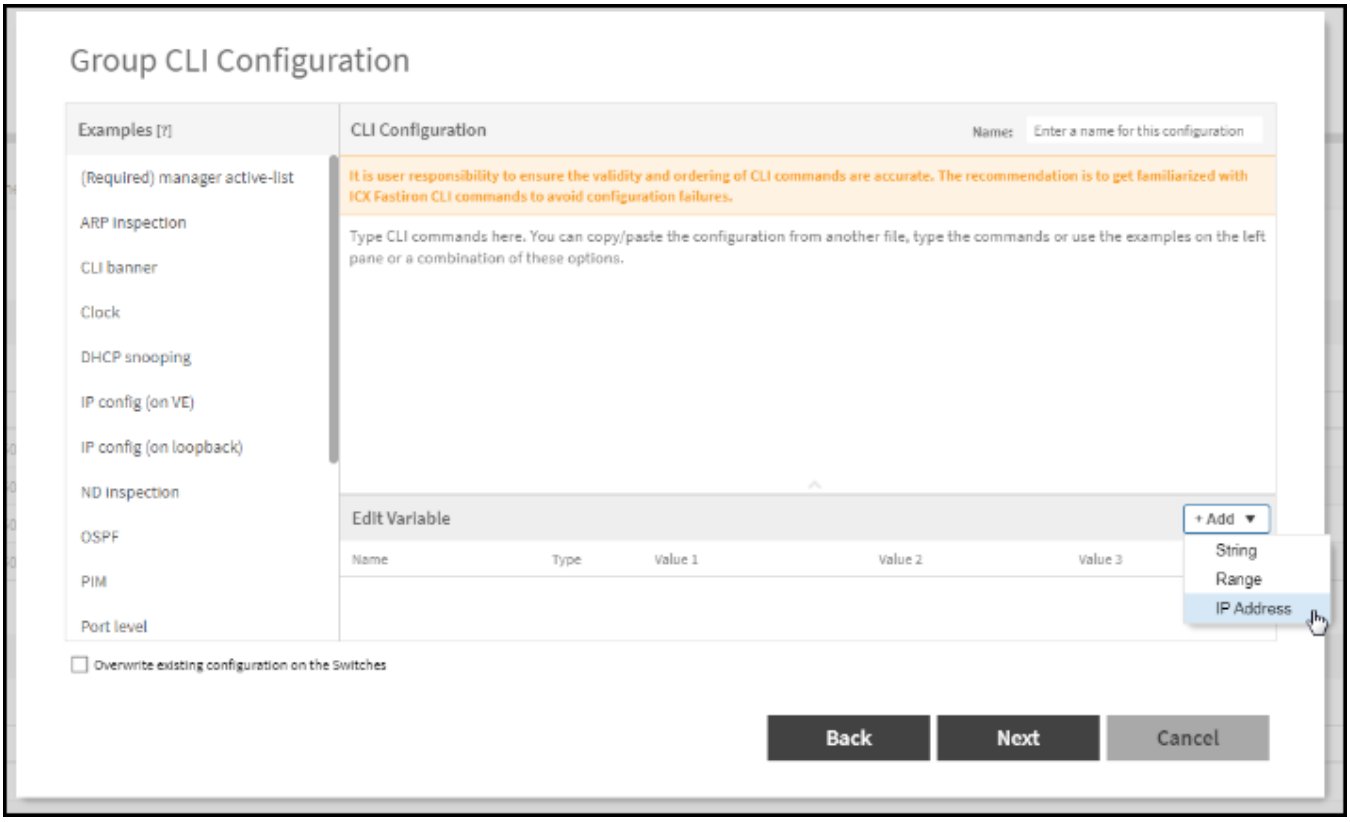


FIGURE 136 Details of fields in IP address in varibale

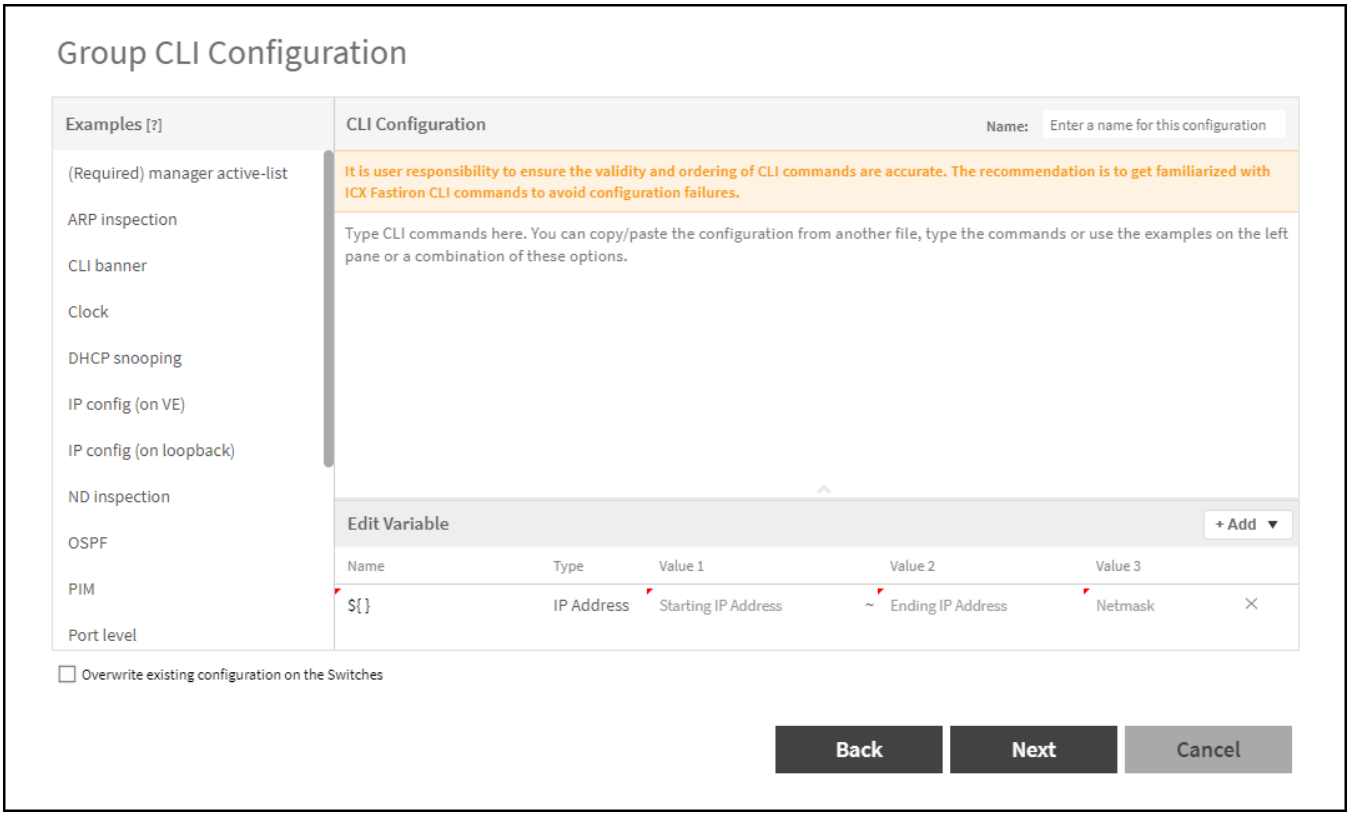
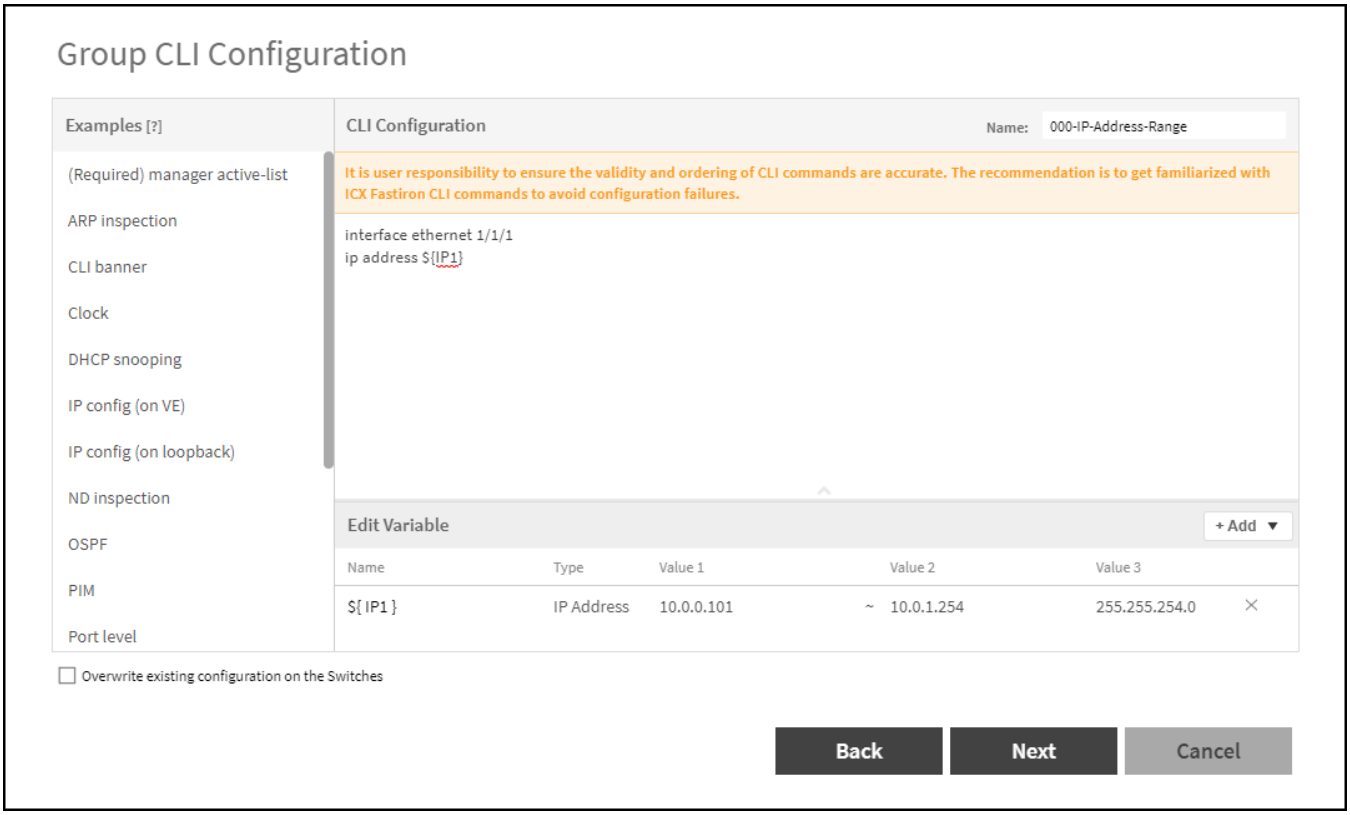


FIGURE 137 Example for IP address in variable



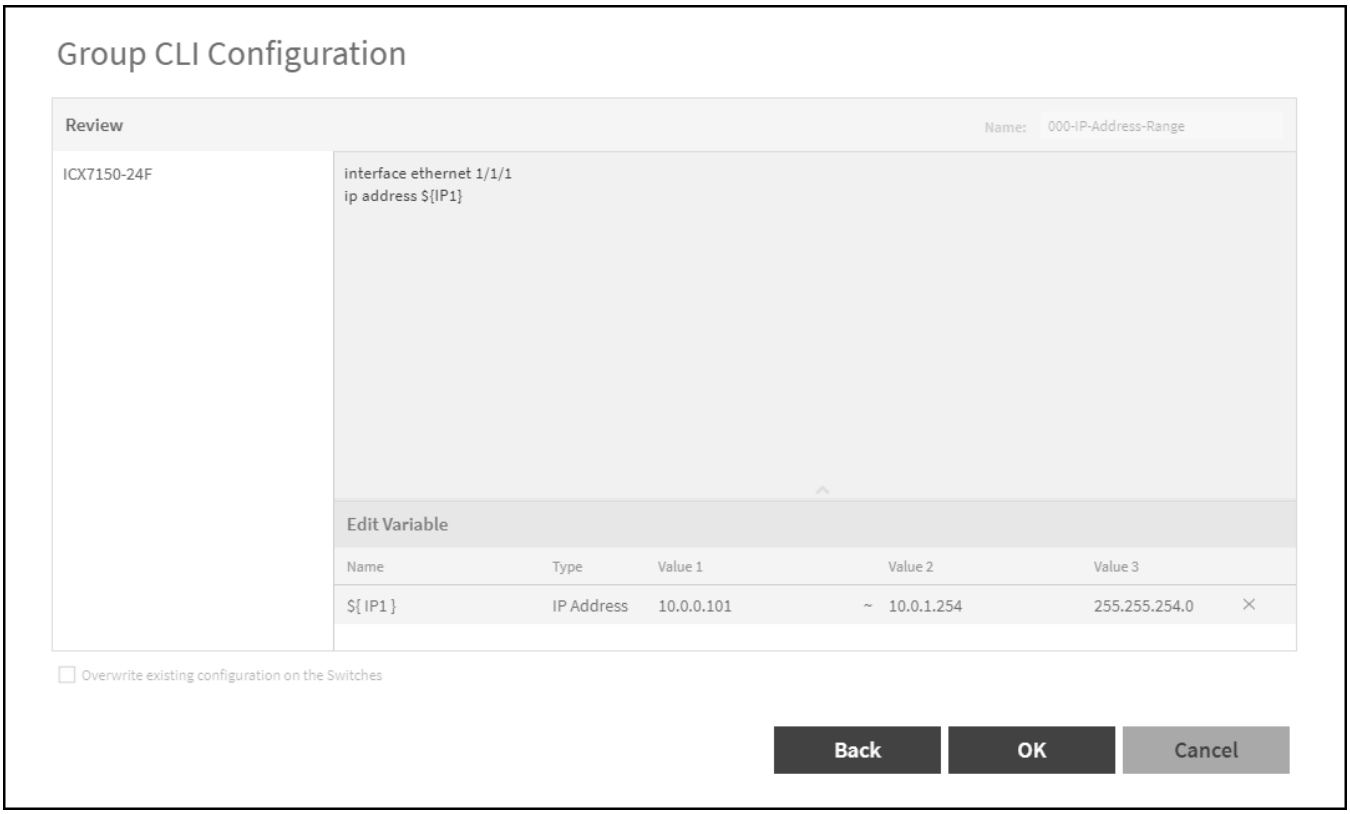
7. Variables asists in applying unique configuration to the switches. For example, IP address can be defined as a variable so that each switch gets assigned a unique IP address . In the **Edit Varible** field, enter the **Name**, **Type**, **Value 1**, **Value 2** and **Value 3** of the variables, where **Value1** denotes the “Starting IP Address”, **Value 2** denotes the “Ending IP Address”, and **Value 3** is the “Netmask".

   NOTE
   The **Edit Variable** field is optional.

   By default, the **Overwrite existing configuration on the Switches** option is not selected and only the factory-default switches (no start-up config) will inherit the group level configuration. If this option is selected, smart zone will replace the existing configuration of the switch with the configuration defined for the group

8. After reviewing the Group CLI Configuration, click **OK**.

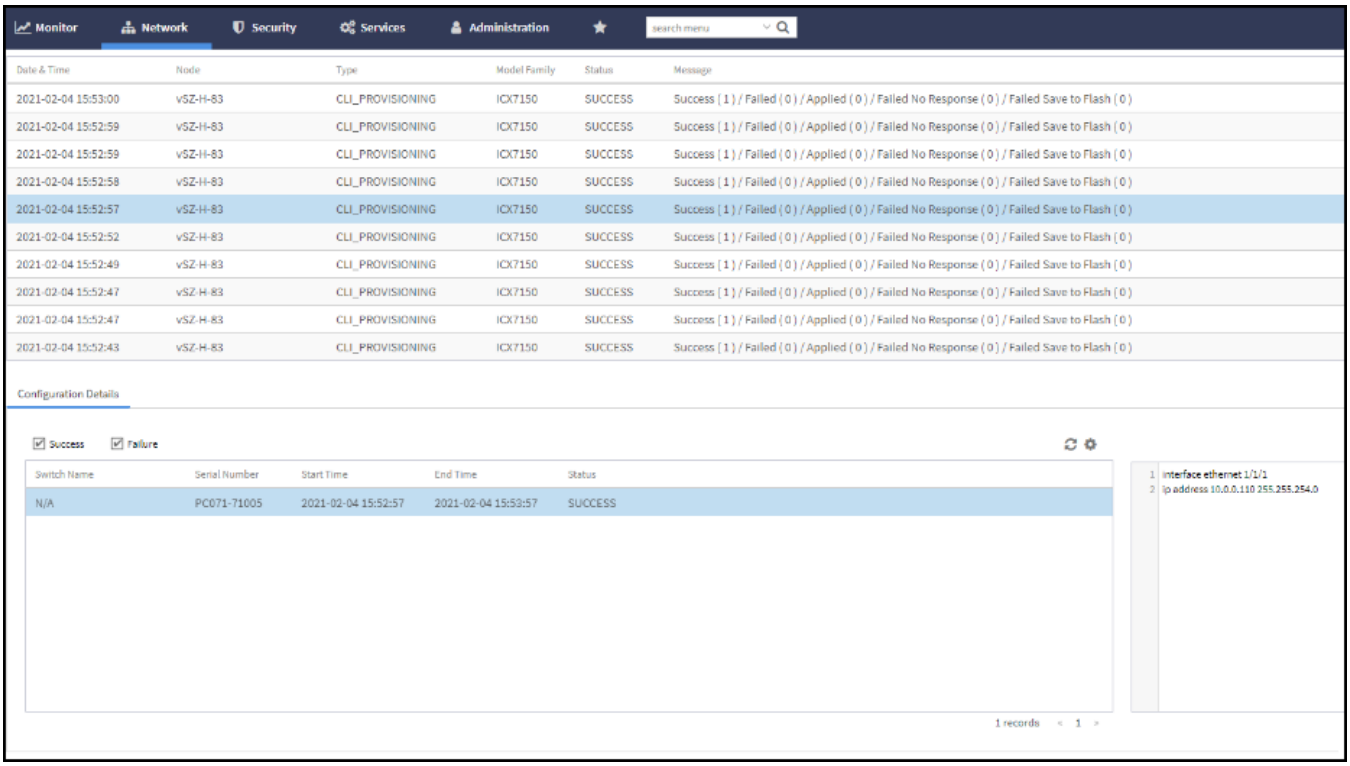
FIGURE 138 Reviewing the Group CLI Configuration



9. A confirmation dialog box is displayed, click **OK**.

10. The switch group is now Group CLI Configuration enabled and is available for provisioning.

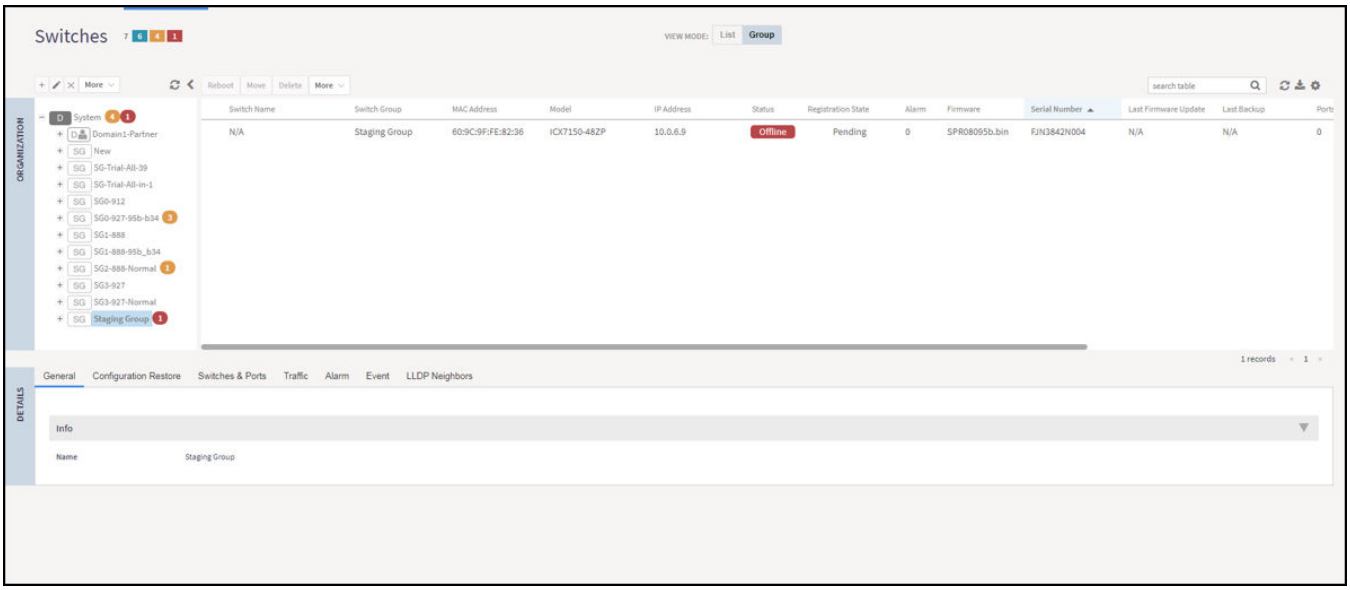
FIGURE 139 Provisioning the Group CLI Configuration Setup



11. After the configuration is setup, any factory default switch joining the group will get the configuration applied and rebooted for the configuration to take effect.

12. From the **Switches** group, select **Switches**.

FIGURE 140 Discovering a New switch



CLI Templates

CLI templates enable users to make incremental configuration changes on the fly to the selected switches. CLI templates are not tied to any switch or switch group. Once defined, they can be applied to any selected switch(es) or Switch Groups.

NOTE
Only an administrator with Full Access permission can update CLI configurations. The validity of CLI commands and their ordering rests solely with the administrator.

Using CLI templates

1. From the **Dashboard**, select **Network** tab.
2. From the **Switches** group, select **Switches**.
3. Click the **Configuration** tab.

4. Click **CLI template**. Click **Create** to create a new CLI template. You can also select a existing template click **Next** to update the CLI commands.

FIGURE 141 Creating a New CLI Template

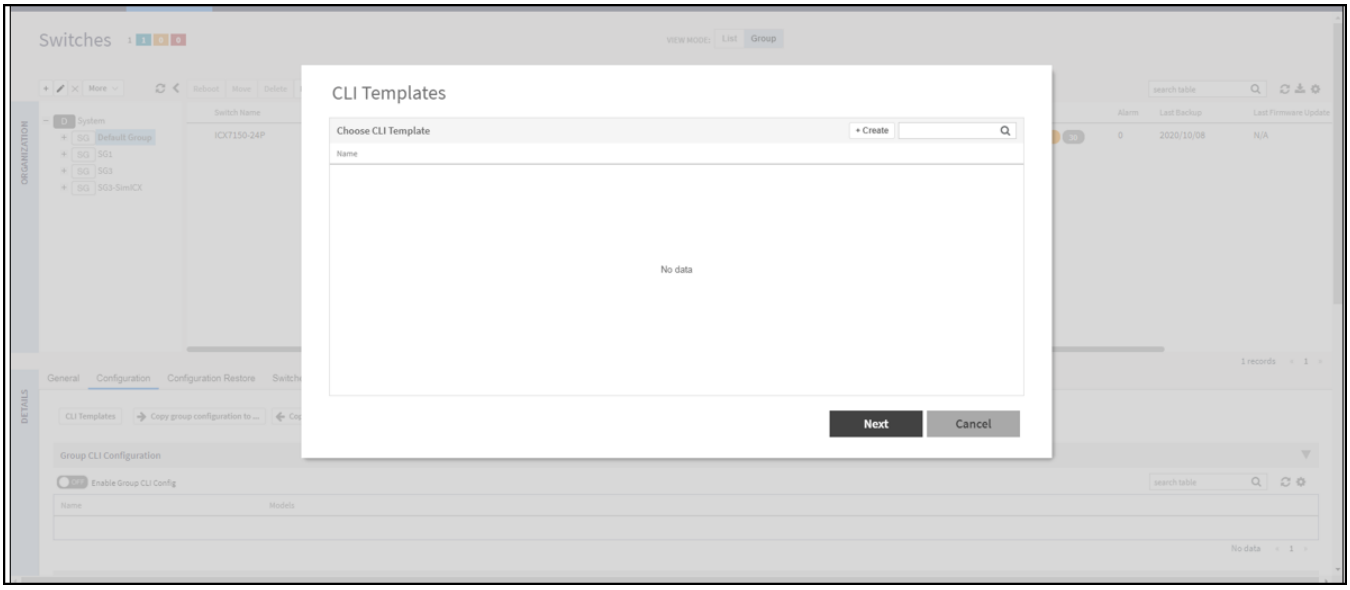
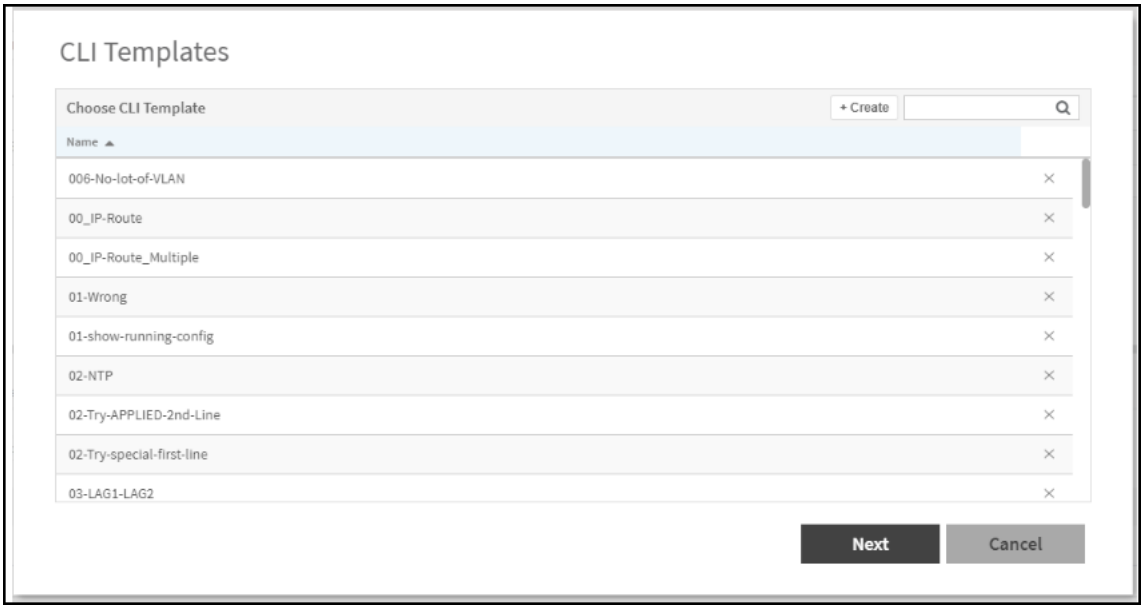
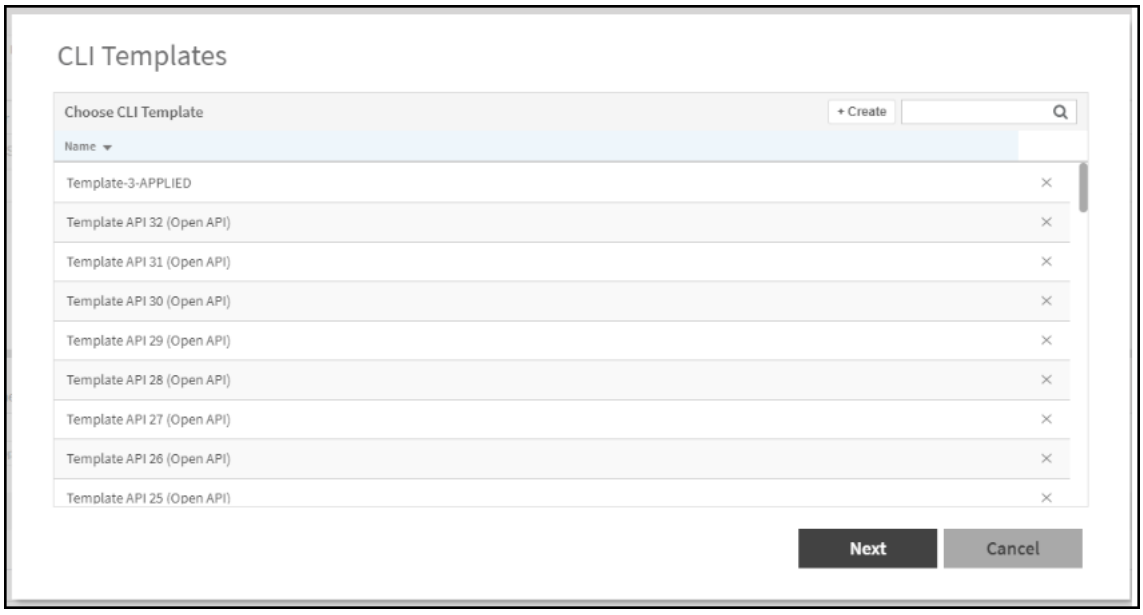


FIGURE 142 Choosing the CLI Template





5. For a new CLI template, complete the following steps.
6. Enter the name of the CLI template in the **Template Name** field.
7. Variables helps to apply unique configuration to the switches. For example, IP address can be defined as a variable so that each switch gets assigned a unique IP address. In the **Edit Variable** field, enter the **Name**, **Type**, **Value 1**, **Value 2**, and **Value 3** for IP address variables, where Value1 denotes the “Starting IP Address”, Value 2 denotes the “Ending IP Address”, and Value 3 is the “Netmask".

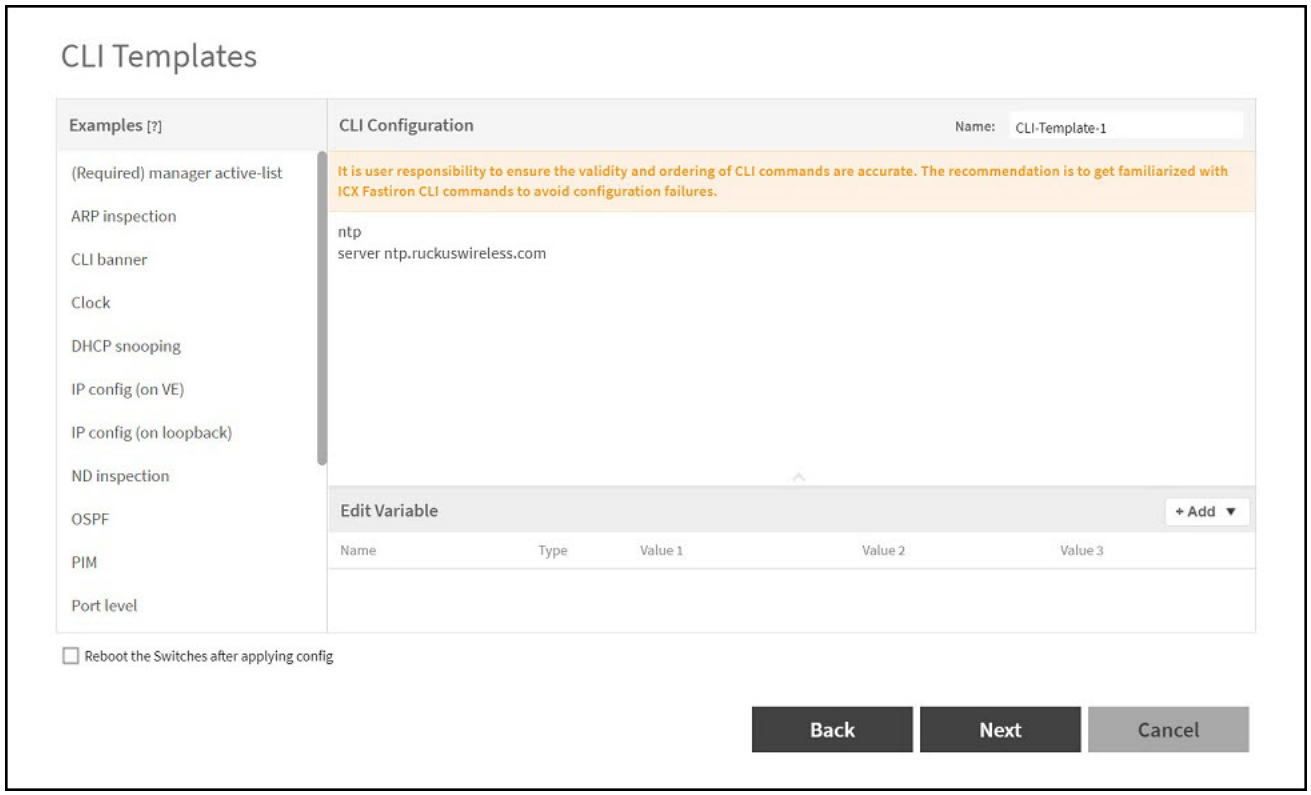
   NOTE
   The **Edit Variable** field is optional.

8. Select **Reboot Switches after applying config** if you want the switch to reload after the configuration update. If you do not select this option, the switch will not reload after the configuration update

9. Insert or edit the command lines in the space provided and click **Next**.Users can choose the CLI commands under the 'Examples' pane to build configuration. Alternatively, CLI commands can be typed directly or copied from a notepad and pasted into the 'CLI Configuration' box.

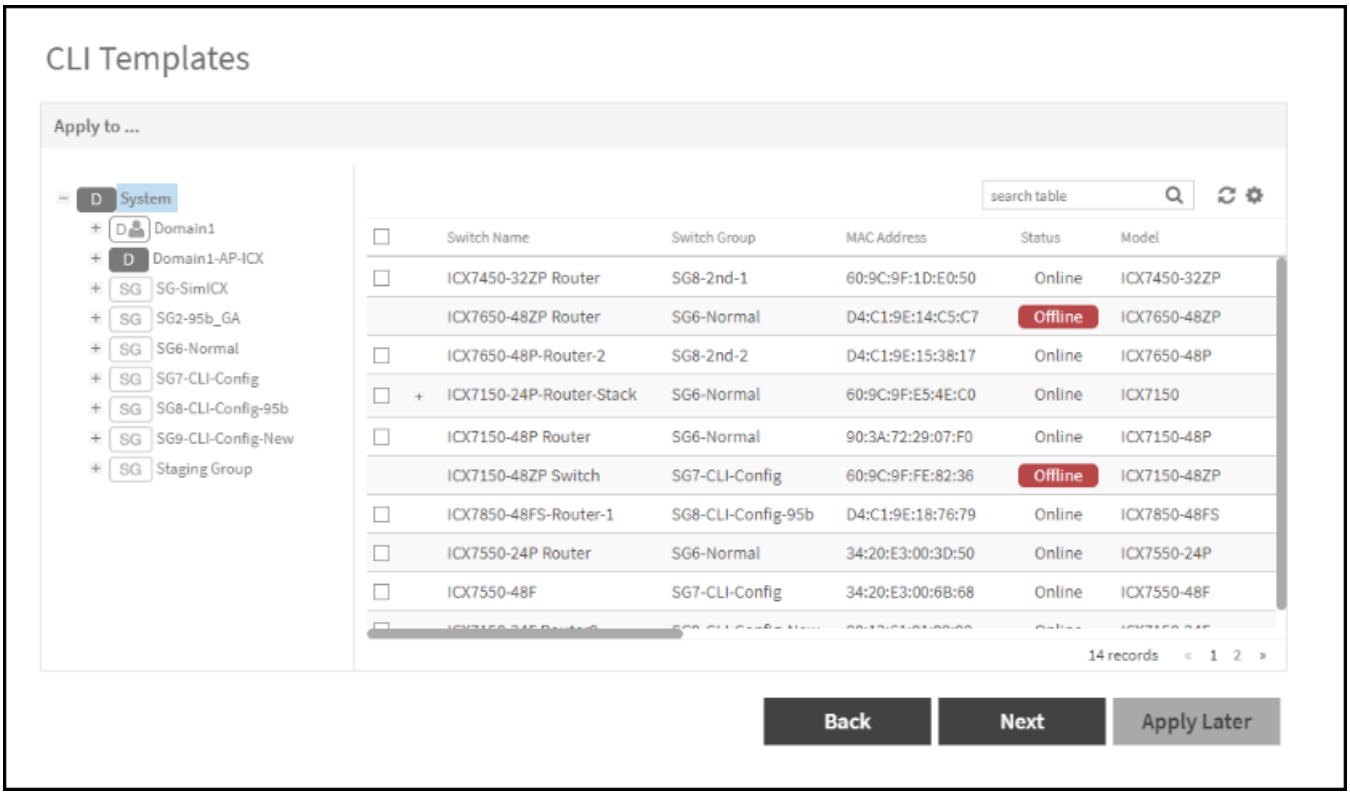
   NOTE
   It is recommended that users get familiarized with FastIron commands and their ordering to avoid any issues with applying the configuration.

FIGURE 143 Editing the CLI Template



10. Select the target switches and click **Next**.

FIGURE 144 Selecting Switches

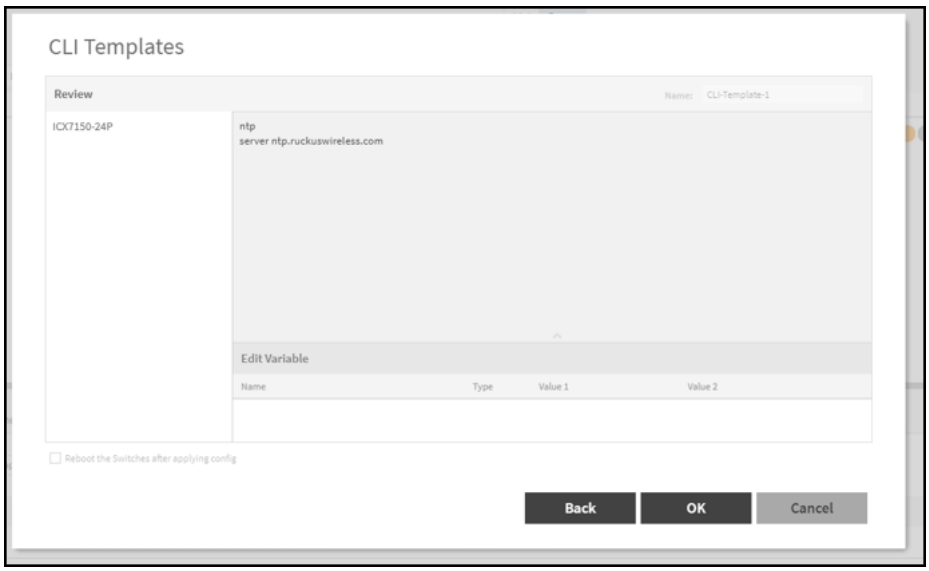


NOTE
Configuration will be applied only to the switches that are online. Users need to re-apply configuration for switches that are offline at a later time when they come back online.

11. After reviewing the CLI template, click **OK**.

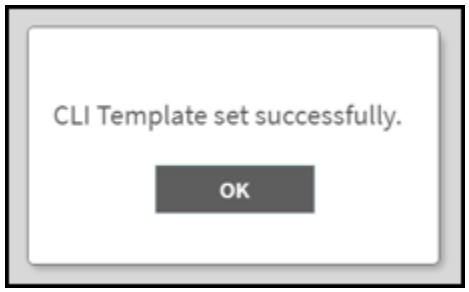
    The **CLI Template** review page is displayed.

    FIGURE 145 Reviewing the CLI Template



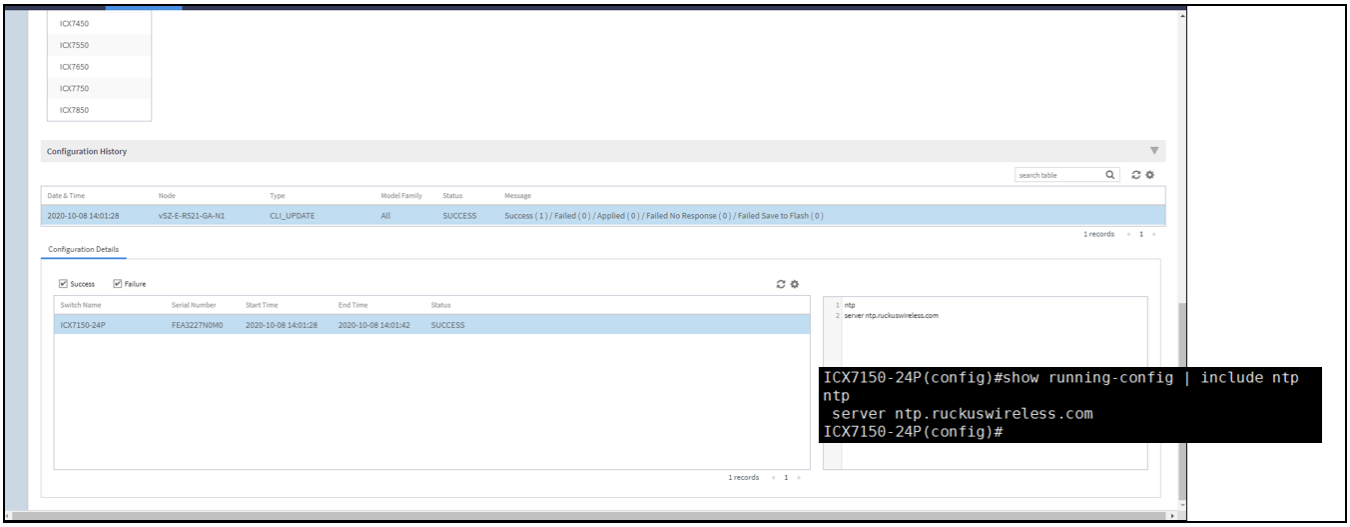
12. After reviewing the CLI Configuration template, click **OK** to save the created template and apply to the selected switches.

    FIGURE 146 Applying the CLI Template



13. Select the **Configuration** tab at the bottom of the Switch page and select **Configuration Details** to ensure the CLI template is successfully added to the switch.

FIGURE 147 Updating the Command Lines to Switch



The following status messages are displayed on the **Status** tab.

- **Success** if the configuration is applied successfully.
- **Failed** if there is a failure in configuring a switch.
- **Applied** if the configuration is partially successful with one ore more informational messages or warnings returned by the switch.

Port Settings

Port level configuration can be viewed and edited from the **Switch Port** page. You can select ports belonging to a single switch or from different switches within a switch group. The search box can be used to filter ports based on port numbers, names, or VLANs. Once the desired list of ports are filtered, you can select the ports and make changes to their existing settings by performing the procedure Creating Switch Level Configuration on page 272.

Configuring Port Settings for a Switch

Port settings enable you to configure ports for a switch, stack, or switch group. You can also invoke the ACL in port configuration for applying the Quality of Service (QoS) settings to proritize VOIP and VIDEO VLAN traffic.

NOTE
Port settings for QoS can only be configured for switches that are executing firmware version 08.0.95 and above.

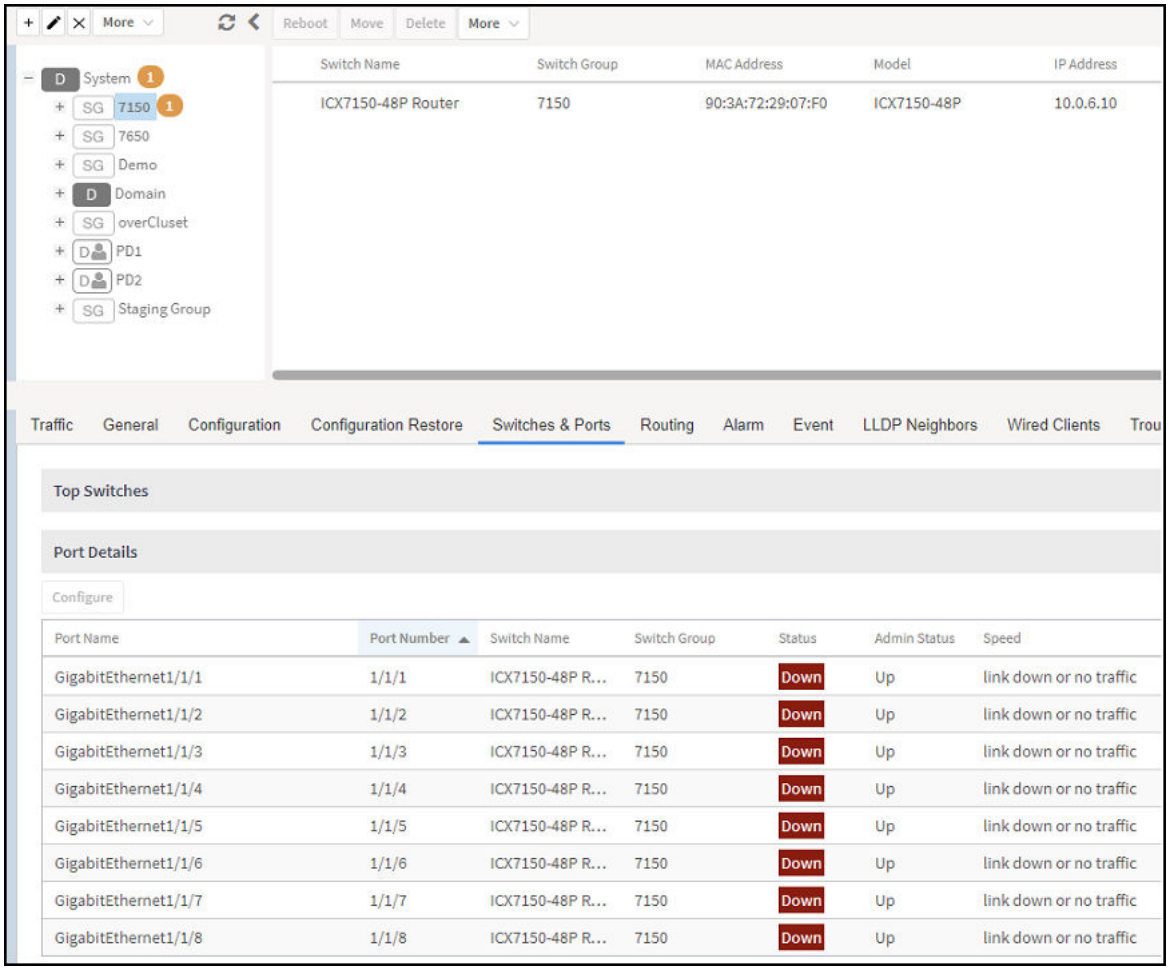
1. From the main menu, go to **Network** > **Wired** > **Switches.**

   The **Switches** page is displayed.

2. Select the switch group, and click the **Switches and Ports** tab.

   The **Switch Port** page is displayed.

   FIGURE 148 Switch Port Page



3. Go to **Network** > **Switches.**

4. Select a switch, under the **Port Details**, select the port that must be updated and click **Configure**.

   The **Port Settings** page is displayed.

   FIGURE 149 Port Settings Showing Single Update

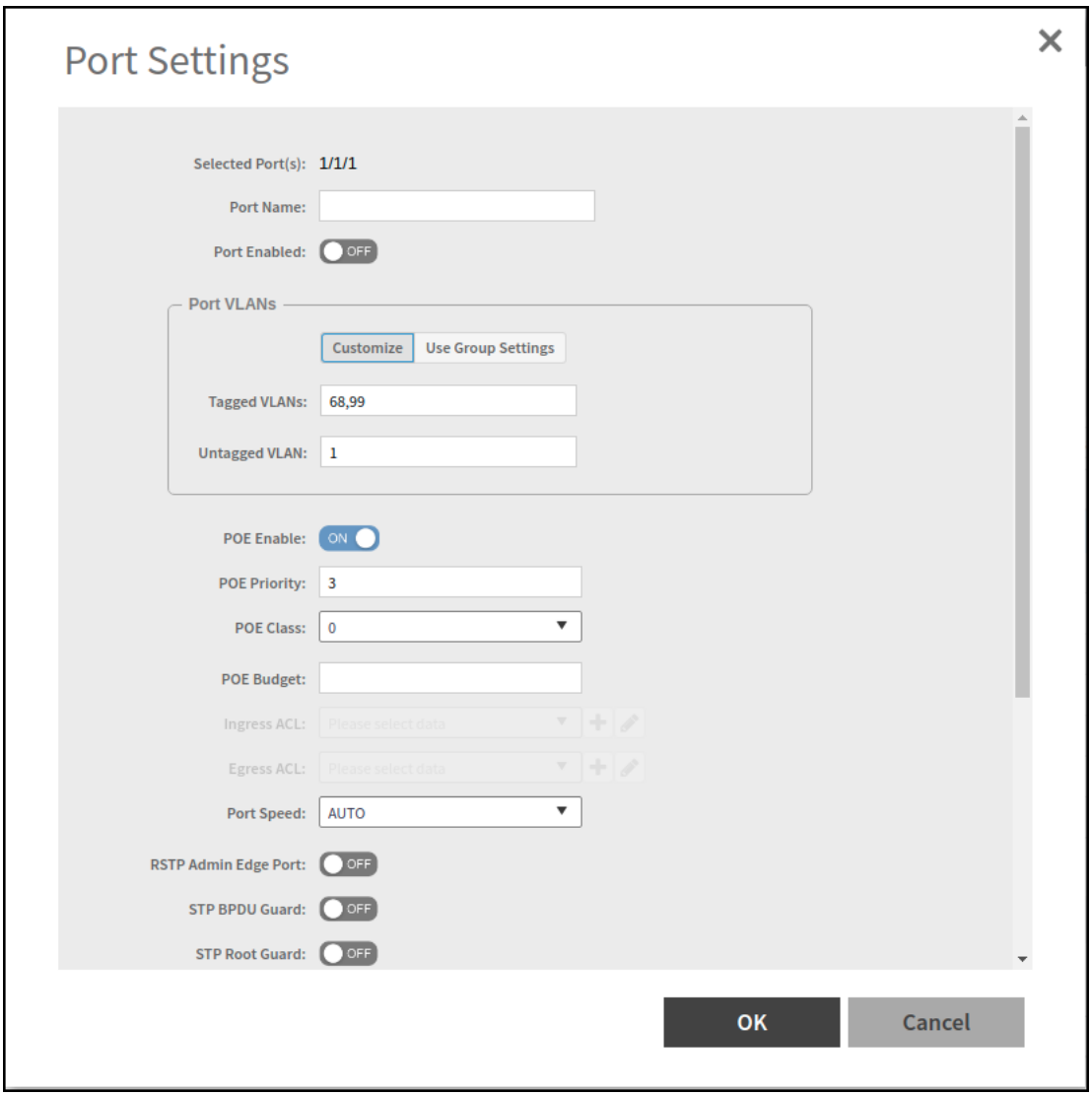


FIGURE 150 Poret Settings Showing Multiple Update

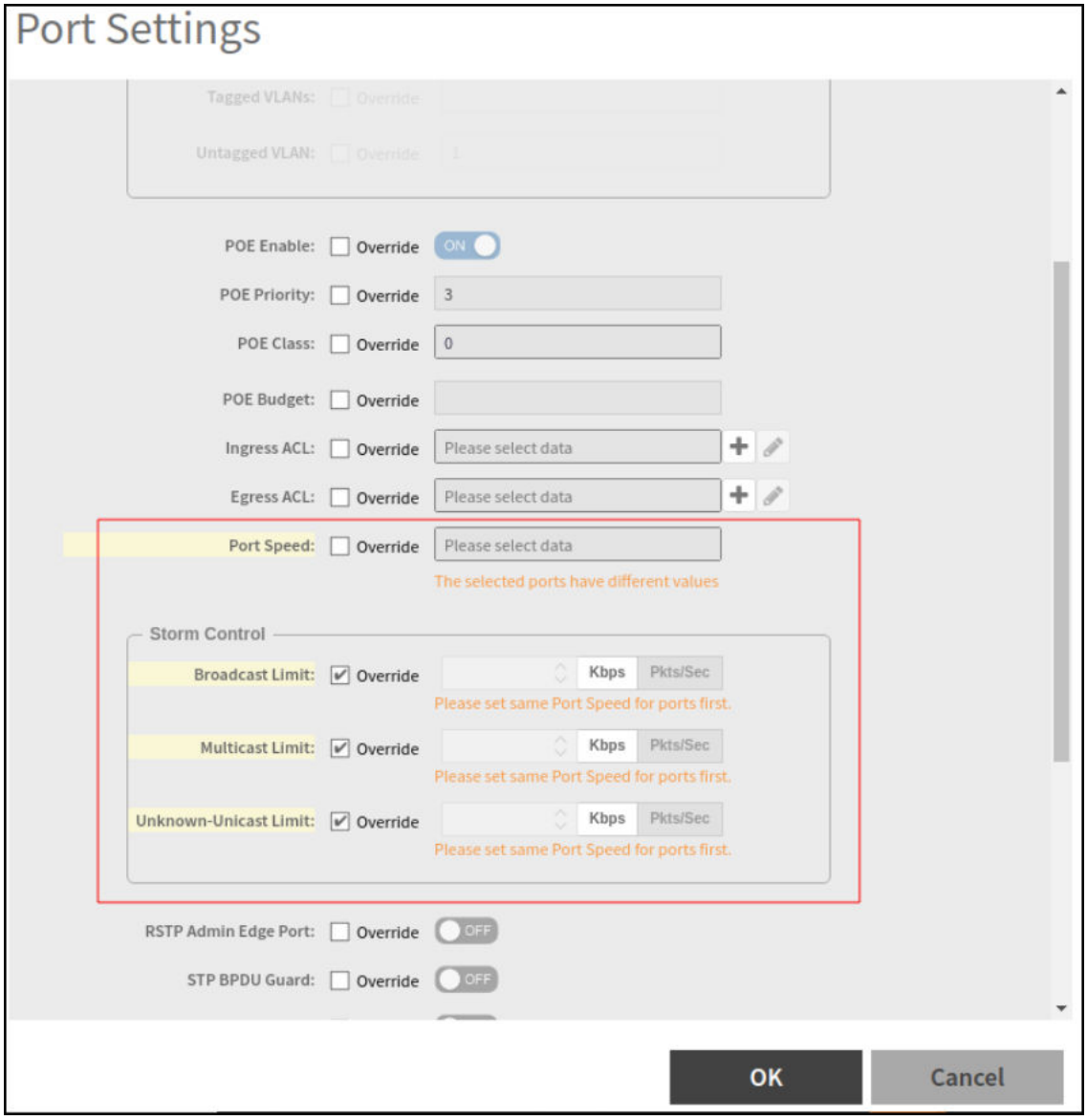
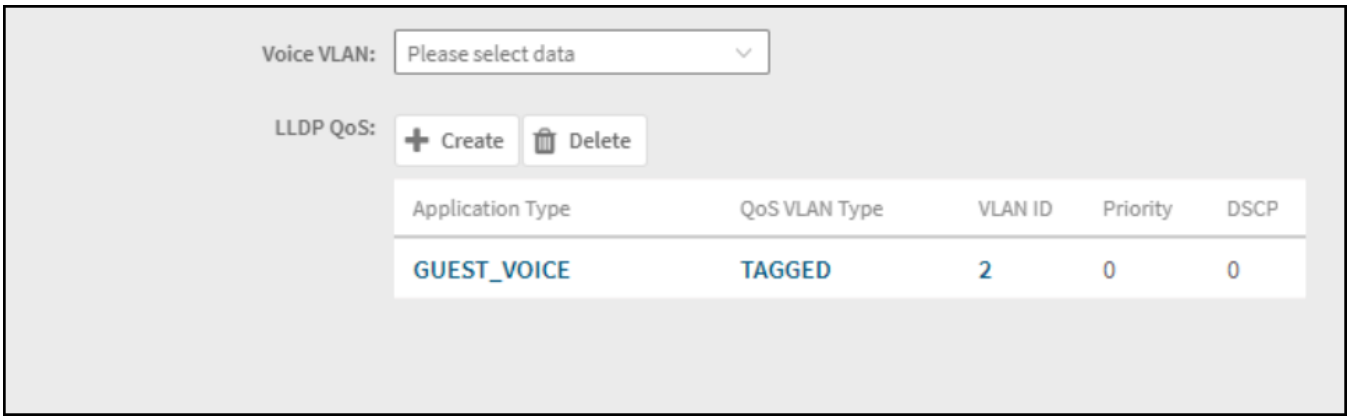


FIGURE 151 Port Settings for QoS


Voice VLAN:
Please select data
LLDP QoS:
Create
Delete
Application Type
QoS VLAN Type
VLAN ID
Priority
DSCP
GUEST_VOICE
TAGGED
2
0
0

5. Configure the following port settings:
   - **Port Name**: Enter the port name.
   - **Port Enabled**: Click to enable the port.
   - **Port VLANs**: If you configure VLAN on both group model configuration and port settings, port level changes takes precedence.
   - **Customize**: Click customize to identify the ports that need to stay customized.
   - **Use Group Settings**: Click user group settings to rebind the identified ports back to the group level.
   - **Port Protected**: Click to enable the protected port.

     NOTE
     Port Protected field is displayed only for the switches using SmartZone 5.2.1 and above.

   - **Tagged VLANs**: Enter the tagged VLAN ID or VLAN ID range.
   - **Untagged VLAN**: Enter an untagged VLAN ID.
   - **POE Enable**: Click to enable PoE.
   - **POE Class**: Selecct the PoE class. You can configure the PoE budget on ports by setting the PoE class to 0 through 4.
   - **POE Priority**: Enter the PoE priority.
   - **POE Budget**: Allows users to manually set the PoE power limit.
   - **Ingress ACL**: Select the ingress ACL from the list.
   - **Egress ACL**: Select the egress ACL from the list.
   - **Port Speed**: Select the required Port Speed from the list.
   - **Storm Control**: If you set Storm Control configuration on a switch, and if this switch joins the controller, you must ensure that the Storm Control configuration on the controller is also set.The Storm Control includes the following fields - Broadcast, Multicast, and Unicast.

     NOTE
     The value 0 pkts/sec and 0 kbps indicates storm control is disabled.

   - **Broadcast Limit**: Enter the Broadcast Limit value in this field. The maximum value in **Pkts/sec** is 8388607 and the minimum value is 1; when the port speed is set to **Auto** or **Optic**, the maximum value in **kbps** is 1000000 and the minimum value is 1; when the port speed is other than auto or optic the minimum value in **kbps** is 1 and the maximum value is equivalent to the selected port speed .
   - **Multicast Limit**: Enter the Multicast Limit value in this field. The maximum value in **Pkts/sec** is 8388607 and the minimum value is 1; when the port speed is set to **Auto** or **Optic**, the maximum value in **kbps** is 1000000 and the minimum value is 1; when the port speed is other than auto or optic the minimum value in **kbps** is 1 and the maximum value is equivalent to the selected port speed .
   - **Unicast Limit**: Enter the Unicast Limit value in this field. The maximum value in **Pkts/sec** is 8388607 and the minimum value is 1; when the port speed is set to **Auto** or **Optic**, the maximum value in **kbps** is 1000000 and the minimum value is 1; when the port speed is other than auto or optic the minimum value in **kbps** is 1 and the maximum value is equivalent to the selected port speed .
   - **RSTP Admin Edge Port**: Click to enable the RSTP Admin Edge Port.
   - **STP BPDU Guard**: Click to enable the STP BPDU Guard.
   - **STP Root Guard**: Click to enable the STP Root Guard.
   - **DHCP Snooping Trust Port**: Click to enable the DHCP Snooping Trust Port.
   - **IPSG**: Click to enable IPSG.
   - **ILLDP**: Click to enable ILLDP.
   - **Voice VLAN**: Select the VLAN (tagged or untagged).
   - **LLDP QoS**: Click to enable LLDP-MED settings.

- **Application type**: Enter one of the application types : **Guest_Voice**, **Guest_Voice_Signaling**, **Softphone_Voice**, **Streaming_Video**, **Video_Conferencing**, **Video_Signaling**, **Voice**, and **Voice_Signaling**.
- **VLAN type**: The VLAN type can be priority-tagged, tagged, or untagged.
- **VLAN ID**: Enter the **VLAN ID** of the VLAN type.
- **Priority**: Enter the priority for the QoS setting.
- **DSCP**: Enter the DSCP value for the LLDP setting.

6. Click **OK**.

VIDEO
PoE per port settings. The below video displays the tasks to be performed to configure PoE on a port.
Click to play video in full screen mode.

Editing Ports Across Multiple Switches

Before 5.2.1 release, the user could edit multiple ports for an individual switch. But after 5.2.1 release, the controller allows the user to edit the ports across multiple switches within the same Switch Group.

For example, if you want to disable port 1/1/11 and 1/1/12 across multiple switches, the controller provides an option to filter the ports list by typing the search criteria.

The search criteria is based on the following.

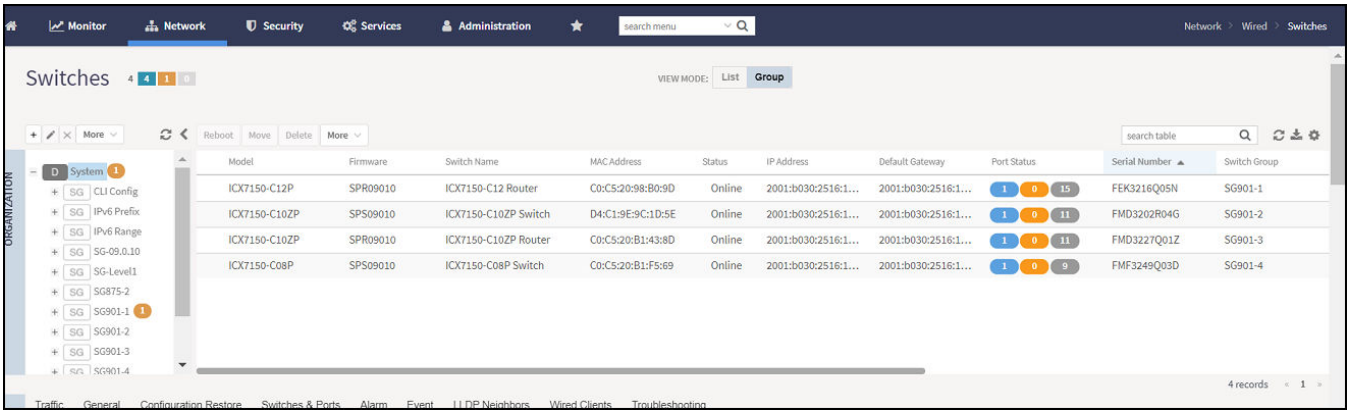
- Switch Name
- Port numbers - comma separated values (1/1/1,1/1/11,1/1/24), (or) Range of ports (1/1/1 to 1/1/20)
- VLAN membership
- PoE detected ports
- Port Status
- Admin Status

You must complete the following steps to edit ports across multiple switches.

1. From the main menu, go to **Network** > **Wired** > **Switches.**

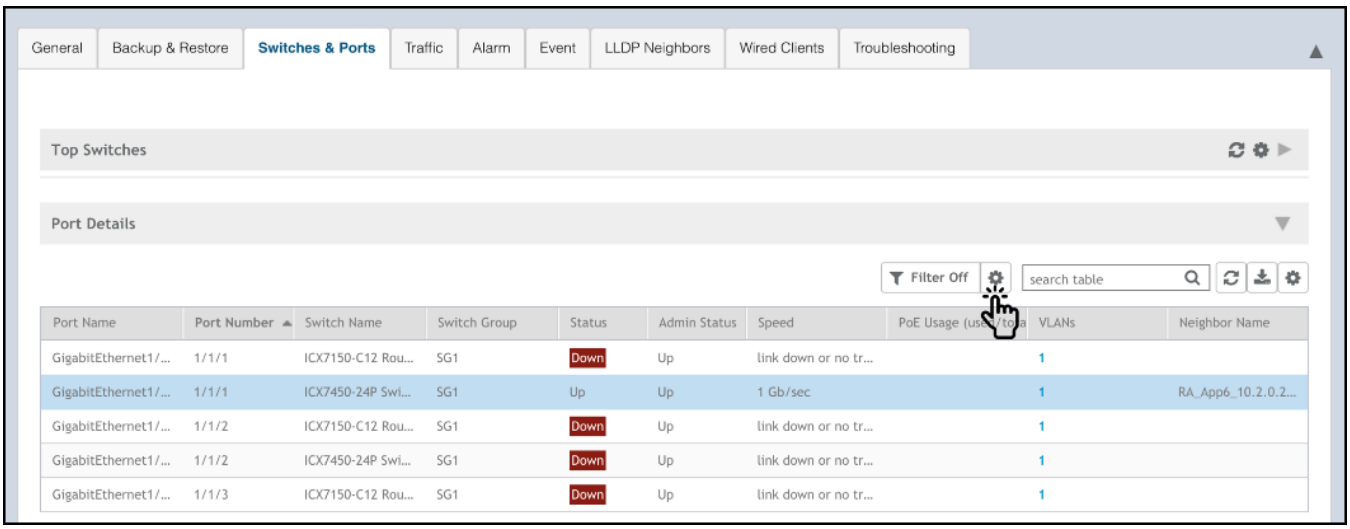
   The **Switches** page is displayed.

   FIGURE 152 Switches Page



2. Select a **Switch Group**.
3. Click the **Switches and Ports** tab.

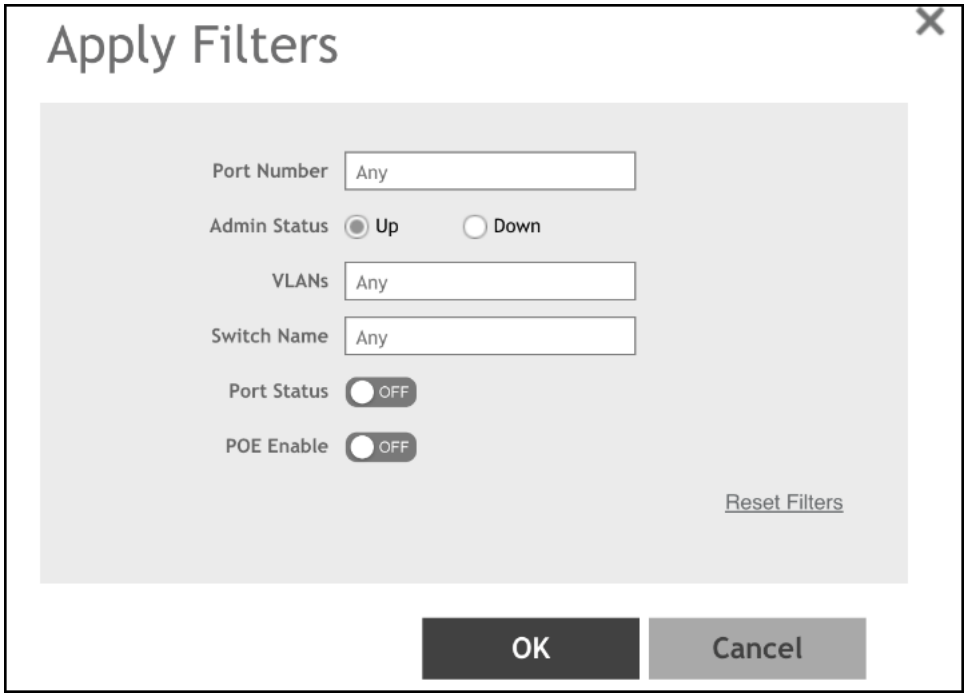
FIGURE 153 Viewing the Switches and Ports Page



4. Click the icon.

   A dialogue box is displayed. The controller provides the following filters to combine several query conditions to filter-out the ports which you want to edit.

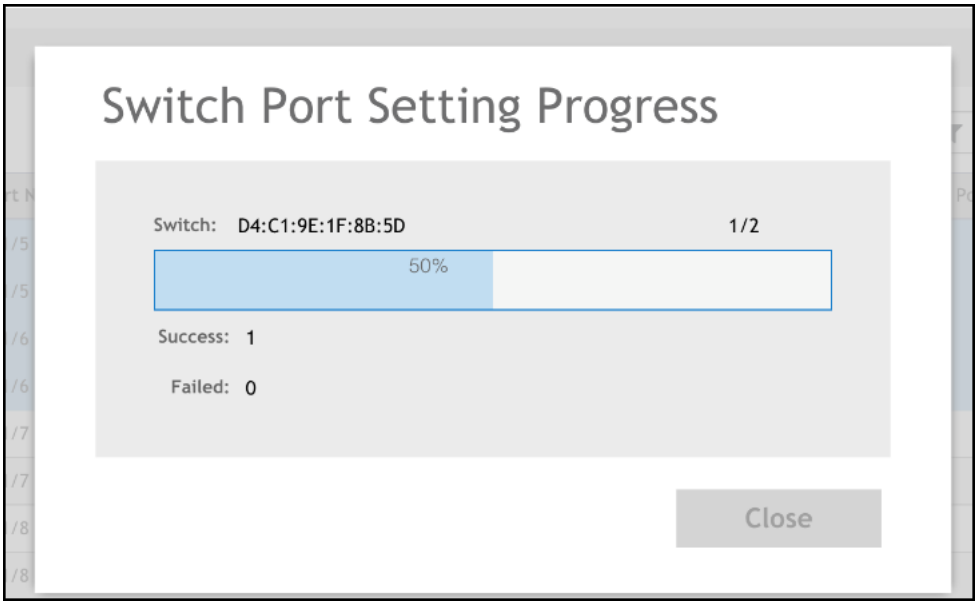
   FIGURE 154 Applying Filter to Edit the Ports



5. Click **OK**.

   The controller applies the above filters to return ports that meet the search criteria.

   FIGURE 155 Showing the Progress of Switches Fulfilling the Search Criteria



Creating Routing Configurations

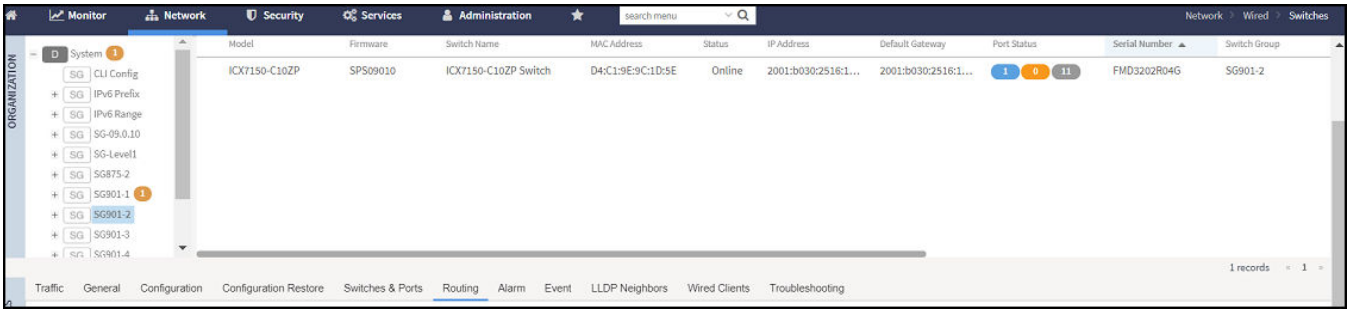
You can create, edit, and delete routing configurations for an switch.

1. From the main menu, go to **Network** > **Wired** > **Switches.**

   The **Switches** page is displayed.

2. Select the switch group or switch and click the **Routing** tab.

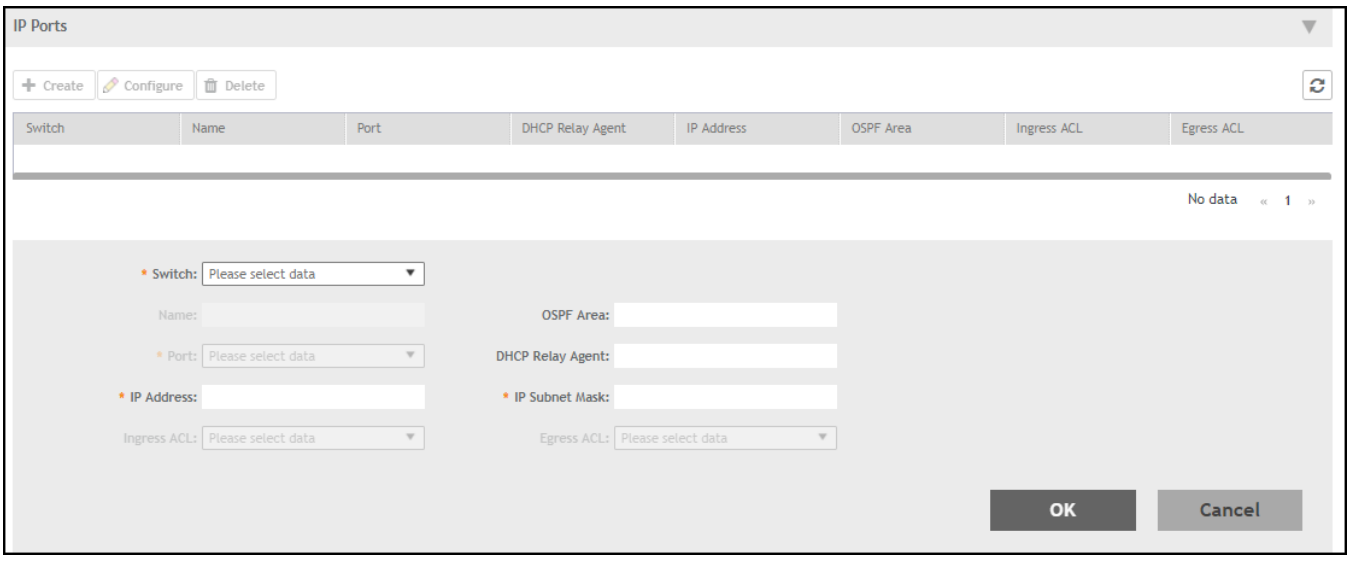
   FIGURE 156 Switch Routing Tab



3. In **IP Ports**, click **Create**.

   The **IP Ports** page is displayed.

   FIGURE 157 IP Ports Page



   Configure the following IP port information:

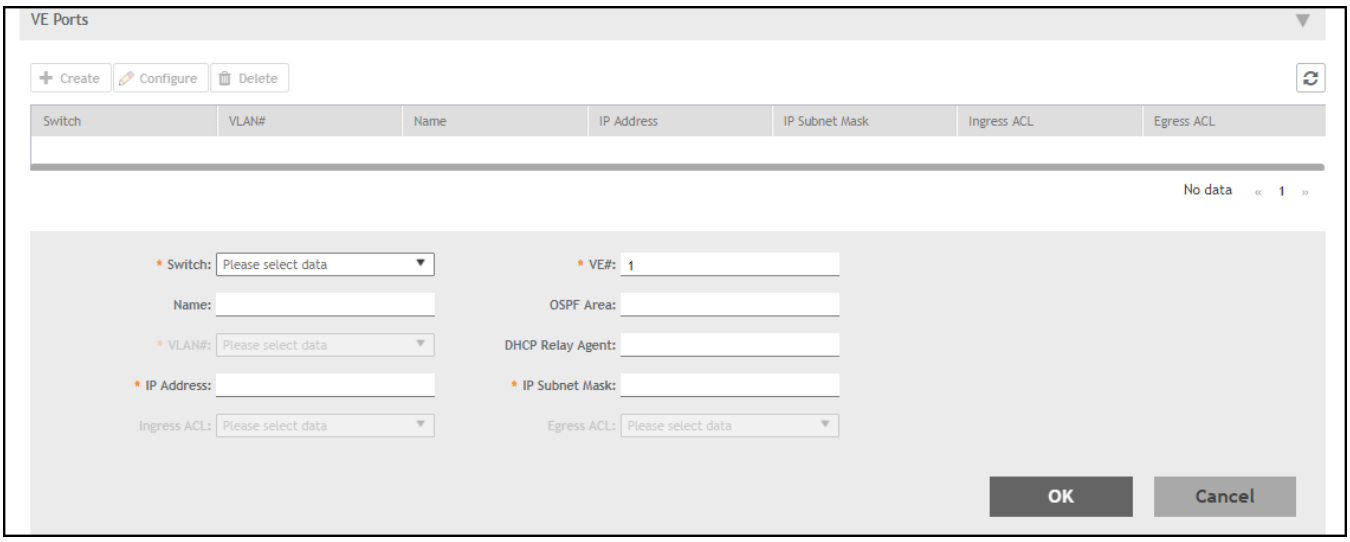
   - **Switch**: Select the switch from the list,
   - **Name**: Enter a name.
   - **OSPF Area**: Enter the OSPF area IPv4 address.
   - **Port**: Select the port number from the list.
   - **DHCP Relay Agent**: Enter the DHCP relay agent IP address.
   - **IP Address**: Enter a unicast IP address.
   - **IP Subnet Mask**: Enter an IP subnet mask.
   - **Ingress ACL**: Select the ACL for the ingress network interface.
   - **Egress ACL**: Select the ACL for the egress network interface.

4. Click **OK**.

5. In **VE Ports**, click **Create**.

   The **VE Ports** page is displayed.

   FIGURE 158 VE Ports Page



   Configure the following VE port information:

   - **Switch**: Select the switch from the list.
   - **VE#**: Enter the VE number. Range: 1 through 4095.
   - **Name**: Enter a name.
   - **OSPF Area**: Enter the OSPF area IPv4 address.
   - **VLAN#**: Select the VLAN from the list.
   - **DHCP Relay Agent**: Enter the DHCP relay agent IP address.
   - **IP Address**: Enter a unicast IP address.
   - **IP Subnet Mask**: Enter an IP subnet mask.
   - **Ingress ACL**: Select the ACL for the ingress network interface.
   - **Egress ACL**: Select the ACL for the egress network interface.

6. Click **OK**.

Managing Link Aggregation Groups (LAGs)

Controller provides an option to define LAGs at an individual switch level.

1. Go to **Network** > **Access Points.**

   The **Create LAG** page is displayed.

2. Enter the following settings:
   - **LAG Name**: Enter a name.
   - **Type**: Select either **Static** or **Dynamic** from the list.
   - **Selected Port**: You can select multiple port numbers from the list.
   - **Tagged VLANs**: Enter the tagged VLAN ID or VLAN ID range.
   - **Untagged VLANs**: Enter an untagged VLAN ID.
3. Click **OK** to apply the LAG configuration onto the selected switch.

Creating a Switch Stack

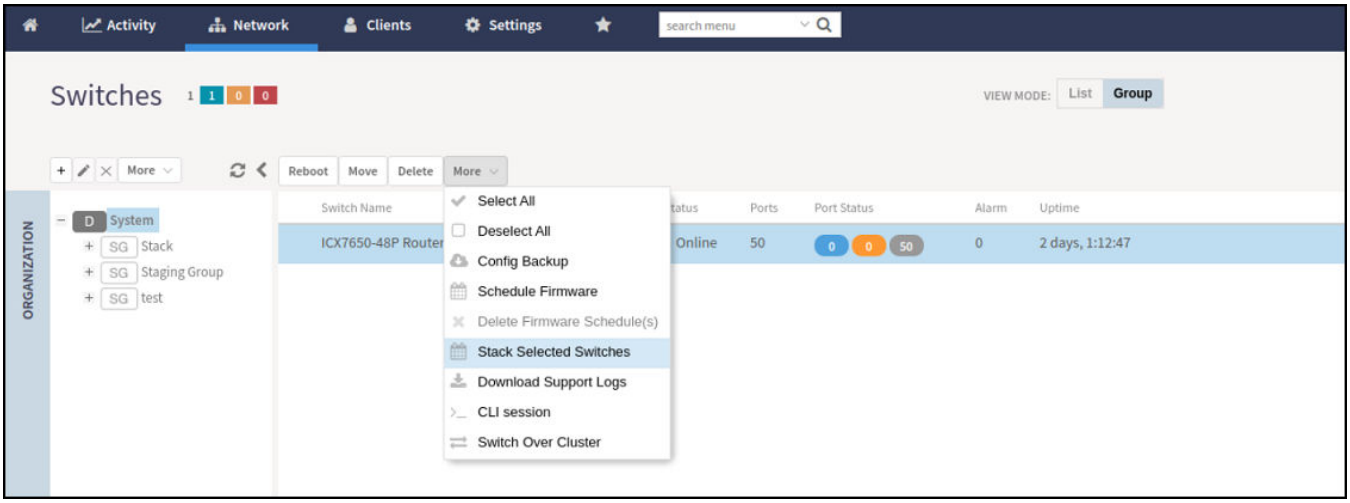
You can create a stack by selecting individual switches that are connected to the controller.

As a pre-requisite, you must configure switch stacking from controller before connecting the switch cables.

Complete the following steps to create a stack of switches.

1. From the main menu, go to **Network** > **Wired** > **Switches.**

   FIGURE 159 Switches Page



2. Select the switches that are to be stacked, and click **More** > **Stack Selected Switches**.

   The **Create Stack** page is displayed.

   FIGURE 160 Creating a Stack

3. Under **Active Role**, select **ON** for the selected switches and click **OK** to create the stack. After 15 minutes switches form stack as seen in the next step.
4. Click Stack

Viewing Port Details

Details on port use are available for individual switches, stacks, and switch groups.

Perform these steps to display information on ports for a switch, stack, or switch group.

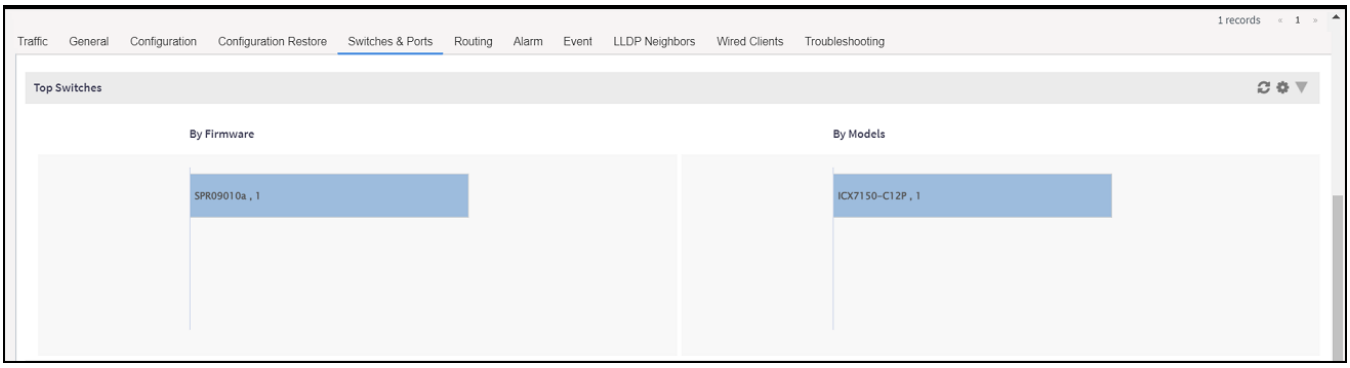
1. From the main menu, go to **Network** > **Wired** > **Switches.**

   The **Switches** page is displayed.

2. Select the switch or group and click the **Ports** tab.

   For a switch group, a **Top Switches** page similar to the following figure is displayed. The graphs provide information on top switches based on firmware and model.

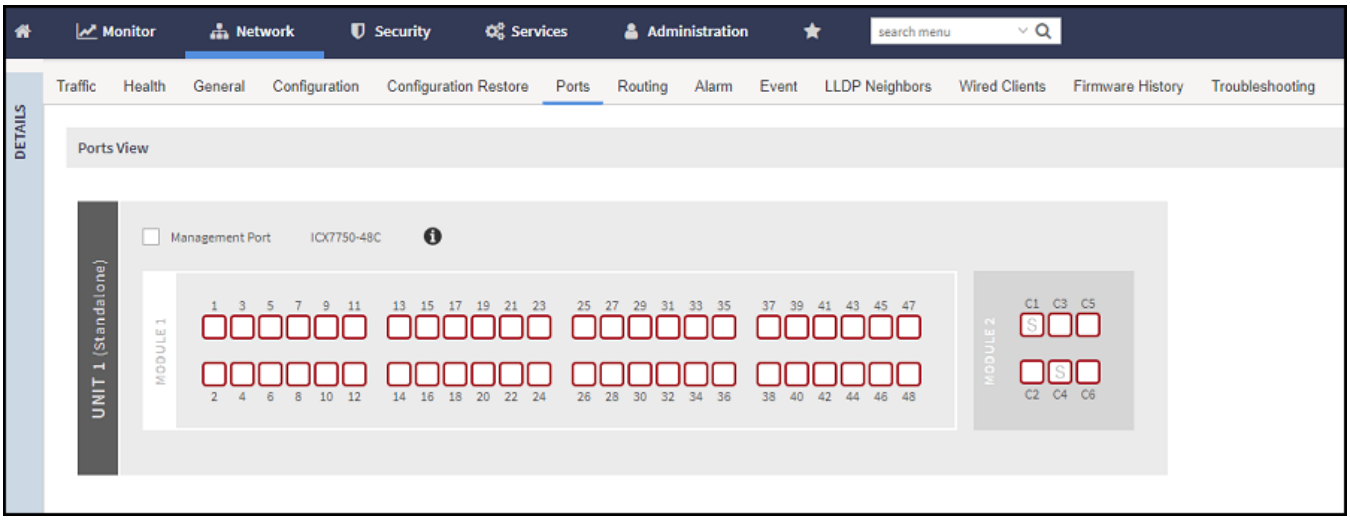
   FIGURE 161 Top Switches Page



3. Click the switch name to view the **Front Panel View** page for additional port information as shown in the following figure.

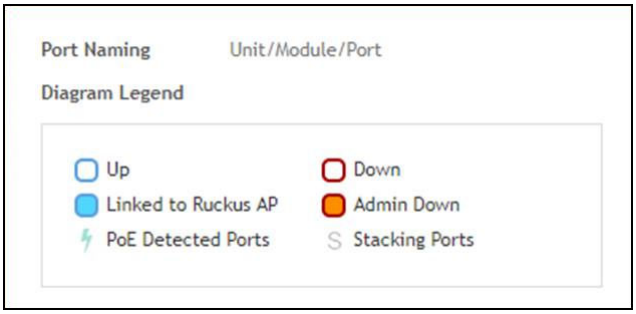
   The **Front Panel View** page provides information on the state of all ports in each switch module, for example port Up, Down, or Administratively Down. Additional port details can be seen by hovering the mouse over the port.

FIGURE 162 Front Panel View



The following figure shows the diagram legend used in the Front Panel View page.

FIGURE 163 Diagram Legend



The following list further describes items in the Front Panel View legend.

- Up: Ports that are up or active
- Warning: Ports that have packet errors
- Down: Ports that are down or inactive
- By Admin: Ports that have been manually disabled by the network administrator

4. Click the switch name to view the **Port Details** page as shown in the following figure.

FIGURE 164 Port Details



The **Port Details** page provides the following information on each port:

> **NOTE**
> Ports for switch stacks are not configurable from the **Port Details** page.

- **Port Name**: The port name
- **Port Number**: The port number
- **Status**: Whether the port is operationally up or down
- **Admin Status**: Whether the port has been set to Up or Down by the network administrator
- **Speed**: The speed of the port
- **PoE Device Type**: Inline power device type, such as 802.3af, 802.3at, or Legacy device
- **PoE Usage (used/total watts)**: The PoE power usage compared to the allocated power
- **VLANs**: The VLANs to which the port is connected
- **Bandwidth IN (%)**: The bandwidth utilization for incoming traffic
- **Bandwidth OUT (%)**: The bandwidth utilization of the port for outgoing traffic
- **LAG Name (Type)**: The name of the Link Aggregation Group (LAG)
- **Optics**: The type of optic
- **Neighbor Name**: When LLDP is enabled, the name of the neighboring device, such as an AP or another switch or router
- **Incoming Multicast Packets**: The total number of incoming multicast data packets
- **Outgoing Multicast Packets**: The total number of outgoing multicast data packets
- **Incoming Broadcast Packets**: The total number of incoming broadcast data packets
- **Outgoing Broadcast Packets**: The total number of outgoing broadcast data packets
- **In Errors**: The number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol
- **Out Errors**: The number of outbound packets that could not be transmitted because of errors
- **CRC Errors**: Indicates that the checksum calculated does not match between the data sender side and the received side. A CRC error usually indicates network transmission problems.
- **In Discard**: The number of inbound packets that were chosen to be discarded (even though no errors are detected) to prevent their being deliverable to a higher-layer protocol. One reason for discarding such a packet could be to free up buffer space.
- **Switch Name**: The name of the switch connected to the port
- **Switch Group**: The name of the switch group connected to the port

You can also filter the list of ports by the VLANs associated with them. Click  to set the filters.

NOTE
In this release only forming a LAG through the controller web user interface is supported. The system does not support configuring LAG interface detail through the controller web user interface. To configure detail settings for LAG after form it, you need to configure it through Switch console directly.



VIDEO
PoE Ports View. View PoE Information from SmartZone.
Click to play video in full screen mode.

Viewing Switch Health

Health information displayed for a switch is based on memory usage and CPU usage statistics.

To view information on the health of a switch or the active controller of a stack, perform the following steps.

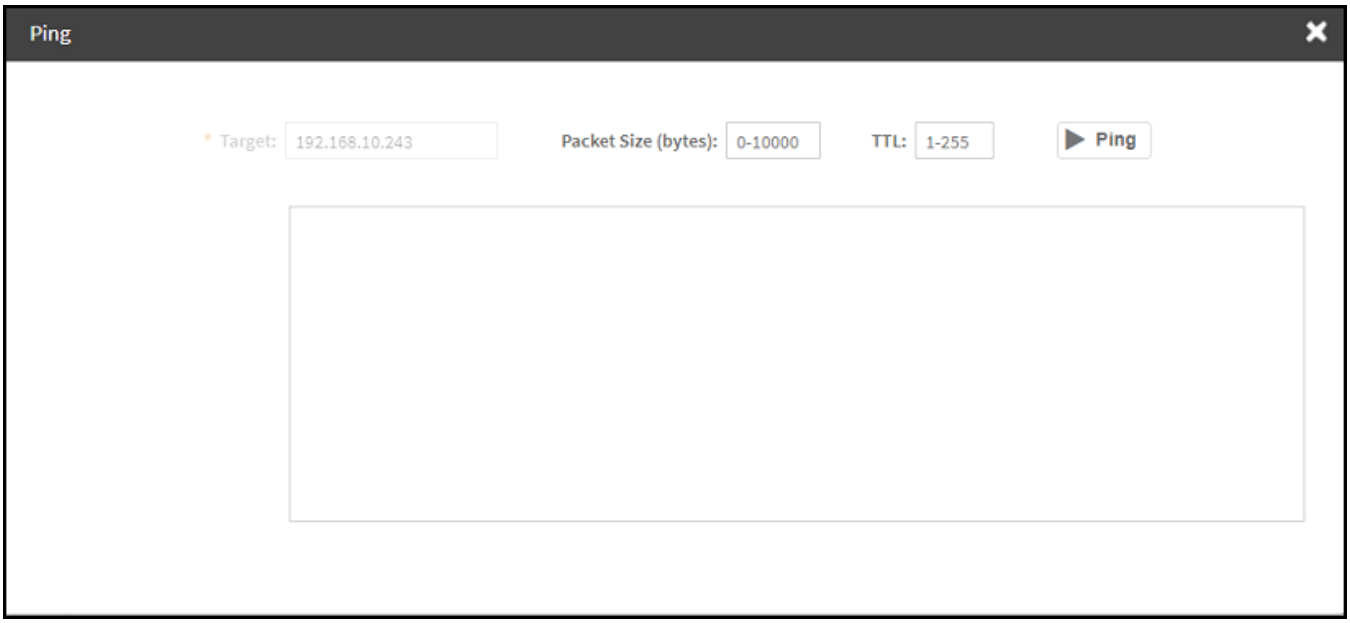
1. From the main menu, go to **Network** > **Wired** > **Switches.**

   The **Switches** page is displayed.
2. Select the switch and then the **Health** tab.
3. Click **Ping**.

   The **Ping** page is displayed.

4. On the **Ping** page, the IP address of the target switch is populated. Type the packet size and the TTL (Time to Live) value after which a packet is discarded from the network. As shown in the following example, after the ping, the page displays the number of data packets transmitted, received, and lost and the time required following the ping from the controller to the switch to establish communication.

   FIGURE 165 Pinging the switch



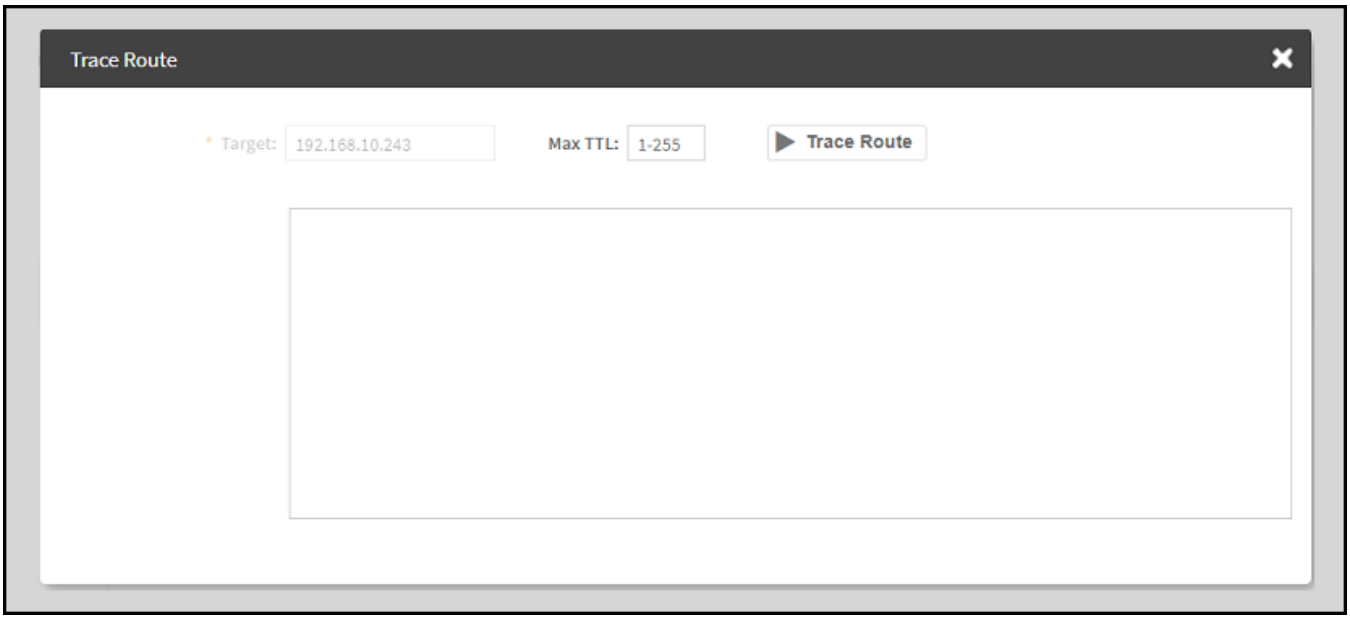
5. Click **Trace Route**.

   The **Trace Route** page is displayed.

6. On the **Trace Route** page, enter the TTL (Time to Live) value after which the packet is discarded from the network.

   As shown in the following example, the page displays the IP address of the hops the packet takes as it traverses the network between the switch and the controller.

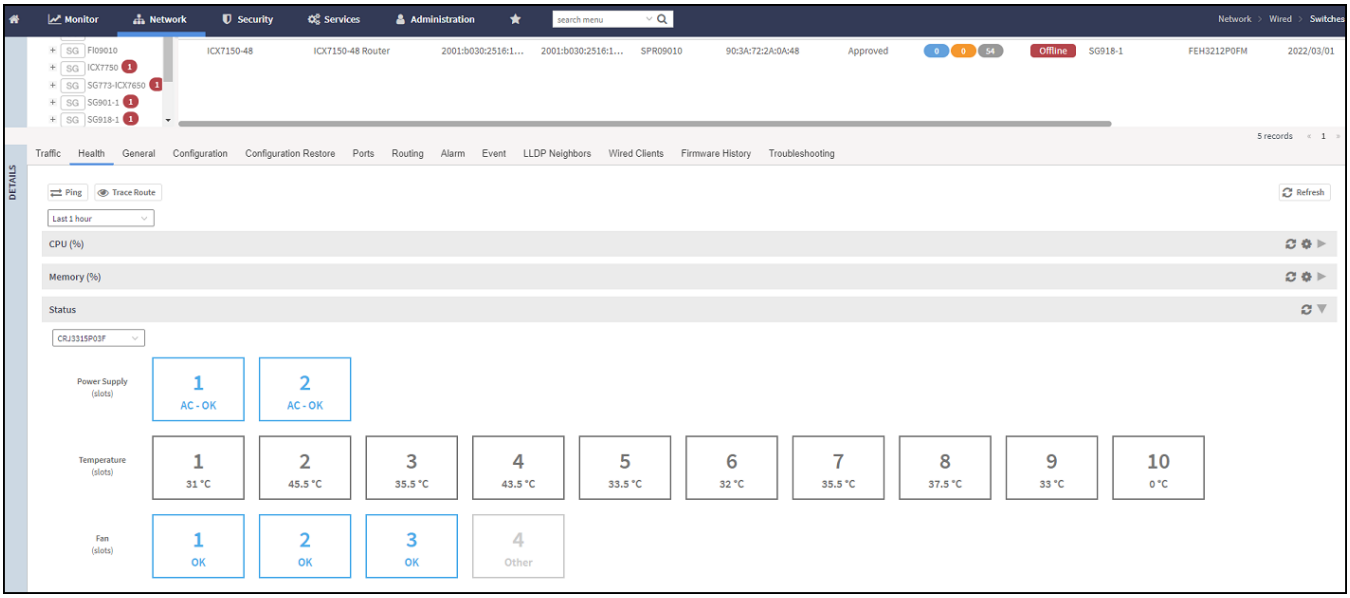
   FIGURE 166 Tracing the packet route through the network



7. From the drop-down menu, select the duration for which you want to view the switch health.

   As shown in the following example, information on switch health is displayed on the **Health** Tab, based on your selections.

   FIGURE 167 Health Tab



   The following information is displayed based on the duration selected:

   - **CPU (%)**: The CPU usage of the switch, including the minimum, maximum, average, and current CPU usage trends of the switch.
   - **Memory (%)**: The memory usage of the switch, including the minimum, maximum, average, and current memory usage trends of the switch.
   - **Status**: The health status of the power supply, temperature, and the fans for up to four switch modules are displayed. OK indicates the parameter and components are in good health.

   You can click  to modify the display settings. You can view the trend as a graph or a table. You can also modify the display to reflect the switch name, MAC address, or IP address.

Viewing Alarms

Syslog messages from the switch are sent to the controller to periodically communicate switch health and status. It also brings your attention to issues that may need resolution at the switch level. You can view these details from the **Alarms** tab for individual switches, stacks and switch groups.

Syslog messages from the switch are categorized as **Major** and **Critical**, and are displayed as **events** in the controller. From these events, the following messages are displayed as **alarms** in the controller interface:

- Power Supply failure
- Fan failure
- Module Insertion or removal
- Temperature above the threshold warning
- Stack member unit failure
- PoE power allocation failure

- DHCP offer dropped message
- Port put into error disable state

The remaining syslog messages which are categorized by other severity levels are listed in the `switchevent.log` file available in **Diagnostics** > **Application Logs**.

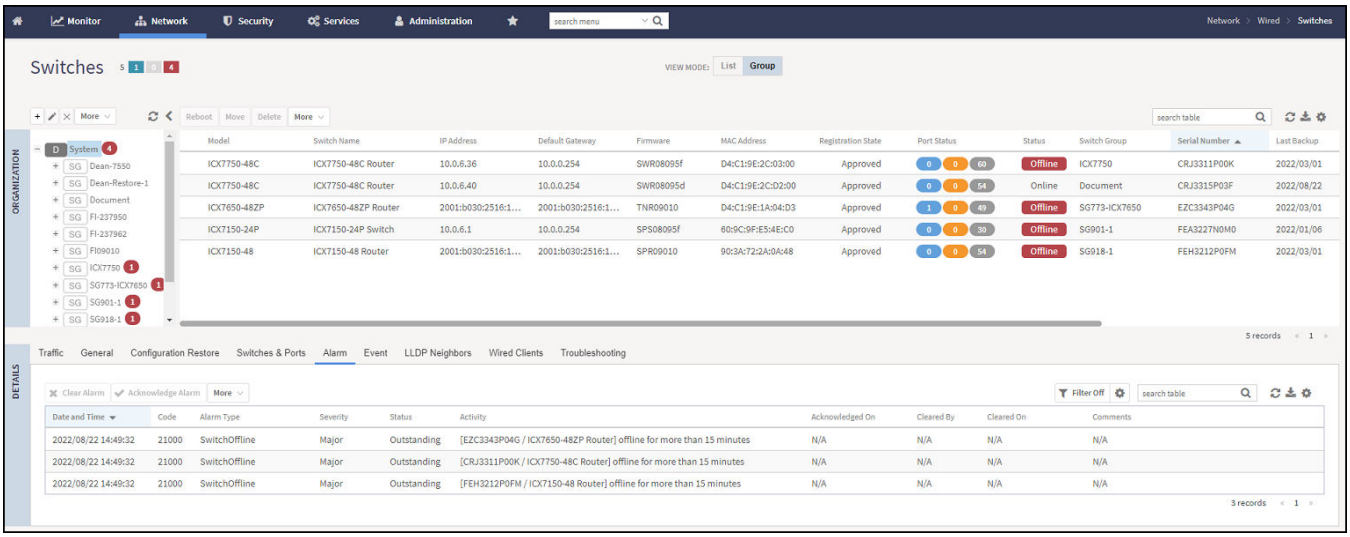
The alarms generate for the switch also reflect in the **Monitor** > **Events and Alarms** > **Events** page.

1. From the main menu, go to **Network** > **Wired** > **Switches.**

   The **Switches** page appears.

2. Select the switch or group. Then select the **Alarms** tab.

FIGURE 168 Switches Alarms Tab



The following information is displayed in the **Alarms** tab:

- Date and Time: Displays the date and time when the alarm was triggered
- Code: Displays the alarm code (see the Alarm and Reference Guide for your controller platform for more information).
- Alarm Type: Displays the type of alarm event that occurred (for example, switch reset to factory settings).
- Severity: Displays the severity level assigned to the events such as Critical, Major, Minor and Warning.
- Status: Indicates whether the alarm has already been cleared or still outstanding.
- Activity: Displays additional details about the alarm, such as how long was the switch offline for
- Acknowledged On: Displays the date and time when the administrator acknowledge the alarm
- Cleared By: Displays information about who cleared the alarm
- Cleared On: Displays the date and time when the alarm was cleared
- Comments: Displays administrator notes recorded during alarm management

Click to export the alarms details to a CSV file. Check the default download folder of your web browser and look for a file named *alarms.csv* and view it using a spreadsheet application

Clearing an alarm removes the alarm from the list but keeps it on the controller's database. Select the alarm from the list and click **Clear Alarm**. The **Clear Alarm** page appears. Type your comments and select **Apply**.

Acknowledging an alarm lets other administrators know that you have examined the alarm. Click **Acknowledge Alarm** to acknowledge an alarm. After you acknowledge an alarm, it will remain on the list of alarms and will show the date and time that you acknowledged it.

You can also view alarms by their severity, status, date and time stamp. Click to apply filters.

Viewing Events

Events are triggered by an occurrence or the detection of certain conditions in the switch. For example, when the temperature of the device reaches warning levels, or when the fan speed changes, an event is triggered. You can view these details from the **Events** tab for individual switches, stacks and switch groups.

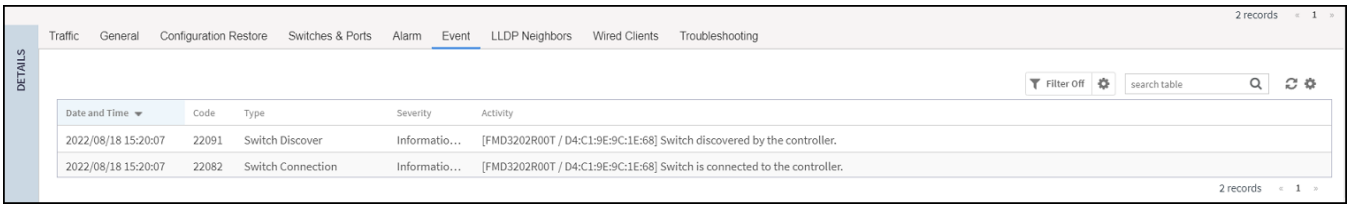
The alarms generate for the switch also reflect in the **Monitor** > **Events and Alarms** > **Events** page.

1. From the main menun, go to **Network** > **Wired** > **Switches.**

   The **Switches** page appears.

2. Select the switch or group. Then select the **Events** tab.

   FIGURE 169 Events Tab



   The following information is displayed in the **Events** tab:

   - Date and Time: Displays the date and time when the event occurred
   - Code: Displays the event code (see the Alarm and Event Reference Guide for your controller platform more information)
   - Type: Displays the type of event that occurred (for example, Switch configuration updated)
   - Severity: Displays the severity level assigned to the events such as Critical, Debug, Informational, Warning, Major etc .
   - Activity: Displays additional details about the event

   Click  to export the events details to a CSV file. Check the default download folder of your web browser and look for a file named *events.csv* and view it using a spreadsheet application

   You can also view alarms by their severity, date and time. Click  to apply filters.

Viewing LLDP Neighbor Information

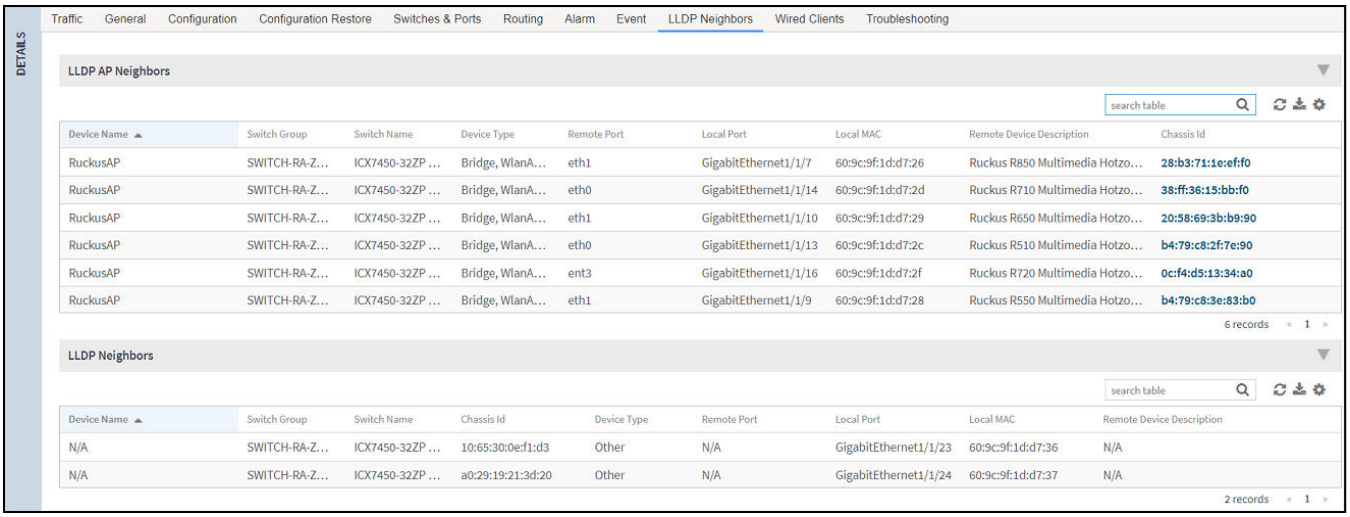
You can view information about the LLDP neighbors such as printers, VOIP devices, or other user equipment connected to the switch, in addition to the LLDP AP neighbors connected to the switch. Link layer discovery protocol or LLDP is used to discover and identify the clients.

1. From the main menu, go to **Network** > **Wired** > **Switches.**

   The **Switches** page appears.

2. Select the switch or group. Then select the **LLDP Neighbors** tab.

FIGURE 170 LLDP Neighbors Connected to the Switch



The following information is displayed in the **LLDP Neighbors** tab for devices to the switch:

- Device Name: displays the name of the LLDP neighbor or AP neighbor connected to the switch
- Remote MAC: displays the remote MAC address of the device
- Device Type: displays the name of the device type (for example, Router)
- Local Port: displays the local port the device is connected to
- Local MAC: displays the local MAC address of the device
- Remote Port: displays the remote port to which the device is connected
- Remote Device: displays the name of the remote device

Viewing Traffic Trends in the Switch

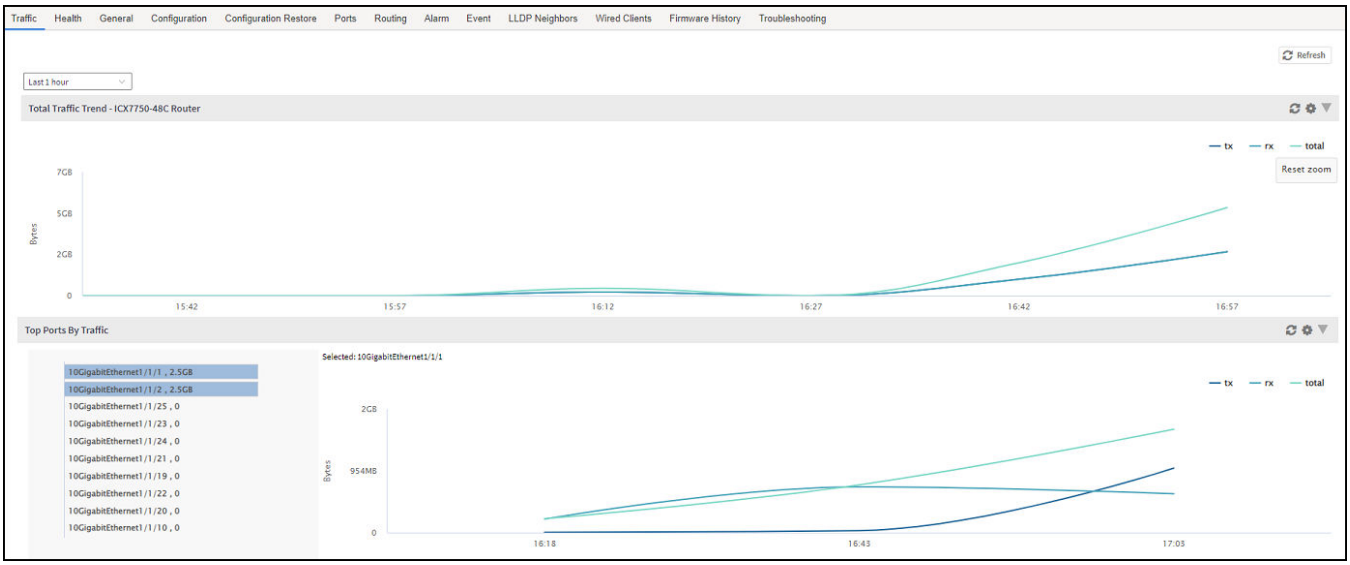
You can view statistical information about how traffic is handled at the switch level. These details are available for individual switches, stacks and switch groups.

1. From the main menu, go to **Network** > **Wired** > **Switches.**

   The **Switches** page appears.

2. Select the switch or group. Then select the **Traffic** tab.

FIGURE 171 Traffic Trend for a Switch



The following information is displayed in the **Traffic** tab. You can view the traffic trend for the last 1 hour or 24 hours:

- Total Traffic Trend: Provides a graphical representation of the network traffic usage over a period of time in the switch or switch group. It also indicates the amount of traffic or data transmitted (tx) and received (rx) by the group in MB, at a certain time and date.
- Top Switch by Traffic: Provides a graphical representation of the top switches that handled maximum network traffic over a period of time, in the switch group. You can click on the switch address to view the traffic trend. This trend is only available for switch groups.
- Top Ports by Traffic: Provides a graphical representation of the top ports that handled maximum network traffic over a period of time, for a switch. You can click on the port address to view the traffic trend. This trend is only available for individual switches.
- Total Multicast Traffic Trend: Provides a graphical representation of the multicast traffic usage over a period of time in the switch or switch group. It also indicates the total number of incoming multicast data packets (multicastIn) and total number of outgoing multicast packets (multicastOut) by the group in MB, at a certain time and date.
- Total Unicast Traffic Trend: Provides a graphical representation of the unicast traffic usage over a period of time in the switch or switch group. It also indicates the total number of incoming unicast data packet (unicastIn) and total number of outgoing unicast packet (unicastOut) by the group in MB, at a certain time and date.
- Total Broadcast Traffic Trend: Provides a graphical representation of the broadcast traffic usage over a period of time in the switch or switch group. it also indicates the total number of incoming broadcast data packets (broadcastIn) and total number of outgoing broadcast packets (broadcastOut) by the group in MB, at a certain time and date.
- Total Port Errors: Provides a graphical representation of the port errors over a period of time in the switch or switch group. It also indicates the total number of inbound packets that contained errors (inErr) and total number of outbound packets that could not be transmitted because of errors (outErr) by the group in MB, at a certain time and date.

Viewing Firmware History of the Switch

You can view the detailed status and result of the firmware update to a switch. You can also view a history of firmware upgrades that were previously carried out on the switch.

You must have upgraded the firmware of the switch as described in Scheduling a Firmware Upgrade for Selected Switches on page 252

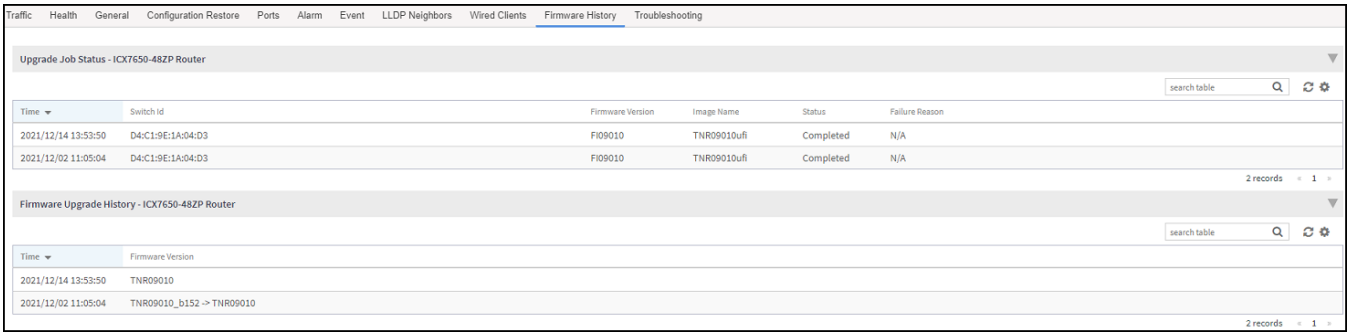
1. From the main menu, go to **Network** > **Wired** > **Switches.**

   The **Switches** page appears.

2. Select the switch or group. Then select the **Firmware History** tab.

   The **Firmware History** tab is displayed.

   FIGURE 172 Viewing Firmware History



   You can verify the status of the upgrade from the **Upgrade Job Status** section which displays the time, switch ID, firmware version, image name, status and failure reasons (if any) for the upgrade.

   The **Firmware Upgrade History** section displays the time of the pervious upgrade operations, and firmware versions to which the upgrade was done.

Configuring the Group Firmware Settings

The Group Firmware Settings allows the user to select default firmware for the switch group. The newly joined switch is upgraded to the selected firmware in the switch group.

NOTE
The default firmware selection at group level does not trigger upgrade for the existing switches in the switch group, it only triggers upgrade for newly joined switch(es)

Complete the following steps to perform the firmware upgrade of newly added switch in the switch group to the default firmware version.

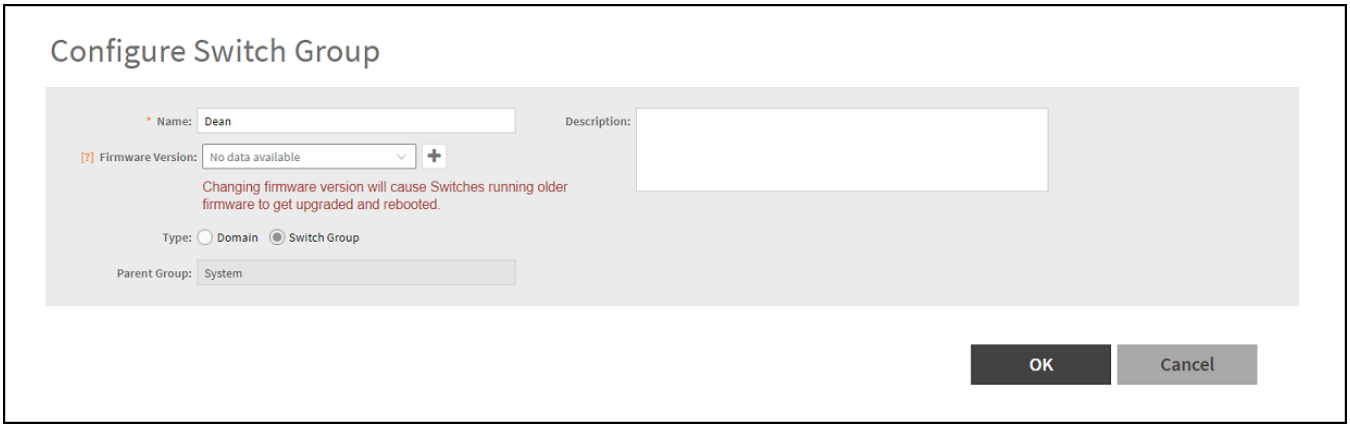
1. From the main menu, go to **Network** > **Wired** > **Switches.**

   The **Switches** page appears.

2. From the **Switches** page, select the switch group that you want to configure, and click .

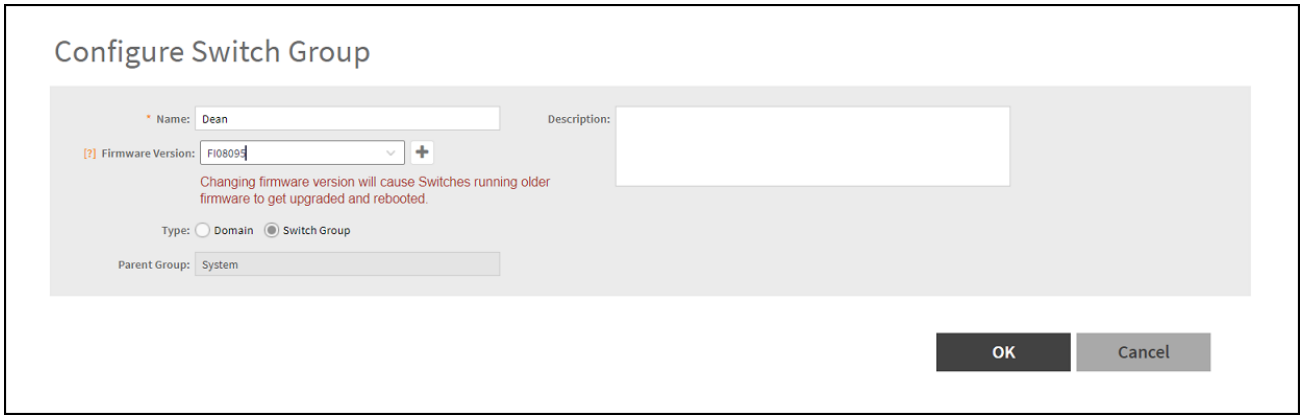
   The **Configure Group** page appears.

   FIGURE 173 Configuring the Switch with Default Version



3. In the **Configure Group** page, configure the following.
   a) Name: Type the name of the switch group that you want to create.
   b) Description: Enter a brief description for the switch group
   c) Firmware version: Select firmware version from the list or retain the default firmware version.

      FIGURE 174 Configuring the switch with Firmware version



      NOTE
      The group firmware settings requires switches to be running SmartZone 5.2.1 or later.

   d) Parent Group: Displays the parent group under which the switch group resides
4. Click **OK**.

Accessing the switch CLI through SmartZone (Remote CLI)

SmazrtZone 5.2.1 introduces this essential feature that allows you to directly access the Switch CLI prompt from the controller web interface. The Remote CLI allows you to establish a secured connection between controller and switch that can span over Internet, and eliminate the need to open VPN connection to switch's network when trying to access CLI through SSH or Telnet.

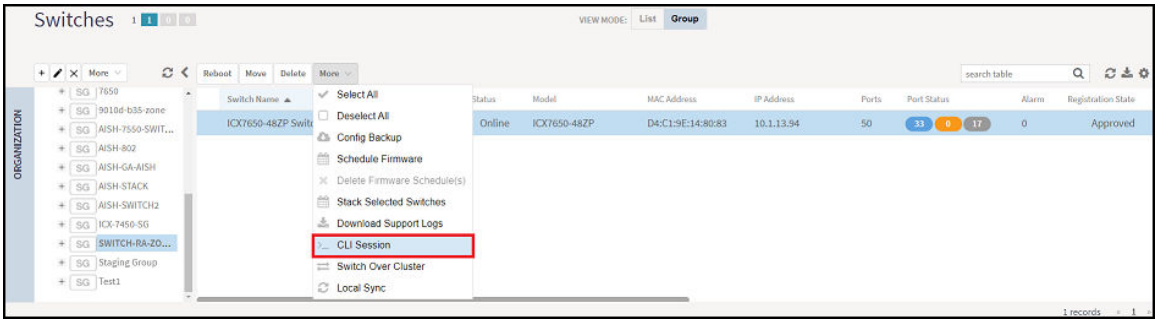
NOTE
This feature can be accessed by only the System Super-Admin in 5.2.1 release.

The administrator must complete the following steps to access a CLI session.

1. From the main menu, go to **Network** > **Wired** > **Switches.**

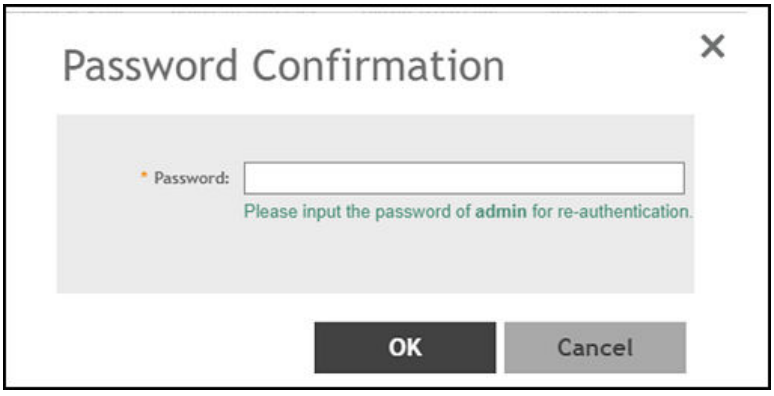
   The **Switches** page is displayed.
2. From the **Switches** page, select a switch.
3. Click **More**, and select **CLI session**.

FIGURE 175 Selecting CLI Session



The **Password Confirmation** dialog box is displayed.

FIGURE 176 Logging into the CLI Session



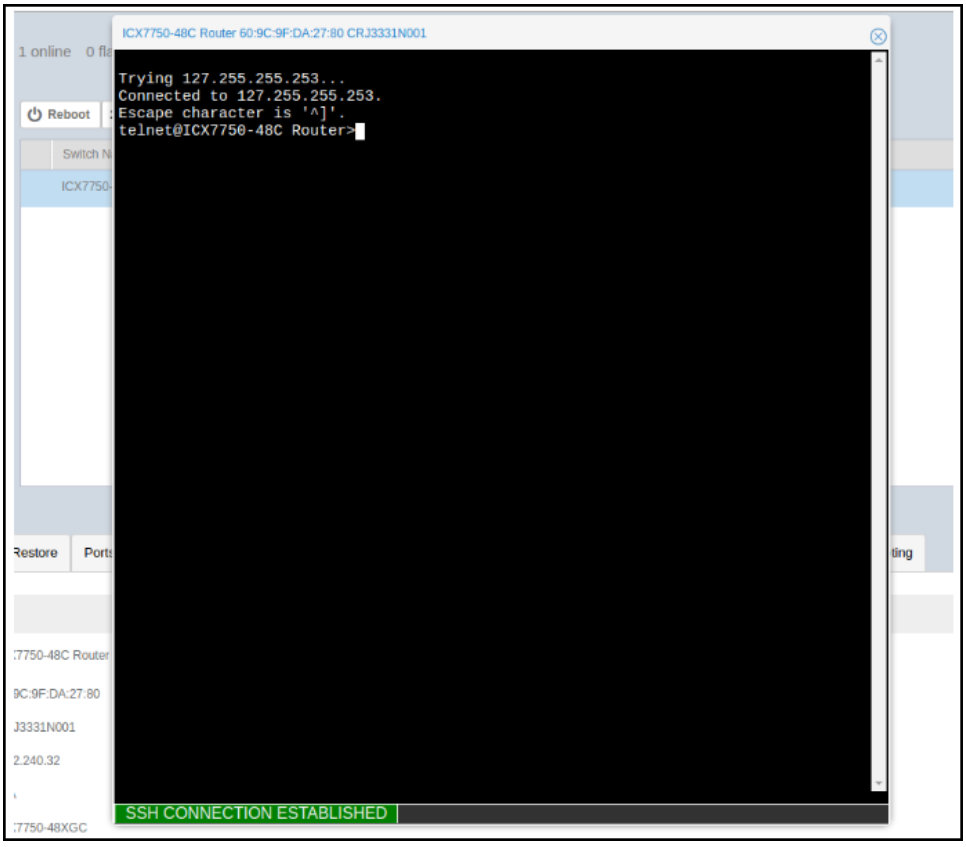
4. Enter the administrator password.

   After login, it takes approximately five seconds to set up a secure session within the secure tunnel established between switch and controller to access switch.

   A CLI Window is displayed.

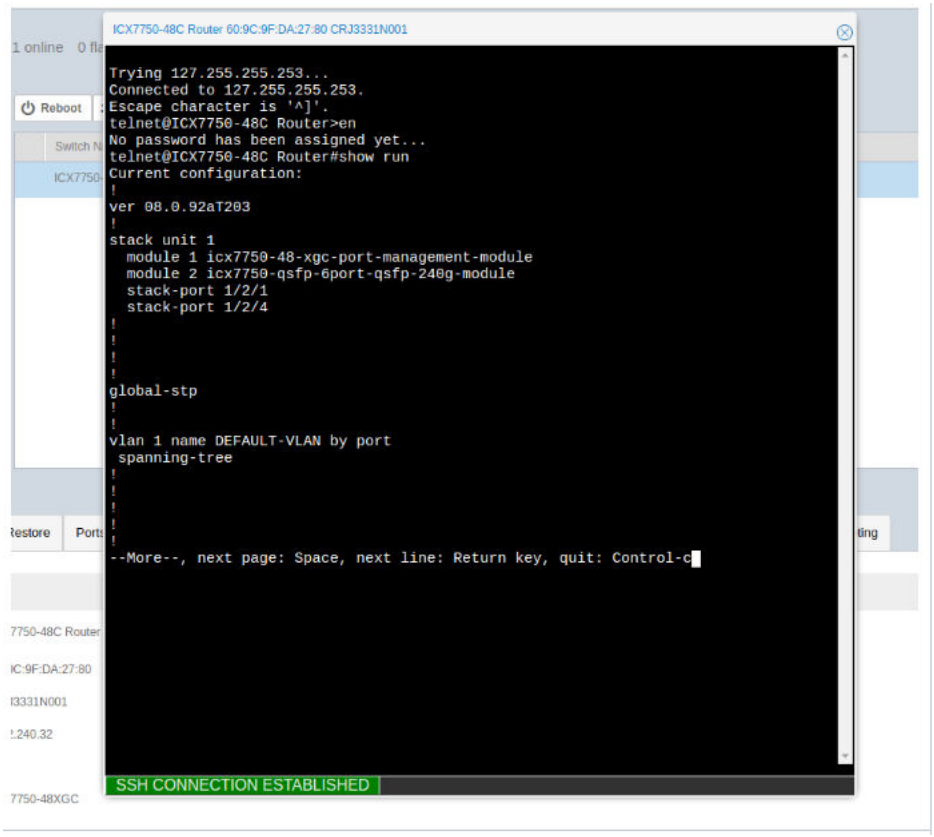
   NOTE
   You do not need to enable telnet server on ICX switches to use Remote CLI.
   However, if telnet authentication is enabled on the switch, you will be prompted to enter the credentials when opening CLI session via SmartZone. The credentials depend on the type of authentication defined on the switch (local user, RADIUS etc.).

FIGURE 177 Accessing Switch Through the CLI Sesion



5. Press the **Spacebar** to skip to the next page, press **Enter** to display the next line, or press **Ctrl + C** to exit.

   FIGURE 178 Example of Paging Display



6. Enter the **exit** command to quit the CLI session.

Viewing PoE Utilization and Health Status of the Switch

Prior to SmartZone 5.2.1, the controller provided the power supply status and PoE utilization for a stack unit. Beginning with SmartZone 5.2.1, the controller provides a view of the PoE utilization in watts, and health status such as the power supply, temperature and fan status of each member in the stack unit.

Complete the following steps to view the health status of each member in the stack unit.

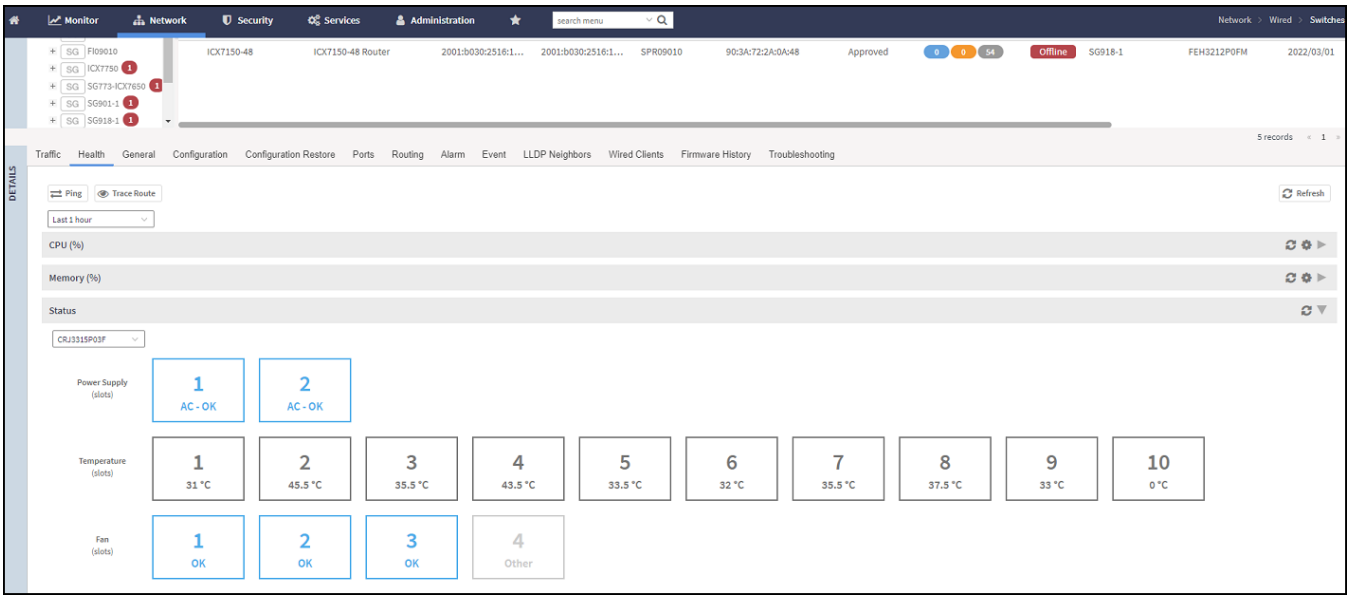
1. From the main menu, go to **Network** > **Wired** > **Switches.**

   The **Switches** page is displayed.

2. Select a stack switch.

3. Click the **Health** tab to view the health status such as the power supply status, temperature, and fan status, of the stack switch.

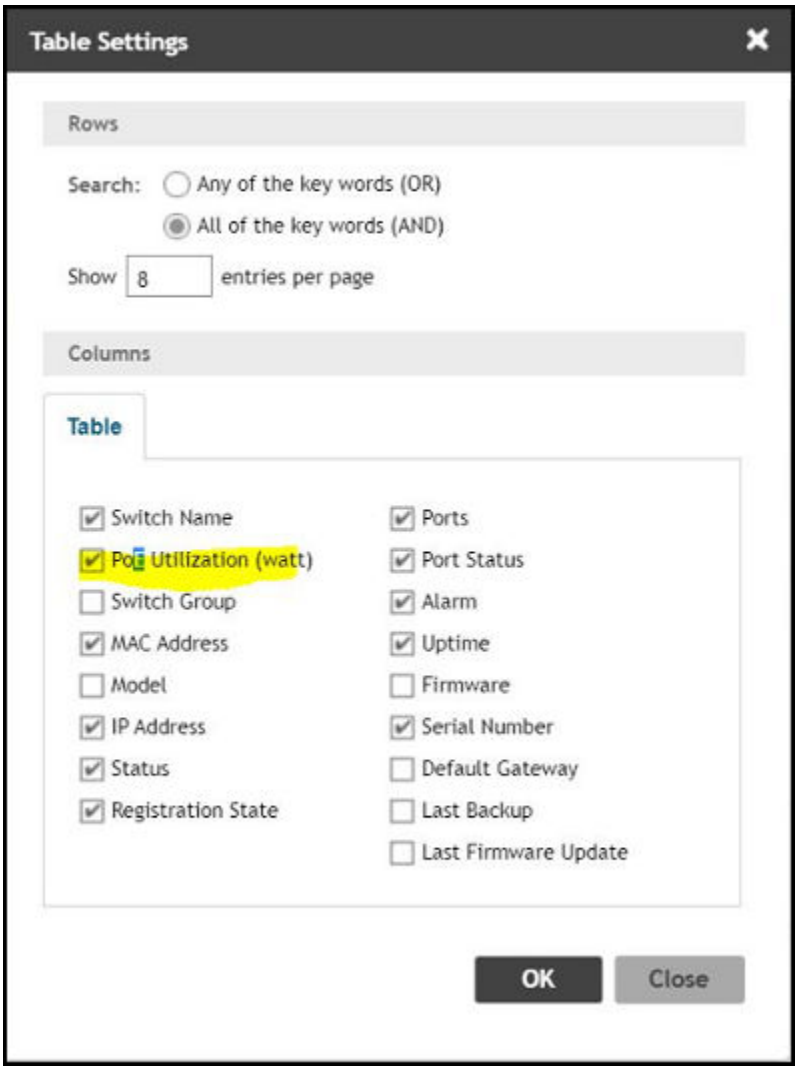
FIGURE 179 Viewing the Health Status of Stack Switch



4. To enable the PoE Utilization, click ⚙ .

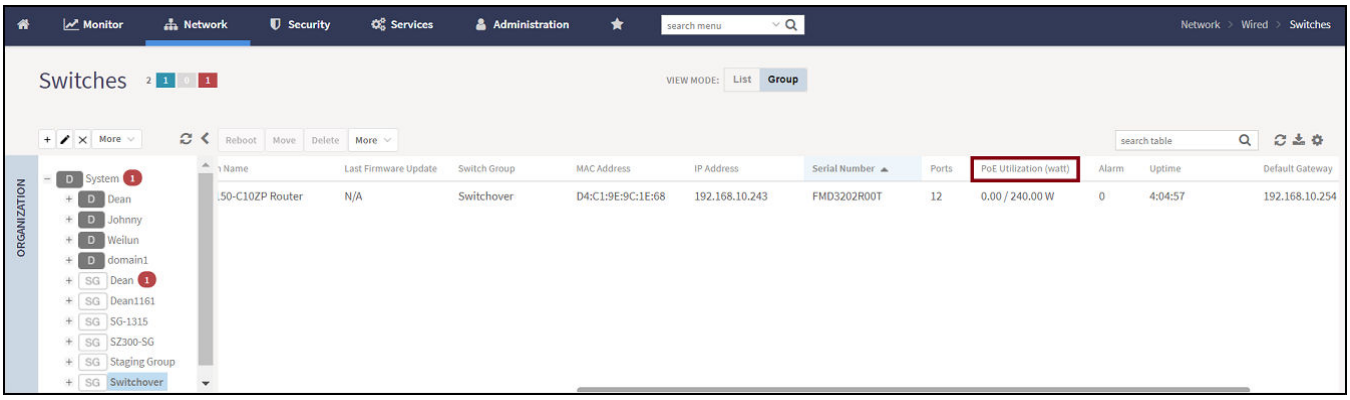
   The **Table Settings** page is displayed.

   FIGURE 180 Enabling the PoE Utilization



5. Select a **Stack Swith**, to view the details in the **PoE Utilization (watt)** field.

FIGURE 181 Viewing the PoE Utilization Field



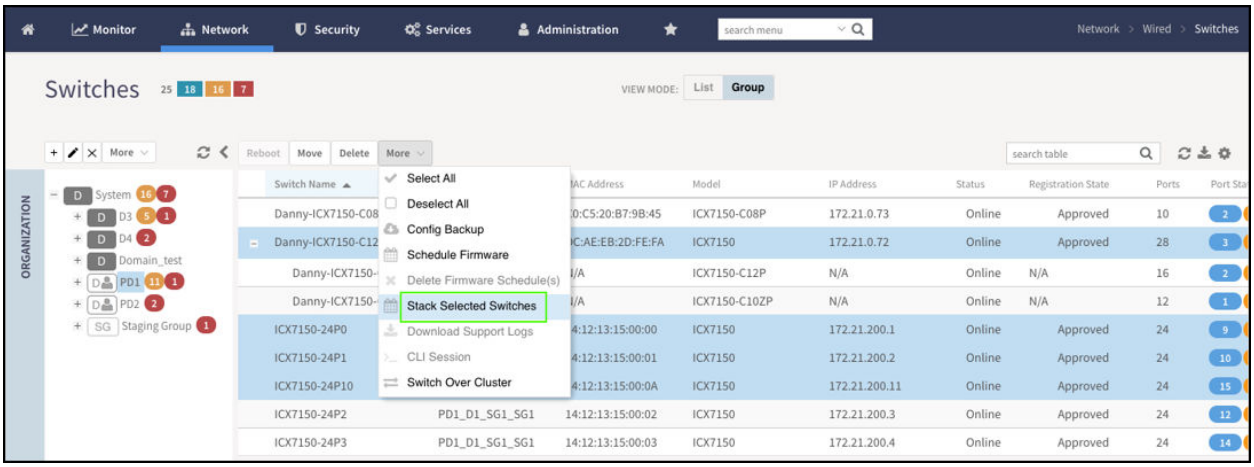
Ability to Convert Standalone Switch to Stack

This feature allows the Standalone switch to convert into a stack by adding member switches.

Complete the following steps to convert standalone switch into stack.

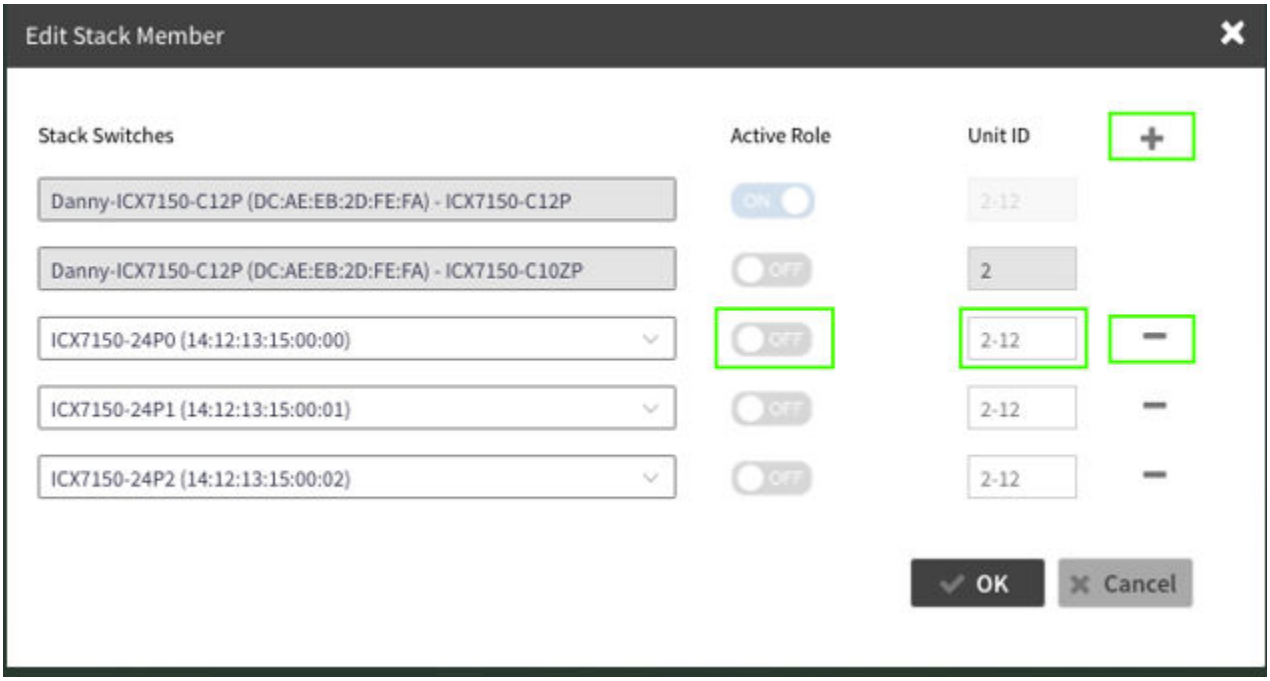
1. From the controller web interface, go to **Network** > **Switches**

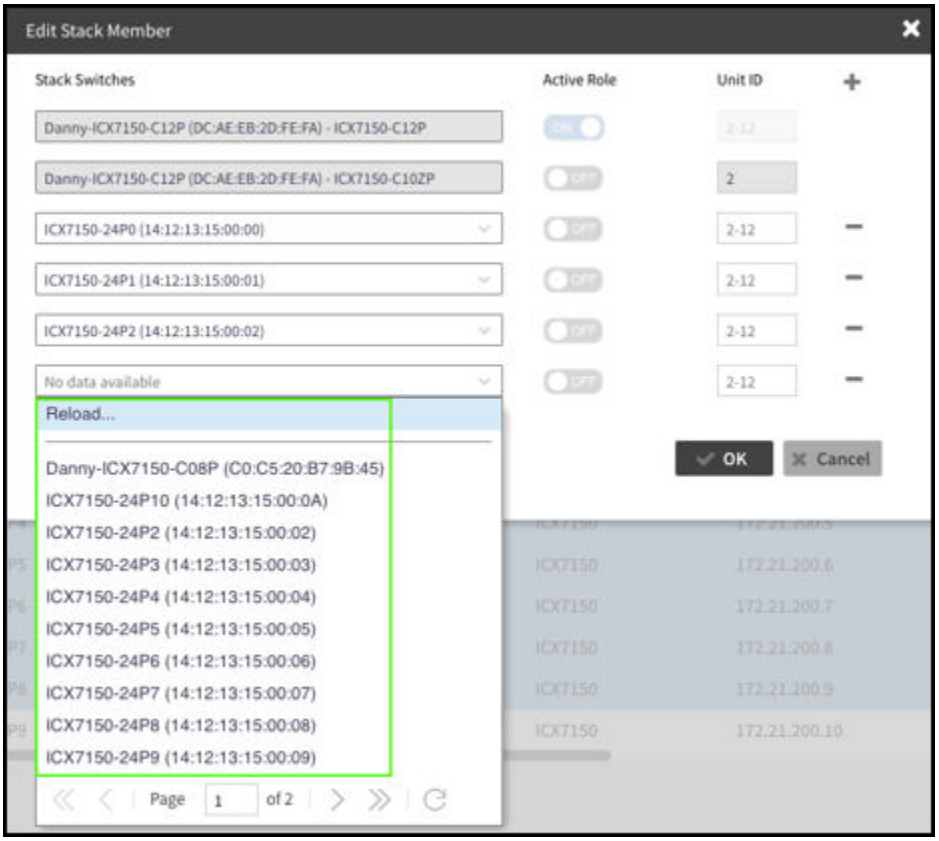
The **Switches** page is displayed.



2. Select stack and standalone switch. Click **More** > **Stack Selected Switches** to add stanalone switch to the stack. The **Create Stack** page is displayed, turn **Active Role** on.

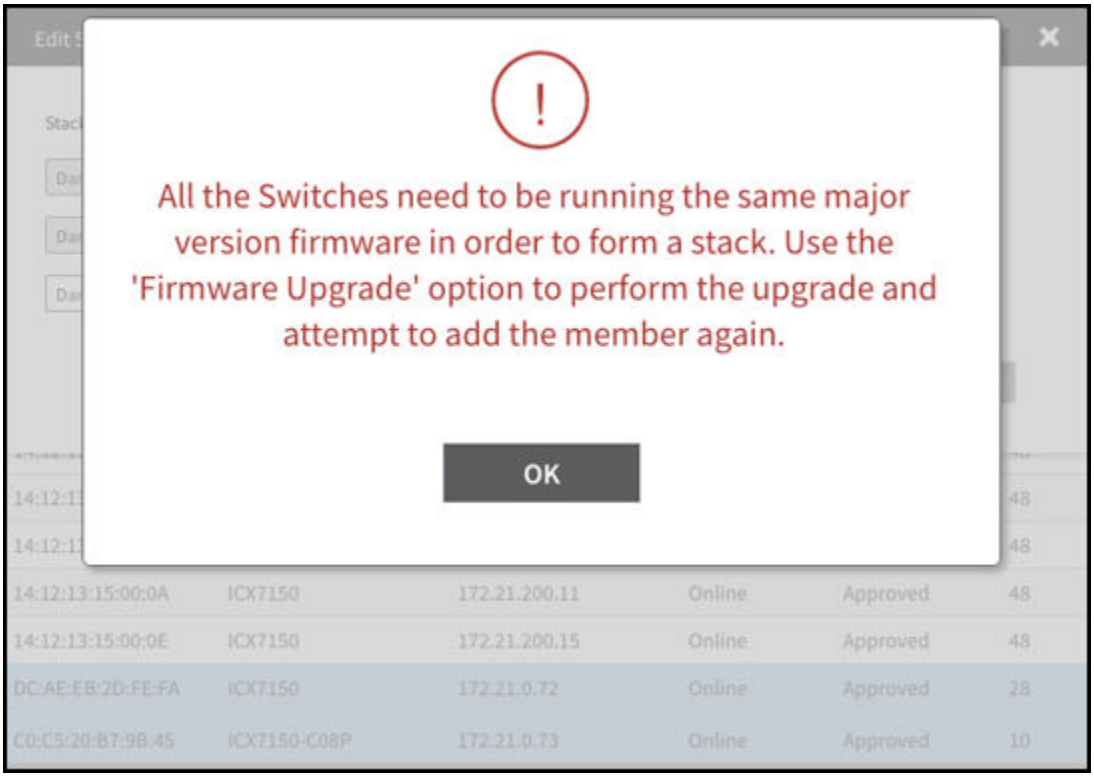
3. In the **Edit Stack Member** page, click **+** or **-** to add or remove the stack entry. A RUCKUS stack contains from two to 12 units configured in a ring or linear topology. The units in a stack are from the same model family; that is, a stack can be an ICX 7150 stack, an ICX 7250 stack, an ICX 7450 stack, an ICX 7650 stack, or an ICX 7850 stack.





4. Click **OK**.

NOTE
If stack and switch are running different version of an image, an error message is displayed.

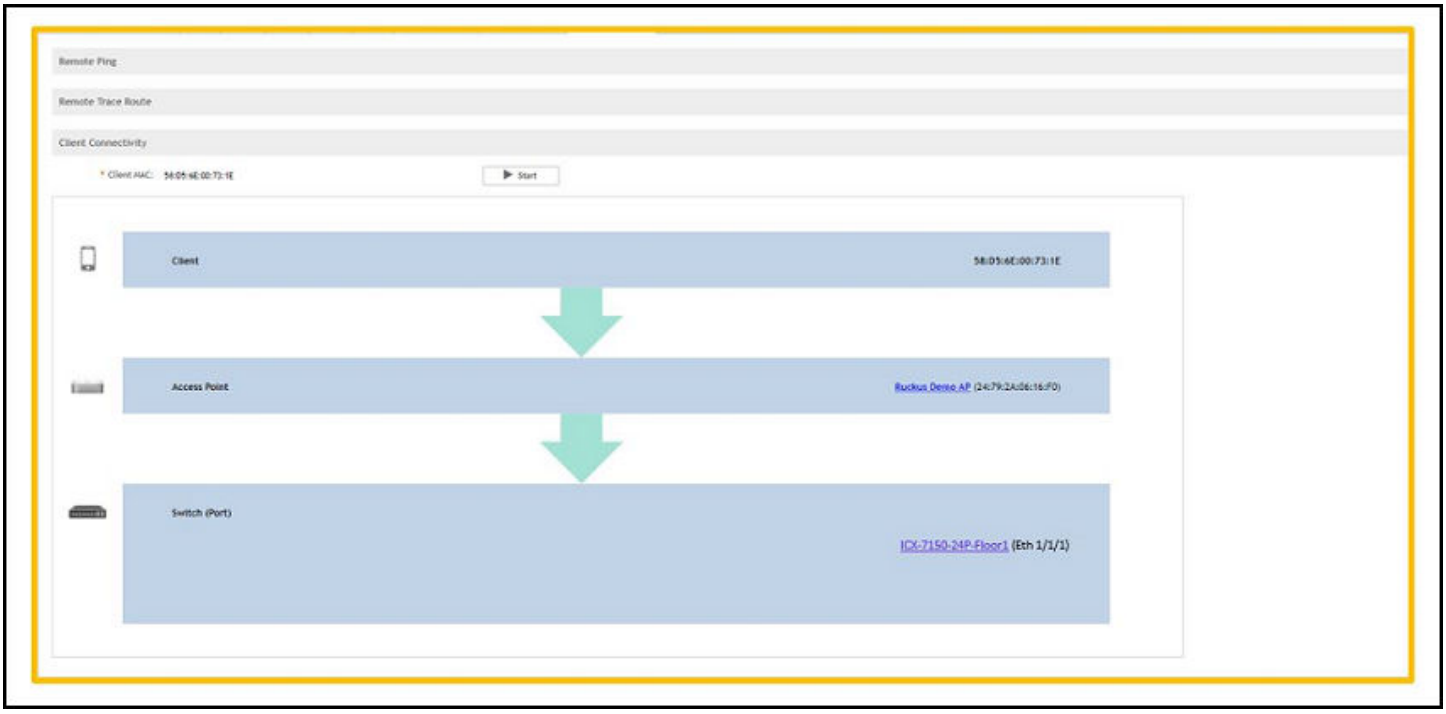


Troubleshooting Switch Issues

You can troubleshoot issues related to wired and wireless clients connected to the switch at the system level from the **Troubleshooting** tab. You can use Remote operations, Client Connectivity and Custom Events to troubleshoot issues with switches or switch groups.

To troubleshoot issues with an AP client, use the MAC address of the client on the **Troubleshooting** tab of a switch or switch group. Once you enter the MAC address of the client, SmartZone displays how the client is connected to the network, including the AP, the switch, and the switch port on which the client MAC is learned. As an example, if a printer is connected to an AP, which in turn is connected to a switch that is managed by a SmartZone controller, you can troubleshoot any connectivity issues between the devices from the **Troubleshooting** tab by providing the MAC address of the printer.

FIGURE 182 Client MAC Search



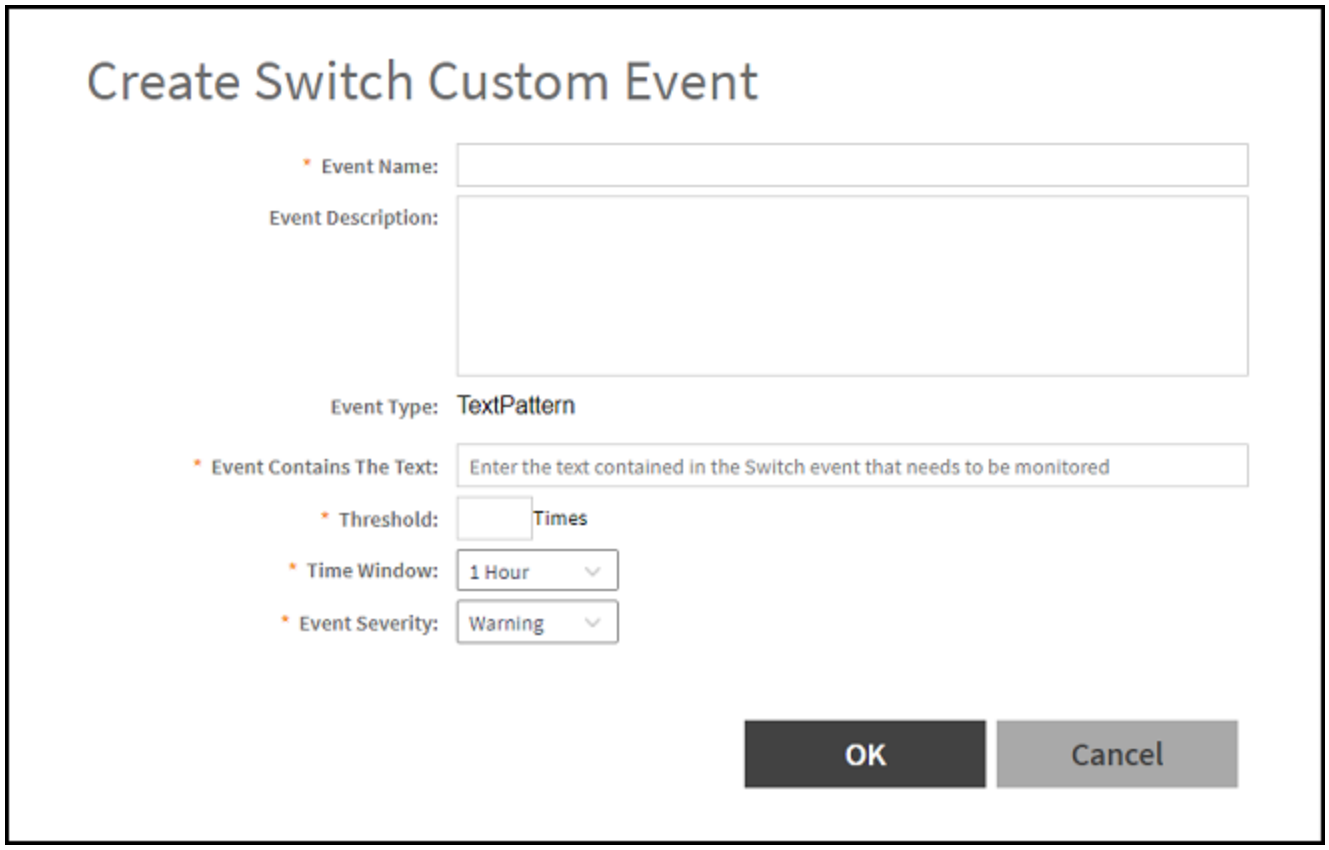
Troubleshooting Using Custom Events

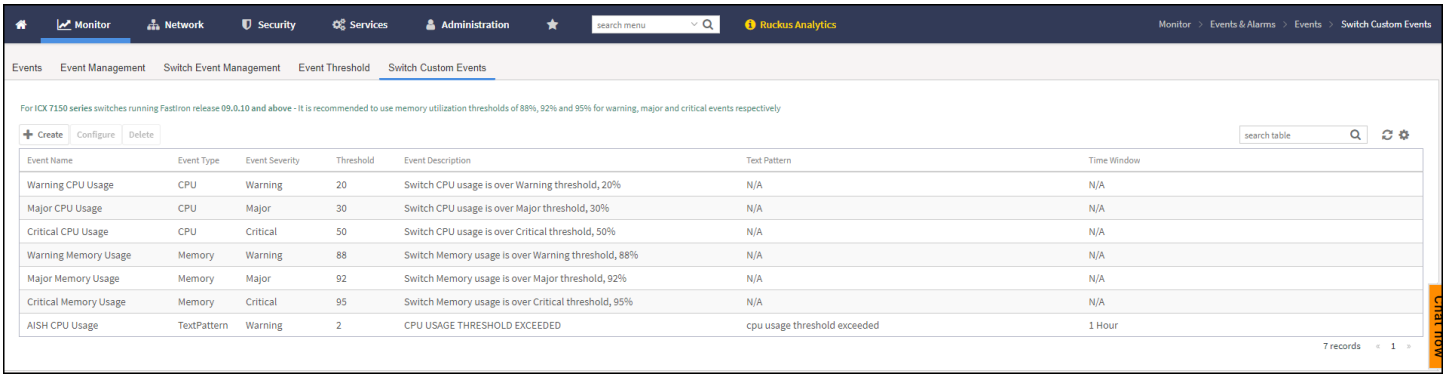
You can create custom events to define failure scenario and use them to generate troubleshoot switch issues.

For example, you can create a "system is unusable" event with the following settings. Based on this event definition and configuration, if any switch sends this message thrice in one hour, the controller triggers a Custom Event. You can view the "system unavailable" event from the **Switch Custom Events** page. For more information on custom events, see Creating Custom Events for ICX Switches on page 98

FIGURE 183 Troubleshooting switch issues through custom events

FIGURE 184 Creating Switch Custom Event





NOTE
It is quite common that entry level switches like ICX 7150 use up 70-80% of the available memory. You can modify the thresholds for memory usage custom events to a higher limit in such cases.

VIDEO
Switch Custom Troubleshooting Demo Verify client to WLAN to switch assignment (Switch Client Troubleshooting).
Click to play video in full screen mode.

Troubleshooting Using Remote Operations

You can use the **Remote Ping** and **Remote Trace Route** options to identify issues with individual switches.

Follow these steps to troubleshoot switch issues using remote ping and traceroute.

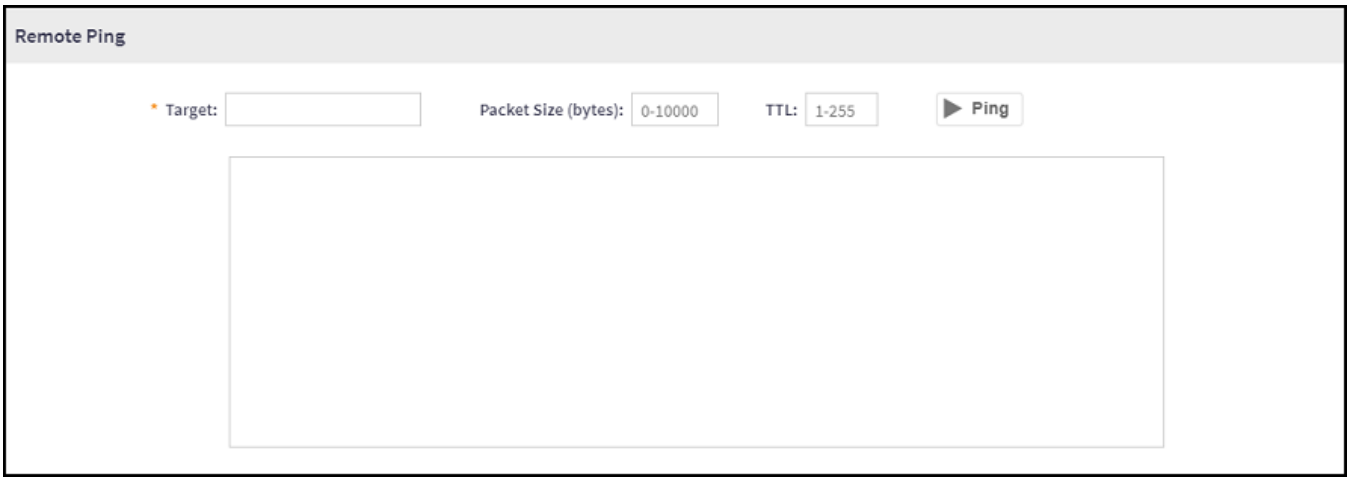
1. From the main menu, go to **Network** > **Wired** > **Switches.**

   The **Switches** page is displayed.
2. Select a switch.
3. Click the **Troubleshooting** tab.
4. Click **Remote Ping**.

   The **Ping** page is displayed.
5. On the **Ping** page, enter the IP address of the destination (target) you are checking, along with the packet size and the TTL (Time to Live) value after which the packet is discarded from the network.
6. Click **Ping**.

   The controller pings the switch at the destination IP address provided. As shown in the following example, the results displayed include the number of data packets transmitted, received, and lost and the time required for the controller to ping the switch to establish communication.

   FIGURE 185 Pinging the switch



7. Click **Remote Trace Route**.

   The **Trace Route** page is displayed.
8. Enter the IP address of the destination being checked for connectivity and the TTL (Time to Live) value after which the packet is discarded from the network.

9. Click **Trace Route**.

   As shown in the following example, the **Trace Route** page displays the IP address of the hops the packet traverses through the network between the switch and the controller.

   FIGURE 186 Tracing the packet route through the network



10. Click **Blink LED** to enable blinking of port LEDs on switches.

11. The Blink LED can be applied to either a single switch, or to switch in the stack by selecting an option **All**, or selecting a particular unit-id from the list. Type the value in seconds. Click **Blink**.

    NOTE
    The value in seconds ranges from 15-120. By deafult, it is 15.

FIGURE 187 Applying Blink LED to Single Switch

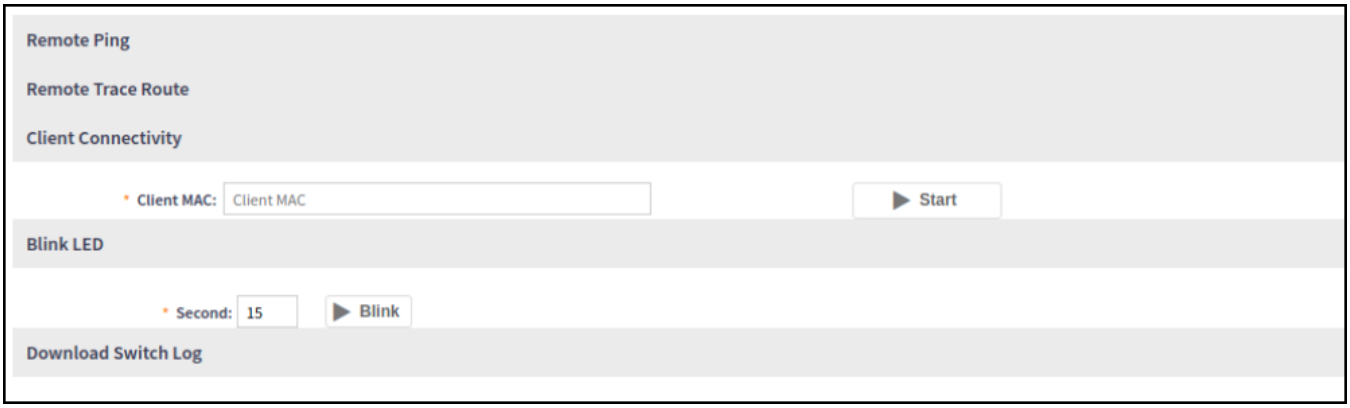
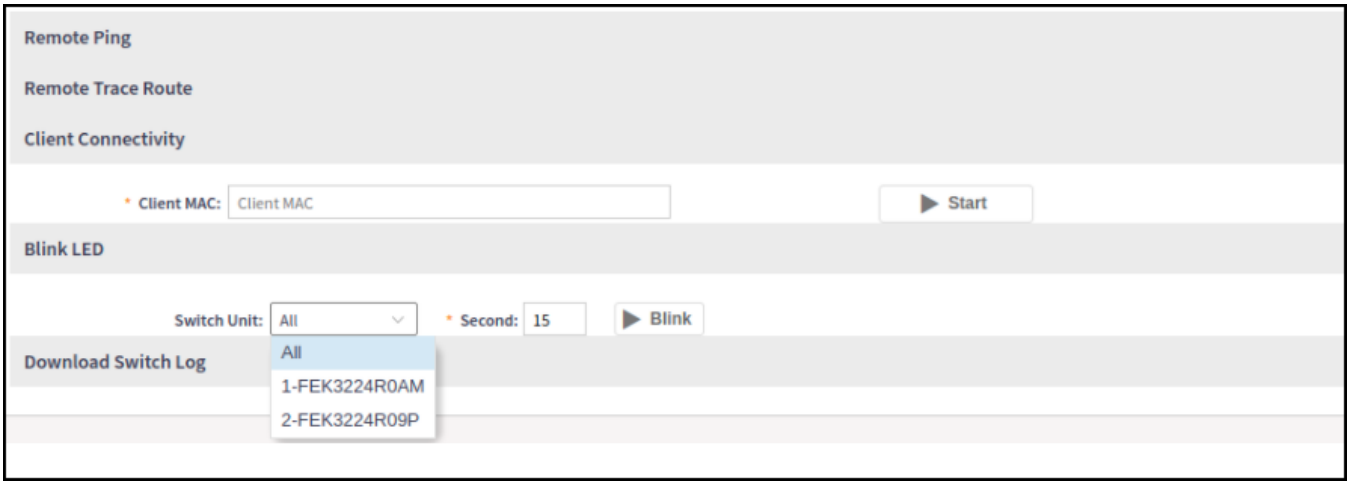


FIGURE 188 Applying Blink LED to Switch on Stack



Cable Testing on ICX Ports

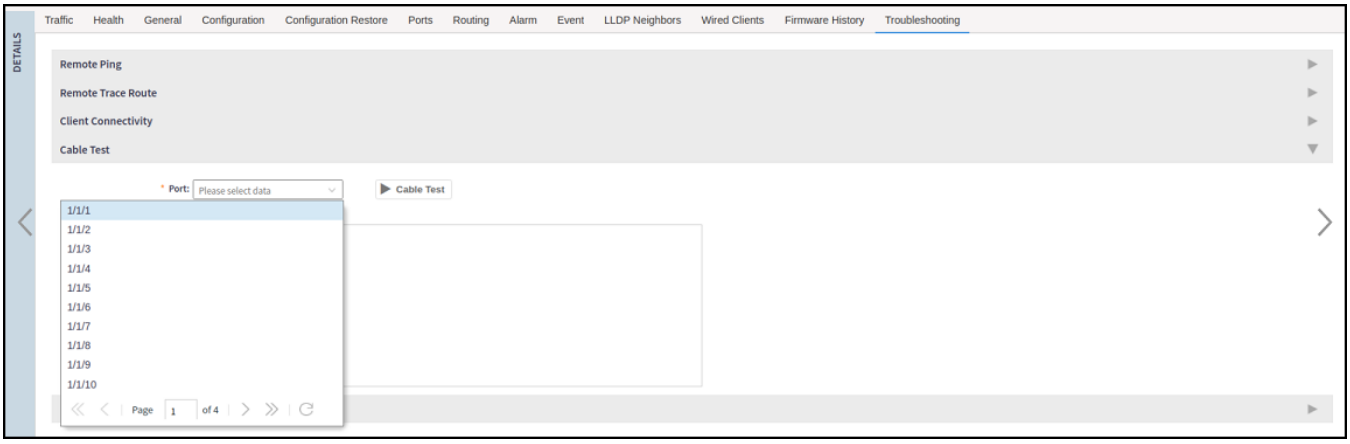
1. On the controller web interface, go to **Network** > **Wired** > **Switches**.

   The **Switches** page is displayed.

2. Select a switch.
3. Click the **Troubleshooting** tab on the lower pane.

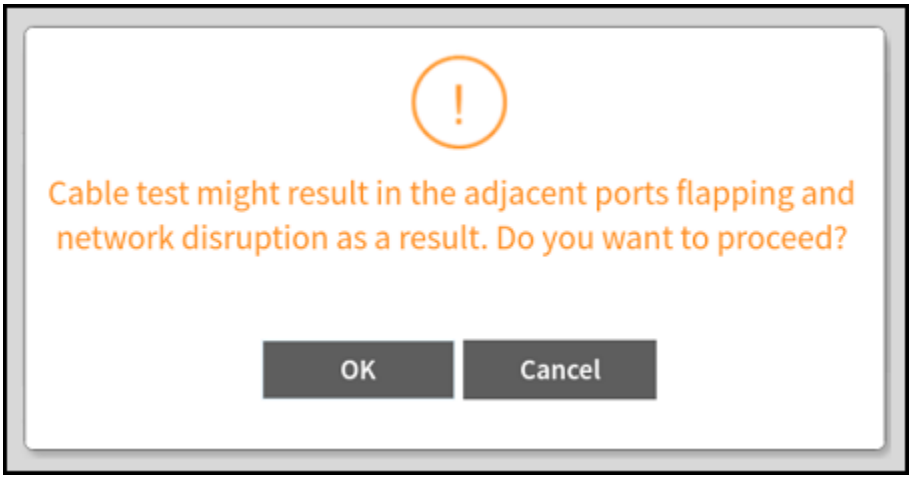
4. Expand the **Cable Test** field by clicking icon.

FIGURE 189 Clicking Troubleshooting Tab



5. Select a port from the **Port** list.

FIGURE 190 Warning Message for Confirmation



NOTE
To execute the cable test, port speed must be set to **Auto**.

Image

6. Click **Cable Test**.

FIGURE 191 Testing Network Connectivity

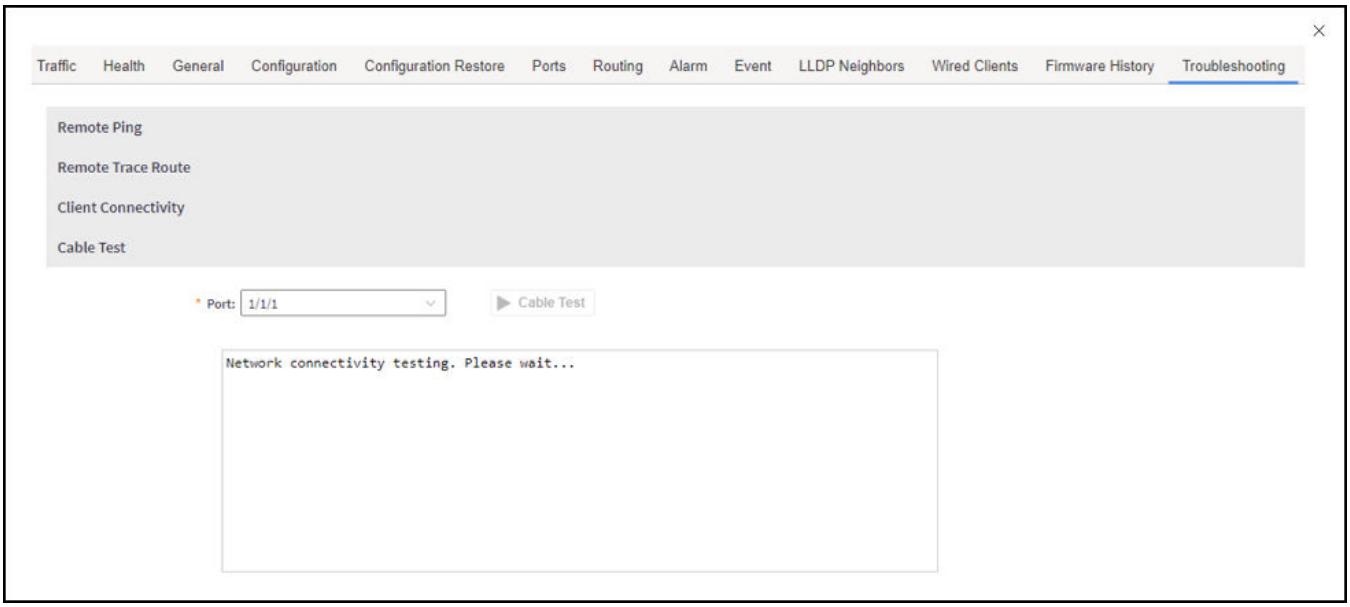
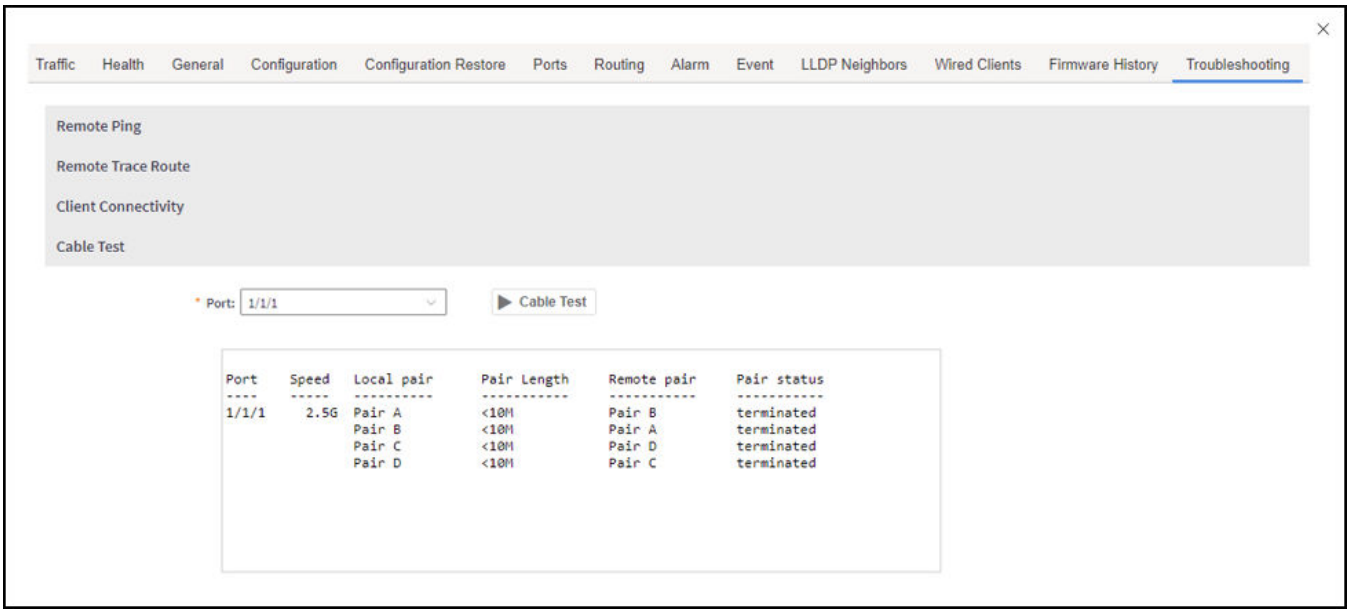


FIGURE 192 Viewing the Cable Test Report



7. If the selected port has the port speed set to **Fixed**, then an error message is displayed as below.

FIGURE 193 Displaying Error Message



Viewing Switches on the Dashboard

The wired dashboard displays detailed information about the health of the switch and displays charts illustrating traffic trends.

1. From the SmartZone interface, click **Monitor** > **Dashboard.**

   The **Dashboard** page is displayed.

2. Click **Wired**.

   The **Wired** page is displayed.

3. Click the Gear icon on the **Health** dashboard.

   The **Settings-Health Dashboard** page is displayed.

4. Click the **Display** tab.

5. From the **View Mode** , select either **Topology** or **Port** view to be displayed on the dashboard.

FIGURE 194 Showing Wired Devices Using Port View Mode

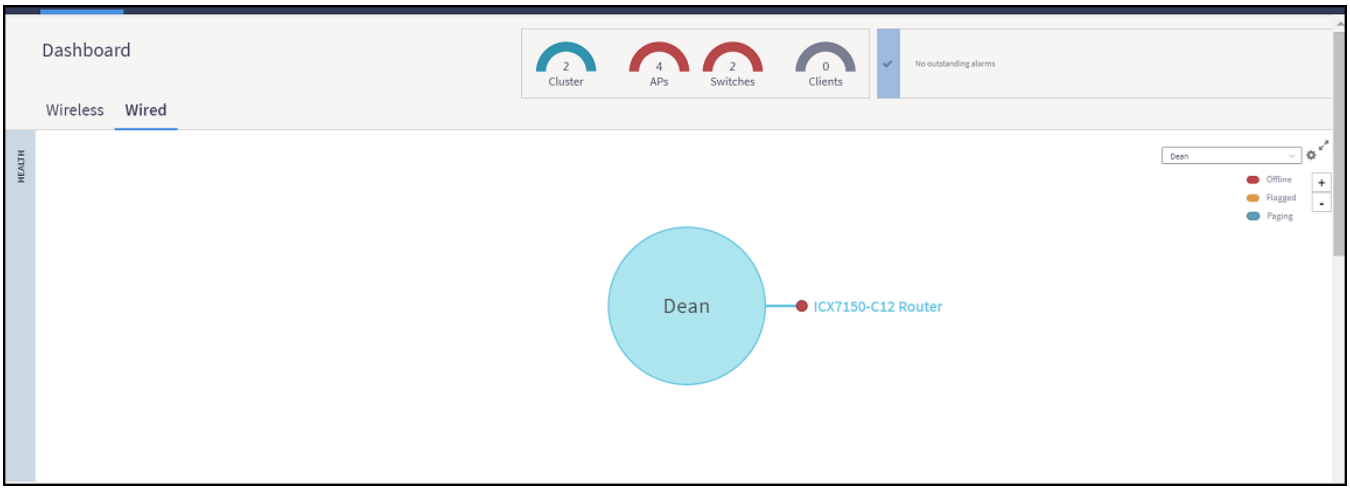
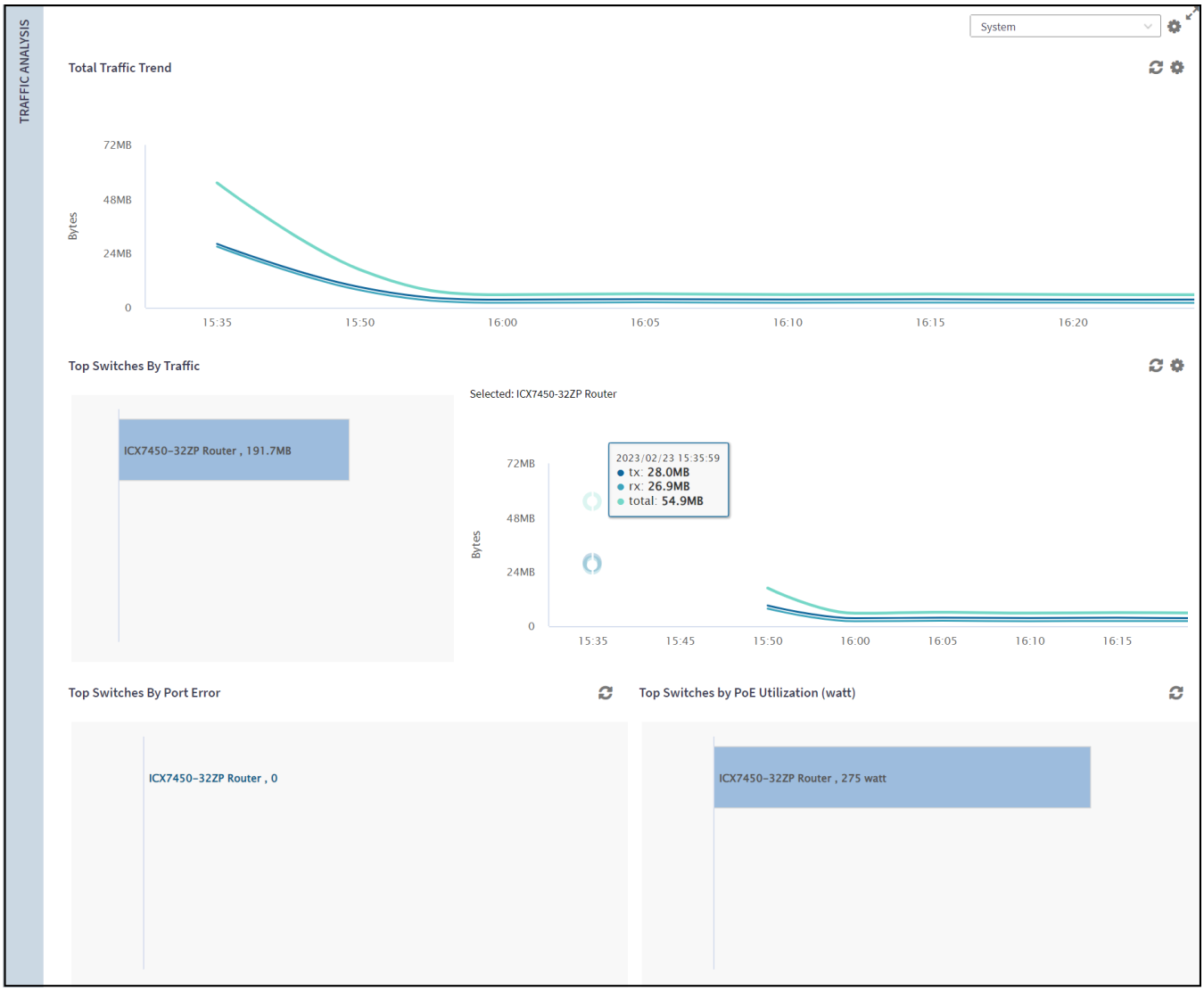


FIGURE 195 Viewing Traffic Analysis



In the port view mode, the **Health** pane displays the number of switches that are online, offline, and flagged.

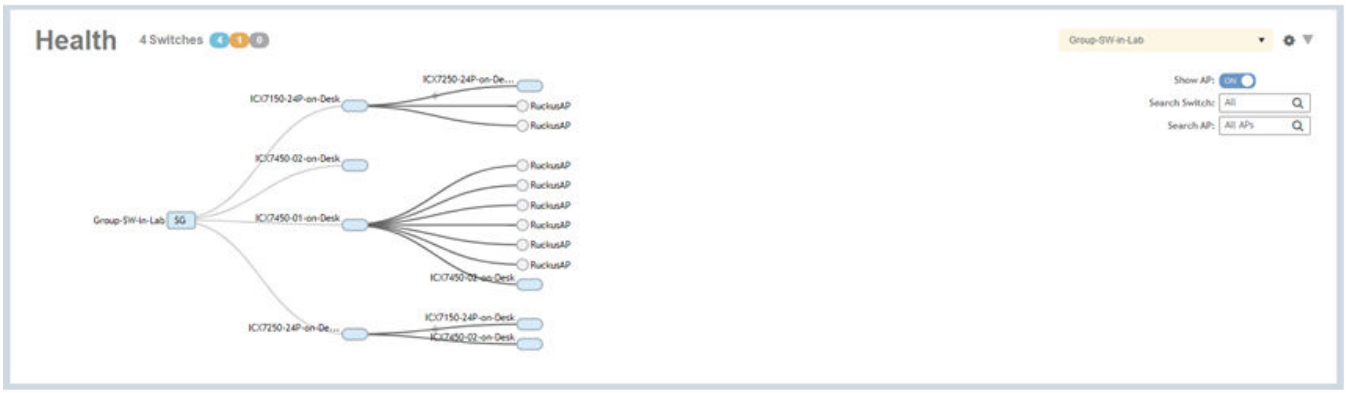
The **Health** pane also displays the number of ports for each port speed (1 Gbps, 2.5 Gbps, 10 Gbps, and so on) or all the ports, and indicates the status of the ports (Up, Down, Down by Admin, Down Total, and Up Total).

The **Traffic Analysis** pane displays the following information:

- Total Traffic Trend
- Top Switches By Traffic
- Top Switches By Port Error

- Top Switches by PoE Utilization (watt)

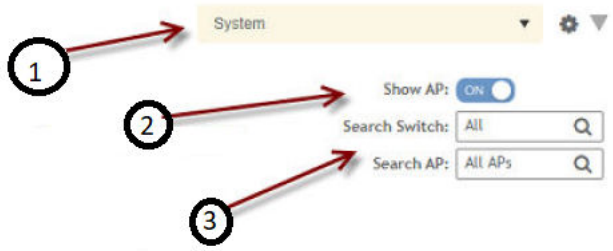
FIGURE 196 Showing Wired Devices Using Topology View Mode



In the topology view mode, the **Health** pane consists of a filter combo box to display domain, sub-domain and switch group in the topology view. The **Show AP** button can be turned on or off to view either the switch or a combination of switch and AP, and **Search** box to search AP or switch based on the device name and MAC address. If you pause the pointer on a link in the topology view, the highlighted link shows the port and LAG information. If you pause the pointer on a device, the highlighted device shows device information such as name, model, MAC address, and IP address (for the switch only).

NOTE
The **Health** dashboard refreshes automatically every 15 minutes to show the latest topology view.

FIGURE 197 Showing Elements on the Health Dashboard



1 - Filter

2 - Topology Type Switch Button

3 - Search Bar

Working with Data and Control Plane

Viewing the System 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..

FIGURE 198 System Cluster Overview - SZ300

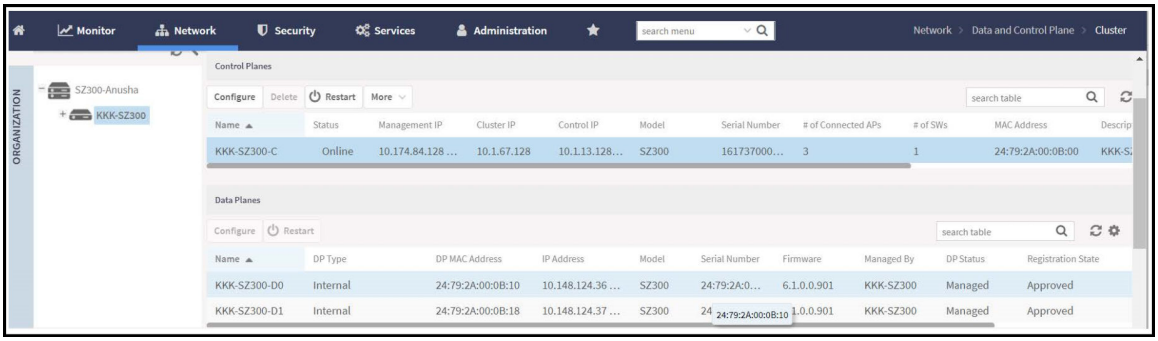
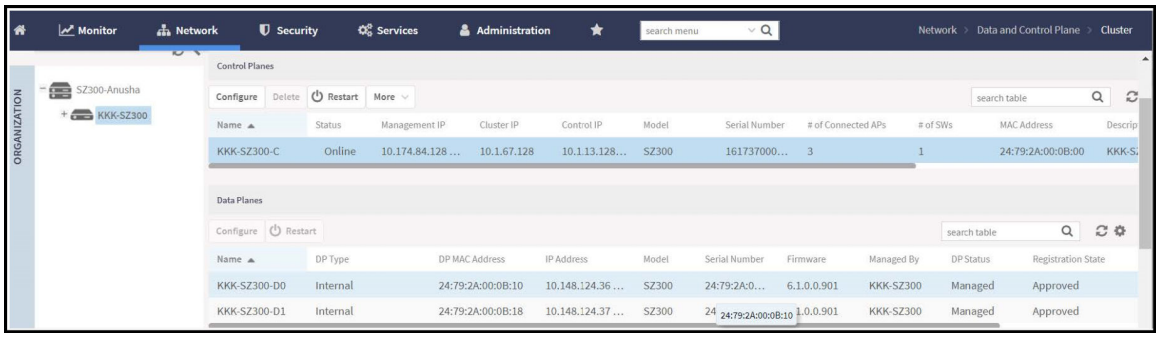


FIGURE 199 System Cluster Overview - vSZ-H



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.

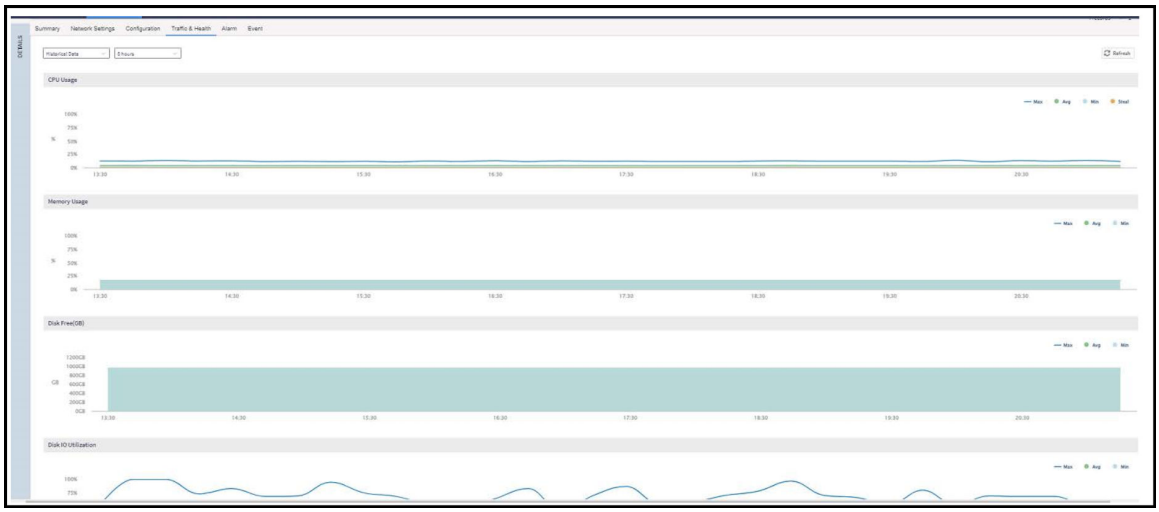
The control plane manages and exchanges routing table information. The control plane packets are processed by the router to update the routing table information. The data plane forwards the traffic along the path according to the logic of the control plane.

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 200 Viewing the Cluster Traffic



Interface and Routing

To configure a cluster node, you must define interface and routing information.

Interface

You can only create one user defined interface, 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.

Static Routing

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

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 201 Cluster Node Chassis



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

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 89 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.
- 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.

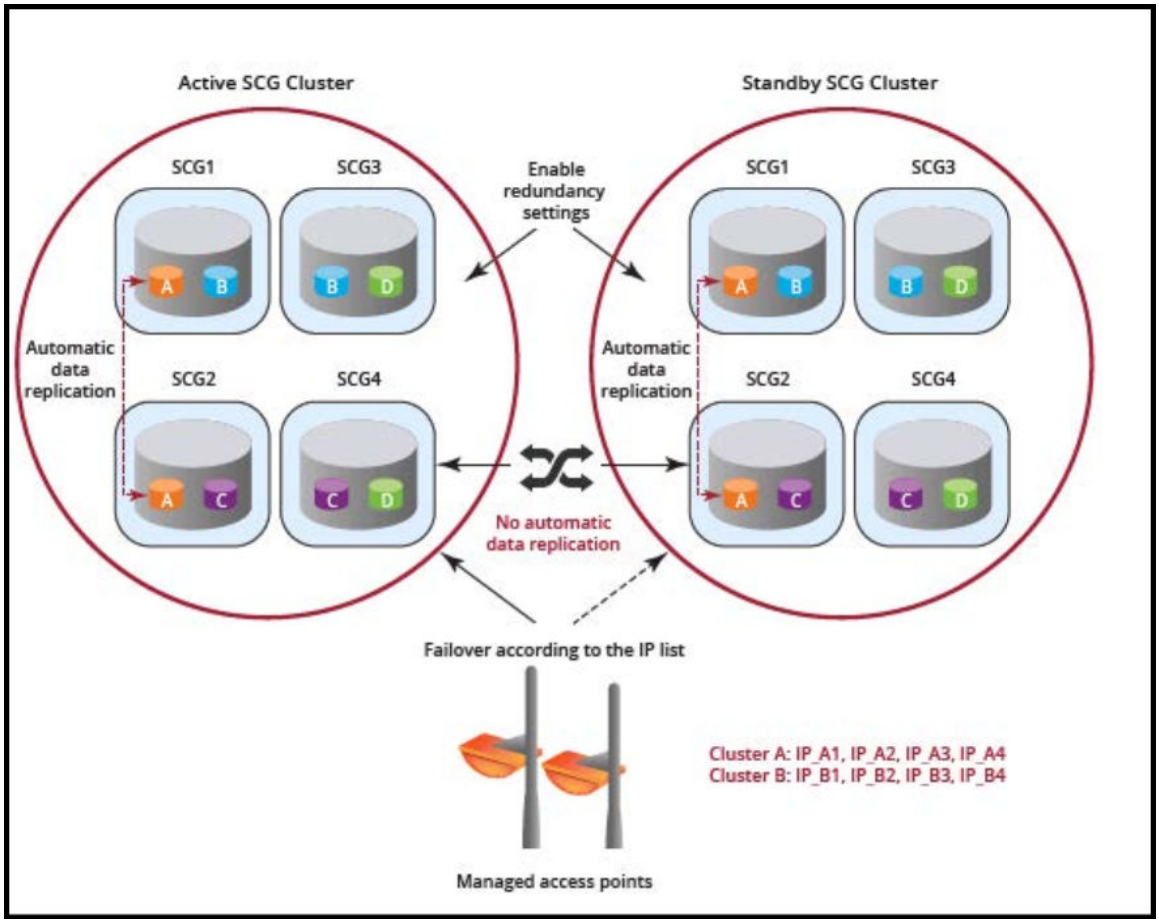
Enabling Cluster Redundancy

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.

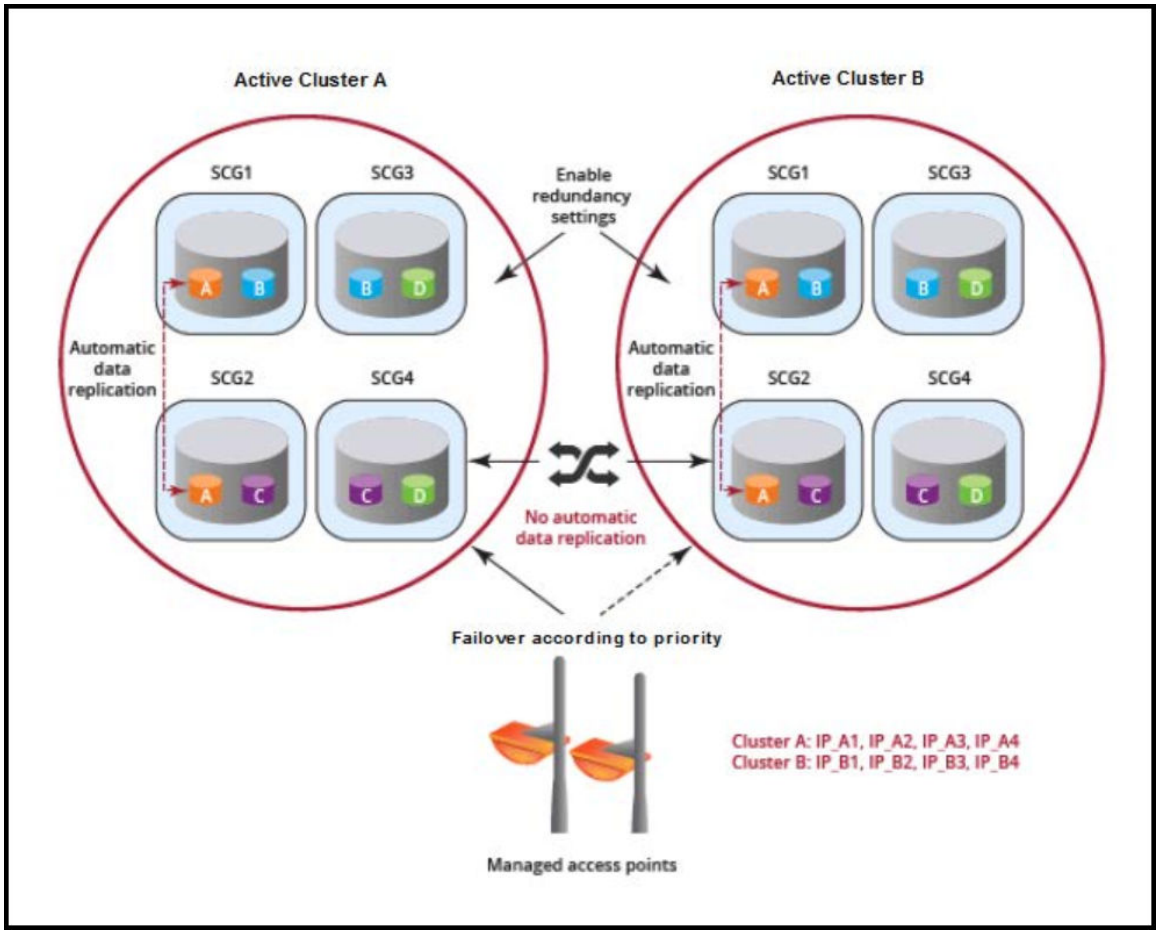
FIGURE 202 Cluster Redundancy for Active-Standby Mode



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 203 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 **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 90 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. • 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). • Only when active cluster is out-of-service (default setting) • Always on service	No	Yes
Schedule Configuration Sync	• 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

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**.

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 91 Configuring Control Plane

Field	Description	Your Action
Physical Interfaces		
IPv4-Control Interface	Indicates the management and IP control settings.	Select the **IP Mode**: • **Static** (*recommended*)—To manually assign an IP address to this interface manually. – 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. – Enter **Control NAT IP**.
IPv4-Cluster Interface	Indicates the IPv4 cluster interface settings	Select the **IP Mode**: • **Static** (*recommended*)—To manually assign an IP address to this interface manually. – 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 91 Configuring Control Plane (continued)

Field	Description	Your Action
IPv4-Management Interface	Indicates the IPv4 management interface settings	Select the **IP Mode**: • **Static** (*recommended*)—To manually assign an IP address to this interface manually. – 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.
IPv6-Control Interface	Indicates the IPv6 control interface settings	Select the **IP Mode**: • **Static** (*recommended*)—To manually assign an IP address to this interface manually. – 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	Select the **IP Mode**: • **Static** (*recommended*)—To manually assign an IP address to this interface manually. – 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.

TABLE 91 Configuring Control Plane (continued)

Field	Description	Your Action
IPv4 Default Gateway & DNS	Indicates the IPv4 gateway that you want to use - Control, Cluster, and Management. **NOTE** When **Access & Core Separation** is enabled, the **Default Gateway** field is hidden. **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.	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.
IPv6 Default Gateway & DNS	Indicates the IPv6 gateway that you want to use - Control, Cluster, and Management. **NOTE** When **Access & Core Separation** is enabled, the **Default Gateway** field is hidden. **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.	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.
User Defined Interfaces **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.		
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.

TABLE 91 Configuring Control Plane (continued)

Field	Description	Your Action
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.

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:

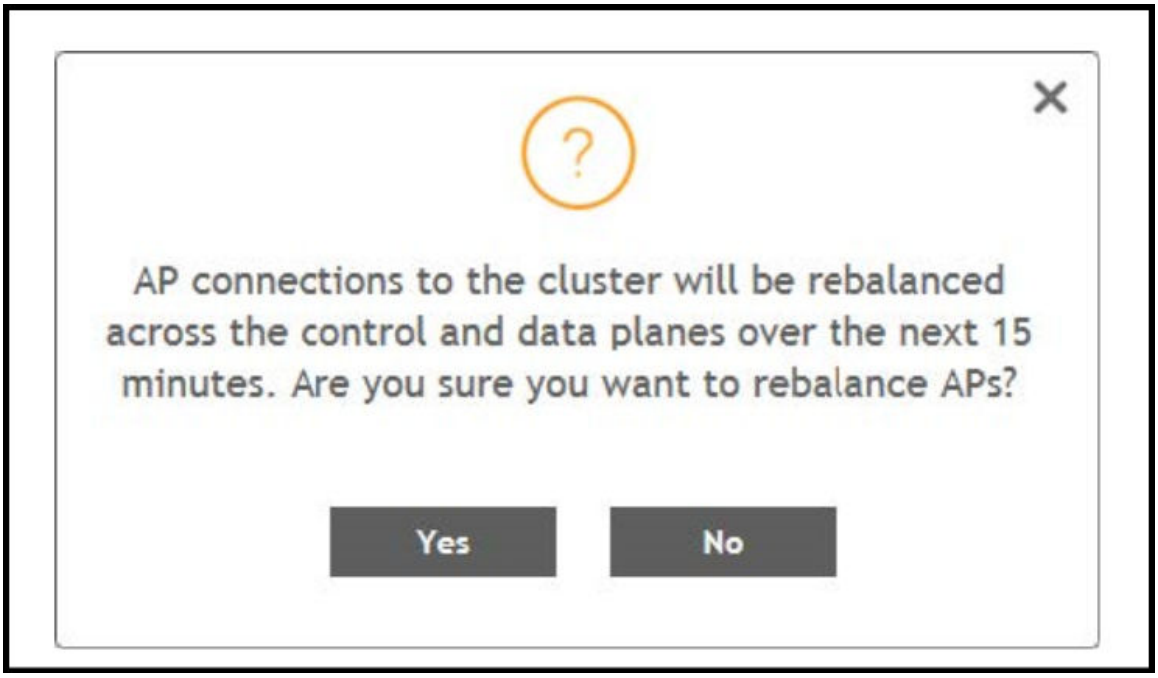
   - **Event 770: Generate ApConfig for plane load rebalance succeeded.**
   - **Event 771: Generate ApConfig for plane load rebalance failed.**

   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 204 AP Rebalancing Form



2. 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.

Configuring the Data Plane

By default, the controller sends traffic from its data plane from a single interface.

NOTE
This feature is managed only by vSZ-E and vSZ-H controllers.

If your organization's network requires separation of the access and core traffic, configure access and core separation on the controller.

To configure a data plane:

1. Go to **Network** > **Data and Control Plane** > **Cluster**.
2. Select the data plane from the list and click **Configure**.The Edit Data Plane Network Settings form appears.
3. Configure the settings as explained in Table 92.
4. Click **OK**.

TABLE 92 Configuring Data Plane

Field	Description	Your Action
Network		

TABLE 92 Configuring Data Plane (continued)

Field	Description	Your Action
Interface Mode	Indicates the traffic direction.	Choose the option: • **Single Interface** (default)—For the controller to send traffic from its data plane from a single interface. • **Access and Core Interface**—For the controller to send traffic to the access and core networks separately. **NOTE** To separate the access and core networks – Use static routes, if the data plane is required to connect to IP addresses in the core network (for example, for DHCP relay or L2oGRE termination) and the destination IP addresses are not part of the core subnet. • **Keep original configuration**—For the controller to keep the original manual Data Plane setup.
Network > **Primary (Access) Interface**		
IP Mode	Indicates the mode of assigning the IP address to this interface.	Select the option: • **Static** (*recommended*)—To manually assign an IP address to this interface manually. – Enter the **IP Address**. – Enter **Subnet Mask** for the IP address. – Enter the **Gateway** router address. – Enter the **Primary DNS Server** IP address. – Enter the **Secondary DNS Server** IP address. – Enter **VLAN** ID to tag traffic. – Choose the **Data NAT IP/Port Configured** option. – Enter **Data NAT IP** address. – Enter **Data NAT Port** address. • **DHCP**—To automatically obtain an IP address from a DHCP server on the network. – Enter **VLAN** ID to tag traffic. – Choose the **Data NAT IP/Port Configured** option.
Network > **IPv6 Primary (Access) Interface**		
IP Mode	Indicates the mode of assigning the IP address to this interface.	Select the option: • **Static** (*recommended*)—To manually assign an IP address to this interface manually. – Enter the **IP Address**. – Enter the **Gateway** router address. – Enter the **Primary DNS Server** IP address. – Enter the **Secondary DNS Server** IP address. • **Auto**—To automatically obtain an IP address from a DHCP server on the network.
Network > **Secondary (Core) Interface** (applicable for **Interface Mode**: **Access and Core Interfaces**)		
IP Address	Indicates the IP address of the core network interface.	Enter the IP address. **NOTE** The secondary/core interface IP address must be configured manually; DHCP is unsupported.
Subnet Mask	Indicates the IP address of the subnet mask.	Enter the subnet mask.

TABLE 92 Configuring Data Plane (continued)

Field	Description	Your Action
VLAN	Indicates that the traffic is tagged with a VLAN ID.	Enter the VLAN ID. **NOTE** If VLANS are configured on both the access and core networks, the VLAN ID that you enter here must be different from the one that you entered for the primary/access interface. **NOTE** You cannot configure the IP address and VLAN settings for a virtual Data Plane from the Primary (Access) and Secondary (Core) Interface sections. Only vSZ-H supports virtual Data Plane.
Disconnect AP when core link down	Indicates that the AP is disconnected secondary core link is down.	Select the check box.
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.
Add	Adds the static route settings.	Click **Add**.
CALEA Relay		
Mark this Data Plane as CALEA Relay (This feature is supported only for vSZ-E and vSZ-H controllers)	Indicates that the data plane uses CALEA relay.	Select the check box.
DHCP Profile		
DHCP Profile	Indicates the data plane DHCP service profile.	Choose the DHCP service profile from the drop-down.
NAT Profile		
NAT Profile	Indicates the data plane NAT service profile.	Choose the NAT service profile from the drop-down.
Syslog		
Enable DHCP syslog	Enables syslog to record the DHCP logs.	Select the check box.
Enable NAT syslog	Enables syslog to record the NAT logs.	Select the check box.
Syslog Server IP	Indicates the IP address of the remote syslog server.	Enter the IP address of the remote syslog server.
Syslog Server Port	Indicates the port number of the remote syslog server.	Enter the Port number of the remote syslog server.

NOTE
You can restart a data plane. To do so, select the data plane from the list and click **Restart**.

NOTE
You can approve or delete a data plane. To do so, select the data plane from the list and click **Approve** or **Delete** respectively. You can also download debug logs or switch over clusters. To do so, select the data plane from the list, click **More** and select **Download** or **Switch Over Clusters** respectively.

NOTE
All configuration changes applicable to vSZ-H are also applicable to SZ100-D.

Monitoring Cluster Settings

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 form 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 form 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.
   - **Cateogry**: 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.

Creating a DP Group

The vSZ-D version in the same DP group must be the same for consistent AP/DP functioning.

NOTE
Creating a DP group affinity profile is supported only for vSZ-E and vSZ-H platforms.

Complete the following steps to create a DP group.

1. Select **Network** > **Data and Control Plane** > **DP group**.
2. Click **Create**.

   The **Create DP group** form is displayed.
3. Enter a **Name** and **Description** for the DP group.
4. Click **Add**.

   The **Add DP** page is displayed.
5. Select Data Plane from the list and click **OK**.

NOTE

- While SZ is upgrading from an older version to a newer version, the system validates whether any DP is assigned a duplicate. If a duplicate is encountered, the following warning message is displayed:

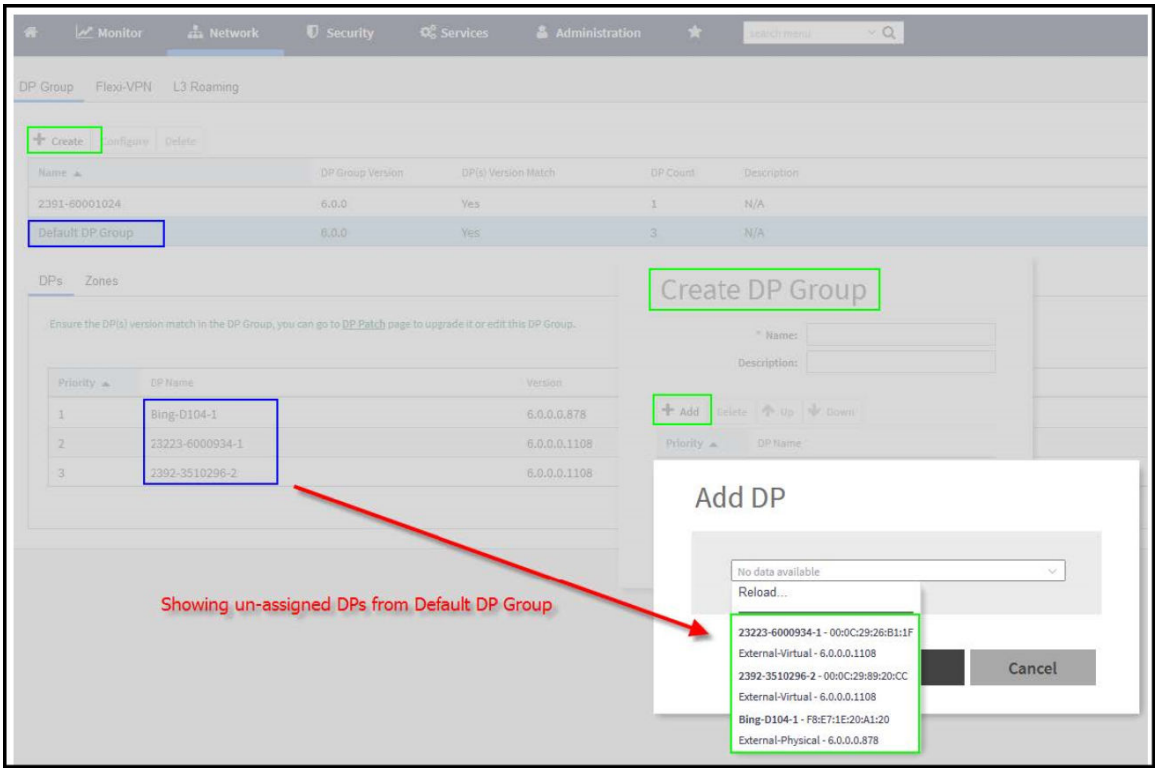
  ```
  There is an over-assigned DP in the DP Zone Affinity profiles. Please go to the
  DP Zone Affinity page to edit and make sure only one DP profile is assigned at
  the same time.
  ```

  Once the over-assigned DPs are removed, SZ can upgrade the system.
- After the configuration that included the over-assigned profiles has been restored, the following message notifies you to correct the configuration:

  ```
  The overlapping DP Group has been detected. There is the over-assigned DP in DP
  Group. Please go to DP Group page to edit and make sure the DP only one DP Group
  assigned at the same time.
  ```

.

FIGURE 205 Creating a DP Group



.

6. Click **OK**.

NOTE
You can edit or delete a DP group. To do so, select the DP Group from the list and click **Configure** or **Delete** respectively.

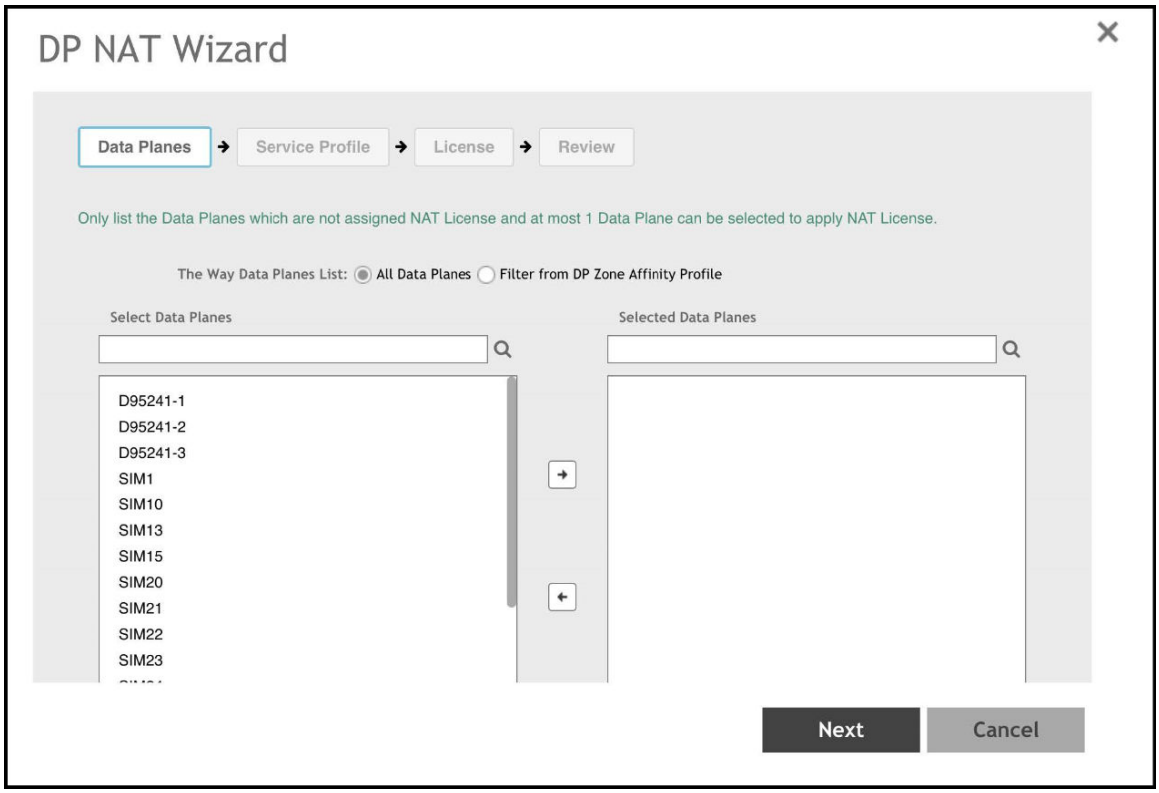
Verifying DP Version Match

From the list, the **DP(s) Version Match** column indicates **Yes** if all the DPs have the same version in the DP Group and **No** if the DPs have different versions in the DP group. You can click the **DP(s)** tab to verify the version of the DP.

DP NAT License Assignment

1. Select the data plane.
2. Option 1 let the user select filter to apply.
3. The "Select Data Planes" is listing DP(s) filtering by option 1.
4. In "Select Data Planes" area, only list DP(s) which has not assigned NAT license.

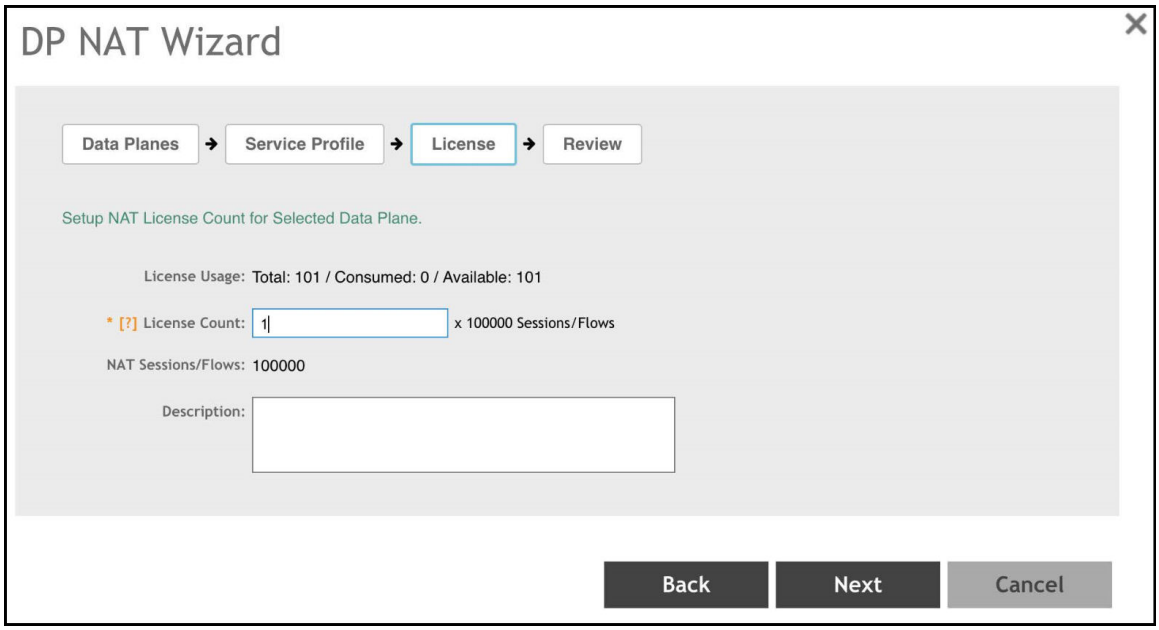
FIGURE 206 DP NAT WIZARD



1. Select the NAT service profile.
2. In NAT service profile option, only list the profile which has not assigned to DP.
3. The existed service profile on DP will be replaced after the wizard completed.

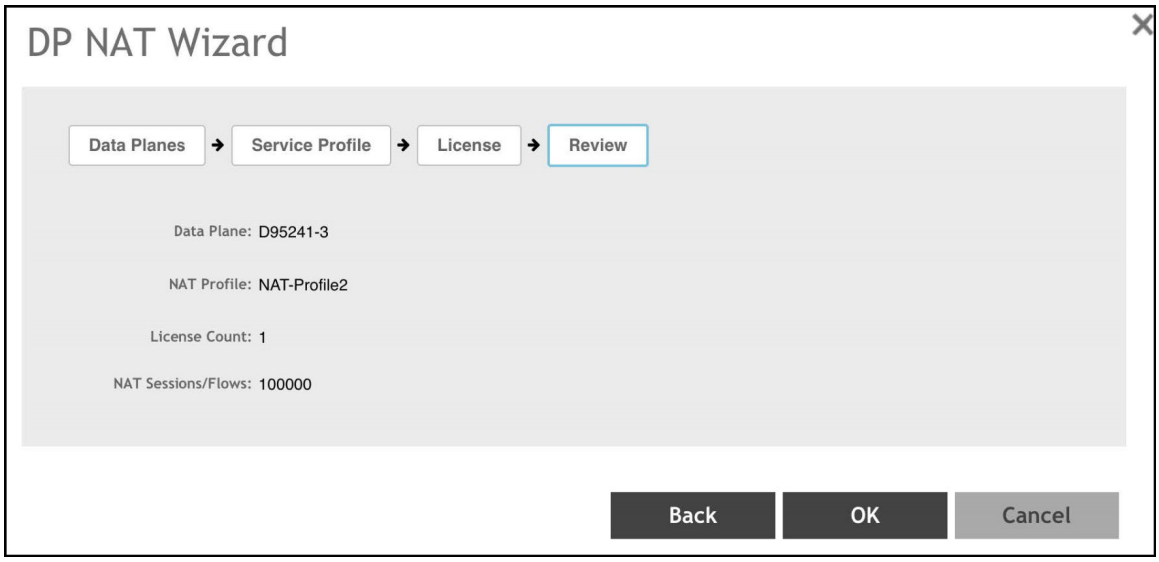
Allocate the sufficient license for DP NAT.

FIGURE 207 DP NAT WIZARD License



Review all DP NAT configuration before applying.

FIGURE 208 DP NAT WIZARD Review



Enabling Flexi VPN

You can enable Flexi-VPN and limit the network resources that a UE can access. Flexi-VPN allows an administrator to customize the network topology, and is thereby able to control the network resources accessible to the end-user. This feature is only supported on vSZ-E and vSZ-H, and is enabled by purchasing the Flexi-VPN license.

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

   The **Flexi-VPN** status page is displayed.
2. Select **Flexi-VPN**.

   NOTE
   The Flexi-VPN option is available only if the Access-VLAN ID is configured in manual mode, and when VLAN Pooling, Dynamic VLAN and Core Network VLAN options, and Tunnel NAT are disabled.

   NOTE
   Flexi-VPN is activated when a Flexi-VPN profile is assigned to a WLAN.

   NOTE
   A maximum of 1024 WLAN IDs can be applied to a Flexi-VPN profile.
   Flexi-VPN supports IPv4 addressing formats and Ruckus GRE tunnel protocol. It does not support IPv6 addressing formats.

The following record table indicates that the Flexi-VPN profile is successfully applied to the WLAN:

- WLAN: displays the name of the WLAN
- Zone: displays the name of the zone
- Zone Affinity Profile: displays the name of the source data plane from which tunneled traffic starts
- Flexi-VPN Profile: displays the name of the destination data plane to where the tunneled traffic terminates

Enabling L3 Roaming Criteria for DP

Using the layer 3 roaming feature, clients can roam across APs in the network (from one data plane to another data plane). This is typically required when the number of clients in the network increases and clients have to roam from a network that they were connected to, to another WLAN network with similar access settings. This feature enables seamless roaming and ensures session continuity between the client and the network.

NOTE
L3 roaming is only supported on vSZ-H and vSZ-E.

You can configure the roaming criteria for a DP so that it uses one of these two options - UE subnet or WLAN VLAN to access another DP to connect to, within a network. Before this, you must ensure that the L3 roaming feature is enabled in the DP.

1. From the main menu, go to **Network** > **Data and Control Plane** > **L3 Roaming**.

   The **L3 Roaming** page is displayed.
2. Select **L3 Roaming**.
3. Click **Configure** to edit the L3 roaming settings.

   The **Edit L3 Roaming** page is displayed.
4. From **Activate**, you can enable the feature for the DP by selecting Enable or Disable from the drop-down menu.
5. From the **Roaming Criteria** list, select one of the following options to define the data format to establish connection between DPs: UE Subnet or WLAN VLAN.
6. Click **OK**.

You have successfully enabled L3 roaming, and also set the roaming criteria based on which DPs would connect within the network.

NOTE
If there are more than 40 DPs been approved, the controller limits you to use L3 Roaming.

NOTE
A fresh controller software installation or upgrade from a version that does not support L3 roaming resets the L3 roaming configuration and it remains disabled. You must enable L3 roaming on a DP again.

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, iIt 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.

Security

- Application Control....373
- Access Control....378
- Authentication....427
- Accounting....441

Application Control

Viewing Application Control Summary

You can view application-wise or port-wise summary in a chart or table format.

To view the application control summary:

1. Select **Security** > **Application Control** > **Summary**.

   This displays the **Summary** page.
2. The **Summary** page can be viewed with following options:
   - Top Applications by: Choose Application or Port from the drop-down menu.
   - Click to view by Chart or Table.
   - Count: Select 10 or 25.
   - Total, 2.4 GHz, 5GHz. 6(5)GHz.
   - Duration: Select Last 1 hour or Last 24 hours.
   - APs: Select All APs or a specific AP.
   - All Clients: Select All Clients, Wired or Wireless clients.

Creating an Application Control Policy

An application control policy is created to limit and classify traffic into priority queues using QoS traffic shaping rules, or to completely block access to an application.

Complete the following steps to create an application control policy.

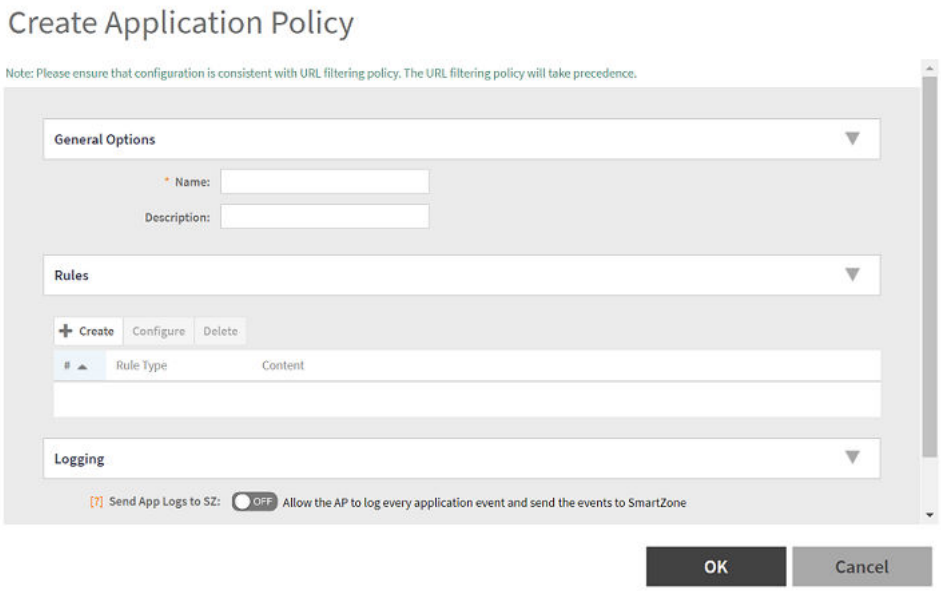
1. From the main menu, go to **Security** > **Application Control** > **Application Policy**.

   The **Application Policy** page is displayed.

2. Click **Create**.

   The **Create Application Policy** dialog box is displayed.

   FIGURE 209 Creating an Application Policy



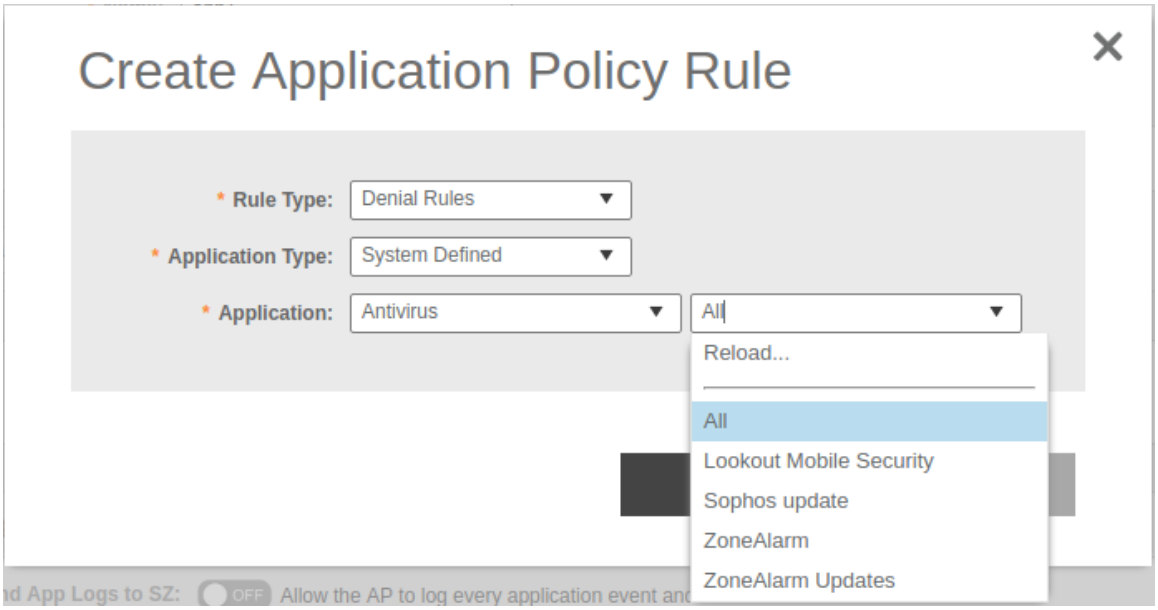
3. Under **General Options**, enter the policy name and description.

4. Under **Rules**, click **Create** to create a new rule.

   NOTE
   Each application policy can contain up to 128 rules.

   The **Create Application Policy Rule** dialog box is displayed.

   FIGURE 210 Creating an Application Policy Rule



5. From the **Rule Type** list, select one of the following options:
   - **Denial Rules**
   - **QoS**
   - **Rate Limiting**
6. From the **Application Type** list, select an application type.
7. From the **Application** field, select the application for which you want to create a policy rule.

   For example, if you select **All** in the Anitvirus application category and save the application rule, the application rule list reflects all antivirus applications and is selected as a single entry in the rule list. A full category is counted as one rule in the allotment of 128 Layer 7 rules in a Layer 7 policy.
8. Click **OK** to save the rule.

   NOTE
   If a rule is already created, you can edit its configuration settings by selecting the rule and clicking **Configure** in the **Create Application Policy** dialog box.

9. Under **Logging**, select the appropriate option for the APs to log events:
   - **Allow the AP to log every application event and send the events to SmartZone**
   - **Allow the AP to log every application event and send the events to external syslog**
10. Click **OK** to save the application control policy.

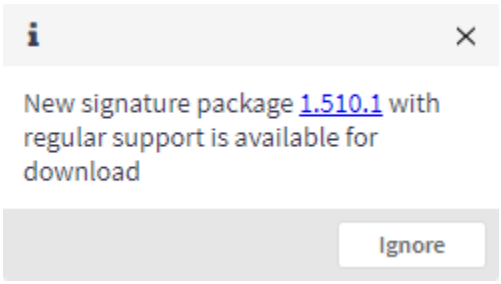
You can continue to apply the application control policy to user traffic.

Working with Application Signature Package

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

SmartZone displays a pop-up notification message whenever a latest signature package is available for download.

FIGURE 211 Pop-up Notification of Application Signature Package

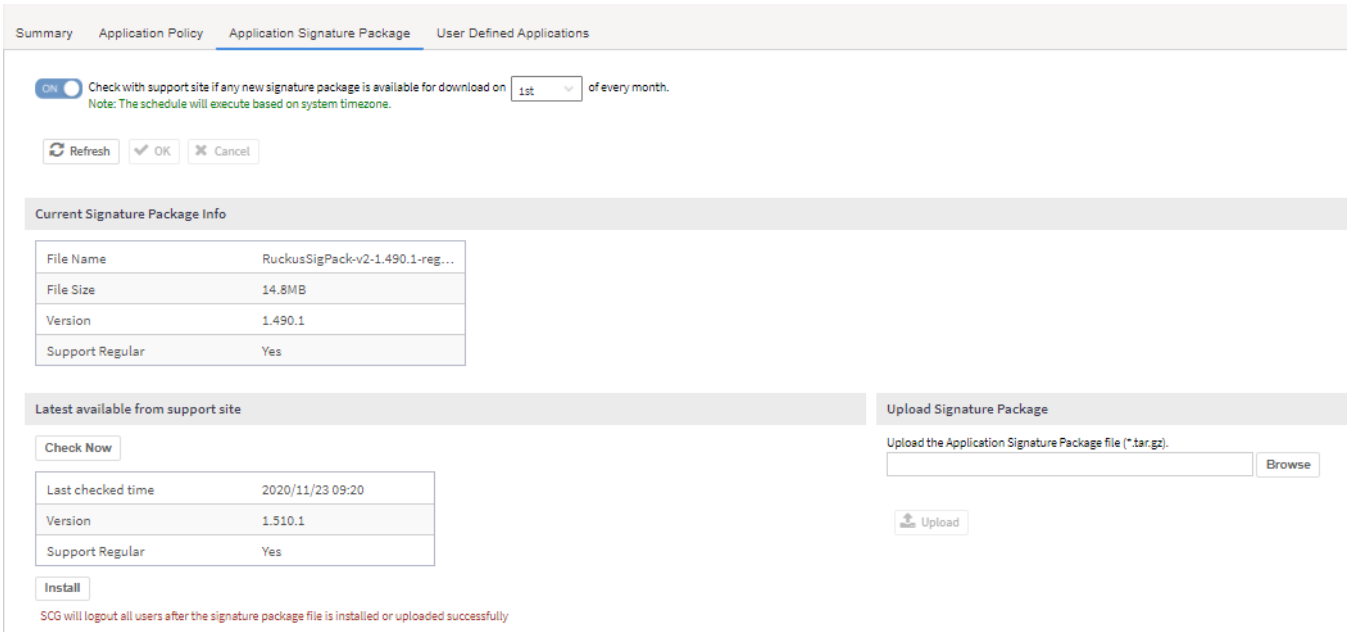


Alternatively, signature package updates or downloads can be scheduled from the RUCKUS download center.

To check for signature package updates:

1. Select **Security** > **Application Control** > **Application Signature Package**.
   This displays **Application Signature Package** page.

   FIGURE 212 Periodic checking of Application Signature Package



2. Select the **Check with support site if any new signature package is available for download on (select the date of the month) from the drop-down menu** option and enter the date to schedule updates every month. By default, this option is set to the first of every month.

   NOTE
   The schedule will execute based on the system timezone.

   The **Current Signature Package Info** section displays the information about the file name, file size, version and type of the signature package.
3. From the **Latest avaiable from support site** section, click **Check now** to check for any latest update.
4. Click **Install** to install the latest signature package.

   After the signature package file is installed or uploaded successfully, SCG will logout all users .

Creating an User Defined Application

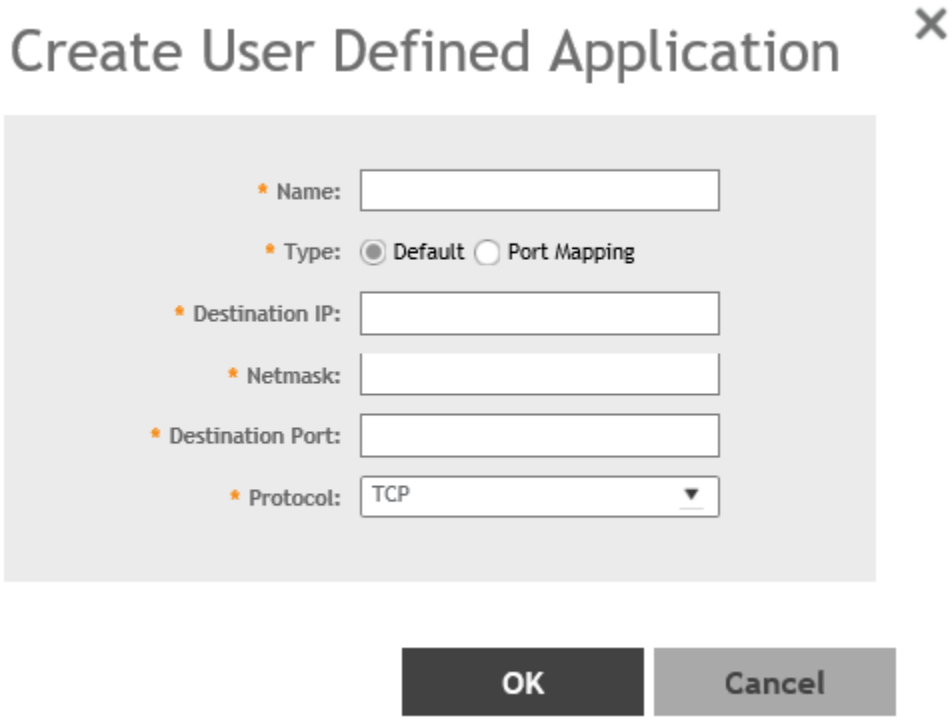
When an application is unrecognized and generically (or incorrectly) categorized, the controller will be unable to monitor its traffic, unless you configure an explicit application identification policy based on IP address/mask, port and protocol.

To configure a user-defined application:

1. Go to **Security** > **Application Control** > **User Defined Applications**.
2. Click **Create**.

   The **Create User Defined Application** page appears.

   FIGURE 213 Creating an User Defined Application



3. Configure the following:
    a. **Name**: Type a name for the application. This is the name that will identify this application on the dashboard.
    b. **Type**: Select Default or Port Mapping Only (destination port).
    c. **Destination IP**: Type the destination IP address of the application.
    d. **Netmask**: Type the netmask of the destination IP address.
    e. **Destination Port**: Type the destination port for the application.
    f. **Protocol**: Select the protocol used by the application. Options include TCP and UDP.
    g. Click **OK**.

You have created the user defined application.

NOTE
You can also edit, clone and delete the application policy by selecting the options **Configure**, **Clone** and **Delete** respectively, from the **User Defined** tab.

Access Control

Managing a Firewall Profile

A firewall profile defines the level of protection. It allows to choose the attributes before applying a policy.

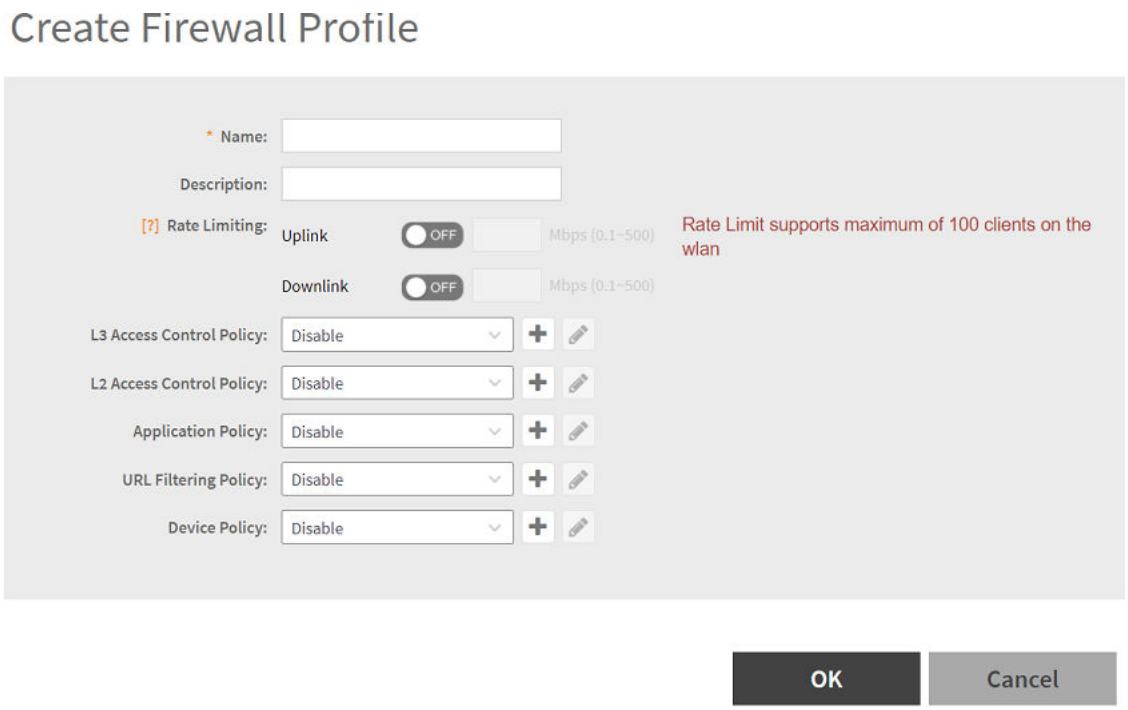
To create a firewall profile, perform the following steps:

1. Select **Firewall**, the **Firewall Profiles** page is displayed.
   The **Summary** tab displays the firewall profiles in chart and graph format. You can filter the profiles based on duration and zone.

2. Select **Profiles** tab and click **Create**.

   This displays the **Create Firewall Profile** page.

   FIGURE 214 Creating Firewall Policy



3. In the **Name** field, enter a name for this profile.
4. In the **Description** field, enter a short description for this profile.
5. In the **Rate Limiting** field, select the **Uplink** and **Downlink** options to specify and apply rate limit values for the device policy to control the data rate.
6. Configure the following policies:

   a. Select the **L3 Access Control Policy** from the drop-down list or click to create a new policy. Refer to Create an L3 Access Control Policy on page 380 for more information.

   b. Select the **L2 Access Control Policy** from the drop-down list or click to create a new policy. Refer to Creating an L2 Access Control Service on page 382 for more information.

   c. Select the **Application Policy** from the drop-down list or click to create a new policy. Refer to Creating an Application Control Policy on page 373 for more information.

   d. Select the **URL Filtering Profile** from the drop-down list or click to create a new profile. Refer to Creating a URL Filtering Policy on page 385 for more information.

   e. Select the **Device Policy** from the drop-down list or click to create a new policy. Refer to Creating a Device Policy on page 390 for more information.

7. Click **OK**.

NOTE
You can also edit, clone and delete a firewall profile by selecting the options **Configure**, **Clone** and **Delete** respectively, from the **Firewall Profiles** page.

NOTE
At system level user can create maximum 64 firewall profiles.

Create an L3 Access Control Policy

An L3 Access Control Policy can be created to block or limit user traffic based on a number of factors, including Source IP address, Port, Destination IP address, Protocol, etc. Additionally, an L3 Access Control Policy can be created to shape traffic according to a configurable Application Control Policy.

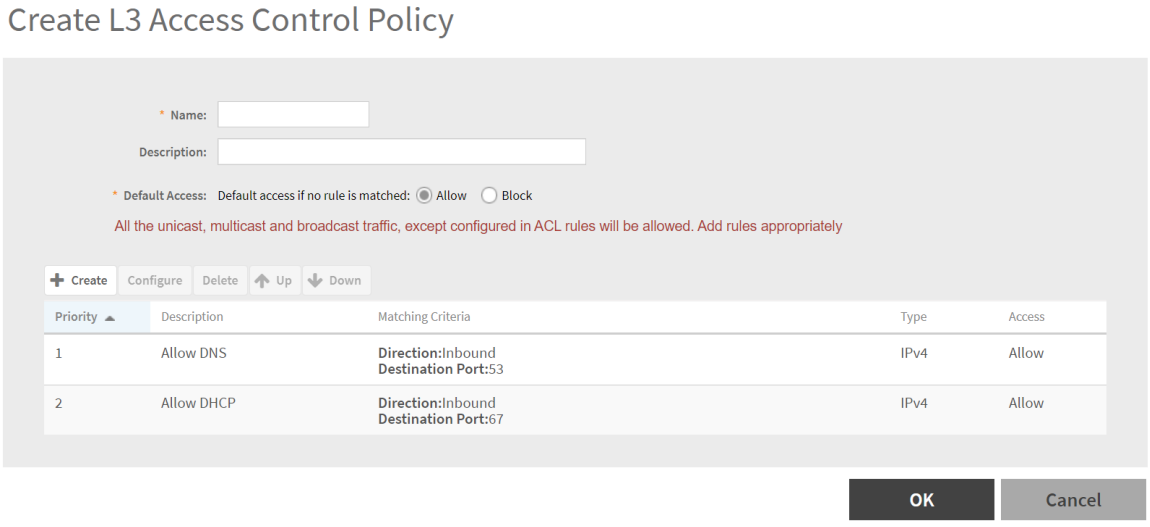
After L3 Access Control Policy is created, it can be applied to any WLAN from the **Wireless LANs** page.

1. Select **Security** > **Access Control** > **L3 Access Control**.

   The **L3 Access Control** page is displayed.
2. Click **Create**.

   This displays the **L3 Access Control Policy** page.

FIGURE 215 Creating an L3 Access Control Policy



3. In the **Name** field, enter a policy name.
4. In the **Description** field, enter a short description for the policy.
5. In **Default Access**, select **Allow** or **Block** if no rule is matched.

6. To assign rules for the policy, click **Create**. The **L3 Access Control** page is displayed.

   Refer to Create an L3 Access Control Policy Rule on page 381 for more information.

   NOTE
   You can set a priority to the policy by selecting the policy and click **Up** or **Down** to set the desired order.

   NOTE
   You can edit or delete a policy rule by selecting the options **Configure** or **Delete** respectively.

7. Click **OK** to save the policy.

After the L3 access control policy is created, it can be applied to any WLAN from the Wireless LANs page.

NOTE
You can edit, clone, or delete a policy by selecting the options Configure, Clone, and Delete respectively, from the L3 Access Control page.

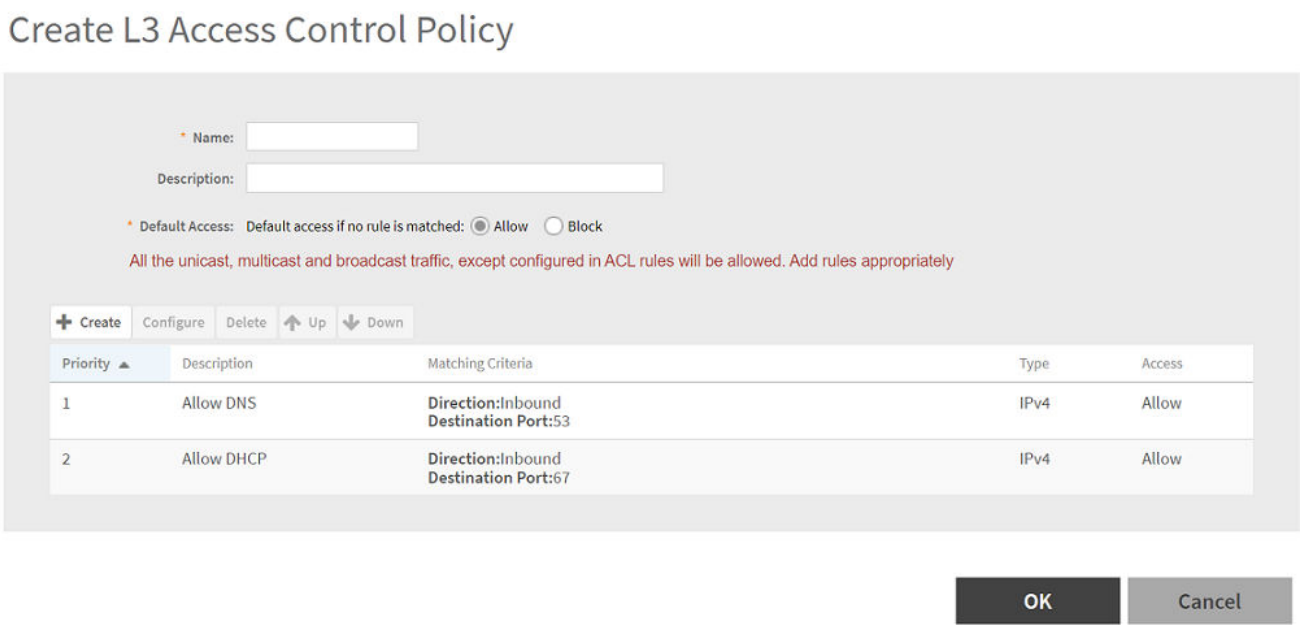
Create an L3 Access Control Policy Rule

An L3 Access Control Policy of multiple traffic control rules, which can be enforced in any order you prefer.

To create an L3 access control policy rule:

1. From the **L3 Access Control Policy** page, click **Create**. The **L3 Access Control Policy Rule** page is displayed.

FIGURE 216 Creating an L3 Access Control Policy Rule



2. Configure the following:
   - **Description**: Type a short description for the access control policy rule.
   - **Access**: Select Allow or Block depending on whether you want to set this rule as the default rule.

     NOTE
     All unicast, multicast and broadcast traffic, except the ACL rules will be allowed or dropped depending on the option selected. Add the appropriate rules.

   - **Protocol**: Select the network protocol to which this rule will apply. Supported protocols include TCP, UDP, UDPLITE, ICMP (ICMPv4), ICMPV6, IGMP, ESP, AH, SCTP.
   - **Type**: Choose the IP version, IPv4 or IPv6.
   - **Source IP**: Enable the option and specify the source **Subnet Network Address** and **Subnet Mask** for IPv4 option type or enter I**Pv6 Network** address for IPv6 option type.
   - **Source Port**: Enable the option and specify the source port to which this rule will apply. To apply this rule to a port range, type the starting and ending port numbers in the two boxes.
   - **Destination IP**: Enable the option and specify the destination **Subnet Network Address** and **Subnet Mask** for IPv4 option type or enter **IPv6 Network** address for IPv6 option type.
   - **Destination Port**: Enable the option and specify the source port to which this rule will apply. To apply this rule to a port range, type the starting and ending port numbers in the two boxes.
   - **Direction**: Select Inbound, Outbound or Dual indicating the direction of the traffic.
3. Click **OK** to save your changes.

NOTE
Alternatively, in **Wireless LANs** configuration under **Firewall Options**, select the **Enable WLAN specific** option or map the firewall profile from the firewall drop-down list which has the L3 access control policy mapped to it.

Creating an L2 Access Control Service

Another method to control access to the network is by defining Layer 2 MAC address access control lists (ACLs), which can then be applied to one or more WLANs or WLAN groups. L2 ACLs are either allow-only or deny-only; that is, an ACL can be set up to allow only specified clients based on the MAC addresses that are configured. Further, L2 ACLs can also be used to allow-only or deny-only clients based on the ether types of the packet where EtherTypes is a field present in the ethernet header of a packet.

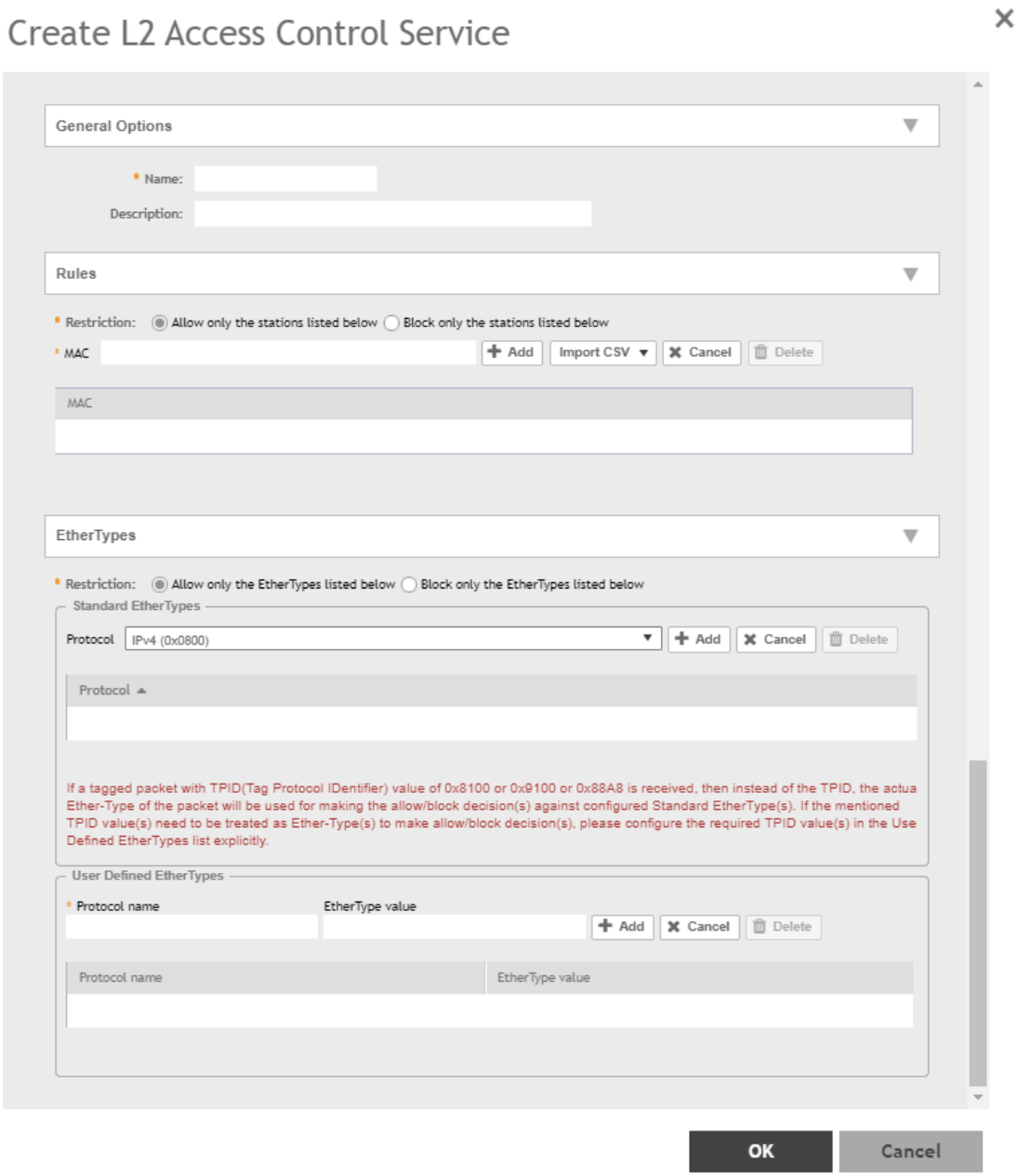
NOTE
If a tagged packet with Tag Protocol Identifier (TPID) value of 0x8100, 0x9100, or 0x88A8 is received, then instead of the TPID, the actual Ether-Type of the packet will be used for making the allow or block decision against the configured Ether-Types. If the mentioned TPID values need to be treated as Ether-Type to make the allow or block decision, configure the required TPID values in the custom Ether-Type list.

1. Select **Security** > **Access Control** > **L2 Access Control**.

2. Click **Create**.

   This displays **Create L2 Access Control Service** page.

FIGURE 217 Creating an L2 Access Control Service



3. Configure the following options:
   a. **General Options**
      - **Name**: Enter a name for this policy.
      - **Description**: Enter a short description for this policy.
   b. **Rules**
      - **Restriction**: Select the default action that the controller will take if no rules are matched. Available options include **Allow only the stations listed below** or **Block only the stations listed below**.
      - **MAC Address**: Enter the MAC address to which this L2 access policy applies and click **Add** or click **Import CSV** to import the MAC address.
   c. **EtherTypes**
      - **Restriction**: The EtherType in the L2 ACL profile allows or blocks the specified EtherType traffic from the clients toward the network. Available options include **Allow only the EtherTypes listed below** or **Block only the EtherTypes listed below**.
      - **Standard Ether Types**: Select a protocol from the **Protocol** list to which this L2 access policy applies and click **Add**.
      - **User Defined Ether Types**: Enter a protocol name and EtherType value in hexadecimal format and click **Add**. A maximum of ten custom EtherTypes can be configured to be allowed or blocked.
4. Click **OK**.

NOTE
Alternatively, in the **Wireless LANs** configuration under **Firewall Options**, select the **Enable WLAN specific** option or map the firewall profile from the firewall list which has the L2 access control policy mapped to it.

NOTE
You can also edit, clone, or delete a policy by selecting the options **Configure**, **Clone**, and **Delete** respectively, from the **L2 Access Control** page.

URL Filtering

Administrators can use the URL filtering feature to block access to inappropriate websites. The Web pages available on the internet are classified into different categories, and those identified to be blocked can be configured based on available categories. Administrators can also create policies based on these categories, to allow or deny user access.

After categorizing websites accessed by the clients connected to the AP, a third-party cloud-hosted URL categorization service is used to categorize the live web traffic generated from the client devices. By default, traffic which is not categorized is allowed. The packets from the client device are dropped only after the URL is successfully categorized, and DENY is configured for the client in the policy.

The AP periodically generates statistics such as the Top 10 Denied URLs/categories, Top 10 URLs/categories by traffic and sends them to controller which collects this information and maintains it based on the filters applied per zone and WLAN.

URLs are typically classified by third-party applications to enhance internet security and usage. To categorize the web page or URL, the network packets must be analyzed. In HTTP packets, the complete URL value is extracted and in HTTPS packets, the domain name of the URL is extracted for URL web page categorization. The AP remembers the signature of the packet it forwards and when the packet is identified as HTTP or HTTPS, it receives the domain name/URL from the packet and sends it to the third-party URL categorization engine to verify the Web category. If the retrieved category is blocked as per the configured policy, packets with the same signature are blocked. Blocked HTTP browser traffic redirects the user to a web page that provides information on why the access to the website was denied. This feature is not applicable to HTTPS traffic and mobile application traffic.

The AP maintains a cache of up to 80000 URL entries and attempts to find the URL category from the local cache. It contacts the third-party URL categorization server only when the URL is not available in the local cache.

Viewing a Summary of URL Filters

The **Summary** page provides administrators with a view to analyze URL traffic based on the user activity over the network.

You can view the top ten URLs by:

- Traffic - displays all URLs accessed (including blocked URLs) the most
- Categories Traffic - displays all categories accessed (including blocked categories) the most
- Clients Traffic - displays all clients accessed (including blocked clients) the most
- Blocked URLs - displays the URLs that have been denied access the most
- Blocked Categorize - displays the URL categories that have been denied the most
- Blocked Clients - displays the clients that have been denied access the most

Creating a URL Filtering Policy

Administrators can create URL filtering policies and reuse them across WLAN controllers. You can define the policy based on the web page categorization, whitelist, blacklist, and web search.

Policies can also be created based on the role assigned to the user. Users can be allowed or denied access to a particular URL based on the role assigned, and the SSID login details for that role.

Complete the following steps to create a URL filtering policy.

1. Go to **Security** > **Access Control** > **URL Filtering** > **Profiles**.

2. Select the **Profiles** tab, and then click **Create**.

   The **Create URL Filtering Policy** page is displayed.



Configure the following options:

- General Options

  Name:: Enter the name of the policy you want to create.

  Description: Enter a brief description to identify the policy.

- **Blocked Categories**: Select one of the categories to block. Selecting the **Custom** option allows the administrator to customize the list of categories to block for the user. You can also use **Select All** to choose all of the categories listed, or **None** to set no filters for the user to access (the user can access any URL in this case because no web page is blocked).
- **Block by Threat Level**: Enable this option and set the slider bar to a threat level. The web reputation score, from1 through 100, gives the reputation index or threat level of a URL being browsed by a user. The reputation score can be used to categorize the threat level of URLs according to the following levels:
  - **Trustworthy**: The web reputation score is in the range of 81 through 100. These are well known sites with strong security characteristics.
  - **Low-Risk**: The web reputation score is in the range of 61 through 80. These are generally benign sites and rarely exhibit the characteristics that expose the user to security risks.
  - **Moderate-Risk**: The web reputation score is in the range of 41 through 60. These are benign sites but have exhibited some characteristics that suggest a security risk.
  - **Suspicious**: The web reputation score is in the range of 21 through 40. These are suspicious sites.
  - **High-Risk**: The web reputation score is in the range of 1 through 20. These are high risk sites.
- **Blacklist & Whitelist**: If web content categorisation, is unable to classify URLs that the user, organization or institution needs, then Whitelist and Blacklist profiles can be created by the administrator. The URLs listed by the administrator under Blacklist are blocked and those listed under Whitelist are allowed access. The domain names under Blacklist and Whitelist take precedence over the default allow or deny action of the URL filter.

The AP matches the URL pattern against all the configured Whitelist and Blacklist profiles through the Extended Global Regular Expressions Print (egrep) program which performs a line-by-line scan of the file and returns lines that contain a pattern matching the given expression. Currently, the exact URL name or a wildcard at the beginning of the URL is used to match the pattern.

Administrators can also add specific IP addresses or wildcard domain names under Whitelist and Blacklist.

In **Domain Name**: Enter the domain name of the web page which you want to deny user access to in the **Blacklist** tab, and enter the domain name of the web page to which you want to provide user access on the **Whitelist** tab. You can define up to 16 domains.

Click **Add**. The domain name or web page is listed in the corresponding tab.

Click **Cancel** to remove the domain name you have entered in the field.

If you want to delete the domain name from the **Blacklist** or **Whitelist** tab, select the URL and click **Delete**.

- Safe Search: Administrators can configure the policy to include a safe search option when users access Google, YouTube, or Bing to search on the internet. Select the respective enable option for Google, YouTube, and Bing. Enabling the option will mandate all users using the policy on the network to use safe search on Google, YouTube, and Bing. By default, FQDN-based safe search is enabled. This option provides a secure connection through HTTPS while allowing access to the internet. To use virtual IP, select the **Virtual IP** option and enter the IP address. If safe search is enabled before uprading to R6.1, the old configuration or virtual IP-based safe search will be retained.

3. Click **OK**.

   The **URL Filtering Policy** form is submitted with the specified configuration settings.

You have created the URL filtering policy. The newly created policy is displayed on the **Profiles** page.

If you click the policy, the following information is displayed:

- Name
- Managed By
- Description
- Filtering Level
- # of Blocked Categorize
- # of Blacklist
- # of Whitelist
- Last Modified By
- Last Modified On

Click **Configure** to edit the policy. Click **Clone** to create a duplicate of the policy, or to make modifications to the existing settings of the clone.

Click **Delete** to delete the policy from the URL Filtering Profile.

Enabling URL Filtering on the Controller

You can enable the URL filtering feature on the WLAN controller to block or allow access to specific web sites or web pages.

By configuring the controller, administrator can create a wireless network SSID and allow or deny access to a category of websites for all users that join this SSID.

Perform the following steps to enable URL filtering on the controller for an available WLAN:

1. Click **Network** tab, select **Wireless LANs**. Select a domain or zone and choose a WLAN from the system tree hierarchy to **Enable URL Filtering** option.

   This displays **Edit WLAN Config** page.

   NOTE
   To enable URL Filtering for a new WLAN, follow the steps to create a new WLAN.

2. Scroll down to **Firewall Options**, click **URL Filtering Policy** option.

   The **URL Filtering Profile** field appears. Select a URL filtering profile from the drop-down menu. To create a new URL filtering policy, refer Creating a URL Filtering Policy on page 385.

   FIGURE 218 Enabling URL Filtering



   NOTE
   Application rules are applied based on the following priority:

   a. User defined Access Control Profile
   b. URL Filtering
   c. Application Control Policy

   User defined rules take precedence over URL filtering.

You have enabled URL filtering on the controller.

Managing URL Filtering Licenses

URL Filtering license for the selected partners-to use the content database is issued for a duration of one year for an AP. Dashboard warnings are issued thirty days before the end of the license term.

You can add licenses over time. For example, you can purchase 100 one-year licenses on January 1st and add another 200 one-year licenses in May. The controller receives a new expiry date for the combined license count of 300 APs.

To view license details such as start date, end date, and capacity, go to **Administration** > **Administration** > **Licenses** > **Installed Licenses**, for For SmartZone 5.2.1 or earlier releases, go to **Administration** > **Licenses** > **Installed Licenses** tab.

For more information on importing installed licenses, synchronizing the controller with the license server, and downloading license files, refer *Managing Licenses*.

When the license capacity is exhausted, event code 1281 is triggered. When the license period expires, alarm code 8003 is generated which indicates that the URL filtering server is unreachable. For more information, refer *Managing Events and Alarms*.

NOTE
A permissive license similar to the BSD 2-Clause License, but with a 3rd clause that prohibits others from using the name of the project or its contributors to promote derived products without written consent.
Copyright (c) 2005, Google Inc. All rights reserved.
Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
- Neither the name of Google Inc. nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

ATTENTION
THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

URL filtering feature is supported only on APs that have a minimum of 256MB RAM.

TABLE 93 List of APs with 256MB or more

E510	T811-CM	T310c/d/n/s	H320
R720	T610/T610s	C110	R610
R500e	H510	T710 / T710s	R510
R310	T504	R710	R600
T300	T301n	T301s	T300e
FZM300 & FZP300	R500	R700	R730
R750	R650	R550	R850
H550	T750	T750SE	

Creating a Device Policy

You can control how devices installed with certain OS configurations can be connected to the network, and also control what they can be allowed to do within the network. Using the device policy service, the system can identify the type of client attempting to connect, and perform control actions such as allowing or blocking access, rate limiting, and VLAN tagging based on the OS rule.

To create a device policy:

1. Click **Security** > **Access Control** and select **Device Policy**.

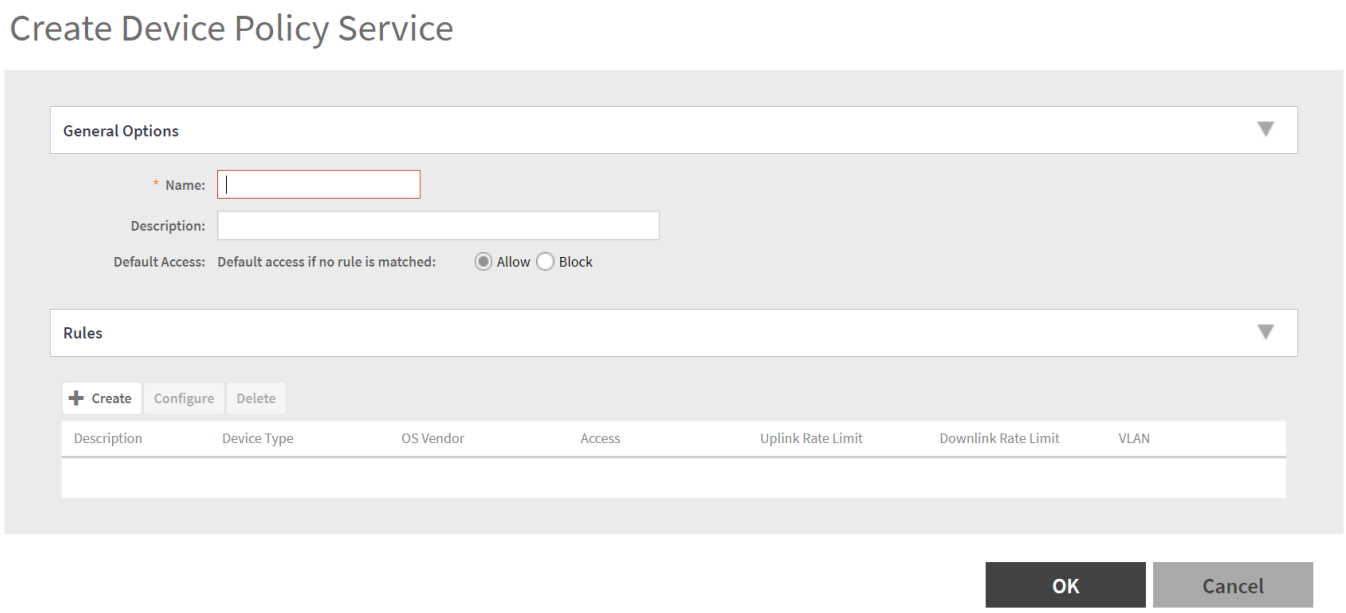
   This displays **Summary** and **Profiles** options.

2. Select **Profiles** tab.

   This displays **Device Policy Service** page.

   NOTE
   The Summary tab displays the device policy services in chart and graph format. Profiles can be filtered based on frequency, duration, APs and zone.

FIGURE 219 Create Device Policy Service



3. Enter the policy service details in the **General Options** section:
   a. **Name**: Enter a name for the device policy.
   b. **Description**: Enter a short description for this device policy.
   c. **Default Access**: Select either Allow or Block. This is the default action that the system will take if no rules are matched.
   d. Under **Rules** section, define the device policy rules. For more information, refer Creating Device Policy Rules on page 392.
   e. Click **OK**.

   NOTE
   You can also edit, clone, and delete a service by selecting the options Configure, Clone, and Delete respectively, from the Device Policy tab.

Enabling Device Policy Service

Enable device policy service. To enable the new device policy perform the following steps:

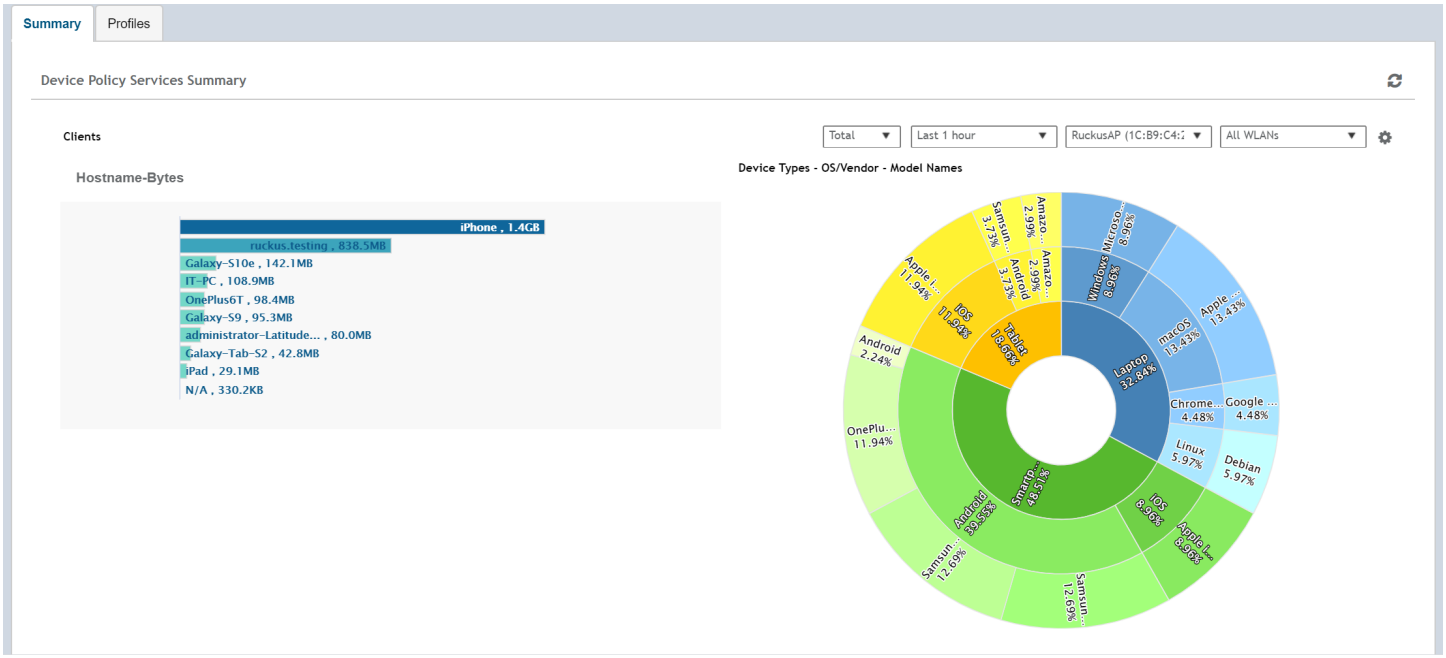
1. Click **Network** tab on the main menu.
2. Select **Wireless LANs**.
3. Select **Create/Configure** tab.
4. Scroll down to **Firewall Options** to enable the firewall profile.

Summary

The summary tab displays device hardware and software attributes as charts.

1. To view wireless client attributes, click **Security** > **Access Control** and select **Device Policy**. `This displays` **`Summary`** `and` **`Profiles`** `options.`
2. Select **Summary** tab. `This displays` **`Summary`** `page.`

FIGURE 220 Summary



The graph has 3 zones -

- Outer zone - Displays the model names of device types.
- Central zone - Displays information of the operating system used by the device type or the vendor name.
- Inner Zone - Displays the device type.
- Core - Displays the number of clients connected. (Hover the mouse to view the information).

The below table lists the filters available in the **Summary** screen.

TABLE 94 Filters

Filter Name	Description
Total/2.4GHz/5GHz	User can selet the radio options from the drop down menu to generate the report.
Last report/Last 1 hour/Last 24 hours	User can select the options from the drop down menu generate the report. Last report - Accumlates stats of 180 seconds from the Access Point. Last 1 hour - Accumlates stats of 60 minutes from the Access Point. Last 24 hours - Accumlates stats of 24 hours from the Access Point.
All APs	By default displays details of the Access Point selected from **Access Points** tab. User can select the option from drop down menu to view a particular AP or all APs.
All WLANs	Displays the WLANs associated with each AP. User can select the option from drop down menu to view a particular WLAN or all WLANs.
Settings - Clients	User can set the preferred display settings. **NOTE** The maximum clients displayed is 20.
Host name - Bytes	This displays traffic consumed per client.

Creating Device Policy Rules

Create rules for every device policy service.

1. Click **Security** > **Access Control** and select **Device Policy**.

   This displays **Summary** and **Profiles** options.

2. Select **Profiles** tab.

   This displays **Device Policy Service** page.

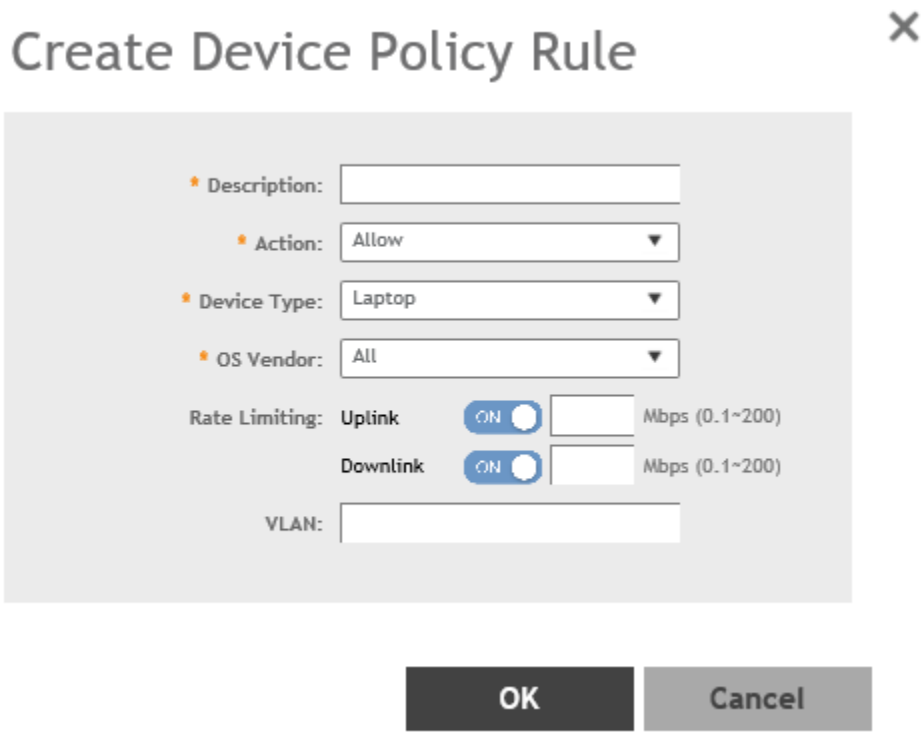
3. In the **Device Policy Service**, click **Create**.

   This displays **Create Device Policy Service**.

4. In **Create Device Policy Service** window, under **Rules**, click **Create**.

   This displays **Create Device Policy Rule** window.

   FIGURE 221 Creating a Device Policy Rule



5. Enter the following policy rule details:
   a. **Description**: Enter a short description for this device policy.
   b. **Action**: Select Allow or Block. This is the action that the system will take if the client matches any of the attributes in the rule.
   c. **Device Type**: Select from any of the supported device types. This feature is also supported on 11 AX APs.
   d. **OS Vendor**: Select from any of the supported OS types.
   e. **Rate Limiting**: Enable the uplink and downlink rate limiting, and enter a rate limit value for each.
   f. **VLAN** : Enter the number of the VLAN in which to segment the client type. The value ranges from 1 through 4094; if no value is entered, this policy does not impact device VLAN assignment.
   g. Click **OK**.

VLAN

VLAN Pooling

When Wi-Fi is deployed in a high density environment such as a stadium or a university campus, the number of IP addresses required for client devices can easily run into the thousands. Placing thousands of clients into a single large subnet or VLAN can result in degraded performance due to factors like broadcast and multicast traffic. VLAN pooling is adopted to address this problem.

VLAN pooling allows administrators to a deploy pool of multiple VLANs to which clients are assigned, thereby automatically segmenting large groups of clients into multiple smaller subgroups, even when connected to the same SSID. As the client device joins the WLAN, the VLAN is assigned to one of the VLANs in the pool based on a hash of the client's MAC address. To use the VLAN pooling feature, you first need to create a VLAN pooling profile, and then you can assign the profile to a specific WLAN or override the VLAN settings of a WLAN group.

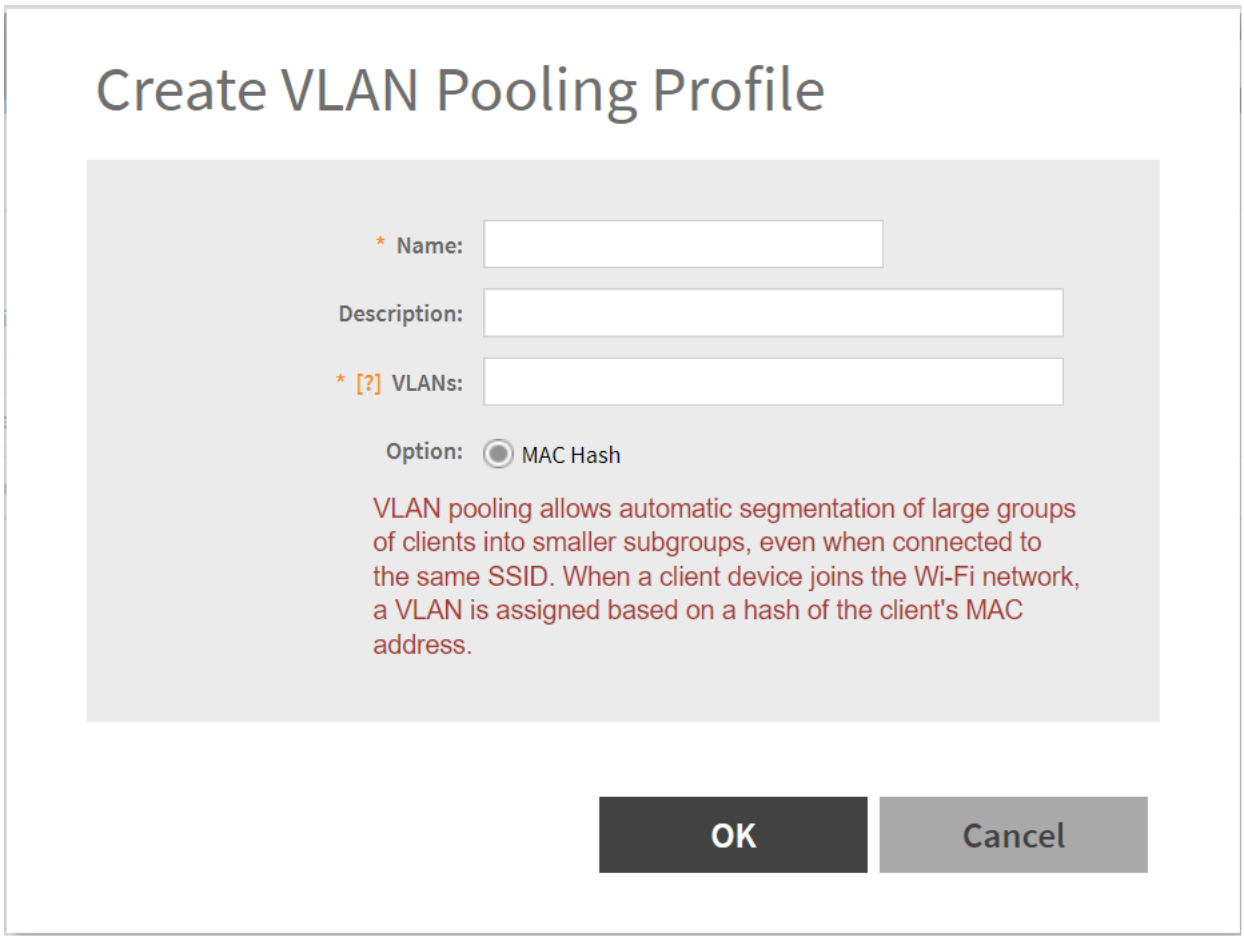
To create VLAN Pooling Profile, perform the following:

1. Click **Security** > **Access Control** > **VLAN** and select **VLAN Pooling**. This displays **`VLAN Pooling`** screen.
2. In the VLAN Pooling Profile screen, click **Create**. This displays `Create VLAN Pooling Profile` window.
3. Enter the Name, Description and VLANs details and click OK.
4. The new VLAN Pooling Profile is displayed in the **VLAN Pooling** page.

NOTE
By default, **Option MAC Hash** is selected.

NOTE
AP model: 11ac wave 2 supports a maximum of 64 VLANs. Other AP models support up to 32 VLANs.

FIGURE 222 Create VLAN Pooling Profile



VLAN Precedence

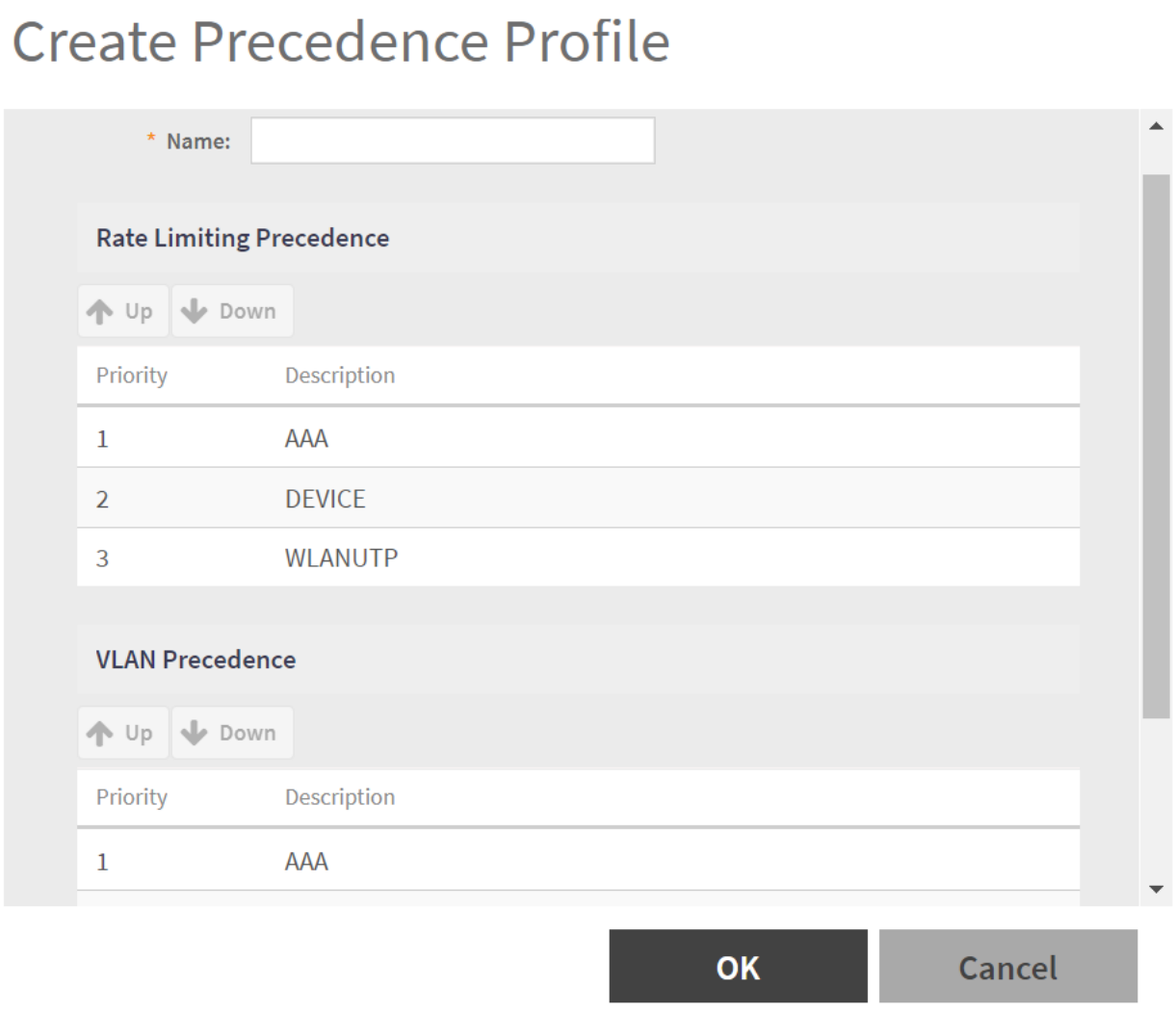
Clients are assigned to VLANs by various methods, and there is an order of precedence by which VLANs are assigned. The assignment is commonly done from lowest to highest precedence. You can also set precedence for Rate limiting attribute of the profile.

NOTE
Each VLAN has a default precedence.

1. To create VLAN Precedence, click **Security** > **Access Control** > **VLAN** and select **VLAN Precedence**. This displays **`VLAN Precedence`** screen.
2. Click **Create**.

   This displays **Create Precedence Profile** page.

FIGURE 223 Create Predence Profile



3. Configure the following:
   a. Name: Enter name of the profile.
   b. Rate Limiting Precedence: Use the Up and Down options to set the Rate Limit priority.

      NOTE
      When SSID Rate Limiting (restricts total usage on WLAN) is enabled, per-user rate limiting is disabled.

   c. VLAN Precedence: Use the Up and Down options to set the VLAN priority.
   d. Click **OK**.

You have created the Precedence profile.

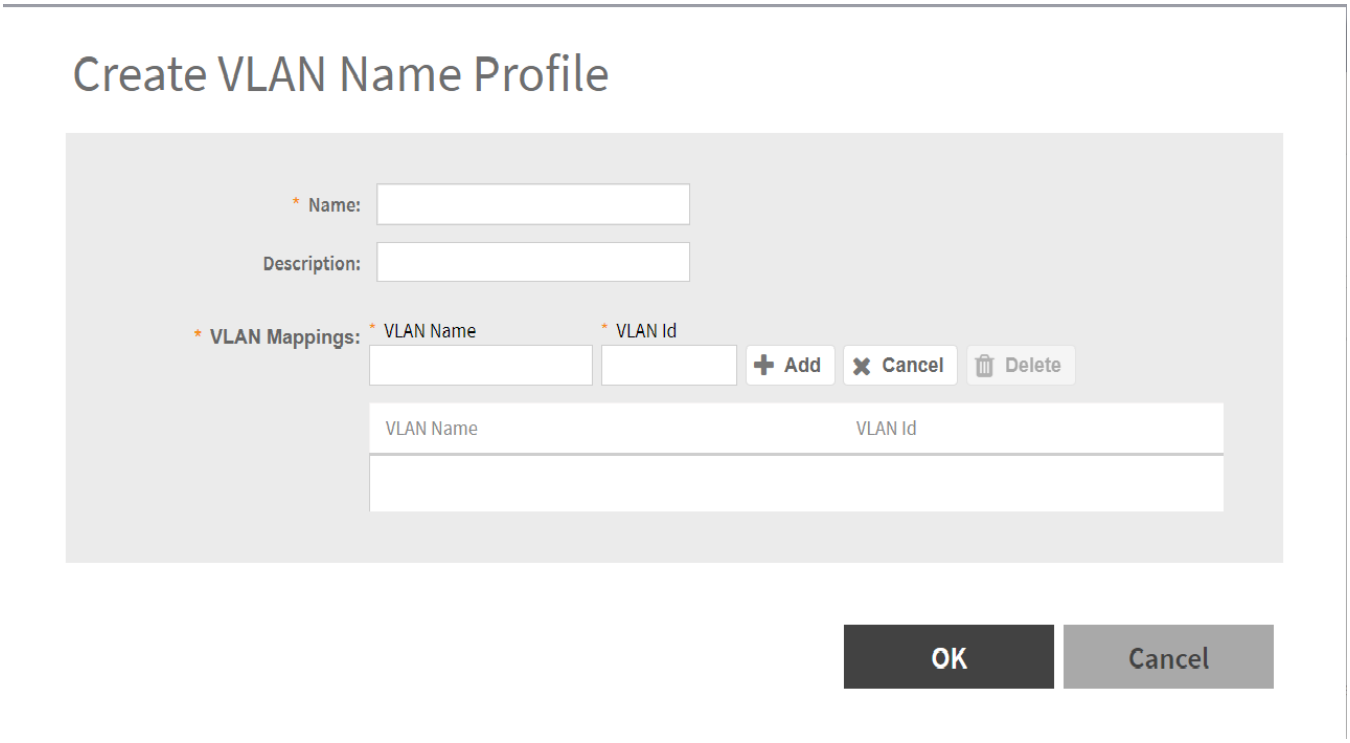
NOTE
You can also edit, clone and delete a profile by selecting the options **Configure**, **Clone** and **Delete** respectively, from the **Precedence** tab.

Creating VLAN Name Profile

Create VLAN Name Profile

1. To create VLAN Name Profile, click **Security** > **Access Control** > **VLAN** > **VLAN Name** This displays **`VLAN Name`** screen.
2. Select an Access Point from the tree and click **Create**.
   This displays **Create VLAN Name Profile** page.

FIGURE 224 Create VLAN Name Profile



3. Configure the following:
   a. Name: Enter name of the profile.
   b. Description: Enter a short description for the VLAN name profile.
   c. VLAN Mapping: Enter VLAN Name and VLAN ID and click **Add**.

The new VLAN name profile is displayed in the below list .

NOTE
You can also cancel or delete the new VLAN name profile .

Users and Roles

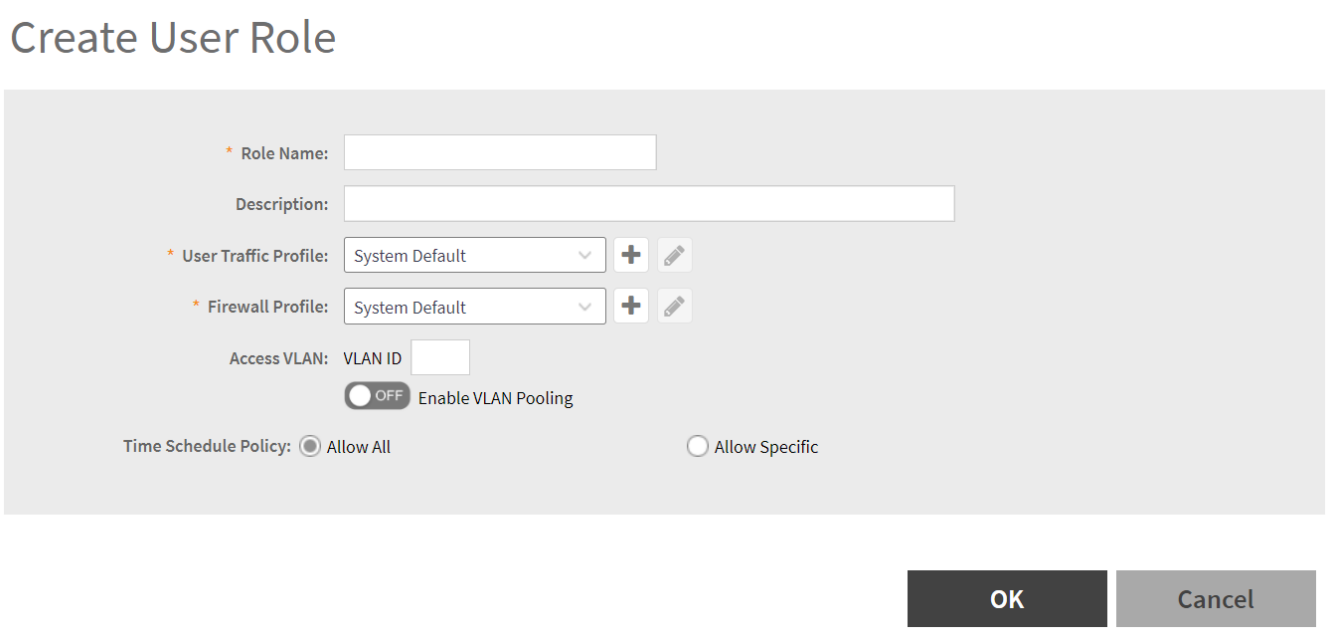
User Roles

An user role is created to limit user access or to allow them to log-in with non-standard client devices.

To create an user role, perform the following:

1. Click **Security** > **Access Control** > **Users & Roles** and select **User Roles**. This displays **`User Roles`** screen.
2. Click **Create**.
   This displays **Create User Role** page.

FIGURE 225 Create User Role



3. In the **Create User Role** window, configure the following:
   - Role Name - Enter name for the user role.
   - Description - Enter description for the user role.
   - User Traffic Profiles - Select user traffic profile from the drop-down menu or create user traffic profile by clicking the + mark. To create user traffic profile, refer *Create User Traffic Profile* .
   - Firewall Profile - Select firewall profile from the drop-down menu or create firewall profile by clicking the + mark. To create Firewall Profile, refer *Managing a Firewall Profile*.
   - Access VLAN - Provide a VLAN ID or select **Enable VLAN Pooling** and select the VLAN ID from the drop-down or create user traffic profile by clicking the + mark.
   - Time Schedule Policy - Select between the **Allow All** or **Allow Specific** options. By default, Allow All option is selected.
4. Click **OK**.

NOTE
You can also edit, clone and delete user roles by selecting the options **Configure**, **Clone** and **Delete** respectively, from the **User Roles** tab.

Local Users

A local user in the controller refers to a registered user who may be given access to the controller hotspot. An account comprises user's personal information, logon details, and the subscription package that is assigned to the user. The controller's local user database can include 802.1X, WISPr, and Zero-IT users.

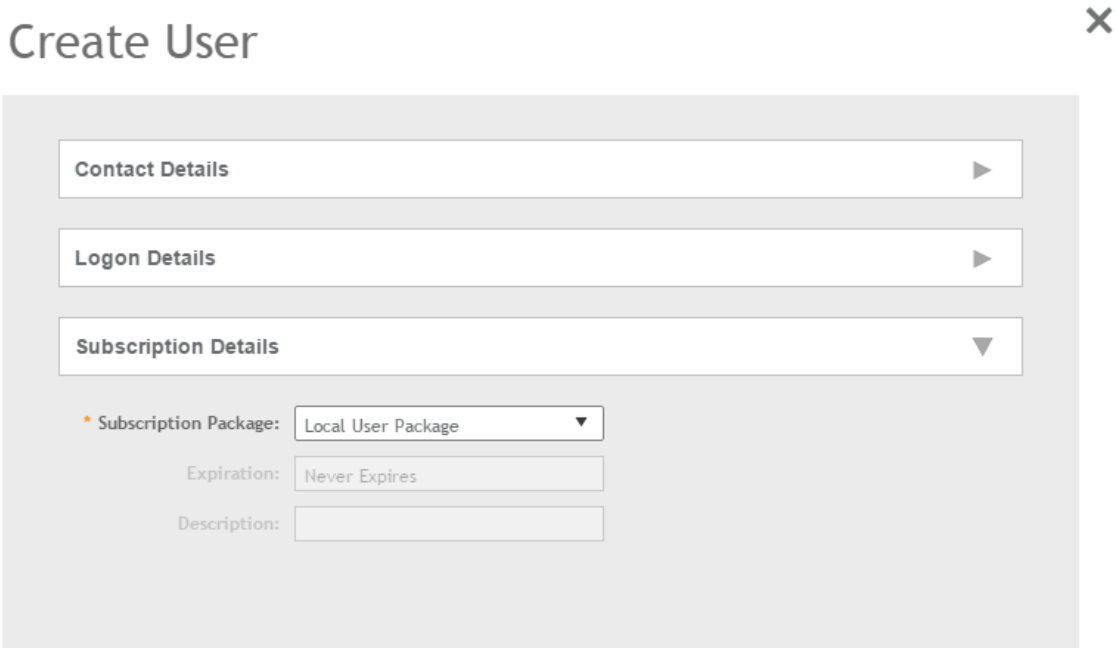
When you create a user account, you will be required to assign a subscription package to the user. Before creating a user account, RUCKUS recommends creating at least one subscription package. See Creating a Subscription Package on page 400 for more information.

1. Click **Security** > **Access Control** > **Users & Roles** and select **Local Users**. This displays **`Local Users`** window.

2. Click **Create**.

   The **Create User** page appears.

   FIGURE 226 Create User



3. In the **Create User** window, configure the following:
   a. In the **Contact Details** section, enter the following:
      - First Name
      - Last Name
      - Email
      - Phone
      - Address
      - City
      - State
      - Zip Code
      - Country
      - Remark
   b. In the **Logon Details** section, enter the details to create the logon credentials for this user:
      - User Name: Enter user name, this is not case sensitive and always displayed in lower case.
      - Password: Enter a password. The password must be at least eight characters in length.
      - Confirm Password: Re-type the password.
   c. In the **Subscription Details** section, select a subscription package from the drop-down menu to the new user.
4. Click **OK**.

You have completed creating a local user.

Select **Enable**, the new user profile is authorized. Select **Disable** to unauthorize the user.

You can view the list of local users by applying filters. Click the icon to do so.

NOTE
You can also edit, clone and delete user by selecting the options **Configure**, **Clone** and **Delete** respectively, from the **Local Users** tab.

Creating a Subscription Package

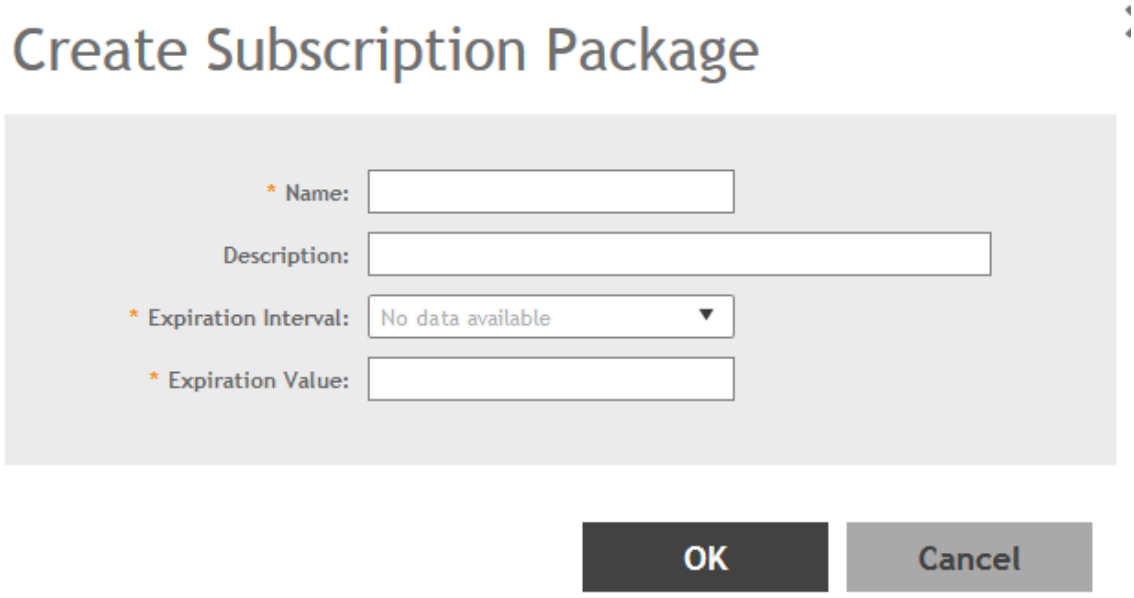
A subscription package defines the characteristics of a subscription that has been created for a registered user. These characteristics include the expiration date of the subscription.

If an user is connected at the time of subscription expiry, the user gets disconnected from the AP and any attempts to re-authenticate fails.

1. Click **Security** > **Access Control** > **Users & Roles** and select **Subscription Package**. This displays **`Subscription Package`** window.
2. Click **Create**.

   This dsiplays **Create Subscription Package** page.

FIGURE 227 Create Subscription Package



3. In the **Create Subscription Package** window, configure the following:
   - Name - Enter the subscription package name.
   - Description - Enter an approriate description for the new package.
   - Expiration Interval - Select the expiration time for the package expiration from the drop-down. Options are: Hour, Day, Week, Month, Year and Never.
   - Expiration Value - Enter the expiration value, if Hour, Day, Week, Month or Year is selected.
4. Click **OK**.

You have completed creating a subscription package.

NOTE
You can also edit and delete a package by selecting the options **Configure** and **Delete** respectively, from the **Subscription Package** tab.

Limitations Applying Role Policies to Users

You must be aware of some limitations in applying roles to a user.

- Role-based policies are only supported in proxy-mode AAA WLANs, where proxy AAA method is used for authentication. If the authentication method is non-proxy AAA, where the AP authenticates the user, the user equipment (UE) cannot be determined and therefore, user-role policies are not supported on non-proxy mode AAA WLANs.
- Typically, the RADIUS/AAA servers return a user attribute to the controller, and the controller assigns it to an UE. However, you must establish a mapping between the user attribute and the user role, so that the user role policy can be applied to the UE. The attribute-role mapping is configured within the AAA policy.
- User Traffic Profiles are configured with various policies such as rate limiting so when a profile is applied to a WLAN, the policies in the profile are applied to all the UEs in the WLAN. The policies can also be applied to a user role in a WLAN, but not all the polices defined in the profile are applied to the role.

  If a role-based VLAN policy is defined in the profile, it cannot be applied to the WLAN if its authenticated based on a L7 method (WebAuth or Hotspot/WISPr). This is because when a VLAN is applied on a per-role basis for a L7 authentication method, the user receives an IP address via DHCP before the UE is authenticated - this happens at layer 3 or 4, and you cannot authenticate the UE and assign a role to it till layer 7 is reached. This results in a mismatch between the VLAN IDs set within the roles, and could possibly lead to service disruptions.
- Precedence profiles are configured at the WLAN level, but impact the manner in which roles are assigned. The manner in which the profile is defined, indicates the order in which policies defined within the profile are assigned. The order of priorities can be customized. For example, if you have WLAN5 configured with VLAN ID 5, An OS policy configured with an iOS VALN ID 10, and a role policy assigned to a student with VALN ID 40, then there are multiple orders one can set when a *student user with iOS connects to WLAN 5*.
- You can assign a UE to a role through RADIUS, or you can use RADIUS attributes to apply policies. However, using RADIUS attributes take precedence over assigning UEs to a role (though it is easy to configure, as the only element required to authenticate the UE is the role information).

  In the RADIUS attributes method, each policy, such a rate limiting or user traffic profile has a unique RADIUS attribute. Therefore, specifying the RADIUS attribute for a policy will override all other forms of the controller policy. For example, if a UE is already assigned to VLAN 7 through RADIUS, setting a RADIUS attribute for VLAN IDs to 9 will override all VLAN=7 configurations in say WLANs, OS policies, role policies etc.

Guests

Guest Passes

Guest passes are temporary privileges granted to guests to allow access wireless LANs.

Many options are provided for customizing guest passes, controlling who is allowed to issue guest passes, and controlling the scope of access to be granted.

With Guest Pass authentication enabled, guests are required to enter a guest pass code when connecting to a guest WLAN. Temporary guest passes can be issued for single user, multiple users, one-time login, time-limited multiple logins for a single guest user, or can be configured so that a single guest pass can be shared by multiple users. Additionally, they can be batch generated, if many short-term guest passes must be created at once.

Guest passes can be generated in two ways:

- Self-Service Generated Guest Passes
- Admin Generated Guest Passes

After generating a guest pass, they can be delivered in the following ways:

- Printout
- Send SMS with guest credentials
- Send email with guest credentials

NOTE
To enable guest pass delivery through email or SMS, you must first configure an email server or an SMS delivery account (Twilio or Clickatell) from the **Email** tab or the **SMS** tab (**Services** > **Guest Access** .

Guest Pass

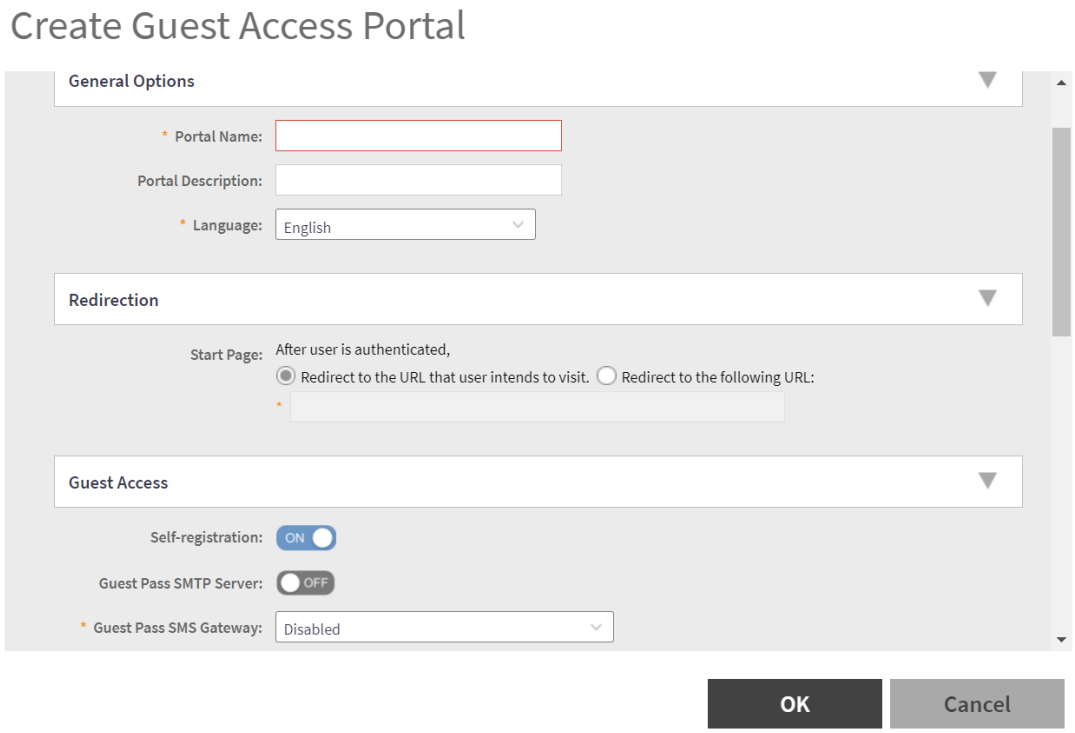
SmartZone Guest Pass Self Registration

Currently Smart Zone Guest Access solution relies on assisted guest pass generation, which means IT or hotel staff needs to generate guest password to the client based on whatever credentials needed. To make the process simpler and for ZD parity, this feature is to make guest self-registration a possibility on SZ, so that steps can be configured and displayed on guest UE to guide them through a step by step process to obtain a key for the guest WLAN access.

Self-service guest pass registration only applies to guest access WLAN.

- Go to **Services** > **Guest Access**.
- Click "Create" to access the Guest pass Portal.
- Enable "Self Registration" by setting it to "ON" position.

FIGURE 228 Self Registration



If the sponsor approval is disabled, when end-user connects to the WLAN, user can finish the registration and get the guest password automatically without any approval.

Admin Generated Guest Passes

Guest passes allow temporary access to wireless LANs.
Step 1: Create a Guest Access Service

1. Follow the instructions in **Creating a Guest Access Portal** to create at least one guest access service in Guest Access Portal.
2. When you finish creating a guest access service, continue to Step 2: Create a Guest Access WLAN on page 403.

Step 2: Create a Guest Access WLAN

Guest passes are generated for specific WLANs only. Guest pass users will only be able to gain access to the WLANs for which the guest pass is generated.

Follow these steps to create a WLAN that will be used for guest access only.

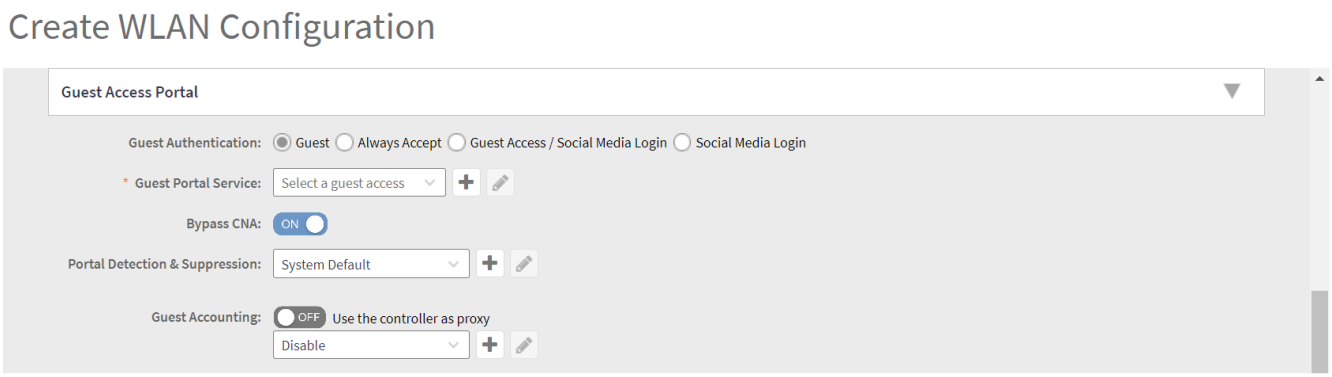
1. Click **Network** > **Wireless LANs**.

   The **Wireless LANs** page appears.
2. Select an Access Point from the tree hierrachy and click **Create**.

   The **Create WLAN Configuration** page appears.
3. In the **Authentication Options**, select **Guest Access**. This displays the **Guest Access Portal** section.

4. In the **Guest Access Portal**, configure the following:
   a. Guest Authentication: Select the option approriately.
   b. Guest Service Portal: Select the guest access from the drop-down list or create guest access portal by clicking the + icon.
   c. Bypass CNA: By default, this option is selected, undo if it is not required.
   d. Portal detection & Suppression: This option is available only when the **Bypass CNA** is selected. Choose from the drop-down list or create a Portal detection & Suppression by clicking the + icon.
   e. Guest Accounting: By default, this option is disabled. Choose from the drop-down list or create AAA server by clicking + icon.
5. When you finish creating a guest access WLAN, continue to Admin Generated Guest Passes on page 403.

FIGURE 229 Creating a WLAN for guest access only



Step 3: Generate a Guest Pass

Follow these steps to generate a guest pass.

1. Click **Security** > **Access Control** > **Guests** and select **Guest Pass**. This displays **`Guest Pass`** window with two sections:
2. In the **Self-Service Generated Guest Passes** section, click on **Generate Guest Pass** and configure the following:
   - **Guest Name** - Enter guest name.
   - **Guest WLAN** - Select the guest WLAN from the drop down menu. To create guest WLAN, refer Step 2: Create a Guest Access WLAN on page 403.
   - **Number of Passes** - Enter number of guest passes to be generated.
   - **Pass Valid For** - Set the validity for the guest pass by entering the number and selecting the period from the drop-down menu. For example, if you want the guest pass to be valid for seven days, type **7** in the first box, and then select **Days** in the second box.

3. Configure the advanced options:
   a) **Pass Generation** - Select **Auto Generate** check box, if to generate the guest pass key automatically.

      To generate guest pass manually, clear **Auto Generate** check box.

      If generating multiple guest pass, the **Auto Generate** check box is not configurable.

   b) **Pass Effective Since** - Set the guest pass validity period by selecting one of the following options:
      - **Effective from the creation time** - This type of guest pass is valid from the time it is created to the specified expiration time, even if it is not being used by any end user.
      - **Effective from first use** - This type of guest pass is valid from the time the user uses it to authenticate with the controller until the specified expiration time. An additional parameter (Guest Pass will expire in X days) can be configured to specify when an unused guest pass will expire regardless of use. The default is 7 days.
      - **Expire new guest pass if not used within [ ] days** - If you want this guest pass to expire if it is unused after you generated it, type the number of days in the box (maximum value is 365 days).

   c) **Max Devices Allowed** - Set the number of users that can share this guest pass.
      - **Limited to [ ]** - If you want a limited number of users to share this guest pass, click this option, and then type the number in the box.
      - **Unlimited** - If you want an unlimited number of users to share this guest pass, click this option.
      - **Session Duration** - If you clicked **Unlimited**, this option appears. If you want require users to log on again after their sessions expire, select the **Require guest re-login after [ ]** check box, and then select a time increment. If this feature is disabled, connected users will not be required to re-log in until the guest pass expires.

   d) In **Remarks** (optional), type your notes about this guest pass, if any.
4. Click **Generate**.

   The page refreshes, the guest pass generated appears in the **Admin Generated Guest Passes** table, along with other guest passes that exist on the controller.

   Select the guest pass and click **Enable** to authorize the guest pass for a user, and **Disable** to revoke the guest pass for a particular user.

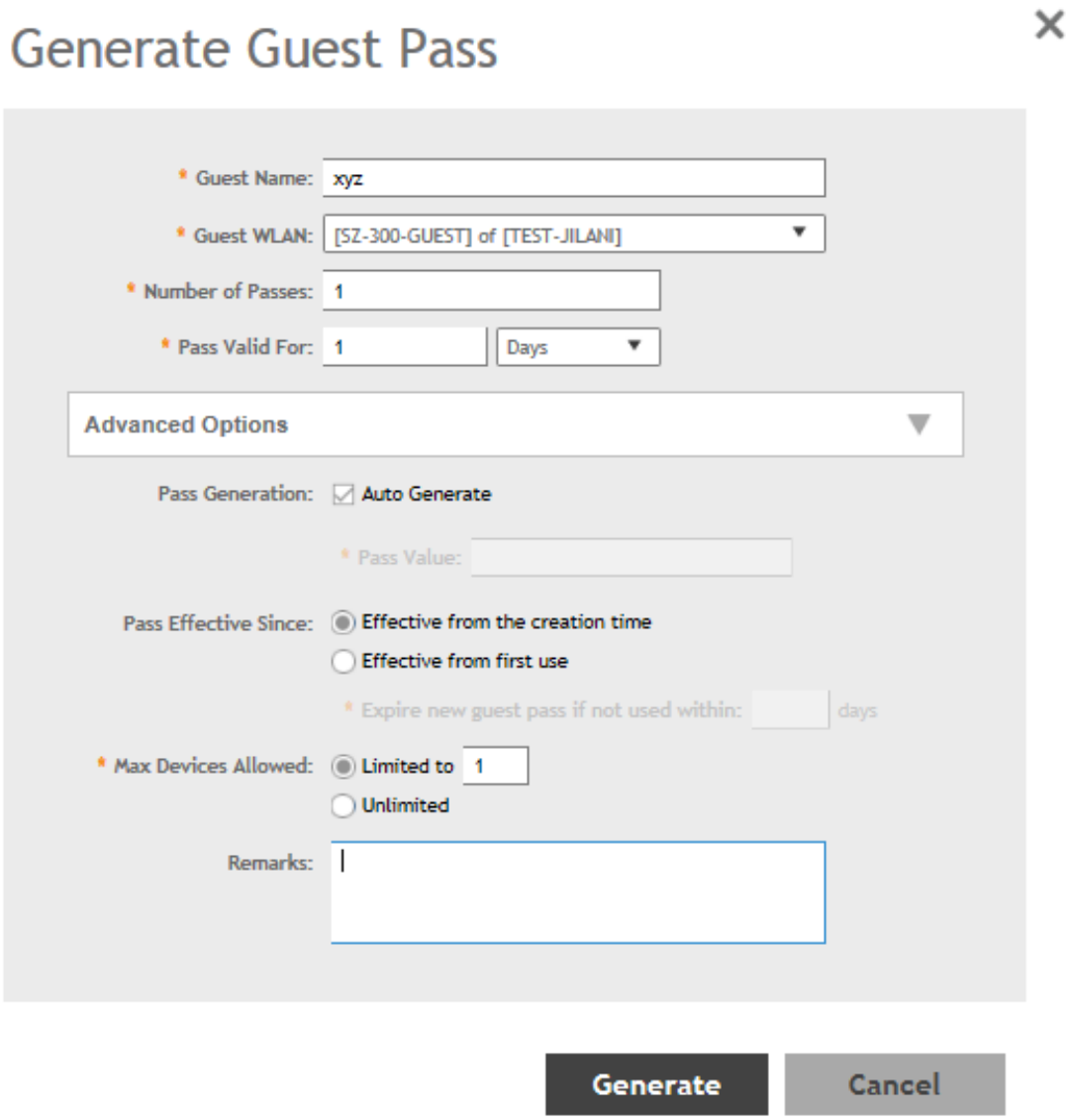
You have completed generating a guest pass. You are now ready to send the guest pass to guest users.

You can view the list of guest passes by applying filters. Click the  icon to do so.
The following information is displayed when you click on the guest pass created:

- Summary: Displays a summary of information about the user and credentials.
- Admin Activities: Displays information about the administrator activities.
- Event: Displays information about events associated with the user.

  Click the  icon to apply filters. Click the  icon to export all the data into a CSV file.

FIGURE 230 Generating a guest pass



NOTE
You can generate maximum 120000 guest passes for SZ100, and 40000 guest passes for vSZ-E.

NOTE
You can generate maximum 40000 guest passes for SZ300, and 1000000 guest passes for vSZ-H.

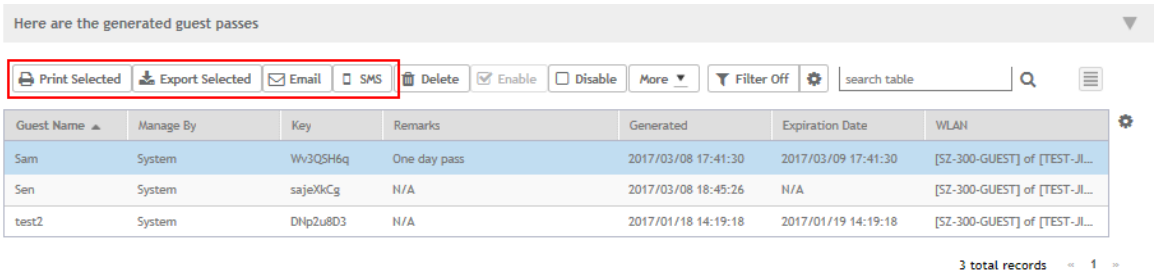
NOTE
The controller GUI allows you to view only 1000 guest passes. To view the guest pass list above 1000 passes, you must use the public API's.

Step 4: Send Guest Passes to Guest Users

Deliver the guest passes to guest users as per the delivery options that you choose.

The page that appears after you generate a guest pass contains options for delivering the guest pass to guest users (see the following image).

FIGURE 231 Options for delivering guest passes to guest users



Generating Guest Passes from an Imported CSV

You can also manually define the guest passes that you want to generate in a comma-separated value (CSV) file (a sample of which is available for download from the **Guest Pass** page).

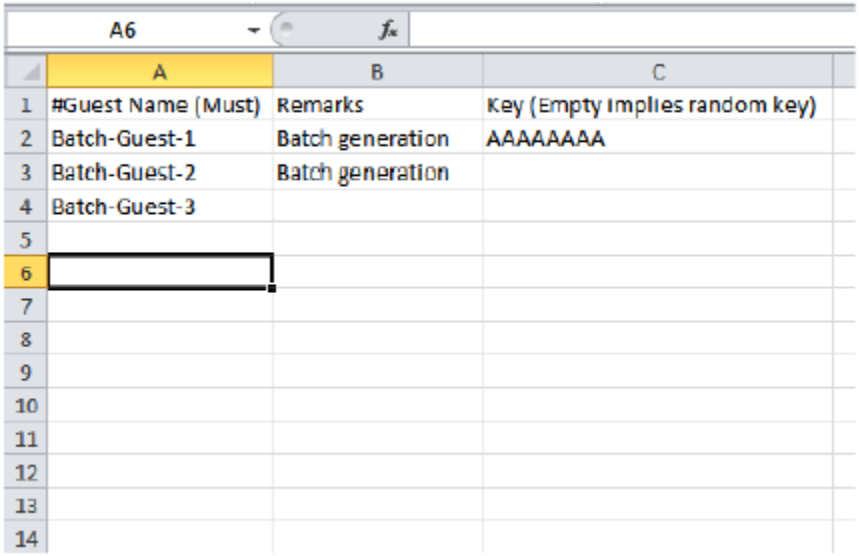
Follow these steps to generate guest passes from an imported CSV file.

1. Click **Security** > **Access Control** > **Guest** > **Guest Pass**.
2. Click **Import Guest Pass**.

   The **Import Guest Pass** form appears.
3. Look for the following text under Browse:

   `To download a sample guest pass, click here.`
4. Click the **here** link to download the sample CSV file.
5. Using Microsoft Excel or a similar application, open the CSV file.
6. In the CSV file, fill out the following columns:
   - #Guest Name (Must): Assign a user name to the guest pass user.
   - Remarks (Optional): Add some notes or comments about this guest pass.
   - Key: Enter a guest pass key or leave it blank so the controller can generate the key automatically.

   FIGURE 232 The sample CSV file when opened in Excel



7. Save the CSV file.
8. Go back to the **Import Guest Pass** page, and then configure the following settings on the Common Guest Pass Settings:
   - **Guest WLAN**: Select the guest WLAN that you created in Step 2: Create a Guest Access WLAN on page 403.
   - **Pass Valid For**: Set the validity period for the guest pass by filling in the two boxes. For example, if you want the guest pass to be valid for seven days, type **7** in the first box, and then select **Days** in the second box.
9. Configure the advanced options:
   a) **Pass Effective Since**: Set the guest pass validity period by selecting one of the following options:
      - **Effective from the creation time**: This type of guest pass is valid from the time it is first created to the specified expiration time, even if it is not being used by any end user.
      - **Effective from first use**: This type of guest pass is valid from the time the user uses it to authenticate with the controller until the specified expiration time. An additional parameter (**Guest Pass will expire in X days**) can be configured to specify when an unused guest pass will expire regardless of use. The default is 7 days.
      - **Expire guest pass if not used within [ ] days**: If you want this guest pass to expire if it is unused after you generated it, type the number of days in the box (maximum value is 365 days).

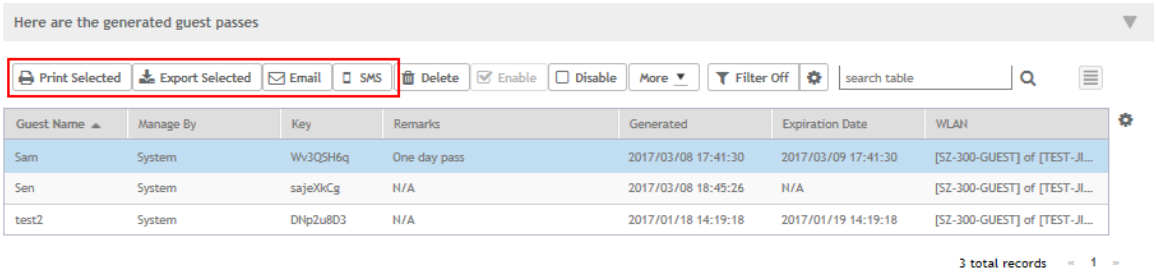
   b) **Max Devices Allowed**: Set the number of users that can share this guest pass.
      - **Limited to [ ]**: If you want a limited number of users to share this guest pass, click this option, and then type the number in the box.
      - **Unlimited**: If you want an unlimited number of users to share this guest pass, click this option.
      - **Session Duration**: If you clicked **Unlimited**, this option appears. If you want require users to log on again after their sessions expire, select the **Require guest re-login after [ ]** check box, and then select a time increment. If this feature is disabled, connected users will not be required to re-log in until the guest pass expires.
10. In **Guest List CSV File** (at the top of the page), click **Browse**, and then select the CSV file you edited earlier.

    The page refreshes, and the number of guest passes that the controller has identified in the CSV file appears below the **Browse** button.
11. Click **Import**.

    The page refreshes, and then the guest pass you generated appears in a table, along with other guest passes that exist on the controller.

You have completed generating a guest pass. You are now ready to send the guest pass to guest users. See Step 4: Send Guest Passes to Guest Users on page 406 for information.

FIGURE 233 The Guest Pass page for importing a CSV file



Guest Pass Template

Creating a Guest Pass Template

A guest pass template is a HTML file which contains variables for the information that guest users need to connect to the controller hotspots (for example, guest name, key, and WLAN name), and actual instructions for connecting to the guest WLAN.

A default printout template exists in the controller. If you want to create your own printout template, follow these steps.

1. Go to **Security** > **Access Control** > **Guest Pass Template**.

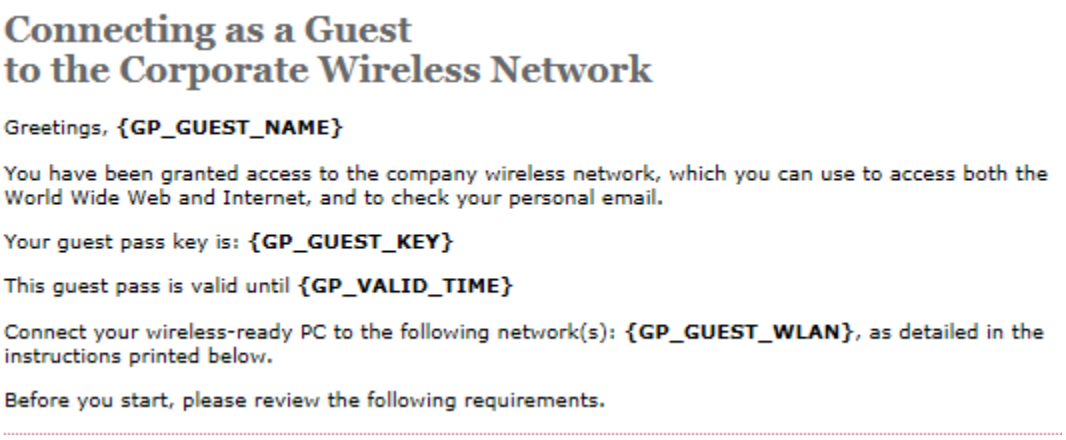
   NOTE
   For SmartZone 5.2.1 or earlier releases, go to **Clients** > **Guests**. Click the **Guest Pass Template**.

   The **Guest Pass Template** page appears.
2. In the **Guest Instruction HTML Template** section, click `default.html`, which is the default guest pass printout template.

   The content of the default guest pass printout template appears in the *Name: default.html*
3. Click **Download** below the template preview area to download a copy of the template to your computer.
4. Using an HTML editor, create a new HTML file.
5. Add content to the file.

   Typically, a printout template contains instructions for connecting to the controller hotspot. See the following image for the content of the default printout template.

   FIGURE 234 Content of the default printout template

6. Insert the following variables into the content of your template:
   - *{GP_GUEST_NAME}*: This is the guest pass user name.
   - *{GP_GUEST_KEY}*: This is the guest pass key.
   - *{GP_VALID_TIME}*: This is the expiration date and time of the guest pass.
   - *{GP_GUEST_WLAN}*: This is the WLAN with which the guest user can associate using the guest name and guest key.
7. Save the file.
8. In the **Guest Instruction HTML Template** page, click the **Upload** button for the template that you are creating.

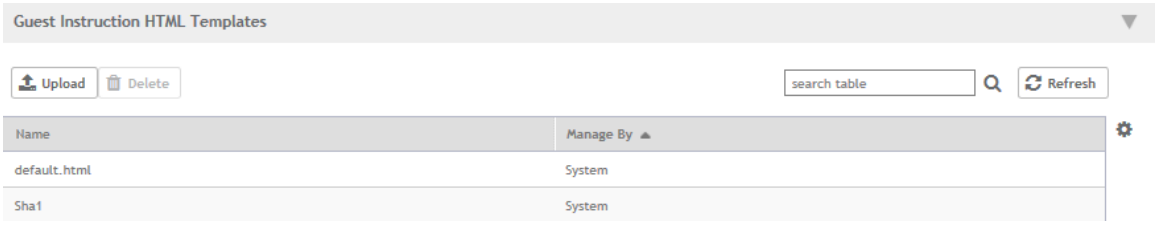
   The **Upload a Template File** form appears on the right side of the page.

9. Configure the **Upload a Template File** options:
   - **Template Name**: Type a name for the template that you are uploading.
   - **Template File**: Click **Browse**, and select the template file you created.
10. Click **Upload**.

    An information message box appears and informs you that the template file has been uploaded successfully.
11. Click **OK**.

    The template file you uploaded now appears in the list of templates.

FIGURE 235 The **Upload a Template File** form



Creating a Guest Instruction SMS Template

A guest SMS template is a text file which contains variables for the information that guest users need to connect to the controller hotspots (for example, guest name, key, and WLAN name), and actual instructions for connecting to the guest WLAN.

A default printout template exists in the controller. If you want to create your own printout template, follow these steps.

1. Go to **Security** > **Acesss Control** > **Guest Pass Template**.

   NOTE
   For SmartZone 5.2.1 or earlier releases, go to **Clients** > **Guests**. The **Guest Pass Template** page appears.

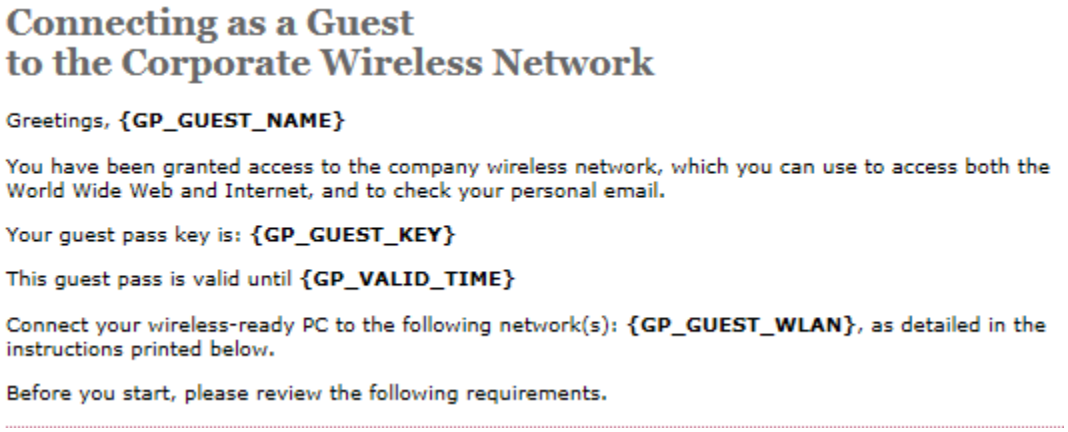
2. In the **Guest Instruction SMS Template** section, click `default.txt`, which is the default guest pass printout template.

   The content of the default guest pass printout template appears in the *Name: default.txt*.
3. Click **Download** below the template preview area to download a copy of the template to your computer.
4. Using an HTML editor, create a new text file.

5. Add content to the file.

   Typically, a printout template contains instructions for connecting to the controller hotspot. See the following image for the content of the default printout template.

   FIGURE 236 Content of the default printout template



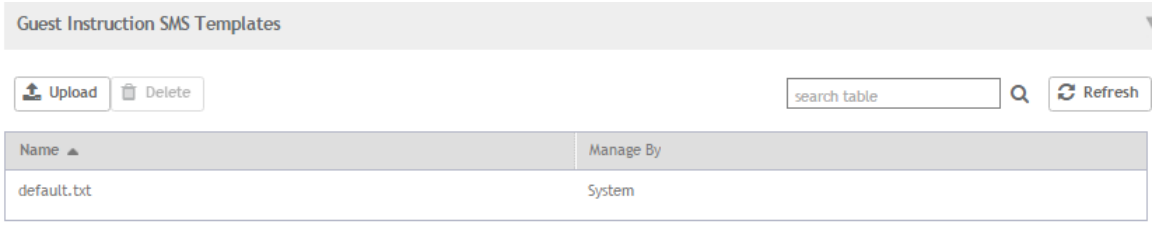
6. Insert the following variables into the content of your template:
   - *{GP_GUEST_NAME}*: This is the guest pass user name.
   - *{GP_GUEST_KEY}*: This is the guest pass key.
   - *{GP_VALID_TIME}*: This is the expiration date and time of the guest pass.
   - *{GP_GUEST_WLAN}*: This is the WLAN with which the guest user can associate using the guest name and guest key.
7. Save the file.
8. In the **Guest Instruction SMS Template** page, click the **Upload** button for the template that you are creating.

   The **Upload a Template File** form appears on the right side of the page.
9. Configure the **Upload a Template File** options:
   - **Template Name**: Type a name for the template that you are uploading.
   - **Template File**: Click **Browse**, and select the template file you created.
10. Click **Upload**.

    An information message box appears and informs you that the template file has been uploaded successfully.
11. Click **OK**.

    The template file you uploaded now appears in the list of templates.

    FIGURE 237 The **Upload a Template File** form



Dynamic PSK

Generating Dynamic PSKs

You can generate new dynamic PSKs to secure the WiFi network.

Follow these steps to generate the dynamic PSKs (DPSKs):

1. Click **Security** > **Access Control** > **Dynamic PSK**. This displays **`Dynamic PSK`**screen.
2. Click **Generate DPSKs**.

   This displays **Generate DPSKs** window .
3. In the **Generate DPSKs** window, configure the following:
   - **WLAN**: Select a DPSK-enabled WLAN from the drop-down list.
   - **Number of DPSKs**: Enter the number of PSKs to be created in a zone. A maximum of 500 Unbound or Group DPSKs can be created in one form submission.

     There are three types of DPSKs:

     - Unbound DPSK (DPSK not binding to a specific device yet) - Once an unbound DPSK is used by a device, it will become bound DPSK and release one slot from the maximum limit of 500.
     - Group DPSK (DPSK that can be shared between devices) - A group DPSK will never become bound, it always occupy one slot from the 500 limit, until the Admin deletes.
     - Bound DPSK (DPSK bound to a specific device) - An Admin can import Bound DPSKs using CSV by specifying the **MAC Address** and create Bound DPSKs regardless of the 25,000 limitation.

SZ version	Max DPSK per zone	Max Unbound DPSK per zone	Max Group DPSK per zone
3.4.x	10K	256	X
3.5.x	10K	256	64
3.6.x	10K	Share 320 slots for Unbound and Group DPSKs	
5.1	25K	Share 500 slots for Unbound and Group DPSKs	
6.1.0	25K	Share 5000 slots for Unbound and Group DPSKs	

     NOTE
     For SZ300/vSZ-H platform, the maximum number of DPSKs is 25,000 per zone or domain and 50,000 for the system.

   - **User Name**: Enter the user name manually or leave it blank if you want the controller to auto-generate the user name.
   - **Passphrase**: Enter the user name manually or leave it blank if you want the controller to auto-generate the passphrase.
   - **User Role**: If you have created user roles, select the user role to assign to the device that connects to the SmartZone network using this DPSK. The device will be assigned the same attributes and permissions (VLAN, UTP, time restrictions, etc.) that have been defined for the assigned user role.
   - **VLAN ID**: Type a VLAN ID within the range 1-4094.
   - **Group DPSK**: If you want multiple devices to be able to use this DPSK, click **Yes** else, click **No** if it used by a single device.
4. Click **Generate**.

You have completed creating dynamic PSKs.

To delete a DPSK, select the DPSK from the list, and then click the **Delete** icon.

Importing Dynamic PSKs

You can import CSV files to create DPSKs to secure the WiFi network.

Follow these steps to import dynamic PSKs (DPSKs):

1. Click **Security** > **Access Control** > **Dynamic PSK**. This displays **`Dynamic PSK`**screen.
2. Click **Download Sample (CSV)** link to download the CSV template for generating DPSKs.

   A sample CSV file is displayed as show in the figure.

   FIGURE 238 Sample CSV file

A	B	C	D	E	F
User Name	MAC Address	VLAN ID	User Role	Passphrase	Group DPSK
DPSK-User-1	00:11:22:33:44:44				
DPSK-User-2	00:11:22:33:44:55	1		passphrase02	
DPSK-User-3	11:22:33:44:55:66	2	testUserRole	passphrase03	
Group-DPSK-1					Y

3. Modify the CSV file as appropriate and save it. The following are the fields that need to be completed in the CSV file:
   - **User Name** (mandatory field): Enter the user name.
   - **MAC Address** (optional): Enter the MAC address of the device for which to generate a DPSK (bound DPSK). If you leave the MAC address field empty, the controller will generate an unbound DPSK.
   - **VLAN ID** (optional): Enter a value to override the WLAN VLAN ID, or leave it empty if you do not want to override the WLAN VLAN ID.
   - **User Role** (optional): If you have created user roles, type the name of the user role that you want to assign to the device that connects to the SmartZone network using this DPSK. The device will be assigned the same attributes and permissions (VLAN, UTP, time restrictions, etc.) that have been defined for the assigned user role.
   - **Passphrase** (optional): Leave it blank if you want the controller to auto-generate the passphrase, or enter the passphrase manually.
   - **Group DPSK** (optional): Enter **Y** to indicate the entry is a Group DPSK if you want multiple devices to use this DPSK.
4. Click **Import CSV**.

   The **Import CSV** dialog box appears.

   NOTE
   Importing a CSV file that contains a MAC address to which an existing DPSK (on the same target WLAN) is already assigned will replace the existing DPSK on the controller database.

5. In **DPSK Enabled WLAN**, select a WLAN from the drop-down list. Only WLANs that support DPSK must be selected.
6. In **Choose File**, click **Browse** to choose the CSV file.

   Click **Clear** if you want to replace the CSV file.

   You can also specify **Group DPSK** in the CSV file.
7. Click **Upload**.

   The generated DPSKs appear in the table on the **Dynamic PSK** page.

   NOTE
   You can import up to 1,000 DPSKs (not over 25K unbound + group DPSKs) at a time.

8. Click **Download CSV** to download a CSV that contains the generated DPSKs.

   The CSV file appears in the following format.

   FIGURE 239 New CSV format

User Name	MAC	WLAN (SSID)	Passphrase	VLAN ID	Created Date	Expiration Date
DPSK-User-1	00:11:22:33:44:44	joe-wlan (joe-wlan)	4#4BSXMe		3/17/2016 18:55	Unlimited
DPSK-User-2	00:11:22:33:44:55	joe-wlan (joe-wlan)	rE<r0[]y	1	3/17/2016 18:55	Unlimited
DPSK-User-3	11:22:33:44:55:66	joe-wlan (joe-wlan)	'q=7vqfE	2	3/17/2016 18:55	Unlimited

You have completed generating DPSKs.

NOTE
Click **Export All** to export all the dynamic PSKs to a CSV file. You can also export specific dynamic PSKs by selected them and clicking **Export Selected**.

Creating a User Traffic Profile

A User Traffic Profile (UTP) can be created to block or limit user traffic based on a number of factors including Source and destination IP address, Port, Protocol, etc. Additionally, a UTP can be created to shape traffic according to configurable application control policy.

To create a user traffic profile, perform the following:

1. Click **Security** and **User Traffic Profile** tab. This displays **User Traffic Profile** window.
2. In **User Traffic Profile** screen, click **Create**. This displays **Create User Traffic Profile** window. In the create user traffic profile window, configure the following:
   - Name - Enter name for the profile.
   - Description - Enter short description for the profile.
   - Rate Limiting - By default, Uplink and Downlink buttons are set to Off. User can select the button to limit the upload and download by entering values.
3. Select an access control for the user profile from the **Traffic Access Control List** and set priority by selecting the rule. To create a traffic control access rule, refer *Creating a User Traffice Access Control Rule*.
4. Select an application policy from the **Application Recoginition and Control** list. To create an application policy, refer *Creating an Application Control Policy*.
5. Select an URL filtering policy from the **URL Filtering Control** list. To create an application policy, refer *Creating a URL Filtering Policy*.
6. Click **OK** to save the new User Traffic Profile.

NOTE
Use **Configure**, **Clone** and **Delete** options in the **Create User TrafficProfile** window to edit, clone or delete.

Restricted Access

The Restricted Access profile can be created without having any blocked ports or enabling well known and any entries in the whitelist ports. Restricted Access Point(AP) profile can be configured multiple ways through SmartZone user interface.

The access point node on the network can be vulnerable to malicious attacks. Access Point(AP) is a critical node on the network and therefore such an attack can expose the whole network. The restricted access profile provides a mechanism to restrict unauthorized access to the AP and allows access only to authorized users thereby increasing the AP's inherent security.

NOTE
Maximum of 5 Restricted AP Access profiles can be created per zone.

The AP currently has the following categories of open ports:

TABLE 95 Well Known Ports on Access Points

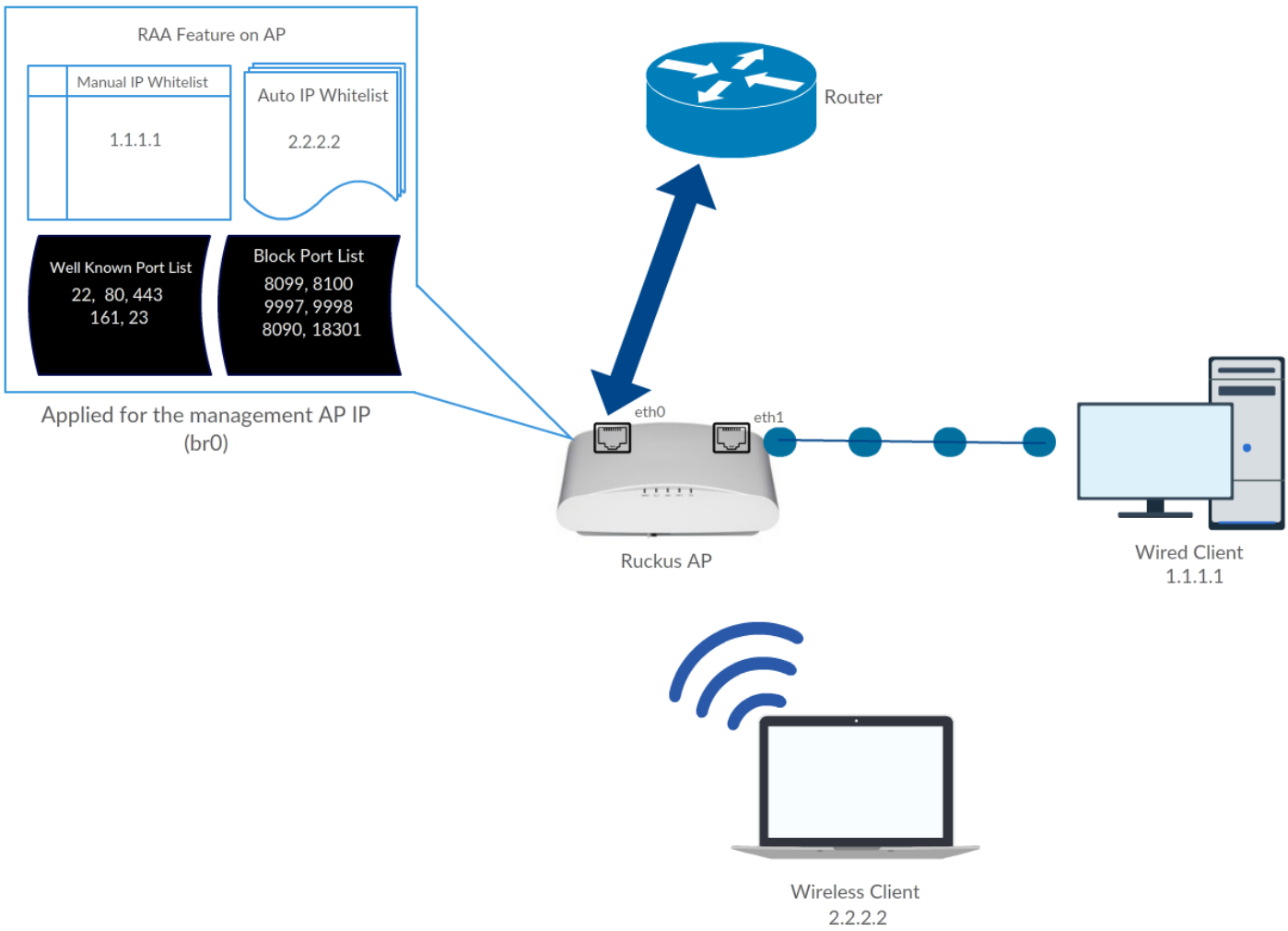
Sl. No.	Port	Use	Protocol
1	80	HTTP	TCP - IPv4 & IPv6
2	22	SSH	TCP - IPv4 & IPv6
3	443	HTTPS	TCP - IPv4 & IPv6
4	161	SNMP	UDP - IPv4 & IPv6
5	23	TELNET	TCP - IPv4 & IPv6

Overview

The Well known Port List includes the ports that are most likely to be exploited, with restricted access enabled, any node on the network trying to access the AP using these ports is blocked. This blocking functionality is configurable from the user interface by an administrator. The administrator can perform the following functions:

- The administrator can allow temporary or permanent access to these ports for an IP or a list of IPs (IP and Subnet). These IP(s) when configured are added to the Manual White List (Max 10) and these IP(s) are given unrestricted access to the AP.
- The administrator can add ports or a range of ports to the Port Black List (Max 10) as well. These ports will be inaccessible for any node on the network that is not part of the Manual White List as configured by the administrator.

FIGURE 240 Restricted Access Overview



Creating Restricted AP Access Profile

The Access Point (AP) is a critical node in the network that can be at risk of the malicious attacks as some of its ports are open. The Restricted AP Access Profile addresses this kind of risk and enhances AP's security.

Restricted AP Access protects the AP in the following ways.

1. By blocking access to the AP's standard well know open ports such as:
    - Port- 22 (TCP -IPv4 & IPv6) - For SSH Operation
    - Port- 23 (TCP - IPv4 & IPv6) - For Telnet Operation
    - Port- 80 (TCP - IPv4 & IPv6) - For HTTP Operation
    - Port- 443 (TCP - IPv4 & IPv6) - For HTTPs Operation
    - Port- 161 (UDP -IPv4 & IPv6) - For SNMP Operation

2. By blocking access to AP's Internal ports (used mainly for Ruckus internal communication) such as:
   - Wisper internal ports
     - Port 9997 (http) : [Subscriber portal]
     - Port 9998 (https): [Subscriber portal]
     - Port 1997 (http): [Captive Portal Listening Server]
     - Port 1998 (https): [Captive Portal Listening Server]
   - Walled Garden internal Ports
     - Port 8090 (http) : [Subscriber portal]
     - Port 8099 (https) : [Subscriber portal]
     - Port 18090 (http) : Captive Portal Listening Server /Redirect server listen port]
     - Port 18099 (https): Captive Portal Listening Server/Redirect server listen port]
   - Speedflex Port 18301
   - Proxy Web server for Unauthorized UEs 8100
   - DNSMASQ 53
3. By providing a mechanism to block any ports or port range to restrict access.
4. By allowing AP to be accessed by authorized users.

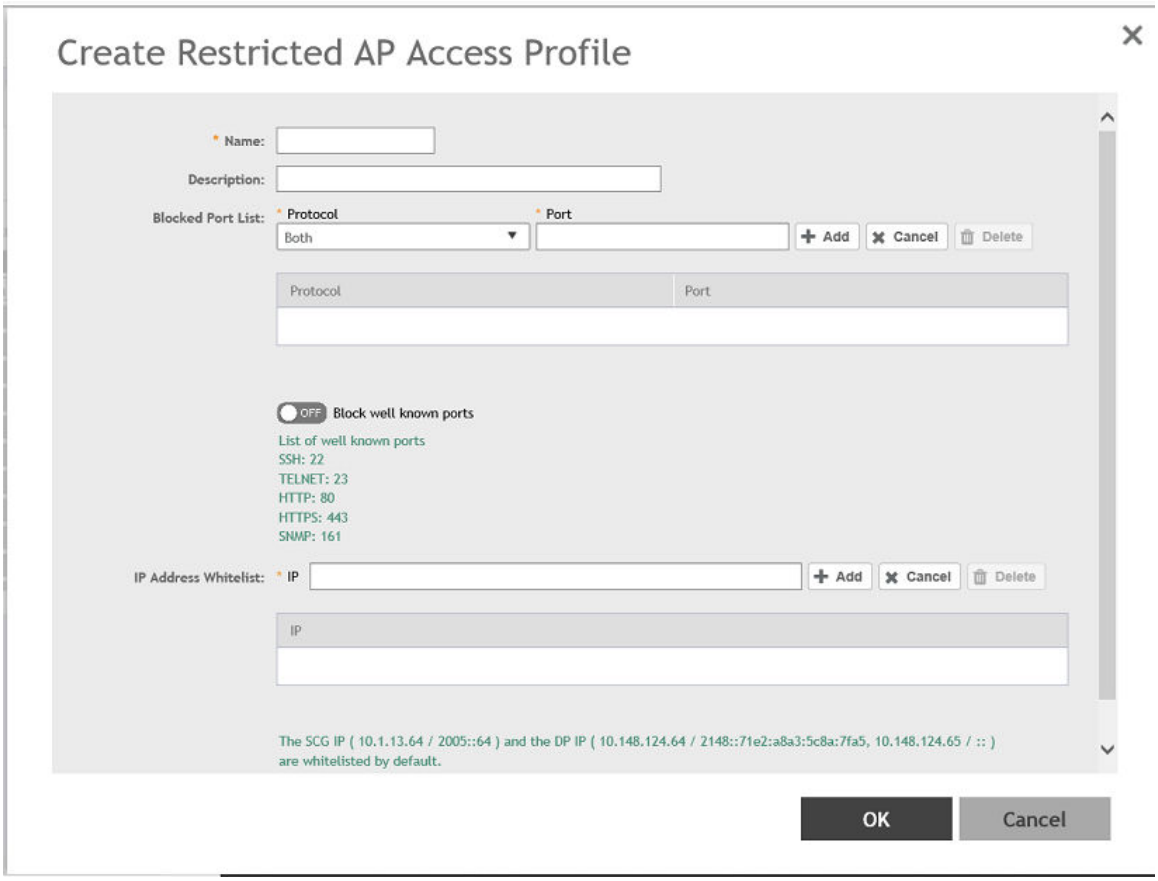
To create a Restricted AP Access profile, perform the following steps.

1. Click **Security** > **Access Control** > **Restricted AP Access**. This displays **`Restricted AP Access`**screen.

2. In **Restricted AP Access** screen. Select a Zone from the system tree and click **Create**

   The **Create Restricted AP Access Profile** page appears.

   FIGURE 241 Creating Restricted AP Access Profile



3. Configure the following:
   a. Name: Type the name of the profile.
   b. Description: Type the description of the profile.
   c. Blocked Port List: Select the protocol (TCP, UDP or Both) from the **Protocol** drop-down, and enter the port number in the **Port** field. You can click **Cancel** to re-type the entry or you can click **Add** to add the entries. The protocol and the port get listed in the table below the Blocked Port List. Click **Delete** to delete the values in the table.
   d. Block well known ports: Enable the slidebar to block the well known ports.
   e. IP Address Whitelist: When Restricted AP Access is enabled, network devices may use non-whitelisted IPv6 IP address for Restricted AP Access related operations, which may cause unexpected result. So, it is recommended to add ipv6 IP addresses manually.
4. Click **OK**.

You have created the Restricted AP Access profile.

Configuring Restricted Access via Services & Profiles

This topic describes configuring Restricted Access via Services & Profile tab.

1. Click **Security** > **Access Control** > **Restricted AP Access**. This displays **`Restricted AP Access`**screen.
2. Click **Restricted Access** tab.
3. Select a **Zone** and from the list select one of the **Restricted AP Access Profile** associated with the zone and click **Configure**.

   This displays **Edit Restricted AP Access Profile** window.
4. Enter the values in the fields and click **Ok**.

   This displays the edited **Restricted Access Profile** in the list.

Fields	Description
Name	Restricted Access Profile name.
Description	Enter a description to identify the Restricted Access Profile.
Blocked Port List	***Protocol** - Choose the protocol for communicating from the drop down list (Both, TCP, UDP) ***Port** - Enter the port numbers. These port numbers will be added to the Blocked Port list. The port numbers can be deleted by selecting the same from the table.
Block well known ports	To add all well know ports to the Blocked Port List, click the **On/Off** switch. The Block well known ports, by default is **Off**.
IP Address Whitelist	***IP** - Enter the IP addresses to allow the communication. These IP addresses will be part of the IP Address Whitelist. The IP Address can be deleted by selecting the same from the table.

Configuring Restricted Access via Access Point

This topic describes the steps to configure Restricted AP Access Profile through Access Point tab.

1. Go to **Access Points** > **Access Points**.
2. Select a Zone from the left column and click **Configure selected Domain/Zone/Group**  icon.

   This displays **Configure Group** screen.
3. In the **Configure Group** screen, navigate to **Advanced Options**. Locate **Restricted AP Access Profile** field.

   To create a Restricted AP Access Profile, click **On/Off** button to **On**.

   NOTE
   By default the **On/Off** button is in the **Off** mode.
4. Click + to **Create Restricted AP Access Profile**.

   This displays **Create Restricted AP Access Profile** screen.
5. Enter the details as provided in the Configuring Restricted Access via Services & Profiles on page 419 topic.
6. The new Restricted AP Access profile is displayed in the **Restricted AP Access** drop-down list.
7. Select the Restricted AP Access profile from the drop-down list to map the RA profile to a particular zone.

Enabling Restricted Access

To enable the Restricted Access, perform the following:

1. Go to **Network** > **Wireless** > **Access Point** > **Access Points**.
2. Select a Zone from the left column and click **Configure selected Domain/Zone/Group**  icon.

   This displays **Configure selected Domain/Zone/Group**
3. Navigate to **Advanced Options**.
4. Click **On/Off** button to **On** mode.

   NOTE
   By default the **On/Off** button is in the **Off** mode.

   This highlights the greyed out **Restricted AP Access Profile**. Select the RA profile from the drop-down list to enable the restricted access for the selected zone.

   The selected **Restricted AP Access Profile** can be edited by clicking .

Creating Blocked Clients

You can deny access to the network for certain clients by using the block client access control feature.

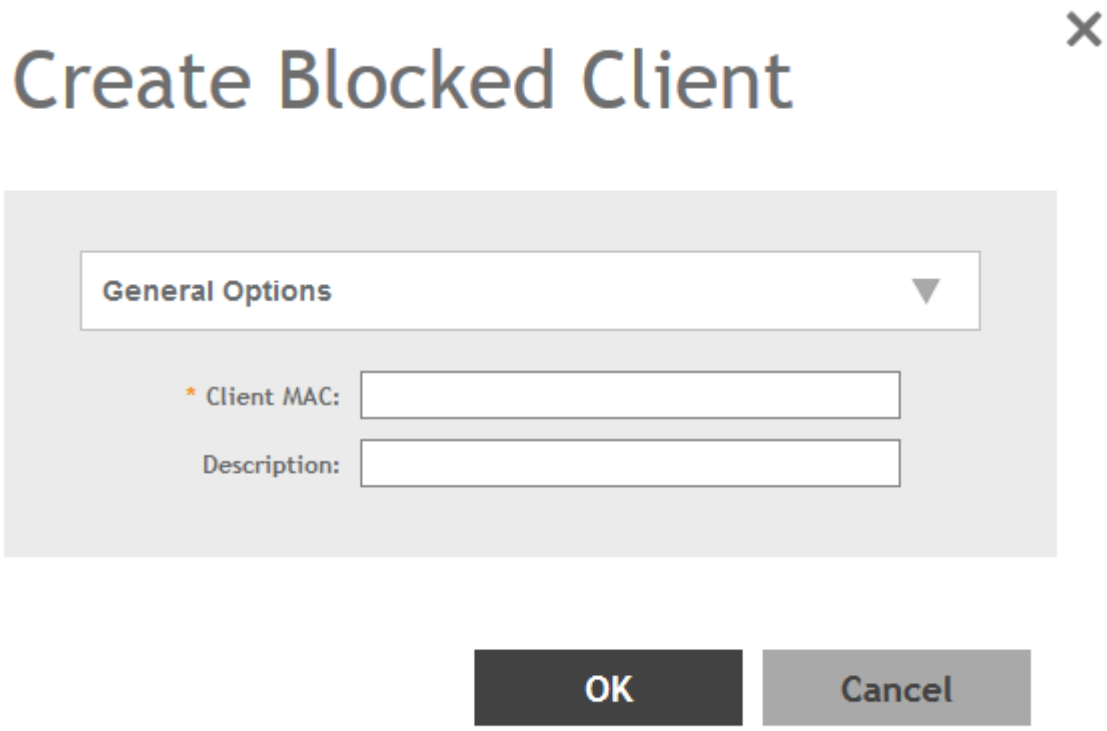
1. Go to **Security** > **Access Control** > **Blocked Client**.

   This displays **Blocked Client** screen.

2. Select a **Zone** from the system tree, click **Create**.

   This displays **Create Blocked Client** page.

   FIGURE 242 Create Blocked Client



3. Configure the following:
   a. Client MAC: Type MAC address of the client that you want to block.
   b. Description: Type a short description for client.
   c. Click **OK**.

You have created the blocked client list.

NOTE
You can also edit, clone and delete a list by selecting the options **Configure**, **Clone** and **Delete** respectively, from the **Blocked Client** tab.

Creating a Client Isolation Whitelist

This feature allows the administrator to manually specify an approved list of wired destinations that may be reachable by wireless clients.

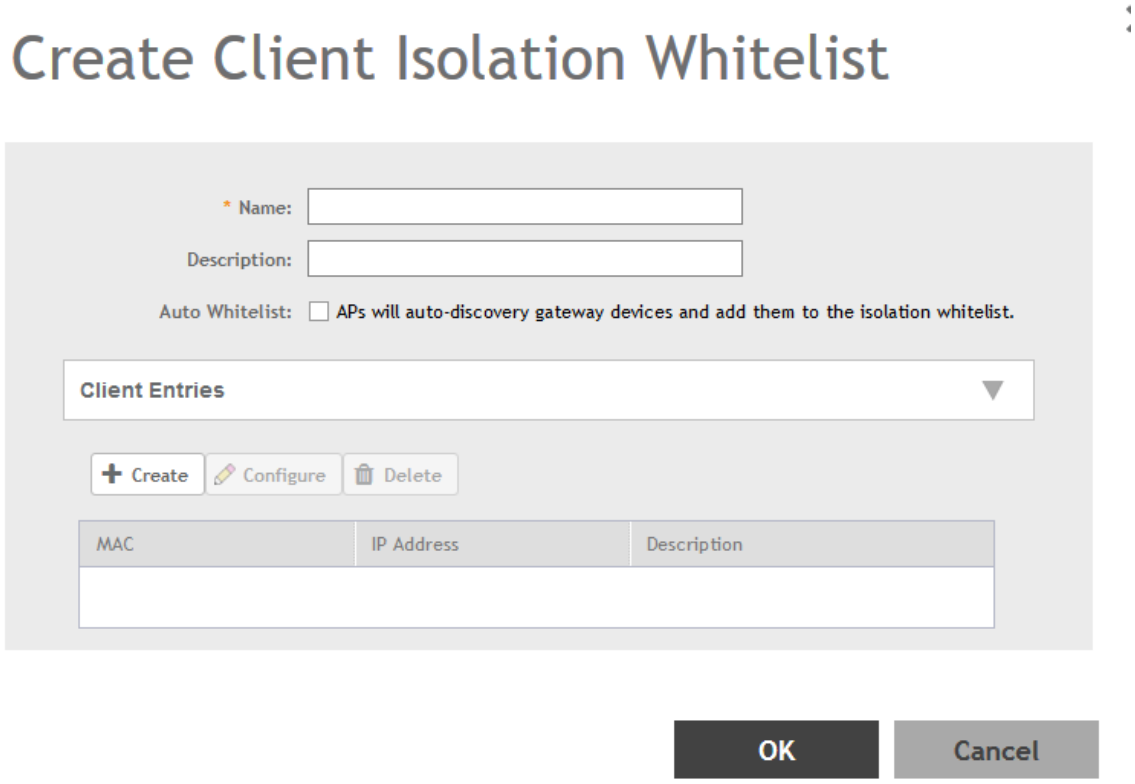
NOTE
The whitelist only applies to destinations that are on the wired network, and it will not work on wireless destinations.

1. Click **Security** > **Access Control** > **Client Isolation Whitelist**. This displays **`Client Isolation Whitelist`**screen.

2. Click **Create**.

   This displays **Create Client Isolation Whitelist** window.

   FIGURE 243 Creating a Client Isolation Whitelist



3. Configure the following:
   a. Name: Enter name of the client.
   b. Description: Enter short description about the client.
   c. Auto Whitelist: Select this check-box if you want AP to automatically scan for devices and include them in the whitelist.
   d. Client Entries: To add the clients to the list, click **Create** and provide client information such as MAC address (mandatory), IP address and Description.
   e. Click **OK**.

You have created the list of whitelisted clients that can access the network.

NOTE
You can also edit, clone and delete the list by selecting the options **Configure**, **Clone** and **Delete** respectively, from the **Client Isolation Whitelist** tab.

Creating Time Based Access Table

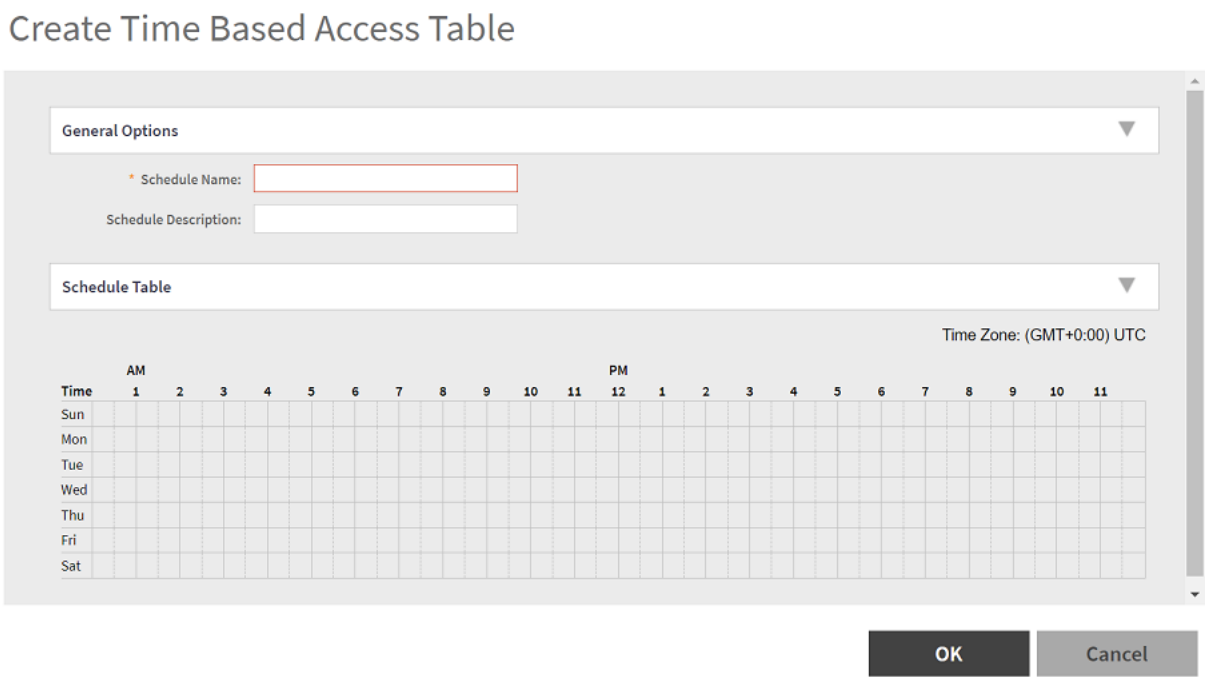
You can control client access to the network by providing a time schedule within which the device can access the network.

1. Go to **Security** > **Access Control**.
2. Select the **Time Schedule** tab, and then select the zone for which you want to create the schedule.

3. Click **Create**.

   The **Create Time Based Access Table** page appears.

   FIGURE 244 Creating a Time Based Access Table



4. Configure the following:
   a. Schedule Name: Type a name for the schedule you want to create.
   b. Schedule Description: Type a short description for this schedule.
   c. Draw the schedule table.
   d. Click **OK**.

You have created the schedule.

NOTE
You can also edit, clone and delete the schedule by selecting the options **Configure**, **Clone** and **Delete** respectively, from the **Time Schedule** tab.

Creating a Traffic Class Profile

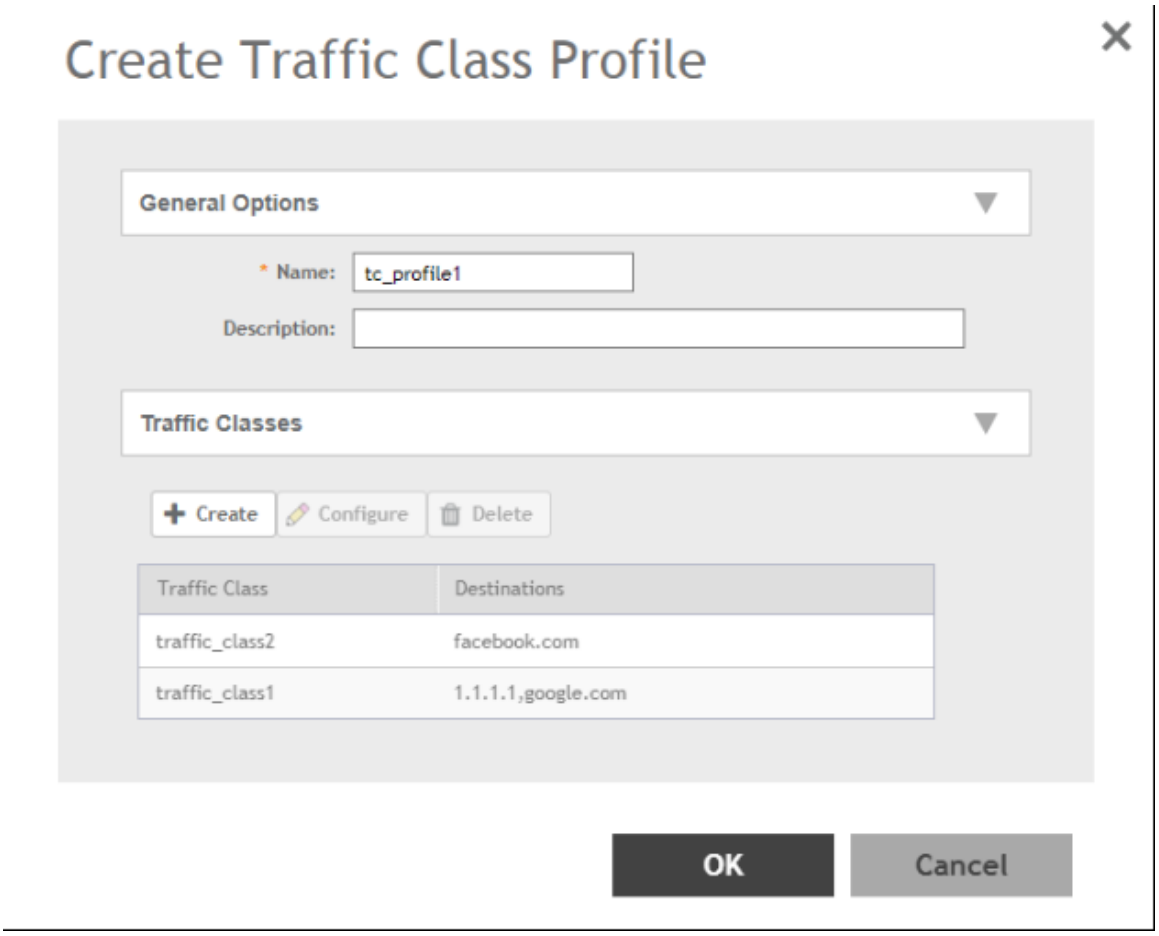
To create a traffic class profile, you must define the basic required settings.

1. Go to **Security** > **Access Control** > **Traffice Classes**.

2. Select the **Zone** from system tree and click **Create**.

   This displays **Create Traffic Class Profile** page.

FIGURE 245 Creating a Traffic Class Profile



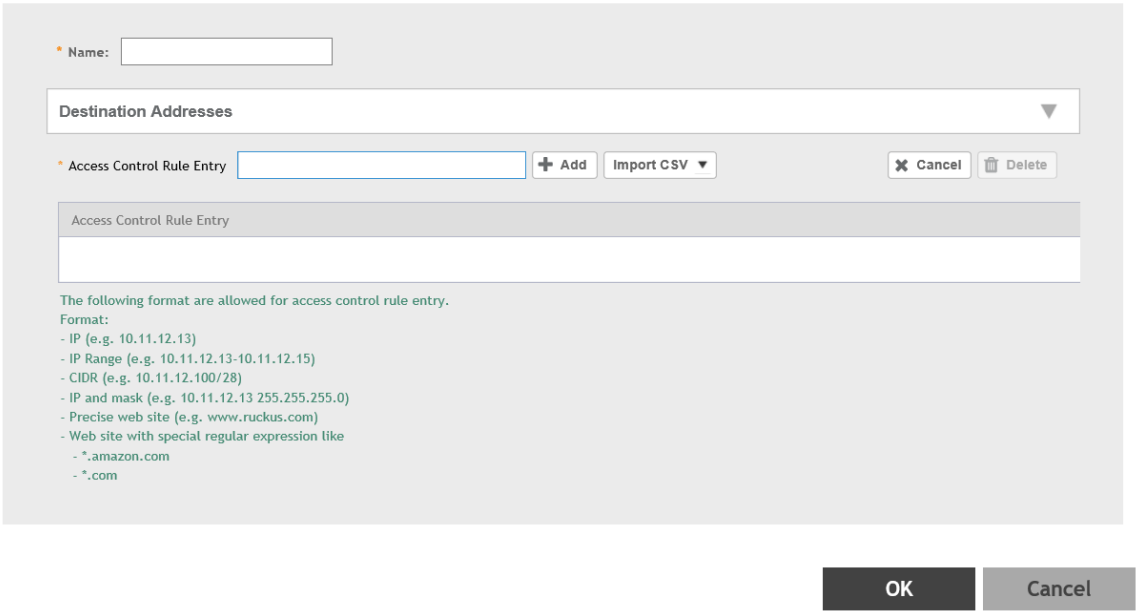
3. Under **General Options**, enter traffic class profile name and description.

4. Under **Traffic Classes**, click **Create** to add a traffic class.

   NOTE
   Only four traffic classes can be added in a single **Traffic Class** profile.

   The **Traffic Class** page appears.

   FIGURE 246 Creating a Traffic Class



5. Enter the name of the traffic class profile.
6. In the **Access Control Rule Entry** field, enter an access control rule in the proper format.
7. Click **Add** to add an access control rule or click **Import CSV** to import an access control list.

   NOTE
   Click the **Import CSV** arrow and select **Download Sample (CSV)** to download the CSV template.

   NOTE
   To delete an access control rule, select an entry and click **Delete**.

8. Click **OK**.

You have created a Traffic Class Profile.

NOTE
IP destination is reachable only when IP is not part of Traffic Class, but present under Split Tunnel. Split-tunnel policy is effective only when both **Split Tunnel** and **Traffic Class** features are enabled together.

Classifying Rogue Policy

You can create rogue classification policy with rules at the zone-level. This helps in automatic classification behavior when a specific-rogue detection criteria are met.

To create a rogue classification policy:

1. Go to **Security** > **Access Control** > **WIPS**.
2. Select the zone for which you want to create the policy and click **Create**.
3. Click **Create**.

   The Create Rogue Classification Policy page is displayed.
4. Configure the following:
   a) **Name** : Type a name for the policy.
   b) **Description** : Type a description for the policy.
   c) **Rogue Classification Rules** : Select the rule from the list and prioritize.
      - To prioritize the classification rule, select the rule from the list and click **UP** or **Down** to position the rule.
      - To create a new classification rule, click **Create** and configuring the following :
        - Click **Create**. The Create Rogue Classification Rules page appears.
        - Configure the following options:
          - **Name**: Enter a name for the rule.
          - **Rule Type**: Select one of following the rule type for the Classification:
            - Ad Hoc
            - Auth Flood
            - CTS Abuse
            - Deauth Flood
            - Disassoc Flood
            - EAP Flood
            - Excessive Power
            - Low RSSI
            - MAC OUI
            - MAC Spoofing
            - Null SSID
            - RTS Abuse
            - Same Network
            - SSID
            - SSID Spoofing
          - **Classification**: Select one of the following action for the selected **Rule Type**:
            - Ignore
            - Know
            - Malicious
            - Rogue
        - Click **OK**. You have created a Rogue classification rule.

        .
5. Click **OK**.

   You have created Rogue classification policy.

NOTE
You can also edit or delete a Rogue classification policy. To do so, select the rogue classification from the list and click **Configure** or **Delete** as required.

NOTE

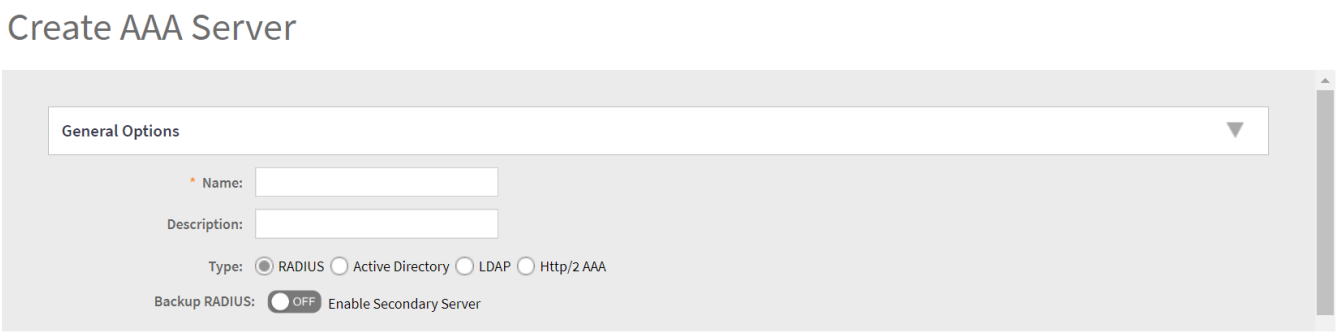
Authentication

Creating Non-Proxy Authentication AAA Server

A non-proxy AAA server is used when APs connect to the external AAA server directly.

1. Go to **Security** > **Authentication** > **Non-Proxy (AP Authenticator)**.
2. Select a Zone from the system tree and click **Create**.
   This displays **Create AAA Server** page.

FIGURE 247 Create AAA Server



3. Configure the following options:
   - General Options
     - Name: Enter a name for the AAA server that you are creating.
     - Description: Enter a short description of the AAA server.
     - Type: Select the type of AAA server that you are creating. Options include **RADIUS**, **Active Directory** and **LDAP Http/2AAA**.
     - Backup RADIUS : Select the **Enable Secondary Server**option if secondary RADIUS server exists on the network. This option is displayed only if **RADIUS** type I selected.
   - Primary Server
     - If you select **RADIUS**, configure the following options:
       - IP Address: Enter the IP address of the AAA server. Both IPv4 and IPv6 addressing formats are supported.
       - Port: Enter the port number of the AAA server. The default RADIUS server port number is 1812.
       - Shared Secret: Enter the AAA shared secret.
       - Confirm Secret: Re-enter the shared secret to confirm.

       If you have enabled the secondary server for Backup RADIUS, you must provide similar information as in the primary server.
     - If you selected **Active Directory**, configure the following options:
       - IP Address: Enter the IPv4 address of the Active Directory server.
       - Port: Enter the port number of the Active Directory server. The default port number (389) must not be changed unless you have configured the Active Directory server to use a different port.
       - Windows Domain Name: Enter the Windows domain name assigned to the Active Directory server (for example, domain.ruckuswireless.com).
     - If you selected **LDAP**, configure the following options:
       - IP Address: Enter the IPv4 address of the LDAP server.
       - Port: Enter the port number of the LDAP server. The default port number is 389.
       - Base Domain Name: Enter the base domain name in LDAP format for all user accounts (for example, dc=ldap,dc=com).
       - Admin Domain Name: Enter the administrator domain name in LDAP format (for example, cn=Admin;dc=*Your Domain*,dc=com).
       - Admin Password: Enter the administrator password for the LDAP server.
       - Confirm Password: Re-enter the administrator password to confirm.
       - Key Attribute: Enter a key attribute to denote users (for example, default: uid)
       - Search Filter: Enter a search filter (for example, objectClass=Person).
4. Under **User Role Mapping**, click **Create** to create a user traffic profile mapping.

   NOTE
   While mapping group attribute value to a user role, avoid special characters, wild-card entries, or duplicate entries regardless of the order. Only the firs-matched entry will be mapped to the user role.

   a) In the **Group Attribute Value** field, enter the value to be sent from AAA as part of an Access-Accept.

   b) Select a user role from the **User Role** list or click **+** to create a user role. For more information, refer to User Roles on page 397.
5. Click **OK**.

NOTE
You can also edit, clone and delete an AAA server by selecting the options **Configure**, **Clone**, and **Delete**, respectively, from the **Non-Proxy (AP Authenticator)** tab.

VIDEO
Non-Proxy AAA Configuration. Creating a Proxy or Non-Proxy Authentication service
Click to play video in full screen mode.

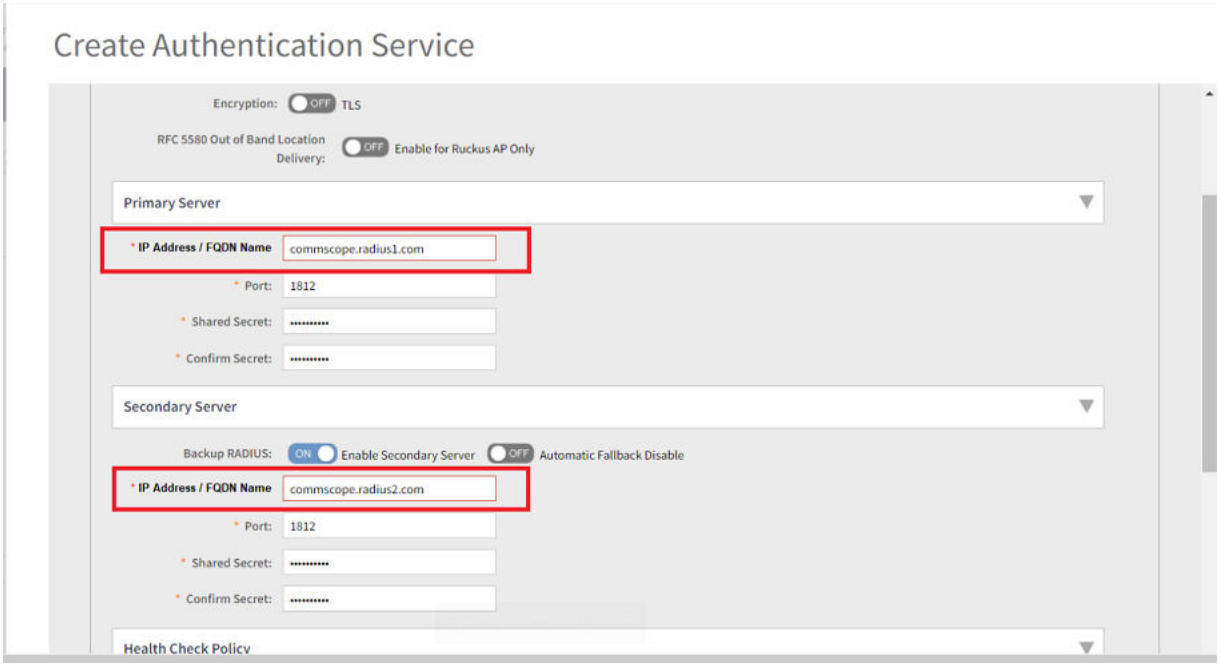
Creating Proxy Authentication AAA Servers

A proxy AAA server is used when APs send authentication or accounting messages to the controller and the controller forwards these messages to an external AAA server.

1. Go to **Security** > **Authentication** > **Proxy (SZ Authenticator)**.
2. Click **Proxy (SZ Authenticator)**.
3. Click **Create**.

   This displays **Create Authentication Service** page.

   FIGURE 248 Creating an Authentication Service



4. Configure the following options:
   - Name: Enter a name for the authentication service that you are adding.
   - Friendly Name: Enter an alternative name that is easy to remember.
   - Description: Enter a description for the authentication service.
   - Service Protocol: Select the type of service protocol for the authentication service you are adding. Options are **RADIUS**, **Active Directory**, and **LDAP**.
     - If you select **RADIUS**, refer to RADIUS Service Options on page 431 for more information.
     - If you select **Active Directory**, configure the following options:
       - Global Catalog: Select the **Enable Global Catalog** support if you want the Active Directory server to provide a global list of all objects.
       - Primary Server: For Encryption, select the **Enable TLS Encryption** check box if you want to use the Transport Layer Security (TLS) protocol to secure communication with the server.

         NOTE
         You must also configure the Trusted CA certificates to support TLS encryption.

       - IP Address: Enter the IPv4 address of the Active Directory server.
       - Port: Enter the port number of the Active Directory server. The default port number (389) must not be changed unless you have configured the Active Directory server to use a different port.
       - Windows Domain Name: Enter the Windows domain name assigned to the Active Directory server (for example, domain.ruckuswireless.com).
     - If you select **LDAP**, configure the following options:
       a. Select **Enable TLS Encryption** check box, if you want to use the Transport Layer Security (TLS) protocol to secure communication with the server.

          NOTE
          You must also configure the Trusted CA certificates to support TLS encryption.

       b. IP Address: Enter the IPv4 address of the LDAP server.
       c. Port: Enter the port number of the LDAP server.
       d. Base Domain Name: Enter the base domain name in LDAP format for all user accounts (for example, dc=ldap,dc=com).
       e. Admin Domain Name: Enter the administrator domain name in LDAP format (for example, cn=Admin;dc=*Your Domain*,dc=com).
       f. Admin Password: Enter the administrator password for the LDAP server.
       g. Confirm Password: Re-enter the administrator password to confirm.
       h. Key Attribute: Enter a key attribute to denote users (for example, default: uid).
       i. Search Filter: Enter a search filter (for example, objectClass=Person).
   - Advanced Options - Domain name: Enter the allowed domain name that you want to add.
   - User Role Mapping:

     NOTE
     While mapping group attribute value to a user role, avoid special characters, wild-card entries, or duplicate entries regardless of the order. Only the firs-matched entry will be mapped to the user role.

     a. In the **Group Attribute Value** field, enter the value to be sent from AAA as part of an Access-Accept.

     b. Select a **User Role** from the list or click  to create a new user role. For more information, refer to User Roles on page 397.

c. Click **OK**.

The mapped user profile is listed.

5. Click **OK**.

NOTE
You can also edit, copy, and delete an AAA server by selecting the options **Configure**, **Clone**, and **Delete**, respectively, from the **Proxy (SZ Authenticator)** tab.

RADIUS Service Options

These are the Radius service options available for the primary and secondary servers.

RFC 5580 Out of Band Location Delivery: If you want out-of-band location delivery (RFC 5580) to apply only to RUCKUS APs, select the **Enable for Ruckus AP Only** check box.

Configure the primary RADIUS server settings as shown in the following table.

Configure the primary RADIUS server settings.

TABLE 96 Primary Server Options

Option	Description
IP Address	Type the IP address of the RADIUS server. IPv4 and IPv6 addressing formats are supported.
Port	Type the port number of the RADIUS server. The default RADIUS server port number is 1812 and the default RADIUS Accounting server port number is 1813.
Shared Secret	Type the RADIUS shared secret.
Confirm Secret	Retype the shared secret to confirm.

If you have a secondary RADIUS server on the network that you want to use as a backup, select the Enable Secondary Server check box, and then configure the settings in the following table.

TABLE 97 Secondary Server Options

Option	Description
Backup RADIUS	Select **Enable Secondary Server**. When a secondary RADIUS server is enabled and the primary RADIUS server becomes unavailable, the secondary Automatic Fallback Disable server takes over the handling of RADIUS requests. When the primary server becomes available again, it takes back control over RADIUS requests from the secondary server. If you want to prevent the primary server from retaking control over RADIUS requests from the secondary server, select the **Automatic Fallback Disable** check box.
IP Address	Type the IP address of the secondary AAA server. IPv4 and IPv6 addressing formats are supported.
Port	Type the port number of the secondary AAA server port number. The default RADIUS server port number is 1812 and the default RADIUS Accounting server port number is 1813.
Shared Secret	Type the AAA shared secret.
Confirm Secret	Retype the shared secret to confirm.

The following options define the health monitoring settings of the primary and secondary RADIUS servers, when the controller is configured as RADIUS proxy for RADIUS Authentication and Accounting messages.

TABLE 98 Health Check Policy

Option	Description
Response Window	Set the time (in seconds) after which, if the AAA server does not respond to a request, the controller will initiate the zombie period (see below). Response Window If the primary AAA server does not respond to RADIUS messages sent after Response Window expires, the controller will forward the retransmitted RADIUS messages to the secondary AAA server. **NOTE** The zombie period is not started immediately after the Response Window expires, but after the configured Response Window plus ¼ of the configured Zombie Period. The default Response Window is 20 seconds
Zombie Period	Set the time (in seconds) after which, if the AAA server does not respond to ANY packets during the zombie period, it will be considered to inactive or unreachable. An AAA server that is marked zombie (inactive or unreachable) will be used to proxy with a low priority. If there are other live AAA servers, the controller will attempt to use these servers first instead of the zombie AAA server. The controller will only proxy requests to a zombie server only when there are no other live servers. Any request that is sent as a proxy to an AAA server will continue to be sent to that AAA server until the home server is marked inactive or unreachable. At that point, the request will fail over to another server, if a live AAA server is available. The default Zombie Period is 40 seconds.
Revive Interval	Set the time (in seconds) after which, if no RADIUS messages are sent as proxy to the AAA server after it has been marked as inactive or unreachable, the controller will mark the AAA server as active again (and assume that it has become reachable again). The default Revive Interval is 120 seconds.
No Response Fail	Click **Yes** to respond with a reject message to the NAS if no response is received from the RADIUS server. Click **No** to skip sending a response.

NOTE
To ensure that the RADIUS fail-over mechanism functions correctly, either accept the default values for the Response Window, Zombie Period, and Revive Interval, or make sure that the value for Response Window is always higher than the value for RADIUS NAS request timeout multiplied by the value for RADIUS NAS max number of retries. For third party APs, you must ensure that the configured Response Window on the controller is higher than the RADIUS NAS request timeout multiplied by the RADIUS value. The maximum number of retries is configured at the 3rd party controller/AP.

Configure the following options.

TABLE 99 Rate Limiting

Options	Description
Maximum Outstanding Requests (MOR)	Set the maximum outstanding requests per server. Type 0 to disable it, or set a value between 10 and 4096.
Threshold (% of MOR)	Set a percentage value of the MOR at which (when reached) the controller will generate an event. Threshold (% of MOR) For example, if the MOR is set to 1000 and the threshold is set to 50%, the controller will generate an event when the number of outstanding requests reaches 500.
Sanity Timer	Set a timer (in seconds) that will be started whenever a condition that generates an event is reached. This helps prevent conditions that trigger events which occur frequently.

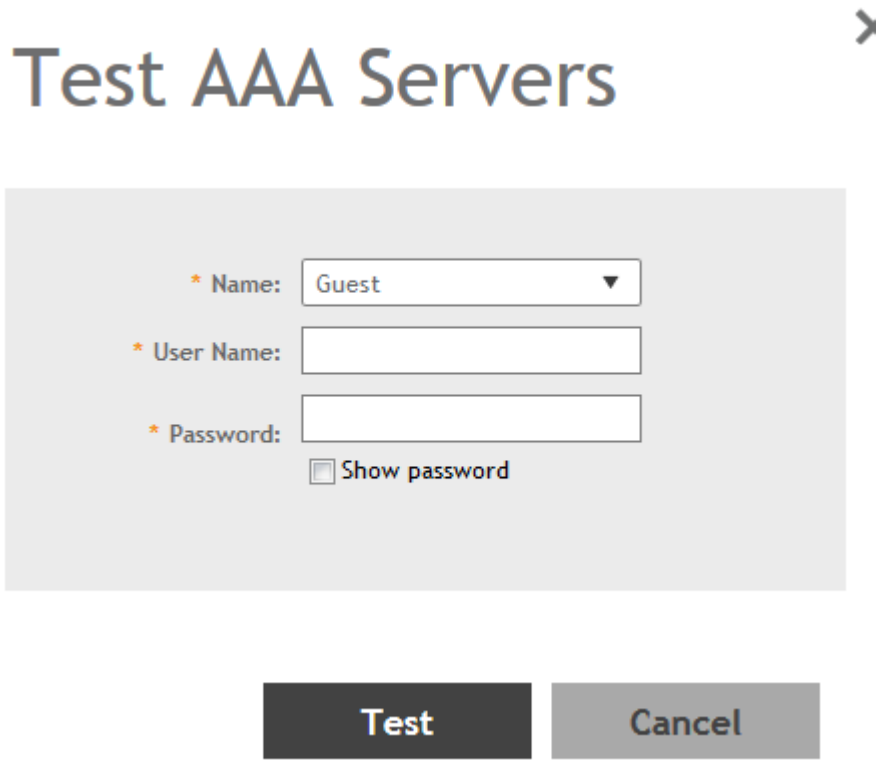
Testing AAA Servers

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 249 Testing an AAA Server



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.

Authentication Support Matrix

It is important to understand the compatibility between AAA servers and different WLANs.

Proxy Mode

In proxy mode, authentication requests are set through the controller.

TABLE 100 Proxy Mode Compatibility

Authentication Source	802.1X	HS 2.0 Secure	Web Auth	Hotspot/WISPr
Local Database	No	Yes	No	Yes
IDM-Provisioned Local DB	Yes	Yes	NA	NA
Active Directory	No*	No	Yes	Yes
RADIUS	Yes	Yes	Yes	Yes
LDAP	Yes	No	Yes	Yes

NOTE
To support 802.1X with Active Directory, an external RADIUS server (such as NPS) must be used.

NOTE
IDM Provisioned username (also called local cache credential) is relevant only in secure access after Onboarding.

NOTE
802.1X (MSCHAPv2 via built-in RADIUS using AD-NPS), WebAuth, and WISPr support AD authentication from SmartZone release in 3.2.

NOTE
802.1X, WebAuth, and WISPr support LDAP authentication from SmartZone release in 3.2. For 802.1X authentication, the user password must be in clear text in the LDAP database.

Non-proxy Mode

In the Non-proxy mode, authentication requests are sent directly by AP and not through the controller. The local database is stored on the controller, therefore, authentication sources such as local database and IDM-provisioned local databases are not supported.

TABLE 101 Non-proxy Mode Compatibility

Authentication Source	802.1X	Zero-IT Onboard	HS 2.0 Onboard	HS 2.0 Secure	Web Auth	Hotspot/WISPr
Active Directory	No	No*	No*	No	Yes	No
RADIUS	Yes	No*	No*	No	Yes	Yes*
LDAP	No	No*	No*	No	Yes	No

(*) From the configuration it may seem like non-proxy RADIUS is supported in WISPr, but the call flow goes through the controller.

Profile Configuration

The following table details proxy and non-proxy AAA server configurations against various platforms.

TABLE 102 Profile Configuration

Feature	SZ100	vSZ-E	vSZ-H	Description
Per-Zone ProxyAAA Profiles	NA	NA	NA	Ability to configure a ProxyAAA profile in a specific zone

TABLE 102 Profile Configuration (continued)

Feature	SZ100	vSZ-E	vSZ-H	Description
Global ProxyAAA Profiles	Yes	Yes	Yes	Ability to configure a ProxyAAA profile globally and then use it across zones
Per-Zone NonProxy AAA Profiles	NA	NA	Yes	Ability to configure a NonProxyAAA profile in a specific zone
Global NonProxy AAA Profiles	Yes	Yes	No	Ability to configure a NonProxy AAA profile globally and then use it across zones

Dynamic Policy Assignment (Proxy Authentication Types)

The following table details dynamic policy assignments across authentication types.

TABLE 103 Dynamic Policy Assignment (Proxy)

Feature	802.1X	Zero-IT Onboard	HS 2.0 Onboard	HS 2.0 Secure	Web Auth	Hotspot/WISPr	MAC Auth	Description
Dynamic Role Assignment	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Ability to assign a user to a particular local Role via a group/role attribute from RADIUS, AD, LDAP. From SmartZone 3.4, Role can contain UTP. Therefore, , when you assign a role, you also get the ACL and Rate Limiting policies.
Dynamic VLAN / VLAN Pool	Yes	NA	NA	NA	No	No	Yes	Ability to assign a user to a VLAN through a VLAN attribute from RADIUS, AD, LDAP. From SmartZone release 3.5, you can also assign VLANs and VLAN pools based on the user role.
Dynamic UTP	Yes				Yes	Yes	Yes	Ability to assign a user to a UTP through an attribute from an authentication source.
Dynamic ACL	Yes	Yes	Yes	No	Yes	Yes	Yes	Ability to assign a specific ACL to a user through an attribute from RADIUS, AD, LDAP.

TABLE 103 Dynamic Policy Assignment (Proxy) (continued)

Feature	802.1X	Zero-IT Onboard	HS 2.0 Onboard	HS 2.0 Secure	Web Auth	Hotspot/WISPr	MAC Auth	Description
Dynamic Rate Limit	Yes	Yes	Yes			Yes	Yes	Ability to assign a specific Rate Limit to a user through an attribute from RADIUS, AD, LDAP.

NOTE
In dynamic ACL and Rate limit, since ACL and rate limit are associated with a UTP, assigning a UTP also assigns an ACL or rate limit.

Dynamic Policy Assignment (Non-Proxy Authentication Types)

The following table details dynamic policy assignments across authentication types.

TABLE 104 Dynamic Policy Assignment (Non-Proxy)

Feature	802.1X	HS 2.0 Secure	Web Auth	Description
Dynamic Role Assignment	No			Ability to assign a user to a local Role through a group/role attribute from the authentication source.
Dynamic VLAN / VLAN Pool				Ability to assign a user to a VLAN through a VLAN attribute from the authentication source.
Dynamic UTP				Ability to assign a user to a UTP through an attribute from the authentication source. **NOTE** From SmartZone release 3.4, UTP contains ACL and rate limit.
Dynamic ACL				Ability to assign a specific ACL to a user through an attribute from the authentication source. **NOTE** ACLs are a part of a UTP. If you configure a UTP without a rate limit,you effectively only have an ACL.
Dynamic Rate Limit				Ability to assign a specific Rate Limit to a user through an attribute from the authentication source. **NOTE** Rate limiting is also a part of a UTP. If you configure a UTP without ACL, you effectively only have a rate limiting policy.

Other Authentication Features

The following table details authentication support for various authentication features.

TABLE 105 Authentication Features

Feature	Supported	Description
Test AAA - RADIUS	Yes	Ability to test a specific username/password against a configured RADIUS serve.
Test AAA - Active Directory	Yes	Ability to test a specific username/password against a configured AD serve.
Test AAA - LDAP	Yes	Ability to test a specific username/password against a configured LDAP serve. **NOTE** Only Non-Proxy LDAP is supported at the Zone Level.
Test AAA - Return a Role	Yes - supported by RADIUS, AD and LDAP	Ability to return a role assignment when testing a AAA server.
RADIUS CoA - Change Role		Ability to change a user's Role through a Change of Authorization (CoA).
RADIUS CoA - Change VLAN		Ability to change a user's VLAN through a Change of Authorization (CoA).
RADIUS CoA - Change ACL		Ability to change a user's ACL through a Change of Authorization (CoA).
RADIUS CoA - Change Rate Limit		Ability to change a user's rate limit through a Change of Authorization (CoA).
RADIUS CoA - Change Authorization		Ability to authorize or deauthorize a user through a Change of Authorization (CoA). **NOTE** The controller does not provide support for CoA or DM in non-proxy mode.

PAP/CHAP Support

The following table details PAP and CHAP support for various authentication features.

TABLE 106 PAP/CHAP Support

Feature	802.1X	Web Auth	Hotspot/ WISPr	MAC Auth	Notes
Proxy-Mode					
Active Directory	Yes	Yes*	Yes	No	PAP / CHAP is supported for Web Authentication and HotSpot/WISPr. NPS interface (AD) is required for WebAuthenticaiton (CHAP) and 802.1X (MSCHAPv2).
RADIUS	Yes	Yes*	Yes	Yes	
LDAP	Yes	Yes*	Yes	No	PAP / CHAP is supported for Web Authentication and HotSpot/WISPr

TABLE 106 PAP/CHAP Support (continued)

Feature	802.1X	Web Auth	Hotspot/ WISPr	MAC Auth	Notes
LDAP-TLS	Yes	Yes*	Yes	No	This support is available from SmartZone version 3.5.
Active Directory (TLS)	Yes	Yes*	Yes	No	This support is available from SmartZone version 3.5. NPS interface (AD) is required for WebAuthenticaiton (CHAP) and 802.1X (MSCHAPv2).
Non-proxy Mode					
Active Directory	No	Yes*	Yes	No	
RADIUS	Yes	Yes*	Yes	Yes	
LDAP	No	Yes*	Yes	No	

NOTE
(*) This is an AP CLI setting:

```
set aaa auth-method pap|chap
```

It is a global setting for all WebAuth WLANs on the AP. The default is CHAP.

Non-Proxy (Social Login)

To configure social media profile for a user, use client ID and client secret options. Social media login can be activated by turing **On** the Social Media enable button.

Creating Social Media Login Profile

When end-user associated with an OAuth 2.0 WLAN, launches his browser. AP redirects it to the OAuth 2.0 provider login page. The end-user should enter his account and password to authenticate with OAuth 2.0 provider. AP sets the end-user status as authenticated and user is able to use internet.

To configure social media authentication configuration, perform the following:

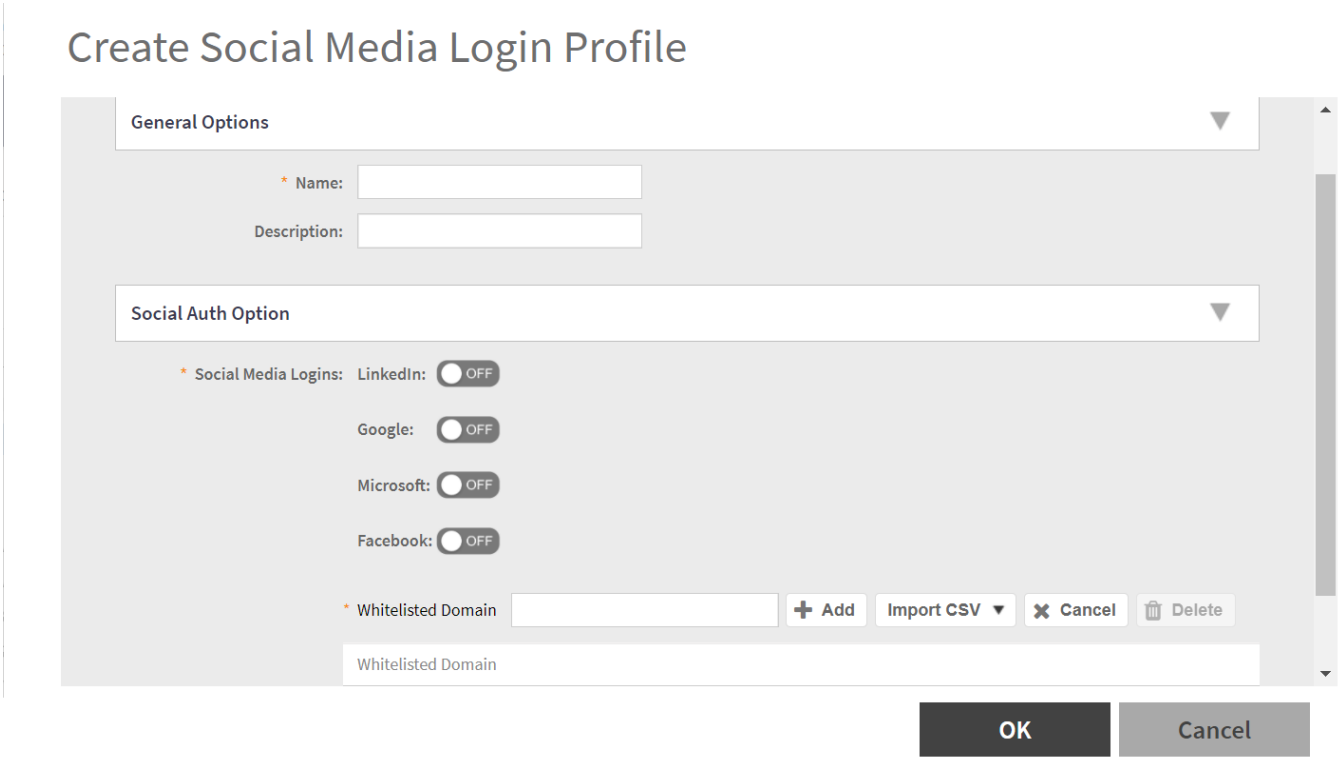
1. Go to **Security** > **Access Control** > **Authentication** > **Non-Proxy (Social Login)**.

   This displays the zones associated with the Non-Proxy (Social Login).
2. In the **Non-Proxy (Social Login)** screen, select a **Zone** and click **Create**.

   This displays **Create Social Media Login Profile** page.
3. Enter the values in **General Options** and enable the **Social Auth Option** tabs.
4. After you have enabled the **Social Media Logins** it is mandatory to provide the client ID/Secret. If you don't have one, click on the hyperlink provided in **Create Social Media Login Profile** screen to generate a and for particular social media website.

5. Add domains to the **Whitelisted Domain** field by entering the domain name. For example,
   - LinkedIn - *.licdn.com, *.linkedin.com
   - Google - *.geotrust.com, *.gstatic.com
   - Facebook - *.facebook.com, *.fbcdn-profile-a.akamaihd.net, *.fstatic-a.akamaihd.net
   - Microsoft - *.geotrust.com, *.live.com, *.microsoftonline.com, *.auth.gfx.ms, *.msauth.net

FIGURE 250 Create Social Media Login Profile



Creating Realm Based Authentication Profile

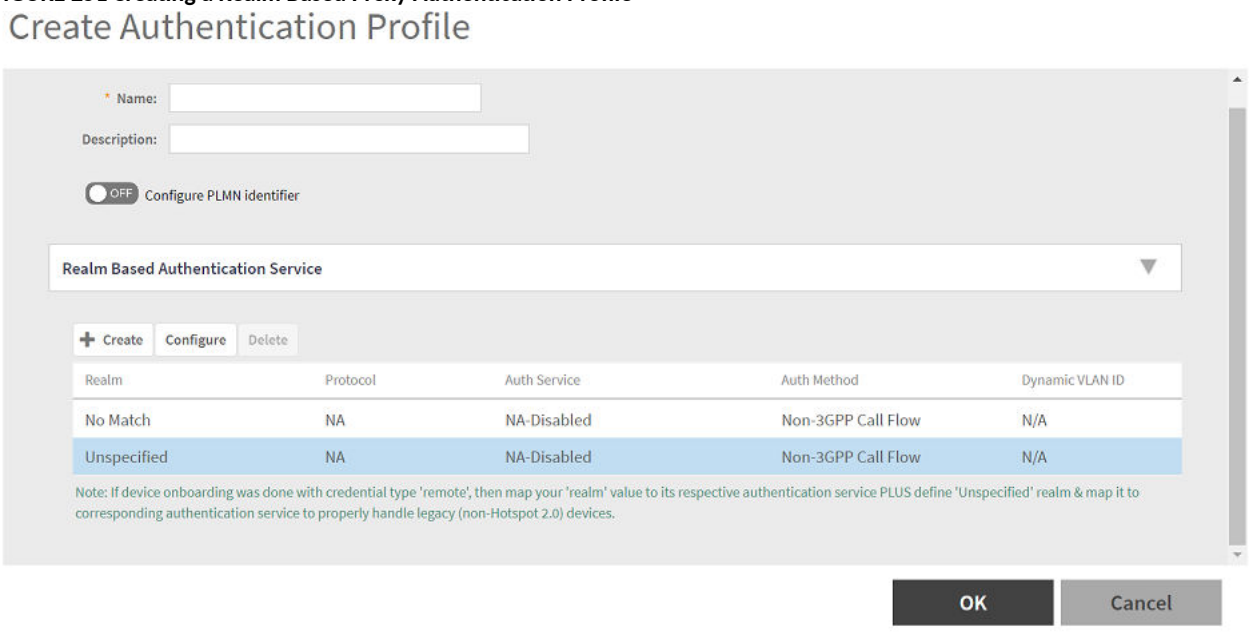
An authentication profile defines the authentication policy when the controller is used as a Radius proxy service for WLANs.

1. Go to **Security** > **Access Control** > **Authentication** > **Realm Based Proxy**.

2. Click **Create**.

   This displays **Create Authentication Profile** page.

FIGURE 251 Creating a Realm Based Proxy Authentication Profile



3. Configure the following:
   a. Name: Type a name for the authentication service profile that you are creating.
   b. Description: Type a short description of the authentication service profile.
   c. Realm-Based Authentication Service
      - Realm: Type wthere the realm is No Match or Unspecified.
      - Protocol: Displays the type of protocol.
      - Auth Service: Select a default authentication service for the realm.
      - Auth Method: Select an authorization method as 3GPP or Non-3GPP call flow.
      - Dynamic VLAN ID: Type the vlan ID.
   d. - Redirect to the URL that the user intends to visit: Allows the guest user to continue to their destination without redirection.
      - Redirect to the following URL: Redirect the user to a specified web page (entered into the text box) prior to forwarding them to their destination. When guest users land on this page, they are shown the expiration time for their guest pass.
4. Click **OK**.

Fast Initial Link Setup (FILS)

Enable Fast Initial Link Setup (FILS) for 802.1X EAP WLAN and select the realm-based AAA configuration and DHCP server IP address.

Combines the authentication, authorization, and DHCP to reduce EAP frames and skip EAPOL 4-way handshake when station reconnects or roams. It requires AAA to support Higher Layer Protocol (HLP) and EAP-RP. The DHCP server requires the Rapid commit. The following WLAN feature combinations are supported by FILS:

- 802.1x(FILS) + WISPr

- 802.1x(FILS) + MAC Auth
- 802.1x(FILS) + 802.11w
- 802.1x(FILS) + FT

NOTE
FILS provides MAC support. When FILS is enabled, the DHCP Rapid Commit Proxy is also enabled by default. However, it is hidden in the screen.

Create FILS Realm Profile

To create FILS Realm Profile, perform the following:

1. Go to **Security** > **Authentication** > **FILS Realm Proxy**.

   This displays **Create FILS Realm Profile** screen.
2. In the **Create FILS Realm Profile** screen, enter the following details:
   - Name: Enter name for the profile.
   - Description: Enter a short description for the profile.
   - Realms: Enter a Realm Name and click **Add**.

     The Realm Name is displayed below.
   - Click **Ok**.

   The new profile is displayed in the **FILS Realm Profile** screen.

   NOTE
   The **FILS Realm Profile** can be created from the **Fast Initial Link Setup** by clicking **+** corresponding to the **Realm Profile**.

Accounting

Creating Non-Proxy Accounting AAA Servers

A non proxy AAA server is used when the APs connect to the external AAA server directly.

1. Go to **Security** > **Access Control** > **Accounting** > **Non-Proxy**.

2. Click **Create**.

   The **Create AAA Server** page appears.

FIGURE 252 Creating an AAA Server



3. Configure the following:
   a. General Options
      - Name: Type a name for the AAA server that you are creating.
      - Description: Type a short description of the AAA server.
      - Type: Select **RADIUS Accounting**.
      - Cluster Redundancy: Click the **Enable Service for Standby Cluster** option to enable cluster redundancy.

        NOTE
        Cluster Redundancy option is available only when this functionality is enabled in cluster configuration.

      - Backup RADIUS (appears if you clicked RADIUS above): Click the **Enable Secondary Server** check box if a secondary RADIUS server exists on the network.
   b. If you selected RADIUS, configure the following options in the Primary and Secondary server sections:
      - IP Address: Type the IP address of the AAA server.
      - Port: Type the port number of the AAA server. The default RADIUS server port number is 1813.
      - Shared Secret: Type the AAA shared secret.
      - Confirm Secret: Retype the shared secret to confirm.
4. Click **OK**.

You have completed creating a Non-proxy Accounting AAA server.

NOTE
You can also edit, clone and delete an AAA server by selecting the options **Configure**, **Clone** and **Delete** respectively, from the **Non-Proxy** tab.

Creating Proxy Accounting AAA Servers

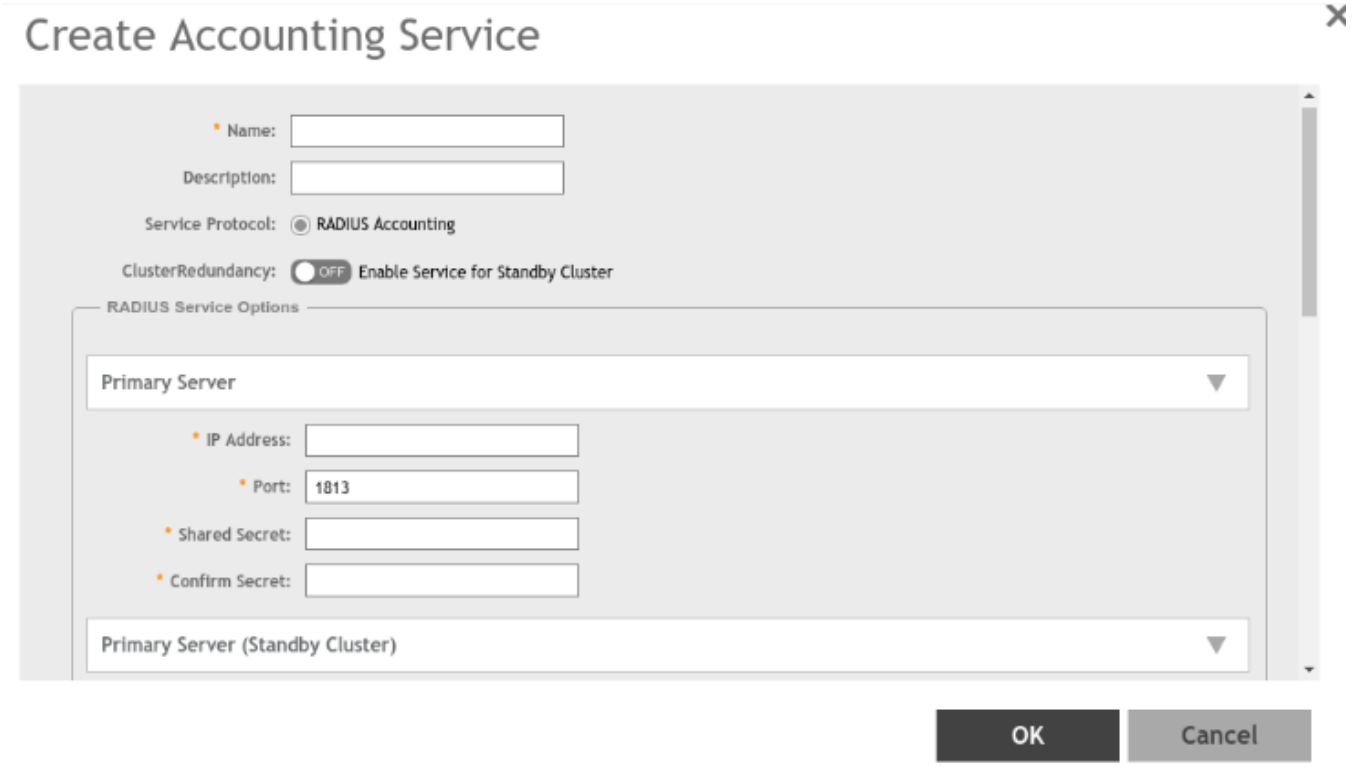
A proxy AAA server is used when APs send authentication/accounting messages to the controller and the controller forwards these messages to an external AAA server.

1. Go to **Security** > **Access Control** > **Accounting** > **Proxy**.

2. Click **Create**.

   The **Create Accounting Service** page appears.

FIGURE 253 Creating an Accounting Service



3. Configure the following:
   a. Name: Type a name for the authentication service that you are adding.
   b. Description: Type a description for the authentication service.
   c. Service Protocol: By default, the RADIUS Accounting is selected. For more information, see RADIUS Service Options on page 431.
   d. Cluster Redundancy: Click the **Enable Service for Standby Cluster** option to enable cluster redundancy.

      NOTE
      Cluster Redundancy option is available only when this functionality is enabled in cluster configuration.

4. Click **OK**.

You have completed creating a Proxy Accounting AAA server.

NOTE
You can also edit, clone and delete an AAA server by selecting the options **Configure**, **Clone** and **Delete** respectively, from the **Proxy** tab.

Creating Realm Based Proxy

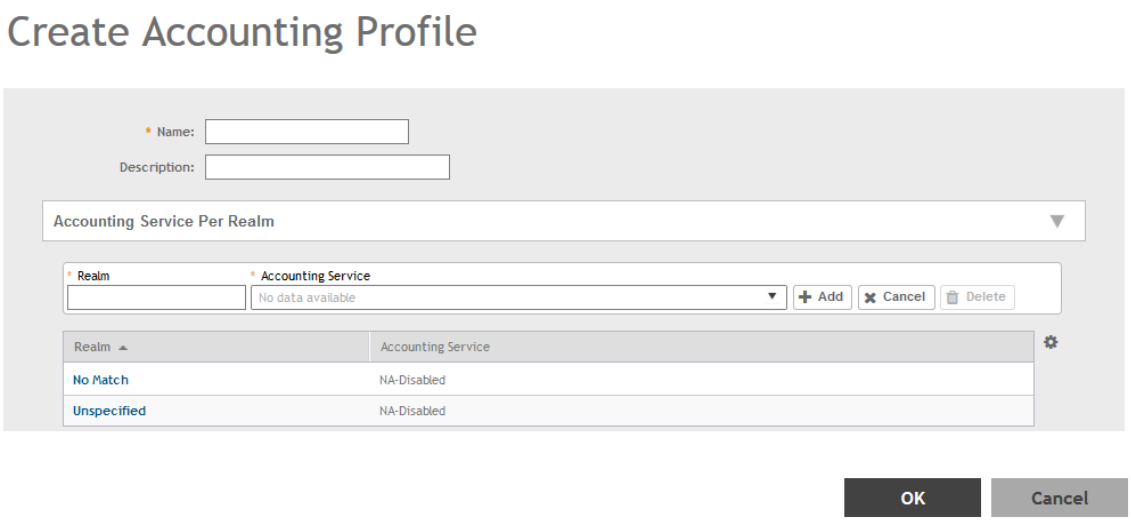
An accounting profile defines the accounting policy when the controller is used as a RADIUS proxy for WLAN services.

1. Go to **Security** > **Access Control** > **Accounting** > **Realm Based Proxy**.

2. Click **Create**.

   The **Create Accounting Profile** page appears.

FIGURE 254 Creating an Accounting Profile



3. Configure the following:
   a. Name: Type a name for the authentication service that you are adding.
   b. Description: Type a description for the authentication service.
   c. Accounting Service per Realm: Specify the accounting service for each of the realms specified in this table. If you set the accounting service for a particular realm to NA-Disabled, then the accounting request is rejected. To create a new service click, **Create** and then configure **Realm** and **Accounting Service**.
4. Click **OK**.

You have completed creating a Realm-based proxy Accounting AAA server.

NOTE
You can also edit, clone and delete an AAA server by selecting the options **Configure**, **Clone** and **Delete** respectively, from the **Realm Based Proxy** tab.

Services

- Working with Hotspots and Portals....447
- Working with Tunnels and Ports....472
- Working with DHCP....496
- Working with Other SmartZone Services....511

Working with Hotspots and Portals

Creating a Guest Access Portal

Using the controller's Guest Access features, you can provide visitors to your organization limited access to a guest WLAN with configurable guest policies. The following sections describe how to configure guest WLANs and access policies that control guest use of your network.

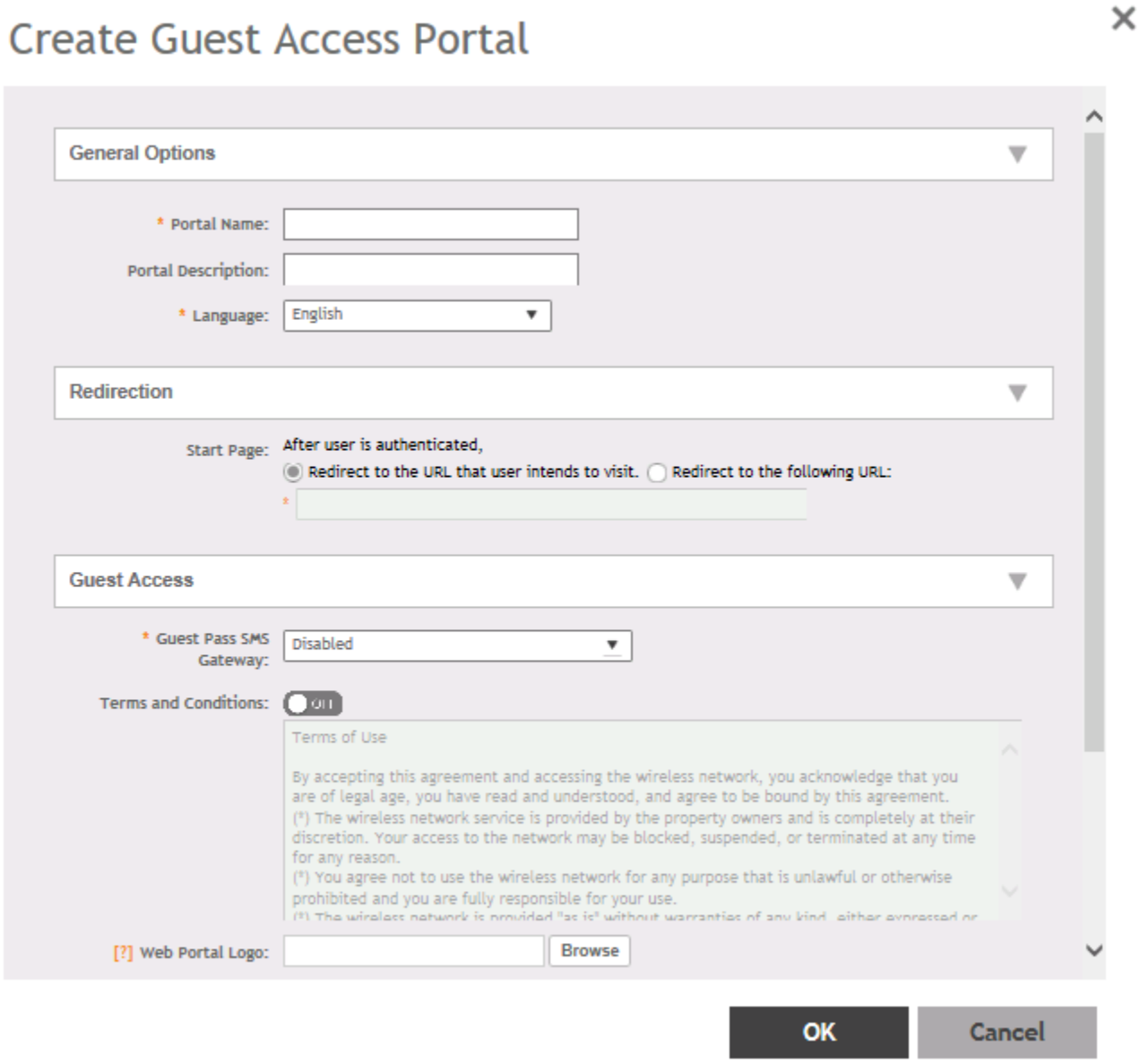
Each guest WLAN must be associated with a Guest Access service portal, which defines the behavior of the guest WLAN interface. Follow these steps to create a guest access service.

1. Go to **Services** > **Hotspots & Portals**.
2. Select the **Guest Access** tab, and then select the zone for which you want to create the portal.

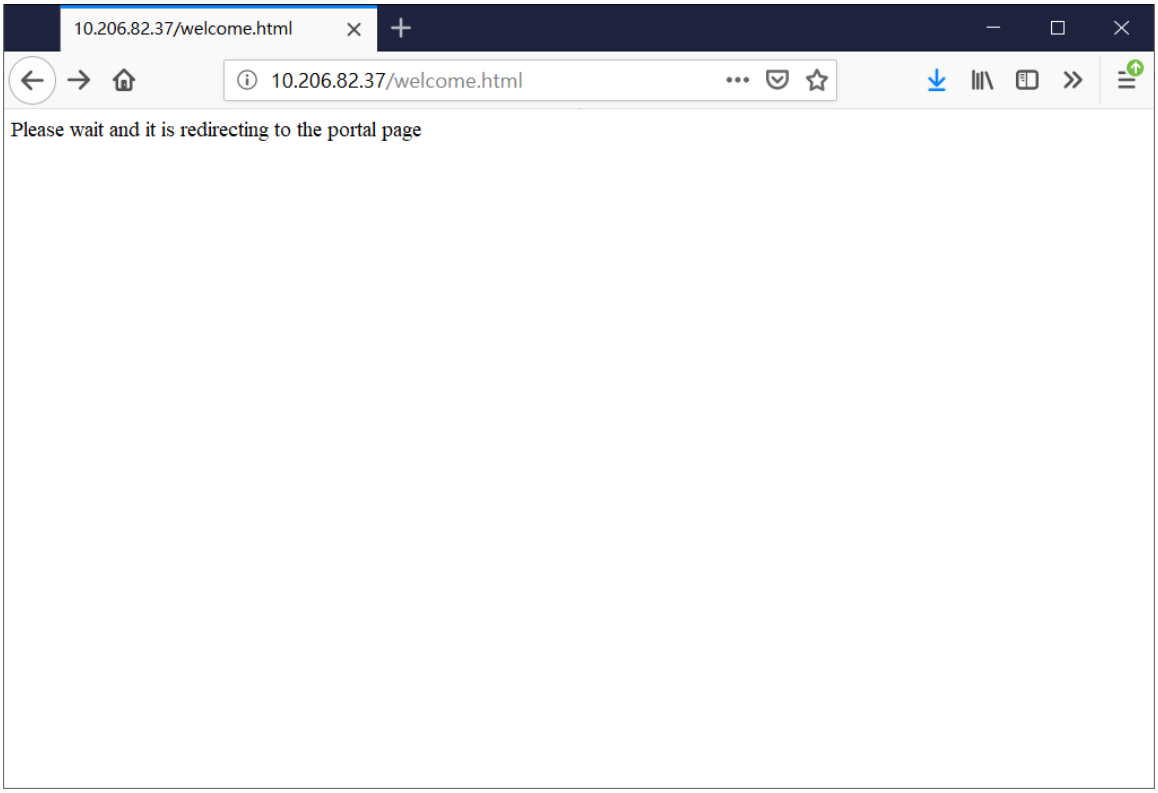
3. Click **Create**.

   The **Create Guest Access Portal** page appears.

FIGURE 255 Creating a Guest Access Portal



4. Configure the following:
   a. General Options
      - Portal Name: Type a name for the guest access service portal that you are creating.
      - Portal Description: Type a short description of the guest access service portal.
      - Language: Select the display language to use for the buttons on the guest access logon page.
   b. Redirection: Select where to redirect the user after successfully completing authentication.
      - Redirect to the URL that the user intends to visit: Allows the guest user to continue to their destination without redirection.
      - Redirect to the following URL: Redirects to the specified domain name or IP address. When the Guest Access Portal's Guest Authentication is "Always Accept" and the Guest Access does nott enable the "Terms and Conditions", the client will be redirected to this page for 3 seconds and then go to the start URL or the original URL the browser opens". After 3 seconds redirect to the Start Page.



   c. Guest Access
      - Self Registration: Enable the option to register for the guest pass.
      - Guest Pass SMTP Server: Enable the option to receive the copy of guest pass by email.
      - Guest Pass SMS Gateway: You can deliver the guest pass to the user using Short Message Service (SMS). But first you need to configure an SMS server. If you previously configured an SMS server, you can select it here or you can select **Disable**.
      - Terms and Conditions: To require users to read and accept your terms and conditions prior to use, **Show Terms and Conditions** check box. The box below, Terms and Conditions which contains the default Terms of Use text, becomes editable. Edit the text or leave it unchanged to use the default text.
      - Web Portal Logo: By default, the guest hotspot logon page displays the RUCKUS logo. To use your own logo, click the **Browse** button, select your logo Web Portal Logo (recommended size is 138 x 40 pixels, maximum file size is 20KB), and then click **Open**.

- Web Portal Title: Type your own guest hotspot welcome text or accept the default welcome text (Welcome to the Guest Access login page).
- Pass Effective Since: Set the guest pass validity period by selecting one of the following options:
  - Effective from the creation time: This type of guest pass is valid from the time it is first created to the specified expiration time, even if it is not being used by any end user.
  - Effective from first use: This type of guest pass is valid from the time the user uses it to authenticate with the controller until the specified expiration time. An additional parameter (Guest Pass will expire in X days) can be configured to specify when an unused guest pass will expire regardless of use. The default is 7 days.
  - Expire guest pass if not used within [ ] days: If you want this guest pass to expire if it is unused after you generated it, type the number of days in the box (maximum value is 365 days).
- Max Devices Allowed: Set the number of users that can share this guest pass.
  - Limited to [ ]: If you want a limited number of users to share this guest pass, click this option, and then type the number in the box.
  - Unlimited: If you want an unlimited number of users to share this guest pass, click this option.
  - Session Duration: If you clicked Unlimited, this option appears. If you want require users to log on again after their sessions expire, select the Require guest re-login after [ ] check box, and then select a time increment. If this feature is disabled, connected users will not be required to re-log in until the guest pass expires.
- Notification Method: Select how the guest pass must be notified to the user. For example: E-Mail, Mobile, and Mobile and E-mail.

d. User Session

- Session Timeout: Specify a time limit after which users will be disconnected and required to log on again.
- Grace Period: Set the time period during which clients will not need to re-authenticate after getting disconnected from the hotspot. Enter a number (in minutes) between 1 and 14399.

5. Click **OK**.

You have completed creating a guest access service.

NOTE
You can also edit, clone and delete a guest access portal by selecting the options **Configure**, **Clone** and **Delete** respectively, from the **Guest Access** tab.

Working with Hotspot (WISPr) Services

A hotspot is a venue or area that provides Internet access to devices with wireless networking capability such as notebooks and smart phones.

Hotspots are commonly available in public venues such as hotels, airports, coffee shops and shopping malls. Configure a traditional (WISPr 1.0) hotspot service to provide public access to users via its WLANs. In addition to the controller and its managed APs, you will need the following to deploy a hotspot:

Captive Portal: A special web page, typically a login page, to which users that have associated with your hotspot will be redirected for authentication purposes. Users will need to enter a valid user name and password before they are allowed access to the Internet through the hotspot.

RADIUS Server: A Remote Authentication Dial-In User Service (RADIUS) server through which users can authenticate.

For installation and configuration instructions for the captive portal and RADIUS server software, refer to the documentation that was provided with them. After completing the steps below, you will need to edit the WLAN(s) for which you want to enable Hotspot service. The controller supports up to 32 WISPr hotspot service entries, each of which can be assigned to multiple WLANs.

Creating a Hotspot (WISPr) Portal

To create a hotspot service, you must define the required basic settings.

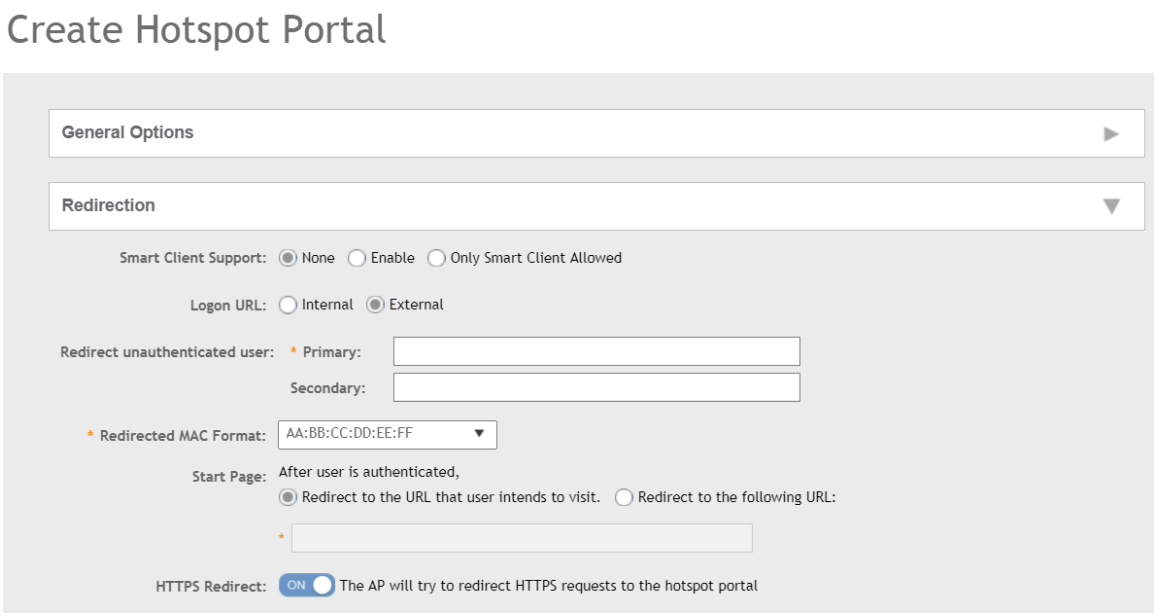
SZ supports only one grace period, session timeout, UTP, VLAN and all UE session related configuration. These configurations for the first WLAN do not work when the UE joins the second WLAN. The configuration works only when the UE roams within the cluster node. The configurations do not work when the client roams from one zone to another zone or from one cluster to another cluster.

Before creating a hotspot, you need to create a user defined interface.

1. Go to **Services** > **Hotspots & Portals** > **Hotspot (WISPr)**.
2. From the **Hotspot (WISPr)** tab select the zone for which you want to create the portal.
3. Click **Create**.

   The **Create Hotspot Portal** page is displayed.

FIGURE 256 Creating a Hotspot (WISPr) Portal



4. Under **General Options**, enter portal name and portal description.

5. Under **Redirection**, select where to redirect the user after successful authentication.
   a. For **Smart Client Support**, select one of the following options:
      - **None**: Disables Smart Client Support on the hotspot service.
      - **Enable**: Enables Smart Client Support.
      - **Only Smart Client Allowed**: Allows only Smart Clients to connect to the hotspot service.
   b. For **Logon URL**, select one of the following options:
      - **Internal**: Indicates the internal URL of the subscriber portal (where hotspot users can log in to the service).
      - **External**: Indicates the external URL of the subscriber portal.

        Selecting **External** provides an option to reroute an unauthorized user to a primary location. You can set the primary location in **Redirect unauthenticated user**. If an unauthorized user is rerouted, the AP redirects the UE to a backup portal.

        The AP subscriber portal supports ZD-style API to login and logout. A customer can use AP IP address to submit the login or logout request.
   c. **Redirect unauthenticated user**: APs can perform WISPr redirection. Native WISPr support is available on SZ-managed APs even if access to SZ is not available. It supports external portal redirection with survivability when APs cannot reach the centralized SZ. It also supports backup portal redirection if primary portal is down. The WISPr authentication load can be distributed to AP or use an AP as a WISPr authentication backup.

      WISPr redirection and survivability is supported only on Ruckus 11AC Wave 1 and later APs. Only ZD-style external WISPr is supported. No NBI is supported for backup.
      - **Primary**: Redirects an unauthenticated user to a specified URL for authentication.
      - **Secondary**: Redirects an unauthenticated user to the backup external portal if the primary URL is down. The AP periodically accesses the primary portal URL to detect and check the availability of the primary URL.

        NOTE
        The AP uses the secondary portal when the AP cannot access the primary portal.
   d. In the **Redirected MAC Format** field, enter the format of the redirection MAC address.
   e. For **Start Page**, select one of the following options:
      - **Redirect to the URL that the user intends to visit**: Redirects users to the page that they want to visit.
      - **Redirect to the following URL**: Sets a different page where users will be redirected (for example, your company website). Enter a domain name or an IP address to be redirected.
   f. Enable **HTTPS Redirect** if you want the AP to redirect HTTPS requests to the hotspot portal. HTTPS requests are dropped if this option is disabled.
6. Under **User Session**, set the session timeout and grace period.
   - **Session Timeout**: Sets a time limit (in minutes) after which users will be disconnected from the hotspot service and required to log in again.
   - **Grace Period**: Sets the time period (in minutes) during which disconnected users are allowed access to the hotspot service without logging in again.

7. Under **Location Information**, set the location ID and location name.
   a. In **Location ID**, enter the ISO and ITU country and area code that the AP includes in accounting and authentication requests. The code includes the following requirements:
      - isocc (ISO-country-code): The ISO country code that the AP includes in RADIUS authentication and accounting requests.
      - cc (country-code): The ITU country code that the AP includes in RADIUS authentication and accounting requests.
      - ac (area-code): The ITU area code that the AP includes in RADIUS authentication and accounting requests.
      - network: Name of the network.

      The following example illustrates a proper location ID entry: isocc=us,cc=1,ac=408,network=Ruckus
   b. For **Location Name**, enter the name of the location of the hotspot service.
8. Under **Walled Garden/Traffic Class Profile**, add a user to a walled garden and provide access.
   - **Walled Garden**
     a. Click ; in **Walled Garden Entry**, enter an IP address or a domain name and click **Add**.
     b. Select the entry and click **Import CSV** to import the CSV file with the user information.
   - **Traffic Class Profile**: Select a traffic class profile from the list or click **+** to create a traffic class profile. Refer to Creating a Traffic Class Profile on page 423 for more information.
9. Under **Advanced Options**, select the required options:
   a. Click **Use Token Redirect URL** and enter a signature signing key.
   b. Click **Enable Internal Node** and enter the internal node.

      NOTE
      If an **Internal node** is enabled, then only one IP is used and the IP domain name and IP ranges are not supported.

10. Click **OK**.

You have completed creating a Hotspot (WISPr) portal.

NOTE
If **Traffic Class Profile** or **Use Token Redirect URL** is enabled, **Smart Client Support** is set to **None**.

NOTE
You can also edit, clone, and delete a Hotspot (WISPr) portal by selecting the **Configure**, **Clone**, and **Delete** options respectively from the **Hotspot (WISPr)** tab.

Working with Hotspot 2.0 Services

You must be aware of Hotspot 2.0 - a Wi-Fi Alliance specification that allows for automated roaming between service provider access points when both the client and access gateway support the newer protocol.

Hotspot 2.0 (also known as Passpoint™, the trademark name of the Wi-Fi Alliance certification) aims to improve the experience of mobile users when selecting and joining a Wi-Fi hotspot by providing information to the station prior to association.

This information can then be used by the client to automatically select an appropriate network based on the services provided and the conditions under which the user can access them. In this way, rather than being presented with a list of largely meaningless SSIDs to choose from, the Hotspot 2.0 client can automatically select and authenticate to an SSID based on the client's configuration and services offered, or allow the user to manually select an SSID for which the user has login credentials.

The controller's Hotspot 2.0 implementation complies with the IEEE 802.11u standard and the Wi-Fi Alliance Hotspot 2.0 Technical Specification.

See the *Hotspot 2.0 Reference Guide for SmartZone* for information on configuring Hotspot 2.0 services, including:

- Working with Hotspot 2.0 operator profiles
- Working with Hotspot 2.0 identity providers
- Creating a Hotspot 2.0 online signup portal

Creating a Hotspot 2.0 WLAN Profile

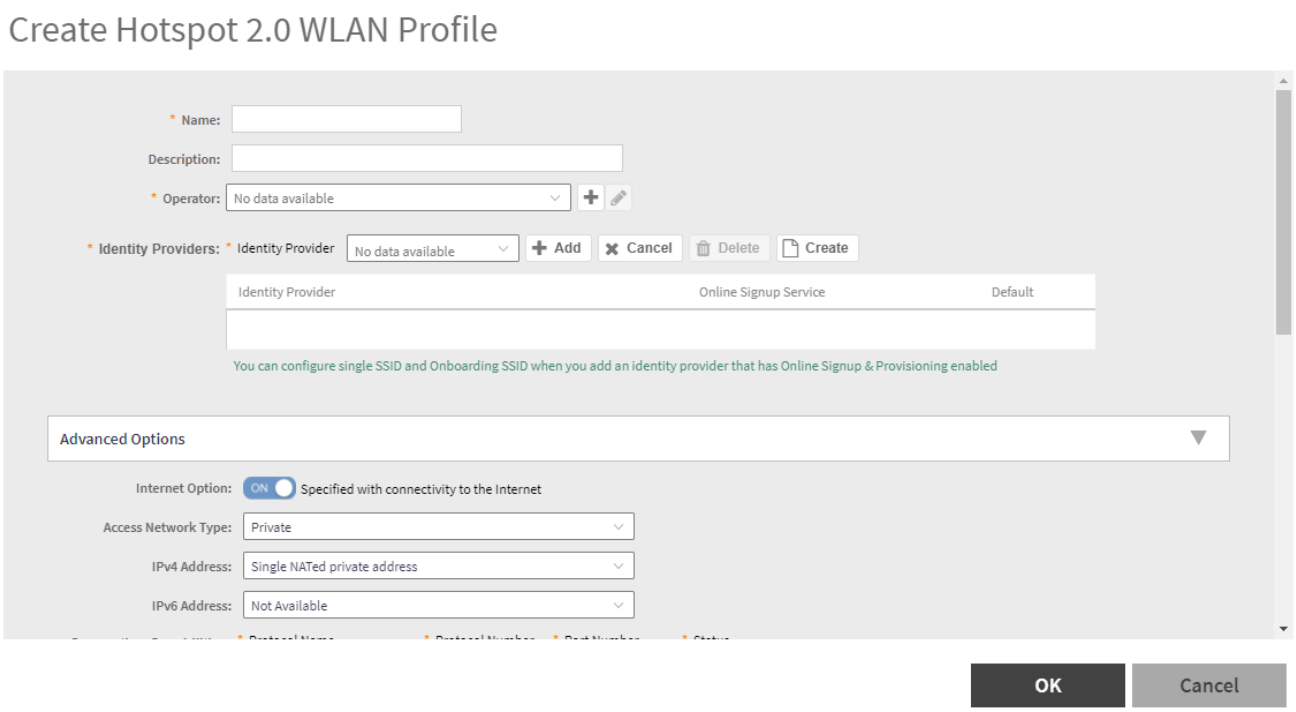
You can assign and Hotspot 2.0 service to a Hotspot 2.0 WLAN, for which you must create a Hotspot 2.0 WLAN profile.

Follow these steps to create a Hotspot 2.0 WLAN profile.

1. Go to **Services** > **Hotspots & Portals**.
2. Select the **Hotspot 2.0** tab, and then select the zone for which you want to create the profile.
3. From WLAN Profile, click **Create**.

   The **Create Hotspot 2.0 WLAN Profile** page appears.

   FIGURE 257 Creating a Hotspot 2.0 WLAN Profile



4. Configure the following:
   a. Name: Enter a name for this WLAN profile. This name identifies the WLAN profile when assigning an HS2.0 service to a HS2.0 WLAN.
   b. Description: Enter a description for the WLAN profile.
   c. Operator: Select the operator profile. This name identifies the service operator when assigning an HS2.0 service to a HS2.0 WLAN.

      You can also click **Create** to create a Hotspot 2.0 WiFi operator. See Creating a Hotspot 2.0 WiFi Operator Profile on page 455 for more information.
   d. Identity Provider: Choose one or more identity providers. Choose the identity provider. You can configure an OSU SSID when you add an Identity Provider which enables OSU and provisioning. Since there may be more than one identity provider per Hotspot 2.0 profiles having its own authentication profile, the No Match and Unspecified mapping could be duplicated. To avoid duplication, the default identity provider is taken as the correct configuration for No Match and Unspecified mapping. OSUSSID can be OSEN or OPEN [Guest].

      You can also click **Create** to create a Hotspot 2.0 identity provider. See Creating a Hotspot 2.0 Identity Provider on page 457 for more information.
   e. Single SSID: Provides capability to support both OSU network and production network on the same WLAN. This option is available only when the Identity Provider has enabled Online Signup & Provisioning.
   f. Onboarding SSID: Allows the devices to connect to a Wi-Fi network automatically, where the service providers engage in roaming partnership to provide seamless access to Wi-Fi networks. Onboarding SSID is an optional configuration when Single SSID is enabled and a mandatory configuration when Single SSID is not enabled. This option is available only when the Identity Provider has enabled Online Signup & Provisioning.
   g. Advanced Options:
      - Internet Options: Specify if this HS2.0 network provides connectivity to the Internet.
      - Access Network Type: Access network type (private, free public, chargeable public, etc.), as defined in IEEE802.11u.
      - IPv4 Address: Select IPv4 address type availability information, as defined in IEEE802.11u
      - IPv6 Address: Select IPv6 address type availability information, as defined in IEEE802.11u
      - Connection Capabilities: Provides information on the connection status within the hotspot of the most commonly used communications protocols and ports.

        Provide the **Protocol Name**, **Protocol Number**, **Port Number** and **Status** to **Add** a new connection.
      - Custom Connection Capabilities: Allows addition of custom connection capability rules. Up to 21 custom rules can be created.

        Provide the **Protocol Name**, **Protocol Number**, **Port Number** and **Status** to **Add** a new connection.
5. Click **OK**.

You have completed creating a Hotspot 2.0 WLAN profile.

NOTE
You can also edit, clone and delete a Hotspot 2.0 WLAN profile by selecting the options **Configure**, **Clone** and **Delete** respectively, from the **WLAN Profile** section in the **Hotspot 2.0** tab.

Creating a Hotspot 2.0 WiFi Operator Profile

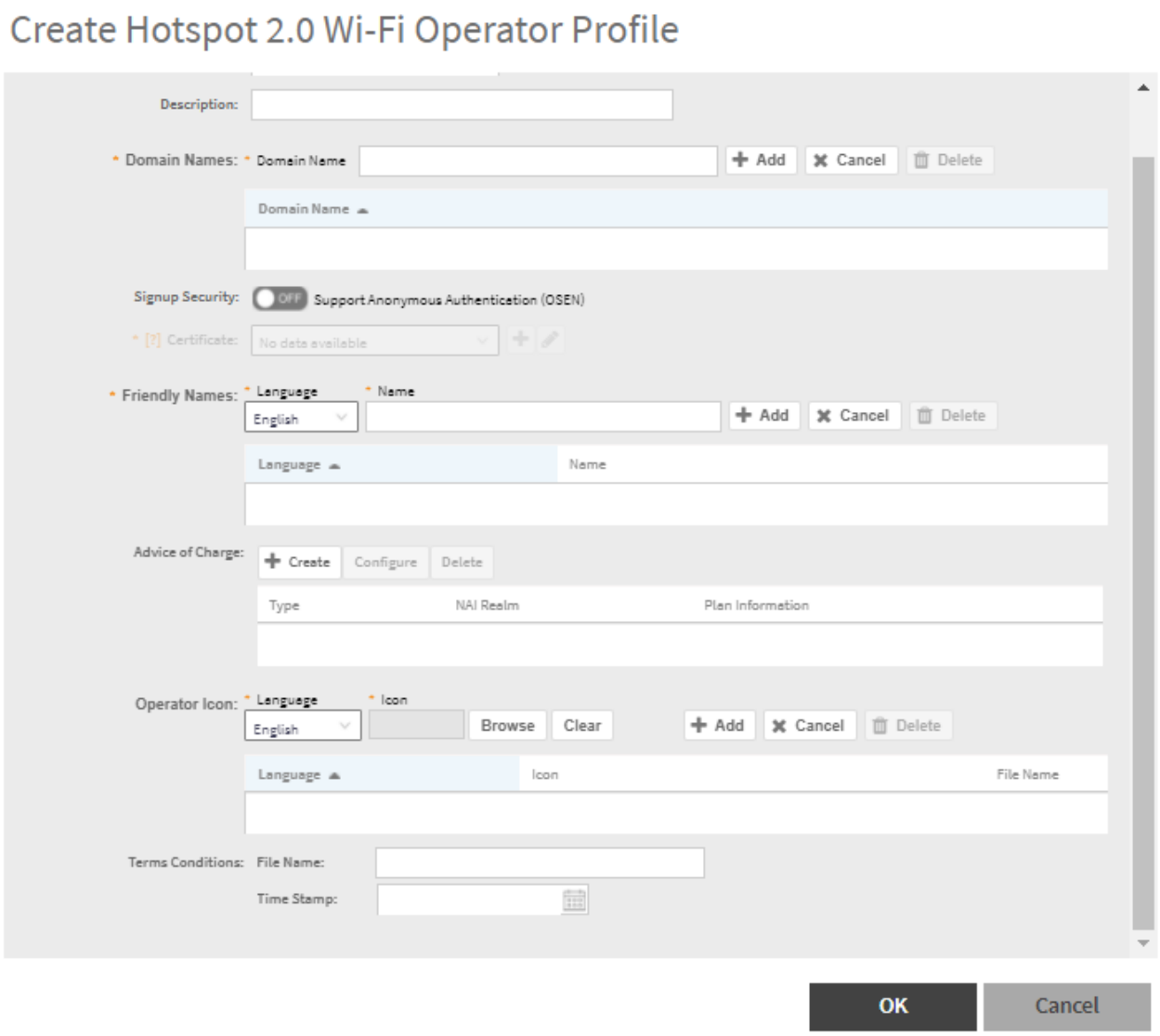
An operator profile defines all the properties pertaining to an operator while a service profile defines the properties related to a service provider. If a WLAN is configured to provide Hotspot 2.0 service, it must be linked exactly like a Hotspot 2.0 operator profile.

1. Go to **Services** > **Hotspots & Portals**.
2. Select the **Hotspot 2.0** tab, and then select the device for which you want to create the profile.

3. From **Wi-Fi Operator**, click **Create**.

   The **Create Hotspot 2.0 Wi-Fi Operator Profile** page is displayed.

   FIGURE 258 Creating a hotspot 2.0 Wi-Fi operator profile



4. Configure the following:
    a. Name: Enter a name for this Wi-Fi operator profile.
    b. Description: Enter a description for the venue profile.
    c. Domain Names: HS2.0 operator's domain name is a mandatory field, which specifies the operator's domain name. Hotspot 2.0 AP broadcasts the domain name to indicate the home Wi-Fi providers.
    d. Signup Security: This is an optional field and is disabled by default. Enabling would mean that operator supports secure onboarding (OSEN).
    e. Certificate: Select the certificate for the operator - AAA. This can be the same certificate as the one used with OSU service.
    f. Friendly Names: HS2.0 operator's friendly name is a mandatory field. Operator's friendly name is displayed on mobile client's screen. It is also used for operator verification during secure onboarding (OSEN). Select the display language from the drop down list.
    g. Advice of Charge: The advice of charge may be issued for the first time or every time a user connects to a Wi-Fi service. The advice of charge must be acknowledged before accessing the network. Click **Create**. The **Create Advice of Charge** form is displayed.
        1. Type: Select one of the following plan type.
            - Time-Based
            - Data-Volume-Based
            - Time-and-Data-Volume-Based
            - Unlimited
        2. NAI Realm: Select one of the following encoding option.
            - Encoding
            - Name
        3. Plan Information: The plan information is provided on a per NAI-realm basis. Each authentication realm can advertise the charges associated with obtaining the network access. Click **Create**, the **Create Plan Information** form is displayed. Update the following plan information.
            - Language
            - Currency
            - XML content
        4. Click **OK**.
    h. Operator Icon: A maximum of two icons can be uploaded for an operator profile. The maximum size of an icon can be upto 64 KB. Select the **Language**, click **Browse** to select an icon, and click **Add**.
    i. Terms Conditions: Allows to communicate the terms and conditions of the Wi-Fi services. Updated terms and conditions can also be communicated to existing service users. Update the following information.
        - File Name
        - Time Stamp
5. Click **OK**.

Creating a Hotspot 2.0 Identity Provider

The Hotspot 2.0 Identity provider provides authentication, accounting and online sign-up service. There can be one or more identity providers per Hotspot 2.0 access WLAN.

To configure the Hotspot 2.0 Identity Provider, go to **Services** > **Hotspot & Portals** > **Hotspot 2.0** > **Identity Provider** and click **Create**. The **Create Hotspot 2.0 Identity Provider** page is displayed. Configure the following details to create a Hotspot 2.0 Identity Provider:

1. Network Identifier

2. Online Signup and Provisioning
3. Authentication
4. Accounting
5. Review

Network Identifier

1. Configure the following:
   a. Name: Enter a name or this network identifier profile.
   b. Description: Enter a description for the network identifier profile.
   c. PLMNs: Each record contains MCC and MNC.

      MCC: Set the correct country code for the geographical location. This is required when the controller sends MAP authentication information. Type the mobile country code digits. Decimal digit strings with maximum length of 3 and minimum length of 2.

      MNC: Set the mobile network code based on the geographical location. This is required when controller sends MAP authentication information. Type the mobile network code digits. Decimal digit strings with maximum length of 3 and minimum length of 2.
   d. Realms: List of NAI realms corresponding to service providers or other entities whose networks or services are accessible via this AP. Up to 16 NAI realm entries can be created. Each NAI realm entry can contain up to four EAP methods. You can add a realm by providing the realm **Name**, **Encoding technique** (choose between RFC-4282 and UTF-8) and **EAP Methods**.
   e. Home OIs: Organization Identifier (OI) is a unique value assigned to the organization. User can configure a maximum of 12 OI values and can adjust the order since the AP takes only 3 OIs in the beacon.
2. Click **Next**.

You have completed creating a Hotspot 2.0 Identity Provider - Network Identifier.

Online Signup and Provisioning

1. Configure the following:
   a. Provisioning Options
      - Provisioning Service: The provisioning service is responsible for any subscription provisioning process in which messages are communicated between the UE and the SZ resulting in a PPS-MO provisioned into the UE. The provisioning supports both SOAP-XML and OMA-DM as communication protocols for the process based on the initial request coming from the UE. The provisioning service supports sign-up; remediation and policy update flows where the UE is provisioned with a full PPS -MO or only with internal node/s of the PPS-MO. Administrator can only set External Internal Provisioning Services, where the administrator is required to fill the external OSU server URL.
      - Provisioning Protocol: Select communication protocols OMA-DM or SOAP-XML.
   b. Online Signup Options
      - OSU NAI Realm: This configuration is only for External Provision Service. In case of Internal Provisioning Service, the NAI realm should be configured per authentication service, which is available during on-boarding.
      - Single SSID NAI: This configuration is for enabling single SSID for WLAN profile, The NAI length can have a maximum of 255 charecters.
      - Common Language Icon: This is the default icon presented in the device for this identity provider in case the device does not find any match for other icons per language in the table.
      - OSU Service Description: This table configures the friendly name, description and icon per language. This information is presented on the device when it receives ANQP message which includes OSU providers. Friendly names, which are required to be part of the OSU certificate is automatically populated in this table. In case description is also included in the OSU certificate it is automatically populated into the table. Administrators are required to set the matched icon per language as included in the OSU certificate.
      - Whitelisted Domain: Add the domain names of the External Portal domain.
2. Click **Next**.

You have completed creating a Hotspot 2.0 Identity Provider - Online Signup and Provisioning.

Authentication

1. Configure the following:
   a. Realm: configure the realm mapping to the authentication service.
   b. Auth Service: map the realm to an external RADIUS server which should be pre-configured.
   c. Dynamic VLAN ID: type the VLAN ID.
2. Click **Next**.

You have completed creating a Hotspot 2.0 Identity Provider - Authentication.

Accounting

1. Configure the following:
   a. Realm: if the authentication's realm is set as remote credential type, administrator should set this realm here to the customer's external accounting server.
   b. Accounting Service: select the accounting service.
2. Click **Next**.

You have completed creating a Hotspot 2.0 Identity Provider - Accounting.

Review

Review the configuration on the page before committing the changes to the server. Click **Create** to create the Hotspot 2.0 Identity Provider.

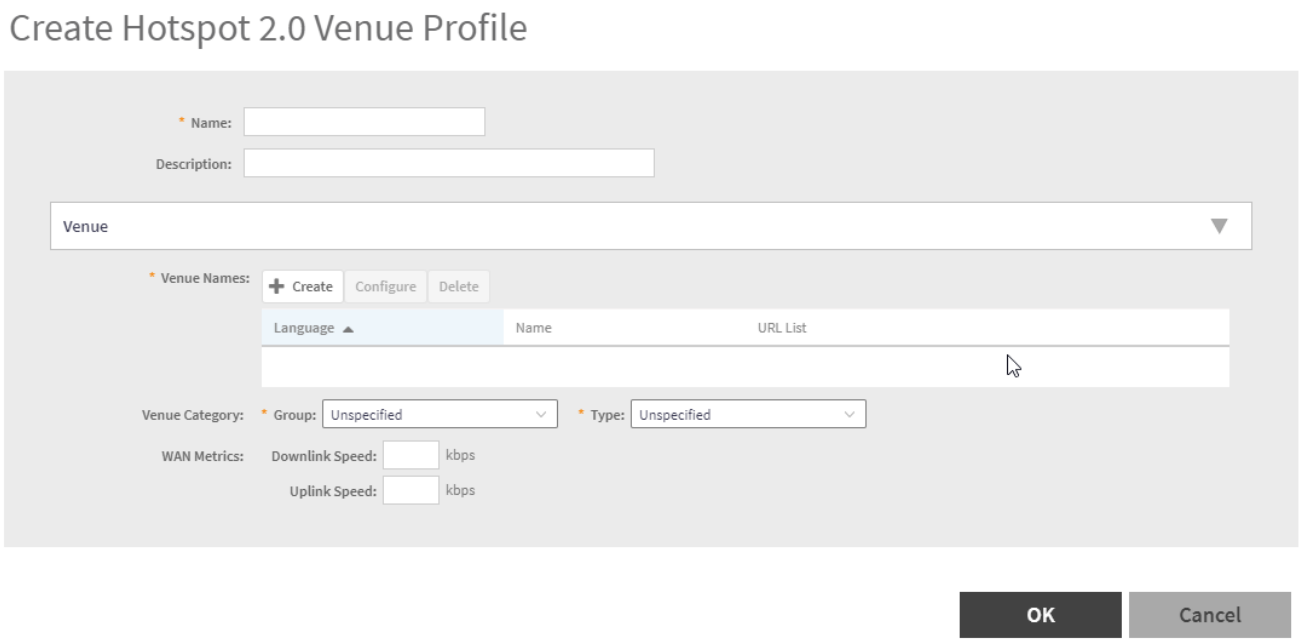
Creating a Hotspot 2.0 Venue Profile

The Hotspot 2.0 technology allows users to seamlessly roam between the provider's home Wi-Fi network and the visited Wi-Fi network in a different location. A Wi-Fi provider can partner with several roaming partners to provide Wi-Fi access to partner's subscribers. Public venues such as institutions, restaurants, and stadiums are considered roaming partners.

1. Go to **Services** > **Hotspots & Portals**.
2. Select the **Hotspot 2.0** tab, and then select the zone for which you want to create the profile.
3. From **Venue profiles**, click **Create**.

   The **Create Hotspot 2.0 Venue Profile** page appears.

FIGURE 259 Creating a Hotspot 2.0 Venue Profile



4. Configure the following:
   a. Name: Enter a name for this venue profile. This name identifies the venue profile when assigning an HS2.0 service to a HS2.0 venue.
   b. Description: Enter a description for the venue profile.
   c. Venue Names: Select the venue from the list or click **Create** to create a new venue. The **Create Venue Names** form is displayed.
      1. Venue Names: Select the language from the list.
      2. Name: Enter a name for the new venue.
      3. URL: Enter additional URLs to the venue name and click **Add**. The URL can have a maximum of 254 charecters. A maximum of four venue URLs can be mapped to a venue name.
      4. Click **OK**.
   d. Venue Category: Select venue group and venue type as defined in IEEE802.11u, Table 7.25m/n.
   e. WAN Metrics: Provides information about the WAN link connecting an IEEE 802.11 access network and the Internet; includes uplink/downlink speed estimates.

      Select the operator profile. This name identifies the service operator when assigning an HS2.0 service to a HS2.0 WLAN.
5. Click **OK**.

You have completed creating a Hotspot 2.0 Venue profile.

NOTE
You can also edit, clone and delete a Hotspot 2.0 venue profile by selecting the options **Configure**, **Clone** and **Delete** respectively, from the **Venue Profile** section in the **Hotspot 2.0** tab.

Creating a Web Authentication Portal

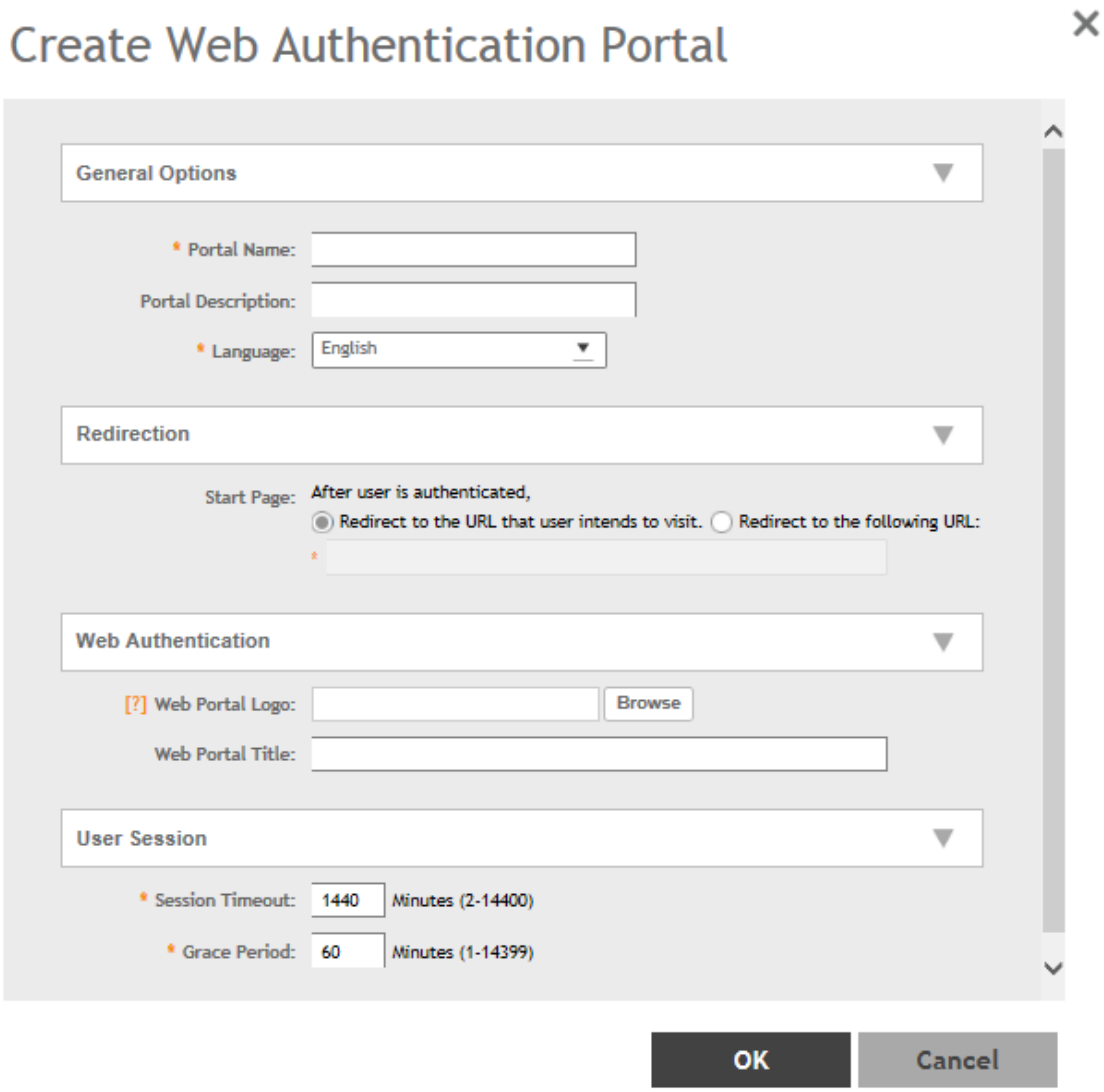
Web Authentication (also known as a “captive portal”) redirects users to a login web page the first time they connect to this WLAN, and requires them to log in before granting access to use the WLAN.

1. Go to **Services** > **Hotspots & Portals**.
2. Select the **Web Auth** tab, and then select the zone for which you want to create the portal.

3. Click **Create**.

   The **Create Web Authentication Portal** page is displayed.

FIGURE 260 Creating a Web Authentication Portal



4. Configure the following options:
   - General Options
     - Portal Name: Type a name for the hotspot service portal that you are creating.
     - Portal Description: Type a short description of the hotspot service portal.
     - Language: Select the display language that you want to use on the web authentication portal.
   - Redirection (Select where to redirect the user after successfully completing authentication.)
     - Redirect to the URL that user intends to visit: Allows the guest user to continue to destination URL without redirection.
     - Redirect to the following URL: Redirect the user to a specified web page (entered into the text box) prior to forwarding to the destination URL. When a guest user lands on this page, the guest pass expiration time is displayed.

       Enter a domain name or IP address to which to be redirected.
   - Web Authentication
     - Web Portal Logo: By default, the web portal page displays the Ruckus logo. To use your own logo, click the **Browse** button, select your web portal logo (recommended size is 138 x 40 pixels, maximum file size is 20 KB), and then click **Open**.
     - Web Portal Title: Type your own web portal title text or accept the default portal title text (Welcome to the Web Authentication login page).
   - User Session
     - Session Timeout: Set a time limit (in minutes) after which users will be disconnected from the hotspot service and will be required to log in again.
     - Grace Period: Set the time period (in minutes) during which disconnected users are allowed access to the hotspot service without having to log in again.
5. Click **OK**.

You have completed creating a Web Authentication.

NOTE
You can also edit, clone, or delete a Web Authentication by selecting the options **Configure**, **Clone**, and **Delete**, respectively, from the **Web Auth** tab.

Creating a UA Blacklist Profile

The controller automatically blocks certain user agents (or software used by a user) from accessing hotspots provided by controller-managed APs. When the controller blocks any of these user agents, an error message appears on the user device. You can add to or remove user agents from this blacklist.

Following are some of the blocked user agents:

- ZoneAlarm
- VCSoapClient
- XTier NetIdentity
- DivX Player
- Symantec LiveUpdate
- Windows Live Messenger
- StubInstaller
- windows-update-agent
- Windows Live Essentials
- Microsoft Dr. Watson for Windows (MSDW)

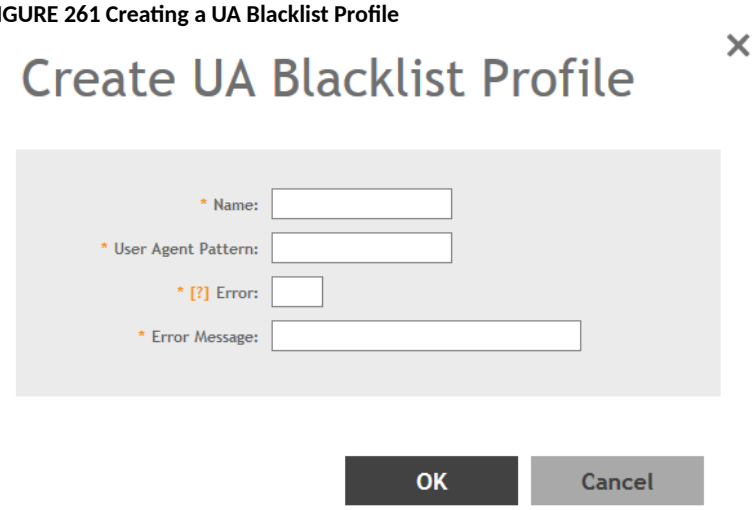
- Avast Antivirus Syncer
- Microsoft Background Intelligent Transfer Service (BITS)
- Google Update
- TrendMicro client
- Skype WISPr

To blacklist a user agent profile:

1. Go to **Services** > **Hotspots & Portals** > **UA Blacklist**.
2. From the **UA Blacklist** tab, click **Create**.

   The **Create UA Blacklist Profile** page is displayed.

   FIGURE 261 Creating a UA Blacklist Profile



3. Configure the following:
   a. Name: Enter the name of the user agent.
   b. User Agent Pattern: Type the agent pattern.
   c. Error: Specify the error message number.
   d. Error Message: Specify the error message.
4. Click **OK**.

You have completed creating a UA Blacklist Profile

NOTE
You can also edit, clone, and delete a UA blacklist profile by selecting the options **Configure**, **Clone** and **Delete** respectively, from the **UA Blacklist** tab.

Creating a Portal Detection and Suppression Profile

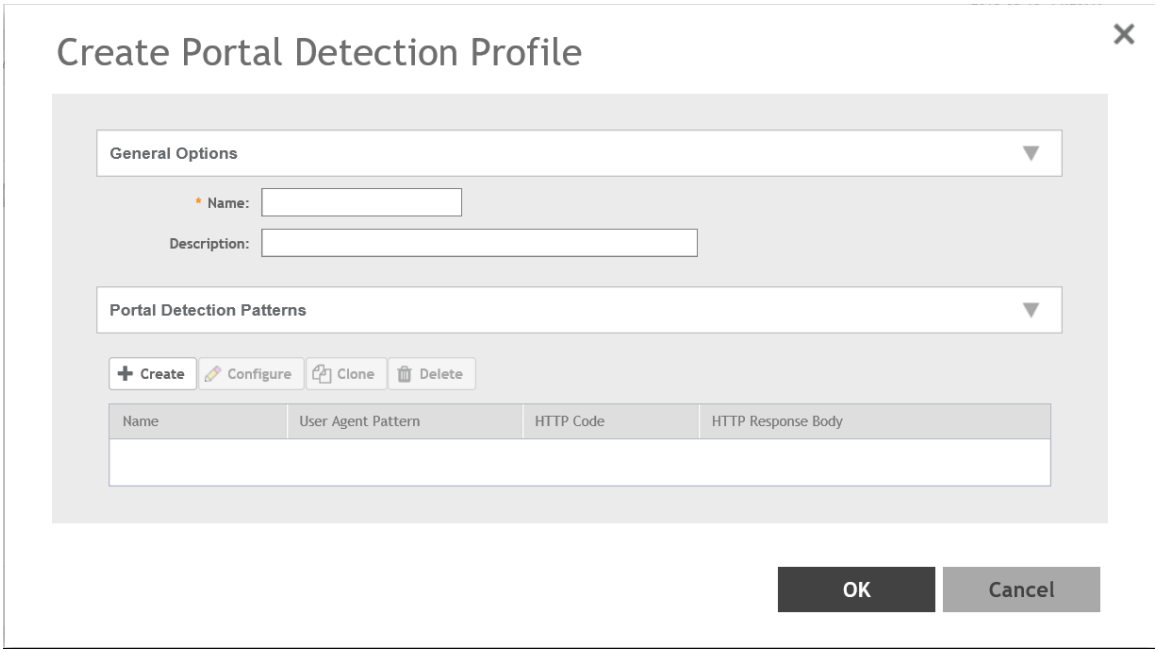
To restrict an unauthorized user in a walled garden, a service operator must set defined policy rules by creating a portal detection and suppression profile.

1. Select **Services** > **Hotspots & Portals** > **Portal Detection & Suppression**.
2. From the **Portal Detection & Suppression** tab.

3. Select a zone and click **Create** to add a portal detection and suppression profile.

   The **Create Portal Detection Profile** page is displayed.

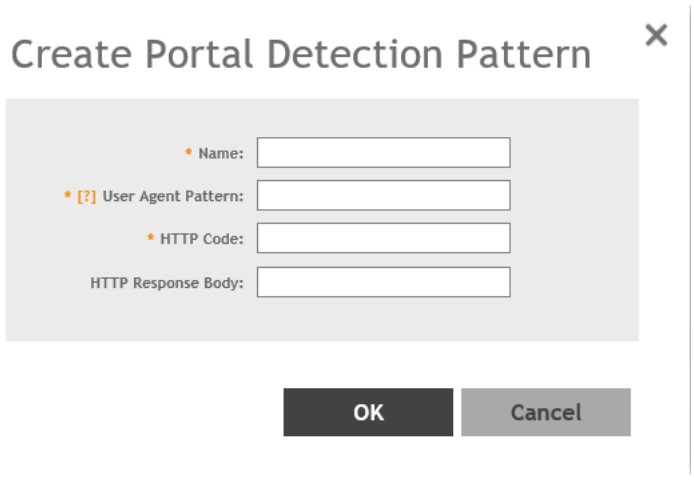
FIGURE 262 Creating Portal Detection Profile



4. Under **General Options**, enter a policy list name and description.
5. Under **Portal Detection Patterns**, click **Create** to create a portal detection pattern.

   The **Create Portal Detection Pattern** page is displayed.

FIGURE 263 Creating Portal Detection Pattern



6. In the **Name** field, enter the name of the portal detection pattern.

7. In the **User Agent Pattern** field, enter the user agent pattern.

   NOTE
   The user agent pattern must follow a regular expression format, starting and ending with .* (for example, .*Android-WiFi.*). The default Captive Portal Detection may not support all the Android devices and the new Microsoft phone if different user agent patterns are used. In this case, new rules must be created to cover such patterns. Using an improper user agent pattern may impact browser behaviors.

8. In the **HTTP Code** field, enter the code.

   NOTE
   The HTTP code range must be from 100 through 599.

9. In the **HTTP Response Body** field, enter the HTML string.
10. Click **OK**.

    NOTE
    To select a **Portal Detection Pattern** profile, **Bypass CNA** must be enabled in the WLAN configuration page. Use **Bypass CNA** to enable or disable Portal Detection Service for HotSpot, Web Authentication, and Guest Access WLAN.

Creating a WeChat Portal

WeChat is a mobile app from Tenecent that enables its users to call and send text messages to one another. If you have WeChat users on the network and you want your WLANs to support WeChat services, you can create a WeChat portal that WeChat users can use.

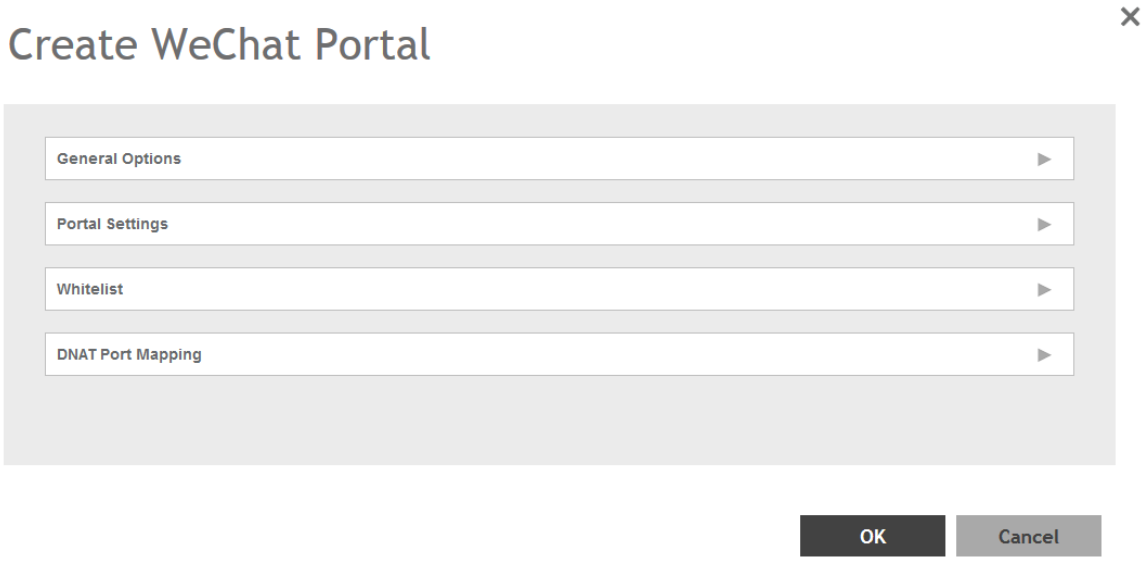
A WeChat portal defines the third party authentication server, also known as the equipment service provider (ESP) server, to which the controller will forward all WeChat authentication requests from wireless devices that are associated with controller-managed APs. In turn, the third party authentication server will forward these authentication requests to the WeChat server.

1. Go to **Services** > **Hotspots & Portals**.
2. Select the **WeChat** tab, and then select the zone for which you want to create the portal.

3. Click **Create**.

   The **Create WeChat Portal** page appears.

FIGURE 264 Creating a WeChat Portal



4. Configure the following:
   a. General Options
      - Name: Type a name for the portal that you are creating.
      - Description: Type a short description of the portal.
   b. Portal Settings: configure the following
      - Authentication URL: Type the authentication interface URL on the third party authentication server. When a managed AP receives a WeChat logon request from a client device, it will send the request to this authentication URL and get the authorization result.
      - DNAT Destination: Type the DNAT destination server address to which the controller will forward HTTP requests from unauthenticated client devices. The DNAT destination server and the authentication server (above) may or may not be the same server.
      - Grace Period: Type the number of minutes during which disconnected users who were recently connected will be allowed to reconnect to the portal without needing to re-authenticate. The default grace period is 60 minutes (range is between 1 and 14399 minutes).
      - Blacklist: Type network destinations that the controller will automatically block associated wireless clients from accessing. Use a comma to separate multiple entries.
   c. Whitelist: Type network destinations that the controller will automatically allow associated wireless clients to access. You can add a single entry or multiple entries.

      To add a single entry, type the entry in **Wall Garden Entry**, and then click **Add**. The entry you added appears in the table below. To add multiple entries, in a comma-separated value (CSV) file, type all the network destinations that you want to add to the whitelist, and then save the CSV file. In the Whitelist section, click **Import CSV**, and then select the CSV file you created. Click Open. The entries in the CSV file are added to the whitelist.
   d. DNAT Port Mapping: specify at least one pair of source-to-destination port mapping. To add a port mapping, type the source and destination ports in the boxes provided, and then click **Add**. The AP will use this information to drop or forward HTTP requests from associated clients to specified ports on the DNAT server. For example, if an HTTP request from a wireless client does not originate from the specified source (from) port, the AP will discard the HTTP request. By default, a port mapping of 80-80 (source-destination) exists.
5. Click **OK**.

You have completed creating a WeChat portal.

NOTE
You can also edit, clone and delete a WeChat service portal by selecting the options **Configure**, **Clone** and **Delete** respectively, from the **WeChat** tab.

Creating Network Segmentation Profile on the vSZ Controller

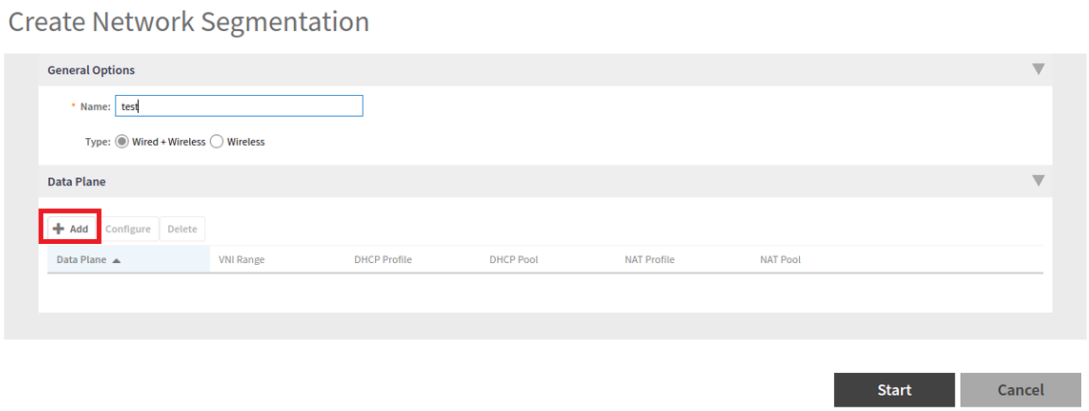
Network Segmentation was designed specifically to target Multi Dwelling Unit (MDU) deployments. Network Segmentation is currently using external Dynamic Pre shared Key (DPSK) to place a single tenant and their devices into their own individual VXLAN (iLAN).

Data Plane (DP) will play the role of Home DP or Partner DP. Each DP plays the home DP role and has its own VXLAN Network Identifier (VNI) range. Home DP facilitates MDU UE, connect with each other based on the same VNI number.

Steps for the creation of Segmentation:

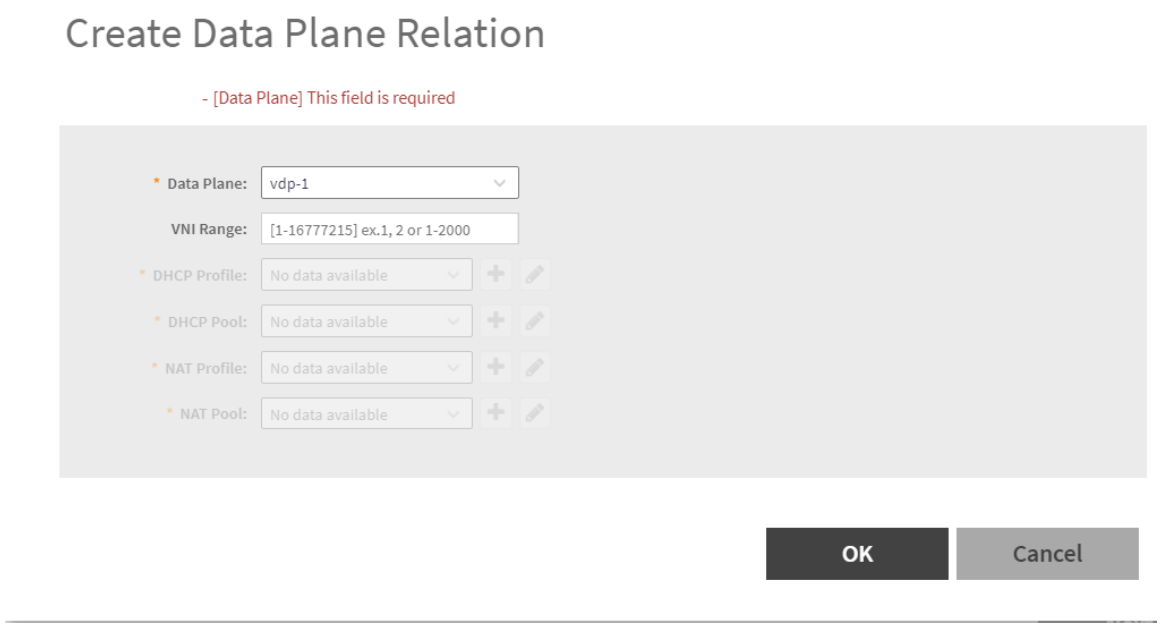
- Go to **Services> Hotspots & Portals > Network Segmentation> Network Segmentation Profiles**
- Click **Create**.

FIGURE 265 Edit Network Segmentation Groups in SmartZone User Interface



- Enter a Network Segmentation Profile name in the Name field.
- Click "Add".

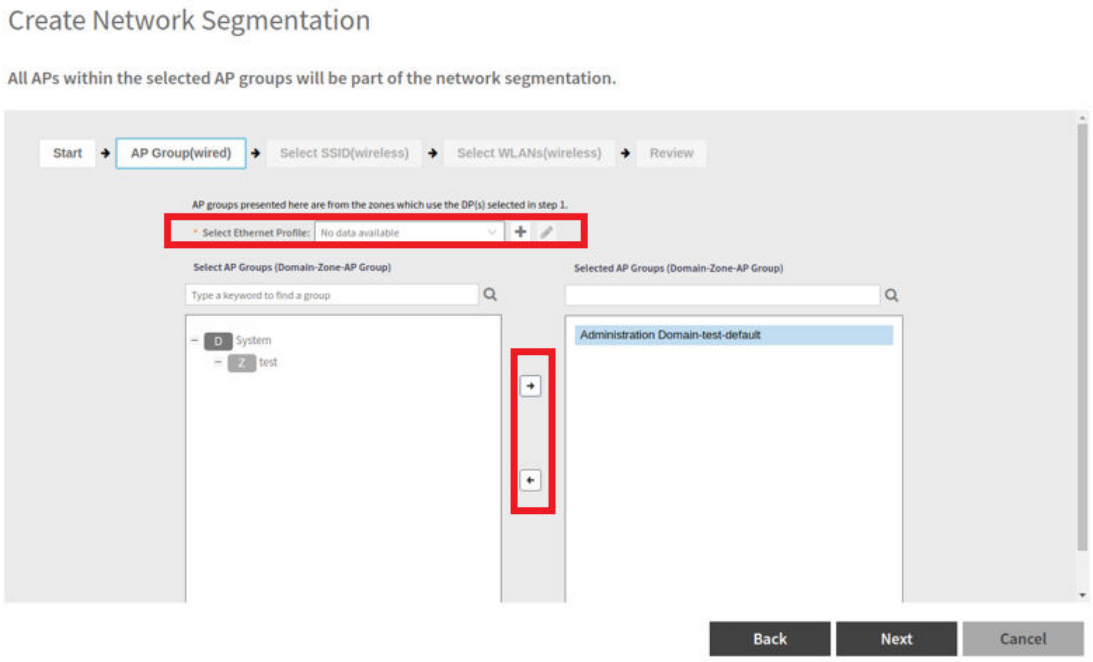
FIGURE 266 Create Data plane Relation



- Select the Data Plane details
- Enter the VNI range; ensure your VNI range is large enough to accommodate all units in the property. Each unit gets its own unique VNI.
- Select/Create DHCP Profile and Pool.
- Select/Create NAT Profile and Pool.
- Click "OK".
- "Select AP Group(s) that will be used for Network Segmentation , refer to the figure below.

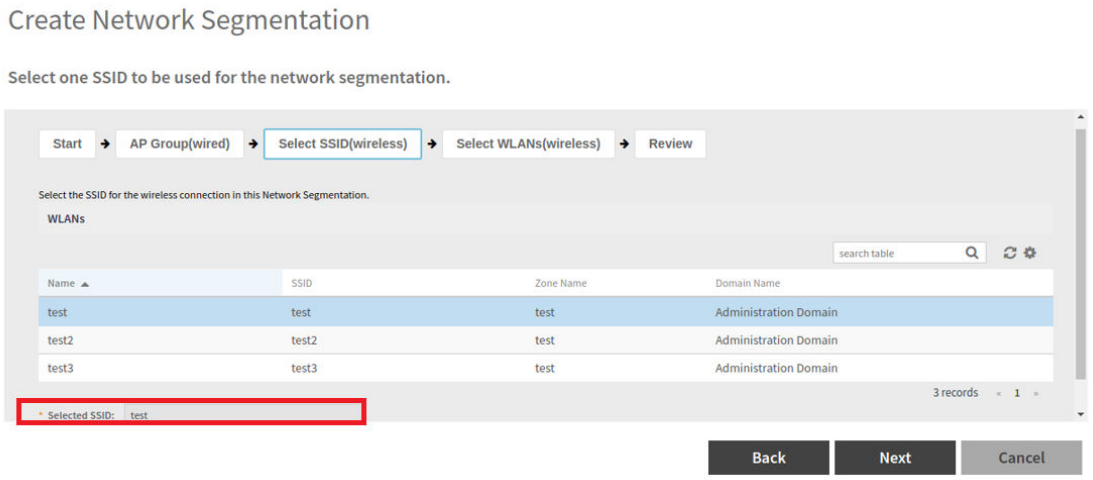
NOTE
This step is not applicable for Wireless group.

FIGURE 267 Add AP Group



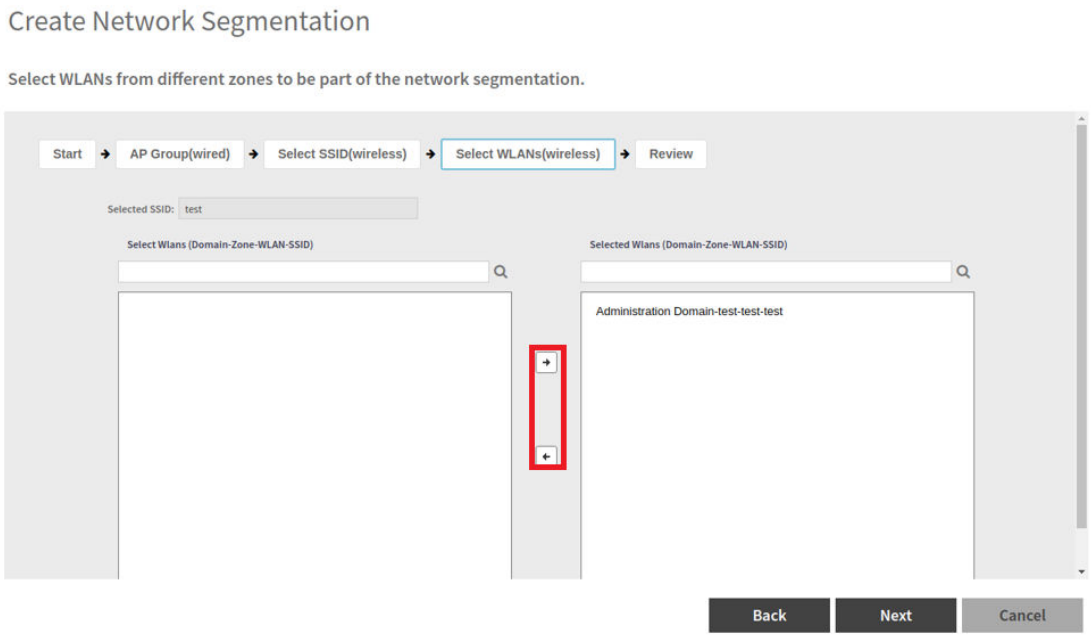
- Create/Select an ethernet profile with enabled Network Segmentation and select AP Model's port to apply.
- Click "Next".
- Select the SSID (wireless) for Network Segmentation.

FIGURE 268 Select SSID(wireless) for Network Segmentation

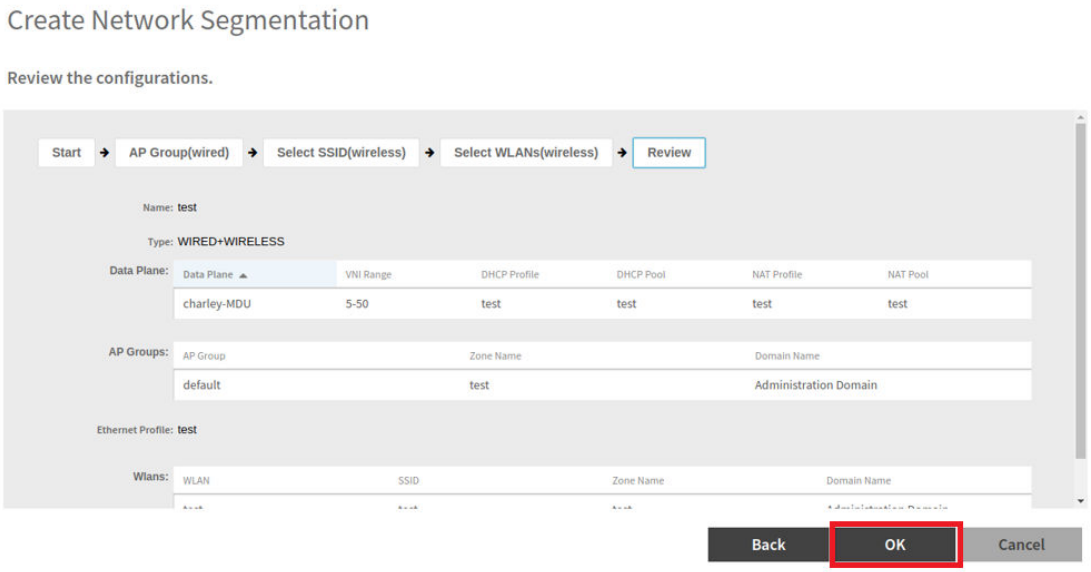


- Click "Next".
- Select WLANs (wireless) for Network Segmentation.

FIGURE 269 Select WLANs (wireless) for Network Segmentation



- Select "Next".
- Review the details entered.



- Click "OK".
- The Network Segmentation Profile is created.

Working with Tunnels and Ports

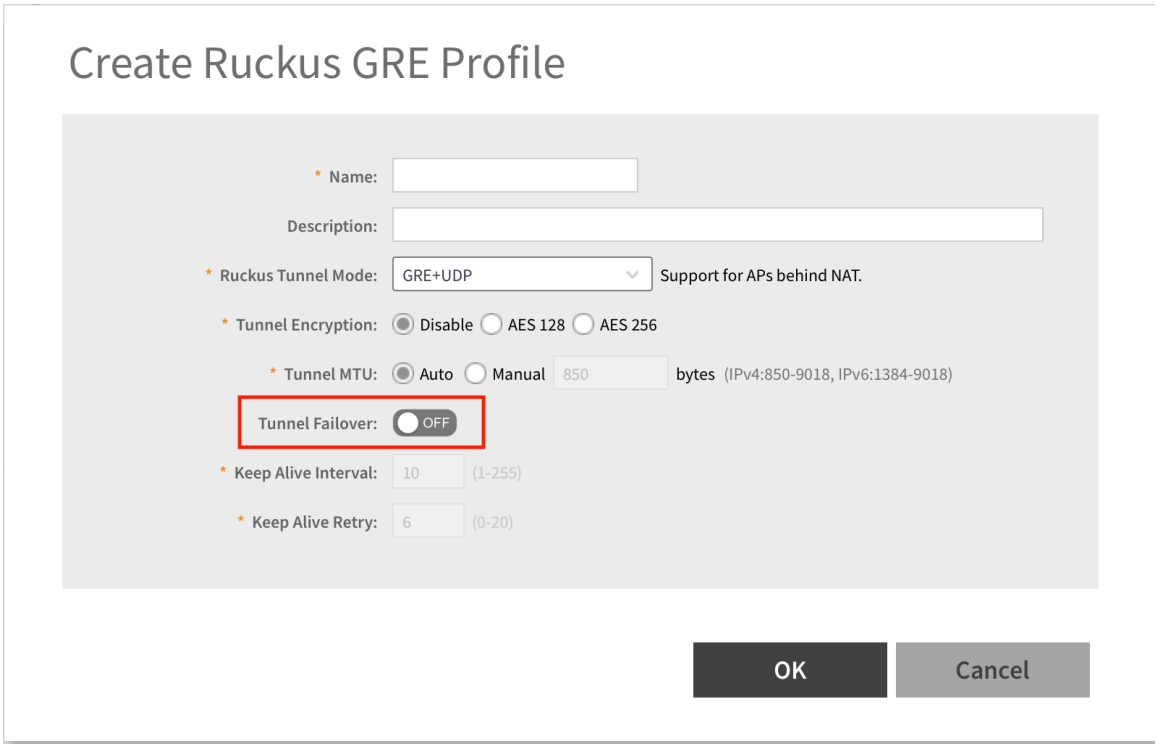
Creating a Ruckus GRE Profile

You can configure the RUCKUS GRE tunnel profile of the controller to manage AP traffic.

NOTE
You can also edit, clone and delete the profile by selecting the options **Configure**, **Clone** and **Delete** respectively, from the **Ruckus GRE** tab.

1. Go to **Services** > **Tunnels & Ports**.
2. Select the **Ruckus GRE** tab, and then select the system for which you want to create the profile.
3. Click **Create**.
   The **Create Ruckus GRE Profile** page appears.

FIGURE 270 Creating a Ruckus GRE Profile



4. Type a name for the profile in the **Name** box.
5. Type a description for the profile in the **Description** box.

6. Select a protocol to use for tunneling WLAN traffic back to the controller by choosing one of the following after clicking the drop-down arrow in the **Ruckus Tunnel Mode** box:
   - **GRE + UDP**—Select this option to allow APs behind a NAT server to tunnel WLAN traffic back to the controller.
   - **GRE**—Select this option to tunnel regular WLAN traffic only.
7. To allow managed APs to decrypt 802.11 packets, and then use an AES encrypted tunnel to send them to the controller. select one of the **Tunnel Encryption** options:
   - Click the **Disable** radio button to allow only the management traffic to be encrypted; data traffic is unencrypted. This is the default option.
   - Click the **AES 128** radio button to use an AES 128-byte encryption tunnel.
   - Click the **AES 256** radio button to use an AES 256-byte encryption tunnel.

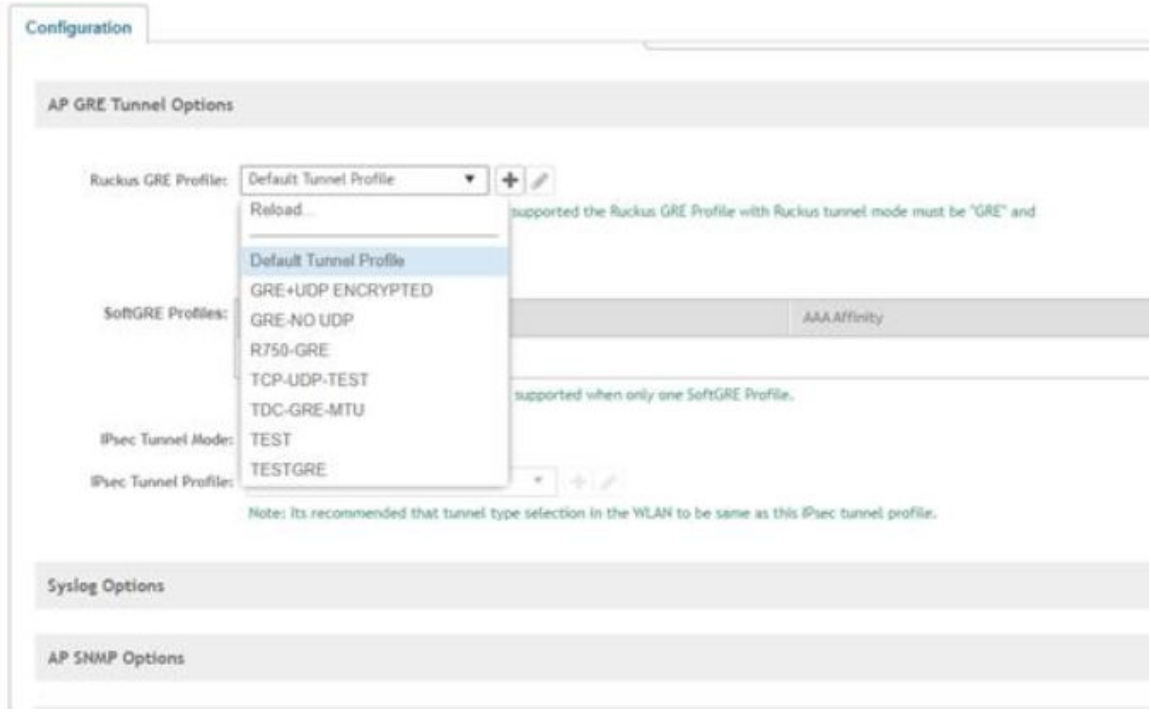
   MTU is the size of the largest protocol data unit that can be passed on the controller network.
8. Set the maximum transmission unit (MTU) for the tunnel using one of the **Tunnel MTU** options:
   - Click the **Auto** radio button. This is the default option.
   - Click the **Manual** radio button and enter the maximum number of bytes. For IPv4 traffic the range is from 850-1500 bytes, for IPv6 traffic the range is from 1384 to 1500 bytes.

   MTU is the size of the largest protocol data unit that can be passed on the controller network.
9. Set the Tunnel failover option with Off/On.
10. Enter the "Keep Alive Interval" value.
11. Enter the "Keep Alive Retry" value.
12. Click **OK**.

13. Go to the zone profile and use the created GRE profile.

    Enter the required information.

    FIGURE 271 How to apply Ruckus GRE Profile



14. Go to the required WLAN to use the GRE profile.
15. Another option is , go to zone level configuration and find "AP GRE Tunnel".
16. Click "+".
17. Create new profile.
18. Go to the required WLAN to use the GRE profile.

Creating a Soft GRE Profile

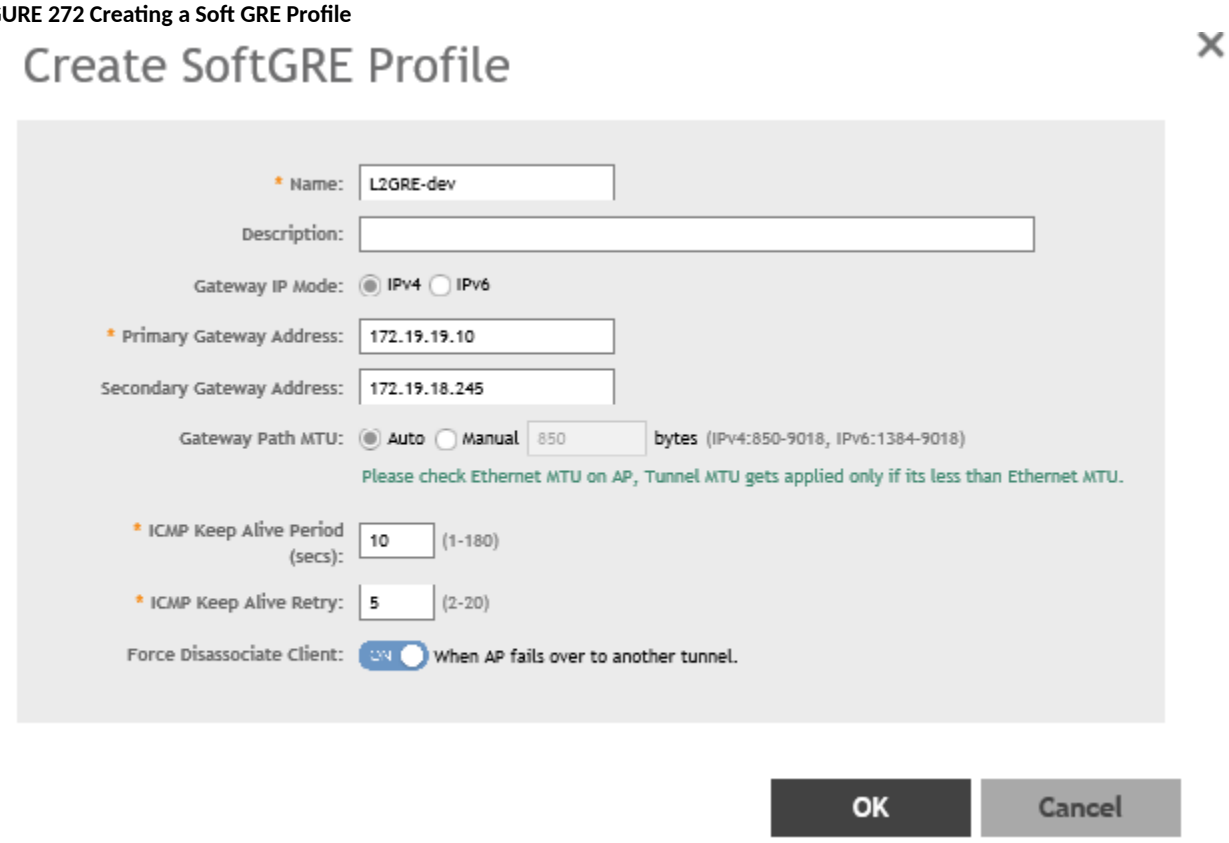
You can configure the Soft GRE tunnel profile of the controller to manage AP traffic.

1. Select **Services** > **Tunnels and Ports**.

2. Select **Soft GRE** and click **Create**.

   The **Create Soft GRE Profile** page is displayed.

FIGURE 272 Creating a Soft GRE Profile



3. Enter profile name and description.
4. Under **Gateway IP Mode**, select **IPv4** or **IPv6** addressing.
5. In the **Primary Gateway Address** field, enter the IP address or fully-qualified domain name (FQDN) of the primary gateway server.
6. In the **Secondary Gateway Address** field, enter the IP address or fully-qualified domain name (FQDN) of the secondary gateway server.

   NOTE
   If the controller is unable to reach the primary gateway server, the controller automatically attempts to reach the secondary gateway address at the IP address specified by you.

7. For **Gateway Path MTU**, set the maximum transmission unit (MTU) for the gateway path.

   Select one of the following options:

   - **Auto**: This is the default option.
   - **Manual**: The transmission range is from 850 through 1500 bytes.

8. In the **ICMP Keep Alive Period** field, enter the time interval in seconds.

   NOTE
   Time interval is the time taken by the APs to send a keepalive message to an active third party WLAN gateway. The range is from 1 through 180 seconds. The default value is 10 seconds.

9. In the **ICMP Keep Alive Retry** field, enter the number of keepalive attempts.

   NOTE
   Keepalive attempts are the number of attempts that the APs wait for a response from the active third party WLAN gateway before failing over to the standby WLAN gateway. The range is from 2 through 10 attempts. The default value is 5 attempts.

10. Under **Force Disassociate Client**, enable **Disassociate client when AP fails over to another tunnel** if you want to disassociate the client when AP fails over to another tunnel.

    NOTE
    You must select this option if you have enabled **AAA Affinity** while configuring the zone.

11. Click **OK**.

You have created the Soft GRE profile.

NOTE
You can also edit, clone, and delete the profile by selecting the options **Configure**, **Clone**, and **Delete** respectively from the **Soft GRE** tab.

Creating an IPsec Profile

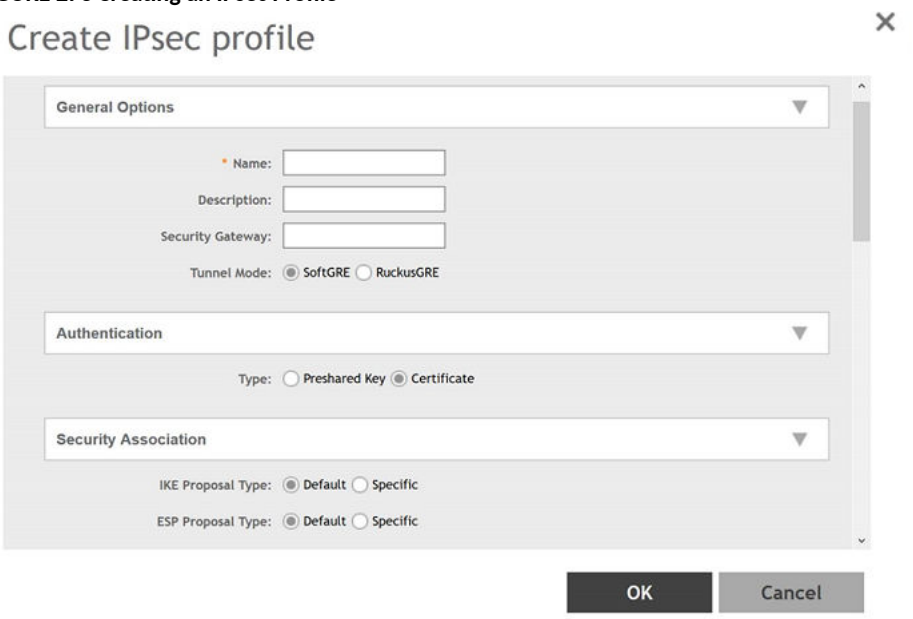
This feature is supported on both 11ac and 11ax APs.

1. Go to **Services** > **Tunnels & Ports**.
2. Select the **IPsec** tab, and then select the zone for which you want to create the profile.

3. Click **Create**.

   The **Create IPsec Profile** page appears.

FIGURE 273 Creating an IPsec Profile



4. Configure the following:
   a. Name: Type a name for the profile.
   b. Description: Type a description for the profile.
   c. Security Gateway: Type the IP address or FQDN of the IPSec server. If you use the IP address, the IP address format that you must enter will depend on the IP mode that is configured on the controller.

      NOTE
      This option appears only when SoftGRE Tunnel Mode option is selected.

   d. Tunnel Mode: Select SoftGRE or RuckusGRE.
   e. IP Mode: Select IPv4 or IPv6 addressing modes
   f. Authentication: Select Preshared Key to use PSK for authentication or Certificate to use an X.509 certificate on the certificate authority (CA) or registration authority (RA) server. The controller uses the CMPv2 protocol to obtain the signed certificate from the CA/RA server.

      If you selected Preshared Key, type the PSK in this box. The PSK must be eight to 128 ASCII characters in length.
   g. Security Association
      1. IKE Proposal Type: Select Default to use the default Internet Key Exchange (IKE) security association (SA) proposal type or select Specific to manually configure the IKE SA proposal. If you clicked Specific, you will need to configure the following settings:
         - Encryption Algorithm: Options include 3DES, AES128, AES192, and AES256.
         - Integrity Algorithm: Options include MD5, SHA1, AES-XCBC, SHA256, SHA384, and SHA512.
         - Pseudo-Random Function: Options include Use integrity ALG, PRF-MD5, PRF-SHA1, PRF-AES-XCBC, PRF-AES-CMAC, PRF-SHA256, and PRF-SHA384.
         - DH Group: Options for Diffie-Hellman groups for IKE include modp768, modp1024, modp1536, modp2048, modp3072, modp4096, modp6144, and modp8192.
      2. ESP Proposal Type: Click Default to use the default Encapsulating Security Payload (ESP) SA proposal type or click Specific to manually configure the ESP proposal. If you clicked Specific, you will need to configure the following settings:
         - Encryption Algorithm: Options include 3DES, AES128, AES192, AES256, and NONE.
         - Integrity Algorithm: Options include MD5, SHA1, AES-XCBC, SHA256, SHA384, and SHA512.
         - DH Group: Options for Diffie-Hellman groups for ESP include None, modp768, modp1024, modp1536, modp2048, modp3072, modp4096, modp6144, and modp8192.

           NOTE
           For the RuckusGRE Tunnel mode option the following IKE and ESP proposals are supported:
           - AES128-SHA1-MODP2048
           - AES256-SHA384-ECP384

           IKE encryption proposals should be greater than or equal to ESP encryption proposal. RuckusGRE over IPsec supports IKEv2 authentication by X.509 certificate only.

   h. Rekey Options
      1. Internet Key Exchange: To set time interval at which the IKE key renews, select a time unit (day, hour, or minute) from the drop-down list, and then type a number in the box. To disable IKE rekey, select the Disable check box. SmartZone 100/Virtual SmartZone Essentials for Release 3.4 Administrator Guide 82 Configuring the Wireless Network Configuring Access Points.
      2. Encapsulating Security Payload: To set time interval at which the ESP key renews, select a time unit (day, hour, or minute) from the drop-down list, and then type a number in the box. To disable ESP rekey, select the Disable check box.

i. Certificate Management Protocol
   1. DHCP Option 43 Sub Code for CA/RA Address: Set the DHCP Option 43 subcode that will be used to discover the address of the CA/RA server on the network. The default subcode is 8.
   2. CA/RA Address: Type the IP address or FQDN of the CA/RA server. If you use the IP address, the IP address format that you must enter will depend on the IP mode that is configured on the controller.
   3. Server Path: Type the path to the X.509 certificate on the CA/RA server.
   4. DHCP Option 43 Sub Code for Subject Name of CA/RA: Set the DHCP Option 43 subcode that will be used to discover the subject name of the CA/RA server on the network. The default subcode is 5.
   5. Subject Name of CA/RA: Type an ASCII string that represents the subject name of the CA/RA server.

j. Advanced Options
   1. DHCP Option 43 Sub Code for Security Gateway: Set the DHCP Option 43 subcode that will be used to discover the address of the security gateway on the network. The default subcode is 7.
   2. Retry Limit: Set the number of times that the controller will attempt to discover the address of the security gateway. The default retry count is 5. Accepted values are 0 (disable) to 16.
   3. Replay Window: Set the ESP replay window (in packets). The default size is 32 packets. Accepted values are 0 (disable) to 32 packets.
   4. IP Compression: To enable IP Payload Compression Protocol (IPComp) compression before encryption, click Enable. The default value is Disable.
   5. Force NAT-T: To enforce UDP encapsulation of ESP packets, click Enable. The default value is Disable.
   6. Dead Peer Detection: By default, the IKE protocol runs a health check with remote peer to ensure that it is alive. To disable this health check, click Disable.
   7. NAT-T Keep Alive Interval: To set the keep alive interval (in seconds) for NAT traversal, type a value in the box. The default keep alive interval is 20 seconds. Accepted values are 1 to 65536. To disable the keep alive interval, click Disable.
   8. FailOver Options: To configure the failover settings when APs are unable to connect, configure the following:
   9. Retry Period: Set the number of days (minimum 3 days) during which APs will keep attempting to connect. To keep try indefinitely, select the **Forever** check box.
   10. Retry Interval: Set the interval (in minutes) between each retry attempt. The default retry interval is 1 minute. Accepted values are from 1 to 30 minutes.
   11. Retry Mode: If you want APs to fall back to the specified primary security gateway, click Revertive. If you want APs to maintain connectivity with the security gateway to which they are currently connected, click **Non-revertive**.

k. Click **OK**.

You have created the IPsec GRE profile.

NOTE
You can also edit, clone and delete the profile by selecting the options **Configure**, **Clone** and **Delete** respectively, from the **IPsec GRE** tab.

Creating an Ethernet Port Profile

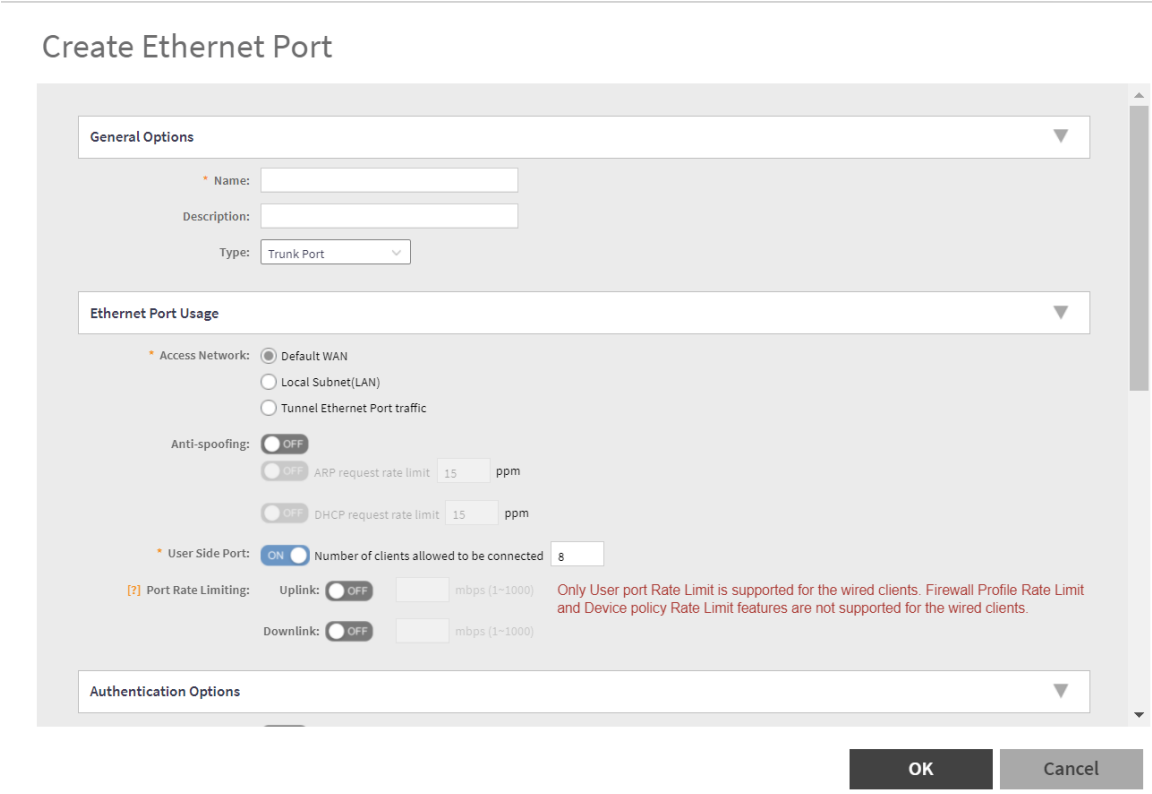
An Ethernet port profile contains settings that define how an AP will handle VLAN packets when its port is designated as a trunk, access, or general port. By default, three Ethernet port profiles exist: General Port, Access Port, and Trunk Port.

1. Select **Services** > **Tunnels and Ports**.
2. Select the **Ethernet Port** tab, and then select the zone for which you want to create the profile.

3. Click **Create**.

   The **Create Ethernet Port** page is displayed.

FIGURE 274 Creating an Ethernet Port Profile



4. Configure the following options:
   - General Options
     - Name: Enter a name for the Ethernet port profile that you are creating.
     - Description: Enter a short description about the profile.
     - Type: The Ethernet port type defines how the AP will manage VLAN frames. You can set Ethernet ports on an AP to one of the following types: Trunk Port, Access Port, or General Port. By selecting the appropriate port type, authentication method, and 802.1X role, you can configure the Ethernet ports to be used for the wired client. If you select a non-user port, there is no restriction on the number of clients supported. If the User Side Port is selected, the maximum number of supported clients is 32 and this number is configurable.
   - Ethernet Port Usage
     - Access Network: Select the required option:
       - Default WAN: Enables default WAN configuration
       - Local Subnet(LAN): Enables DHCP service on ethernet ports. In the **VLAN Options**, ensure to select the **VLAN Untag ID** in ethernet profile same as the DHCP NAT VLAN ID.
       - Tunnel Ethernet Port Profile: Enables tunneling on the ethernet port
     - Anti-spoofing: Prevents attacks on genuine clients from rogue clients that could lead to service disruption, data loss, and so on. This is achieved by matching the MAC address or IP address (IPv4) of the client with the address in the RUCKUS database. If the addresses do not match, the packet is dropped. These checks are also performed on ingress data packets to catch spoofed data packets early.
       - ARP request rate limit: The ARP request rate limits the number of ARP requests from the connected clients to prevent ARP flooding. Enter the number of packets to be reviewed for Address Resolution Protocol (ARP) attacks per minute. In ARP attacks, a rogue client sends messages to a genuine client to establish connection over the network.
       - DHCP request rate limit: The DHCP request rate limits the number of DHCP requests from the connected clients to prevent DHCP flooding. Enter the number of packets to be reviewed for DHCP pool exhaustion, per minute. When rogue clients send a DHCP request with a spoofed address, an IP address from the DHCP pool is assigned to it. If this happens repeatedly, the IP addresses in the DHCP pool are exhausted, and genuine clients may miss out on obtaining the IP addresses.

         NOTE
         When you enable anti-spoofing, an ARP request rate limiter and a DHCP request rate limiter are automatically enabled with default values (in packets per minute) which are applied per client; implying that each client connected to an interface enabled with anti-spoofing is allowed to send a maximum of "X" ARP and DHCP request packets per minute (ppm). The "X" value is configured on the interface to which the client is connected.

         NOTE
         Force-DHCP will be enabled by default when anti-spoofing is enabled, and it cannot be changed after anti-spoofing is enabled.

     - User Side Port: The Ethernet port must be configured as a User Side Port for QinQ to work.
       - Number of clients allowed to be connected: Enter the number of clients that can be connected to the User Side Port. The maximum number of clients that can be connected is 32.
   - Authentication Options
     - 802.1X: Select this check box to enable 802.1X authentication.
     - 802.1X Role: Select the authenticator role from the menu. Options include Supplicant, MAC-based Authenticator, and Port-based Authenticator. When you select Supplicant, you can customize the user name and password to authenticate as a supplicant role or use the credentials of the AP MAC address. When you select Port-based Authenticator, only a single MAC address host must be authenticated for all hosts to be granted access to the network. If you select MAC-based Authenticator, each MAC address host is individually authenticated. Each newly learned MAC address triggers an EAPOL request-identify frame.

  - Enable client visibility regardless of 802.1X authentication: If client visibility is enabled, you can view connected wired client information. Client visibility is enabled by default if the 802.1x authentication method is selected. For the open authentication method, you must enable client visibility based on your requirements.

    NOTE
    You can view statistical information about wired clients without enabling 802.1X authentication.

- Supplicant: Select the authentication type
  - MAC Address: Select this option to use the AP MAC address as the username and password.
  - Custom: Enter customized Username and Password to authenticate.
- VLAN Options
  - VLAN Untag ID: Enter the ID of the native VLAN (typically 1), which is the VLAN into which untagged ingress packets are placed upon arrival. If your network uses a different VLAN as the native VLAN, configure the VLAN Untag ID of the AP Trunk port with the native VLAN used throughout your network. If **Local Subnet** option is selected in **Ethernet Port Usage**, then VLAN ID configured should be the same as one of DHCP NAT VLANs.
  - VLAN Members: Enter the VLAN IDs that you want to use to tag WLAN traffic that will use this profile. You can enter a single VLAN ID or a VLAN ID range (or a combination of both). The valid VLAN ID range is from 1 through 4094. If **Local Subnet** option is selected in **Ethernet Port Usage**, then only DHCP NAT VLANs are allowed on trunk port.
  - Enable Dynamic VLAN: Select this check box if you want the controller to assign VLAN IDs on a per-user basis. Before enabling dynamic VLAN, you must define on the RADIUS server the VLAN IDs that you want to assign to users.

    NOTE
    The Enable Dynamic VLAN option is only available when the Type is set to Access Port and 802.1X authentication is set to MAC-based Authenticator.

    NOTE
    If you enable client visibility, a maximum of 16 clients can be connected to a port regardless of the 802.1X authentication. The same limitation applies when 802.1X authentication is enabled and client visibility is not enabled.

  - Guest VLAN: If you want to assign a device that fails authentication to remain able to access the Internet but to internal network resources only, select this check box.
  - QinQ VLAN: Select the check box and update the ranges:
    - QinQ SVLAN Range: Enter a SVLAN range. The range is 2 through 4095.
    - QinQ CVLAN Range: Enter a CVLAN range. The range is 2 through 4095.

      NOTE
      For QinQ VLAN to work, the User Side Port and Enable Dynamic VLAN must be enabled.

- Authentication and Accounting Services
  - Authentication Server: Select the check box and a controller from the menu to use the controller as a proxy authentication server.
  - Accounting Server: Select the check box and a controller from the menu to use the controller as a proxy accounting server.
  - Enable MAC authentication bypass: Select this check box if you want to use the device MAC address as access credentials (user name and password).
- RADIUS Options
  - NAS ID: Set the NAS ID for the AP to communicate with the RADIUS server. Options include using the AP MAC address or any user-defined address.
  - Delimiter: If the AP MAC address is selected to configure the NAS ID, then you can choose between Dash or Colon as delimiters to separate.

- Firewall Options

  NOTE
  The User Side Port must be enabled to configure the Firewall Profile, Application Recognition and Control, and URL Filtering Policy.

  NOTE
  While mapping group attribute values to the user role, avoid special characters or duplicate entries regardless of the order.

  - Firewall Profile: Select the firewall profile for wired ports.
  - Application Recognition and Control: Enable the option for the wired clients.
  - URL Filtering Policy: Enable the option for the wired clients.
  - L2 Access Control Policy: Select the Layer 2 policy for wired ports. When User Side Port is not enabled, the Layer 2 Access Control wired support policy can be mapped directly to the wired port. When the User Side Port is not enabled, an a Layer 2 Access Control wired support policy can be mapped directly to the wired port. If the User Side Port is enabled, the Layer 2

    Access Control wired support policy can be mapped to the wired port by way of the firewall profile. Click  to create a new policy. Refer to Creating an L2 Access Control Service on page 382.

- Click **OK**.

NOTE
You can edit, copy, or delete the profile by selecting the options **Configure**, **Clone**, or **Delete**, respectively, from the **Ethernet Port** tab.



VIDEO
Creating Ethernet Port Profiles. Creating an Ethernet port profile (securing secondary wired port), port types explained
Click to play video in full screen mode.

Creating a Tunnel DiffServ Profile

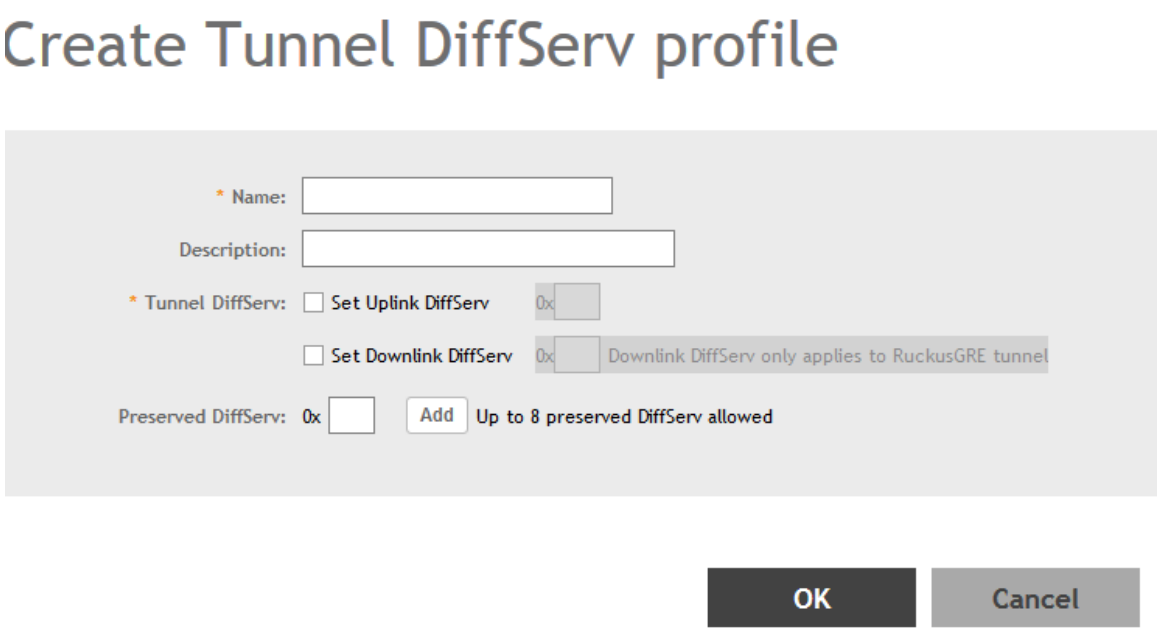
If you need to configure the type of traffic (ToS) bit settings for the access side traffic from RUCKUS APs, follow these steps to create a Differentiated Services (DiffServ) profile. This profile can only be applied to Ruckus GRE and SoftGRE traffic.

1. Go to **Services** > **Tunnels and Ports**.
2. Select the **DiffServ** tab, and then select the zone for which you want to create the profile.

3. Click **Create**.

   The **Create Tunnel DiffServ Profile** page appears.

FIGURE 275 Creating a Tunnel DiffServ Profile



4. Configure the following:
   a. Name: Type a name for the DiffServ profile that you are creating.
   b. Description: Type a brief description for the DiffServ profile.
   c. Tunnel DiffServ: configure the following options.
      1. Set Uplink DiffServ: Select the check box if you want to set the Differentiated Services field for uplink user traffic from RUCKUS APs towards either the controller or a third SmartCell Gateway 200/Virtual SmartZone High-Scale for Release 3.4.1 Administrator Guide 92 Managing RUCKUS AP Zones Creating a DiffServ Profile party gateway via SoftGRE. Configure the desired value to be set by the RUCKUS AP.
      2. Set Downlink DiffServ: Select the check box if you want to set the Differentiated Services field for downlink user traffic from the controller towards the AP, and then configure the desired value to be set by the RUCKUS AP.
   d. Preserved DiffServ: Configure up to eight (8) entries in the preserved DiffServ list. The Preserved DiffServ list allows the preservation of values that have been already marked in incoming packets either in uplink or downlink traffic.
   e. Click **OK**.

You have created the DiffServ profile.

NOTE
You can also edit, clone and delete the profile by selecting the options **Configure**, **Clone** and **Delete** respectively, from the **DiffServ** tab.

Communications Assistance for Law Enforcement Act (CALEA)

The Communications Assistance for Law Enforcement Act is a law passed by the United States to enhance the ability of law enforcement agencies to conduct electronic surveillance by requiring that telecommunications carriers and manufacturers of telecommunications equipment to modify and design their equipment, facilities, and services to ensure that they have built-in surveillance capabilities.

NOTE
This feature only applies to virtual SmartZone platform (vSZ-H).

1. Go to **Services** > **Tunnels and Ports**.
2. Select the **CALEA** tab.
3. Server IP: Type the CALEA server IP address. and click **OK**.
4. Click **Create**.

   The **Create UE MAC** page appears.

   NOTE
   The list of client health will only list top 100 clients.

5. MAC Address: Type the MAC address of the client/user equipment for which CALEA mirroring is required. The MAC address is sent by the SZ controller to the vSZ-D.
6. Click **OK**.

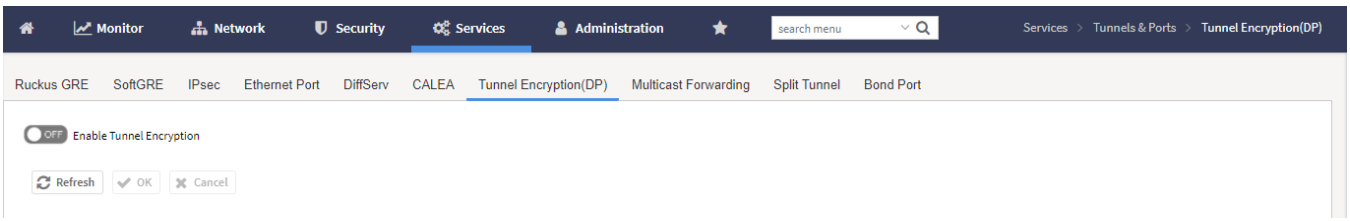
Enabling Tunnel Encryption

You can use the tunnel encryption feature to encrypt data for a private network, through a public network. This feature is available in vSZ-H and vSZ-E.

1. Go to **Services** > **Tunnels and Ports**.
2. Select the **Tunnel Encryption(DP)** tab.

   The **Tunnel Encryption (DP)** page appears.

   FIGURE 276 Tunnel Encryption (DP)



3. Select the **Enable Tunnel Encryption** check-box.
4. Click **OK**.

You have successfully enabled tunnel encryption.

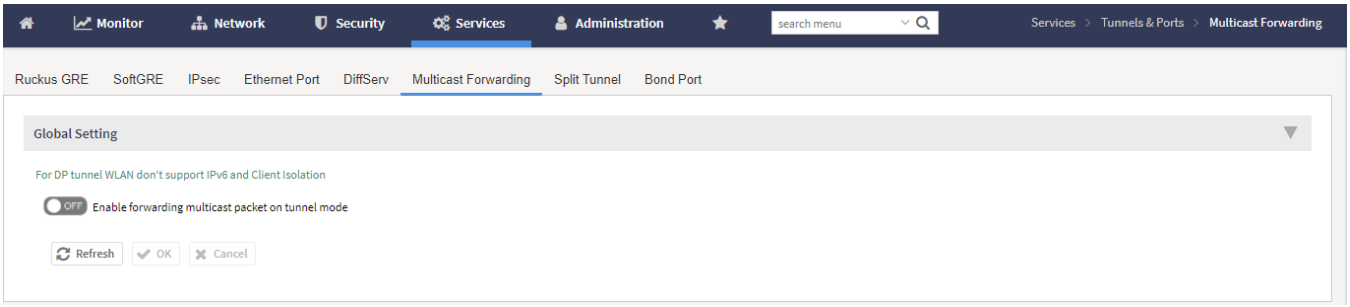
Forwarding Multicast Packets

In multicast forwarding, a group of hosts are typically grouped under a multicast IP address. Data can then be transmitted from the source to the IP address which in turn transmits data to the various hosts assigned to the multicast IP. This is a point-to-multipoint data transmission. This feature is only available in SZ100.

1. Go to **Services** > **Tunnels and Ports**.
2. Select the **Multicast Forwarding** tab.

   The **Multicast Forwarding** page appears.

   FIGURE 277 Forwarding Multicast Packets



3. In **Global Setting**, select the **Enable forwarding multicast packet on tunnel mode** check-box.
4. Click **OK**. The form is submitted and multicast packet forwarding is enabled.

You have successfully enabled multicast forwarding for data packets in the tunnel mode.

Split Tunnel Profile

A Split Tunnel Profile can be created to manage corporate and local traffic by sending only corporate traffic to the controller. A split tunnel ensures that local traffic does not incur the overhead of the round trip to the controller, which decreases traffic on the WAN link and minimizes latency for local application traffic. Using a split tunnel, a remote user is associated with a single SSID (rather than multiple SSIDs) to access corporate resources, such as a mail server and local resources (for example, a local printer).

Split Tunnel Profile Limitations

Before enabling the Split Tunnel Profile, consider the following limitations:

- Split Tunnel Profile does not support a zone where mesh-enabled APs are present.
- Split Tunnel Profile and Express Wi-Fi are not supported together on the same WLAN.
- For both features to work properly, the configured IP rules for a split tunnel and a walled garden must be different.
- Split Tunnel Profile does not support DHCP/NAT.
- Split Tunnel Profile does not support wired clients.
- The limitations applicable to DHCP/NAT also apply to Split Tunnel Profile.
- Wispr-related (web-auth) WLANs are not supported on Split tunnel WLAN.
- ICMP is not supported towards LBO split-path where SNAT happens.
- IPv6 addresses are not supported in split-tunnel.
- Multicast discovery of bonjour devices will not happen over LBO.

- As the data traffic is established from server side, TFTP protocol is not supported.
- As the server rejects the data connection which does not have the NAT IP sent by the client, the FTP active mode is not supported with split-tunnel .

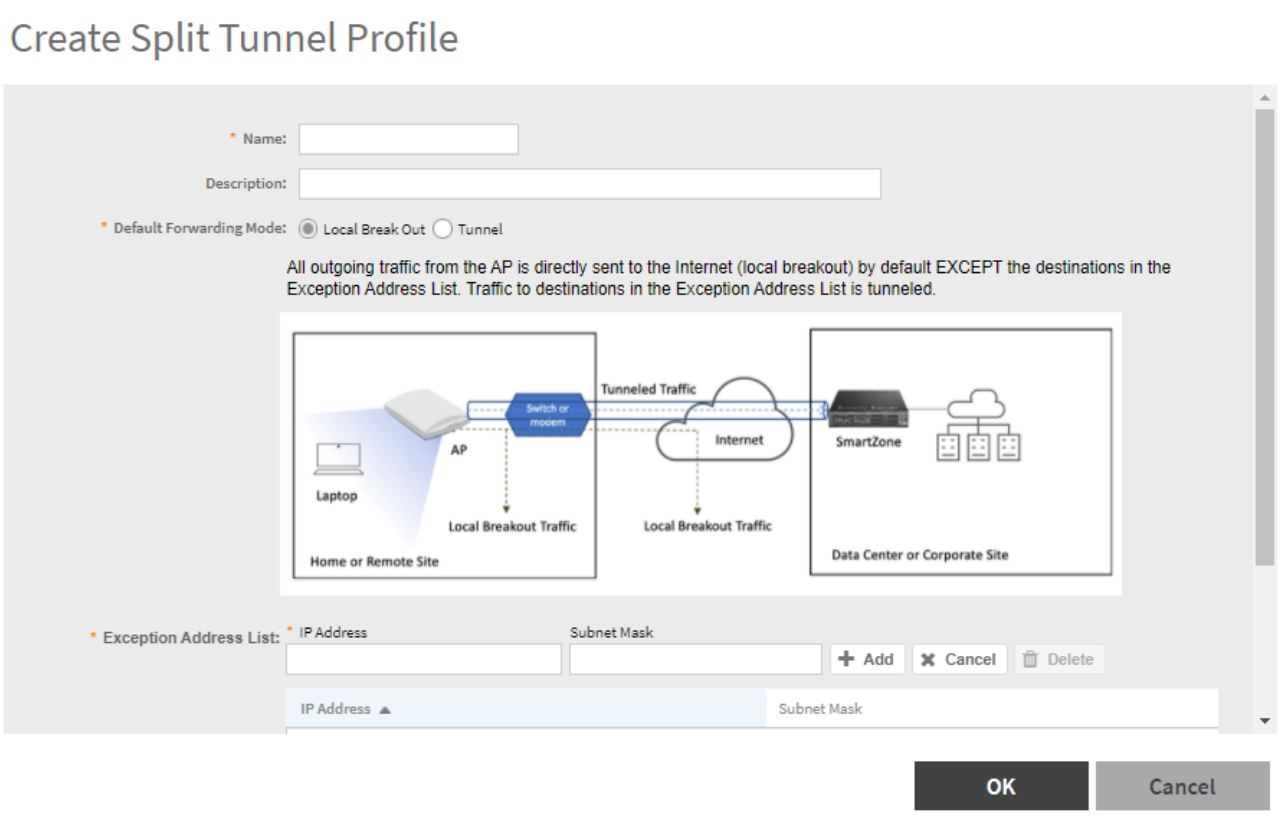
Creating a Split Tunnel Profile

Complete the following steps to configure a split tunnel profile:

1. Select **Services** > **Tunnels and Ports** > **Split Tunnel**.
2. Select the zone for which you want to create the profile and click **Create**.

   The **Create Split Tunnel Profile** window is displayed.

   FIGURE 278 Creating a Split Tunnel Profile



3. Enter the split tunnel profile information:

   NOTE
   RuckusGRE or SoftGRE must be enabled on the WLAN before mapping it to a Split Tunnel Profile.

   a. In the **Name** field, type a name for the split tunnel profile.
   b. In the **Description** field, type a short description for the split tunnel profile.
   c. In **Default Forwarding Mode** field, select one of the following option:
      - **Local Break Out**: All outgoing traffic from the AP is by default sent to the Internet (local breakout) except for the destinations in the Exception Address List. Traffic to destinations in the Exception Address List is tunneled.
      - **Tunnel**: All outgoing traffic from the AP is by tunneled except for the destinations in the Exception Address List. Traffic to destinations in the Exception Address List is directly sent to the Internet (local breakout).
   d. In the **IP Address** field, enter the destination IP address.
   e. In the **Subnet Mask** field, enter the destination IP subnet mask.
   f. Click **Add** to add the destination IP details.
   g. Click **OK**.

   NOTE
   You can also edit, clone or delete the profile by selecting the options **Configure**, **Clone**, and **Delete** respectively from the **Split Tunnel** tab.

Creating a Bond Port Profile

A Bond port profile aggregates multiple network interfaces into a single logical interface. Existing ethernet configurations must be removed before forming a bonding interface. As both ethernet links should operate at the same speed, link speed must be downgraded and should set to 1 Gbps.

Following default configurations are chosen when the bond is formed on the AP:

```
Mode: 8023AD
LACP-rate: slow
MII-Mon: 100 (ms)
Xmit-Hash: layer2+3
```

To create a bond-port profile:

1. Go to **Services** > **Tunnels & Ports** > **Bond Port**.
2. Select the zone or AP group and click **Create**.

   The **Create Bond Profile** page is displayed.
3. Configure the following options:
   a. **General Options**
      1. **Name**: Enter a name for the Bond port profile that you are creating.
      2. **Description**: Enter a short description about the profile.
      3. **Type**: The ethernet port type configuration. You can set the ethernet ports on an AP to one of the following types: **Trunk Port**, **Access Port**, or **General Port**.
   b. **VLAN Options**
      1. **VLAN Untag ID**:
      2. **VLAN Members**:
4. Click **OK**.

Managing Core Network Tunnels

Tunneling protocols allows a user to access or provide a network service that the network does not support or provide directly.

Creating Bridge Forwarding Profiles

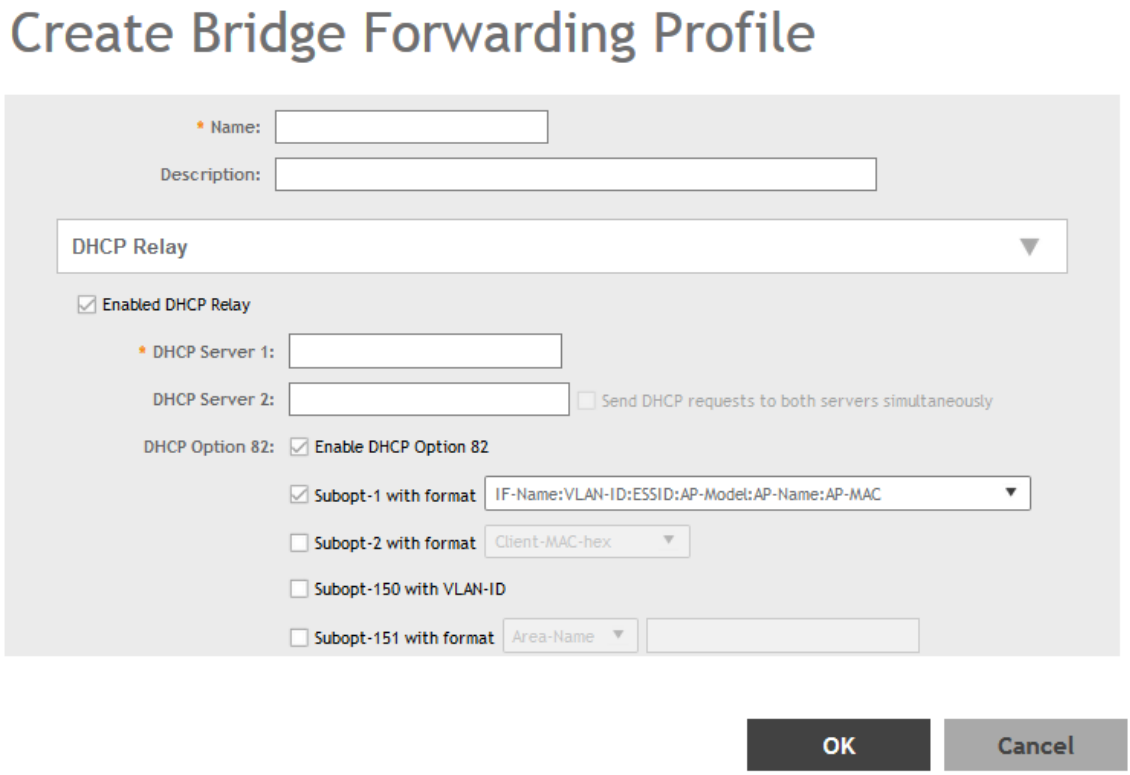
An Bridge forwarding profile defines the DHCP configuration for the core network.

NOTE
This feature is available only on vSZ-H platform.

1. Go to **Services** > **Tunnels and Ports** > **Core Network Tunnel** > **Bridge**.
2. Select the zone for which you want to create the profile.
3. Click **Create**.

   The **Create Bridge Forwarding Profile** page appears.

FIGURE 279 Creating a Bridge Forwarding Profile



4. Configure the following:
    a. Name: Type a name for the profile that you are creating.
    b. Description: Type a brief description for the profile.
    c. DHCP Relay: Select the **Enable DHCP Relay**check-box and configure the DHCP server IP address and DHCP option 82 settings.
        1. DHCP Server 1: Type the IPv4 address of the DHCP server that will allocate IP addresses to DHCP clients.
        2. DHCP Server 2: If a secondary DHCP server exists on the network, type the IPv4 address of the secondary server.
        3. DHCP Option 82: Select this check box if you want the DHCP relay agent (in this case, the controller) to insert specific identification information into requests that are forwarded to the DHCP server. If you enabled DHCP Option 82, you can configure the following Option 82 sub-options by selecting the corresponding check boxes:
            - Subopt-1 with format: You can customize sub-option 1 (Circuit ID) to send only the AP's MAC address in hexadecimal format or the MAC address and ESSID. The default format is: IFName:VLAN-ID:ESSID:AP-Model:AP-Name:AP-MAC.
            - Subopt 2 with format: You can customize sub-option 2 (Remote ID), which sends the client's MAC address by default, to send the AP's MAC address, or the client MAC plus ESSID or AP MAC plus ESSID.
            - Subopt-150 with VLAN ID: This sub-option encapsulates the VLAN ID.
            - Subopt-151 with format: This sub-option can encapsulate either the ESSID or a configurable Area Name.
            -
    d. Click **OK**.

You have created the Bridge forwarding profile.

NOTE
You can also edit and delete the profile by selecting the options **Configure** and **Delete** respectively, from the **Bridge** tab.

Creating L2oGRE Forwarding Profiles

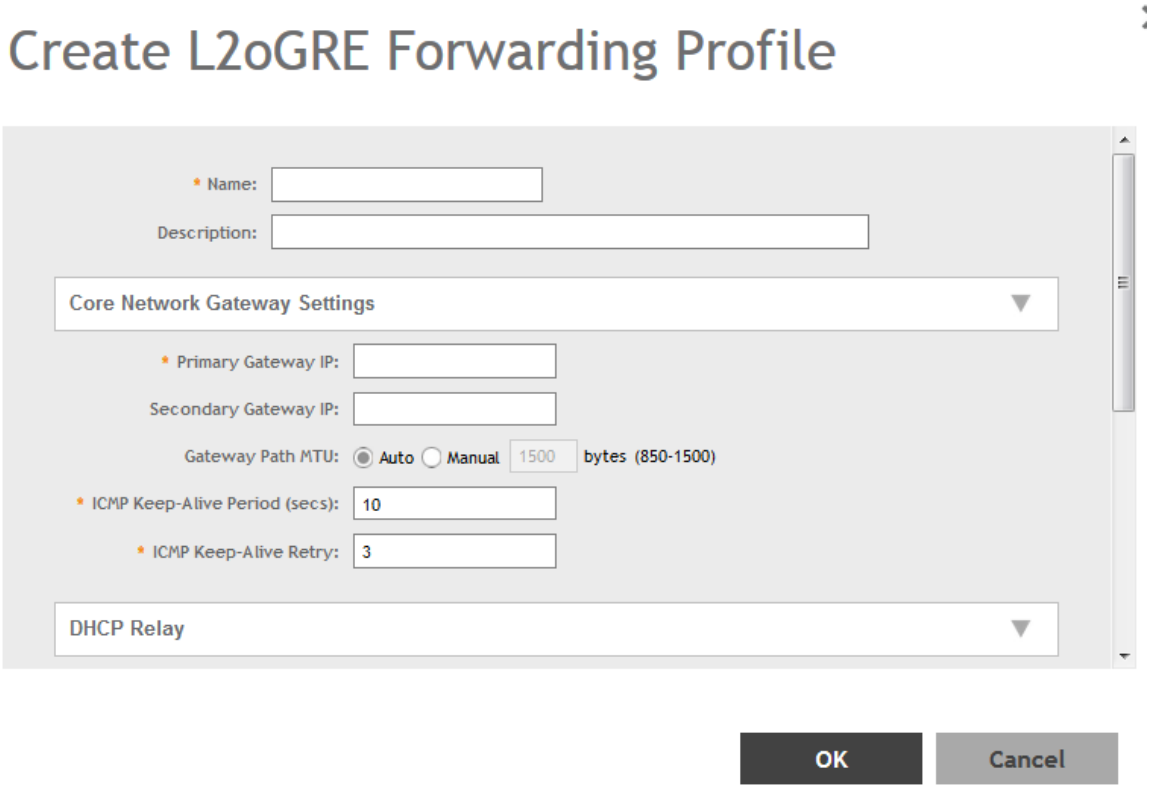
An L2oGRE forwarding profile defines the gateway and tunnel configuration for the core network of L2oGRE tunnels.

1. Go to **Services** > **Core Network Tunnel** > **L2oGRE**.
2. Select the zone for which you want to create the profile.

3. Click **Create**.

   The **Create L2oGRE Forwarding Profile** page appears.

FIGURE 280 Creating a L2oGRE Forwarding Profile



4. Configure the following:
   a. Name: Type a name for the profile that you are creating.
   b. Description: Type a brief description for the profile.
   c. Core Network Gateway Settings
      1. Primary Gateway IP: Type the IP address of the primary gateway for the L2oGRE tunnel.
      2. Secondary Gateway IP: Type the IP address of the secondary gateway for the L2oGRE tunnel. If the primary gateway is unreachable, this gateway will be used for the L2oGRE tunnel.
      3. Gateway Path MTU: Set it the MTU manually or use Auto (default). MTU is the size of the largest protocol data unit (in bytes) that can be passed on the controller network.
      4. ICMP Keep-Alive Period (secs): Set the time in seconds between sending retry messages to the keepalive IP address. Enter an integer between 2 and 255. The default is 10 seconds.
      5. ICMP Keep-Alive Retry: Set the retry period to send messages to the keepalive IP address. The default value is 3 retries.
   d. DHCP Relay: Select the **Enable DHCP Relay**check-box and configure the DHCP server IP address and DHCP option 82 settings.
      1. DHCP Server 1: Type the IPv4 address of the DHCP server that will allocate IP addresses to DHCP clients.
      2. DHCP Server 2: If a secondary DHCP server exists on the network, type the IPv4 address of the secondary server.
      3. DHCP Option 82: Select this check box if you want the DHCP relay agent (in this case, the controller) to insert specific identification information into requests that are forwarded to the DHCP server. If you enabled DHCP Option 82, you can configure the following Option 82 sub-options by selecting the corresponding check boxes:
         - Subopt-1 with format: You can customize sub-option 1 (Circuit ID) to send only the AP's MAC address in hexadecimal format or the MAC address and ESSID. The default format is: IFName:VLAN-ID:ESSID:AP-Model:AP-Name:AP-MAC.
         - Subopt 2 with format: You can customize sub-option 2 (Remote ID), which sends the client's MAC address by default, to send the AP's MAC address, or the client MAC plus ESSID or AP MAC plus ESSID.
         - Subopt-150 with VLAN ID: This sub-option encapsulates the VLAN ID.
         - Subopt-151 with format: This sub-option can encapsulate either the ESSID or a configurable Area Name.
   e. Click **OK**.

You have created the L2oGRE forwarding profile.

NOTE
You can also edit and delete the profile by selecting the options **Configure** and **Delete** respectively, from the **L2oGRE** tab.

SoftGRE Support

This appendix describes the SoftGRE support that the controller provides and the supported deployment topology.

Overview of SoftGRE Support

There are numerous equipment vendors serving the service provider market today. Among these vendors, the more prominent ones include Alcatel-Lucent (ALU), Ericsson, NSN, Huawei and Cisco. Most of these vendors support different tunneling and mobility management protocols at their packet gateways.

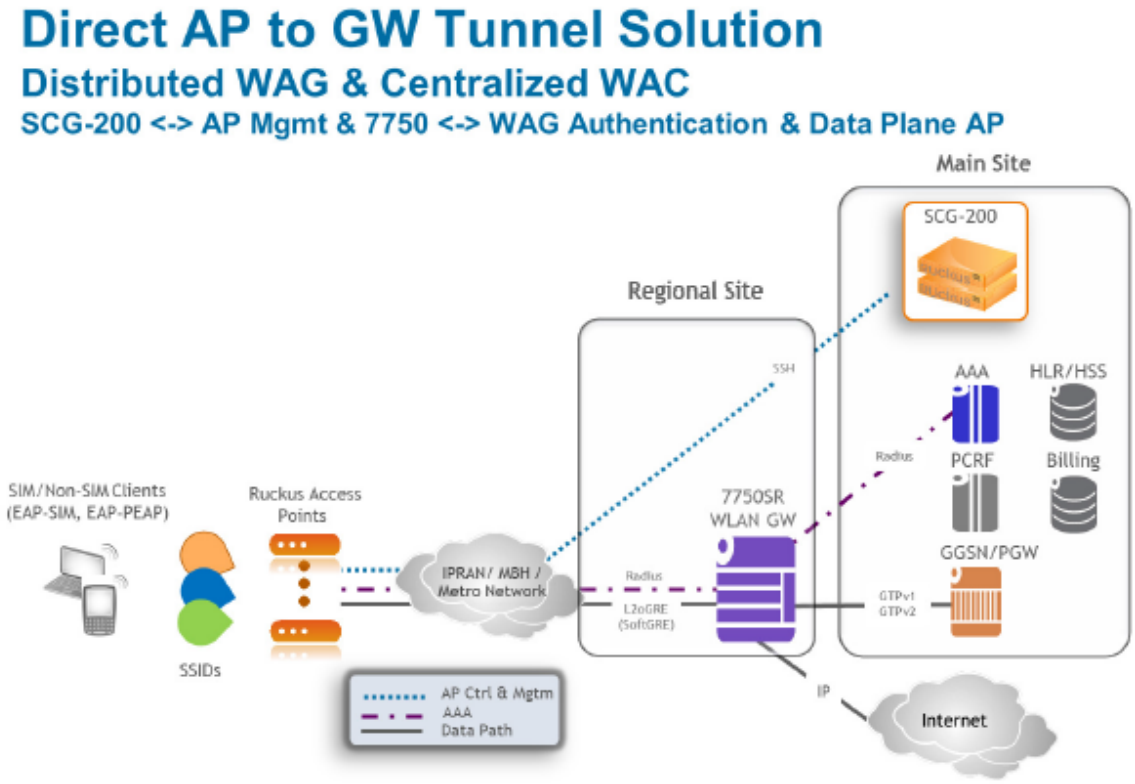
Since most (if not all) of these equipment vendors do not develop access points themselves, they are publishing SoftGRE specifications to enable access point vendors (such as RUCKUS) to support SoftGRE on their devices.

Supported Deployment Scenario

The controller supports SoftGRE in the deployment scenario wherein the controller functions purely as an AP controller. In this deployment topology, the controller only manages the RUCKUS APs and does not perform other functions. All control paths (RADIUS Authentication/Accounting) and data paths (SoftGRE tunnel) terminate on the third party WLAN gateway.

If 802.1x authentication is used, the RADIUS server will be outside of the SoftGRE tunnel. If open, WISPr-based authentication is used, the portal or redirect function will be on the edge router or northbound of the edge router. The controller does not play any role in the control and data path functions.

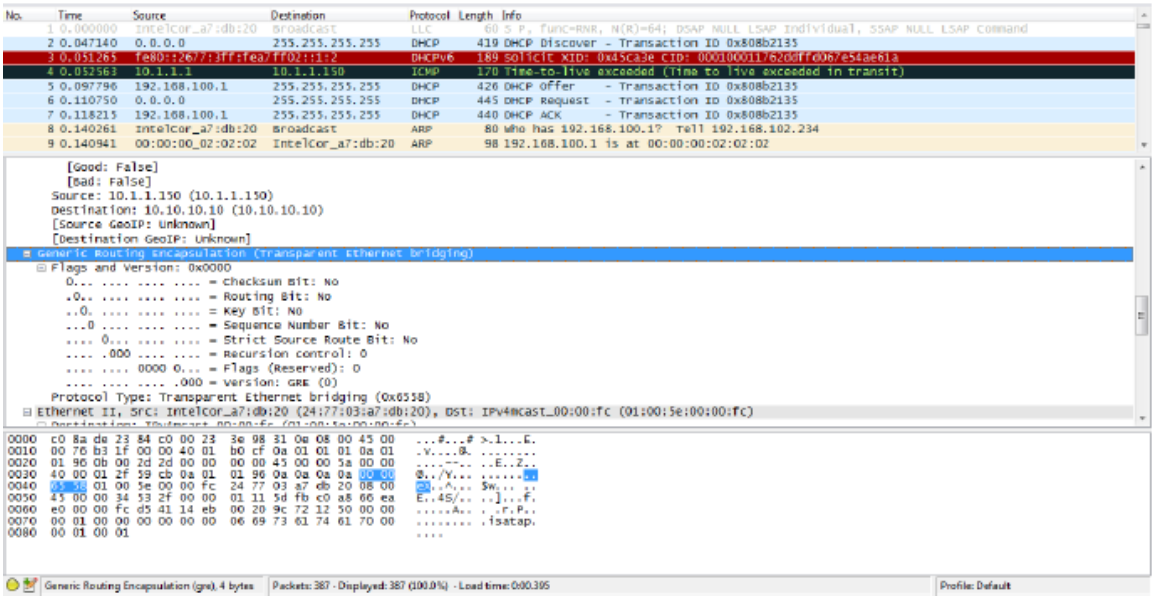
FIGURE 281 The controller as a pure AP controller



SoftGRE Packet Format

The following figure displays a screen shot of SoftGRE packet capture data.

FIGURE 282 Example of SoftGRE packet format



Configuring And Monitoring AP Zones

If no tunneled WLANs exist in the zone, you can change the tunnel type from SoftGRE to GRE or GRE + UDP.

MVNO accounts are currently unsupported by SoftGRE tunnels. If you create an MVNO account and assign an AP zone that is using a SoftGRE tunnel, an error message appears.

1. Follow the steps as described in Creating an AP Zone on page 105 to change the tunnel type from SoftGRE.
2. Scroll down to the **AP GRE Tunnel Options** section and select the **Ruckus GRE Profile** or click Add to create a new profile.
3. From the Create Ruckus GRE Profile window, select the **Ruckus Tunnel Mode** to which you want to change from SoftGRE.

   If you attempt to change the tunnel type when a tunneled WLAN exists within the zone, the following error message appears:

   ```
   Unable to update the configuration of the AP zone. Reason: It is disallowed to change the
   tunnel type, because it
   has tunneled WLAN.
   ```

4. Click **OK**.

   The zone configuration information is displayed.

SoftGRE SNMP MIBs

The following table lists the SoftGRE OIDs.

TABLE 107 OIDs related to SoftGRE

Parent Node	Node Name	OID
ruckusWLANAPInfo	ruckusSCGWLANAPMacAddr	1.3.6.1.4.1.25053.1.3.2.1.1.2.3.1.1
	ruckusSCGWLANAPSoftGREServer	1.3.6.1.4.1.25053.1.3.2.1.1.2.3.1.2
	ruckusSCGWLANAPSoftGREGWAddr	1.3.6.1.4.1.25053.1.3.2.1.1.2.3.1.3
	ruckusSCGWLANAPSoftGREActive	1.3.6.1.4.1.25053.1.3.2.1.1.2.3.1.4
	ruckusSCGWLANAPSoftGRETxPkts	1.3.6.1.4.1.25053.1.3.2.1.1.2.3.1.5
	ruckusSCGWLANAPSoftGRETxBytes	1.3.6.1.4.1.25053.1.3.2.1.1.2.3.1.6

TABLE 107 OIDs related to SoftGRE (continued)

Parent Node	Node Name	OID
	ruckusSCGWLANAPSoftGRERxPkts	1.3.6.1.4.1.25053.1.3.2.1.1.2.3.1.7
	ruckusSCGWLANAPSoftGRERxBytes	1.3.6.1.4.1.25053.1.3.2.1.1.2.3.1.8
	ruckusSCGWLANAPSoftGRETxPktsErr	1.3.6.1.4.1.25053.1.3.2.1.1.2.3.1.9
	ruckusSCGWLANAPSoftGRERxPktsErr	1.3.6.1.4.1.25053.1.3.2.1.1.2.3.1.10
	ruckusSCGWLANAPSoftGRETxPktsDropped	1.3.6.1.4.1.25053.1.3.2.1.1.2.3.1.11
	ruckusSCGWLANAPSoftGRERxPktsDropped	1.3.6.1.4.1.25053.1.3.2.1.1.2.3.1.12
	ruckusSCGWLANAPSoftGRETxPktsFrag	1.3.6.1.4.1.25053.1.3.2.1.1.2.3.1.13
	ruckusSCGWLANAPSoftGREICMPTotal	1.3.6.1.4.1.25053.1.3.2.1.1.2.3.1.14
	ruckusSCGWLANAPSoftGREICMPNoReply	1.3.6.1.4.1.25053.1.3.2.1.1.2.3.1.15
	ruckusSCGWLANAPSoftGREDisconnect	1.3.6.1.4.1.25053.1.3.2.1.1.2.3.1.16

SoftGRE Events and Alarms

If there is no downstream traffic in the tunnel, APs that belong to the zone configured for SoftGRE send out-of-band ICMP keep-alive messages (interval is configurable) to the active third party WLAN gateway. If an AP does not receive a response from the active WLAN gateway, it triggers an alarm and it automatically creates a SoftGRE tunnel to the standby WLAN gateway.

If the AP does not receive a response from the standby WLAN gateway either, the AP disconnects all tunneled WLAN services. It continues to send keep-alive messages to both the active WLAN gateway (primary GRE remote peer) and standby WLAN gateway (secondary GRE remote peer). If it receives a response from either WLAN gateway, the AP restores all tunneled WLAN services automatically.

There are four types of events that APs send to the controller:

- Failover from primary GRE remote peer to secondary GRE remote peer
- Failover from secondary GRE remote peer to primary GRE remote peer.
- Tunnel disconnected because both primary and secondary GRE remote peers are unreachable
- Tunnel restored because either primary or secondary GRE remote peer is reachable

For the list of alarms and events related to SoftGRE that APs generate, refer to SoftGRE Events on page 495 and SoftGRE Alarms.

SoftGRE Events

SoftGRE related events that APs send to the controller.

Following are the events related to SoftGRE that AP generates.

apSoftGRETunnelFailOverPtoS
AP [{apname@apMac}] fails over from primaryGRE [{address}] to secondaryGRE [{address}].
Code: 611
Severity:
Attributes:

- "apMac"="xx:xx:xx:xx:xx:xx"
- "primaryGRE"="xxx.xxx.xxx.xxx"
- "secondaryGRE"="xxx.xxx.xxx.xxx"

apSoftGRETunnelFailOverStoP
AP [{apname@apMac}] fails over from secondaryGRE [{address }] to primaryGRE [{address}].
Code: 612
Severity: Warning

	Attributes: • "apMac"="xx:xx:xx:xx:xx:xx" • "secondaryGRE"="xxx.xxx.xxx.xxx" • "primaryGRE"="xxx,xxx.xxx.xxx"
apSoftGREGatewayReachable	AP [{apname@apMac}] is able to reach [{softgreGW}] [{softgreGWAddress}] successfully. Code: 613 Severity: Informational Attributes: • "apMac"="xx:xx:xx:xx:xx:xx" • "softgreGW"="primaryGRE" • "softgreGWAddress" = "xxx.xxx.xxx.xxx"
apSoftGREGatewayNotReachable	AP [{apname@apMac}] is able to reach [{softgreGW}] [{softgreGWAddress}] successfully. Code: 614 Severity: Critical Attributes: • apMac"="xx:xx:xx:xx:xx:xx" • "softGREGatewayList"="xxx.xxx.xxx.xxx, yyy,yyy.yyy.yyy"

Working with DHCP

DHCP/NAT

DHCP/NAT functionality on SZ-managed APs and DPs (data planes) allows customers to reduce costs and complexity by removing the need for DHCP server/NAT router to provide IP addresses to clients. For data traffic aggregation and services delivery you can choose appropriate user profile for DHCP and NAT services on vSZ-D.

AP-based DHCP/NAT

In highly distributed environments, particularly those with only a few APs per site, the ability for an AP or a set of APs to provide DHCP/NAT support to local client devices simplifies deployment by providing all-in-one functionality on the AP, which eliminates the need for a separate router and DHCP server for each site. It also eases site management by providing central control and monitoring of the distributed APs and their clients.

> **NOTE**
> While changing from a non-DHCP or a non-NAT enabled zone to a DHCP or a NAT enabled zone, the AP will start the DHCP services on the gateway AP.

Three general DHCP scenarios are supported:

- SMB Single AP: DHCP is running on a single AP only. This AP also functions as the Gateway AP.
- SMB Multiple APs (<12): DHCP service is running on all APs, among which two of the APs will be Gateway APs. These two Gateway APs will provide the IP addresses as well as Internet connectivity to the clients via NAT.
- Enterprise (>12): For Enterprise sites, an additional on site vSZ-D will be deployed at the remote site which will assume the responsibilities of performing DHCP/NAT functions. Therefore, DHCP/NAT service will not be running on any APs (they will serve clients only), while the DHCP/NAT services are provided by the onsite vSZ-D.

Profile-based DHCP

The DHCP Server is designed in-line in the data plane and provides extreme scale in terms of IP address assignment to clients. This feature is especially useful in high density and dynamic deployments like stadiums, train stations where large number of clients continuously move in & out of WiFi coverage. The DHCP server in the network needs to scale to meet these challenging requirements. The DHCP server on the vSZ-D provides high scale IP assignment and management with minimal impact on forwarding latency. The DHCP server allows IP assignment only when a DHCP license assignment policy is created for a specific vSZ-D. A maximum of 101k IP assignments are allowed for each vSZ-D. Additional IP assignments requires additional licensing.

NOTE
DHCP Server/NAT function if enabled is supported only for wireless client IPv4 address assignment.

Profile-based NAT

With NAT service enabled, all the WiFi client traffic is NATed by the vSZ-D before being forwarded to the core network. The NAT license assignment policy for specific vSZ-D must be created. Each vSZ-D supports up to 2 million NAT ports (traffic sessions) and 128 public IP addresses for NAT. This feature essentially reduces the network overhead significantly since this reduces the MAC-table considerations on the UP-stream switches significantly. Again, very useful in high density deployments.

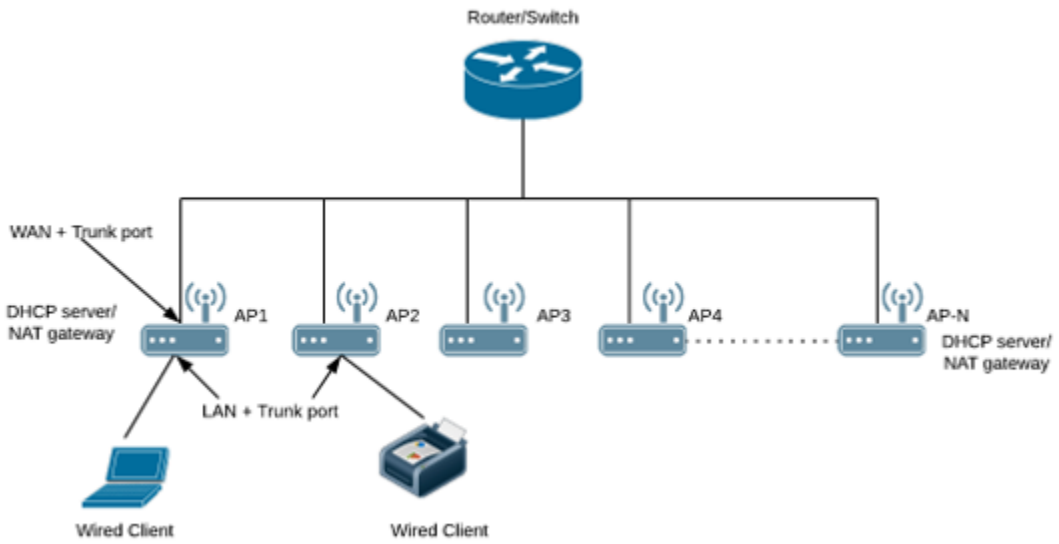
Network Topology

There are three types of network topologies for APs. They are:

Single AP Topology

All the APs in the zone get their IP from the WAN router and provides the DHCP/NAT service. If H510/H320 is configured as GAP by manual port selection, then LAN1 and LAN2 configuration will be pushed to eth1 and eth2 ports of H510/H320 APs instead of eth0 and eth1 ports.

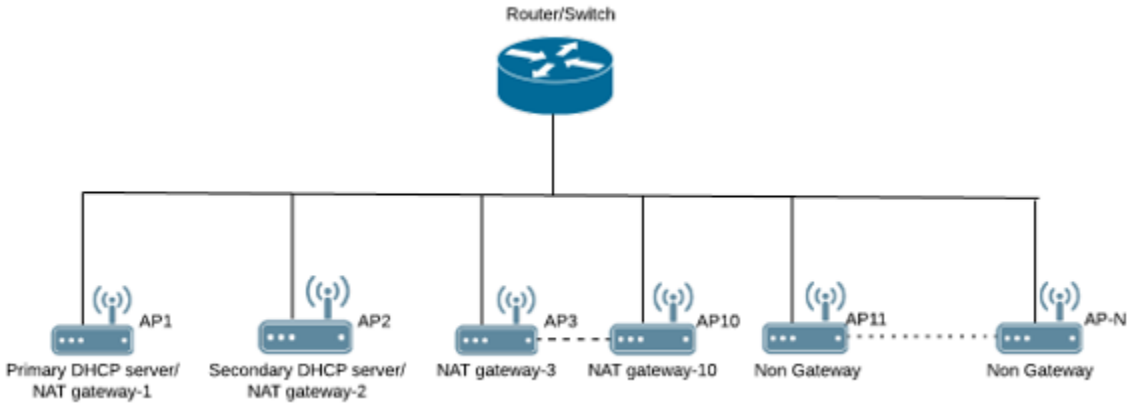
FIGURE 283 Single AP Topology



Multiple AP (Flat Network) Topology

All the APs in the zone get their IP from the WAN router and designated APs provide the DHCP/NAT service. A maximum of two APs be can select for DHCP service (Primary and Secondary) and ten APs for NAT Gateway.

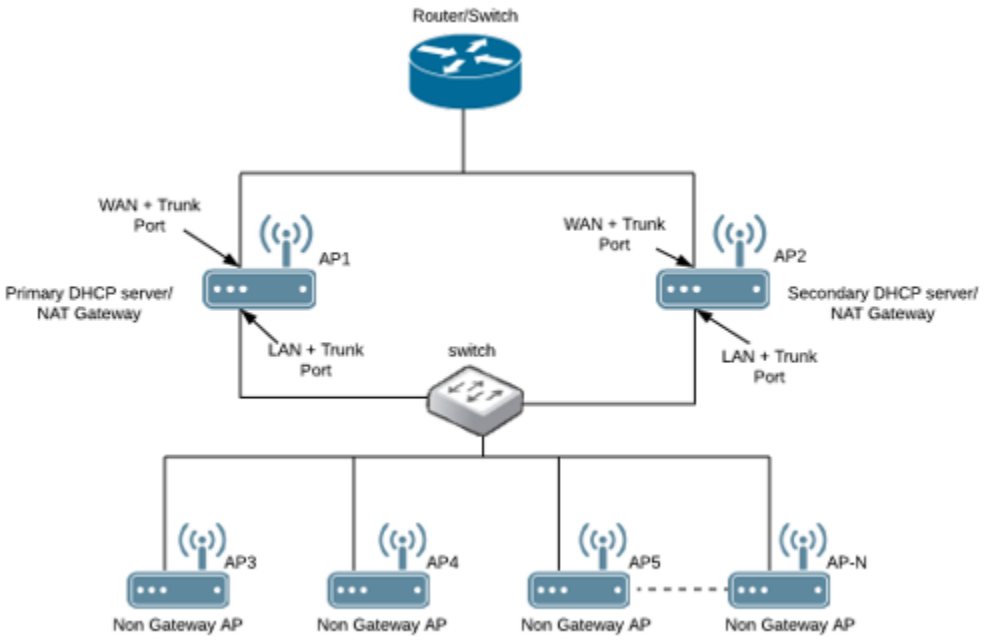
FIGURE 284 Multiple AP (Flat Network) Topology



Hierarchical AP Topology

Designated APs provide the DHCP/NAT service. Gateway APs get the IP address from the WAN router and non-gateway APs get the IP from the Gateway APs. If H510/H320 is configured as GAP by manual port selection, then LAN1 and LAN2 configuration will be pushed to eth1 and eth2 ports of H510/H320 APs instead of eth0 and eth1 ports. In order to configure eth0 ports of H510/H320 the user needs to configure LAN5/LAN3 Ports respectively for the H510/H320 APs.

FIGURE 285 Hierarchical AP Topology



Hierarchical Network Topology

Hierarchical network topology along with DHCP/NAT runs on single and multiple APs The Gateway APs can directly be connected to the service providers' route/switch and can get the public IPs. The NGAPs can get the private IPs from the GAP through the DHCP/NAT service. Wired client such as printers and laptops can be directly connected to the LAN port of the GAP or WAN ports of Non-GAPs and hence can be operational without the use of external DHCP/NAT. Basic Mesh Topology is supported where the GAP is root the AP and all other NGAP can be the Mesh APs.

The Dynamic WAN Port Detection (DWPD) algorithm detects the WAN port among eth0/eth1/eth2 of the APs and marks only one port of AP as WAN. LAN port selection is based on the availability of wired port with tunnel enabled. All other wired ports on the AP will be marked as LAN.

Expected behavior in case of a three port AP are as follows:

- Eth0: connected to WAN

  Final result after DWPD: Eth0=WAN, ETH1=LAN, ETH2=WAN
- Eth1: connected to WAN

  Final result after DWPD: Eth0=LAN, ETH1=WAN, ETH2=WAN
- Eth2: connected to WAN

  Final result after DWPD: Eth0=LAN, ETH1=WAN, ETH2=WAN

Using DWPD you can do plug-n-play without worrying about the configuration of WAN or LAN ports. Wired client connectivity for each AP where all the APs in the zone run DHCP/NAT service. All ethernet ports can be configured as LAN port and wired clients can be used to connect. LAN port profile enables APs with multiple ethernet ports to be configured as LAN ports. Hence there is no need for a separate switch if the multi-port AP is GAP and all the required wired and NGAP AP can be connected directly to the number of available ethernet ports.

While using DHCP NAT-HN with DWPD, the AP will ignore the eth port configuration which is pushed from the interface. The AP will select the WAN and LAN ports dynamically. After successful detection of the WAN port, it marks the other port as LAN port. When it marks an eth port as LAN, DWPD chooses untagged VLAN ID as 1 by default. This configuration for LAN port is not changeable. Hence, wired client can get the IP address from DHCP Pool VLAN ID 1. If you want to configure eth port VLAN ID to 100 through the interface, manually select WAN port and apply appropriate eth port profile to the eth0 and eth1 ports of AP.

> **NOTE**
> If APs or clients connected to a LAN switch come up before the DWPD process completes on the Gateway APs, the clients or NGAPs may get IP addresses from the WAN VLANS (the default VLAN or non-default VLAN, which is part of WAN).

Configuring AP-based DHCP Service Settings

Using DHCP service settings, you can configure an AP to assign private IP addresses to Wi-Fi clients and wired clients without the need for a separate DHCP server (router).

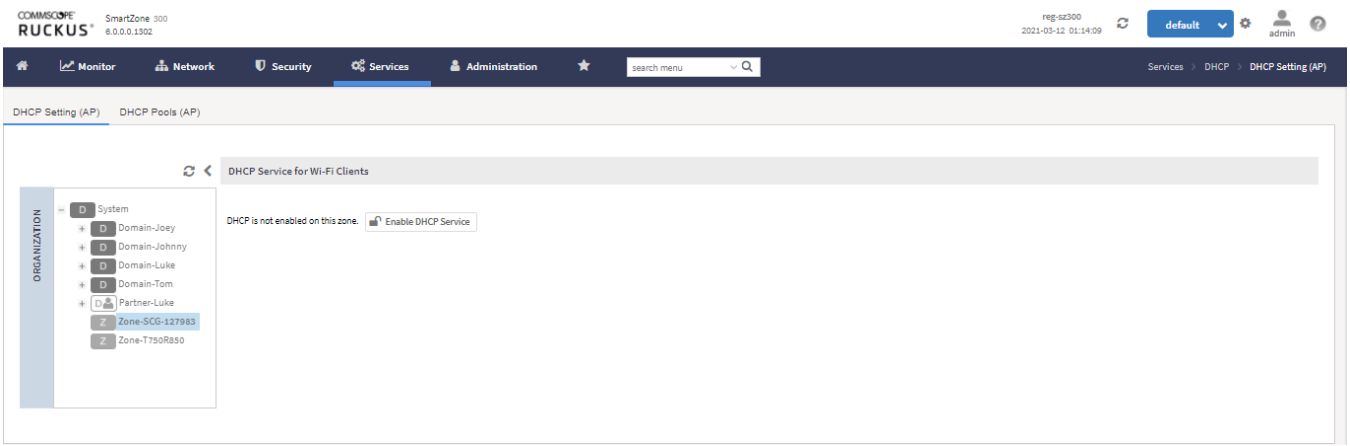
Before you configure the DHCP Service, consider the following:

- There must be minimum one and maximum 10 APs acting as Gateway AP (GAP) based on the topology selected during DHCP and NAT configuration. There is no count in the number of APs acting as Non-Gateway APs (NGAP).
- For a single non-Gateway AP (NGAP) you can connect eth0 of NGAP to LAN port (usually eth1) of GAP.
- For more than one NGAP you need a minimum L2 switch to connect the LAN port of GAP to all the NGAPs
- For APs having more than 2 ethernet ports, all the eth ports except the WAN backhaul (usually eth0) can be configured as LAN ports. In such case a separate switch may not be required.

To configure DHCP services:

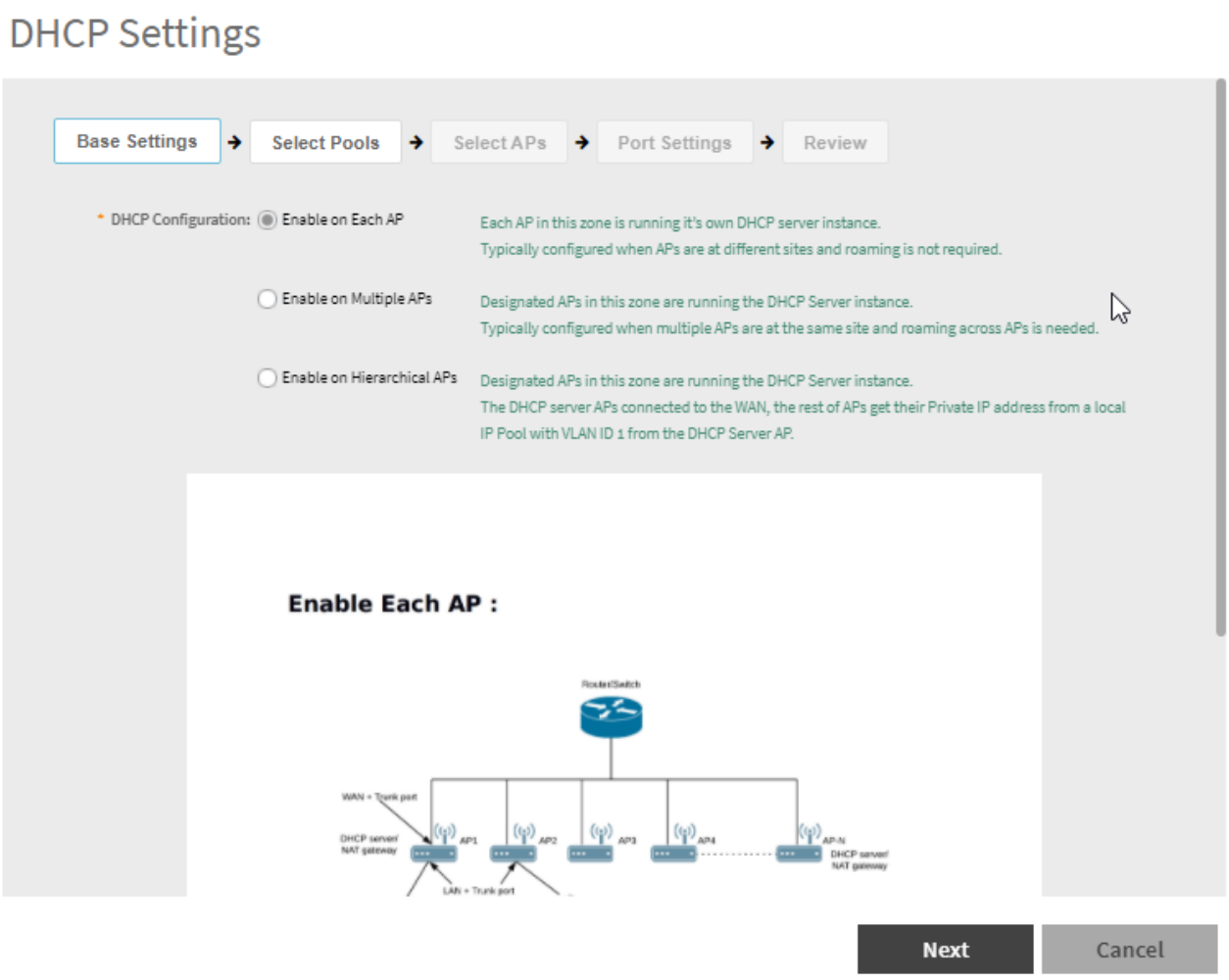
1. Go to **Services** > **DHCP** > **DHCP Setting (AP)**.

FIGURE 286 Enabling DHCP Service



2. Select a Zone from the zone list on the left side of the screen, and click **Enable DHCP Service**.

FIGURE 287 DHCP Settings wizard

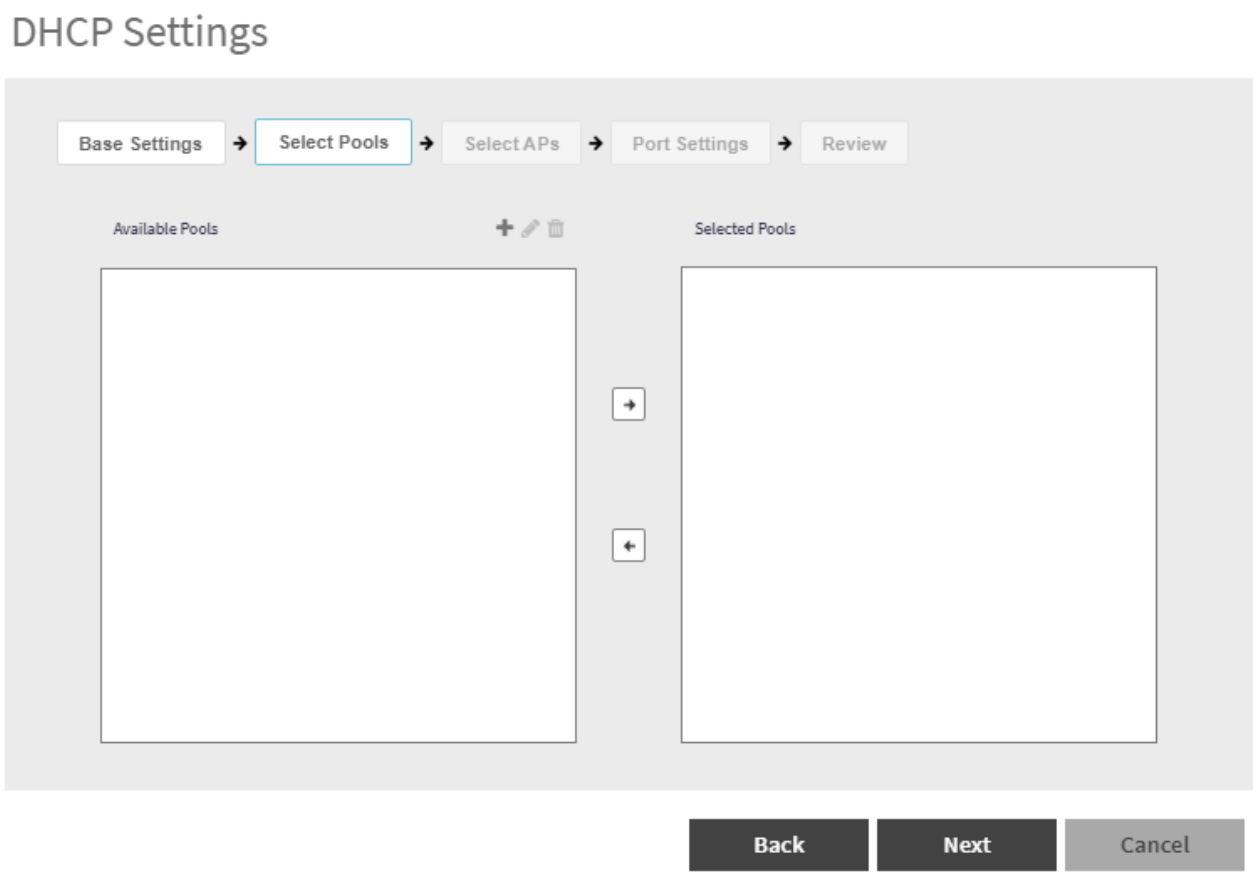


3. On the first page of the wizard (**Base Settings**), configure the **DHCP Configuration** as follows:
   - **Enable on Each AP**: Each AP in this zone gets the IP from the WAN router and runs its own DHCP server instance. This option is typically used when APs are at different sites and roaming is not required
   - **Enable on Multiple APs**: Designate which APs will provide DHCP/NAT service. This option is typically used when multiple APs are at the same site and roaming is required. This option also allows you to choose whether to automatically or manually specify which APs will provide DHCP service.
   - **Enable on Hierarchical APs**— Designate which APs will provide DHCP/NAT service. The DHCP Server AP connect to the WAN and the other AP get its private IP address from the local IP pool with VLAN ID 1 from the DHCP Server AP.
4. Click **Next**.

5. On the next wizard screen, (**Select Pools**), select up to four DHCP pools from which to assign client IP addresses.

   NOTE
   For the **Enable on Hierarchial APs** DHCP configuration, one of the pools must be VLAN ID 1.

FIGURE 288 Selecting Pools



   NOTE
   If you have not already created DHCP pools, you can do so from within the wizard. Click the Plus (+) icon and configure the IP address pools as described in the Creating an AP DHCP Pool on page 505.

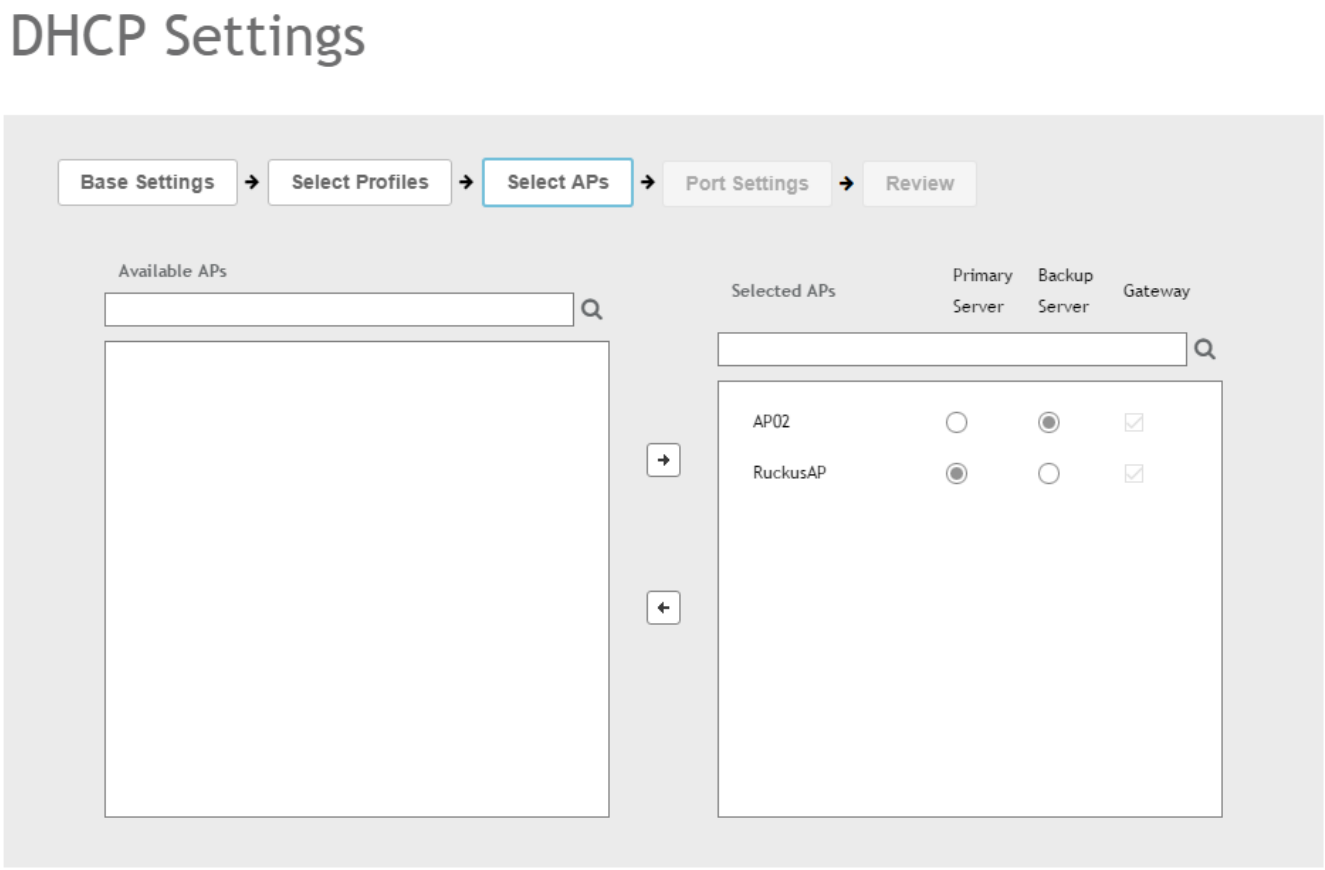
6. Click **Next**. The **Select APs** screen appears.

   NOTE
   If you selected **Auto Select AP** on the first wizard screen, this configuration screen will be skipped.

7. On the **Select APs** wizard screen, select the APs specific to the base DHCP settings:

   NOTE
   For the **Enable on Multiple APs** DHCP configuration, you can select a maximum of two APs for DHCP service (Primary and secondary) and a maximum of ten APs can as selected for NAT Gateway.

FIGURE 289 Selecting APs



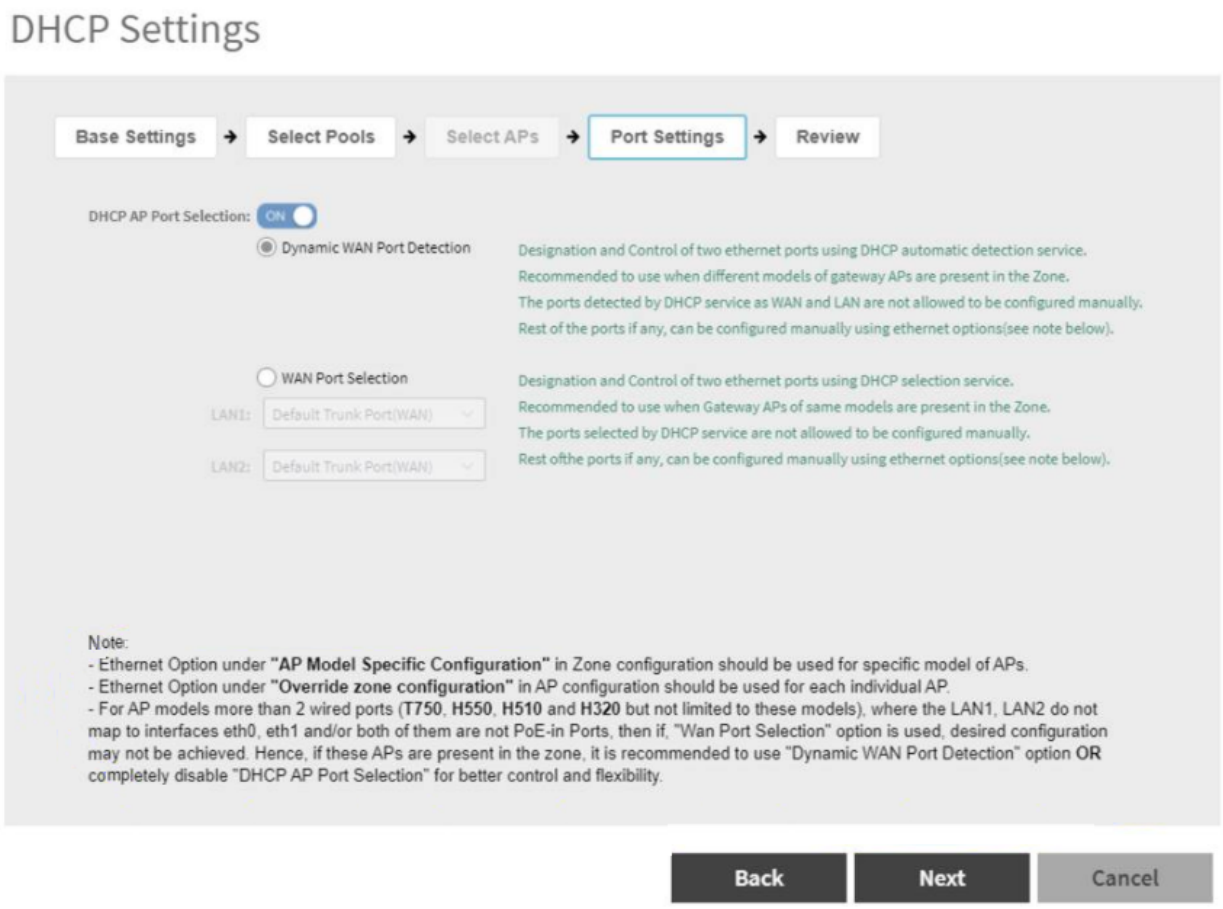
8. Click **Next**. The **Port Settings** screen is displayed.

9. On the **Port Settings** wizard screen, click **DHCP AP Port Selection** to configure the port settings for **Enable on Each AP** and **Enable on Hierarchical APs** options. Configure the following:

   NOTE
   For AP models with more than two wired ports, where LAN1 and LAN2 do not map to eth0 and eth1 interfaces respectively, and where both are not PoE-In ports, it is recommended to use Dynamic WAN Port Detection option or disable DHCP AP Port Selection.

- **Dynamic WAN Port Detection**(DWPD)—WAN is automatically identified by default and the LAN will be selected.The non-DWPD ports can be configured. It is recommended to use this option when different models of gateway APs are present in the Zone. The ports detected by DHCP service as WAN and LAN are not allowed to be configured manually. Rest of the ports, if any, can be configured as follows:
  - For specific models of APs, use the ethernet option in **AP Model Specific Configuration**. Refer to Table 49 on page 142.
  - For each individual AP, use the ethernet option in **Override zone configuration**. Refer to Table 49 on page 142.
- **WAN Port Selection**—Manually assign port to WAN and LAN. This setting overrides the original port configuration of a zone. It is recommended to use when Gateway APs of the same model are present in the zone. The ports selected by the DHCP service are not allowed to be configured manually. Rest of the ports, if any, can be configured manually using ethernet options. Select the **LAN1** and **LAN2** options from the drop-down. Rest of the ports, if any, can be configured as follows:
  - For specific models of APs, use the ethernet option in **AP Model Specific Configuration**. Refer to Table 49 on page 142.
  - For each individual AP, use the ethernet option in **Override zone configuration**. Refer to Table 49 on page 142.

FIGURE 290 Port Settings



10. Click **Next**.
11. On the **Review** screen, review your settings to make sure everything is correct. Once you are satisfied with your settings, click **OK** to confirm.

You have configured the DHCP server settings and applied them to an AP (or multiple APs). These APs will now provide DHCP/NAT functionality and assign IP addresses to wireless clients from the DHCP address pools you specified.

Creating an AP DHCP Pool

Creating a DHCP pool is necessary for assigning IP addresses to clients. Multiple address pools can be created and assigned to APs that are running DHCP services. When a client is then connected to the wireless network, it assigns an IP address from the DHCP pool(s) as specified.

Follow the steps below to configure a DHCP pool for an IP address allocation:

1. From the main menu go to **Services** > **DHCP** > **DHCP Pools (AP)**.
2. Select the zone to create the pool.
3. Click **Create**.

   The **Create DHCP Pool** page appears.

4. Configure the following:
   - **Name**: Type a name for the pool you want to create.
   - **Description**: Type a description of the pool you want to create.
   - **VLAN ID**: Type the VLAN ID for the pool.
   - **Subnet Network Address**: Type the IP subnet network address (for example, 192.168.0.0).
   - **Subnet Mask**: Type the subnet mask IP address (for example, 255.255.255.0).
   - **Pool Start Address**: Type the first IP address to be allocated to clients from the pool (for example, 192.168.0.1).
   - **Pool End Address**: Type the last IP address to be allocated to clients from the pool (for example, 192.168.0.253).

     NOTE
     The maximum number of supported IPs per pool is 1000. In each zone, there can be a maximum of 4 pools. Therefore, the total maximum supported IPs per zone is 4000 (4 pools x 1000 IPs).

   - **Primary DNS IP**: Type the primary DNS server IP address.
   - **Secondary DNS IP**: Type the secondary DNS server IP address.
   - **Lease Time**: Enter the IP address lease time, after which clients will have to renew or request new IP addresses.
5. Click **OK**.

You have created a DHCP address pool. You can now apply this address pool to a DHCP service, as described in Configuring AP-based DHCP Service Settings on page 499.

NOTE
You can also edit, clone and delete the address pool by selecting the options **Configure**, **Clone** and **Delete** respectively, from the **Pool** tab.

Creating Profile-based DHCP

DHCP profile can be applied to vSZ-D and the vSZ-D server can assign IP to the UE based on the profile rule. Different pools with the same subnet can be created without overlapping IP range.

NOTE
DHCP supports only access-side network.

- Configuring Global Settings on page 506
- Configuring DHCP Pool Settings on page 507

Configuring Global Settings

To configure Profile-based DHCP Global settings:

1. Go to **Services** > **DHCP & NAT** > **DHCP Profiles (DP)**.
2. Click **Create**, the Create DHCP Profile page appears.

3. Configure the following:
   - **Profile Name**: Type a name for the DHCP profile you want to create. AP supports 32 bytes.
   - **Description**: Type a description of the settings you want to create.
   - **Domain Name**: Type the domain name address.
   - **Primary DNS Server**: Type the primary domain name server address.
   - **Secondary DNS Server**: Type the secondary domain name server address.
   - **Lease Time**: Type the duration in Hours, Minutes and Seconds. Range: 1 through 86400 seconds.
   - **DHCP Option43 Space**: Click **Create**, the Create DHCP Option43 Space form appears. Configure the following:
     - **Space Name**: Type a name for Option43 space.
     - **Description**: Type a description for Option43 space.
     - Under **Option43 Sub Option**, click **Create** and configure the following:
       - **Sub Option Name**: Type a sub option name.
       - **Type**: Select the required option from the drop-down.
       - **Code**: Enter a code. Range: 1 through 254.
       - Click **OK**, you have created Option43 Sub Option.
     - Click **OK**, you have created Option43 Space.
   - **Hosts**: Click **Create**, the Create Host Configuration form appears. Configure the following:
     - **General Options**
       - **Host**: Type a name for the host settings that you want to create.
       - **Description**: Type a description for the host settings that you want to create.
     - **Policy Options**
       - **MAC Address**: Type the MAC address of the DHCP host.
     - **Assigning Options**
       - **Broadcast Address**: Type the broadcast IP address.
       - **Fixed Address**: Type the fixed IP address of the host.
       - **Gateway**: Type the gateway IP address.
       - **DNS Server**: Type the IP address of the DNS server.
       - **Domain Name**: Type the domain name.
       - **Host Name**: Type the host name.
       - **Lease Time**: Type the duration in Hours, Minutes and Seconds. Range: 1 through 86400 seconds.
     - Click **OK**, you have created DHCP Host configuration.
4. Click **OK**.

   You have created DHCP Profile settings.

Configuring DHCP Pool Settings

To configure DHCP pool settings:

1. Go to **Services** > **DHCP & NAT** > **DHCP Profiles (DP)**.
2. Select the DHCP prolife from the list for which you want to configure the pool settings.
3. Select the **Pools** tab page.

4. Click Create and configure the following:
   - **General Options**
     - **Pool Name**: Type a name for the pool configuration.
     - **Description**: Type a description for the pool configuration.
   - **Policy Options**
     - **Policy Type**: Select **VLAN** or **VNI** option.

       NOTE
       For policy type:
       - Either VLAN range or QinQ VLAN must be configured.
       - QinQ VLAN cannot be configured when VLAN range is 1.
       - Combination of VLAN range and QinQ VLAN should be unique among DHCP Pools in DHCP profile.

     - **VLAN Range**: Type the VLAN range. Range: 1, 2 through 4095. For example: 1, 2 or 2-3.
     - **QinQ VLAN**: Select the check box and update the following:

       NOTE
       This feature is supported only in vSZ-H platform.

       - **QinQ SVLAN Range**: Type a SVLAN range. Range: 2 through 4095.
       - **QinQ CVLAN Range**: Type a CVLAN range. Range: 2 through 4095.
   - **Assigning Options**
     - **Subnet**: Type the IP address.
     - **Subnet Mask**: Type the network address.
     - **Broadcast Address**: Type the broadcast IP address.
     - **Pool Range**: Type the address range for the pool.
     - **Exclude Pool**: Type the address range that must be excluded.
     - **Primary Gateway**: Type the primary gateway IP address.
     - **Secondary Gateway**: Type the secondary gateway IP address.
     - **Primary DNS Server**: Type the IP address of the primary DNS server.
     - **Secondary DNS Server**: Type the IP address of the secondary DNS server.
     - **Domain Name**: Type the domain name.
     - **Host Name**: Type the host name.
     - **Lease Time**: Type the duration in Hours, Minutes and Seconds. Range: 1 through 86400 seconds.
   - **Option43 Value**
     - Click **Create**, the Create Option43 value form appears. Configure the following:
       - Choose the **Space** Name or click **Create** to configure Option 43 Space Name.
       - Enter a **Description**.
     - Click **OK**, you have configured Option43 value.
5. Click **OK**.

   You have created DHCP pool configuration.

Creating Profile-based NAT

A NAT Profile could be applied to a vSZ-D. The NAT server settings work independently. You must configure the following settings to create a NAT profile:

NOTE
NAT does not support multiple public subnet/VLAN.

- Configuring NAT Global Settings on page 509
- Configuring NAT Pool Setting on page 509

Configuring NAT Global Settings

To create a NAT global setting:

1. Go to **Services** > **DHCP & NAT** > **NAT Profiles (DP)**.
2. Click **Create**, the Create NAT Profile page appears.
3. Configure the following:
   - **Profile Name**: Type a name for the NAT profile that you want to create. AP supports 32 bytes.
   - **Description**: Type a description for the profile that you want to create.
   - **Subnet**: Type the IP address.
   - **Prefix**: Type a prefix value. Maximum range: 31.
   - **Public VLAN**: Type the VLAN range. Range: 2 through 4095.
   - **Gateway**: Type the gateway IP address.
4. Click **OK**.

   You have created a NAT Profile.

Configuring NAT Pool Setting

To configure NAT pool settings

1. Go to **Services** > **DHCP & NAT** > **NAT Profiles (DP)**.
2. Select the NAT profile from the list and click the **Pools** tab.
3. Click **Create**, the Create Pool Configuration page appears.

4. Configure the following:
   - **General Options**
     - **Pool Name**: Type a name for the NAT pool settings that you want to create.
     - **Description**: Type a description for the pool settings that you want to create.
   - **Policy Options**
     - **Policy Type**: Select **VLAN** or **VNI** option.

       NOTE
       For policy type choose to do one of the following;:
       › Update VLAN range
       › Update QinQ VLAN range
       › Leave both the fields blank for RADIUS-based NAT setup

     - **Private VLAN Range**: Type the VLAN range and click **Add**. Range: 1 through 4095. For example: 1 or 1-2.
     - **Private QinQ VLAN Range**: Type **SVLAN** range, **CVLAN** range and click **Add**. Range: 2 through 4095. For example: 2 or 2-3.

       NOTE
       This feature is supported only in vSZ-H platform.

   - **Translation Options**
     - **Port Range**: Type the port range. Range: 10000 through 65534. For example: 10000-20000.
     - **Public Address Range**: Type the public address range.

       Note: This public address must not be duplicated with the other public address in the same subnet, which includes applied NAT Profile and vSZ-D's Access and Core Interface Address.
5. Click **OK**.

   You have created a NAT pool setting.

Configuring DHCP/NAT with Mesh Options

To configure DHCP/NAT with mesh option:

1. Enable Mesh Option in zone level. Refer to **Mesh Options** in Creating an AP Zone on page 105.
2. From the Access Points page, select the AP to be assigned as the Root AP.
3. Click **Configure**.
4. Select Mesh-specific options and select Root AP mode.
5. Multiple address pools can be created and assigned to APs that are running DHCP services. Refer, Creating an AP DHCP Pool on page 505.
6. From the Services page, enable DHCP on the zone.
7. Edit the DHCP Service on the AP by selecting the required VLANs and APs as Gateway APs. Refer, Configuring AP-based DHCP Service Settings on page 499.

Working with Other SmartZone Services

Understanding WiFi Calling

Mobile service providers offer services where you can make voice calls or send and receive text messages from their mobile phones using a WiFi network, without changing the mobile number.

Built-in software applications on smart phones provide seamless authentication of the device when on the Wi-Fi network with the mobile carrier network. When WiFi calling is enabled by the mobile carrier, an IPSec tunnel is established between the phone and the mobile network through which calls are routed.

Due to increasing use of Wi-Fi for device connections, WiFi Calling is seeing high demand by many service providers worldwide, which allows them to differentiate their WiFi access. Though the end-user device and Mobile Packet Core communicate directly over encrypted tunnels, it is important for the Wi-Fi network to detect and prioritize this type of traffic for an optimal application experience.

This feature supports WiFi calling traffic recognition and prioritization above other network traffic, with visibility for Wi-Fi calling stats for the network operator. Following are some benefits of using WiFi calling in Ruckus networks:

- QoS ensures advanced identification rules prioritize voice traffic over data traffic
- Seamless roaming across APs
- Voice call analytics and reporting aid in planning network resource and troubleshooting
- Accurate classification and prioritization of voice calls over WiFi on WLANs
- Enables users to define priorities for voice, video, background and best effort on the WiFi calls generated from a particular carrier phone. For example, you can prioritize your choice of carriers WiFi calls over other WiFi calls.
- Easy to setup and offers the flexibility to add more than one ePDG FQDN/address for a carrier
- WiFi call prioritization when mobile phones roams form one AP to another

Analyzing Wi-Fi Calling Statistics

You can view a summary of the Wi-Fi calling traffic by the top ten SSIDs by traffic and ePDGs by traffic. The trends provide information about the Wi-Fi usage, and uplink and downlink speeds.

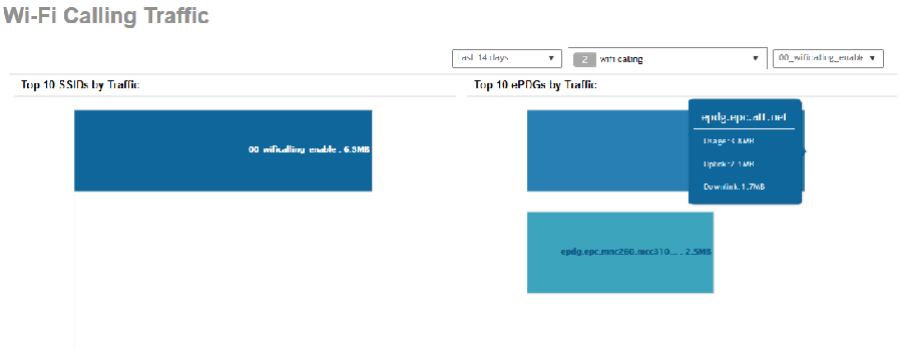
Go to **Services** > **Others** > **Wi-Fi Calling** > **Summary**.

The **Wi-Fi Calling Clients** area provides the following information about clients using Wi-Fi Calling feature, such as:

- Hostname: The name of the user equipment or device that is connected to the Wi-Fi
- MAC Address: The MAC address of the user equipment
- Carrier Name: The name of the carrier network or service provider used by the user equipment, such as AT&T, Sprint, T-Mobile, and so on.
- Priority: The priority set for the Wi-Fi call through this device, such as voice, video, best effort, and background
- Traffic Session: The amount of data that is transmitted during the Wi-Fi call

- Traffic (uplink/downlink): The speed with which data is transmitted during the Wi-Fi call

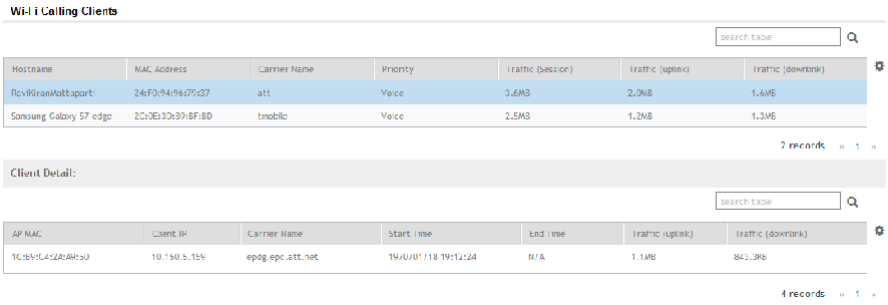
FIGURE 291 Analyzing Wi-Fi Calling Traffic



The Clients detail section provides the following information about the client involved in the Wi-Fi call:

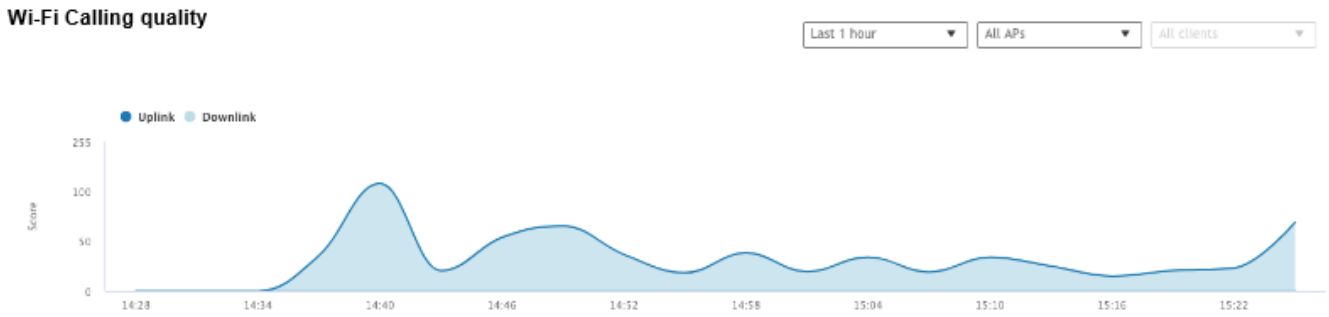
- AP MAC: The MAC address of the AP
- Client IP: The IP address of the client
- Carrier Name: The name of the carrier, for example, epdg.epc.att.net
- Start Time: The time when the client initiated the Wi-Fi call
- End Time: The time when the client completed the Wi-Fi call
- Traffic (uplink/downlink): The speed with which the data is transmitted during the Wi-Fi call session

FIGURE 292 Wi-Fi Calling Client Details



The **Wi-Fi Calling quality** chart displays the uplink and downlink Wi-Fi calling quality. Call quality can be filtered based on Time, the AP list, and the client MAC address list.

FIGURE 293 Wi-Fi Call Quality Chart



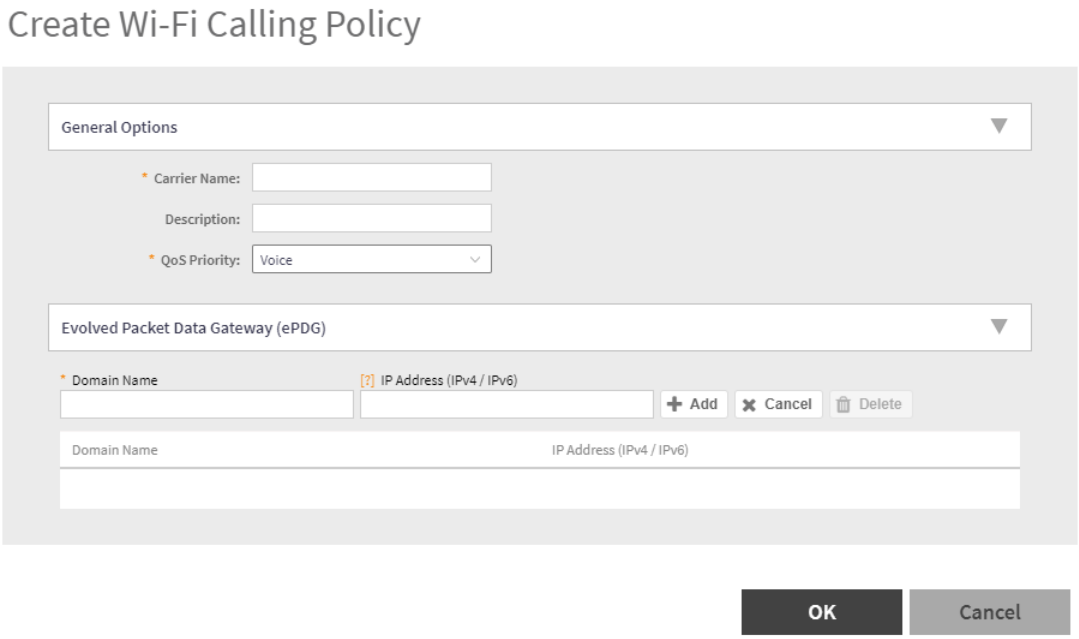
Creating a WiFi Calling Profile

You can classify the voice packets in a WiFi call based on the carrier, by creating a WiFi calling profile.

1. Go to **Services** > **Others** > **WiFi Calling** > **Profiles**.
2. Click **Create**.

   The **Create Wi-Fi Calling Policy** page appears.

   FIGURE 294 Creating a WiFi Calling Policy



3. In **General Options**, configure the following:

   Carrier Name: Enter the name of the carrier based on which you want to create a rule to prioritize the voice calls

   Description: Enter a brief description about the profile

   QoS Priority: From the drop-down menu, select the Quality of Service feature based on which you want to prioritize the calls
4. In **Evolved Packet Data Gateway (ePDG)**, configure the following:

   Domain Name: Enter the domain name. For example, epdg.epc.att.net

   IP Address optional: Enter the IP address for the domain. Providing the IP address enables better WiFi calling QoS during roaming.
5. Click **Add** to include the domain.

   The AP will verify the domain IP address before qualifying the WiFi call.
6. Click **OK** .

   The WiFi calling profile is created and displayed with its name, QoS priority, number of ePDGs associated and management domain.

   NOTE
   You can edit, clone and delete the profile by clicking **Configure**, **Clone** and **Delete**, respectively.

Configuring WiFi Calling in WLAN

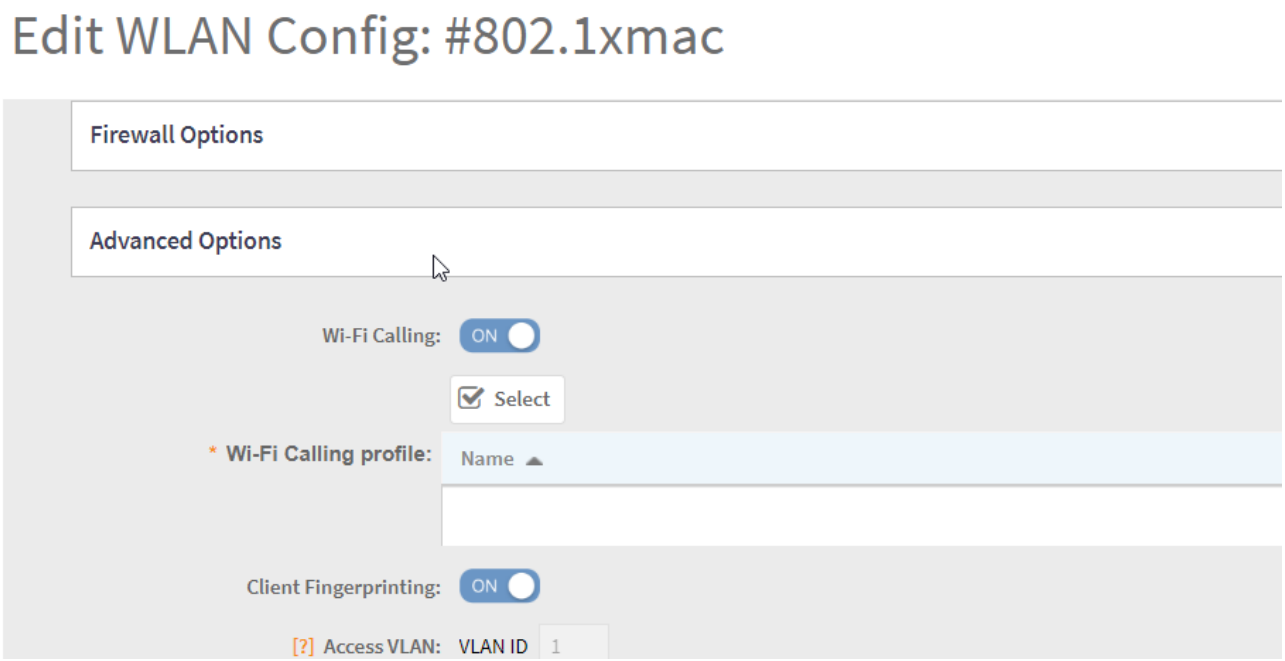
You can also edit the WLAN configuration to select a WiFi calling profile.

1. Go to **Network** > **Wireless LANS**.

2. Select the WLAN for which you want to enable WiFi calling and click **Configure**.

   The **Edit WLAN Configuration** page appears. You can also enable WiFi calling when you create a fresh WLAN configuration, by clicking **Create**.

   FIGURE 295 Configuring WiFi Calling in a WLAN



3.
4. In **Advanced Options**, move the **WiFi Calling** radio button to ON. WiFi calling is enabled.
5. Click **Select**.

   The **WiFi Calling Policies** page appears.

   From the list under **Available Profiles**, identify the ones you want and click the **->** icon. The profile(s) is moved under **Selected Profiles**. You can use the **<-** icon to de-select the profile for the WLAN.
6. Click **OK**.

   The profile(s) selected are displayed under the **WiFi Calling Profile** field.

You have selected the WiFi calling profile that you want to apply to the WLAN.

Bonjour

Bonjour is Apple's implementation of a zero-configuration networking protocol for Apple devices over IP.

Bonjour allows OS X and iOS devices to locate other devices such as printers, file servers and other clients on the same broadcast domain and use the services offered without any network configuration required.

Multicast applications such as Bonjour require special consideration when being deployed over wireless networks. Bonjour only works within a single broadcast domain, which is usually a small area. This is by design to prevent flooding a large network with multicast traffic. However, in some situations, a user may want to offer Bonjour services from one VLAN to another.

SmartZone provides two features for controlling how and where Bonjour services are available to clients:

- Bonjour Gateway on page 516: Bridge Bonjour services from one VLAN to another.
- Bonjour Fencing on page 518: Limit the range in physical space at which Bonjour services are available to clients.

Bonjour Gateway

Bonjour Gateway policies enable APs to provide Bonjour services across VLANs.

The controller's Bonjour gateway feature provides an mDNS proxy service configurable from the web interface to allow administrators to specify which types of Bonjour services can be accessed from/to which VLANs.

In order for the Bonjour Gateway to function, the following network configuration requirements must be met:

- The target networks must be segmented into VLANs.
- VLANs must be mapped to different SSIDs.
- The controller must be connected to a VLAN trunk port.

Additionally, if the VLANs to be bridged by the gateway are on separate subnets, the network has to be configured to route traffic between them.

Creating Bonjour Gateway Policies

A Bonjour Gateway policy must be created for an AP zone before the policy can be deployed to an AP or group of APs.

To create a Bonjour Gateway policy:

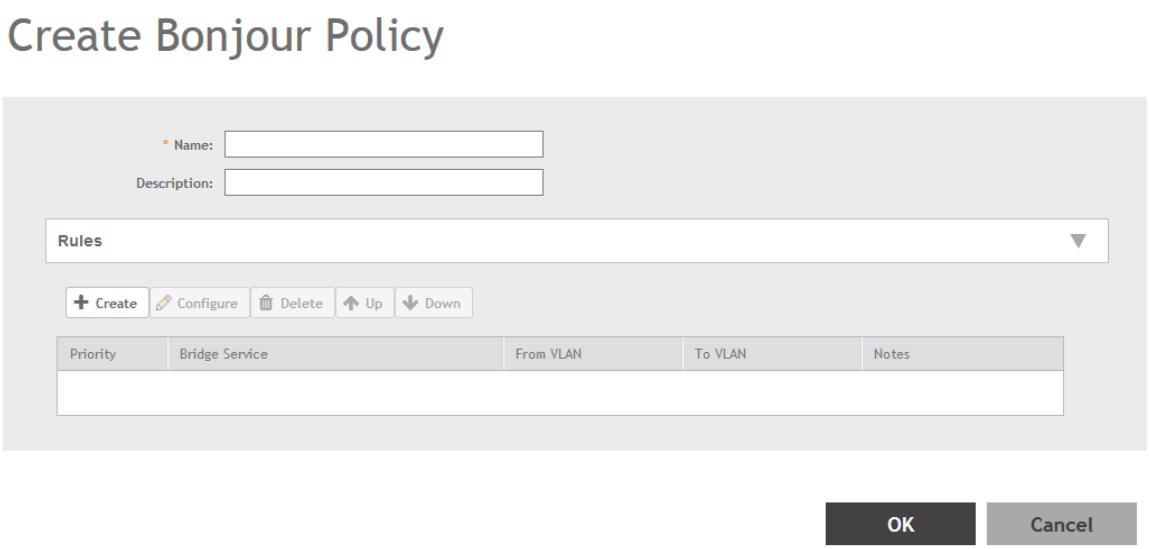
1. Go to **Services** > **Others** > **Bonjour** > **Gateway**.
2. Select the zone for which you want to create the policy.
3. Select the **Enable Bonjour gateway on the AP** option.

   Bonjour allows OS X and iOS devices to locate and use other devices such as printers, file servers and other clients on the same broadcast domain (within the same VLAN). Bonjour Gateway enables bridging mDNS service across VLANs.

4. Click **Create**.

   The **Create Bonjour Policy** page is displayed.

   FIGURE 296 Creating a Bonjour Gateway Policy



5. Configure the following:
   a. **Name**: Type a name for the policy.
   b. **Description**: Type a description for the policy.
   c. **Rules**: Create the policy rule by configuring the following
      1. Click **Create**. The **Create Bonjour Policy Rule** page appears.
      2. Configure the following options:
         - **Bridge Service**: Select the Bonjour service from the list.
         - **From VLAN**: Select the VLAN from which the Bonjour service will be advertised.
         - **To VLAN**: Select the VLAN to which the service should be made available.
         - **Notes**: Add optional notes for this rule.
      3. Click **OK**.

         You have created a Bonjour policy rule.
   d. Click **OK**.

You have created a Bonjour policy with a rule.

NOTE
You can also edit, clone and delete the policy by selecting the options **Configure**, **Clone** and **Delete** respectively, from the **Gateway** tab.

You may now continue to apply this Bonjour gateway policy to an AP or AP group, as described in Applying a Bonjour Gateway Policy to an Individual AP on page 518.

Applying a Bonjour Gateway Policy to an Individual AP

Once a Bonjour Gateway policy is created, you can select which AP will serve as the gateway for Bonjour services.

To apply a Bonjour Gateway policy to an AP:

1. Go to **Network** > **Wireless** > **Access Points**.
2. Select the AP that you want to configure from the zone in which the AP exists.
3. Click **Configure**.
4. Expand the **Advanced Options**, and in **Bonjour Gateway**, enable the check box next to **Enable as Bonjour Gateway with policy**, and select the policy you created from the drop-down list.
5. Click **OK** to save your changes.

Bonjour Fencing

Bonjour Fencing provides a mechanism to limit the scope of Bonjour (mDNS) service discovery in the physical/spatial domain.

While Bonjour Fencing is related to Bonjour Gateway, they are two separate features designed for different purposes. Bonjour Gateway bridges mDNS services across VLANs, and is useful because mDNS/Bonjour packets are restricted to the same VLAN/subnet and cannot be routed to other VLANs. Bonjour Fencing limits the range of Bonjour service discovery within physical space, which is useful because logical network boundaries (e.g. VLANs) do not always correlate well to physical boundaries within a building/floor.

The following considerations should be taken into account before deploying Bonjour fencing policies:

- Bonjour fencing is not supported on Mesh APs.
- Switch interfaces to which APs are connected must be configured in VLAN trunk mode so that Bonjour traffic gets forwarded across VLANs based on Bonjour Gateway Policies.
- Bonjour fencing is implemented at the AP, not at the controller.
- Fencing policies can be applied on a zone level only, and cannot be configured per AP group.
- In order for a wired fencing policy to work properly, wireless fencing for the same mDNS service should also be enabled. If wired fencing is enabled but wireless is disabled, APs that are not the "closest AP" will be unable to determine whether the source of the mDNS advertisement was wired or wireless.
- Bonjour fencing will work for local breakout scenarios, but will not work for tunnel based configuration. (This feature is supported only for SZ300 controllers)

  NOTE
  If hop 0 and hop 1 service records come in the same packet from a Bonjour server, AP will always give priority to hop 1 service record. Since tagging happens for hop1 service, hop 0 service can also be discovered by Bonjour clients.

Creating Bonjour Fencing Policies

Bonjour Fencing policies can be created and applied to a zone at the same time using the Fencing tab on the **Services and Profiles > Bonjour** screen.

NOTE
Bonjour Fencing for a particular service does not work if another service from same server which is not fenced is enabled simultaneously.

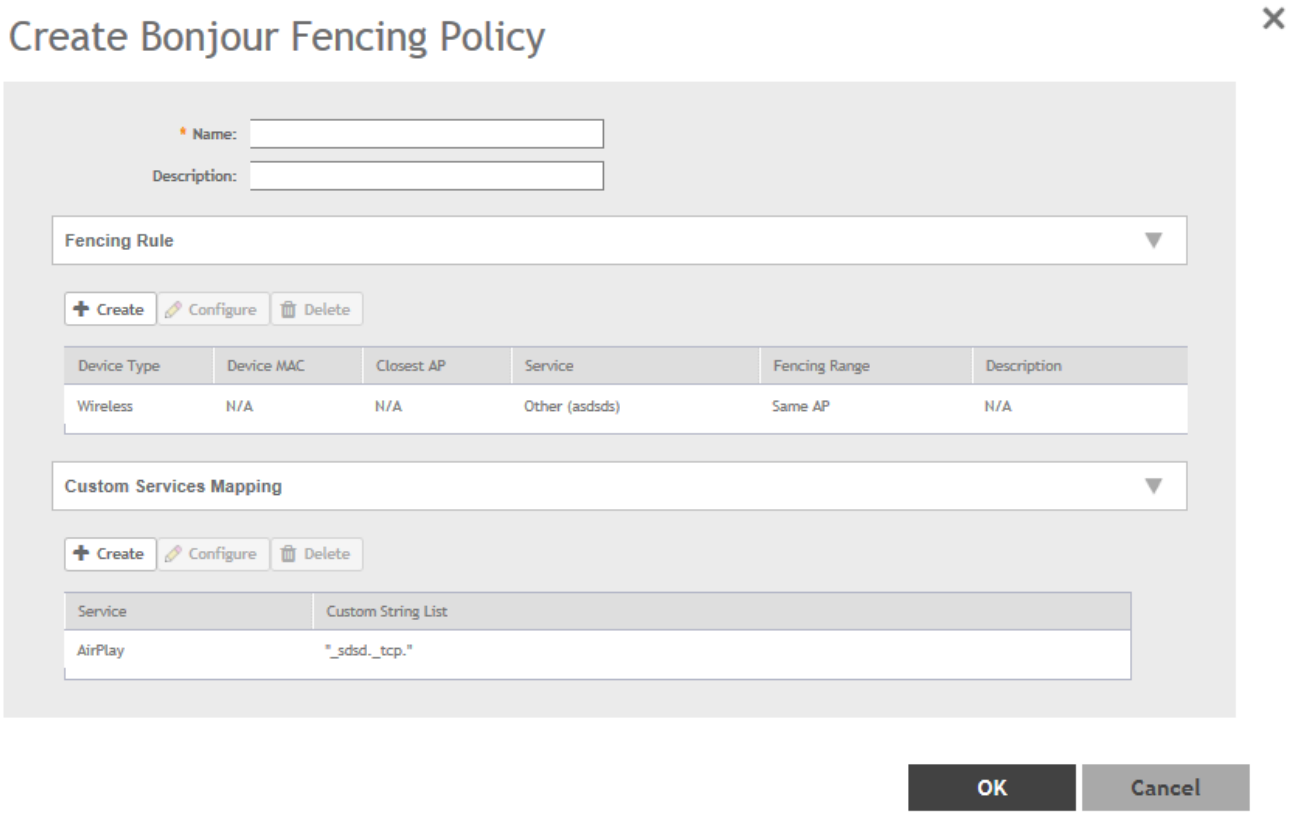
To create a Bonjour Fencing policy:

1. Go to **Services** > **Others** > **Bonjour** > **Fencing**.
2. Select the zone for which you want to create the policy.

3. Click **Create**.

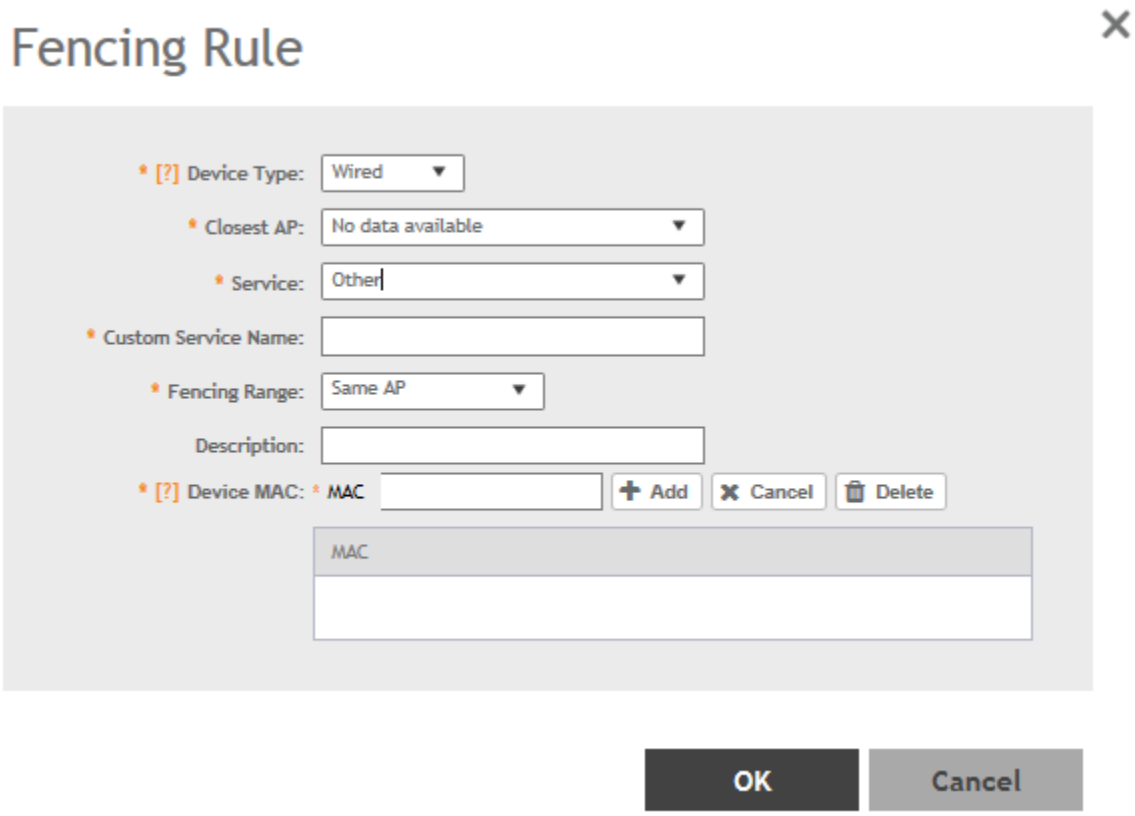
   The **Create Bonjour Fencing Policy** page appears.

FIGURE 297 Creating a Bonjour Fencing Policy



4. Configure the following:
   a. **Name**: Type a name for the policy.
   b. **Description**: Type a description for the policy.
   c. **Fencing Rule**: Create the policy rule by configuring the following:

FIGURE 298 Fencing Rule



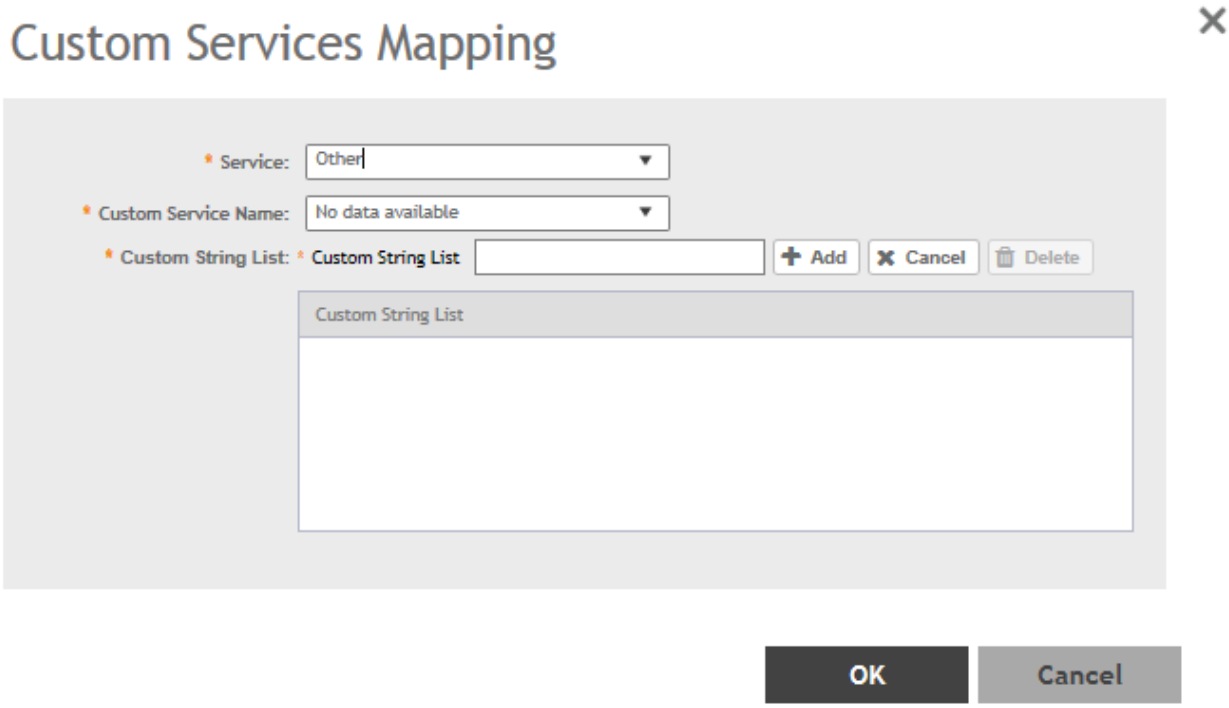
1. Click **Create**. The **Fencing Rule** page appears.
2. Configure the following options:
   - **Device Type**: Select the Wireless or Wired network connection method for the device advertising bonjour services.
   - **Closest AP**: Select the closest AP to create a physical anchor point for fencing, and the closest AP is auto-detected for wireless devices, based on the AP association.
   - **Service**: Select one of the bonjour services from the drop-down list. In 5.0, two new services, **Chromecast** and **Other** are added. Chromecast behaves as the standard service. If you select **Other**, the **Custom Service Name** appears which is used for service mapping. Regardless of the device type selected only three services for Other option.
   - **Custom Service Name**: For mapping services other than the custom services regardless of the Device Type. You can create a maximum of three service with the same custom service name.
   - **Fencing Range**: Select the fencing range to be the Same AP or 1-Hop AP Neighbors.
   - **Description**: Specify any notes you may need to refer.
   - **Device MAC**: Specify the MAC address of the device advertising bonjour services. This option is available only for Wired Device Type. It supports up to four wired MAC addresses.

3. Click **OK** to save the rule.

   You have created a Bonjour fencing rule. Each policy can contain up to 32 rules.

d. **Custom Services Mapping**: Create services mapping by configuring the following:

FIGURE 299 Create Custom Services Mapping



1. Click **Create**. The **Custom Services Mapping** page appears.
2. Configure the following options:
   - **Service**: Select one of the Bonjour services from the drop-down list.

     Per Service, has only one entry for Custom Services Mapping. For example: AppleTV and Chromecast, have only one entry with custom strings (three at most) and Other type has one entry with custom strings (three at most) because it allows three Other rules.
   - **Custom Service Name**: Lists all **Custom Service Name** with Service type **Other** created in the Fencing Rule. This field is available if you select the **Other** option from the **Service** drop-down.
   - **Custom String List**: Enter the name in the format **_xxxx._xtcp** or **_xxxx._xudp**. You can create only one entry for Custom service and three entries for other service.
3. Click **OK** to save the services mapping policy.

   You have created a Custom Services Mapping policy.

e. Click **OK** to save the policy.

You have created a Bonjour fencing policy.

NOTE
You can also edit or delete the policy by selecting the options **Configure** or **Delete** respectively, from the **Fencing** tab.

3rd Party Service

SZ supports integration for Ekahau and Aeroscout/Stanley tags and information is forwarded to the Ekahau and Aeroscout servers respectively. This enhancement provides support for Real-Time Location Service (RTLS) tags without requiring them to be associated to the network.

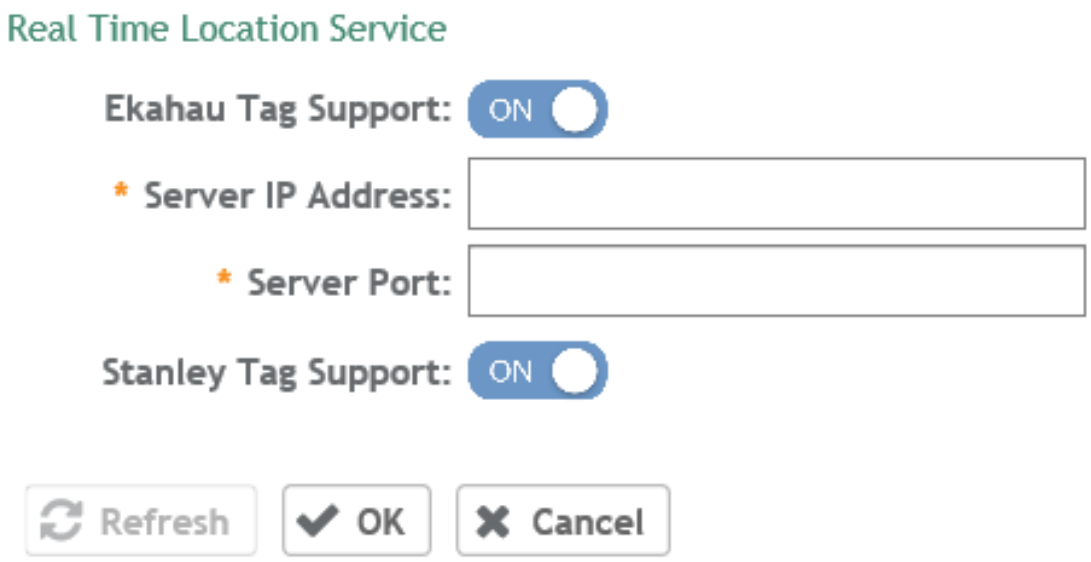
Enabling Ekahau and Aeroscout/Stanley RTLS Tags

To locate tag positions, SZ allows you to enable Ekahau and Aeroscout/Stanley RTLS tags.

1. Select **Services** > **Others** > **3rd Party Service** > **RTLS**.

   The **RTLS** page is displayed.

   FIGURE 300 Enabling Ekahau and Aeroscout/Stanley Tag Support



2. Select a zone to enable the tags.
3. To enable **Ekahau Tag Support**, set **Ekahau Tag Support** to **ON**.
4. In the **Server IP Address** field, enter the IP address of the server to which data is forwarded.
5. In the **Server Port** field, enter the server port to which data is forwarded.
6. To enable **Stanley Tag Support**, set **Stanley Tag Support** to **ON**.
7. Click **OK**.

Vendor-Specific Attribute (VSA) Profile

The SmartZone UI provides the VSA profile, where the user can define VSAs to be included in authentication and accounting messages. The AP receives the configuration from the Change and Configuration Management (CCM) and appends the VSAs to each user equipment (UE) authentication and accounting request and forwards the requests to the AAA server.

For HotSpot WISPr, the UE authentication is handled by the northbound Interface (NBI) where Real Application Clusters (RAC) appends the VSAs to the authentication messages and the AP appends the VSAs to the accounting messages.

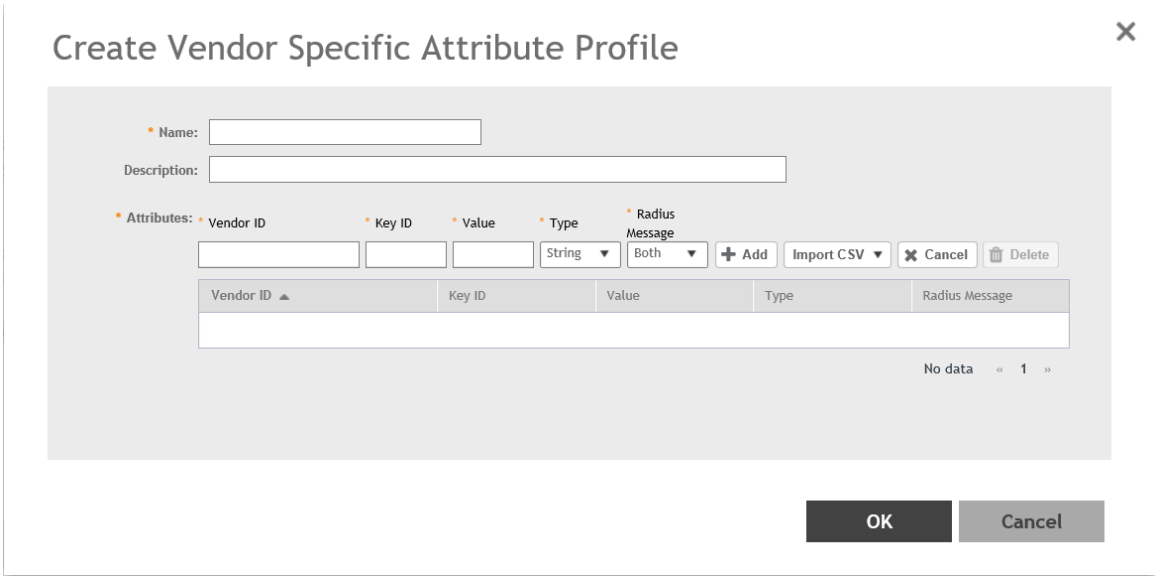
Creating a Vendor-Specific Attribute Profile

Perform the following procedure to add the VSAs in the RADIUS authentication and accounting messages.

1. Select **Services** > **Others** > **Vendor Specific Attribute**.
2. From the **Vendor Specific Attributes Profile** page, select the zone for which you want to create a VSA profile. and click **Create**.

   The **Create Vendor Specific Attribute Profile** page is displayed.

   FIGURE 301 Creating a Vendor-Specific Attribute Profile



3. Enter the profile name and description.

4. Under **Attributes**, define the VSA profile by completing the following steps:
   a) In the **Vendor ID** field, enter an integer from 1 through 65536.

      NOTE
      Do not configure the vendor IDs 25053 (Ruckus) and 14122 (WISPr) because they are reserved for internal use only. If you try to configure these vendor IDs, the system throws an error message.

   b) In the **Key ID** field, enter an integer from 0 through 255.
   c) In the **Value** field, enter an integer or string depending on the **Type** selected.

      NOTE
      The integer range is from 0 through 2147483647. The maximum length of a string is 247 characters.

   d) In the **Type** list, select from the following options:
      - **Integer**
      - **String**
   e) In the **Radius Message** list, select from the following options:
      - **Accounting**: The attributes defined in the VSA profile are included in the accounting messages.
      - **Authentication**: The attributes defined in the VSA profile are included in the authentication messages.
      - **Both**: The attributes defined in the VSA profile are included in both the accounting and authentication messages.
5. Click **Add** to add the VSA profile or click **Import CSV** to upload a CSV file containing multiple VSA profiles.

   NOTE
   To download a CSV template, click the **Import CSV** arrow and select **Download a CSV Sample**.

   The VSA profiles are added to the **Attributes** table. Check the VSA information in the **Attributes** table for any modifications.

   NOTE
   You can edit the VSAs by clicking the **Vendor ID** in the **Attributes** table.

   NOTE
   A maximum of 32 VSAs can be added to a VSA profile. A maximum of 4 VSA profiles can be configured for a zone.

6. Click **OK** to update the VSA profile to the database.

NOTE
To edit a VSA profile, select a VSA profile and click **Configure** in the **Vendor Specific Attribute Profile** page.

NOTE
To associate a VSA profile to a WLAN, refer to Associating a VSA Profile to a WLAN Configuration on page 525.

NOTE
You can also configure a VSA profile in the zone and WLAN templates. For more information, refer to *Working with Zone Templates* and *Working with WLAN Templates* respectively .

Associating a VSA Profile to a WLAN Configuration

Perform the following procedure to associate a VSA profile to a WLAN configuration.

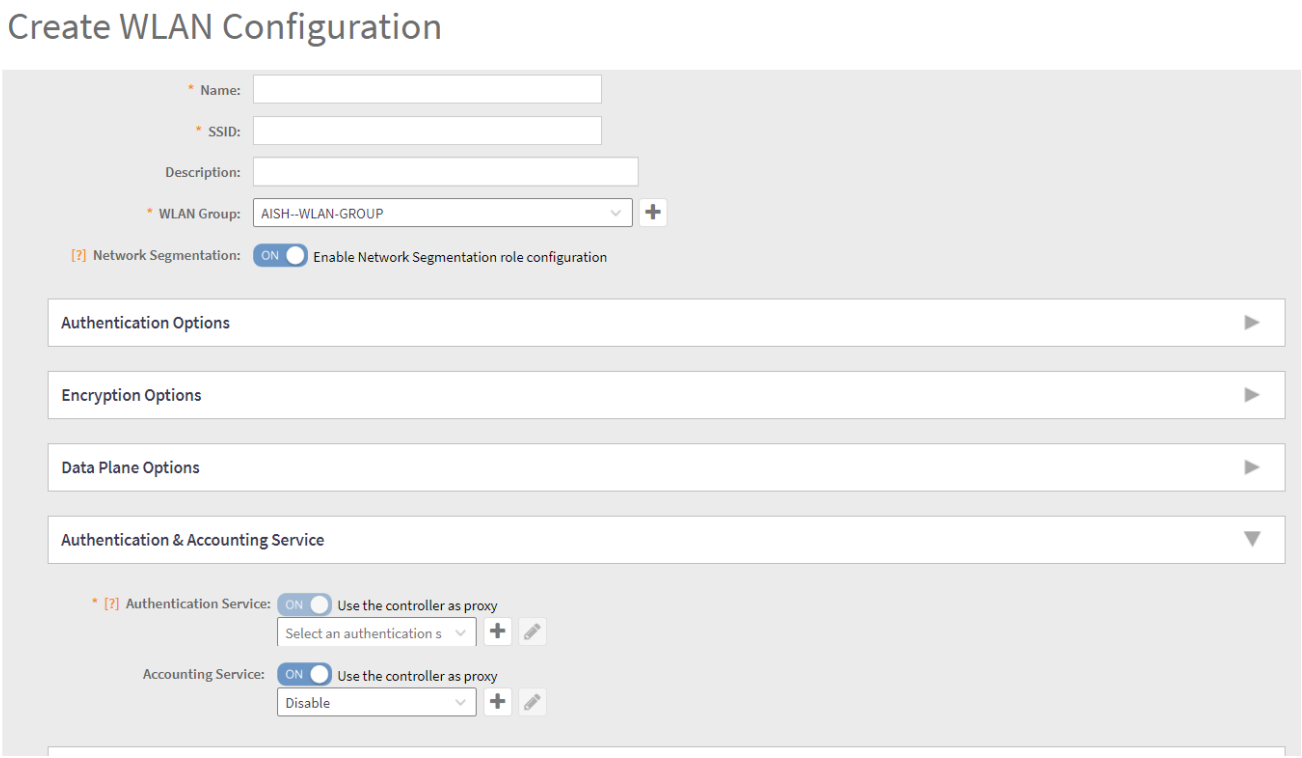
1. On the main menu, click **Network** > **Wireless LANs**.

   The **Wireless LANs** page is displayed.

2. Select the zone where the VSA profiles are created and click **Create**.

   The **Create WLAN Configuration** page is displayed.

   FIGURE 302 Creating a WLAN Configuration



3. Under **General Options**, enter the WLAN name and SSID.
4. Under **Authentication and Accounting Service**, complete the following steps:select the authentication service profile.
   a) Under **Authentication Service**, click **Use the controller as proxy** and select the authentication service profile.
   b) Under **Accounting Service**, click **Use the controller as proxy** and select the accounting service profile.
5. Under **Radius Options**, click **Vendor Specific Attribute Profile** and select a VSA profile.

   NOTE
   By default, **Vendor Specific Attribute Profile** is disabled.

   NOTE
   Click  to configure the VSA profile.

6. Under **Advanced Options**, in **Access VLAN**, enter the VLAN ID.

   NOTE
   Enter an integer from 2 through 4094 for **VLAN ID**.

7. Click **OK**.

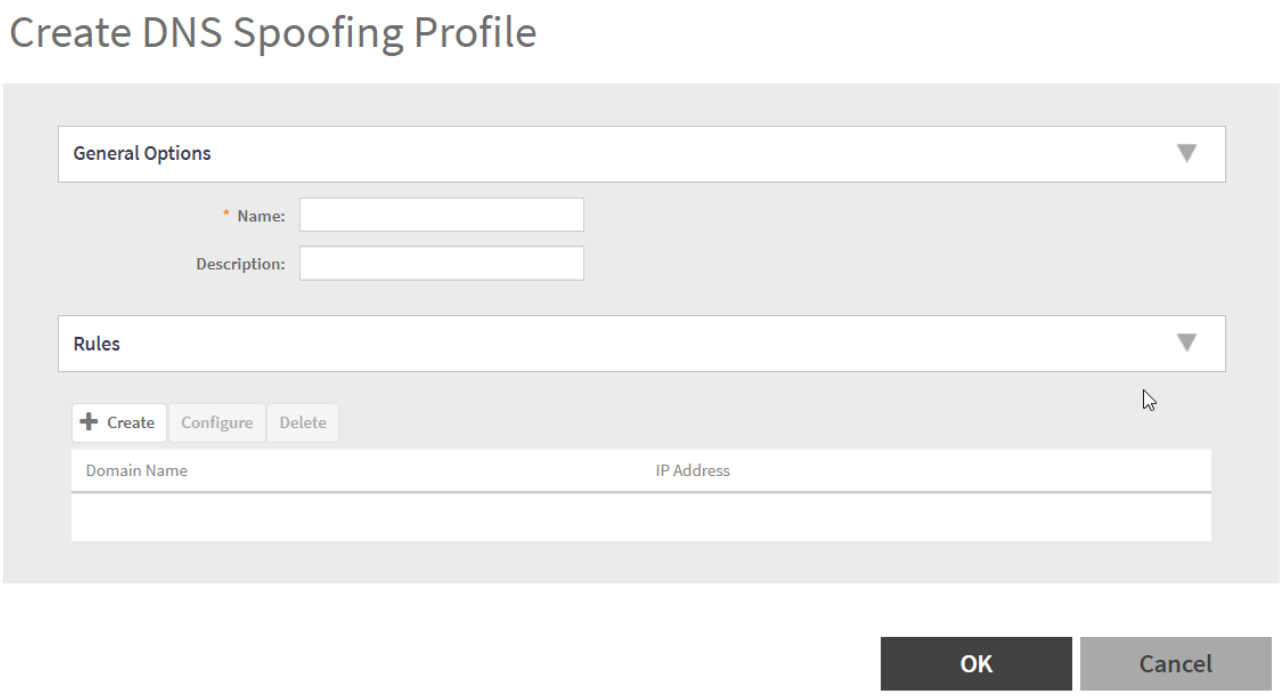
   NOTE
   The WLAN configuration is shown in the **Access Points** page for the zone where VSA profiles are created.

Creating a DNS Spoofing Profile

By creating a DNS spoofing profile, you can specify the IPv4 or IPv6 address of the DNS server. The AP then transmits the data packets to the DNS server.

1. Go to **Services** > **Others** > **DNS Spoofing**
2. Select the zone for which you want to create profile.
3. Click **Create**.
   The **Create DNS Spoofing Profile** page is displayed.

   FIGURE 303 Creating DNS Spoofing Profile



4. Configure the following:
   a) Name: Enter a name for the DNS spoofing profile.
   b) Description: Enter a short description for the profile.
   c) Click **Create**, and the **Create Rules** dialog box is displayed.
   d) In the **Domain Name** field, enter the domain name of the DNS server.
   e) In the **IP Adress** field, enter the IPv4 or IPv6 of the DNS server and click **Add**. If the user sends DNS request with the domain name configured in the DNS Spoofing profile, then the AP responds with the IP address configured in the DNS Spoofing profile for the requested domain name.
   f) Click **OK** to confirm the rules.
   g) Click **OK** to confirm the creation of DNS spoofing profile.

NOTE
You can also edit, clone or delete the profile by selecting the options **Configure**, **Clone** or **Delete** respectively, from the **DNS Spoofing** tab.

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 108 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.

TABLE 108 SNMP v2 Agent Settings (continued)

Field	Description	Your Action
Privilege	Indicates the privileges granted to this community.	Select the required privileges: • **Read-Only**—Privilege only to read. • **Read-Write**—Privilege only to read and write. • **Notification**—Privilege to: – **Trap**—Choose this option to send SNMP trap notification. – **Inform**—Choose this option to send SNMP notification. 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 follwoing table.

TABLE 109 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 109 SNMPv3 Agent Settings (continued)

Field	Description	Your Action
Authentication	Indicates the authentication method.	Choose the required option: • **SHA**—Secure Hash Algorithm, message hash function with 160-bit output. a. Enter the **Auth Pass Phrase**. b. Choose the **Privacy** option. – **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. a. Enter the **Auth Pass Phrase**. b. Choose the **Privacy** option. – **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.	Select the required privileges: • **Read-Only**—Privilege only to read. • **Read-Write**—Privilege only to read and write. • **Notification**—Privilege to: – **Trap**—Choose this option to send SNMP trap notification. – **Inform**—Choose this option to send SNMP notification. 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**.

AP SNMP Agent Profile

Simple Network Management Protocol (SNMP) is one of the widely accepted protocols to manage and monitor network devices. The SNMP agent is a program that is packaged within the network element. These agents are enabled and configured in Zone/AP Group/AP for communicating with the network management system.

AP SNMP Agent Profile can be created, enabled and configured in two ways as described in the below sections.

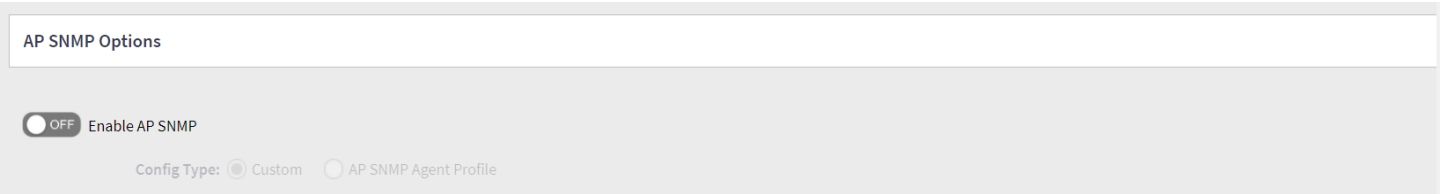
NOTE
AP SNMP Agent Profile can be created, enabled and configured directly through **Services** > **Others** > **AP SNMP Agent Profile** and follow steps from the section **Config Type - Custom**

NOTE
To create, enable and configure and AP SNMP Agent Profile through Zone APs **Network** > **Access Points** as described in the below steps.

To enable SNMP options via Zone APs through controller interface, perform the following steps:

1. Click **Network** tab, under wireless select **Access Points** .
2. Click **+**. This displays **Create Domain** page.
3. In the **Create Domain**, select **Type** as **Zone**. This displays **Create Zone** page.
4. Scroll down to **AP SNMP Options** menu. By default, the **Enable AP SNMP** radio button is disabled.
5. Click **Enable AP SNMP** radio button to enable **AP SNMP Options**. This displays **Config Type** options **CustomAP SNMP Agent Profile**.

FIGURE 304 Enabling AP SNMP Options for Zone AP



Config Type - Custom

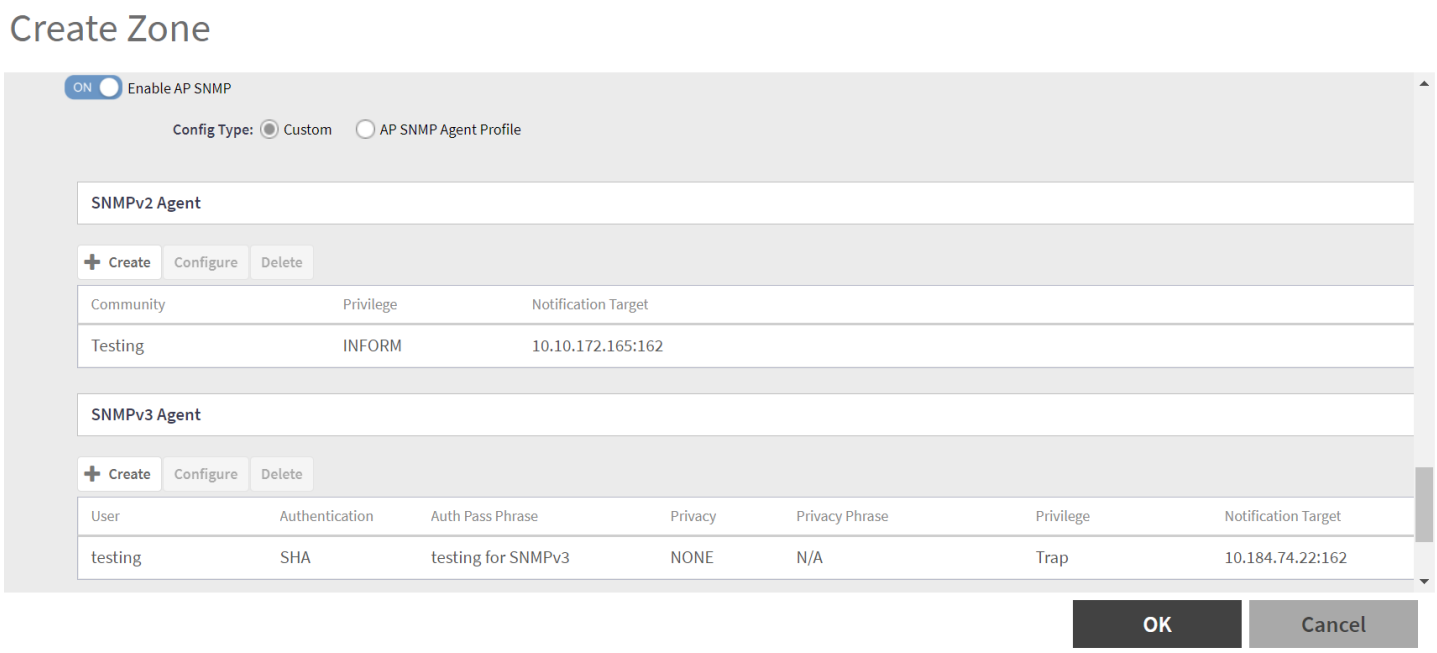
After enabling the AP SNMP radio button, **Config Type** option is highlighted and by default **Custom** type is selected. In the **Custom** config type, user can create/configure/delete **SNMPv2 Agent** and **SNMPv3 Agent**.
SNMPv2 Agent

1. To create **SNMPv2 Agent**, click **Create** in **SNMPv2 Agent** section. This displays **Create SNMPv2 Agent** page. In the create SNMPv2 Agent page, enter **Community** name and choose the **Privilege** type by selecting the check box options -
   - Read-Only
   - Read-Write
   - Notification - Enter the **Target IP** and **Target Port** details and click **Add**. Select if the notification is a **Trap** or **Inform**.
2. Click **OK**. The new SNMPv2 agent details is displayed in the **SNMPv2 Agent** section.

SNMPv3 Agent

1. To Create **SNMPv3 Agent**, click **Create** in **SNMPv3 Agent** section. This displays **Create SNMPv3 Agent** page. This displays **Create SNMPv3 Agent** page. In the **Create SNMPv3 Agent** page, enter name, select **Authentication** options **SHA** or **MD5**, enter **Auth Pass Pharse**, select **Privacy** options **None**, **DES** or **AES** and choose the **Privilege** type by selecting the check box options -
   - Read-Only
   - Read-Write
   - Notification - Enter the **Target IP** and **Target Port** details and click **Add**. Select if the notification is a **Trap** or **Inform**.
2. Click **OK**. The new SNMPv3 agent details is displayed in the **SNMPv3 Agent** section.

FIGURE 305 Enable AP SNMP Options - Custom

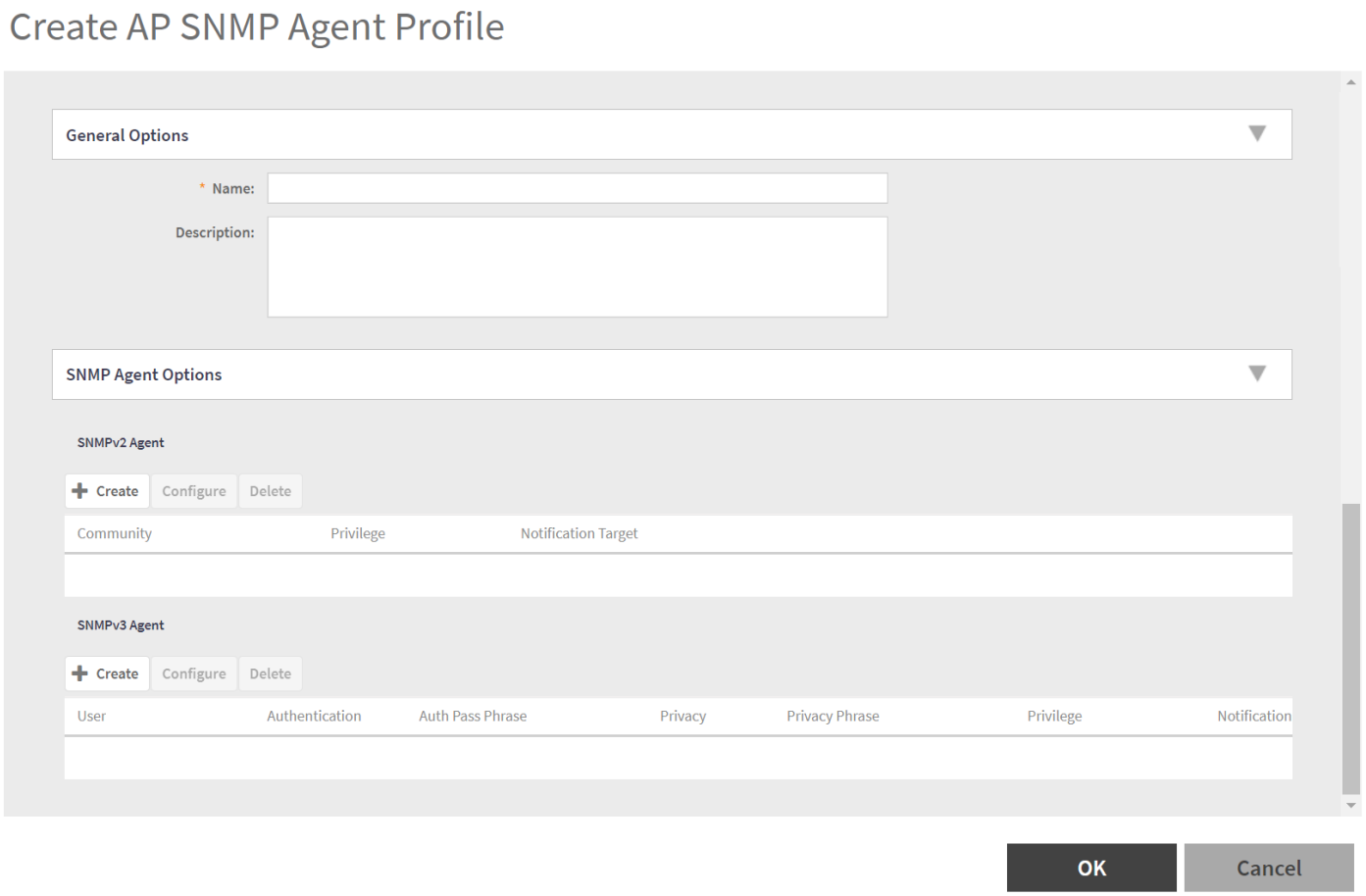


Config Type - AP SNMP Agent Profile

After enabling the AP SNMP radio button, **Config Type** option is highlighted. Select config type **AP SNMP Agent Profile**. This displays **AP SNMP Agent ProfileAdd (+)** and **Edit** button.

1. To create **AP SNMP Agent Profile**, click **Add (+)**. This displays **Create AP SNMP Agent Profile**.
2. **General Options** - Enter the **Name** and **Description** for **AP SNMP Agent Profile**.
3. **SNMP Agent Options** - User can create/configure/delete **SNMPv2 Agent** and **SNMPv3 Agent** as described in the **Config Type - Custom**section.

FIGURE 306 Enable AP SNMP Agent Profile



Creating an External Syslog Server Profile

The MSPs (Managed Service Provider) can set the external syslog servers one by one. This feature extracts the external syslog server setting as a profile. These profiles will be regulated by the MSP framework. The customers can then select the partner's domain-level profile while setting up a zone or an AP to send the syslog data to the syslog server on the network.

NOTE
This feature is supported only on vSZ-H.

NOTE
A maximum of 16 profiles can be created per partner domain.

To create an external syslog server profile:

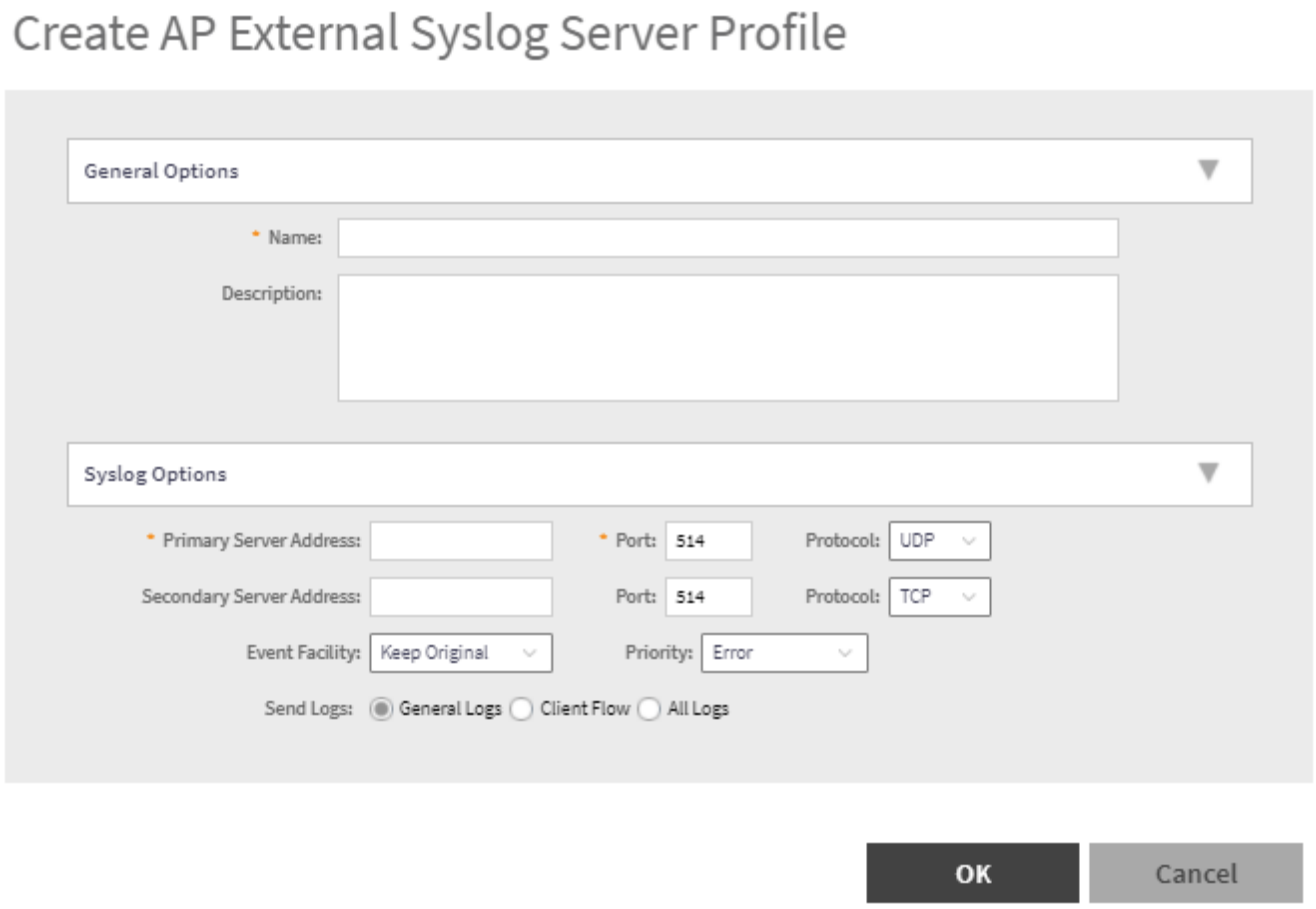
1. Select **Services** > **Others** > **AP External Syslog Server**.

   The **AP External Syslog Server Profile** page is displayed.

2. Click the **Create**.

   The **Create AP External Syslog Server Profile** page is displayed.

FIGURE 307 Creating AP External Syslog Server Profile



3. Configure the following:
   - Name: Enter a name for the profile you want to create.
   - Description: Enter a short description for the profile.
   - Primary Server Address: Enter the primary server IP address to send the syslog messages.
     - Port: Enter the server port to which the messages must be forwarded.
     - Protocol: Select the protocol.
   - Secondary Server Address: Enter the secondary server IP address to send the syslog messages if the primary server goes down.
     - Port: Enter the server port to which the messages must be forwarded.
     - Protocol: Select the protocol.
   - Event Facility: Select the facility level that will be used by the syslog message. Options include: Keep Original, Local0 (default), Local1, Local2, Local3, Local4, Local5, Local6, and Local7.
   - Priority: Select the lowest priority level for which events will be sent to the syslog server. For example, to only receive syslog messages for events with the warning (and higher) priority, select **Warning**. To receive syslog messages for all events, select **All**.
   - Send logs: Choose to send the General Logs, Client Logs or All Logs
4. Click **OK**.

Administration

- System 535
- External Services 572
- Administration 587
- Help 657

System

System Info

Viewing System Settings

You can view the system information such as the controller version, firmware version, license information, control and data plane details from the **General Settings** tab.

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

- Controller Version
- Control Plane Software Version
- Data Plane Software Version
- AP Firmware Version (hover over the field to see the firmware type)
- Cluster Name
- Number of Planes
- System Name
- System Uptime
- Serial Number
- System Capacity of Cluster
- 3GPP Tunneling License
- AP Capacity License
- AP Direct Tunnel License
- Data Plane Capacity License

FIGURE 308 General Settings - SZ300

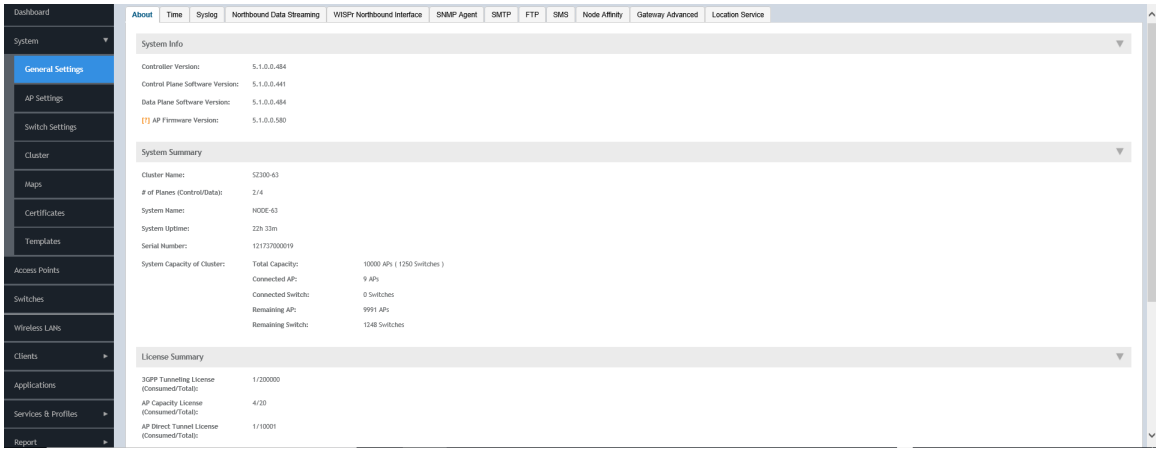
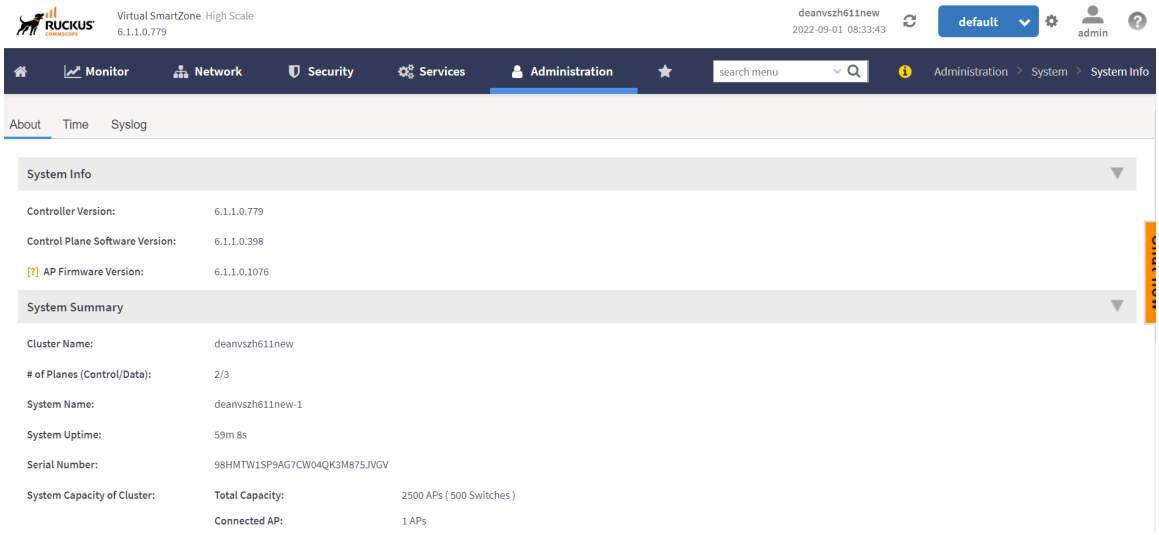


FIGURE 309 General Settings - vSZ-H



NOTE
For the SZ300 and vSZ-H platforms, the AP to switch ratio is 5:1. For more details, refer to *SmartZone Upgrade Guide* and *Virtual SmartZone Getting Started Guide*.

Configuring Advanced Gateway Options

You can configure advanced gateway options. This feature no longer depend on flat file changes.

To configure advanced gateway options:

1. Go to **Administrator** > **External Services** > **Advanced Gateway (GTP)**.
2. Configure the following options:
   - **GTP Network Service Access Point Identifier [NSAPI]**—Selects NSAPI for GTP message. The default setting is **1**.
   - **Include IMEI IE in GTP Messages**—Enables or disables IMEI IE in GTP messages. The default setting is **No**.

NOTE
In IMEI IE, the controller will send the MAC address of the UE appended with FFFE.

- **Include ECGI in GTPV2 Messages**—Used only when the S5/S8 interface is used for GTPv2:
- **Include TAI in GTPV2 Messages**—Used only when the S5/S8 interface is used for GTPv2.
- **GTPv2 Interface Type**—Choose the interface type. S2a or S5_S8.

  NOTE
  The default GTPv2 interface for the controller is S2a.

- **Include SCG-RAI in GTPV2 Messages**—Enables or disables SCG-RAI in GTPV2 messages. The default setting is **No**.
- **Include SCG-SAI in GTPV2 Messages**—Enables or disables SCG-SAI in GTPV2 messages. The default setting is **No**.

3. Click **OK**.

Configuring Node Affinity

Node affinity enables administrators to manually configure the controller nodes to which APs will connect.

To do this, set the order of preferred nodes on the node affinity page. Node affinity is implemented at the AP zone level, which means that all APs that belong to a zone will have the same node affinity settings.

If you want APs that belong to the same zone to connect to the same node whenever possible, you can configure set the preferred node for a particular zone.

NOTE
An affinity profile defines the order of the nodes to which APs that belong to the same zone will connect.

NOTE
Node affinity profile works only if it is restored in the same cluster. If the configuration must be restored to a different cluster, disable node affinity and remove the node affinity profiles containing nodes that are not available in the new cluster.

NOTE
Node affinity is not supported on the vSZ-H and vSZ-D platforms.

Enabling Node Affinity

To enable and configure node affinity:

1. Go to **System** > **General Settings** > **Node Affinity**.
2. Select **Enable Node Affinity**. Node Affinity Profile appears.
3. To:
   - Create an new profile:
     a. Click **Create**, the Create Node Affinity Profile form appears.
     b. Enter a **Name** and **Description**.
     c. In the **Node Order** list, select the node and click **Up** or **Down** to position the node in the required order.
     d. Click **OK**.
   - Edit the default profile:
     a. Select the profile from the list and click **Configure**. The Edit Node Affinity Profile form appears.
     b. Edit the **Name** and **Description**.
     c. In the **Node Order** list, select the node and click **Up** or **Down** to position the node in the required order.
     d. Click **OK**.

NOTE
When you enable node affinity, disable cluster redundancy.

4. To set the number of times an AP will attempt to connect to the preferred node, enter the **# of Node Retry for Preferred Node**.

   The default value is 3 and the accepted range is 1 to 10. If the AP is unable to connect to the preferred node, it will attempt to connect to the node that is next in the order of node priority.

5. In the **Zone Assignment** section, set the node affinity profile that you want each zone to use. Select the Zone from the list and click **Assign Profile**. The Assign Node Affinity Profile to Selected Zones form appears.
6. Select the **Node Affinity Profile** from the drop-down and click **OK**.
7. Click **OK**.

Disabling Node Affinity

Follow these steps to disable node affinity:

1. From **System** > **General Settings** > **Node Affinity**.
2. Clear the **Enable Node Affinity** check box.
3. Click **OK**. You have disabled node affinity.

Working with Maps

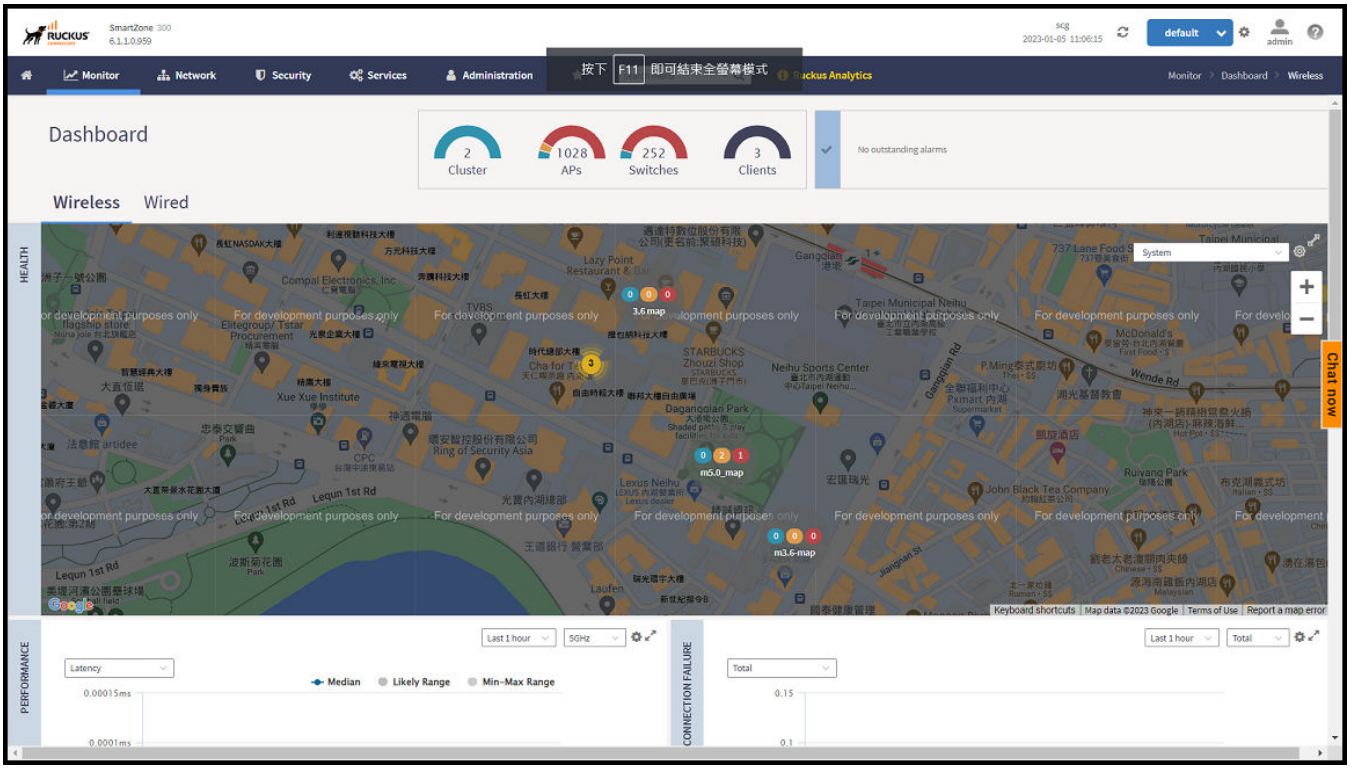
Importing floorplan maps into SmartZone allows you to further customize the information displayed on the Dashboard and Access Points pages, and monitor your APs, zones, groups, clients and traffic statistics all within the world map view on the Dashboard.

Additionally, you can use the maps to quickly locate more specific information on a venue or zone, and drag and drop APs onto the floor plan map to represent their locations in physical space in your venue.

Once a map is imported and GPS coordinates are entered, an icon representing the venue appears on the world map on the Dashboard. The icon displays the current number of APs (Online, Flagged and Offline). You can hover over the icon for more information.

Double-click the map icon or click **Zoom into this map** to view the imported map in the Dashboard.

FIGURE 310 Imported Maps on the Dashboard



Importing a Floorplan Map

The controller provides a user-friendly workflow for importing a map of your venue floorplan, placing APs in their respective physical locations on the map, and scaling the map to match the actual dimensions of your venue.

Floorplan maps allow you to view site/venue/floor-specific details such as:

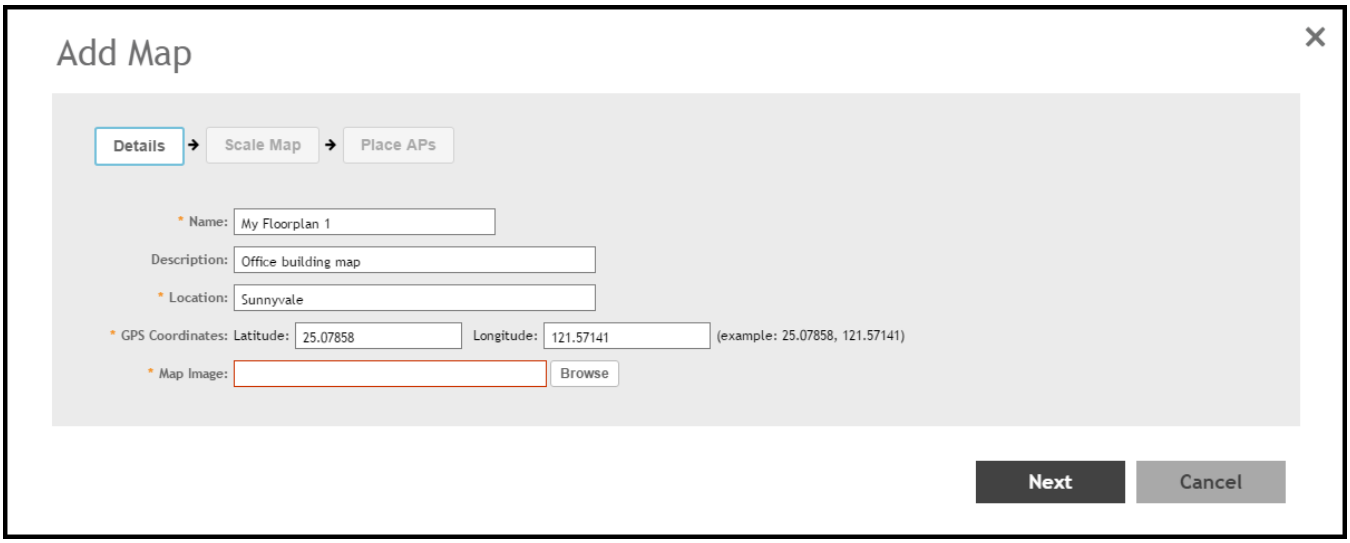
- AP status, performance, and health conditions
- Client connections to an AP
- Location-specific trouble spots related to AP or client connectivity

To import a floorplan map:

1. Go to **Network** > **Wireless** > **Maps**.
2. From the System tree hierarchy, select the location where you want to create a map and click the **Add** icon button. The **Add Map** form appears.
3. On the **Details** tab, enter a **Name** and optionally a **Description** to identify the map.
4. Enter a **Location** for the map. Alternatively, you can choose the location from the auto-completion options. After you select the location, the GPS Coordinates are automatically updated.

5. For **GPS Coordinates**, you can enter the **Latitude** and **Longitude** values.

   FIGURE 311 Creating the Add Map form



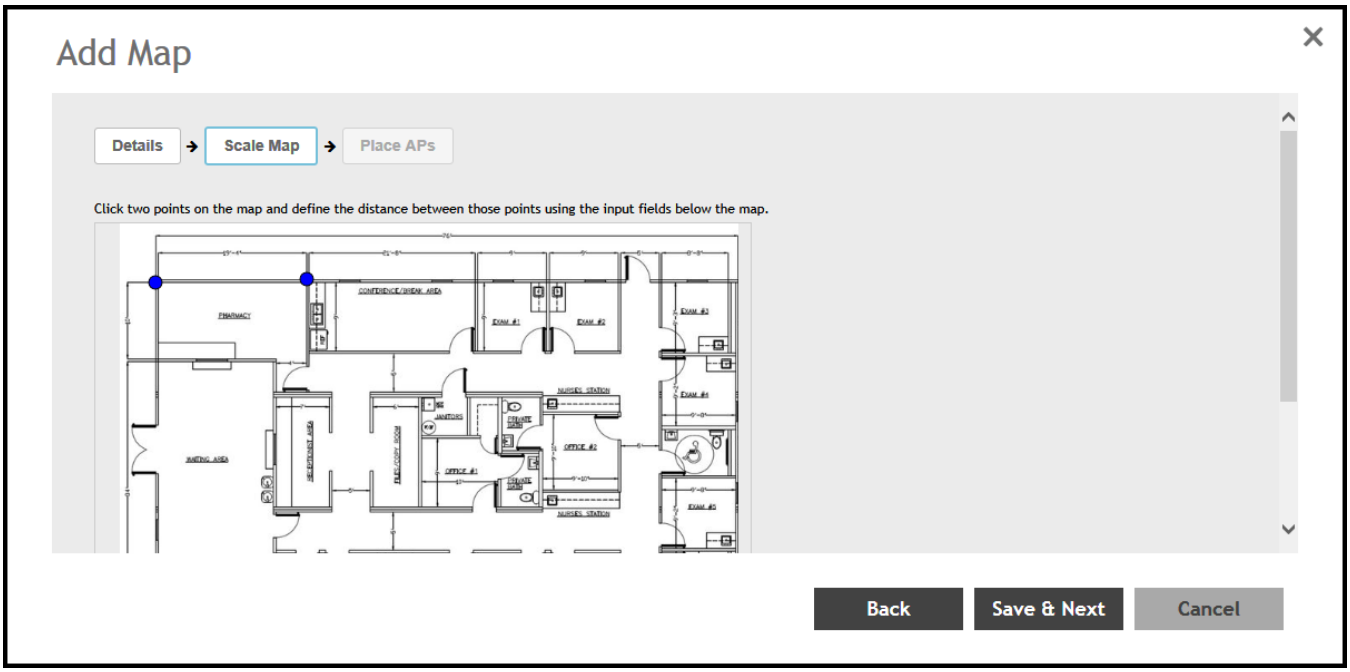
6. To add a **Map Image**, click **Browse** and select a site, venue, or floor map in jpg, jpeg, png, bmp or svg file formats.

   NOTE
   The maximum file size per indoor map is 5MB.

7. Click **Next**, the **Scale Map** tab is displayed.

8. Click two points on the map between which you know the distance. Blue dots appear to show the points you selected.

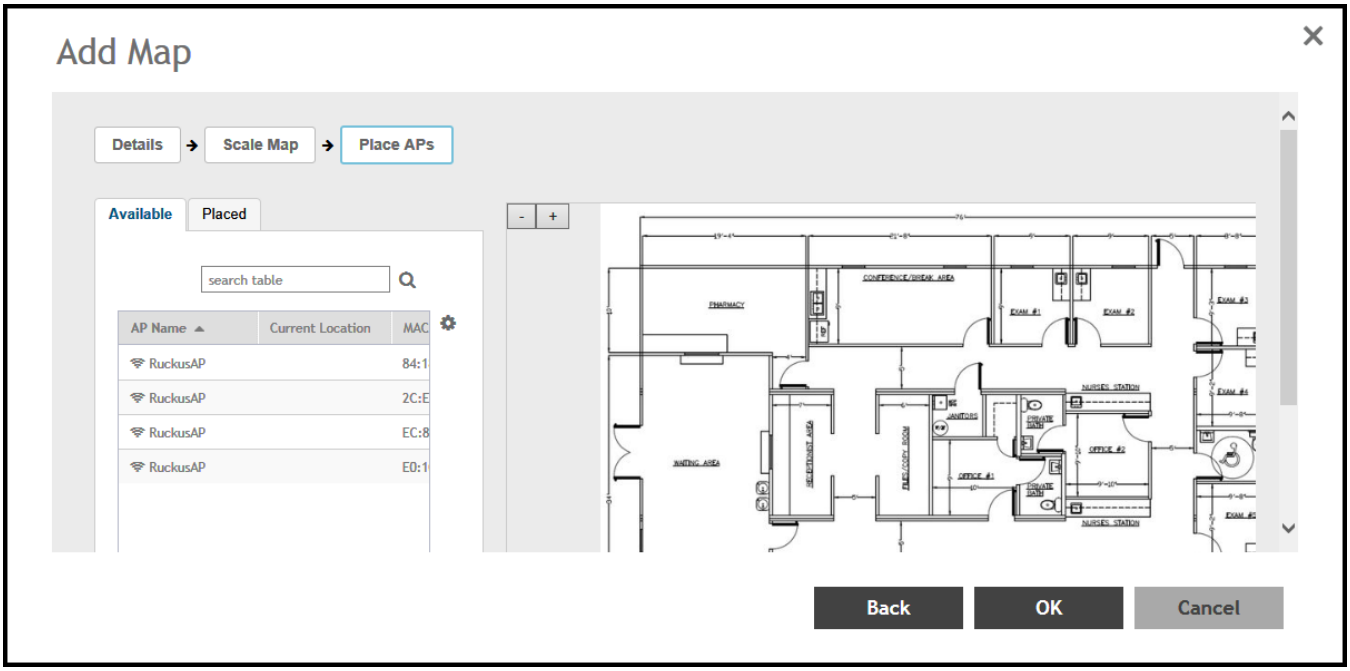
FIGURE 312 Indicating the Selected Points on the Map



9. Enter the **Physical Distance** between the two points and select the unit of measurement (mm, cm, m, ft, yard).
10. Click **Save & Next**. The **Place APs** tab appears.

11. From the **Available** list, drag the APs and place them in their physical locations on the map. Click the **Placed** tab to see the list of placed APs.

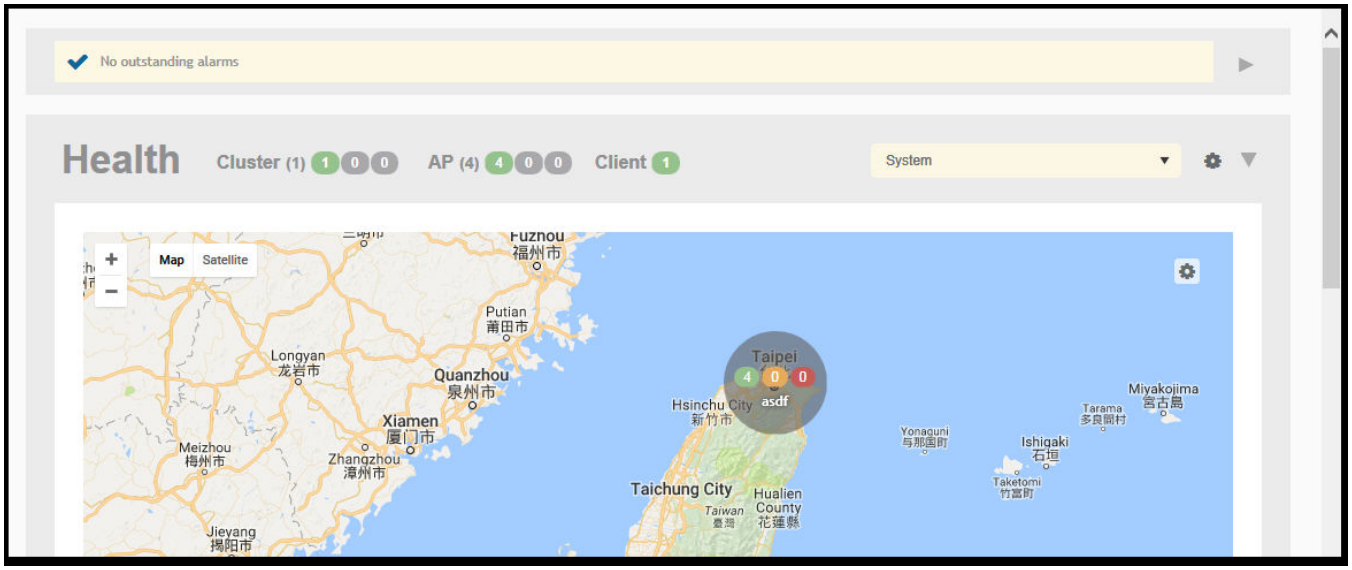
    FIGURE 313 Dragging and dripping to place APs on the Floorplan



12. Once you are happy with the placement of your APs on the map, click **OK** to save your map.

Your venue now appears as an icon on the world map on the Dashboard, located at your venue's actual physical location (if you entered the GPS coordinates correctly). The Dashboard icon that represents your venue provides an overview of the number of APs in the venue and their status. Hover over the icon to view more details, or click one of the links to zoom in to the venue floorplan map you imported.

FIGURE 314 Importing Venue Map Icon



NOTE
You can also edit or delete a map. To do so, select the map from the list and click the **Edit** or **Delete** icons respectively.

Viewing RF Signal Strength

Radio Frequency (RF) signal strength can be viewed using a heat map for a specific location.

The heat map helps us identify the RF signal strength in a specific location. It provides heat maps using actual path loss information from the environment. You can view an indoor floor plan map for an AP.

To view the RF signal strength:

1. Go to **Network** > **Wireless** > **Maps**.
2. From the System tree hierarchy, select the location of the map that you want to view.
3. Select the **Show Signal Coverage** check box and choose the required RF frequency. For example, 2.4 GHz or 5 GHz. The heat map is displayed with a color-gradient legend. High signal strength appears in red. The color changes as the signal strength reduces.

FIGURE 315 RF Coverage Heat Map

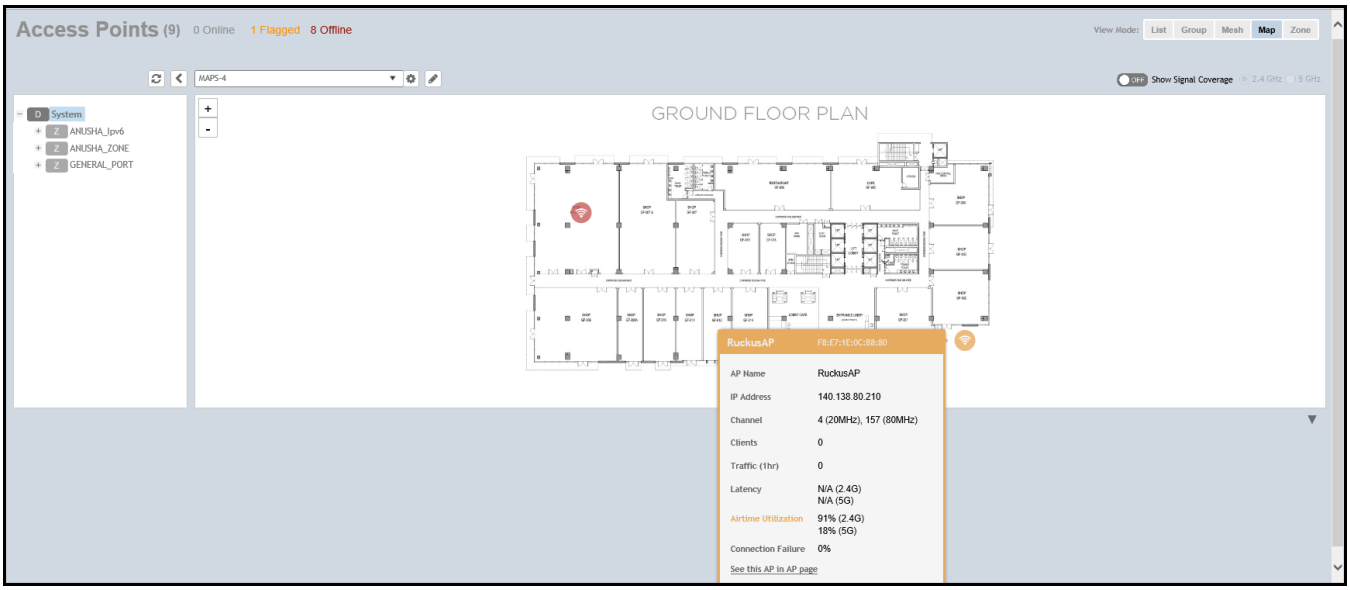


Monitoring APs Using the Map View

Use the Map view on the **Access Points** page to monitor APs in relation to your venue's floorplan.

1. Go to **Network** > **Wireless** > **Access Points**.
2. In **View Mode**, click the **Map** button. The map view is displayed with your placed APs.
3. Hover over an AP to view the following AP-specific details:
   - **AP Name**: The name of the AP, if configured. If not, the default AP name is "RuckusAP."
   - **IP Address**: The current IPv4 or IPv6 address assigned to the AP.
   - **Channel**: Displays the channel (2.4 GHz / 5 GHz) in use, along with the channel width in parentheses.
   - **Clients**: The number of currently connected wireless clients.
   - **Traffic**: The total traffic volume over the last 1 hour.
   - **Latency**: The average time delay between AP and connected clients.
   - **Airtime Utilization**: Percent of airtime utilized, by radio.
   - **Connection Failure**: Percent of client connection attempt failures.

   FIGURE 316 Hover to AP to view details



4. To view more specific details on the AP, click the **See this AP in AP page** link.
5. To view the RF signal strength, select the **Show Signal Coverage** check box and choose the required RF frequency. For example, 2.4 GHz or 5 GHz.

   The heat map is displayed with a color-gradient legend. High signal strength appears in red. The color changes as the signal strength reduces.

Time

Configuring System Time

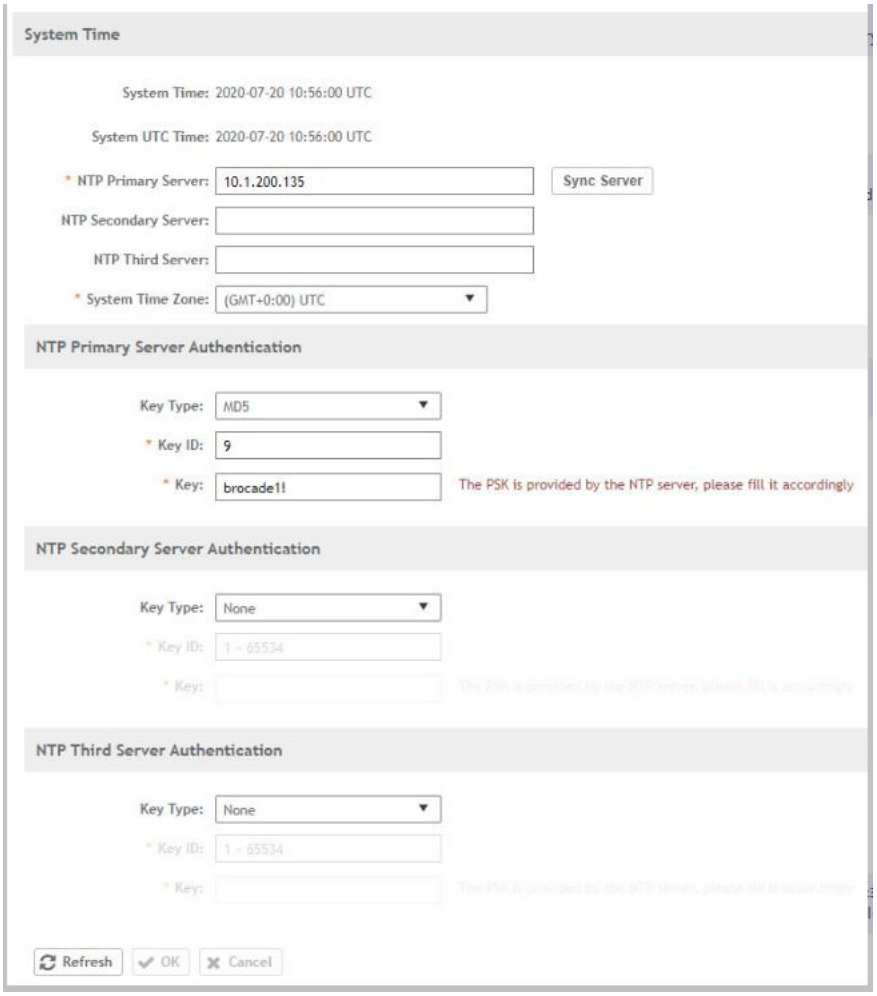
The controller has three external Network Time Protocol (NTP) servers that are used to synchronize the time across Access Points, Cluster nodes, and vDPs.

NOTE
The controller supports version 4.2.6p5 of NTP. The controllers and Access Point does not accept broadcast and multicast NTP packets that would result in the timestamp, these packets are ignored by default.

To edit the system time:

1. Go to **Administration** > **System** > **Time**.
2. Configure the following:
   a. NTP Primary Server: Enter the primary NTP server address that you want to use.

FIGURE 317 Setting System Time



NOTE
By default, the address of NTP Primary Server is http://ntp.ruckuswireless.com.

b. Click **Sync Server** to enable the controller to sync up with the NTP server configured and then to sync the cluster-follower nodes, APs, and vDPs with the controller time.

c. System Time Zone: Select the time zone from the drop-down that you want the controller to use. The default time zone is (GMT +0:00) UTC.

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

To establish this communication, in the **NTP Server Authentication** field, configure **Key Type** as MD5 or SHA1, **KEY ID** in the range of (1 to 65534, and **Key or PSK** as negotiated for each of the NTP servers.

3. Click **OK**.

Time Based Role Policy

Role Based Time Schedule has two options - Always and specific

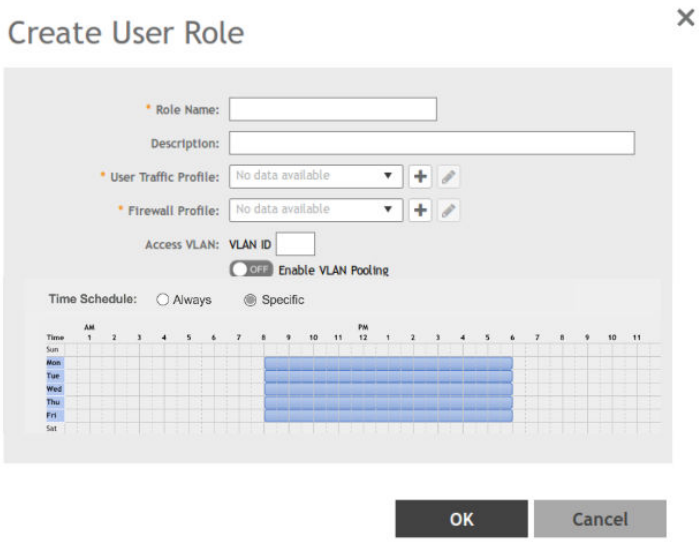
NOTE
COA does not support for this feature.

The objective is to support the role-based policy similar with the Zone Director functions and GAV enhancement. We can configure the role can be used (allowed) in a certain period.

Time Based Role Policy:

1. Select **Monitor**>**Clients**> **Users and Roles**.
2. Click the **Create** tab.

   The **Create User Role** page appears.



3. To allow permissions on Time Schedule, select **Always**/**Specific**

   Always: The role can be allowed anytime.

   Specific: Only the allowed schedule can access.

Role-based OS Policy

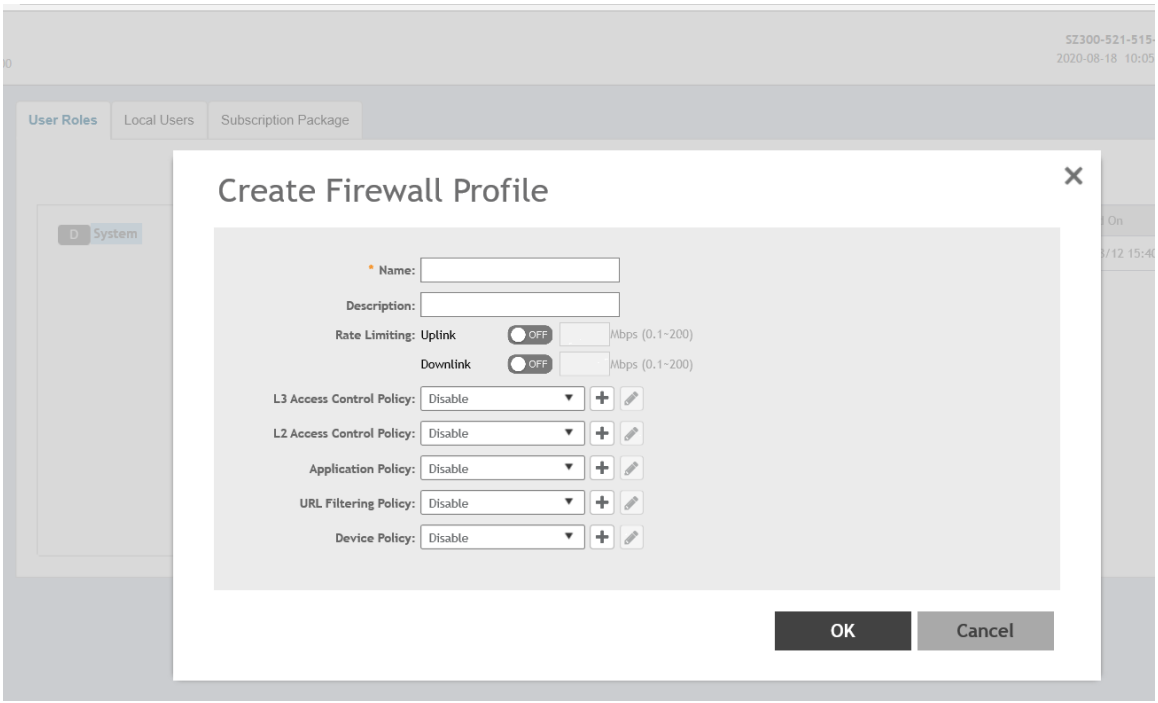
NOTE

NOTE
COA does not support for this feature.

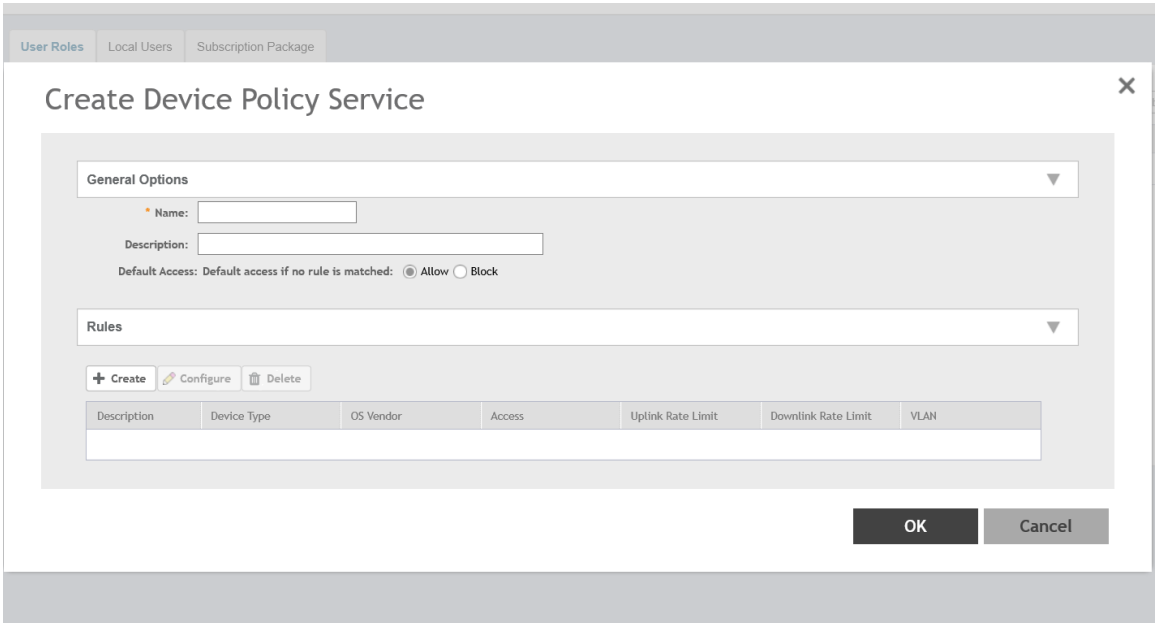
Role can select Firewall Profile and Firewall Profile selects Device Policy.

1. Select **Monitor**> **Clients**> **Users and Roles**.
2. Click the **Create** tab.

   The **Create User Role** page appears.
3. Select the Firewall Profile.



4. Create the device Policy.



5. Enter the **Name** , assign the device policy.
6. Click **Create**
7. Click **Ok**

Role Based Policy for Zone Director Parity

NOTE
COA does not support for this feature.

The objective is to support the role-based policy similar with the Zone Director functions and GAV enhancement. We can configure the role in Smart Zone.

Role Based Policy Allow/Deny:

1. Select **Network**> **Wireless Lans**> **Create**.
2. Click the **Create** tab.

   The Create **WLAN Configuration** page appears.
3. Under **Advanced Options**, select **User Role Access**.
4. To allow permissions on role based, select **Allow All**/**Allow Specific**

   Allow all: All matched role can access this WLAN.

   Allow Specific: Only the selected role can access this WLAN. The user's access request will be denied by AP.

FIGURE 318 Role Permission

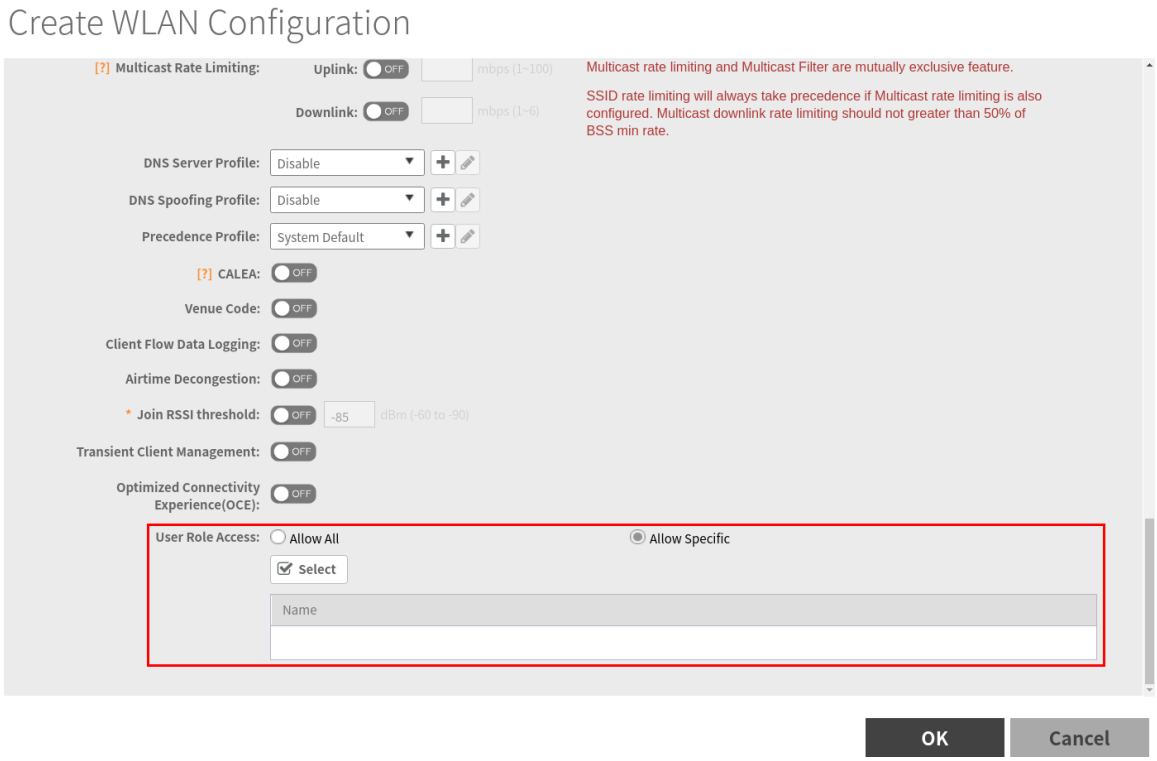
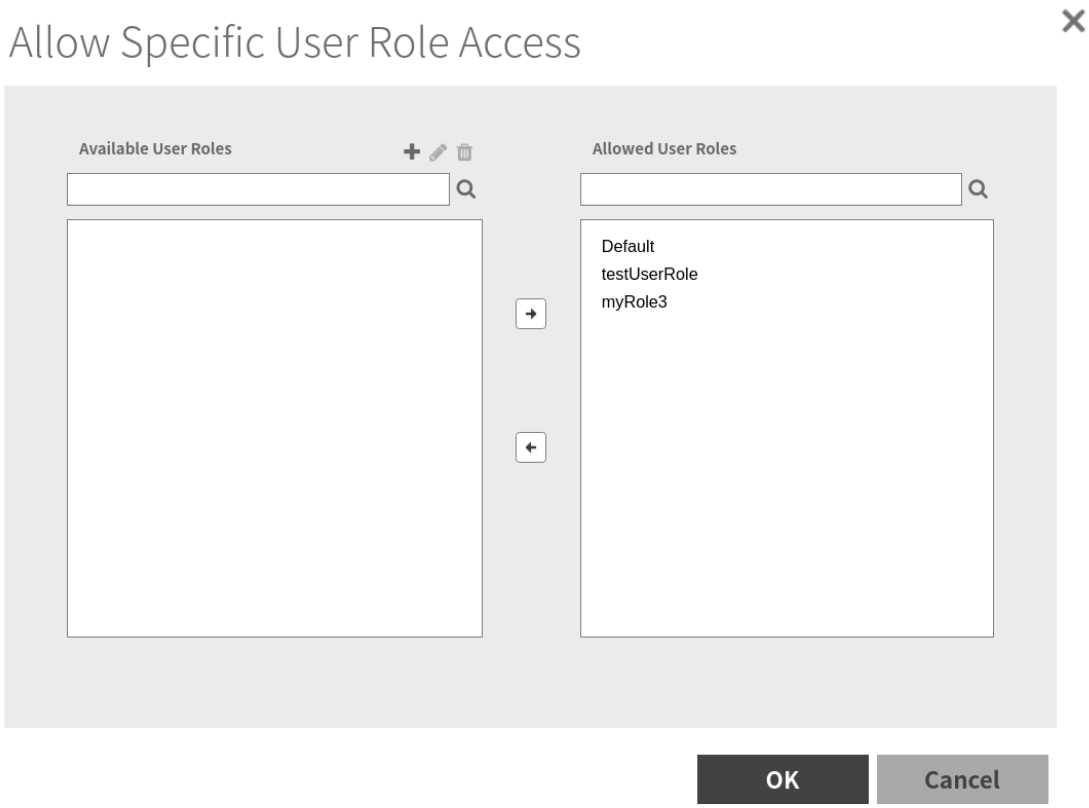


FIGURE 319 Role Permission addition



WLAN's Advanced Options includes a new item User Role Access. It has 2 options - Allow All and Allow Specific.

The option is displayed for DPSK wlans and 802.1x enabled wlans that requires authentication service.

Maximum supported Roles per WLAN is 256 (partner domain max 128 + MSP domain max 128).

AP has all role configurations and WLAN has the role allow/deny configuration.

RAC parses Access-Accept, find the matched role and send back to AP.

AP based on RAC's role and role allow/deny configuration to decide to accept or reject.

NOTE
COA does not support for the feature.

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 110 Syslog Server Configuration Settings

Field	Description	Your Action
Primary Syslog Server Address	Indicates the syslog server on the network.	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.
SecondarySyslog ServerAddress	Indicates the backup syslog server on the network, if any, in case the primary syslog server is unavailable.	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 110 Syslog Server Configuration Settings (continued)

Field	Description	Your Action
Application Logs Facility	Indicates the facility for application logs.	a. Select the option from the drop-down. Range: 0 through 7. b. Select one of the following **Filter Severity**: 1. **Emerg** 2. **Alert** 3. **Crit** 4. **Error** 5. **Warning** 6. **Notice** 7. **Info** 8. **Debug**: Default option
Administrator Activity Logs Facility	Indicates the facility for administrator logs.	a. Select the option from the drop-down. Range: 0 through 7. b. Select one of the following **Filter Severity**: 1. **Emerg** 2. **Alert** 3. **Crit** 4. **Error** 5. **Warning** 6. **Notice** 7. **Info** 8. **Debug**: Default option
Other Logs Filter Severity	Indicates the facility for comprehensive logs.	Select one of the following **Filter Severity**: a. **Emerg** b. **Alert** c. **Crit** d. **Error** e. **Warning** f. **Notice** g. **Info** h. **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: • **All events** — Send all controller events to the syslog server. • **Alleventsexceptclientassociation/ 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 110 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: • **Critical** • **Major** • **Minor** • **Warning** • **Informational** • **Debug**

Certificates

All the security certificates that the controller uses for its web interface, AP portal, and hotspots are managed from a central storage.

By default, a RUCKUS-signed SSL certificate (or security certificate) exists in the controller. However, because this default certificate is signed by RUCKUS and is not recognized by most web browsers, a security warning appears whenever you connect to the web interface or users connect to the AP portal or a hotspot. To prevent these security warnings from appearing, you can import an SSL certificate that is issued by a recognized certificate authority (CA).

If you are implementing Hotspot 2.0 on the network and you want to support anonymous authentication using OSU Server-Only Authenticated L2 Encryption Network (OSEN), you will need to import a trust root certificate, server or intermediate certificate and private key.

Importing New Certificates

When you have a 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.

Follow these steps to import a signed server certificate:

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. In the main menu, click **Administration**. Under **System** menu, hover mouse over the **Certificates** and select **SZ as a Client Certificate**.

NOTE
From the application select, **Administration**>**System** > **Certificates** > **Installed Certs**.

3. Click **Import**, the Import Certificate form appears.
4. Enter a **Name** to identify the certificate.
5. Enter a **Description** about the certificate.
6. For **Service Certificates**, click **Browse** and select the location where the certificate is saved.
7. For **Intermediate CA certificates**, click **Browse** and select the location where the certificate is saved. If you need to upload additional intermediate CA certificates to establish a chain of trust to the signed certificate, you can select up to four certificates.
8. If you are using this SSL certificate for a Hotspot 2.0 configuration, you must also import a root CA certificate. To import **Root CA certificate**, click **Browse** and select the location where the certificate is saved.
9. You can import the **Private Key** file either by
   - uploading file—choose **Upload** and click **Browse** to select the location.
   - using CSR—choose **Using CSR** and select the CSR that you generated earlier.
10. Enter the **Key Passphrase** that has been assigned to the private key file.
11. Click **OK**.

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

NOTE
only CRT or PEM format is supported for the CA certificate.

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 and Guest Access WLAN control traffic.
   - **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. In the main menu, click **Administration**. Under **System** menu, hover mouse over the **Certificates** and select **CSR**.

2. Click **Generate**, the Generate CSR form appears.
3. Enter the following details:
   - **Name**—A name for this CSR.
   - **Description**— 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**.
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.

Managing AP Certificates

AP certificates are valid for a period of time and have to be replaced when they expire.

NOTE
Although AP Certificate Expire Check is enabled by default, when an AP with an expired certificate joins the controller, this check automatically gets disabled. To restore security:

- All APs with expired certificates need to be replaced with a new valid certificate
- Manually enable certificate check using `ap-cert-expired-check` CLI command in the config mode

You must get AP Certificate Replacement before your AP certificate expires. The system generates an *apCertificateExpireSystem* alarm and event when an AP certificate expires.

To get an AP Certificate replacement:

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

2. In the AP Request List area, those APs with the **Need Export** column marked **Yes** needs certificate replacement. Those marked with **No** means that the certificate request has already been exported.

   NOTE
   Use the Search terms option to look for APs by name, model, serial number, or description.

3. Click **Export** and select one of the following options:
   - **Export All APs Certificate Request**—Exports the certificates for all the AP
   - **New APs**—Exports the certificates for new APs or APs that need to regenerate their certificates.

   NOTE
   All exported AP Certificate request (.req) files generated from a cluster include it's name. To manage multiple export request files, change the file name before uploading it to uniquely identify the file.

4. Login https://support.ruckuswireless.com/ with your credentials.
5. From the right pane go to **Tools** > **Certificate Renewal**. The Certificate Renewal Requests page appears.
6. Click **Browse** to select the **.req** file exported from Certificate Refresh page.
7. Enter the Email address for communication.
8. Click **Upload**, you will receive an e-mail acknowledgment from RUCKUS.
9. From the Certificate Renewal Request page, check the **Status** column of your request. After the request is processed, you will receive the response from RUCKUS, with a link to the .res response file for Import on the Certificate Refresh page.
10. From the AP Certificate Replacement page of the application, click **Import AP certificate Response (.res) file**. The Import AP certificate for replacement form appears.
11. Click **Browse** and select the file.
12. Click **OK**.

    NOTE
    All APs included in the imported response (.res) file reboot after their certificate is refreshed.

13. From the Certificate Status area, check the **Status** column of the AP. If the status is:
    - **Updating**—Controller is in the process of updating the certificate.
    - **Update Failed**—Controller failed to update the certificate.

    NOTE
    The AP reports to the controller at 15-minute intervals. As a result, it may take up to 15 minutes for the AP to update its certificate status on the web interface.

14. Click **Reset Update Failed AP**, to reset the status of the APs for which certification update failed. The status of the AP will change.
15. Check the **Update Stats** to know the status of the AP certificates.
16. Once all the APs are updated with the new certificates, manually enable the `ap-cert-expired-check` CLI command in the config mode to restore security and reject APs that try to connect with expired certificate

    .

Importing Trusted CA Certificates

When a controller receives a server's certificate, it matchs 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:

1. In the main menu, click **Administration**. Under **System** menu, hover mouse over the **Certificates** and select **SZ Trusted CA Certificates/ Chain (external)**.
2. Click **Import**, the Import CA Certs (Chain) form appears.
3. Enter a **Name**.
4. Enter a **Description** of the certificate.
5. For **Intermediate CA Certificates**, click **Browse** and select the file. If you need to upload additional intermediate CA certificates to establish a chain of trust to the signed certificate, you can select up to four certificates.
6. For **Root CA Certificate**, click **Browse** and select the file.
7. 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.

AP Validate SZ Controller

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

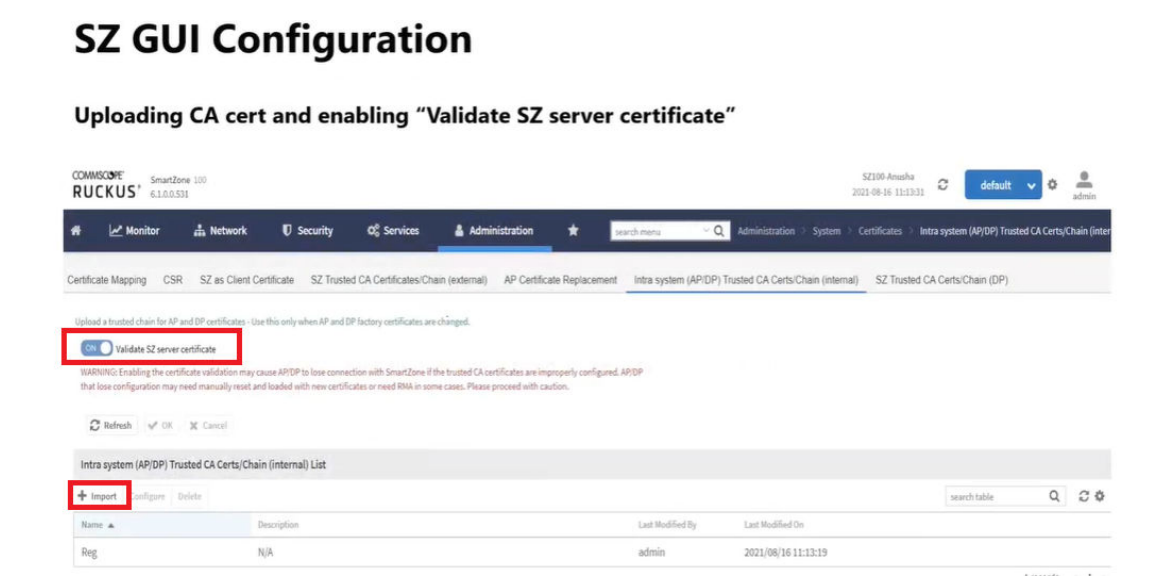
Smart Zone can edit the Domain name after the installation

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

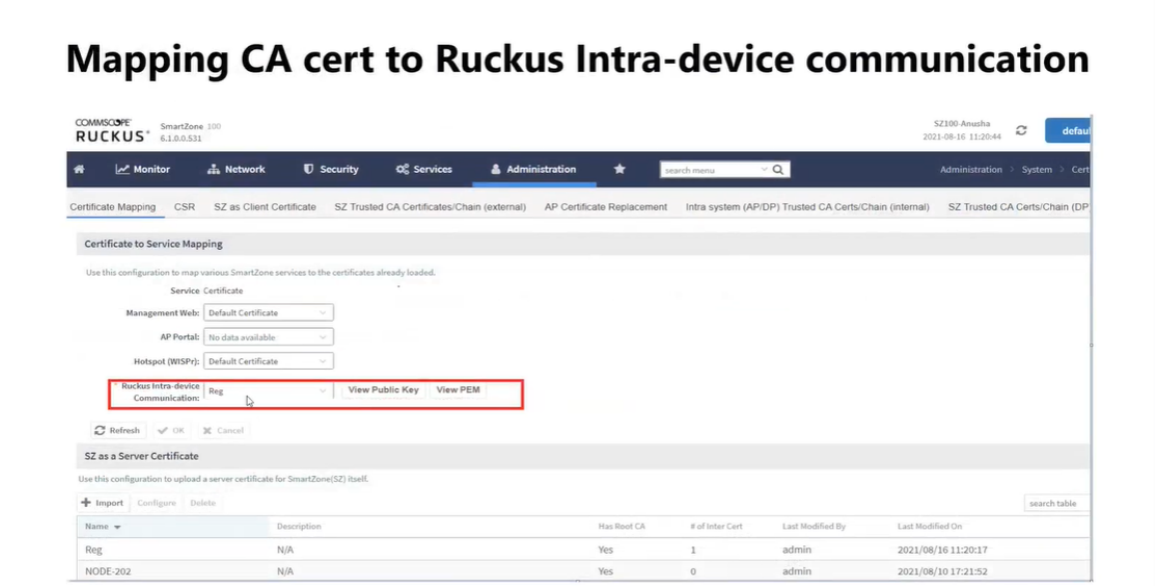
When Server validation is enabled, SZ will push the configurations to AP.

Follow the below steps for the validation of server certificates:

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



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.



7. The certificate will be validated when AP connects to SCG.

8. Configuration Method:

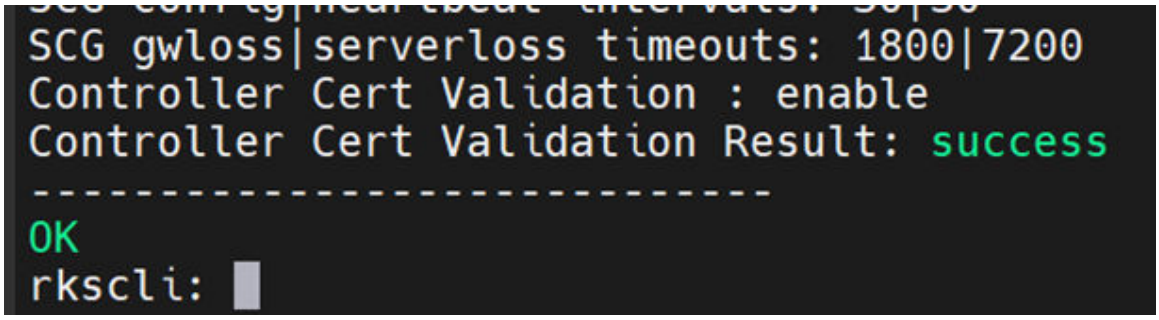
   Part 1:Using Public Key

   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.

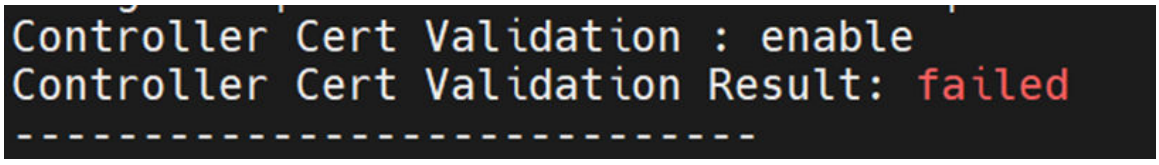
     Success message : ssl_cert_verify_callback:294 SSL Verification OK.

     In Ap CLI execute command "get scg ".



   - If public key is not matching error message,

     In Ap CLI execute command "get scg ".

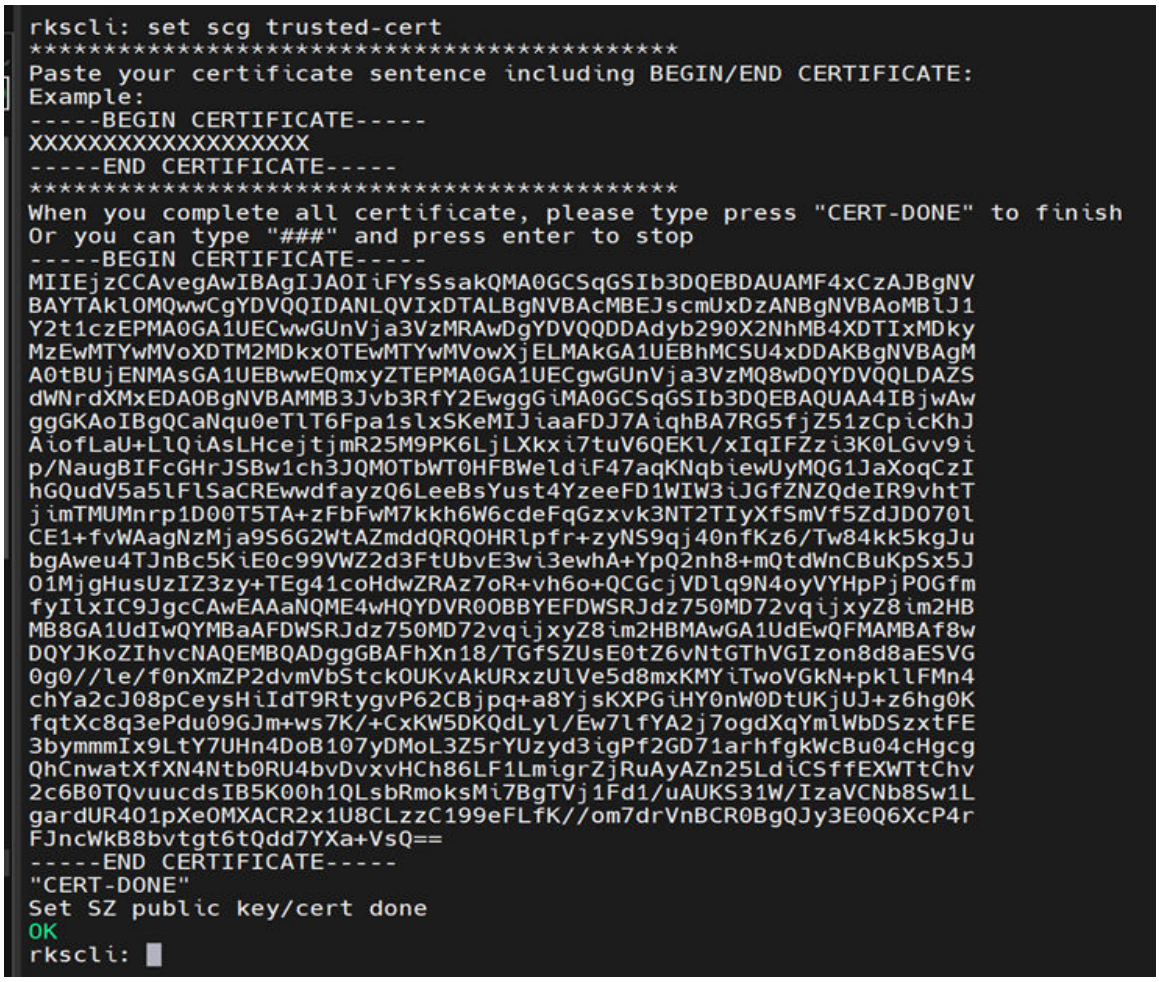


     SSL certificate verification failed.

     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 ".



- 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.

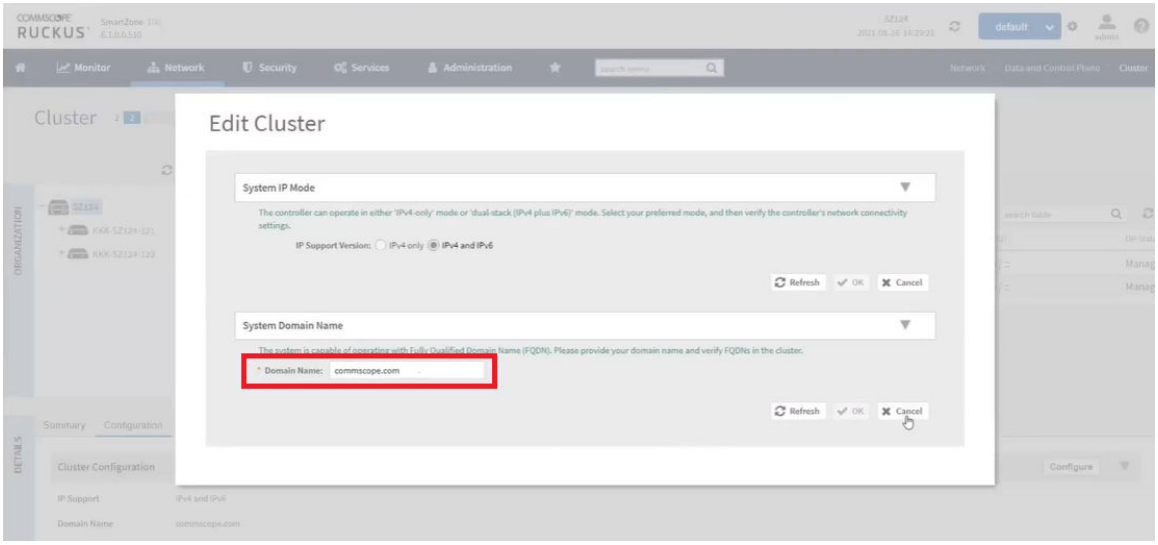
9. Domain name configuration:

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

TABLE 111

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.



DataPlane validates SmartZone

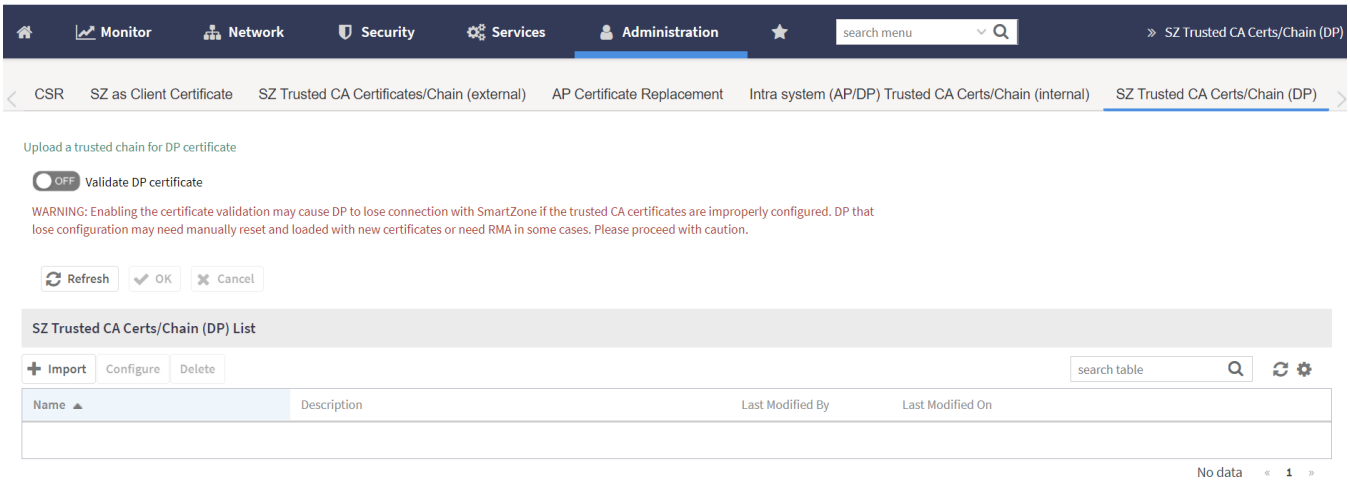
DataPlane validates the incoming SmartZone certificate to check if the certificate is valid.

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

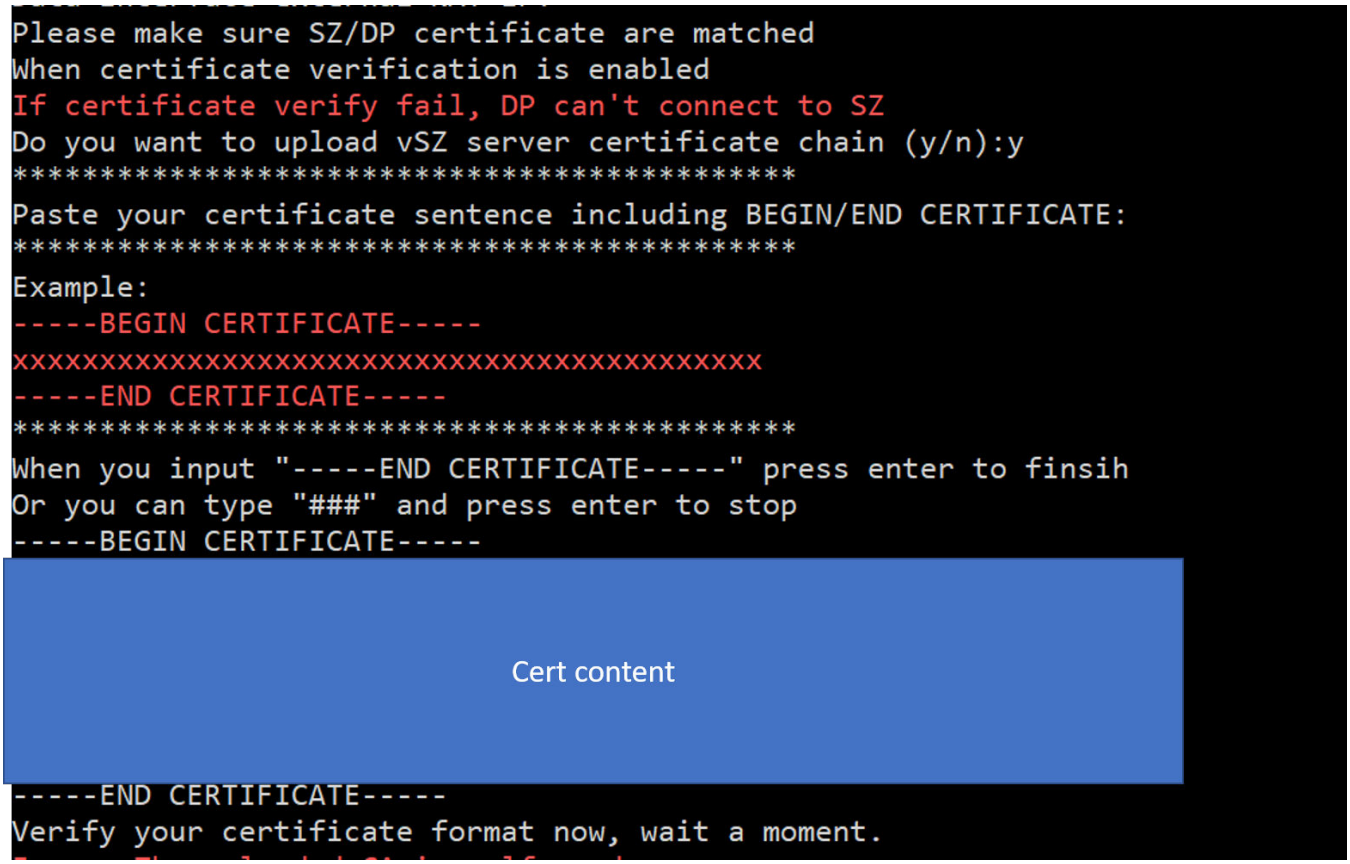
1. Import the DataPlane setup script and upload the certificate in SZone Trusted CACerts/Chain (DP).

FIGURE 320 Upload DataPlane Certificate



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

FIGURE 321 Setup Upload Certificate



3. 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.

Templates

Configuring Templates

Working with Zone Templates

You can create, configure, and clone zone templates.

To view details about a zone template, go to **Administration** > **System** > **Templates** > **Zone Templates** and click a zone. The respective contextual tabs are displayed at the bottom of the page.

TABLE 112 Zone Templates: Contextual Tabs

Tab	Description
Zone Configuration	Displays details of the respective zone template.
AP Group	Displays details of the respective AP group. You can create or configure an AP group. Refer to *Creating an AP Group*.
WLAN	Displays details of the respective WLAN and WLAN group. You can create or configure a WLAN and a WLAN group. Refer to *Working with WLANs and WLAN Groups*.
Hotspots and Portals	Displays details of the respective hotspots and portals. Refer to *Working with Hotspots and Portals*.
Access Control	Displays details of the respective access control. Refer to *Configuring Access Control*.
Authentication and Accounting	Displays details of the respective authentication and accounting servers. Refer to *Authentication* and *Accounting* respectively.
Bonjour	Displays details of the respective Bonjour services. Refer to *Bonjour*.
Tunnels & Ports	Displays details of the respective tunnels and ports. Refer to *Working with Tunnels and Ports*.
WIPS	Displays details of the respective WIPS policies. Refer to *Classifying Rogue Policies*.
Radius	Displays details of the respective VSA profiles. You can create or configure a VSA profile. Refer to Creating a Vendor-Specific Attribute Profile on page 523.

Creating Zone Templates

To create a zone template:

1. Go to **Administration** > **System** > **Templates** > **Zone Templates**.

   NOTE
   For SmartZone 5.2.1 or earlier releases, from the application select, **System** > **Templates** > **Zone Templates**.

2. Click **Create**, the Create Zone Template form appears.
3. Enter the template details as explained in the following table.

TABLE 113 Zone Template Details

Field	Description	Your Action
General Options		
Zone Name	Indicates a name for the Zone.	Enter a name.
Description	Indicates a short description.	Enter a brief description
AP Firmware	Indicates the firmware to which it applies.	Select the firmware.
Country Code	Indicates the country code to ensure that this zone uses authorized radio channels.	Select the country code.
Location	Indicates generic location.	Enter the location.
Location Additional Information	Indicates detailed location.	Enter additional location information.
GPS Coordinates	Indicates the geographical location.	Enter the following coordinates in meters or floor: • **Longitude** • **Latitude** • **Altitude**
AP Admin Logon	Indicates the admin logon credentials. For the Default Zone, the SZ cluster name is used as the default login ID and password.	Enter the **Logon ID** and **Password**.

TABLE 113 Zone Template Details (continued)

Field	Description	Your Action
Time Zone	Indicates the time zone that applies.	Select the option: • **System Defined**: Select the time zone. • **User defined**: a. Enter the **Time Zone Abbreviation**. b. Choose the **GMT Offset time**. c. Select **Daylight Saving Time**.
AP IP Mode	Indicates the IP version that applies.	Select the option: • **IPv4 only** • **IPv6 only** • **Dual**
Historical Connection Failures	Allows the zone APs to report client connection failures so that the administrator can view past connection problems from the Troubleshooting menu.	Click the button.
DP Zone Affinity Profile	Specifies the DP affinity profile for the zone. **NOTE** This option is supported only on vSZ-H.	Select the zone affinity profile from the list.
SSH Tunnel Encryption	Specifies the encryption that reduces the load on control of SSH traffic.	Select the required option: • **AES 128** • **AES 256**
Cluster Redundancy	Provides cluster redundancy option for the zone. **NOTE** Cluster redundancy is supported only on SZ300 and vSZ-H.	Select the required option: • **Zone Enable** • **Zone Disable**
Radio Options		
Channel Range	Indicates that you want to override the 2.4GHz channel range that has been configured for the zone.	Select **Select Channel Range (2.4G)** check boxes for the channels on which you want the 2.4GHz radios to operate. Channel options include channels 1 to 11. By default, all channels are selected.
DFS Channels	Allows ZoneFlex APs to use DFS channels.	Click to enable the option.
Channel 144	Provides channel 140 and 144 support for 11ac and 11ax APs. Enabling this option supports 20 MHz, 40 MHz, or 80 MHz channel modes. The 80+80 MHz and 160 MHz modes are supported if the AP supports these modes. Disabling this option provides Channel 140 support only to 20 MHz mode. **NOTE** This option is available for selection only if you enable the **DFS Channels** option. **NOTE** This feature is currently supported only in the United States.	Click to enable the option.
Channel Range (5G) Indoor	Indicates for what channels want the 5GHz radios to operate.	Select the check boxes.

TABLE 113 Zone Template Details (continued)

Field	Description	Your Action
Channel Range (5G) Outdoor	Indicates for what channels want the 5GHz radios to operate.	Select the check boxes.
Radio Options b/g/n (2.4 GHz)	Indicates the radio option 2.4 GHz configurations.	Select the following options: • **Channelization**—Set the channel width used during transmission to either **20** or **40** (MHz), or select **Auto** to set it automatic. • **Channel**—Select the channel to use for the b/g/n (2.4GHz) radio, or select **Auto** to set it automatic. • **TX Power Adjustment**—Select the preferred TX power, if you want to manually configure the transmit power on the 2.4GHz radio. By default, TX power is set to **Full/Auto** on the 2.4GHz radio. **NOTE** If you choose Min, the transmit power is set to 0dBm (1mW) per chain for 11n APs, and 2dBm per chain for 11ac APs. If you choose Max, the transmit power is set to the max allowable value according to the AP's capability and the operating country's regulations.
Radio Options a/n/ac (5 GHz)	Indicates the radio option 5 GHz configurations.	Select the following options: • **Channelization**—Set the channel width used during transmission to either **20**, **40**, **80**, **80+80** or select **Auto**. • **Channel**—For Indoor and Outdoor, select the channel to use for the a/n/c (5GHz) radio, or select **Auto**. • **TX Power Adjustment**—Select the preferred TX power, if you want to manually configure the transmit power on the 5GHz radio. By default, TX power is set to **Full/Auto** on the 5GHz radio. **NOTE** If you choose Min, the transmit power is set to 0dBm (1mW) per chain for 11n APs, and 2dBm per chain for 11ac APs. If you choose Max, the transmit power is set to the max allowable value according to the AP's capability and the operating country's regulations.
AP GRE Tunnel Options		
Ruckus GRE Profile	Indicates the GRE tunnel profile.	Choose the GRE tunnel profile from the drop-down.
Ruckus GRE Forwarding Broadcast	Forwards the broadcast traffic from network to tunnel.	Click the option to enable forwarding broadcast.
Soft GRE Profiles	Indicates the SoftGRE profiles that you want to apply to the zone.	a. Click the **Select** checkbox, a form is displayed. b. From the A**vailable Profiles**, select the profile and click the -> icon to choose it. You can also click the + icon to create a new SoftGRE profile. c. Click **OK**.

TABLE 113 Zone Template Details (continued)

Field	Description	Your Action
IPsec Tunnel Mode	Indicated the tunnel mode for the Ruckus GRE and SoftGRE profile.	Select an option: • Disable • SoftGRE • Ruckus GRE
IPsec Tunnel Profile	Indicates the tunnel profile for SoftGRE. **NOTE** Select the same tunnel type for IPsec tunnel profile in WLAN configuration.	Choose the option from the drop-down.
Syslog Options		
Enable external syslog server for Aps	Indicates if an external syslog server is enabled.	Select the check box and update the following details for the AP to send syslog messages to syslog server. If the primary server goes down, the AP send syslog messages to the secondary server as backup: • **Primary Server Address** • **Secondary Server Address** • **Port** for the respective servers • **Portocol**: select between UDP and TCP protocols • **Event Facility** • **Priority** • **Send Logs**: you can choose to send the General Logs, Client Logs or All Logs
AP SNMP Options		
Enable AP SNMP	Indicates if the AP SNMP option is enabled.	Select the check box.
SNMPv2 Agent	Indicates SNMPv2 Agent is applied.	a. Click **Create** and enter **Community**. b. Select the required **Privilege**: **Read** or **Write**. c. Click **OK**.
SNMPv3 Agent	Indicates SNMPv3 Agent is applied.	a. Click **Create** and enter **User**. b. Select the required **Authentication**: • **None** • **SHA** 1. Enter the **Auth Pass Phrase** 2. Select the **Privacy** option. For **DES** and **AES** options, Enter the **Privacy Phrase**. • **MD5** 1. Enter the **Auth Pass Phrase** 2. Select the **Privacy** option. For **DES** and **AES** options, Enter the **Privacy Phrase**. c. Select the required **Privilege**: **Read** or **Write**. d. Click **OK**.
Advanced Options		
Channel Mode	Indicates if location-based service is enabled.	Select the check box and choose the option.
Auto Channel Selection	Indicates auto-channel settings.	Select the required check boxes and choose the option.
Background Scan	Runs a background scan.	Select the respective check boxes and enter the duration in seconds.

TABLE 113 Zone Template Details (continued)

Field	Description	Your Action
Smart Monitor	Indicates AP interval check and retry threshold settings.	Select the check box and enter the duration and threshold.
AP Ping Latency Interval	Measures the latency between the controller and AP periodically, and send this data to SCI	Enable by moving the radio button to ON to measure latency.
AP Management VLAN	Indicates the AP management VLAN settings.	Choose the option. If you select **VLAN ID**, enter the VLAN ID that you want to assign (valid range is from 1 to 4094). To keep the same management VLAN ID that has been configured on the AP, click **Keep AP's settings**. **ATTENTION** For standalone APs, set the AP ethernet port to trunk before changing the AP Management VLAN settings.
Rogue AP Detection	Indicates rogue AP settings. **NOTE** Rogue detection AP in active-active mode cluster redundancy environment is restricted from storing its own BSSIDs to avoid considering its own APs as rogues attacking.	Enable the option.
Rogue Classification Policy	Indicates the parameters used to classify rogue APs. This option is available only if you enable the **Rogue AP Detection** option.	Select the options for rogue classification policy: • – **Enable events and alarms for all rogue devices** – **Enable events and alarms for malicious rogues only** • **Report RSSI Threshold** - enter the threshold. Range: **0** through **100**. • **Protect the network from malicious rogue access points** - Enable the option and choose one of the following: – **Aggressive** – **Auto** – **Conservative** • **Radio Jamming Detection** - enable the option and enter the **Jamming Threshold** in percentage.
DoS Protection	Indicates settings for blocking a client.	Select the check box and enter the: • duration in seconds to Block a client for • number of **repeat authentication failures** • duration in **seconds** to be blocked for every repeat authentication failures.
Load Balancing	Balances the number of clients across APs.	Select one of the following options and enter the threshold: • **Based on Client Count** • **Based on Capacity** • **Disabled** **NOTE** If **Based on Capacity** is selected, **Band Balancing** is disabled.
Band Balancing	Balances the bandwidth of the clients.	Select the check box and enter the percentage.

TABLE 113 Zone Template Details (continued)

Field	Description	Your Action
Location Based Service	To disable the LBS service for this AP group, clear the Enable LBS service check box. To use a different LBS server for this AP group, select the Enable LBS service check box, and then select the LBS server that you want to use from the drop-down list.	Select the check box and choose the options.
Client Admission Control	Indicates the load thresholds on the AP at which it will stop accepting new clients. **NOTE** Client admission cannot be enabled when client load balancing or band balancing is enabled.	Select the **Enable** check box 2.4 GHz Radio or 5GHz Radio and update the following details: • **Min Client Count** • **Max Radio Load** • **Min Client Throughput**
AP Reboot Timeout	Indicates AP reboot settings.	Choose the required option for: • **Reboot AP if it cannot reach default gateway after** • **Reboot AP if it cannot reach the controller after**
Recovery SSID	Allows you to enable or disable the Recovery(Island) SSID broadcast on the controller.	Enable **Recovery SSID Broadcast**
Direct Multicast	Indicates whether multicast traffic is sent from a wired device, wireless device or from the network.	Select one or more of the following: • **Multicast Traffic from Wired Client** • **Multicast Traffic from Wireless Client** • **Multicast Traffic from Network**

4. Click **OK**.

NOTE
You can select a zone from the list and edit, clone or delete its template by selecting the options **Configure**, **Clone** or **Delete** respectively.

Applying Zone Templates

To apply a zone template:

1. Go to **Administration** > **System** > **Templates** > **Zone Templates**.

   NOTE
   For SmartZone 5.2.1 or earlier releases, from the application select, **System** > **Templates** > **Zone Templates**.

2. From the list, select the zone template that you want to apply and click **Apply**. The Apply Zone Templates form appears.
3. From **Select AP Zone**, select the required zone.
4. Click **Apply**.

Exporting Zone Templates

You can export a zone template.

To export a zone template:

1. Go to **Administration** > **System** > **Templates** > **Zone Templates**.

NOTE
For SmartZone 5.2.1 or earlier releases, from the application select, **System** > **Templates** > **Zone Templates**.

2. Select the zone template that you want to export and click **Export Template**.
3. A pop-up appears prompting you to **Open** or **Save** the zone template file with .**bak** extension. Click:
   - **Open**—To view the template file
   - **Save**—Select the destination folder where you want to save the template file and then click **Open** to view it.

Importing Zone Templates

You can import zone templates and upload them to the system.

NOTE
Configuration references to global services or profiles cannot be imported, manually configure it after importing.

To import a zone template:

1. Go to **Administration** > **System** > **Templates** > **Zone Templates**.

   NOTE
   For SmartZone 5.2.1 or earlier releases, from the application select, **System** > **Templates** > **Zone Templates**.

2. Click **Import**, the Import Zone Templates form appears.
3. Click **Browse** and select the template file.
4. Click **Upload**.

Working with WLAN Templates

You can create, configure, and clone a WLAN template.

To view details about a WLAN template, go to **Administration** > **System** > **Templates** > **WLAN Templates** and click a zone. The respective contextual tabs are displayed at the bottom of the page.

TABLE 114 WLAN Templates: Contextual Tabs

Tab	Description
General	Displays details of the respective WLAN template.
WLAN	Displays details of the respective WLAN. You can create or configure a WLAN. Refer to *Creating a WLAN Configuration*.
Hotspots and Portals	Displays details of the respective hotspots and portals. Refer to *Working with Hotspots and Portals*.
Access Control	Displays details of the respective access control. Refer to *Configuring Access Control*.
Authentication and Accounting	Displays details of the respective authentication and accounting servers. Refer to *Authentication* and *Accounting* respectively.
Tunnels & Ports	Displays details of the respective tunnels and ports. Refer to *Working with Tunnels and Ports*.
Radius	Displays details of the respective VSA profiles. You can create or configure a VSA profile. Refer to Creating a Vendor-Specific Attribute Profile on page 523.

Creating WLAN Templates

To create a WLAN template:

1. Go to **Administration** > **System** > **Templates** > **WLAN Templates**.

NOTE
For SmartZone 5.2.1 or earlier releases, from the application select, **System** > **Templates** > **WLAN Templates**.

2. Click **Create**, the Create WLAN Template form appears.
3. Enter a **Template Name**.
4. Enter a **Description**.
5. Select the **Template Firmware**.
6. Choose the **AP IP Mode**.
7. Select **AP SoftGRE Tunnel** to enable all WLANs defined in this template to tunnel traffic to SoftGRE through the AP.
8. Click **OK**.

NOTE
You can select a WLAN and edit, clone or delete its template by selecting the options **Configure**, **Clone** or **Delete** respectively.

Applying a WLAN Template

You can apply the WLAN template to zones where the AP's firmware version is later than the Zone templates firmware version. An unsupported firmware version of the WLAN template is automatically upgraded to its next version before being upgraded to the current version.

To Apply a WLAN template to a zone:

1. Go to **Administration** > **System** > **Templates** > **WLAN Templates**.

NOTE
For SmartZone 5.2.1 or earlier releases, from the application select, **System** > **Templates** > **WLAN Templates**

2. From the list, select the WLAN template that you want to apply and click **Apply**. The Apply WLAN Template to selected zones form appears.
3. From **Available AP Zones**, select the required zone and click the  Move button.
4. Click **Next**, the **Apply WLAN template to selected zones** form appears.
5. Select the required options:
   - Create all WLANs and WLAN profiles from the template if they don't already exist in the target zone(s)
   - If the target zone(s) has WLANs or WLAN profile with the same name as the template, overwrite current settings with settings from the template.
6. Click **OK**, you have applied the template to the zone.

DNS Servers

Creating a DNS Server Profile

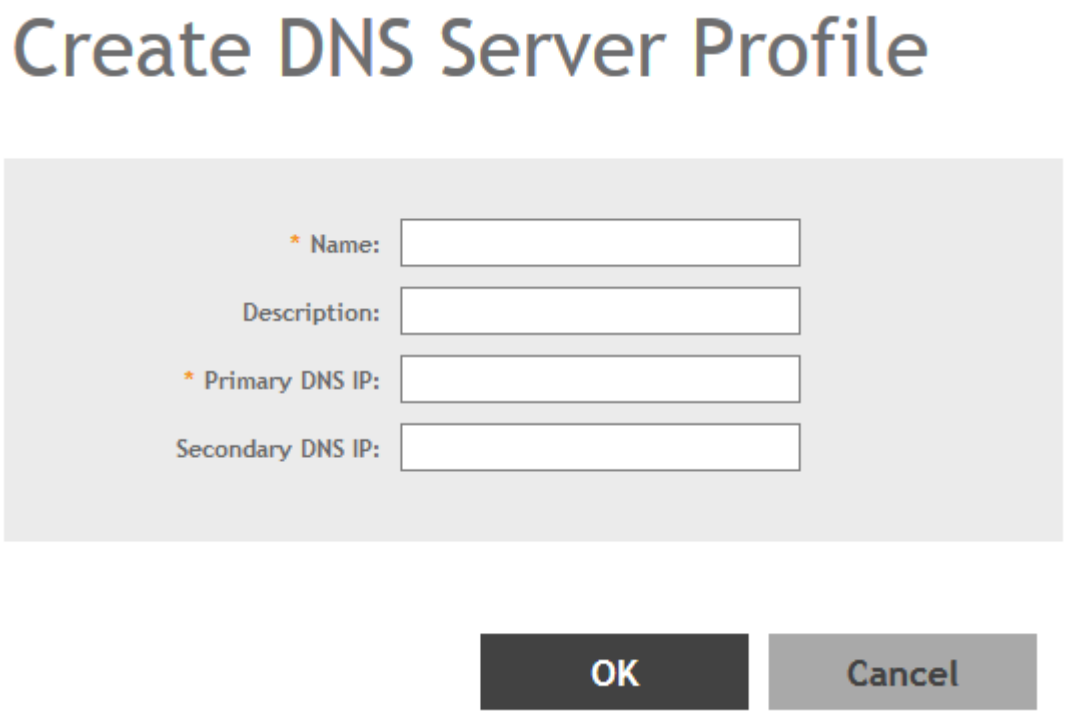
By creating a DNS server profile, you can specify the primary and secondary address of the DNS server that will be used to transmit data packets to the DNS server.

1. Go to **Security** > **Access Control**.
2. Select the **DNS Servers** tab, and then select the zone for which you want to create the profile.

3. Click **Create**.

   The **Create DNS Server Profile** page appears.

   FIGURE 322 Creating a DNS Server Profile



4. Configure the following:
   a. Name: Type a name for the DNS server profile.
   b. Description: Type a short description for profile.
   c. Primary DNS IP: Type the primary DNS IP address.

      NOTE
      This feature supports IPv4 format.

   d. Secondary DNS IP: Type the secondary DNS IP address.

      NOTE
      This feature supports IPv4 format.

   e. Click **OK**.

You have created the DNS Server Profile.

NOTE
You can also edit, clone and delete the profile by selecting the options **Configure**, **Clone** and **Delete** respectively, from the **DNS Servers** tab.

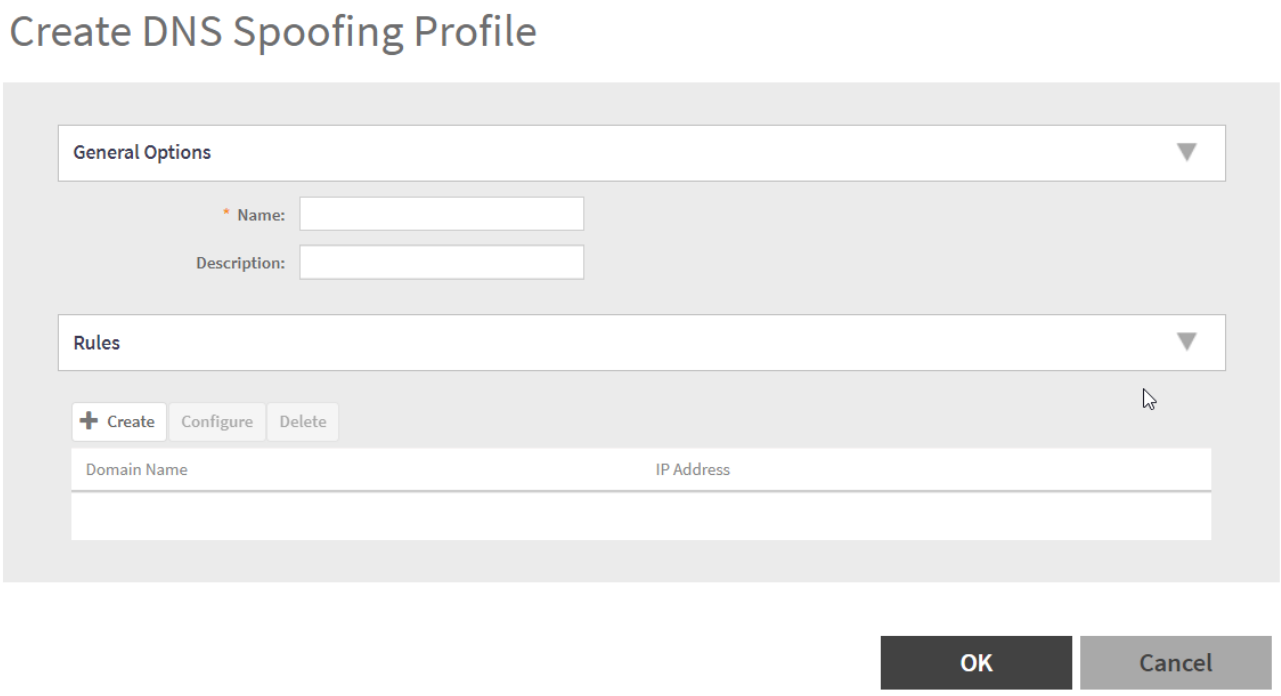
Creating a DNS Spoofing Profile

By creating a DNS spoofing profile, you can specify the IPv4 or IPv6 address of the DNS server. The AP then transmits the data packets to the DNS server.

1. Go to **Services** > **Others** > **DNS Spoofing**
2. Select the zone for which you want to create profile.
3. Click **Create**.

   The **Create DNS Spoofing Profile** page is displayed.

   FIGURE 323 Creating DNS Spoofing Profile



4. Configure the following:
   a) Name: Enter a name for the DNS spoofing profile.
   b) Description: Enter a short description for the profile.
   c) Click **Create**, and the **Create Rules** dialog box is displayed.
   d) In the **Domain Name** field, enter the domain name of the DNS server.
   e) In the **IP Adress** field, enter the IPv4 or IPv6 of the DNS server and click **Add**. If the user sends DNS request with the domain name configured in the DNS Spoofing profile, then the AP responds with the IP address configured in the DNS Spoofing profile for the requested domain name.
   f) Click **OK** to confirm the rules.
   g) Click **OK** to confirm the creation of DNS spoofing profile.

      NOTE
      You can also edit, clone or delete the profile by selecting the options **Configure**, **Clone** or **Delete** respectively, from the **DNS Spoofing** tab.

External Services

Ruckus Services

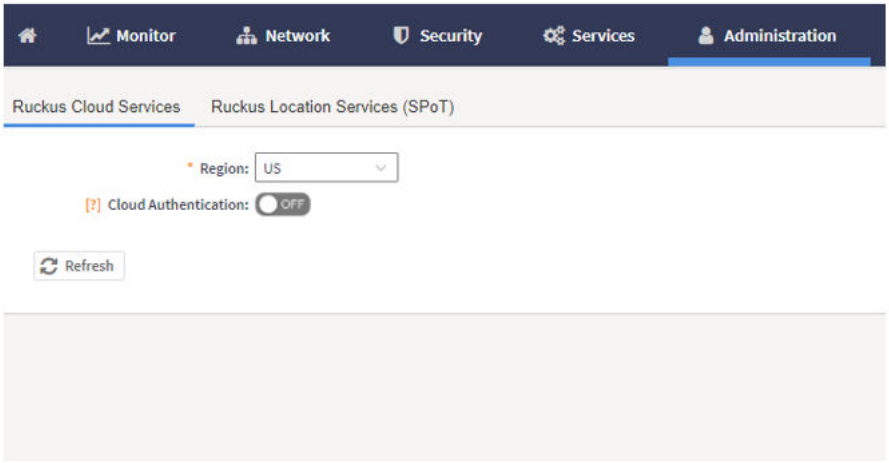
Configuring Cloud Services

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**.

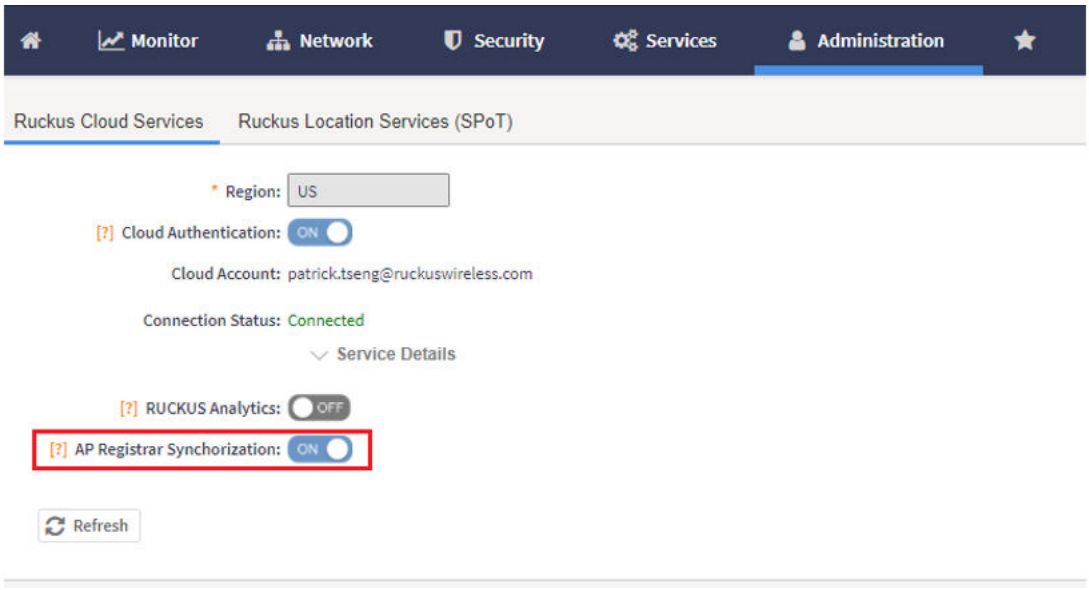
   The **Ruckus Cloud Services** page is displayed.

   FIGURE 324 Configuring Cloud Services



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

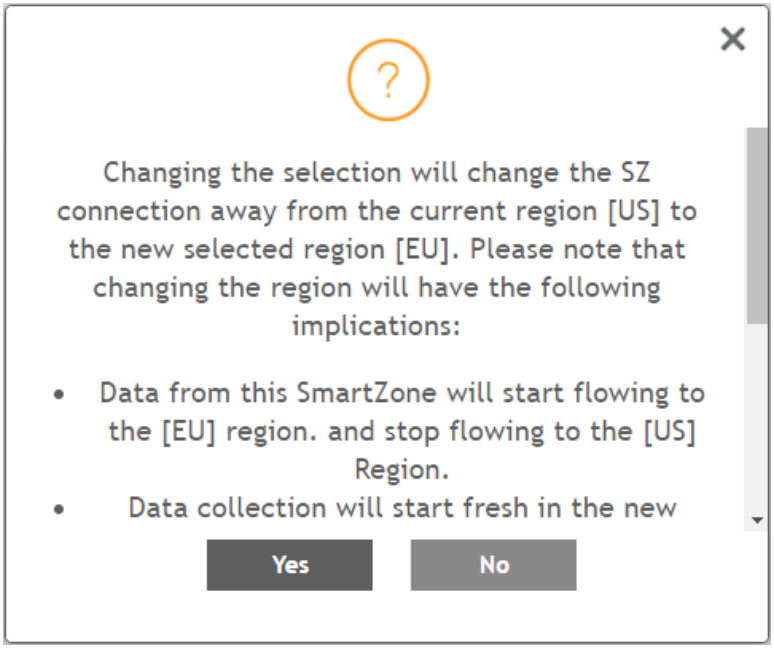
FIGURE 325 The Log in Page



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

A confirmation dialog box is displayed.

FIGURE 326 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 Analytics**.

   The connection status for RUCKUS Cloud Analytics is displayed.

6. Select **AP Registrar Synchronization**.

FIGURE 327 Selecting Export All Batch Provisioning APs

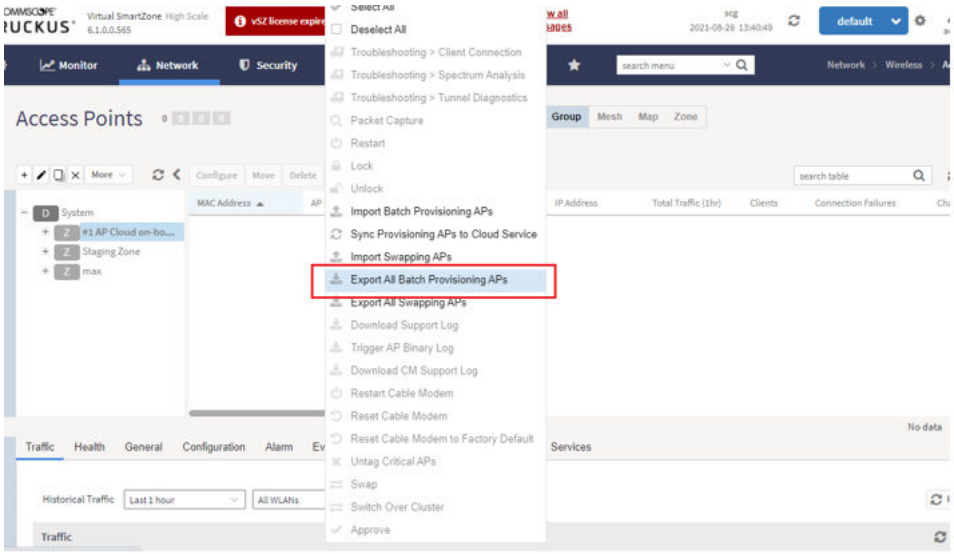
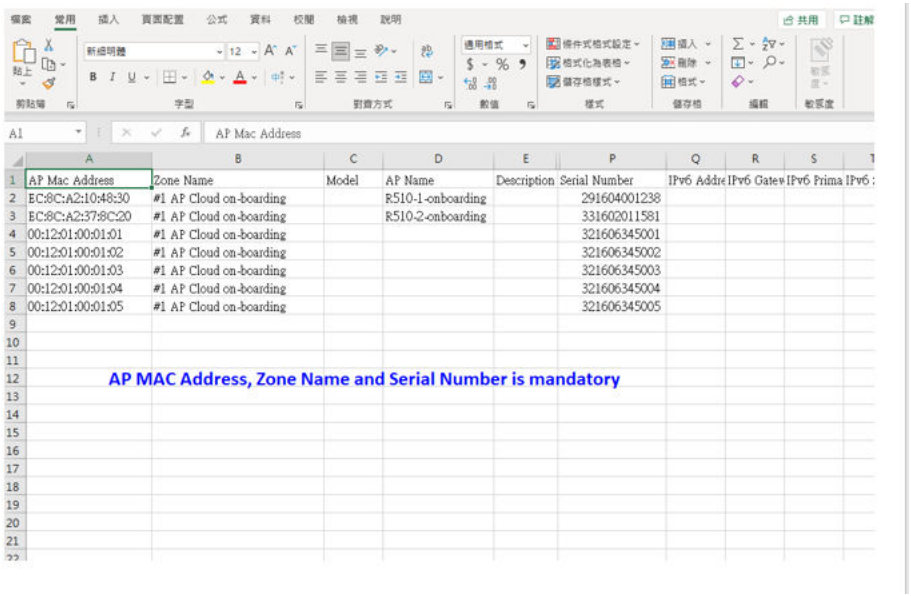


FIGURE 328 Exporting the CSV File

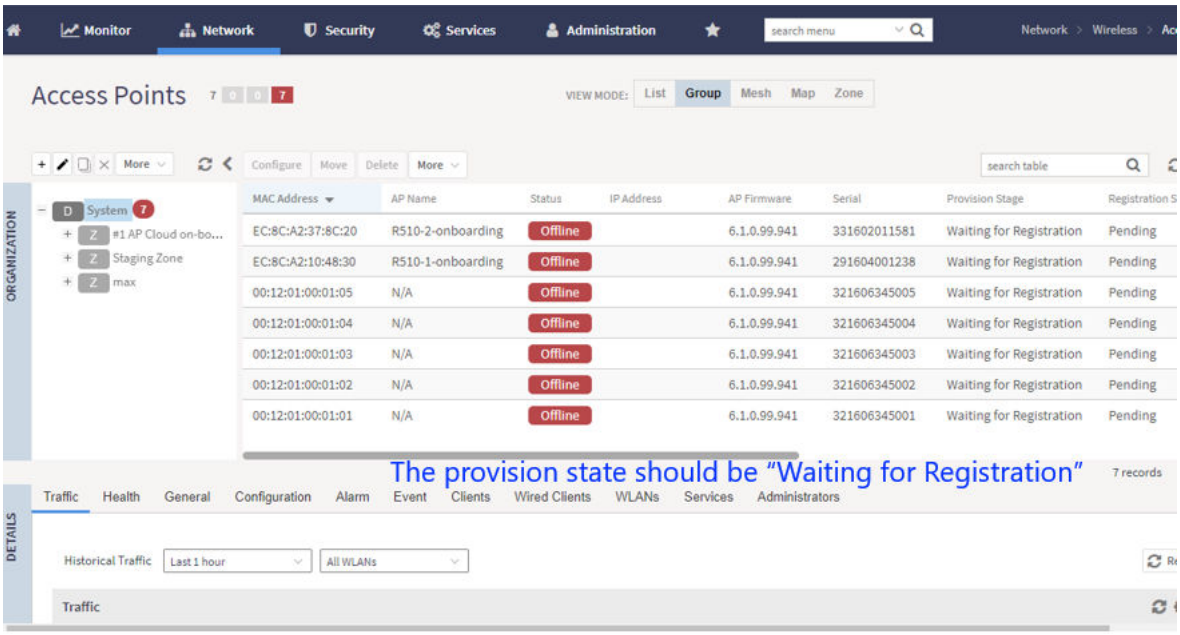


7. Go to **Network** > **Access points**. Select an AP and click **More.**. From the list, select **Export All Batch Provisioning APs**. A blank provisioning AP template is exported from SZ. Ensure that the AP MAC address, the zone name, and the serial number are entered in the CSV file.

8. Import the provisioning AP list to an AP Zone.

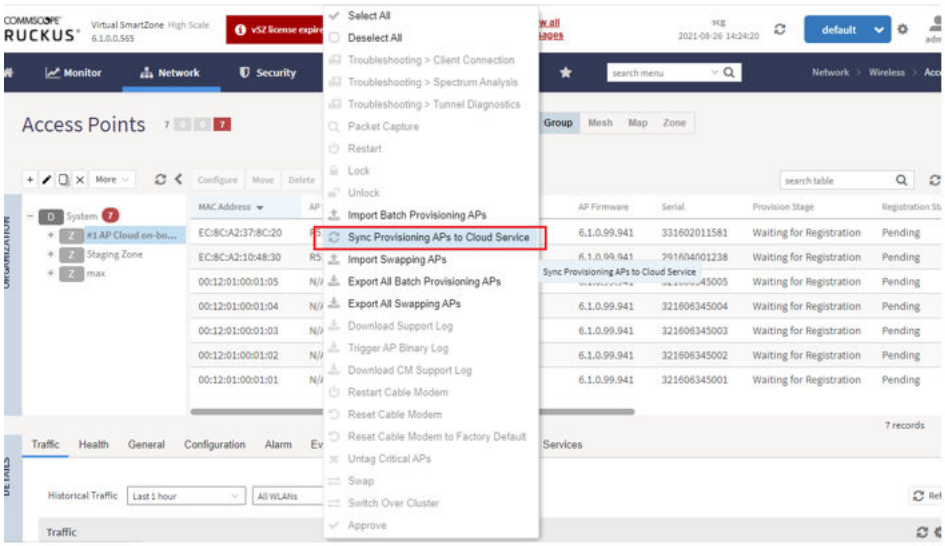
   NOTE
   The provision stage of the AP should be "Waiting for Registration".

FIGURE 329 Importing CSV File



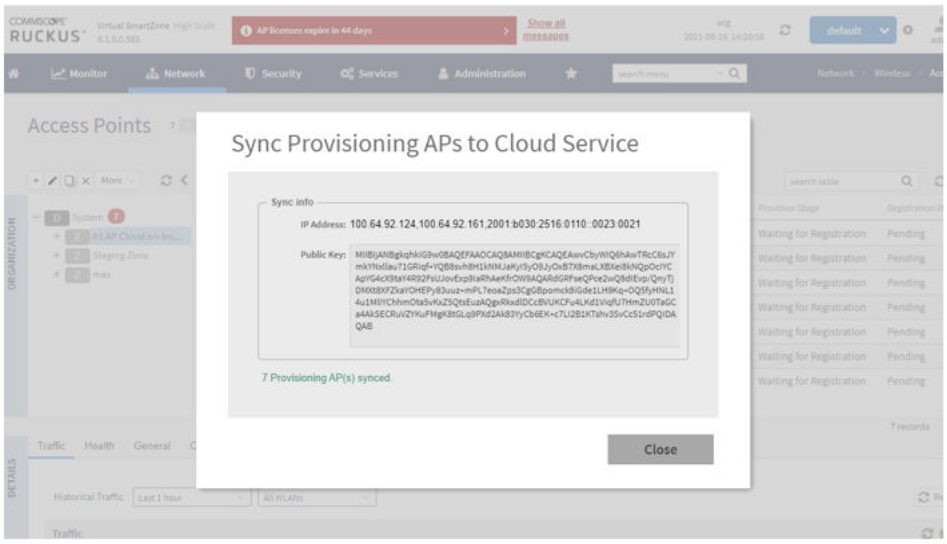
9. Click **More**, and select **Sync Provisioning APs to Cloud Service** from the list.

FIGURE 330 Selecting Sync Provisioning APs to Cloud Service



10. Ensure synchronization is successful.

FIGURE 331 Ensuring Synchronization Success



Location Service

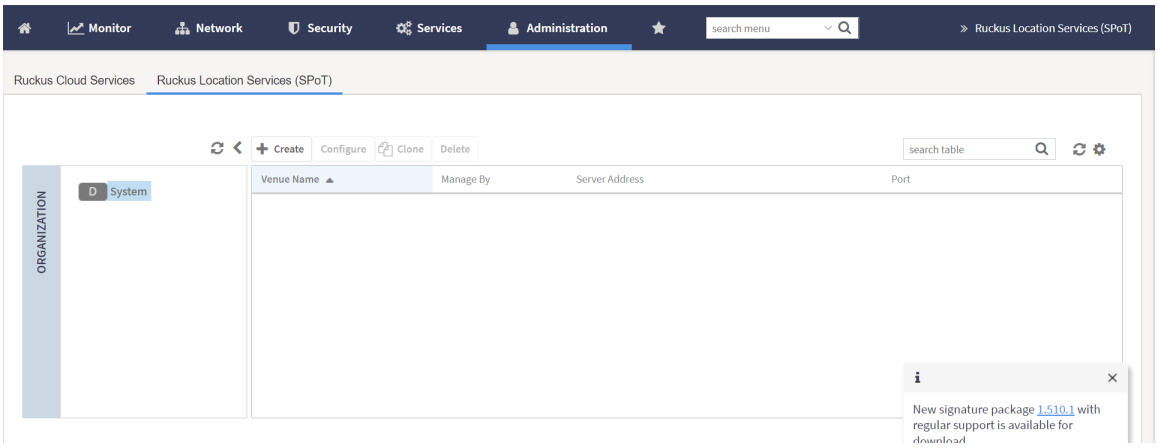
If your organization purchased the RUCKUS Smart Positioning Technology (SPoT) location service, the controller must be configured with the venue information that is displayed in the SPoT Administration Portal.

After completing purchase of the SPoT location service, you will be given account login information that you can use to log into the SPoT Administration Portal. The Admin 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 will need to enter the same venue information in the controller.

1. Select **Administration** > **External Services** > **Ruckus Service** > **Ruckus Location Services (SPoT)**.

   The **Location Service** page appears.

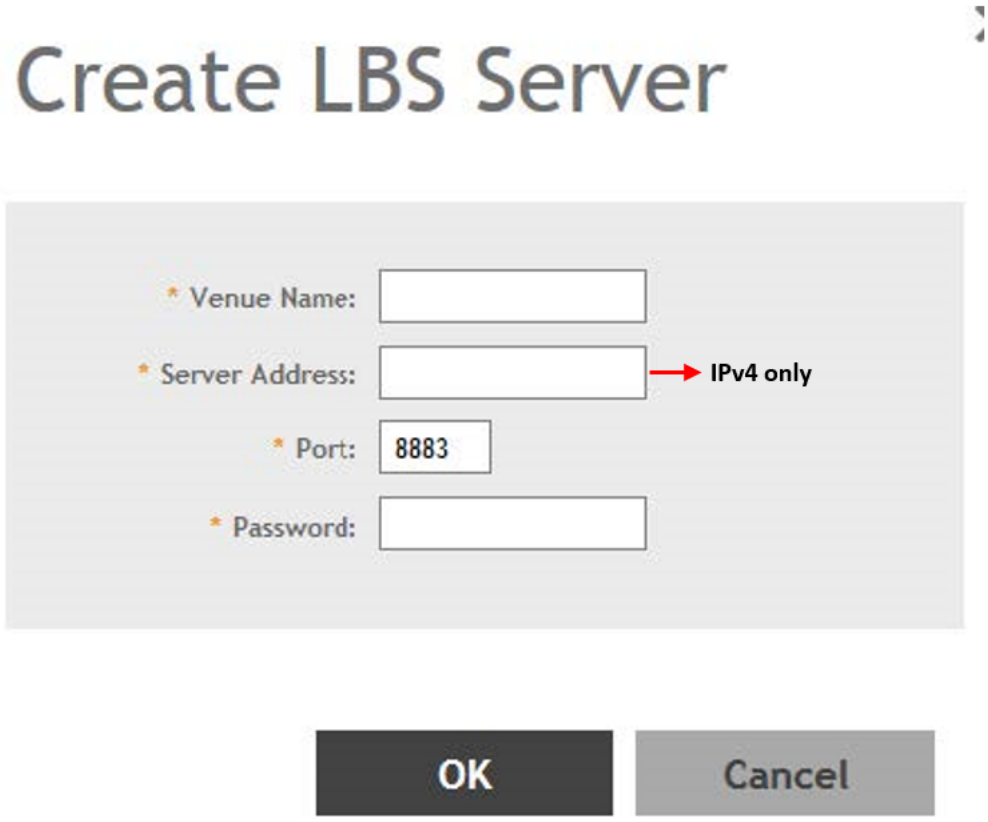
FIGURE 332 Location Service



2. Click **Create**.

   The **Create LBS Server** page appears.

   FIGURE 333 Creating an LBS Server



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

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

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

   NOTE
   Default port number is 8883.

6. In the **Password** field, enter the password to access the server.
7. Click **OK**.

You have completed creating a location-based service on the controller.

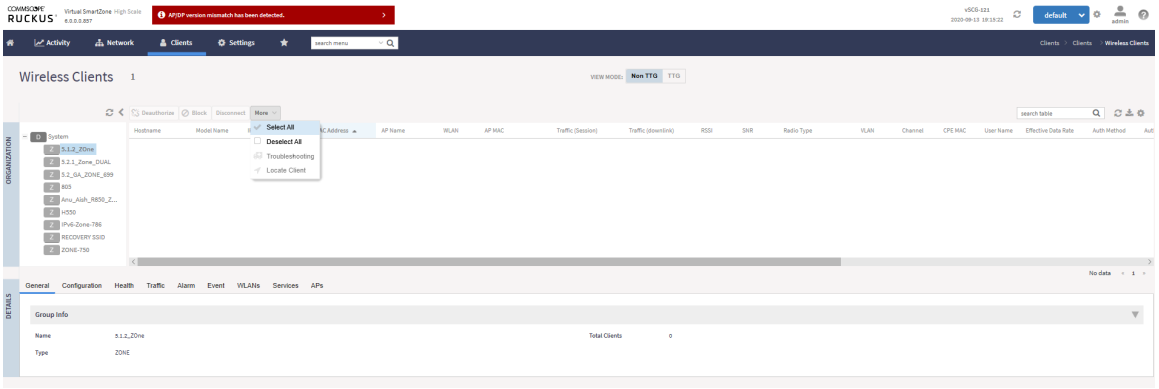
NOTE
You can also edit, clone, and delete the location service by selecting the options **Configure**, **Clone**, and **Delete** respectively from the **Location Services** tab.

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 via the default route.

Locate a Device on SZ Indoor Map

The user wants to locate the client(device) and the controller attempt to approximate the location of the client using data from more than one AP.

The Client location can be found out as per the image below:



1. The SZ side will select some APs.
   - Find the AP which the client connecting to.
   - Find APs which deployed in the same zone and placed in the same indoor map.
   - Use at most **10** APs closing to the managed AP(incl. managed AP itself) as targets.
   - Invoking their CLI.
2. APs will return their 'detected table' to the SZ.
   - The AP has hold a table max **2046** entries which AP detected recently of probe request.
   - The AP has its own age-out mechanism**(60 sec)** to maintain the table.
     - The previous detected record rssi value will be turn to 0 after 60 sec.
     - The record will be removed once the table more than 2046, delete the oldest record first.
3. The SZ filter those result with specific client MAC.
4. Calculate and draw the map and then display.
   - If more than one AP, we can have relatively accurate location of the client.
   - If only one AP(the client connecting one) we can display the AP's location.

Configuring Advanced Gateway Options

You can configure advanced gateway options. This feature no longer depend on flat file changes.

To configure advanced gateway options:

1. Go to **Administrator** > **External Services** > **Advanced Gateway (GTP)**.
2. Configure the following options:
   - **GTP Network Service Access Point Identifier [NSAPI]**—Selects NSAPI for GTP message. The default setting is **1**.
   - **Include IMEI IE in GTP Messages**—Enables or disables IMEI IE in GTP messages. The default setting is **No**.

NOTE
In IMEI IE, the controller will send the MAC address of the UE appended with FFFE.

- **Include ECGI in GTPV2 Messages**—Used only when the S5/S8 interface is used for GTPv2:
- **Include TAI in GTPV2 Messages**—Used only when the S5/S8 interface is used for GTPv2.
- **GTPv2 Interface Type**—Choose the interface type. S2a or S5_S8.

NOTE
The default GTPv2 interface for the controller is S2a.

- **Include SCG-RAI in GTPV2 Messages**—Enables or disables SCG-RAI in GTPV2 messages. The default setting is **No**.
- **Include SCG-SAI in GTPV2 Messages**—Enables or disables SCG-SAI in GTPV2 messages. The default setting is **No**.

3. Click **OK**.

Northbound Data Streaming

Configuring Northbound Data Streaming Settings

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 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.

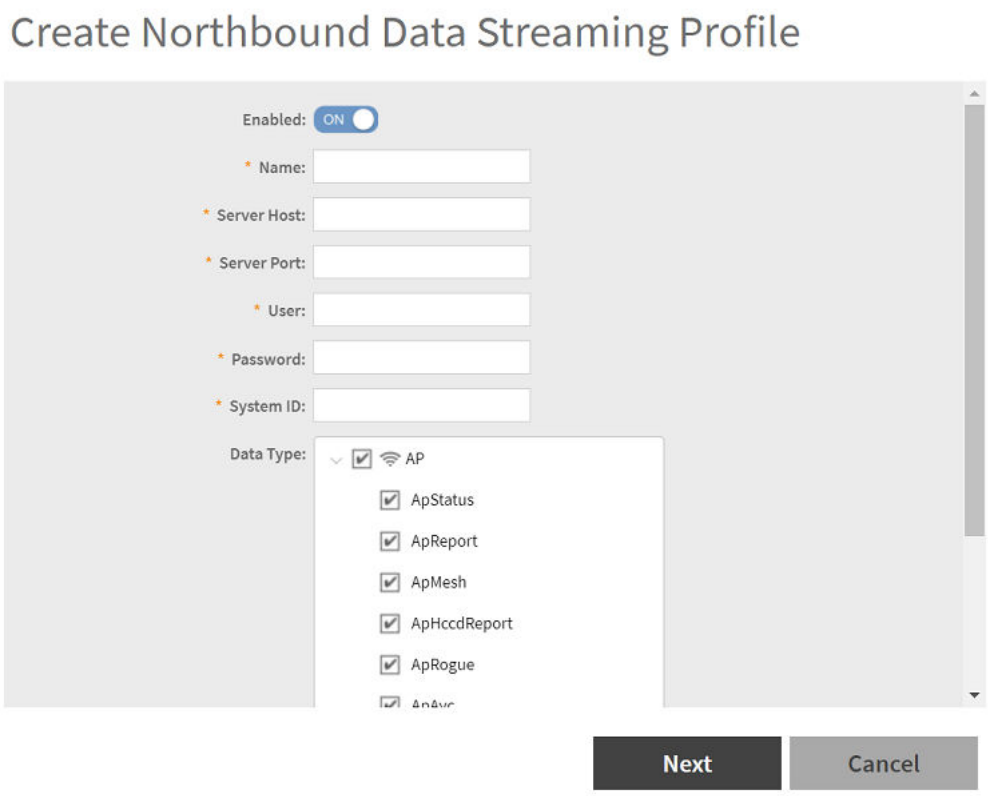
NOTE
You can create a maximum of two SCI profiles simultaneously.

Follow these steps to configure the Northbound Data Streaming server settings.

1. Go to **Administrator** > **External Services** > **Northbound Data Streaming**.

2. Click **Create**. The **Create Northbound Data Streaming Profile** form is displayed.

FIGURE 334 Creating Nortbound Data Streaming Profile



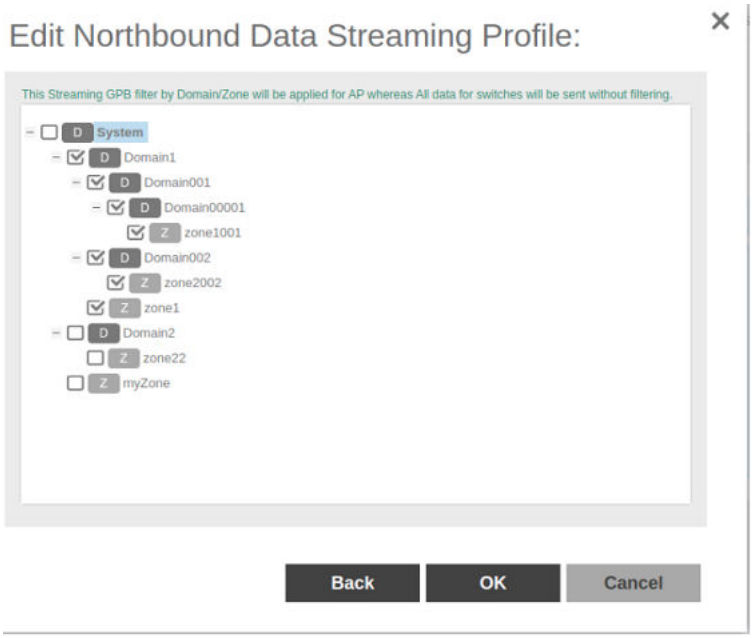
3. Enter the following details:
   - Enabled: Configures the Northbound Data Streaming profile.
   - Name: Specifies the profile name.
   - Server Host: Specifies the IP address to the Northbound Data Streaming host server.

     NOTE
     The SCI profile supports only the IPv4 format.

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

5. For APs, from the **System** tree, select the required Domain or Zone to send KPIs or statistics to Northbound Data Streaming server. For Switches, KPIs or statistics are sent to SCI or Northbound Data Streaming server without filtering.

   FIGURE 335 Selecting Zone or Domain



6. Click **OK**.

   The updated profile is listed in the table.

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

   NOTE
   You can also edit or delete a Northbound Data Streaming profile. To do so, select the Northbound Data Streaming profile from the list and click **Configure** or **Delete** as required.

Setting the Northbound Portal Password

Third-party applications use the northbound portal intrface to authenticate users and to retrieve user information during the UE association.

Follow these steps to configure the northbound portal interface:

1. Go to **Administrator** > **External Services** > **WISPr Northbound Interface**.
2. Select **Enable Northbound Interface Support**, and enter the **User Name** and **Password**.
3. Click **OK**.

WISPr Northbound Interface

SNMP Agent

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 115 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: • **Read-Only**—Privilege only to read. • **Read-Write**—Privilege only to read and write. • **Notification**—Privilege to: – **Trap**—Choose this option to send SNMP trap notification. – **Inform**—Choose this option to send SNMP notification. 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 follwoing table.

TABLE 116 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.
Authentication	Indicates the authentication method.	Choose the required option: • **SHA**—Secure Hash Algorithm, message hash function with 160-bit output. a. Enter the **Auth Pass Phrase**. b. Choose the **Privacy** option. – **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. a. Enter the **Auth Pass Phrase**. b. Choose the **Privacy** option. – **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.	Select the required privileges: • **Read-Only**—Privilege only to read. • **Read-Write**—Privilege only to read and write. • **Notification**—Privilege to: – **Trap**—Choose this option to send SNMP trap notification. – **Inform**—Choose this option to send SNMP notification. 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**.

FTP

Configuring FTP Server Settings

The controller enables you to automatically back up statistics files, reports, and system configuration backups to an external 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.

SMTP

Configuring 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**.

SMS

Configuring the 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:

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 ths 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.

Administration

Admins and Roles

Managing Administrator and Roles

The controller must be able to manage various administrators and roles that are created within the network in order to assign tasks and functions, and to authenticate users.

Creating User Groups

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

1. Go to **Administration** > **Administration** > **Admins and Roles**.
2. Select the **Groups** tab.
3. Click **Create** after selecting the system domain.

   The **Create User Group** page appears.

4. Configure the following:
   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. To select the right set of resource permission, refer to Resource Group Details.

      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. Domain: Select the domain from the list of domains to which this user group will be associated. From **Select Domains**, choose the domains you want to assign to this user group. Click the  icon and they appear under **Selected Domains** now. Use the  icon to deselect the domains assigned to the group.
   e. Click **Next**.
   f. 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.
   g. Click **Next**.
   h. Review: Verify the configuration of the user group. Click **Back** to make modifications to the configuration settings.
   i. 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 117 Resource Group Table

Resource Category	Resources
SZ	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	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	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 117 Resource Group Table (continued)

Resource Category	Resources
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

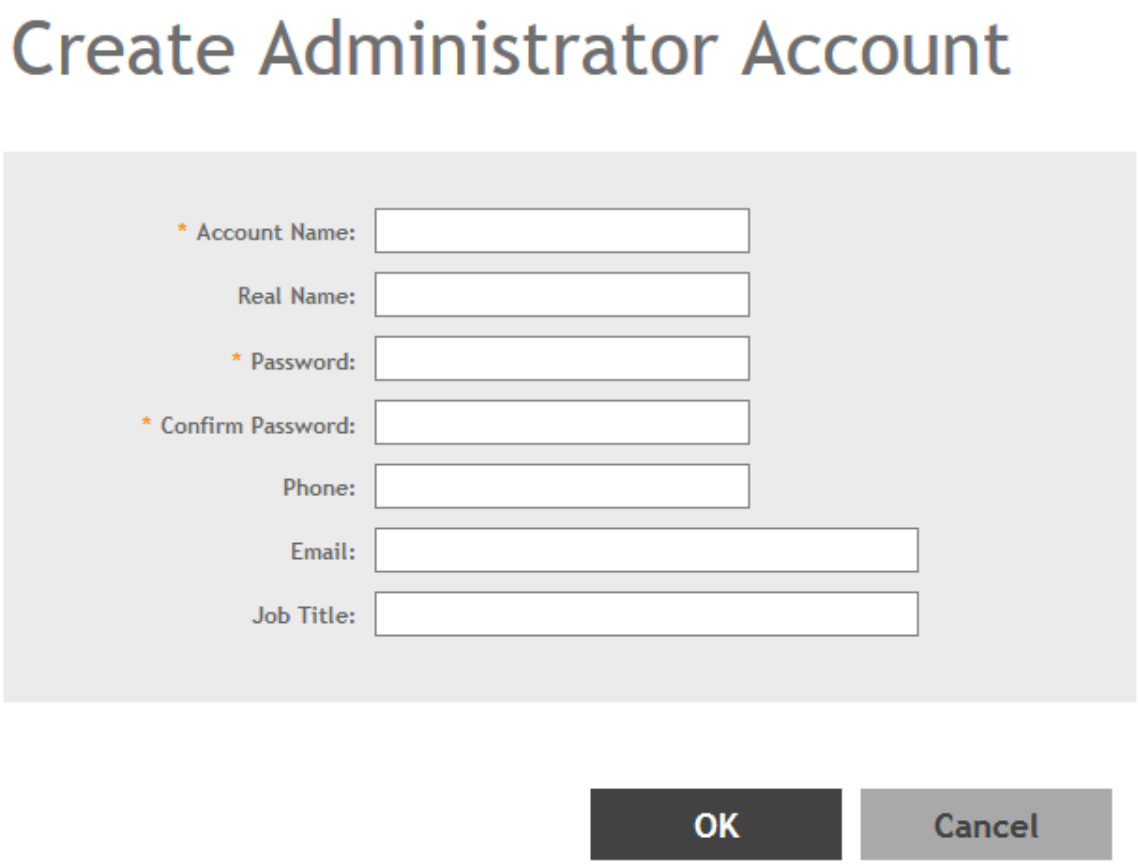
The controller supports the creation of additional administrator accounts. This allows you to share or delegate management and monitoring functions with other members of your organization. You can also modify the status of the administrator account by locking or unlocking it.

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

3. Click **Create**.

   The **Create Administrator Account** page appears.

   FIGURE 336 Creating an Administrator Account



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**.

You have created the administrator account.

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

NOTE
Administrator users mapped to different domain other than system domain have to login using accountname@domain as the User.

Unlocking an Administrator Account

When multiple user access authentications fail, the administrator account is locked. A super administrator 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 login as a super administrator 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 Administrator Accounts

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

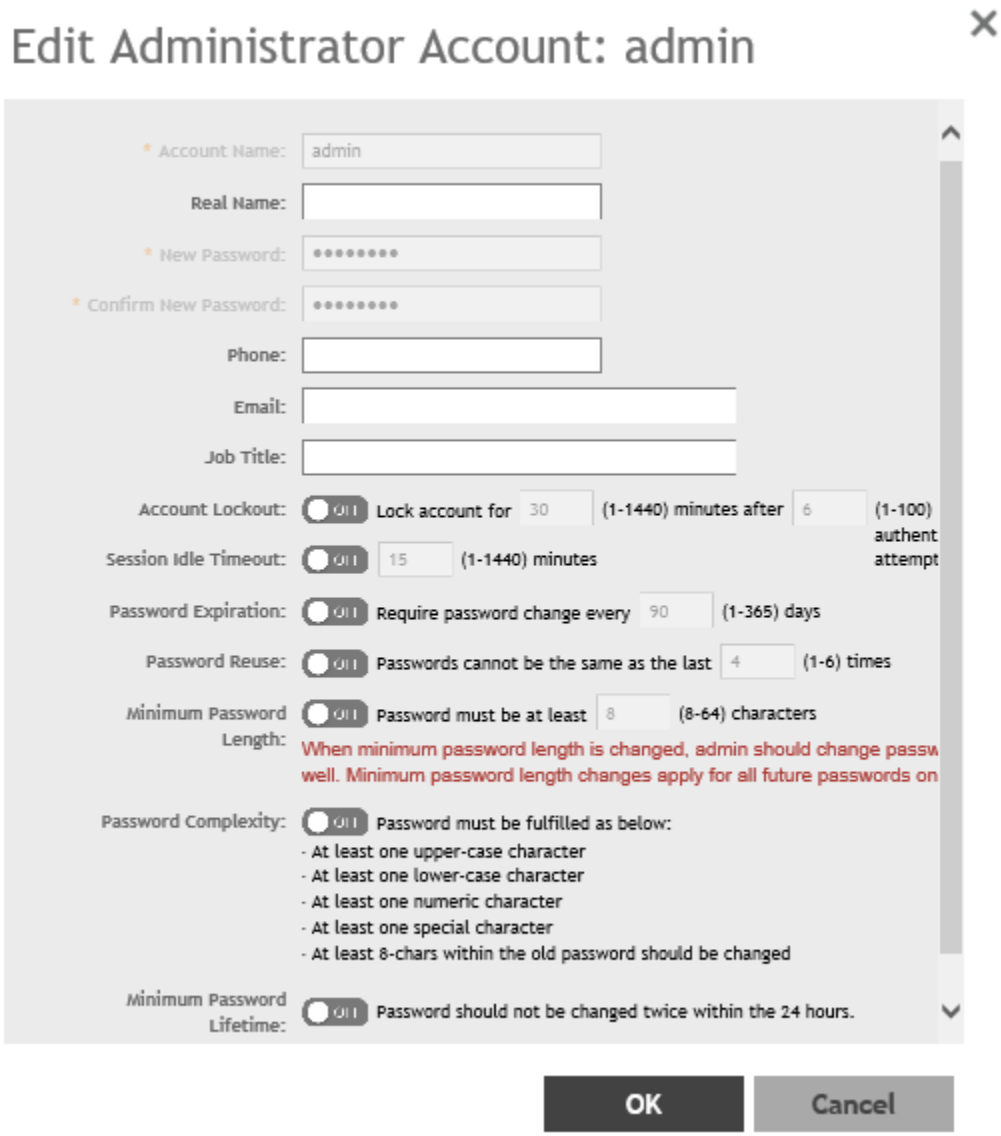
You must log in as a **System Default Super Admin** to set the rules.

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.

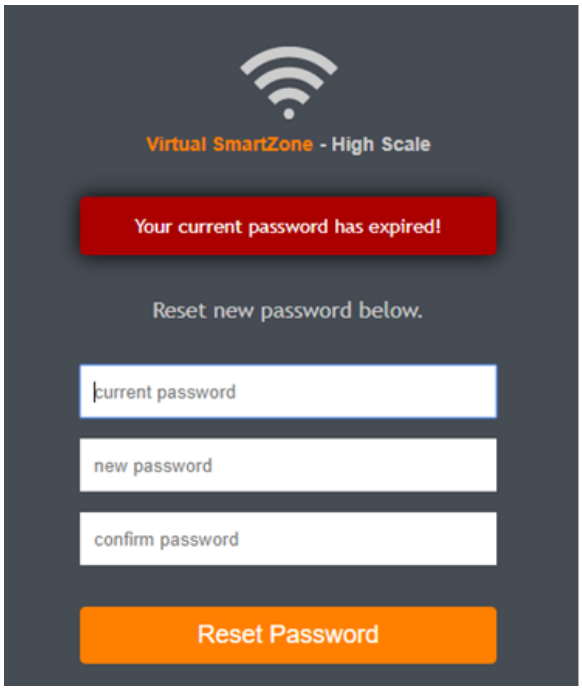
FIGURE 337 Configuring an Administrator Account



4. Configure the following:
   - Real Name: Type the name of the administrator.
   - Phone: Type the phone number.
   - Email: Type 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 in order 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 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 will be prompted to change or reset your password as soon as you login. Reset the password as shown in the figure.

     FIGURE 338 Resetting the old 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 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 changed

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

5. Click **OK**.

   The **Password Confirmation** page is displayed.
6. Enter the **Password**.
7. Click **OK** to apply the new configuration.

You have configured an administrator account.

Working with AAA Servers

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

Configuring SZ Admin AAA Servers

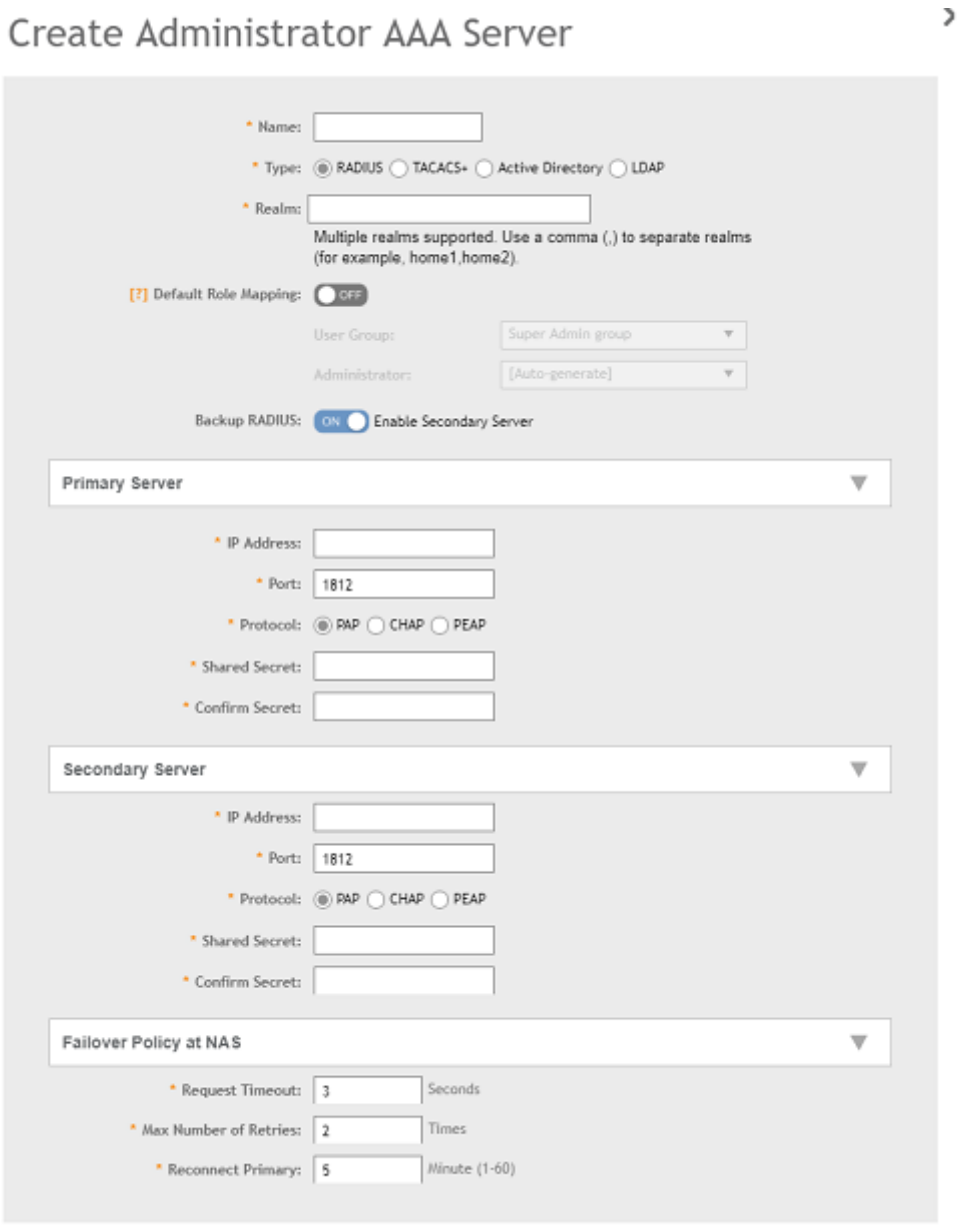
To add and manage AAA servers that the controller can use to authenticate users, complete the following steps.

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

2. From **AP AAA Servers**, click **Create**.

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

   FIGURE 339 Creating an Administrator AAA Server



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. For **Backup RADIUS**, select **Enable Secondary Server** if a secondary RADIUS server exists on the network. Refer to step 9 for configuration settings.

8. Under **Primary Server**, configure the settings of the primary AAA server.
   - **IP Address**: Enter the IP address of the AAA 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 protocol PEAP and PAP, 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.
   - **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.
9. Under **Secondary Server**, configure the settings of the secondary RADIUS server.
   - **IP Address**: Enter the IP address of the AAA 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 protocol PEAP and PAP, 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, and delete the server by selecting the options **Configure**, **Clone**, and **Delete**, respectively, from the **Administrator** tab.

Testing SZ Admin AAA Servers

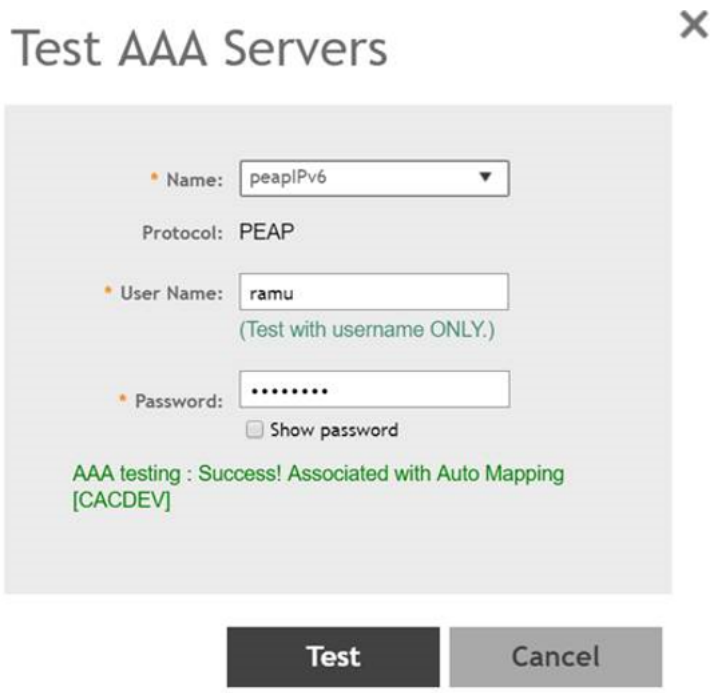
To ensure that the controller administrators are able to authenticate successfully with the RADIUS server type that you selected, RUCKUS strongly recommends testing the AAA server after you set it up.

The test queries the RADIUS server for a known authorized user and return groups associated with the user that can be used for configuring roles within the controller.

1. Select **Administration** > **Admins & Roles** > **AAA**.
2. Select the created AAA server and click **Test AAA**.

   An example for testing a RADIUS server is shown.

   FIGURE 340 Testing an AAA Server: RADIUS



   The **Protocol** field is displayed only for RADIUS server that depends on the SZ AAA server configuration.
3. In the **Name** field, select the AAA server that you created.
4. In the **User Name** field, enter an existing user name that is associated to a user group.

   NOTE
   For TACACS+ server, test with username appended with configured service.

5. In the **Password** field, enter password for the user name you specified.
6. Click **Test**.

If the username is associated with an user group, the following message is displayed: "AAA testing: Success! Associated with Auto Mapping". If the username is not associated with any user group, the following message is displayed: "AAA testing: Success! No SZ User or Default role mapping associated".

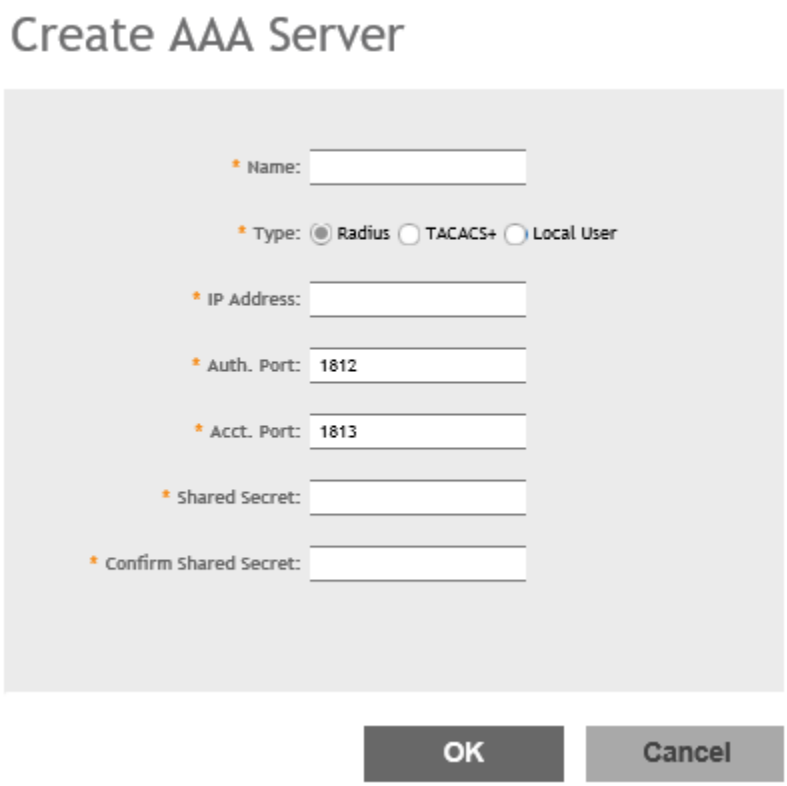
Configuring Switch AAA Servers

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. From **Switch AAA Servers**, click **Create**.

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

   FIGURE 341 Creating a Switch AAA Server



3. Enter the AAA server name.
4. For **Type**, select the type of AAA server to authenticate users:
   - **RADIUS**
   - **TACACS+**
   - **Local User**
5. Enter the following information:
   - **IP Address**: Enter the IP address of the AAA server.
   - **Auth Port**: Enter the authentication port that the server is using.
   - **Acct Port**: Enter the accounting port that the server is using.
   - **Shared Secret**: Enter the shared secret.
   - **Confirm Shared Secret**: Re-enter the shared secret to confirm.
6. Click **OK**.

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

NOTE
ICX switch fails to delete the TACACS+ and Radius AAA servers when pushed from the SZ or vSZ if SNMP query is disabled in the switch or if this is a pre-configured switch before joining SZ or vSZ.

Configuring Switch AAA Server Settings

To configure and manage AAA servers, complete the following steps.

1. Select **Administration** > **Administration** > **Admins and Roles** > **AAA** .
2. From **Switch AAA Setting** configure the following.

   Login Athentication

   - **SSH Authentication**: Enable the option for secure authentication.
   - **Telnet Authentication**: Enable the option to set Telnet authentication. This option requires SSH authentication to be enabled.
   - **First Pref**: Select the first preferred authentication system.
   - **Second Pref**: Select the second preferred authentication system.
   - **Third Pref**: Select the third preferred authentication system.

   Authorization

   - **Command Authorization**: Enable this option to assign the following authorization services:
     - **Level**: Select the required privilege: **Port Config**, **Read Only**, or **Read Write**.
     - **Server 1**: Select the authorization method for the first server.
     - **Server 2**: Select the authorization method for the second server.
   - **Exec Authorization**: Enable this option to authorize the user to access the privilege mode.
     - **Server 1**: Select the authorization method for the first server.
     - **Server 2**: Select the authorization method for the second server.

   Accounting

   - **Command Accounting**: Enable this option to track the following accounting services:
     - **Level**: Select the required privilege: **Port Config**, **Read Only**, or **Read Write**.
     - **Server 1**: Select the tracking method for the first server.
     - **Server 2**: Select the tracking method for the second server.
   - **Exec Accounting**: Enable this option to track the services in the privilege mode.
     - **Server 1**: Select the tracking method for the first server.
     - **Server 2**: Select the tracking method for the second server.
3. Click **OK**.

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 SZ Admin AAA Servers on page 595.

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 590. 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 587.

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

   NOTE
   Refer to Configuring SZ Admin AAA Servers on page 595.

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 590.

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 590.

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 587.

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

   NOTE
   Refer to Configuring SZ Admin AAA Servers on page 595.

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

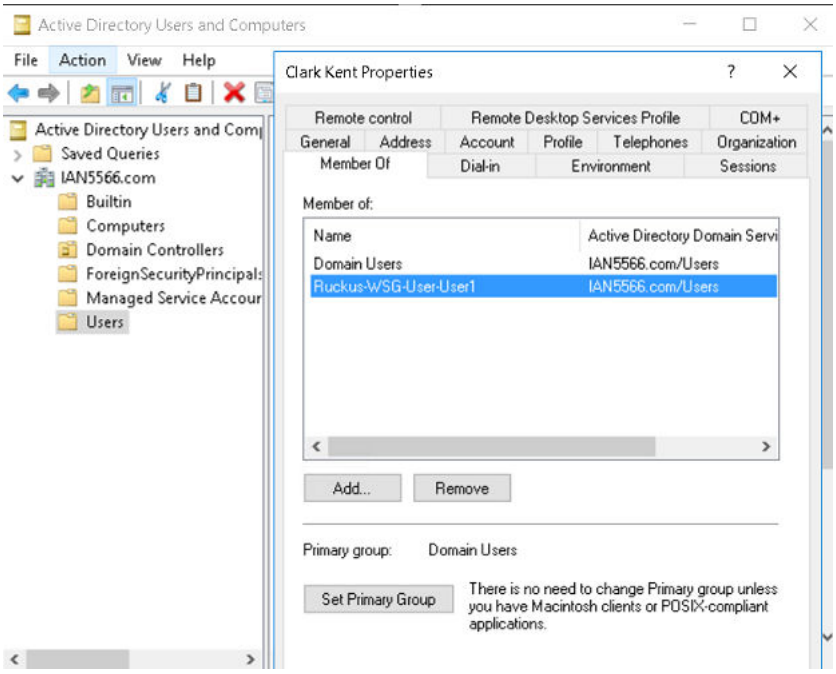
About Active Directory (AD) Support

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 342 About AD 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 590. In this example, AD 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 587 .

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

   NOTE
   Refer to Configuring SZ Admin AAA Servers on page 595.

5. 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 590.

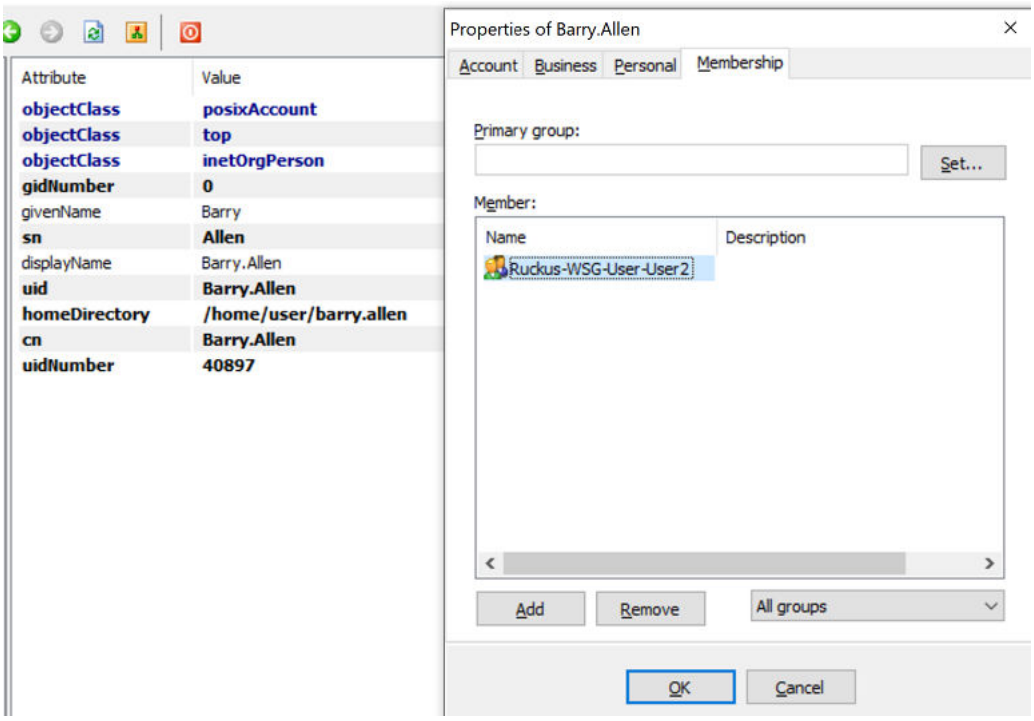
About LDAP Support

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.

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

   FIGURE 343 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 590. 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 587.

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

   NOTE
   Refer to Configuring SZ Admin AAA Servers on page 595.

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

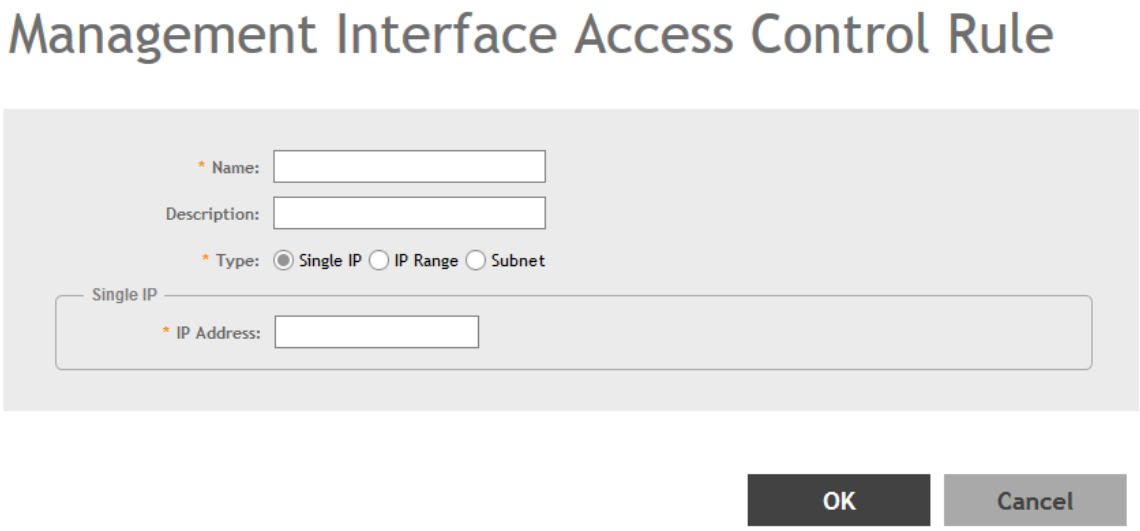
   NOTE
   The value of super-login depends on the realm configured for the AAA profile. Refer to Creating Administrator Accounts on page 590.

Enabling the Access Control List

You can control access to management interfaces from CLI or SSH.

1. Go to **Administration** > **Administration** > **Admins and Roles**.
2. Select the **Access Control List** tab.
3. Select **Enable**.
4. Click **Create**.
   The **Management Interface Access Control Rule** page appears.

FIGURE 344 Management Interface Access Control Rule



5. Configure the following:
   a. Name: Type the name that rule you want to create to access the management interface.
   b. Description: Type a short description for the rule.
   c. Type: Select one of the following
      - Single IP: Type the IP address of the interface that can be accessed per this rule.
      - IP Range: Type the range of IP address that will be allowed access.
   d. Subnet: Type the network address and subnet mask address of the interface that will be allowed access.
   e. Click **OK**.

You have created the access control list rule.

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

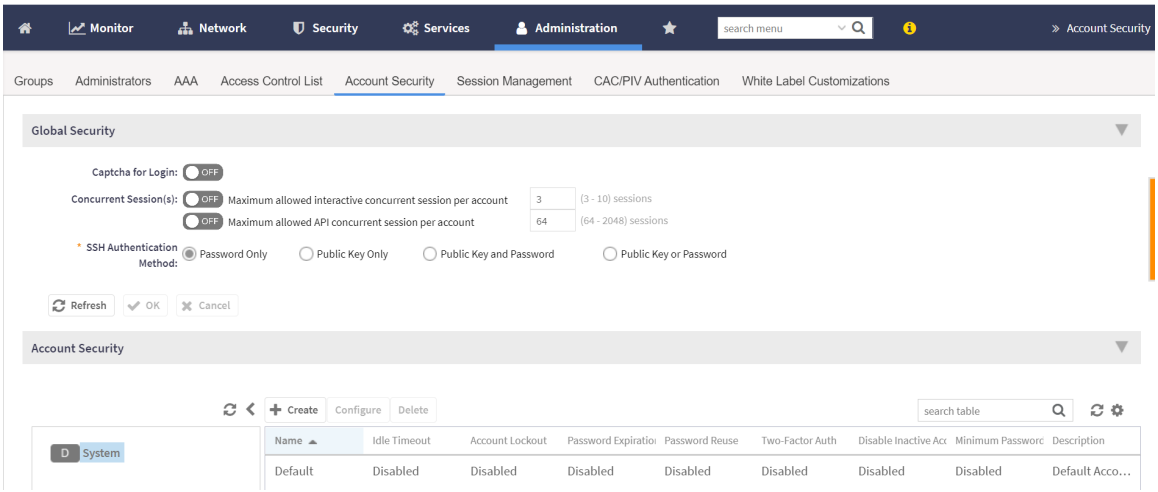
Creating Account Security

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

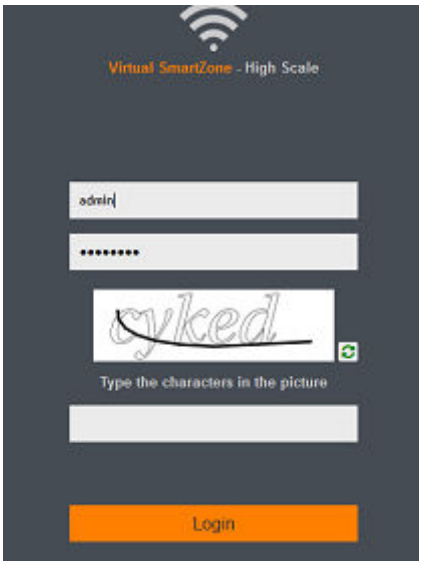
   The **Global Security** section and **Account Security** section is displayed.

FIGURE 345 Account Security page



3. From Global Security, configure the following:
   a. Captcha for Login: select the option to enable Captcha for login. 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 login to the web interface, the captcha characters are displayed in the login page as shown.

      FIGURE 346 Captcha enabled in the login page

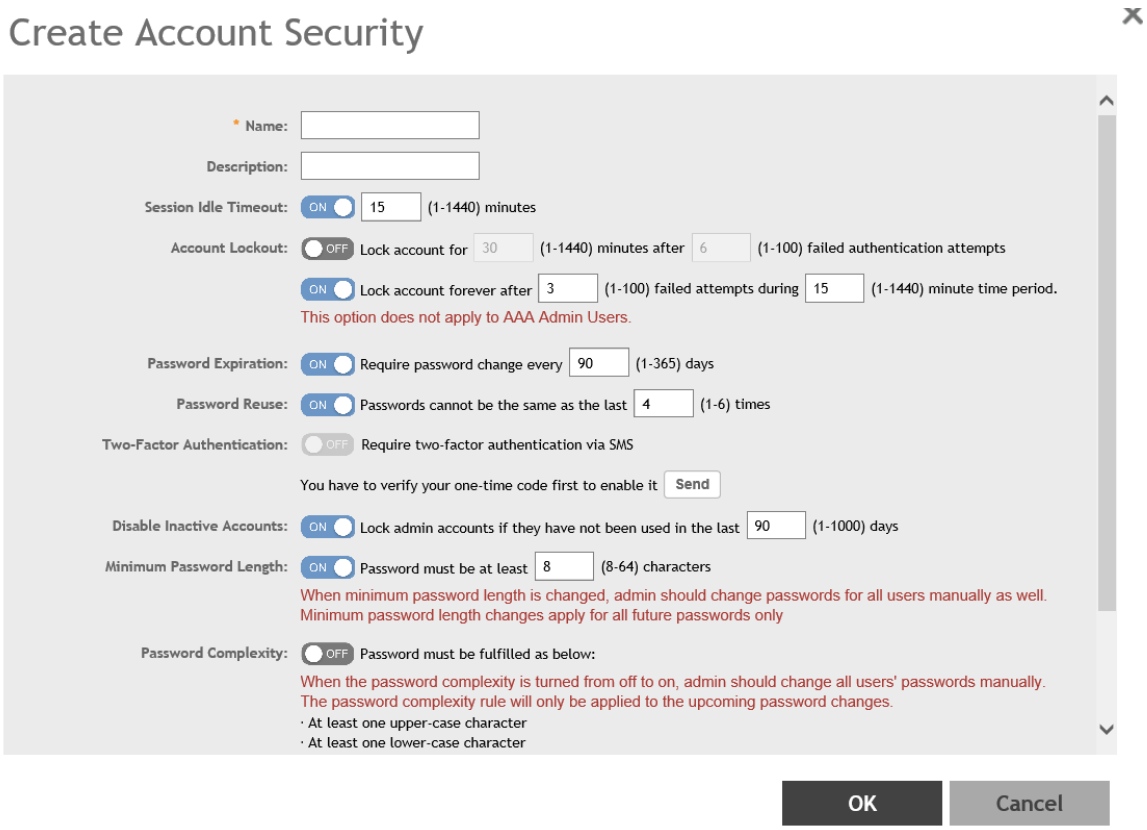
      

      Type the characters as shown in the captcha picture and login. The characters in the captcha image are case sensitive and can be refreshed if not clear.
   b. Concurrent sessions: Click the required options and enter the number of sessions allowed:
      - **Maximum allowed interactive concurrent session per account**
      - **Maximum allowed API concurrent sessions per account**
   c. Click **OK**.

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

   The **Create Account Security** page appears.

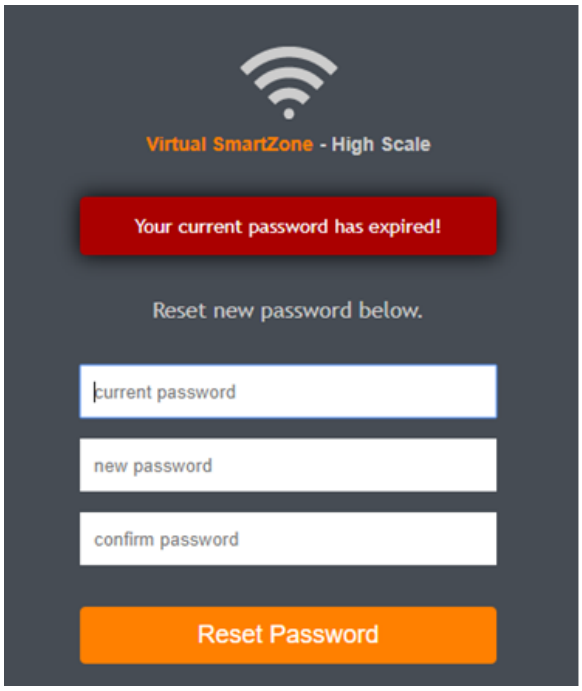
FIGURE 347 Creating Account Security



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 will be prompted to change or reset your password as soon as you login. Reset the password as shown in the figure.

     FIGURE 348 Resetting the old 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).
   - 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.

- 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 changed

  Select the option.
- 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.

You have created the account security profile.

NOTE
You can also edit and delete the profile by selecting the options **Configure** and **Delete** respectively, 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 above 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 which identifies the SZ 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 Ruckus support (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.

FIGURE 349 Sample Session Termination for Web Interface Session.

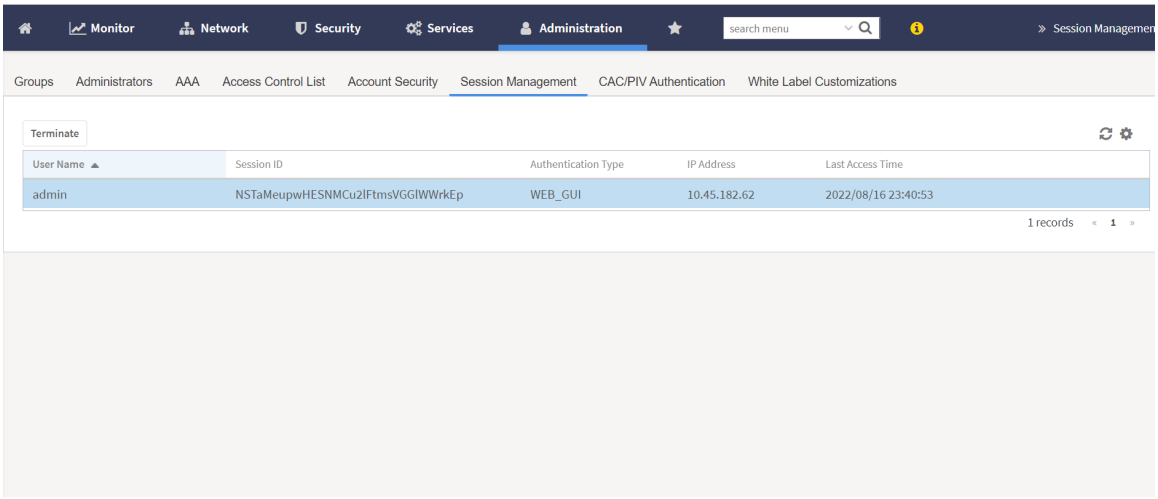
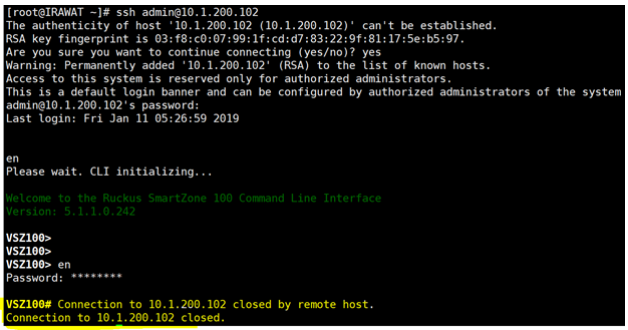
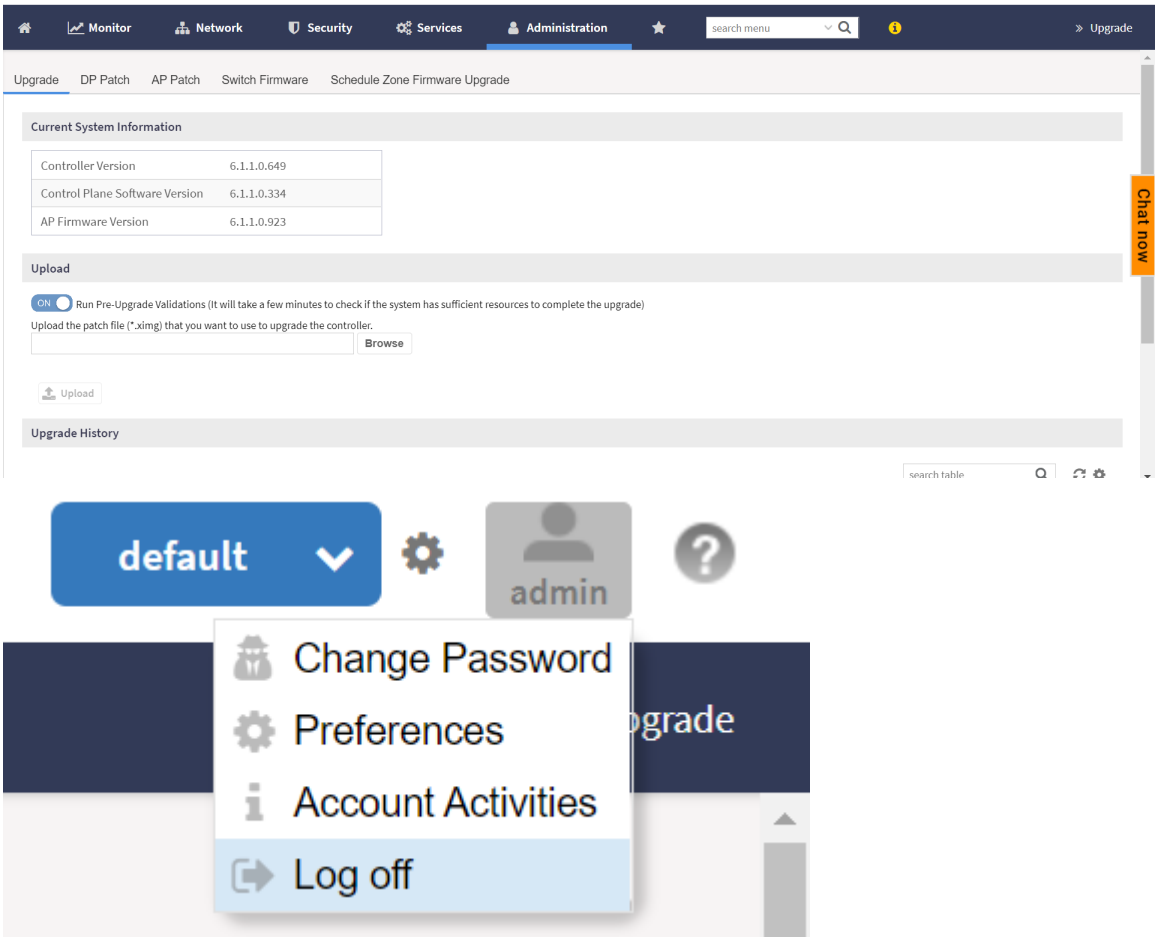


FIGURE 350 Sample Session Termination for CLI Session.



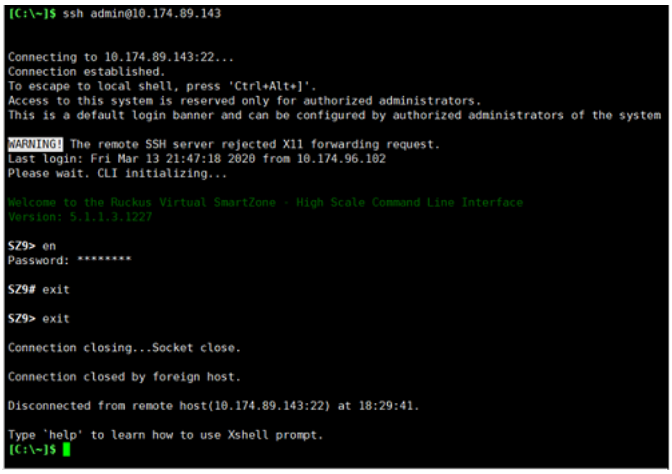
4. Click the **Admin** icon in the upper right corner and select log off from the drop-down list.

FIGURE 351 Logging out from the UI



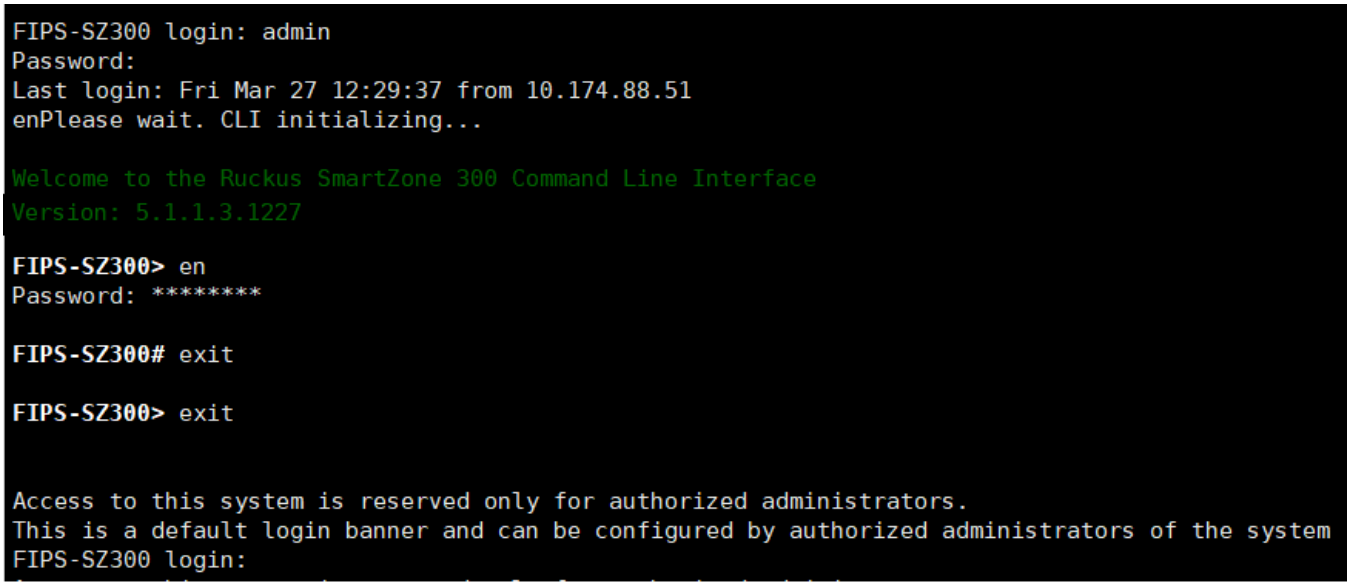
5. You can also logout by typing "exit" command in the SSH session.

   FIGURE 352 Logging out from the SSH session



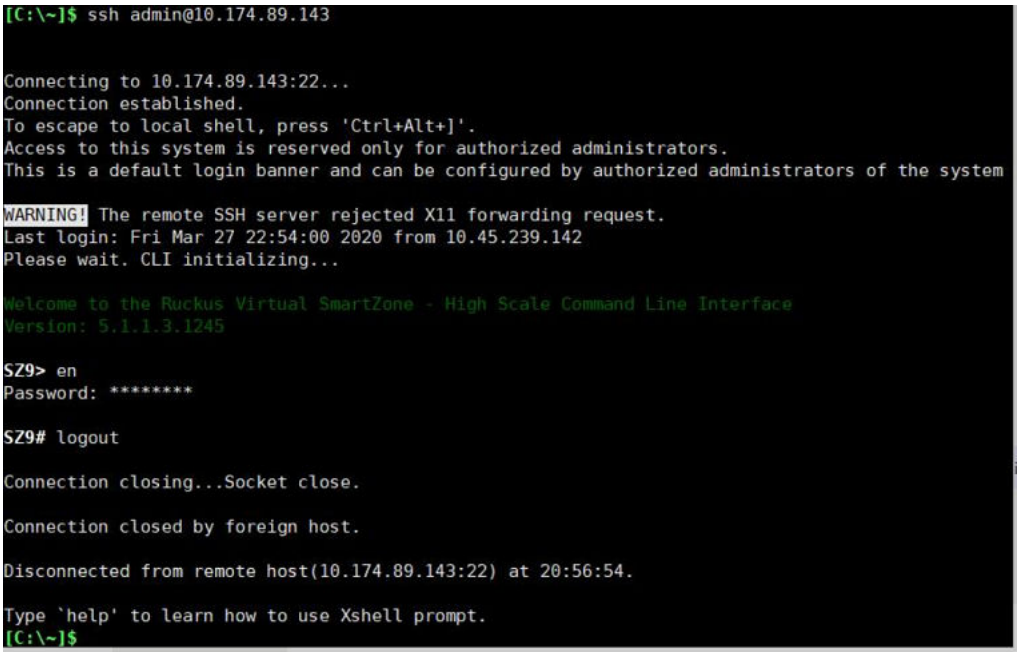
6. You can also logout by typing " exit" command at the console prompt.

   FIGURE 353 Logging out using the console prompt



7. You can also logout by typing "logout" at the CLI prompt

FIGURE 354 Logging out using CLI prompt



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.

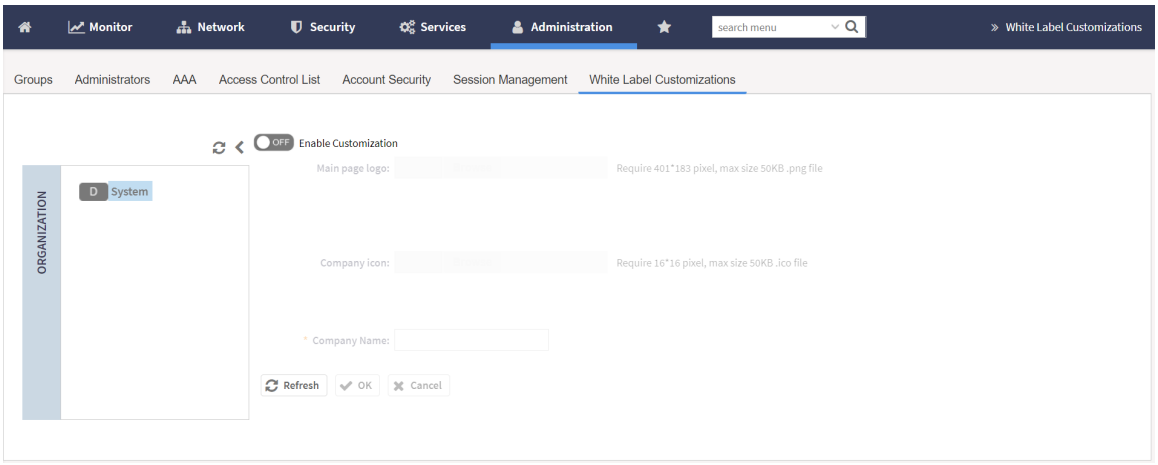
1. From the **Dashboard**, Click the **Administration** tab.
2. From **Administration,** select **Admins and Roles**.
3. Click the **White Label Customizations** tab.

4. Set the **Enable Customization** button 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.

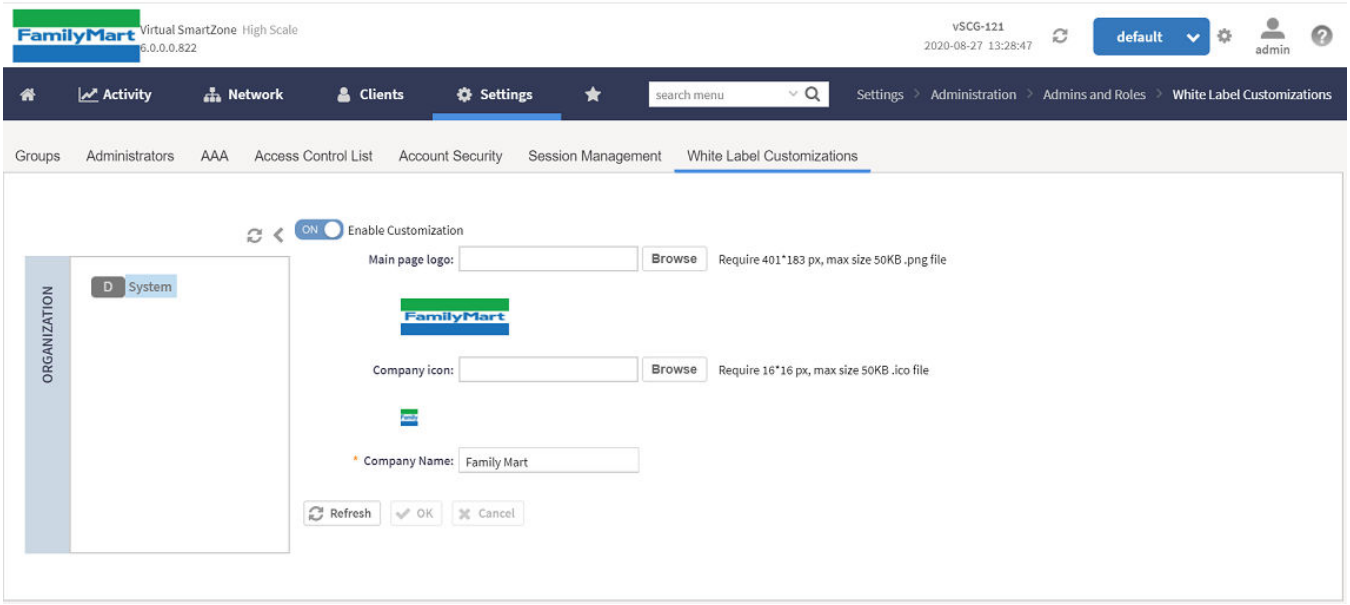
FIGURE 355 Enabling White Label Customization



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

   Clicking **OK** accepts the changes and the company logo is changed, as shown in the following figure.

FIGURE 356 New Logo Replaces Initial Logo



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

Backup and Restore

Cluster

Administrating the Cluster

SmartZone Cluster Mode

SmartZone system state has two cluster modes.

The two cluster modes are -

- Crash mode
- Suspend mode

Crash mode

The system cluster enters this mode when system meets unexpected error during fresh install or reboot flow. The system runs into ir-recoverable error and should be set to reset-factory settings.

System enters into *Crash mode* in any one of the below conditions:

1. System reboot with environment inconsistency.
    a. Model
    b. Port group (SZ 100)
    c. Firmware Version
2. Fresh install fail.
3. Join cluster fail.

Suspend mode

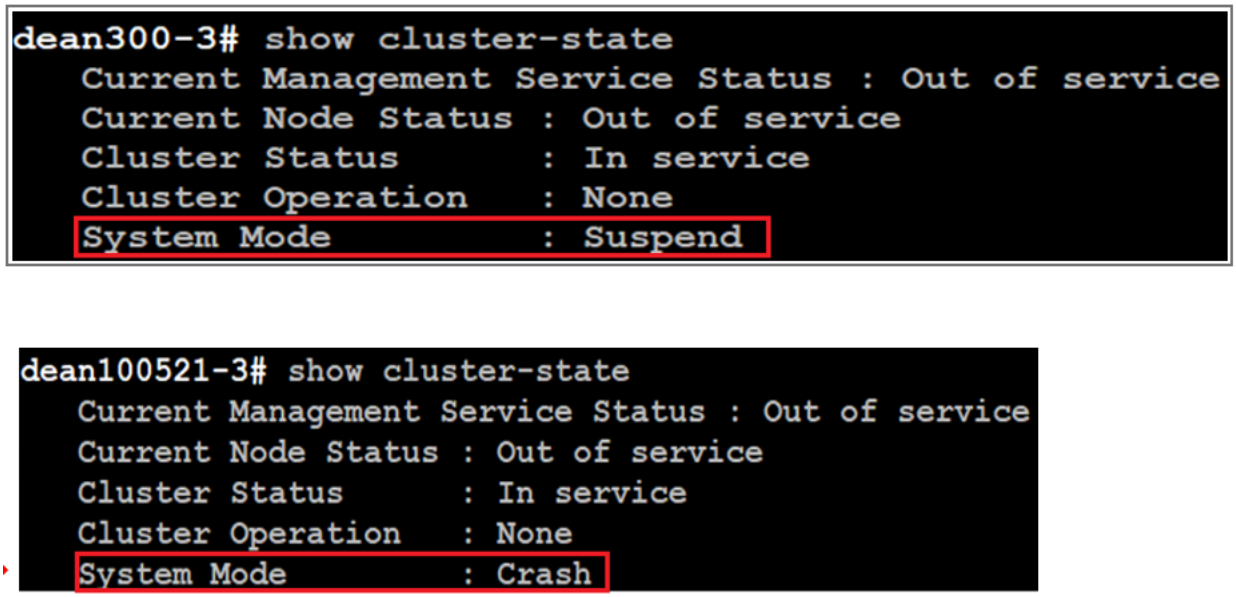
The system enters this mode if there is an environment error during reboot flow. The configurer sets up suspend flag and stops all applications. The system can be recoved by rebooting as it is a temporary fail.

System enters into *Suspend mode* in any one of the below conditions:

1. Platform applications cannot be launached successfully.
2. Failed on membership authentication in cluster .

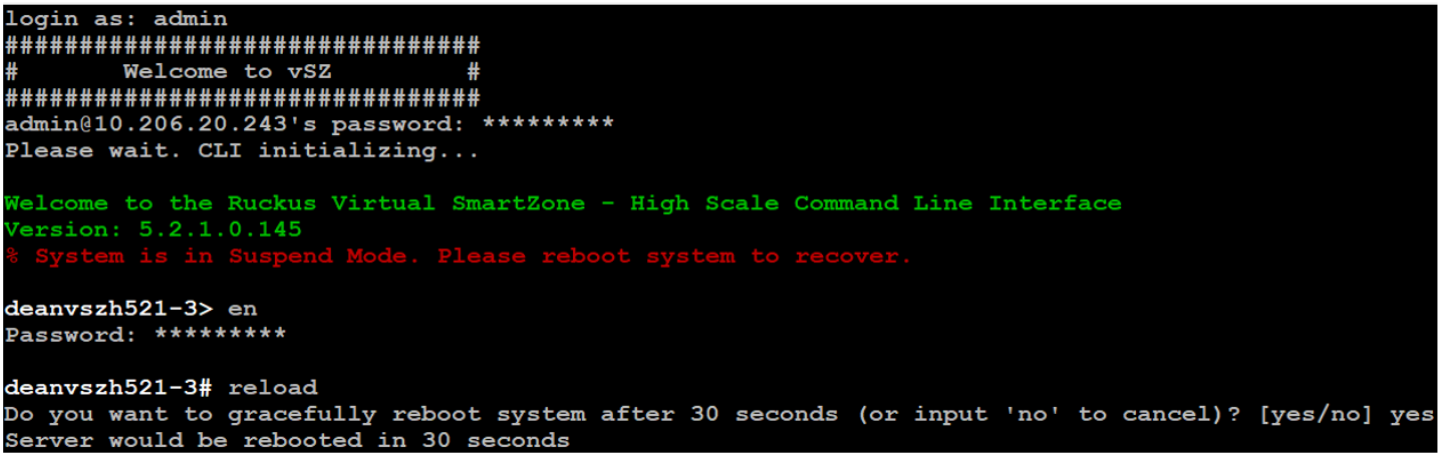
To check status of the cluster state, use **show cluster state** command.

FIGURE 357 Crash and Suspended modes



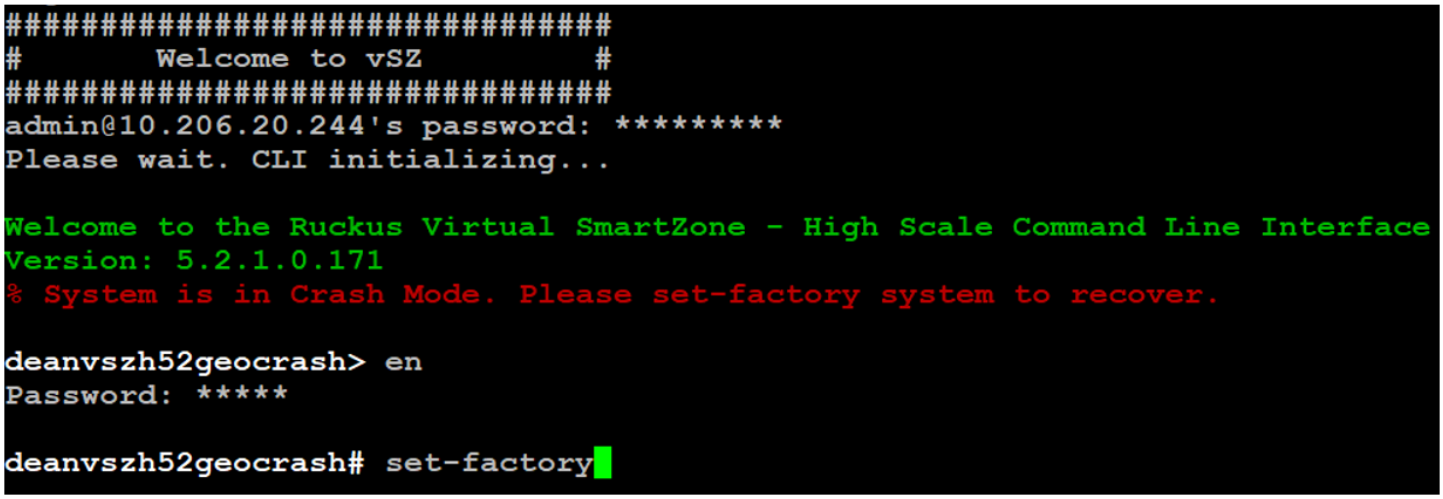
To recover system in case of *Suspend mode*, use **reload** command. System automatically detects suspend flag and clears before launching applications.

FIGURE 358 reload



To reset system to factory settings in case of *Crash mode*, use **set-factory** command.

FIGURE 359 set-factory



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, ilt 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.

Disaster Recovery

Creating cluster backup and restoring cluster configurations periodically helps manage disaster recovery.

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 118 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			

TABLE 118 Contents of a cluster configuration backup file (continued)

Configuration Data	Administration Data	Report Data	Identity Data
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**.

You have completed configuring the controller to create a backup automatically.

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.

You have completed configuring the controller to export the configuration backup file to an FTP server.

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.

You have completed downloading a copy of the configuration backup.

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.
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.

You have completed restoring a system configuration backup file.

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 appears: `Are you sure you want to back up the cluster?`
4. Click **Yes**.

   The following message appears: `The cluster is in maintenance mode. Please wait a few minutes.`

   When the cluster backup process is complete, a new entry appears 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 **Administration** > **Administration** > **Backup and Restore**.
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.

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.

You have completed restoring the cluster backup.

Replacing a Controller Node

Replacing a Controller Node in Multi-Node Cluster

This section describes how to replace a controller node in a multi-node cluster. Removing a node and joining a new node is the standard process to replace a node.
Step 1: Wipe-out Upgrade Controller Node

If the Controller node does not match with the existing cluster version, prepare a new Controller and wipe-out upgrade to the same version of the running cluster. See Performing a Wipe-out Upgrade for Controller Node on page 624.
Step 2: Remove RMA Controller Node

Choose a controller that will remain in the cluster and follow the steps:

1. Log on to the web interface of the chosen controller using administrator credentials.
2. Go to **Network** > **Data and Control Plane**>**Cluster** and locate the node that you want to replace in the cluster planes.

   NOTE
   For SmartZone 5.2.1 or earlier releases, select **System** > **Cluster**.

3. Click **Delete** to remove the node from the cluster.

Step 3: Join the New Controller Node

To join the new controller into the running cluster:

1. Prepare a proper version of the controller by wipe-out upgrade. See Performing a Wipe-out Upgrade for Controller Node on page 624.
2. Set up the node as a new controller, and then join the existing cluster. For step by step instructions, refer to the *Getting Started Guide*.

Replacing a Controller Node in Single Node Cluster

This section describes how to replace a controller node in single node cluster. Original configuration backup and a new node are required.
Step 1: Wipe-out Upgrade Controller Node

If the Controller node does not match with the existing cluster version, prepare a new Controller and wipe-out upgrade to the same version of the running cluster. See Performing a Wipe-out Upgrade for Controller Node on page 624.
Step 2: Join New Controller Node

Set up the node as a new controller. For step by step instructions, see the *Getting Started Guide*.
Step 3: Configuration Restore

With original configuration backup follow the steps to restore the configuration in cluster:

1. Prepare the new controller to which you will restore the cluster backup.
   a. Either obtain a new controller or factory reset an existing controller.
   b. Log on to the controller as a system administrator.
   c. Run the setup command to configure the controller's network settings.
   d. Complete the controller setup process from the **CLI**.
2. After you complete the controller setup, log on to the controller web interface as a system administrator.
3. Go to **Administration** > **Administration**>**Backup and Restore**.

   NOTE
   For SmartZone 5.2.1 or earlier releases, select **Administration** > **Backup and Restore**.

4. Select the **Configuration** tab.
5. Click **Upload**. After the configuration file is uploaded successfully, it appears in the Configuration section.
6. Restore the configuration backup to the node either using the web interface or the **CLI**.
   - To use the web interface:
     a. Go to **Administration** > **Backup and Restore** page.
     b. In the **Configuration** tab, locate the configuration backup file that you want to restore.
     c. Click **Restore**.
     d. Follow the prompts (if any) to complete the restore process.
   - To use the **CLI**:
     a. Log on to the **CLI** of the node as a system administrator.
     b. Run the **restore config** command.

Performing a Wipe-out Upgrade for Controller Node

If the firmware version on this controller (shown in the Cluster Information page) does not match the firmware version for new cluster setup or join an existing, a message appears and prompts you to upgrade the controller's firmware. Click **Upgrade**, and then follow the prompts to perform the upgrade.

NOTE
Refer Cautions & Limitations of Administrating a Cluster on page 647 for more information.

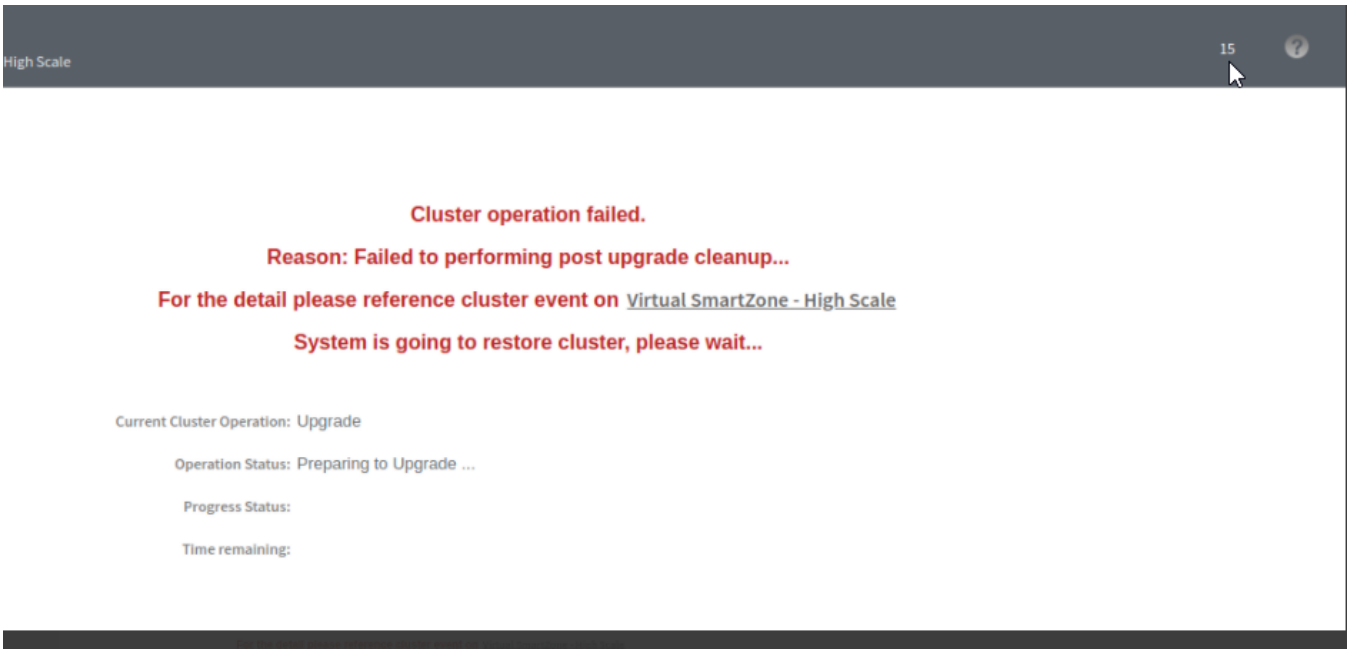
- For controller running firmware version 5.1 or later can do wipe-out upgrade successfully to greater than 5.1.
- For controller running firmware version earlier than 5.1, apply a KSP patch to make wipe-out upgrade successful Contact Ruckus support to receive a KSP patch to apply the patch from CLI.

Restoring a Cluster Automatically on Upgrade Failure

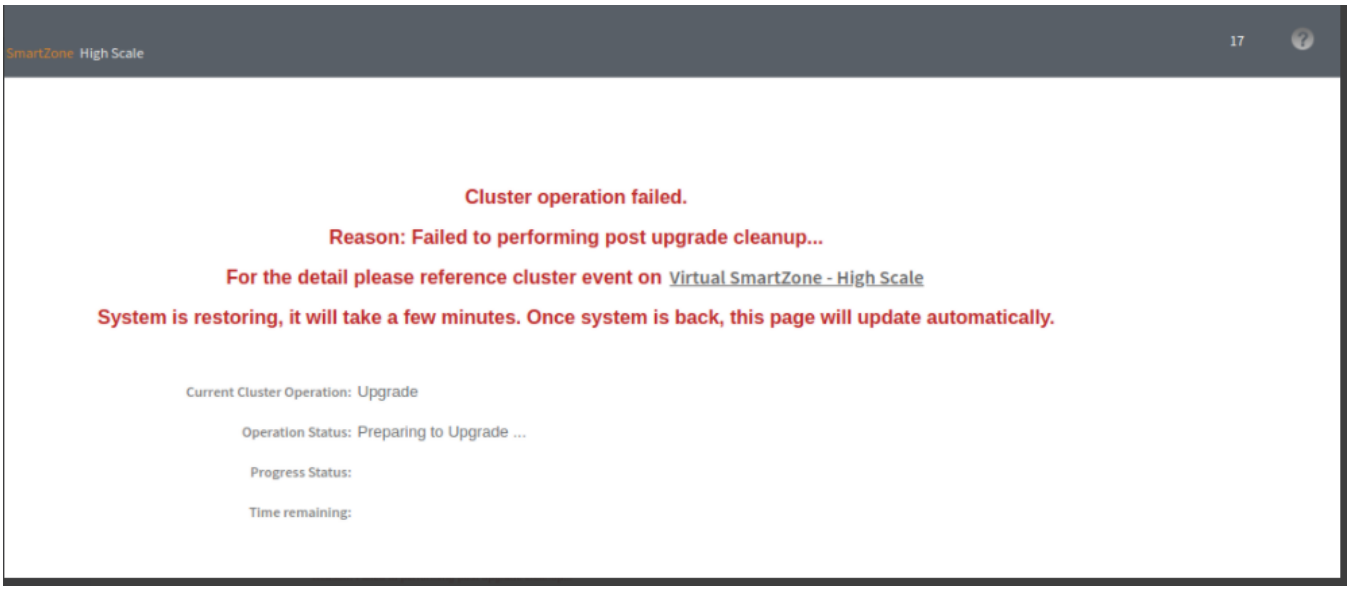
When cluster upgrade fails in the middle, the system will automatically restore the cluster with the backup file prepared in the beginning of the upgrade process and goes back to previous version of the image. The user does not need to manually restore the cluster.

When the cluster fails to upgrade and a restore action is triggered, the system performs the following process:

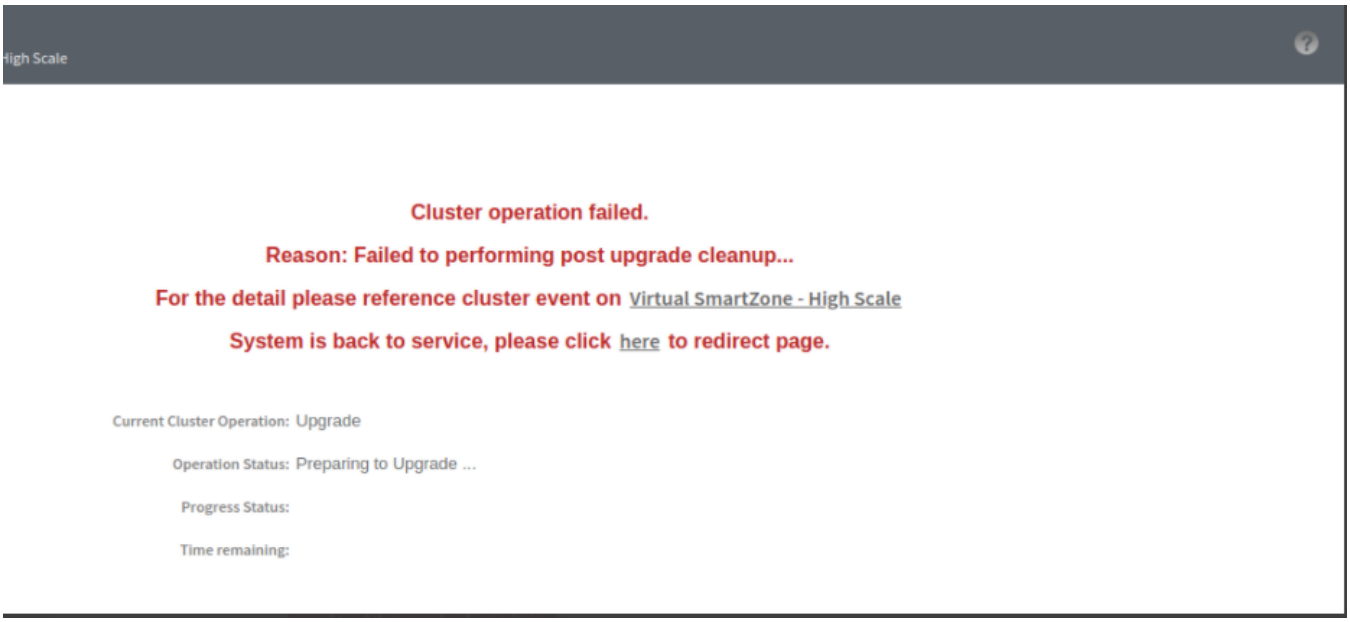
- **FIGURE 360** Starting a restore process



- **FIGURE 361** Restoring cluster



- **FIGURE 362** Cluster back to service



Configuration

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 additional 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.

Backing Up Configuration

There are two methods you can use to back up the controller configuration:

Backing Up Configuration from the CLI

There are two methods you can use to back up the controller configuration either using the web interface or CLI (Command Line Interface).

Follow these steps to back up the controller configuration from the **CLI**.

1. Log on to the controller **CLI** as a system administrator.
2. Run the **enable** command to enable privileged mode on the **CLI**.

```
ruckus> enable
Password: ********
ruckus#
```

3. Run the **backup config** command to start backing up and transferring the node configuration to an FTP server.

```
ruckus# backup config <ftp-username> <ftp-password> <ftp-server-address> <ftp-server-port>
Do you want to backup configuration (yes/no)? yes
Backup Configuration process starts
Backup Configuration process has been scheduled to run. You can check backup version using 'show
backup-config'
```

4. Run the **show backup-config** command to verify that the backup file has been created.

You have completed backing up the controller node to an external FTP server.

Backing Up Configuration from the Web Interface

1. For information on how to back up the controller configuration to an external FTP server automatically, see Backing up Cluster Configuration on page 619.
2. In **Auto Export Backup**, click **Enable**.
3. In FTP Server, select the FTP server to which you want to export the backup file.
4. 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, the following message appears: `FTP server connection established successfully`.

   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.
5. After you verify the controller is able to connect to the FTP server successfully, click **OK** to save the FTP server settings.

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.
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.

You have completed restoring a system configuration backup file.

Backing Up and Restoring the Controller's Network Configuration from an FTP Server

In addition to backing up and restoring the controller's network configuration from its own database, the controller supports backup and restore of its network configuration from an FTP server using the CLI.

This section describes the requirements for backing up and restoring the controller's network configuration from an FTP server, the information that is included in the backup file, and how to perform the backup and restore process.

To back up and restore the controller's network configuration from an FTP server, the controller must have already been set up and in service. In case of a multi-node cluster, all the nodes in the cluster must be in service.

The following table lists the network configuration that is backed up from the control and data planes when you perform a backup procedure to an FTP server.

TABLE 119 Information that is backed up to the FTP server

Control Plane	Data Plane
• Control interface • Cluster interface • Management interface • Static routes • User-defined interfaces	• Primary interface • Static routes • Internal subnet prefix

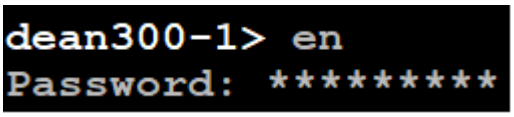
Backing Up to an FTP Server

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.

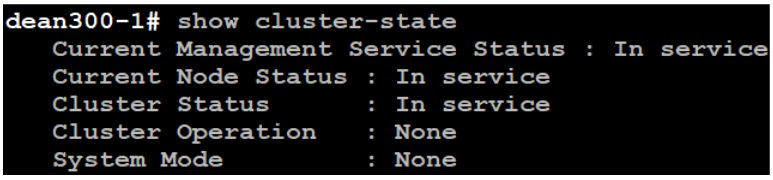
   FIGURE 363 Enable privileged mode



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.

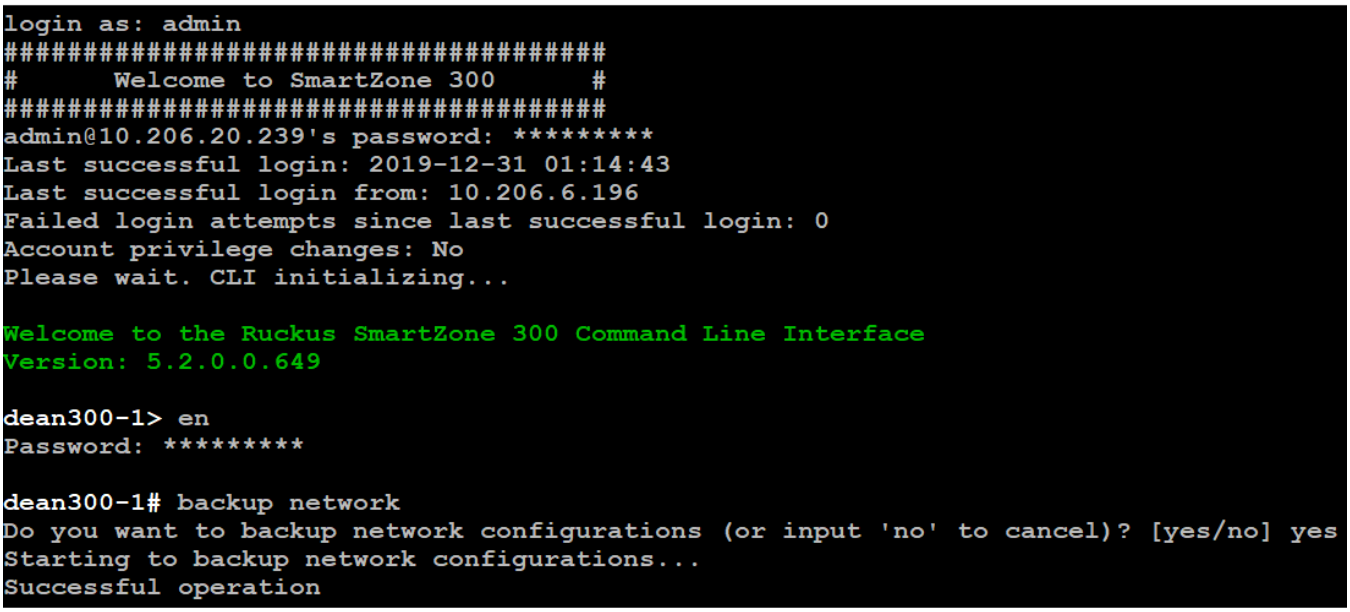
   FIGURE 364 Verify that both the node and the cluster are in service



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 365 Run backup network



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 366 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.

7. 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
```

   FIGURE 367 `Succeed to copy to remote FTP server` indicates that you have exported the backup file to the FTP server successfully

```
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
```

8. 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.

You have completed backing up the controller to an 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:

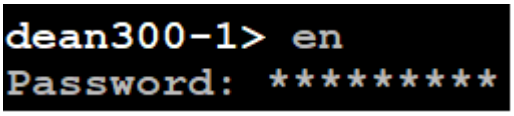
- Only release 2.1 and later support restoring from an FTP server.
- In this current release, restoring the entire cluster from an FTP server is unsupported. The restore process must be performed on one node at a time.
- Restoring from an FTP server can only be performed using the **CLI**.

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.

1. Log on to the controller from the **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.

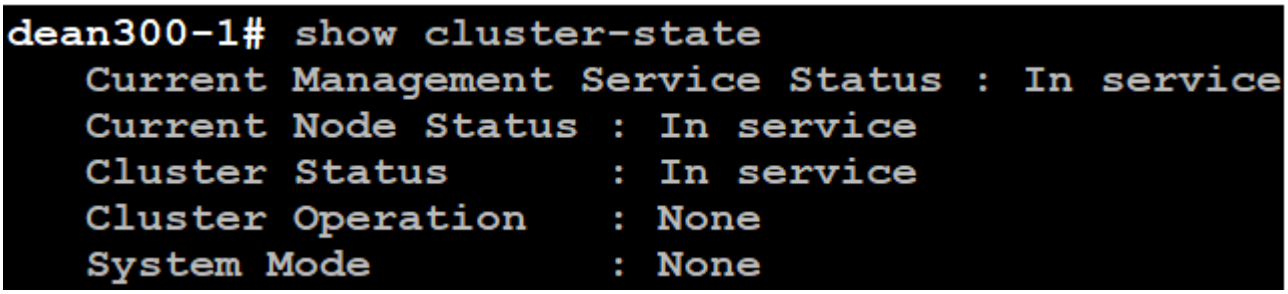
   FIGURE 368 Enable privileged mode

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 369 Verify that both the node and the cluster are in service

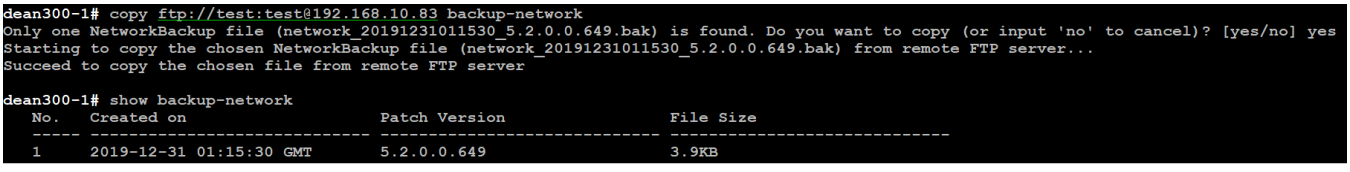
4. Enter the following command to log on to the FTP server and check for available backup files that can be copied to the controller:

   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 370 Verify that the backup file was copied to the controller successfully

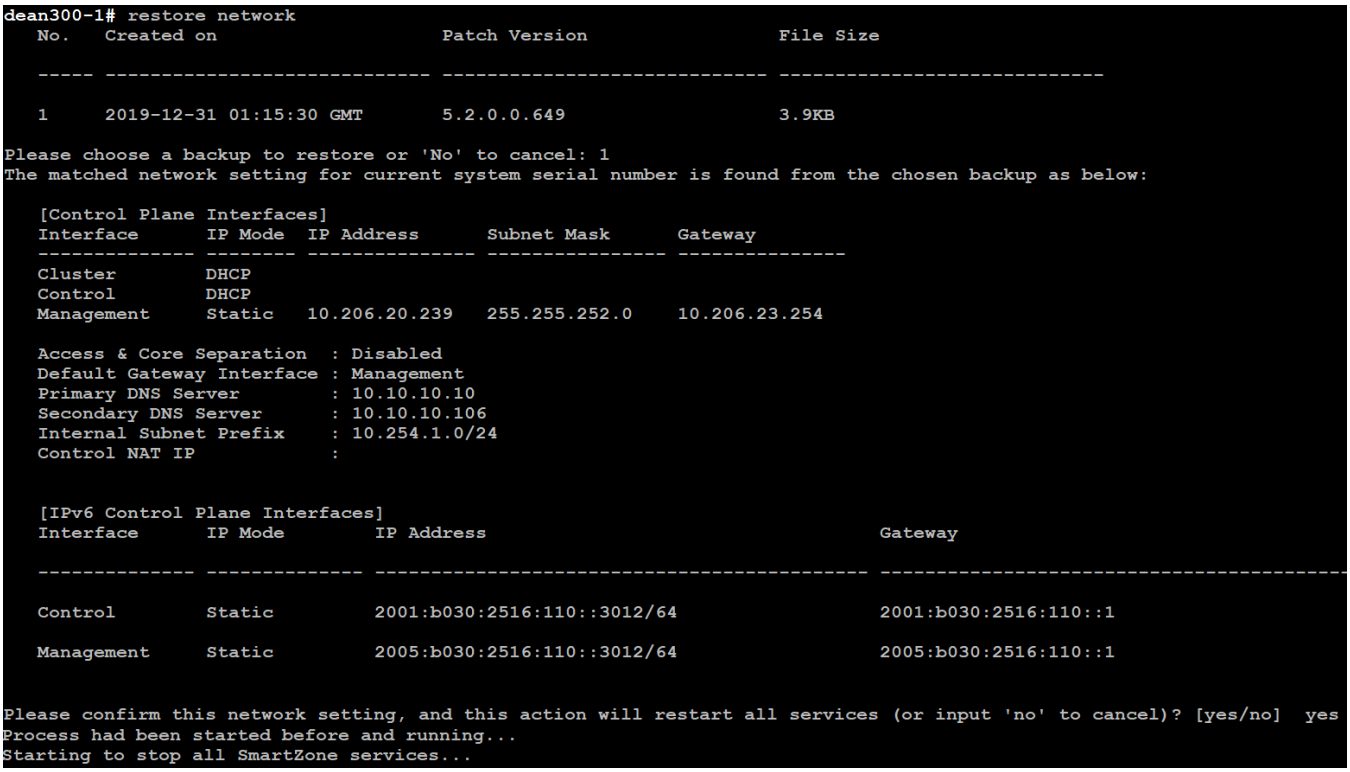
   

7. Run restore network to start restoring the contents of the backup file to the current controller.

   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 371 Enter the number that corresponds to the backup file that you want to restore



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.

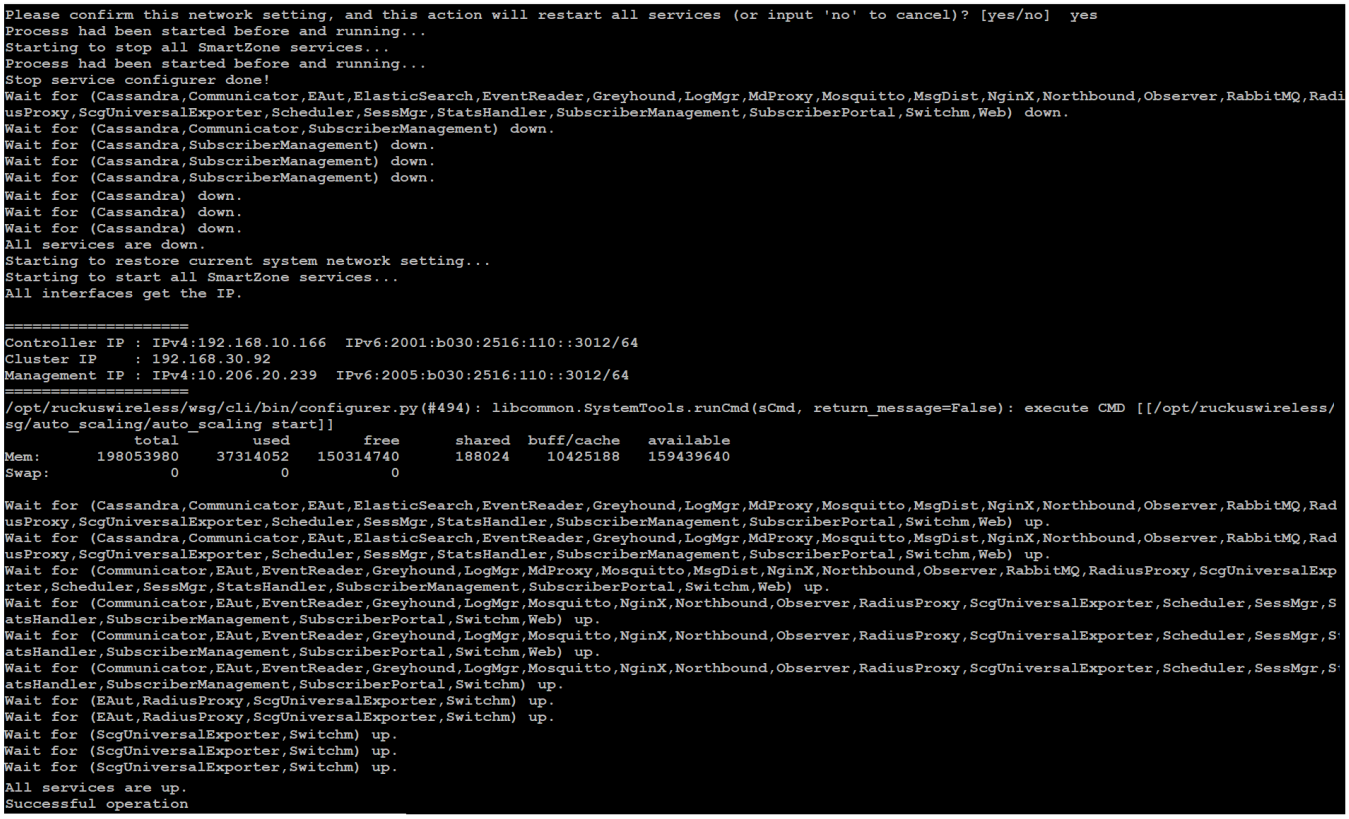
      This will enable the controller to roll back to the current configuration, in case there is an issue with the restore process.
   c) Clean up the current network configuration.

   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.

11. Restart all services.

    When the restore process is complete, the following message appears on the CLI: `All services are up!`

    FIGURE 372 The controller performs several steps to restore the backup file



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 373 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.

Support Information

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

To access these guides, select **Adminstraion** > **Help** and select the required guide.

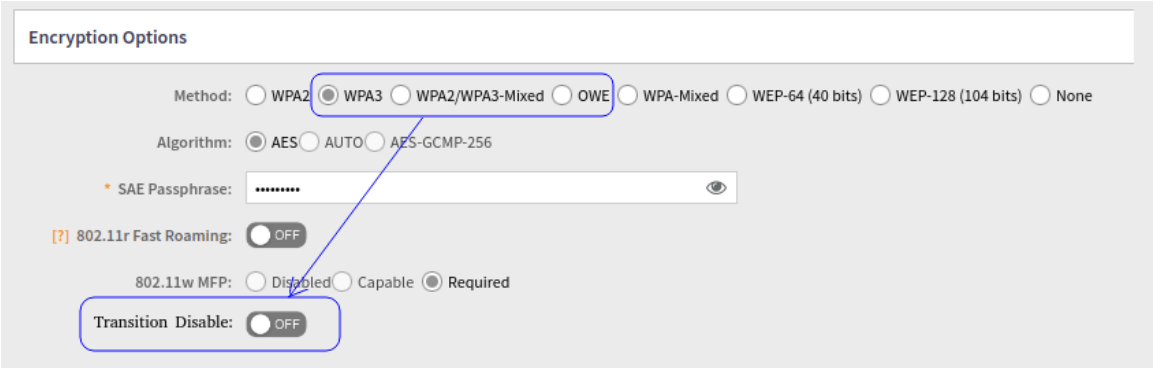
WPA3 R3 Support

SAE Hash to Element (H2E)

Instead of generating password with ECC/FFC groups by looping, H2E provides a way for direct hashing to obtain the ECC/FFC password element.

An AP that supports H2E sets the SAE H2E bit in Extended RSN Capabilities field in Beacon and Probe Response.

Transition Disable Indication



- Transition on/off option is provided in the Encryption Options.
- Beacon Protection

  Beacon Protection can only be enabled when PMF is enabled. When Beacon Protection is enabled, the bit 84 in Extended Capability IE should be set to 1. AP should protect Beacon via adding MMIE in all Beacon frames. The BIGTK (Beacon Integrity Group Temporal Key) and BIPN (BIGTK Packet Number) is used for this purpose.

  BIGTK should be renewed whenever there are GTK (Group Temporal Key) updates.
- Operating Channel Validation (OCV)

  AP and STA need to include OCI (Operating Channel Information) as below if it indicates it is OCV Capable.
  - Set bit 14 (OCVC) in RSN capability in RSNE.
  - Add OCI KDE (00-0F-AC-13) in EAPOL M2/M3 and group key update M1/M2 frames. If OCI KDE is incorrect, AP should silently discard the frame.

Upgrade

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.

If you are managing a vSZ-H controller, you can also perform system configuration backup, restore, and upgrade from the controller command line interface.

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.
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 622 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.

Uploading an AP Patch File

New AP models and firmware updates are supported without the need to upgrade the controller image by using the AP patch files supplied by RUCKUS.

1. Go to **Administration** > **Administration** > **Upgrade**.
2. Select the **AP Patch** tab.
3. In Patch File Upload, click **Browse** to select the patch file (with extension .patch).
4. Click **Open**.
5. Click **Upload**. The upload status bar is displayed, and after the patch file is uploaded, the section is populated with the patch filename, size, firmware version, and supporting AP models.
6. Click **Apply Patch**. The apply patch status bar is displayed.

   After the patch file is updated, you will be prompted to log out.

   When you login again, the **AP Patch History** section displays information about the patch file such as start time, AP firmware and model.

You have successfully updated the AP models and AP firmware with the patch file, without having to upgrade the controller software.

Verifying the Upgrade

You can verify that the controller upgrade was completed successfully.

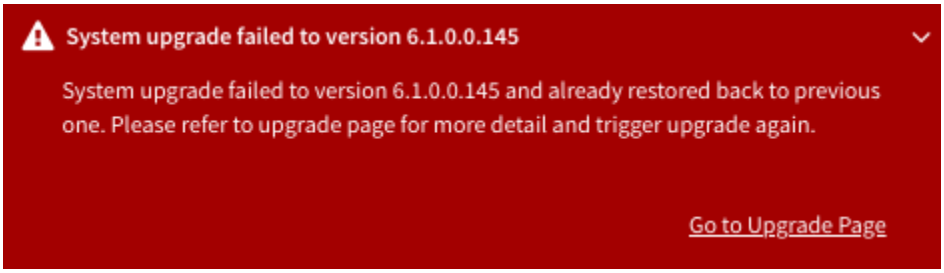
1. Go to **Administration** > **Administration** > **Upgrade**.
2. In the **Current System Information** section, check the value for *Controller Version*. If the firmware version is newer than the firmware version that controller was using before you started the upgrade process, then the upgrade process 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 374 Global Warning Message

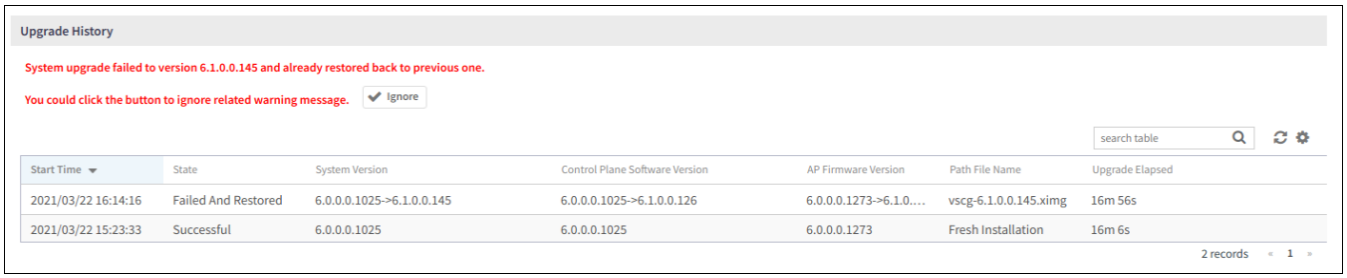


NOTE
Click the **Go to Upgrade Page** link to initiate the **Backup & Upgrade** process again.

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 375 Upgrade History Table



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.

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 622 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 622.
- 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 628 for remote backup instructions and Restoring from an FTP Server on page 630 for remote restore instructions.

Upgrading the Data Plane

You can view and upgrade the virtual data plane version using patch files. This feature is applicable only for virtual platforms.

Upgrading vSZ-D

vSZ support APs starting version 3.4. You must first upgrade vSZ before upgrading vSZ-D, because only a new vSZ can handle an old vSZ-D. There is no order in upgrading the AP zone or vSZ-D. During the vSZ upgrade, all tunnels stay up except the main tunnel which moves to the vSZ. Once the upgrade procedure is completed, allow ten minutes for the vSZ-D to settle.

Upgrade to R5.0 does not support data migration (statistics, events, administrator logs). Only the existing system and the network configuration is preserved. For more information, contact Ruckus support.

Upgrading SZ100-D

SZ100-D is shipped with 3.6.1 release version and you must upgrade it to 5.1 release version. As vSZ manages SZ100-D, ensure that vSZ has the same or later version than SZ100-D. Otherwise, upgrade vSZ before upgrading SZ100-D. SmartZone release 5.1.1 supports SZ100-D. For more information, refer to the *Ruckus SmartZone100-D Quick Setup Guide*.

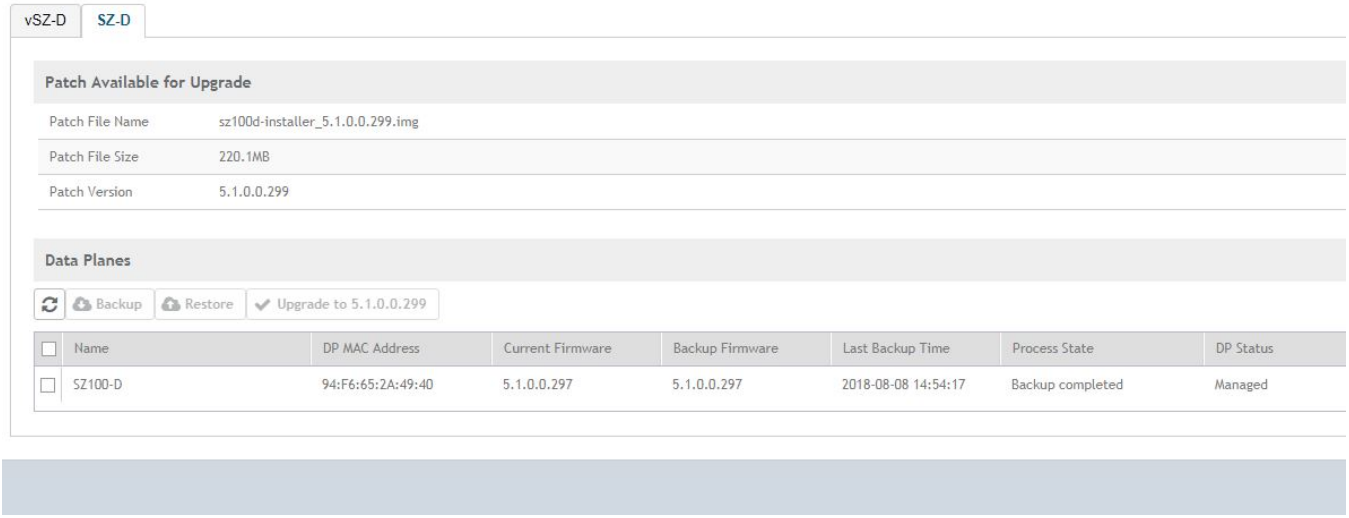
To Upgrade the Data Plane:

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

2. Select the **DP Patch** tab.

   The **DP Patch** page appears.

   FIGURE 376 DP Patch - Data Plane Upgrade



3. In **Patch File Upload**, click **Browse** to select the patch file (.ximg file).
4. Click **Upload**. The patch files is uploaded.

   The controller automatically identifies the Type of DP (vSZ-D or SZ-D) and switches to the specific Tab page. 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.
   The following details are displayed:

   - Patch File Name: Displays the name of the patch file.
   - Patch File Size: Displays the size of the patch file.
   - Patch Version: Displays the version of the patch file.

5. In **Data Planes**, identify the data plane you want to upgrade, and then choose a patch file version from **Select upgrade version**.
6. Click **Apply** to apply the patch file version to the virtual data plane.

   The following information about the virtual data plane is displayed after the patch file upgrade is completed.

   - Name: Displays the name of the virtual data plane.
   - DP MAC Address: Displays the MAC IP address of the data plane.
   - Current Firmware: Displays the current version of the data plane that has been upgraded.
   - Backup Firmware: Displays the backup version of the data plane.
   - Last Backup Time: Displays the date and time of last backup.
   - Process State: Displays the completion state of the patch file upgrade for the virtual data plane.
   - DP Status: Displays the DP status.

You have successfully upgraded the virtual data plane.

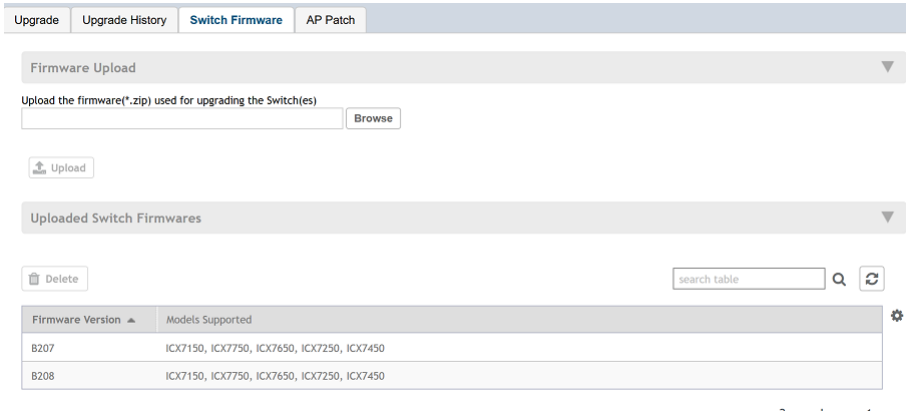
NOTE
To have a copy of the data plane firmware or move back to the older version, you can select the data plane from the list and click **Backup** or **Restore** respectively.

Uploading the Switch Firmware to the Controller

You can upload the latest available firmware to a switch from the controller, thereby upgrading the firmware version of the switch.

1. Select **Administration** > **Administration** > **Upgrade**.
2. Select the **Switch Firmware** tab.

FIGURE 377 Upgrading the Switch Firmware



3. In Firmware Upload click **Browse** to select the firmware file for upgrading the switch.
4. Click **Open**.
5. Click **Upload**. The upload status bar is displayed, and after the firmware file is uploaded, the **Uploaded Switch Firmwares** section is populated with the firmware version and switch models it supports.

You have successfully uploaded the switch firmware to the controller.

Scheduling a Firmware Upgrade for Selected Switches

You can upgrade or downgrade the firmware version of a switch or multiple switches that you are monitoring. You can upgrade the firmware on demand or schedule a firmware update for a list of selected switches.

Upload a valid firmware which is greater than version 8.0.80 to the controller.

NOTE
Ensure you sync the controller to the NTP server during installation. You can also do this from, go to **Administration** > **System** > **Time** > **Switches**.

To upgrade the firmware for a group of switches, you must select multiple switches at the same time and perform steps 3 to 7. For more information on uploading the switch firmware, see Uploading the Switch Firmware to the Controller on page 642

NOTE
Only firmware versions later than ICX 8.0.80 are supported.

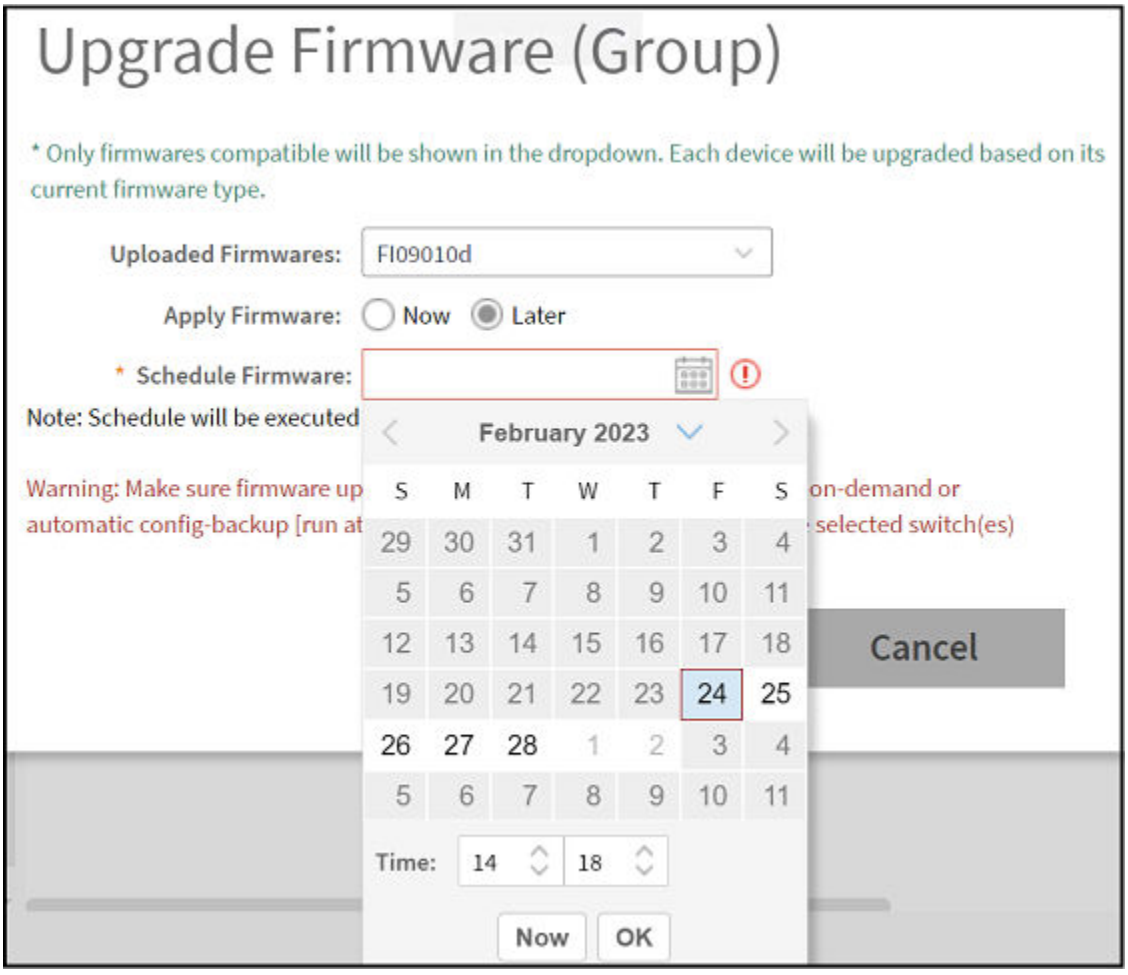
Scheduling Firmware Upgrade

1. From the main menu, go to **Network** > **Wired** > **Switches.**
   The **Switches** page appears.
2. From the **Switches** page, select the switch that you want to upgrade and click **More**.

3. From the drop-down menu, select **Schedule Firmware**.

   The **Upgrade Firmware** page appears.

   FIGURE 378 Scheduling Firmware Upgrade



4. From **Uploaded Firmware**, select the firmware version that you want the switch to be upgraded to
5. In **Firmware Type**, select type of firmware you want to upload to the switch. Options include Switch and Router images.
6. In **Apply Firmware**, set when you want to apply the new firmware version to the switch. You can select Now or Later to schedule your upload. If you select Later, then you must select the date from the **Schedule Firmware** field.

7. Click **OK**.

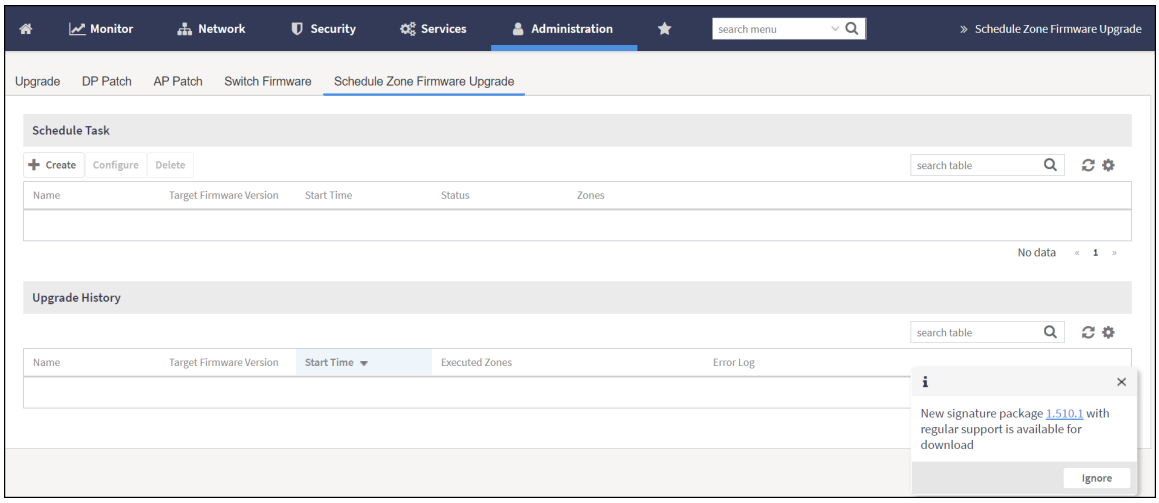
   If you want to delete the schedule you created; From **More**, click **Deleted Firmware Schedule(s)**.

   Schedule Zone Firmware Upgrade

   •Allow user setup a schedule time to upgrade/downgrade single or multiple zone firmware.

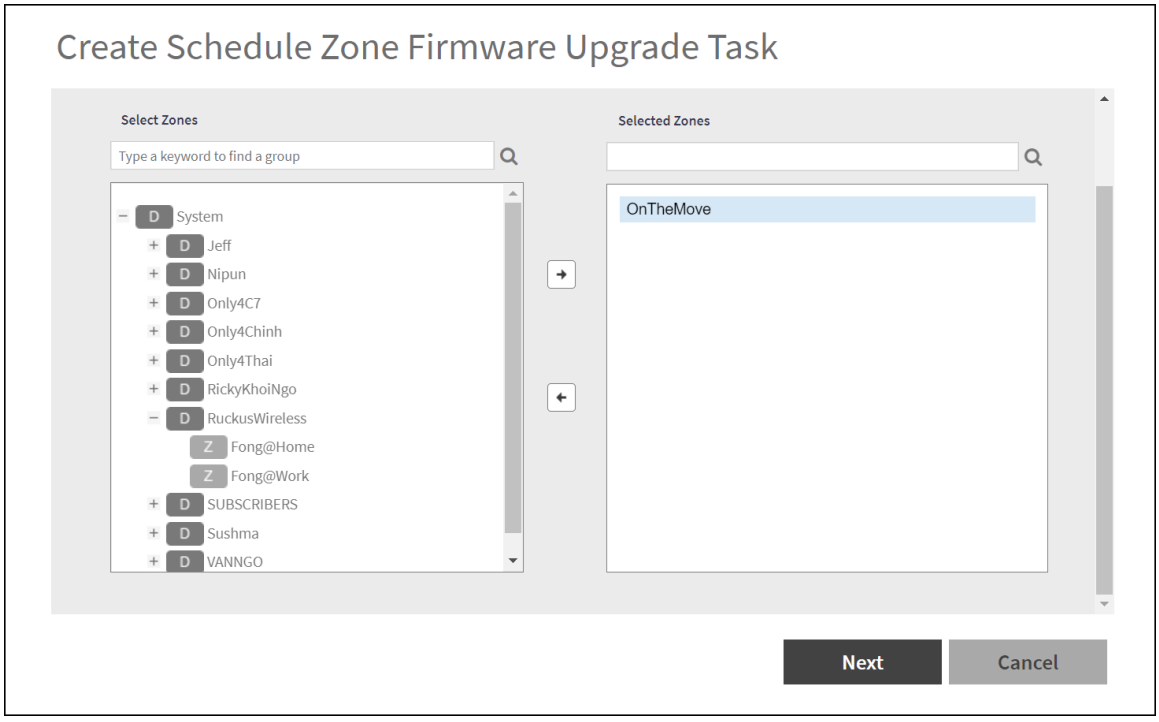
   •After a zone firmware upgrade/downgrade task is executed, user can see the zone firmware change history.

   a. From the main menu, go to **Administration** > **Upgrade** > **Schedule Zone Firmware Upgrade**.

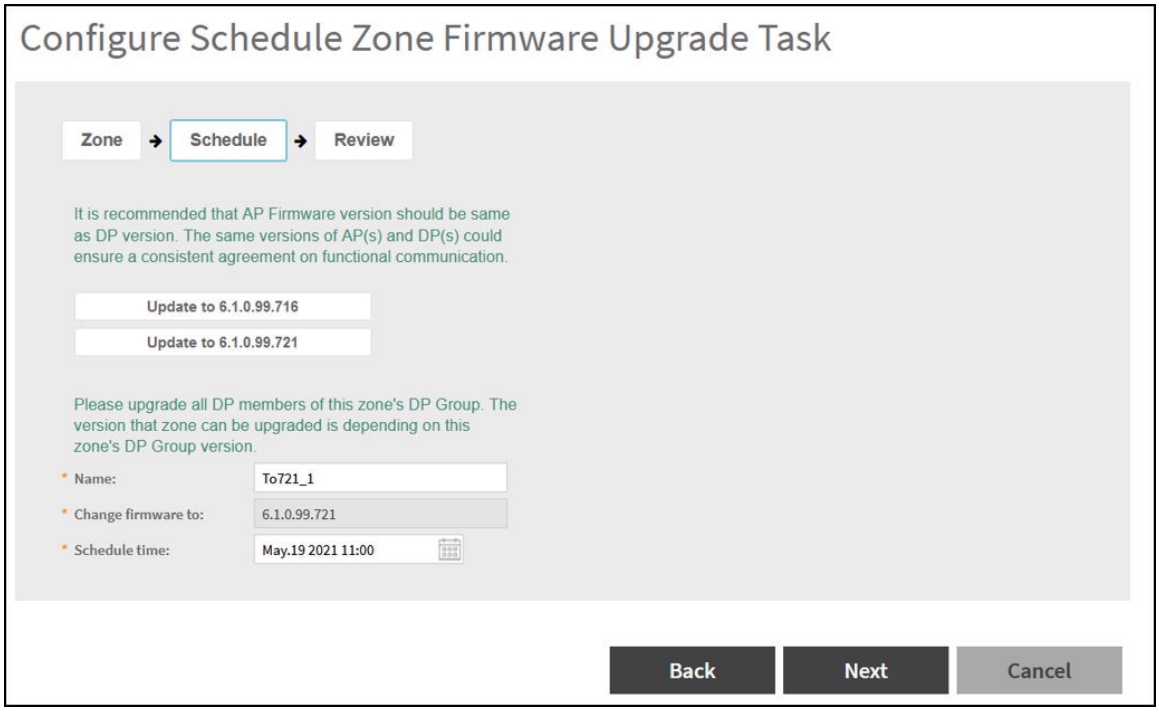


   b. Click "Create"

   c. Add the zone to schedule



d. Click "Next".



e. Enter the Name

f. Enter "Change Firmware to"

g. Enter the scheduled time of upgrade.

h. Click "next"

i. Review the task and click "Ok"

Scheduling a Firmware Upgrade for Switch Group

You can upgrade a switch group on a Level 1 group that has no default firmware setting. The forced upgrade allows the device to remain in the same firmware type (Layer 2 still Layer 2, Layer 3 still Layer 3) with only a change to the version type.

NOTE
If the switch group has a default firmware selected the **Firmware Upgrade** option is unavailable.

Complete the following steps to perform a firmware upgrade on the switch group.

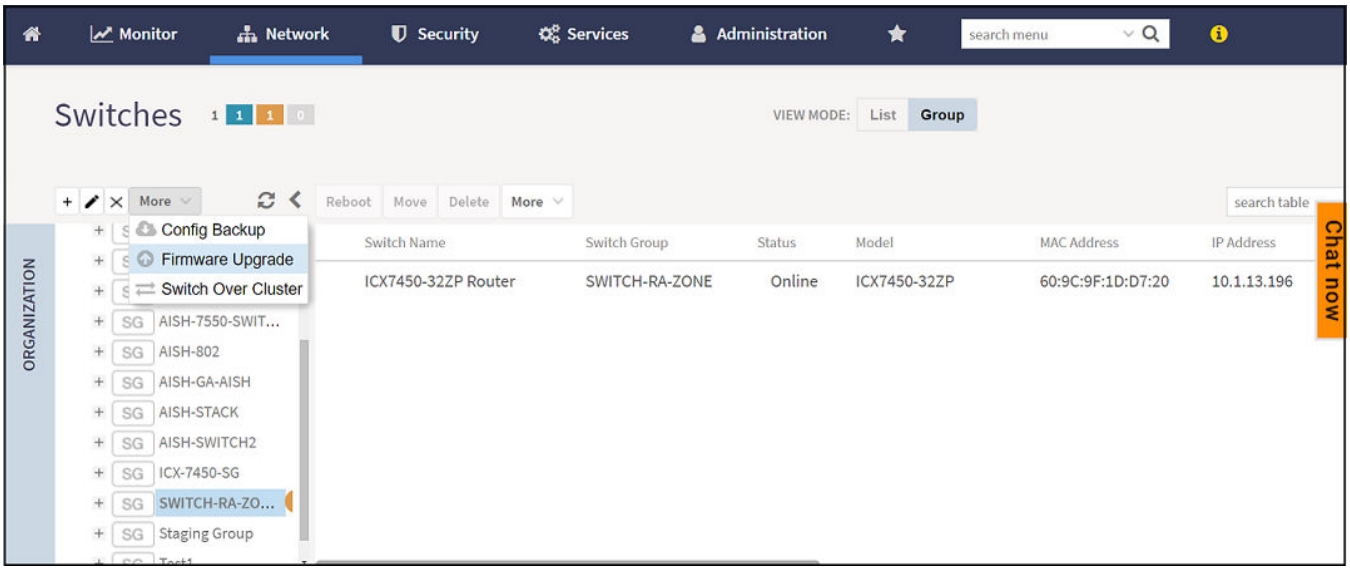
1. From the main menu, go to **Network** > **Wired** > **Switches**.

   The **Switches** page is displayed.

2. From the **Switches** page, select the switch group.

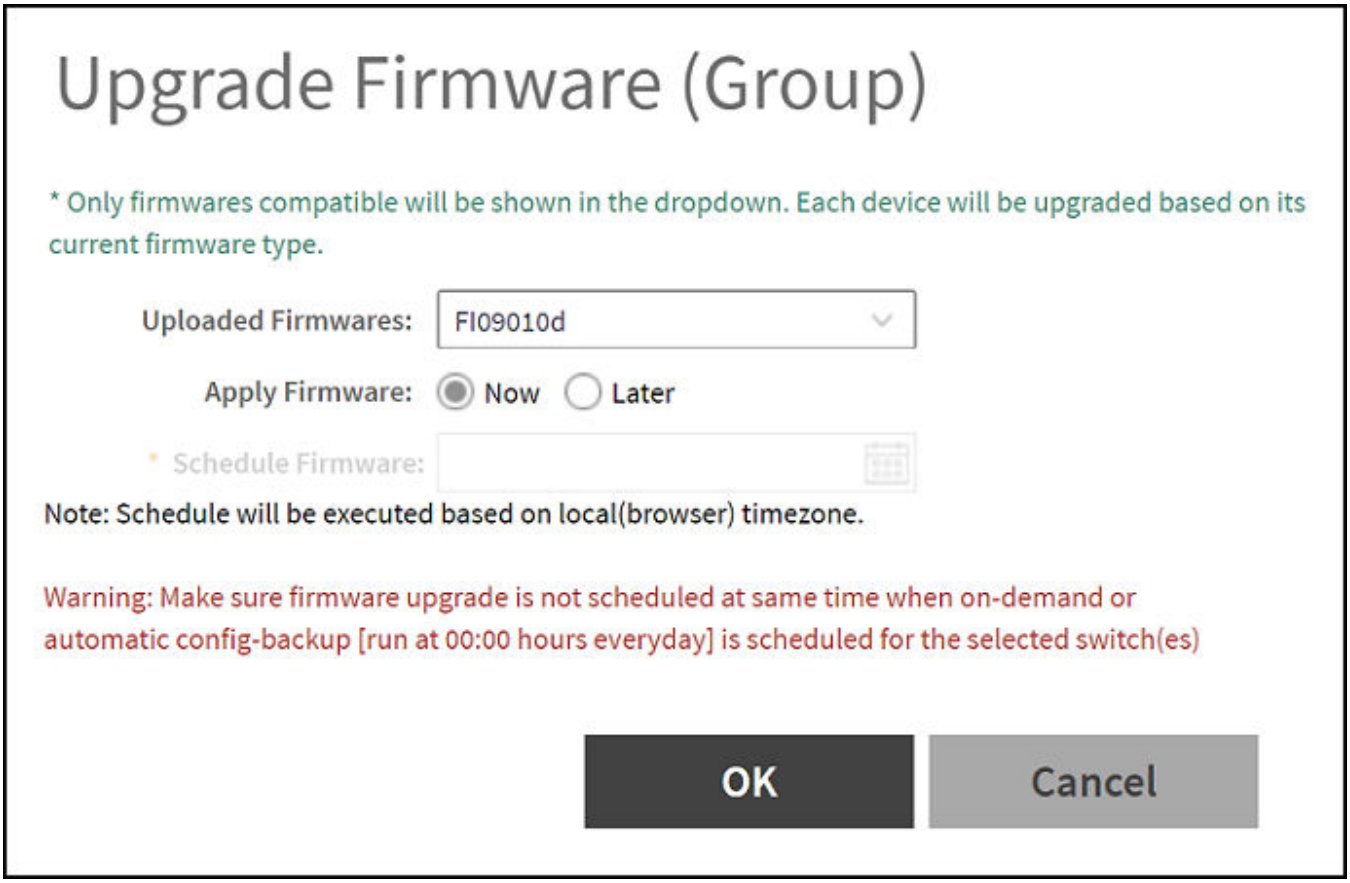
3. Click **More**, and select Firmware Upgrade.

FIGURE 379 Selecting Firmware Upgrade for a Switch Group



The **Upgrade Firmware (Group)** page is displayed.

FIGURE 380 Scheduling the Upgrade for a Switch Group



4. Configure the following options.
   a. **Uploaded Firmwares**: Select firmware from the list.
   b. **Apply Firmware**: Select Now or Later to set the new firmware version to the switch group.
   c. **Schedule Firmware**: If you select Later for **Apply Firmware**, you must select the date to schedule the upload.
5. Click **OK**.

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 639.

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.

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 SZ Admin AAA Servers on page 595 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.

Licenses

The features "Installed licenses", License servers and URL filter licenses are available in **Ruckus Software Licensing guide**.

Viewing Installed Licenses

You can synchronize the license data, import a license file into the controller if it is unable to connect to the Ruckus SmartLicense system, and release licenses bound to an offline controller by downloading a copy of the licenses.

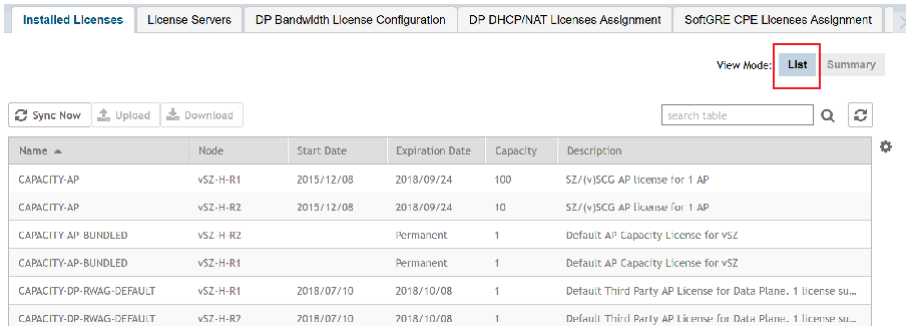
Perform these steps to check installed licenses.

1. Go to **Administration** > **Licenses**.
2. Select the **Installed Licenses** tab.

   The **List** view is displayed as shown in the following example.
3. Select **List** as the View Mode.

   The license **List** view is displayed as shown in the following example.

   FIGURE 381 License List View



   In the **List** view, the following information is displayed for licenses that have been uploaded to the controller:

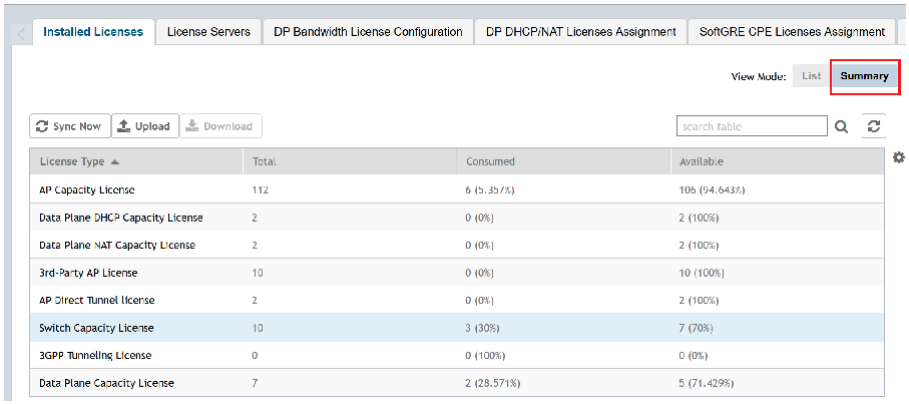
   - Name: The name of the node to which the license was uploaded
   - Node: The name of the controller node
   - Start Date: The date when the license file was activated
   - Expiration Date: For time-bound licenses, the date when the license file expires
   - Capacity: The number of units or license seats that the license file provides
   - Description: The type of license

4. Select **Summary** as the View Mode.

   In the **Summary** view, the information shown in the following example is displayed for the licenses that have been uploaded to the controller.

   - License Type: The type of license uploaded
   - Total: The total licenses (both consumed and available)
   - Consumed: The number of licenses consumed
   - Available: The licenses available

   FIGURE 382 License Summary View



Importing Installed Licenses

If the controller is disconnected from the Internet or is otherwise unable to communicate with the RUCKUS SmartLicense system (due to firewall policies, etc.), you can manually import a license entitlement file into the controller.

NOTE
The option to import a license file manually into the controller is only available if the controller is using the cloud license server.

1. Obtain the license file. You can do this by logging on to your RUCKUS Support account, going to the license management page, and then downloading the license file (the license file is in .bin format).
2. Log on to the controller web interface, and then go to **Administration** > **Administration** > **Licenses**.
3. Select the **Installed Licenses** tab.
4. Select the node for which you are uploading the license file and click **Upload.**

   The **Upload License** page appears where you must provide the following information:

   - Select Controller: Select the node for which you are uploading the license file.
   - Select License File: Click **Browse**, locate the license file (.bin file) that you downloaded from your RUCKUS Support account, and then select it.

The page refreshes, and the information displayed changes to reflect the updated information imported from the SmartLicense platform.

Synchronizing the Controller with the License Server

By default, the controller automatically synchronizes its license data with the selected license server every 24 hours. If you made changes to the controller licenses (for example, you purchased additional licenses) and you want the controller to download the updated license data immediately, you can trigger a manual synchronization.

1. Log in to the controller web interface, and select **Administration** > **Administration** > **Licenses**.
2. Select the **Installed Licenses** tab.
3. Click **Sync Now**.

   When the sync process is complete, the `Sync license with the license server successful` message is displayed. If the previously saved license data is different from the latest license data on the server, the information in the **Installed Licenses** section refreshes to reflect the latest data.

Downloading License Files

If you need to release licenses bound to an offline controller and allow those licenses to be used elsewhere (on a different controller), you can download a copy of the controller licenses. The option to download a copy of the controller licenses is only available if the controller is using the RUCKUS cloud license server.

1. Log on to the controller web interface, and then go to **Administration** > **Administration** > **Licenses**.
2. Select the **Installed Licenses** tab.
3. Click **Download**.

   The **Download License** page appears. In **Select Controller**, select the controller node for which you want to download the license files.

   NOTE
   You can upload and download license files only if the controller is using the RUCKUS cloud license server.

4. Click **Download**. Your web browser downloads the license files from the controller.
5. When the download is complete, go to the default download folder that you have configured for your web browser, and then verify that the binary copy of the license files (with .bin extension) exists.

You have completed downloading copies of the controller licenses.

Configuring License Bandwidth

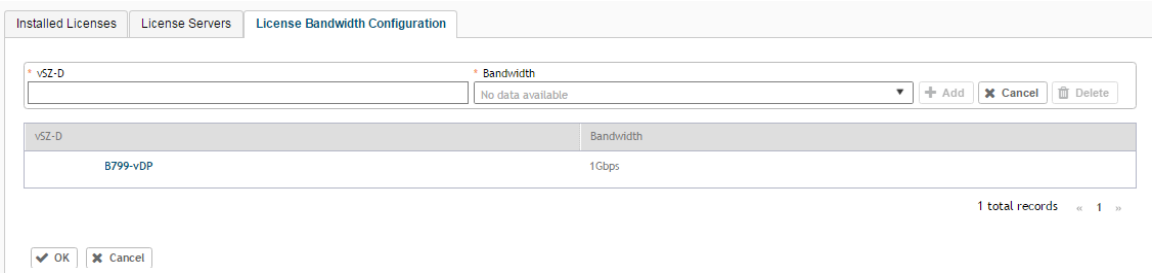
You can assign a license bandwidth for a virtual data plane provided it is already approved. Each virtual data plane can be configured with only one bandwidth license. This feature is applicable only to virtual platforms.

1. Go to **Administration** > **Administration** > **Licenses**.

2. Select the **License Bandwidth Configuration** tab.

   The **License Bandwidth Configuration** page appears.

   FIGURE 383 License Bandwidth Configuration



3. In **vSZ-D**, type the name of the virtual data plane.

   NOTE
   SZ100 and SZ144 controllers are not supported with external DPs (vSZ-D/SZ100-D/SZ144-D).

4. From the **Bandwidth** drop-down menu, select the license bandwidth you want to assign to the virtual data plane. Default is 1Gbps.
5. Click **Add**. The vSZ-D with the assigned license bandwidth is displayed.
6. Click **OK**.

   The message `Submitting form appears`, and the vSZ-D is assigned a bandwidth.

You have successfully assigned a license bandwidth to the virtual data plane.

Configuring the License Server

RUCKUS manages the licenses that you have purchased for the controller with the - Cloud License Server.

Cloud License Server, also known as the SmartLicense server, is a cloud-based server that stores all of the licenses and support entitlements that you have purchased for the controller. For information on how to set up and activate your SmartLicense account, refer to the *RUCKUS SmartLicense User Guide*.

1. Go to **Administration** > **Administration** > **Licenses**.
2. Select the **License Server** tab.

   The server details and synchronization history are displayed.
3. Click **Configure**.

   The **License Server Configuration** page is displayed.

   - Select the Cloud License Server option to use the *RUCKUS SmartLicense server*.
4. Click **OK**.
5. Click **Sync Now** . The controller saves the selected license server configuration, deletes all of its saved license data, and then automatically synchronizes the license information with the selected license server.

Configuring the DHCP/NAT License Assignment

License assignment specifies the capability of each Data Plane, which has the ability to assign IPs by DHCP feature and translate packets by NAT feature. Though these features already exist, starting 5.0, customers must purchase license to enable these features.

NOTE
This feature is supported only on virtual platform.

Configuring URL Filtering Licenses

You can configure the number of URL filtering licenses on an AP within a zone.

You can both limit the number of URL filtering licenses per zone, and also configure the AP to have unlimited licenses.

If an AP has a URL filtering license enabled, URL filtering can be enabled for all WLANs within the same zone.

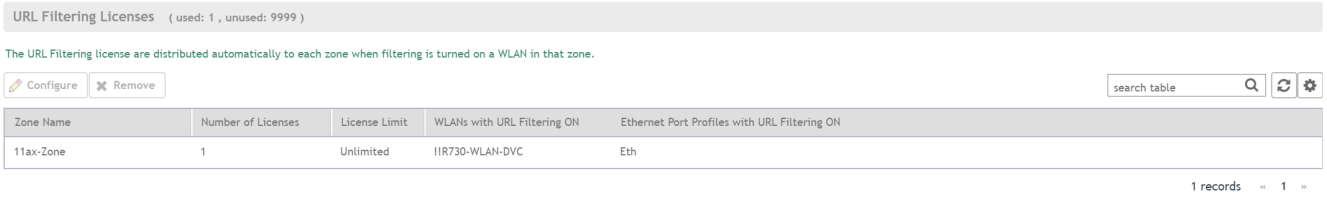
If the URL filtering license is deleted in a zone, URL filtering services are disabled on all the WLANs within that zone. If you want to add the license back again, you must enable URL filtering on the zone or WLAN.

If the license limited to the zone is specified, you cannot move or add more APs with URL filtering enabled to that zone. For example, if you have set the license limit to 3, you cannot add a fourth AP to the zone.

NOTE
Number of trial licenses for SZ300 and vSZ-H controllers is 10,000 licenses.

1. Select **Administration** > **Licenses**.
2. Select the **URL Filtering Licenses** tab.

FIGURE 384 URL Filtering Licenses



The **URL Filtering Licenses** tab displays the following information:

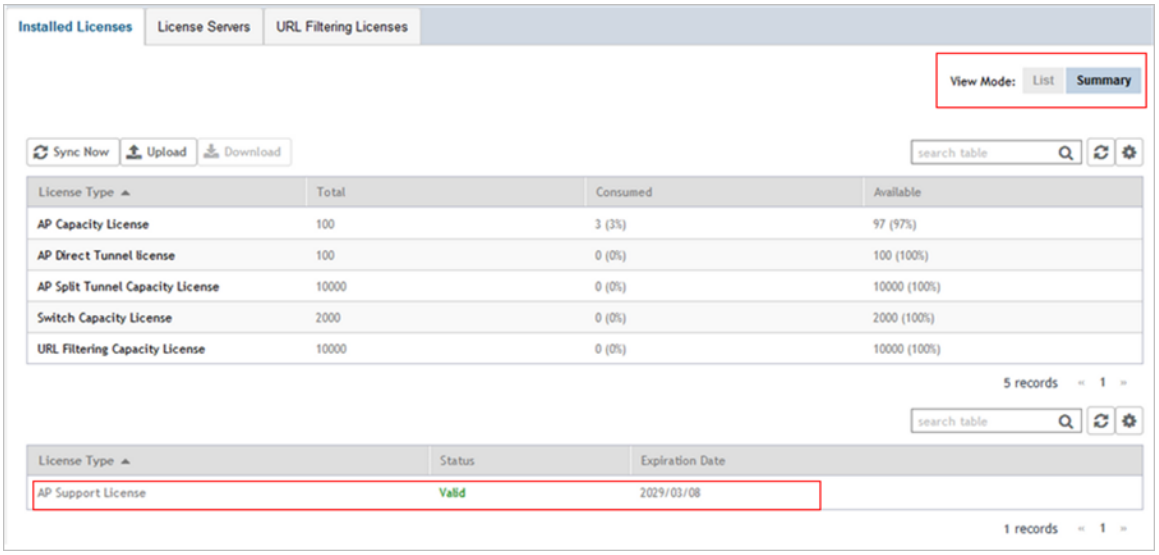
- Zone Name: The name of the zone within which APs are present.
- Number of Licenses: Displays the total number of licenses allocated to the zone.
- License Limit: Displays the number of APs (with URL filtering enabled) that can be accommodated within the zone. Can be set to a specific value or Unlimited.
- WLANs with URL Filtering ON: Displays all the WLANs within the zone that have the URL filtering service enabled.
- Ethernet Port Profiles with URL Filtering ON: Displays the Ethernet port profiles within the zone that have the URL filtering service enabled.

3. Select the URL license and click **Configure**.
   The **URL Filtering Licenses** page appears.
4. Configure the License Limit as appropriate for the zone.
5. Click **OK**.

Support AP Licensing for the Controller

In the previous SmartZone releases, users were unable to view the AP support license information untill the controller displayed a warning message during system upgrade.

From the current release, users can view the AP support license information on the controller web user interface by navigating to **Administration**>**Administration**> **Licenses** > **Installed License** retrieved from the license server at any given point of time. To view the AP license status and validity click **View** > **Summary** tab.



ZD Migration

ZoneDirector to SmartZone Migration

SmartZone controllers are better equipped to handle large WiFi deployments such as within campuses and when customers are vastly distributed; therefore, RUCKUS recommends that you migrate existing ZoneDirector deployments to SamrtZone controller deployments. You can migrate ZoneDirector AP configuration information to SmartZone controllers from the controller itself, using a migration tool.

The AP models should be supported by the controller.

NOTE
Not more than 50 AP's will be migrated from Zone Director to Smart Zone.

TABLE 120 Migration Support Matrix

SmartZone Version	ZoneDirector Version
3.5.x	9.13x
3.5.x	9.13.x, 10.0.x, 10.1.x
3.5.x	9.13.x, 10.0.x, 10.1.x
3.5.x	9.13.x, 10.0.x, 10.1.x

CAUTION
Do not power off the AP during the migration process.

1. Go to **Administration** > **Administration** > **ZD Migration**.

   The **ZoneDirector Migration** page appears.
2. Configure the following:
   a. ZoneDirector IP Address: Type the IP address of the ZD that you want to migrate.
   b. Admin Credentials: Enter the username and password details to access/login to ZD.
   c. Click **Connect**. Lists of APs connected to the ZD deployment are displayed.
   d. Click **Select AP** to choose the AP information that you want to migrate from ZD.
   e. Click **Migrate** to migrate the AP. The controller imports the ZD configuration and applies it to the selected AP.

   The **ZoneDirector Migration Status** section displays the status of the migration. When completed successfully, a success message is displayed. If migration fails, a failure message is displayed and you can attempt the migration process again.

   NOTE
   To migrate ZoneDirector Mesh APs to SmartZone, upgrade ZoneDirector to its supported version. For information on the supported versions, refer 5.2.1 release notes.

Admin Activities

Monitoring 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
   - Managed By: Displays the system that manages the admin activities.
   - Source IP: Displays the IP address of the device form 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.

Help

Rest API

Ports to open for AP-Controller Communication

The table below lists the 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 121 Ports to open for AP-Controller Communication Inbound table

Ports to Open for AP-Controller Communication Port Number	Layer 4 Protocol	From (Sender)	To (Listener)	Interface	Configurable from Web Interface?	Purpose
21	TCP	AP	Control plane of • SZ-100 • SZ-200 • SZ-300 • vSZ	Control	No	ZD/Solo APs can download SZ AP firmware and converting themselves to SZ APs.
20-21	TCP	SZ	External FTP server	Control, Cluster, Management	No	Transfer date to external FTP servers
22	TCP	AP	Control plane of : SZ-100 SZ-300 vSZ	Control	No	SSH Tunnel for management
49	TCP	TACACS+ Server	TACACS+ Server	Management, Cluster, Control	No	TACACS_Plus
53	TCP/UDP	DNS Server	DNS	Management, Cluster, Control	No	DNS
67,68	UDP	DHCP Server	SZ	Control, Cluster, Management	No	DHCP Protocol
69	UDP	ZD AP	SZ	Control	No	ZD Migration
80	TCP	Walled-Garden Web Server	CaptivePortal with HTTP Proxy	Management, Cluster, Control	No	WISPr_WalledGarden

TABLE 121 Ports to open for AP-Controller Communication Inbound table (continued)

Ports to Open for AP-Controller Communication Port Number	Layer 4 Protocol	From (Sender)	To (Listener)	Interface	Configurable from Web Interface?	Purpose
Port 91 (AP firmware version 2.0 to 3.1.x) and 443 (AP firmware version 3.2 and later)	TCP	AP	vSZ control plane	Control	No	AP firmware upgrade APs need Port 91 to download the Guest Logo and to update the signature package for the ARC feature. **NOTE** Starting in release 3.2, the controller uses an HTTPS connection and an encrypted path for the firmware download. The port used for AP firmware downloads has also 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 443 and 91 in the network firewall.
123	UDP	Follower SZ nodes	Master SZ node	Cluster	No	Sync system time among SZ nodes
161	UDP	SNMP Client	SZ	Management	No	Simple Network Management Protocol (SNMP)
389	TCP/UDP	LDAP Server	RAC	Management, Cluster, Control	Yes	SZ to LDAP
443	TCP	• AP • vSZ-D	vSZ control plane	Control	No	Access to the vSZ/SZ control plane over secure HTTPS
443	HTTPS	Controller	License server	Control	No	Cloud license server

TABLE 121 Ports to open for AP-Controller Communication Inbound table (continued)

Ports to Open for AP-Controller Communication Port Number	Layer 4 Protocol	From (Sender)	To (Listener)	Interface	Configurable from Web Interface?	Purpose
514	TCP/UDP		rsyslog	Management, Cluster, Control	No	Remote Syslog
636	TCP	LDAPS Server	RAC	Management, Cluster, Control	Yes	SZ to LDAPS Server
546,547	UDP	DHCP v6 Server	SZ	Control, Cluster, Management	No	DHCP v6 Protocol
1812	UDP	SZ-RAC	External AAA	Management, Cluster and Control **NOTE** The Management interface is applicable when vSZ-H is in single interface mode. If in 3-interface mode with Access and Core separation Disabled it will depend on the configured Management traffic interface.	Yes	To Support Radius Proxy Authentication

TABLE 121 Ports to open for AP-Controller Communication Inbound table (continued)

Ports to Open for AP-Controller Communication Port Number	Layer 4 Protocol	From (Sender)	To (Listener)	Interface	Configurable from Web Interface?	Purpose
1813	UDP	AP	RAC (Radius Access Controller)	Management, Cluster, Control **NOTE** The Management interface is applicable when vSZ-H is in single interface mode. If in 3-interface mode with Access and Core separation Disabled it will depend on the configured Management traffic interface.	No	Radius_Auth profile defines both inbound and outbound traffic. lo specified here is for inbound traffic only.
2083 (Radsec)	TCP	AAA server	SZ	Control, Cluster, Management	No	The default destination port number for RADIUS over TLS is TCP/2083 (As per RFC-6614)
2084 (CoA/DM Over RADSEC)	TCP	AAA server	SZ	Control, Cluster, Management	No	SZ as RADSEC server listens on port 2084 for incoming TLS connection from client (AAA Client) to process CoA/DM messages over RADSEC
3268	TCP	AD Server (MSTF-GC)	RAC	Management, Cluster, Control	Yes	SZ to AD (MSTF-GC)
3799	UDP	External AAA Server (free Radius)	SZ-RAC (vSZ control plane)	Control, Cluster, Management	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.
4443	TCP	JITC CAC	SZ	Control	No	Since R5.1.2, mainly for JITC CAC login support. This port is opened for NGINX to configure for client cert authentication.
5353	UDP	AP	SZ	Control	No	Resolves hostnames to IP addresses

TABLE 121 Ports to open for AP-Controller Communication Inbound table (continued)

Ports to Open for AP-Controller Communication Port Number	Layer 4 Protocol	From (Sender)	To (Listener)	Interface	Configurable from Web Interface?	Purpose
6379,6380	TCP	SZ	SZ	Cluster	No	Internal communication among SZ nodes
7000	TCP/UDP	SZ	SZ	Cluster	No	Cassandra (database) cluster communication and data replication
7443	TCP	Legacy Public API Client	SZ	Management	No	Deprecated Public API
7500	UDP	SZ	SZ	Cluster	No	SZ Clustering Operation
7800	TCP/UDP	SZ	SZ	Cluster	No	Cluster node communication for cluster's operations
7801	TCP	SZ	SZ	Cluster	No	A protocol stack using TCP on JGroups library for node to node communication on SZ
7800-7805	TCP	SZ	SZ	Cluster	No	A protocol stack using TCP on JGroups library for node to node communication
7810	TCP	SZ	SZ	Cluster	No	A protocol stack using FD_SOCK on JGroups library for node to node communication
7811	TCP	SZ	SZ	Cluster	No	A protocol stack using FD_SOCK on JGroups library for node to node communication
7812	TCP	SZ	SZ	Cluster	No	A protocol stack using FD_SOCK on JGroups library for node to node communication
8022	No (SSH)	Any	Management interface	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.
8090	TCP	Any	vSZ control plane	Control	No	Allows unauthorized UEs to browse to an HTTP website
8099	TCP	Any	vSZ control plane	Control	No	Allows unauthorized UEs to browse to an HTTPS website
8100	TCP	Any	vSZ control plane	Control	No	Allows unauthorized UEs to browse using a proxy UE
8200	TCP	• AP • DP	SZ	Control	No	Captive Portal OAuth service port for HTTP

TABLE 121 Ports to open for AP-Controller Communication Inbound table (continued)

Ports to Open for AP-Controller Communication Port Number	Layer 4 Protocol	From (Sender)	To (Listener)	Interface	Configurable from Web Interface?	Purpose
8222	TCP	• AP • DP	SZ	Control	No	Captive Portal OAuth service port for HTTPS
8280	TCP	• AP • DP	SZ	Control	No	Captive Portal Web Proxy service port for HTTPS
8443 **NOTE** The Public API port has changed from 7443 to 8443.	TCP	Any	vSZ management plane	Management	No	Access to the controller web interface via HTTPS
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	SZ	SPoT	Management, Cluster, Control	No	Communication between SZ and SPoT
9080	HTTP	Any	vSZ control plane	Management, Control	No	Northbound Portal Interface for hotspots
9191	TCP	AP-MD	SZ-MD	Cluster	No	Communication between AP-MD and SZ-MD

TABLE 121 Ports to open for AP-Controller Communication Inbound table (continued)

Ports to Open for AP-Controller Communication Port Number	Layer 4 Protocol	From (Sender)	To (Listener)	Interface	Configurable from Web Interface?	Purpose
9300-9400	TCP	SZ	SZ	Cluster	No	Internal communication between nodes within the cluster (ElasticSearch database)
9300 - 9311	TCP	SZ	SZ	Cluster	No	Internal communication between nodes within the cluster (ElasticSearch database)
9443	HTTPS	Any	vSZ control plane	Management, Control	No	Northbound Portal Interface for hotspots.
9997	TCP	Client Device	SZ control Plane	Control	No	Internal Subscriber Portal in HTTP protocol
9998	TCP	Any	vSZ control plane	Control	No	Hotspot WISPr subscriber portal login/logout over HTTPSl
11211	TCP	SZ Local Modules	SZ memproxy	Cluster	No	Internal proxy for saving in-memory data to memcached
11311	TCP	SZ	SZ	Cluster	No	Memory cache server
12223	UDP	AP	vSZ control plane	Control	No	LWAPP discovery, send image upgrade request to ZD-APs via LWAPP (rfc5412). **NOTE**
18301	UDP	• AP • UE	SZ	Management, Cluster, Control	No	SpeedFlex tests the network performance between AP, UE,and SZ.
33434 - 33534	UDP	SZ	SZ	Management, Cluster, Control	No	ICX Trouble Shooting (traceroute).
65534, 65535	TCP	SZ CS	DP	Management	No	DP Debug
443	TCP	ICX	vSZ control plane	Control	No	Access to the vSZ/SZ control plane over secure HTTPS.
	TCP	ICX	vSZ control plane	Control	No	This is for FIPS build only. Access to the vSZ/SZ control plane over secure HTTPS.

TABLE 122 vDP/ SZ300 DP/ SZ100 Data Group(PG-2):

Port Number	Layer 4 Protocol	From (Sender)	To (Listener)	Interface	Configurable from Web Interface?	Purpose
22	TCP	• AP • vSZ-D	vSZ control plane	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/control interface IP address.

NOTE
Communication between APs is not possible across NAT servers.

Replacing Hardware Components

This appendix describes how to replace hardware components (including hard disk drives, power supply units, and system fans) on the controller.

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.

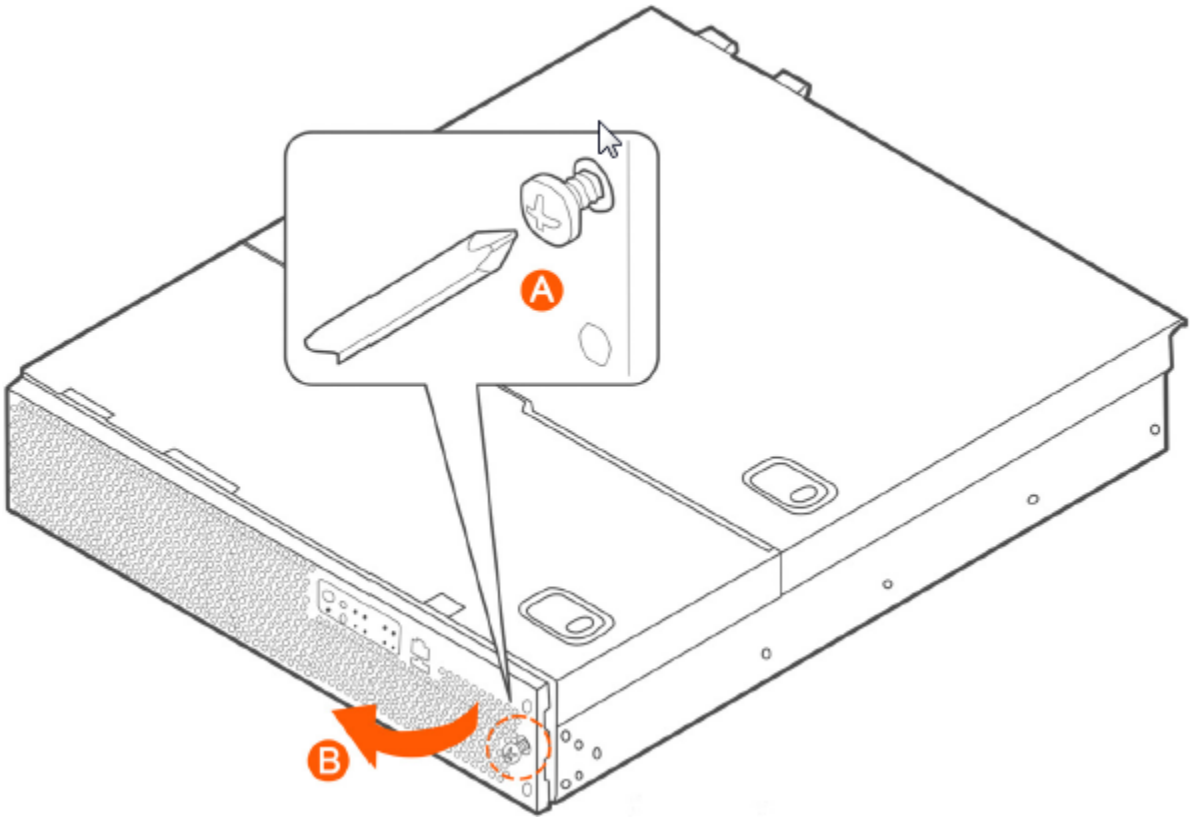
You need to remove the front bezel for tasks such as:

- 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 386).
2. Rotate the bezel to the left to free it from the pins on the front panel (see B in Figure 386), and then remove it.

FIGURE 385 Removing the front bezel



Removing an HDD Carrier from the Chassis

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

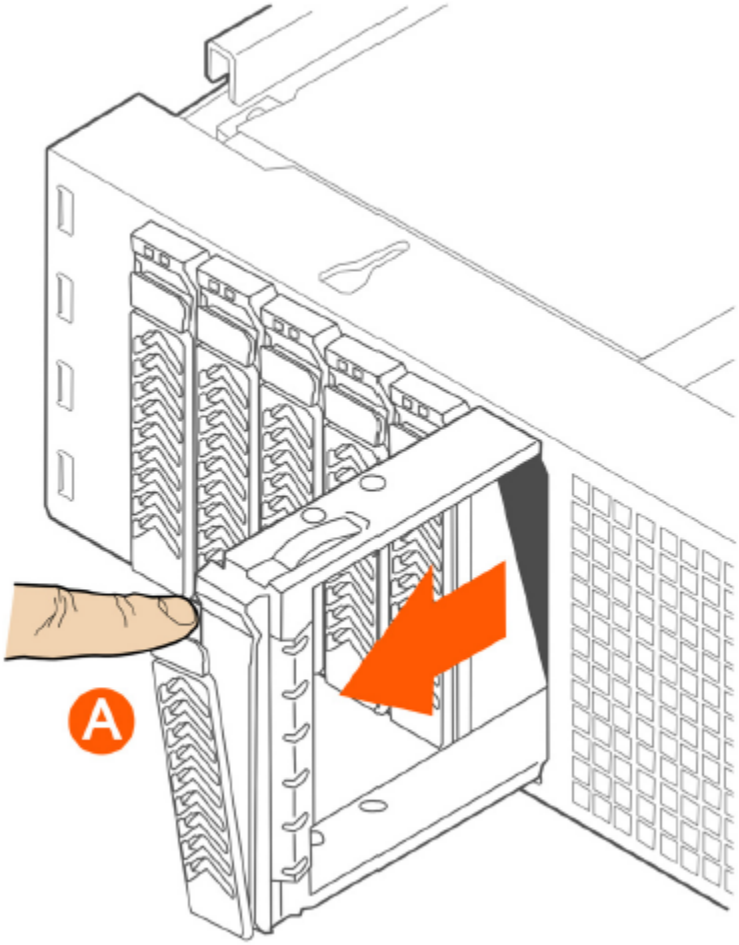
1. Remove the front bezel (see Removing the Front Bezel on page 664).
2. Select the drive bay where you want to install or replace the drive.

   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 387).

4. Pull the drive carrier out of the chassis.

FIGURE 386 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 388). Set the screws aside for use with the new drive.

2. Lift the drive out of the carrier (see B in Figure 388).

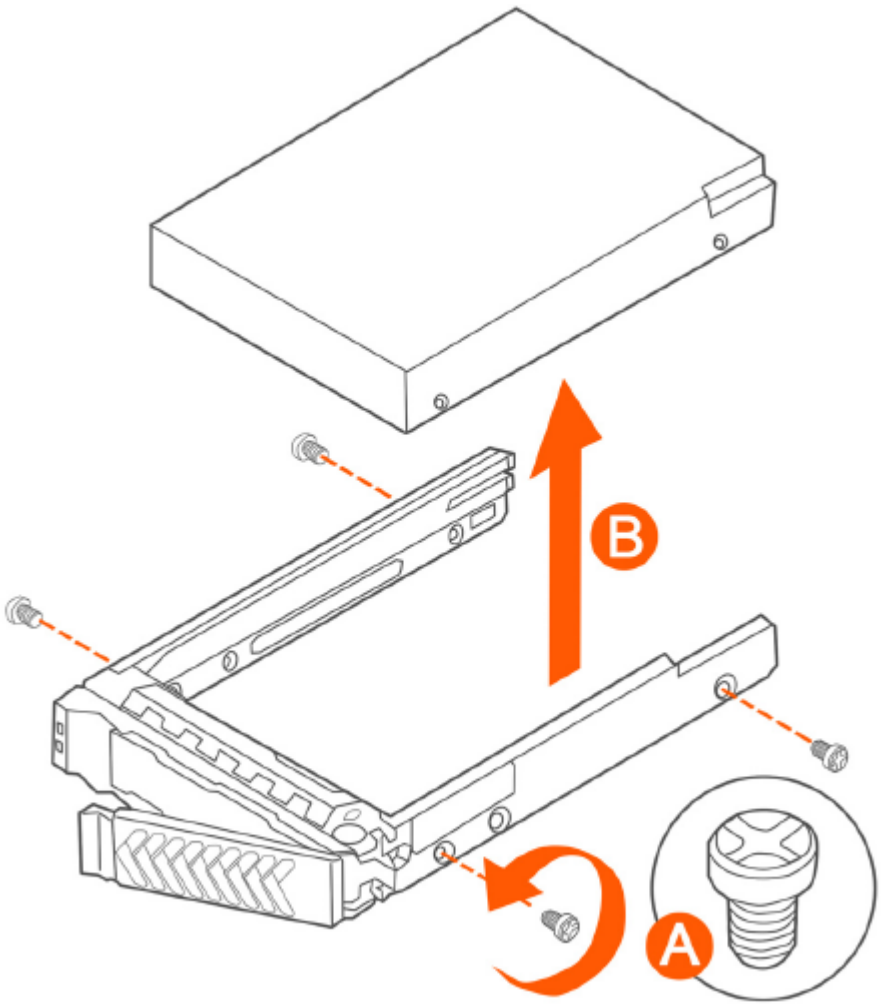


FIGURE 387 Removing the hard drive

3. Install the new drive in the drive carrier (see A in Figure 389), and then secure the drive with the four screws that come with the carrier (see B).

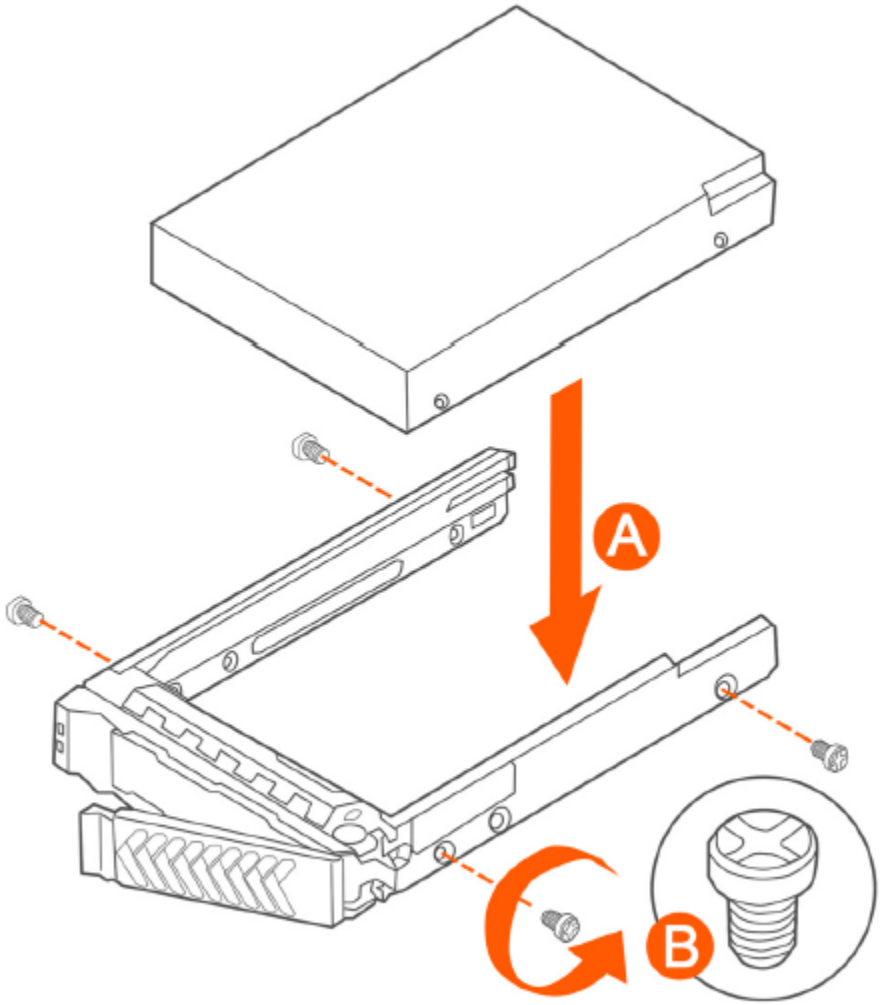


FIGURE 388 Installing the hard drive

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 390).

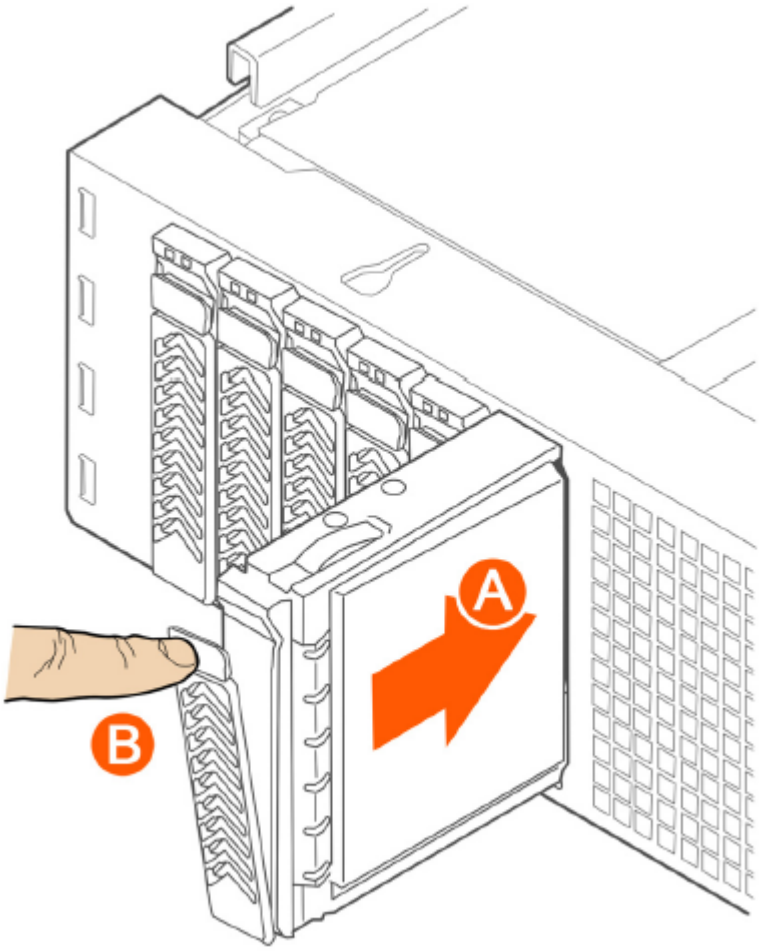


FIGURE 389 Inserting the carrier back into the chassis

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.

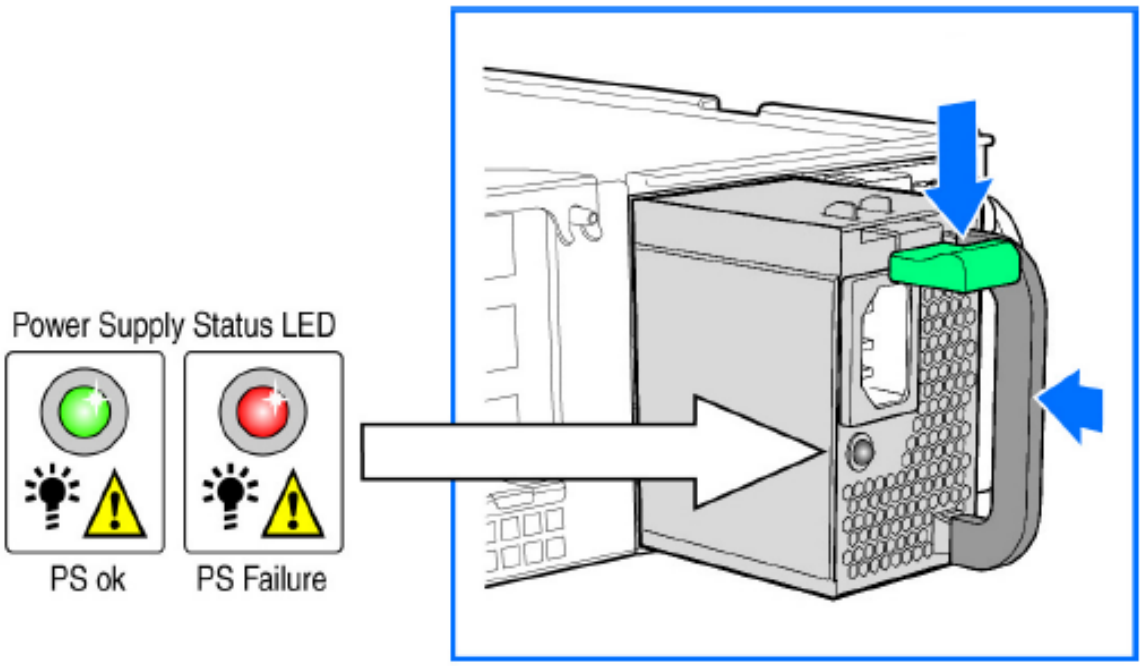
Follow these steps to remove and replace a PSU.

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.

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 390 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.

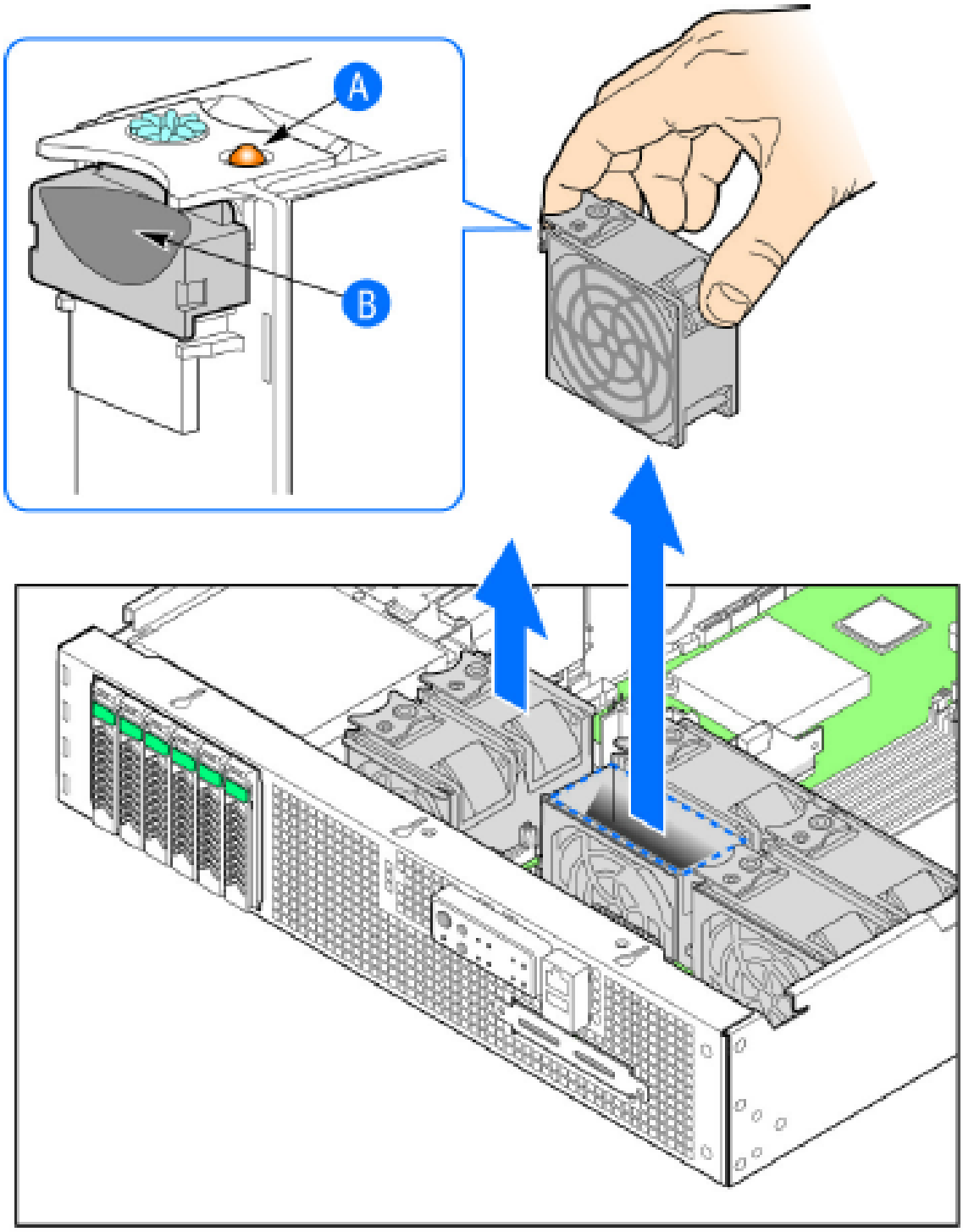
Electrostatic discharge (ESD) can damage internal components such as printed circuit boards and other parts. RUCKUS recommends that you only perform this procedure with adequate ESD protection. At a minimum, wear an anti-static wrist strap attached to the ESD ground strap attachment on the front panel 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 391 Replacing a system fan



vSZ-H SSID Syntax

The following sections describe the supported SSID syntax in the following vSZ-H release versions:

SSIDs Supported in Release 1.1.x

Release 1.1.x supports a specific set of SSID syntaxes, which may be different from the syntaxes supported in other releases.

The following table describes the SSID syntaxes that are supported in release 1.1.x.

TABLE 123 Supported SSID syntaxes in 1.1.x

Web Interface	Length	Between 1 and 32 characters, including characters from printable characters (ASCII characters space (32) to ~ (126)
	Supported Characters	• A-Z • a-z • 0-9 • _space_!"#$%&'()*+,-./ • :;<=?@ • [\]^_` • {|}
CLI	Length	Unsupported
	Supported Characters	Unsupported

SSIDs Supported in Release 2.1.x

Release 2.1.x supports a specific set of SSID syntaxes, which may be different from the syntaxes supported in other releases.

The following table describes the SSID syntaxes that are supported in release 2.1.x.

TABLE 124 Supported SSID syntaxes in 2.1.x

Web Interface	Length	Between 1 and 32 characters, including characters from printable characters (ASCII characters space (32) to ~(126)
	Supported Characters	• A-Z • a-z • 0-9 • _space_!"#$%&'()*+,-./ • :;<=?@ • [\]^_` • {|}
CLI	Length	Between 2 and 32 characters
	Supported Characters	All characters, but the space character cannot be the first or last character in the SSID

SSIDs Supported in Release 2.5.x

Release 2.5.x supports a specific set of SSID syntaxes, which may be different from the syntaxes supported in other releases.

The following table describes the SSID syntaxes that are supported in release 2.5.x.

TABLE 125 Supported SSID syntax in 2.5.x

Web Interface	Length	Between 1 and 32 characters, including characters from printable characters (ASCII characters space (32) to ~ (126)
	Supported Characters	• A-Z • a-z • 0-9 • _space_!"#$%&'()*+,-./ • :;<=?@ • [\]^_` • {|}
CLI	Length	Between 2 and 32 characters
	Supported Characters	All characters

SSIDs Supported in Release 3.0 and Above

Release 3.0 and above supports a specific set of SSID syntaxes, which may be different from the syntaxes supported in other releases.

The following table describes the SSID syntaxes that are supported in release 3.0 and above.

TABLE 126 Supported SSID syntax in 3.0 and above

Web Interface and CLI	Length	Between 2 to 32 characters are supported
	Characters	Unsupported: ` and $(Space is allowed, but it must include at least one non-space character (" abc" is valid, however only space such as " " is invalid). **NOTE** One Chinese word is regarded as three special characters.

ZoneDirector SSID Syntax

The following sections describe the supported SSID syntax in the following vSZ-H release version:

SSIDs Supported in Releases 9.8 and 9.7

ZoneFlex releases 9.8 and 9.7 support a specific set of SSID syntaxes, which may be different from the syntaxes supported in other releases.

TABLE 127 Supported SSID syntaxes in ZoneFlex 9.8 and 9.7

Web Interface	Length	Between one and 32 characters
	Supported Characters	All printable ASCII characters from space (32) to ~(126)
	Exceptions	The space character (32) cannot be the first or last character in the SSID. Otherwise, the following error message appears: `can only contain between 1 and 32 characters, including characters from ! (char 33) to ~ (char 126).`

TABLE 127 Supported SSID syntaxes in ZoneFlex 9.8 and 9.7 (continued)

CLI	Length	Between one and 32 characters
	Supported Characters	All printable ASCII characters from space (32) to ~(126)
	Exceptions	The space character (32) can be placed anywhere in the SSID (including the beginning or end) provided that it enclosed by a double quotation mark.

Supported SSIDs in ZoneFlex Release 9.6

ZoneFlex release 9.6 supports a specific set of SSID syntaxes, which may be different from the syntaxes supported in other releases.

TABLE 128 Supported SSID syntaxes in ZoneFlex 9.6

Web Interface	Length	Between two and 32 characters
	Supported Characters	All printable ASCII characters from space (32) to ~(126)
	Exceptions	The space character (32) cannot be the first or last character in the SSID. Otherwise, the following error message appears: `can only contain between 1 and 32 characters, including characters from ! (char 33) to ~ (char 126).`
CLI	Length	Between two and 32 characters
	Supported Characters	All printable ASCII characters from space (32) to ~ (126)
	Exceptions	The space character (32) can be placed anywhere in the SSID (including the beginning or end) provided that it enclosed in a double quotation mark (for example, “RUCKUS SSID”).

ZoneFlex AP SSID Syntax

The following sections describe the supported SSID syntax in the following ZoneFlex AP release versions:

Supported SSIDs in Releases 9.8, 9.7, and 9.6

ZoneFlex release 9.8, 9.7, and 9.6 support a specific set of SSID syntaxes, which may be different from the syntaxes supported in other releases.

TABLE 129 Supported SSID syntaxes in ZoneFlex AP 9.8, 9.7, and 9.6

Web Interface	Length	Between one and 32 characters
	Supported Characters	All printable ASCII characters from space (32) to ~(126)

TABLE 129 Supported SSID syntaxes in ZoneFlex AP 9.8, 9.7, and 9.6 (continued)

CLI	Length	Between one and 32 characters
	Supported Characters	All printable ASCII characters from space (32) to ~ (126)
	Exceptions	The space character (32) can be placed anywhere in the SSID (including the beginning or end) provided that it enclosed in a double quotation mark (for example, "RUCKUS SSID"). If the space character is not enclosed in a double quotation mark, the space character and any characters after that will be ignored. For example, if you run the command "**set ssid wlan0 ruckus-ap 123**", the controller CLI will run the command as "**set ssid wlan0 ruckus-ap 123**".

Web Server Support

The **https://my.ruckus** web page is a supplementary tool for reporting a problem without much understanding of the infrastructure.

This page is hosted on the AP's Web Server. This feature is independent of the controller being accessible to the AP and provides the first level information required by the support engineer to diagnose a problem. When the AP is managed by SZ, the web-server shall be turned off and the page may not be accessible. You can turn on the web-server by using the **set https enable** command, which the controller may turn off later to conserve memory on the AP.

When connected to an authenticated WLAN, you can enter https://my.ruckus on a web browser and view the following diagnostic information:

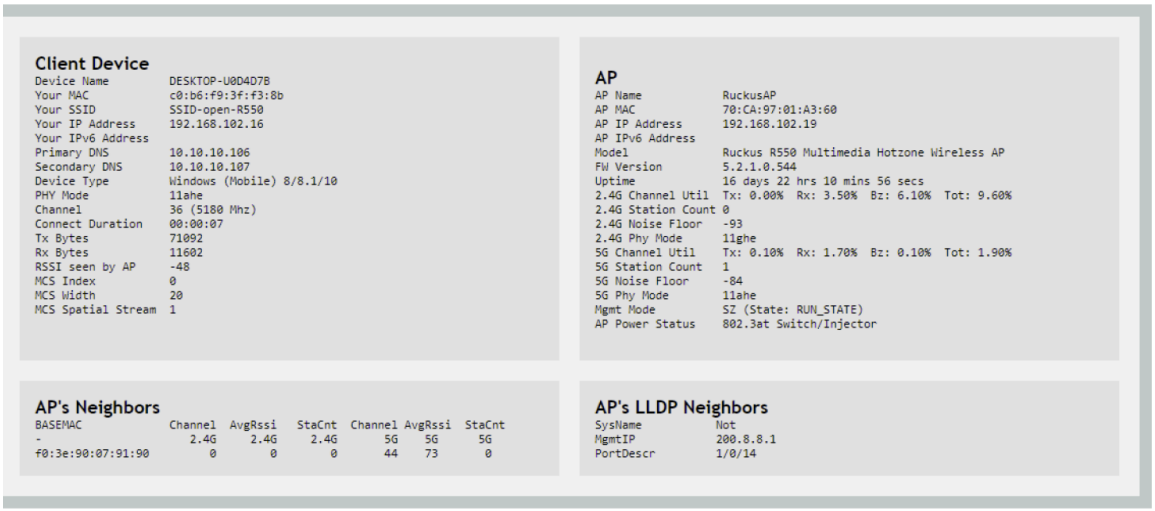
- Client Device
- AP
- AP's Neighbors (Wireless)
- AP's LLDP Neighbors (Wired)

FIGURE 392 Viewing Diagnostic Information in WPA2 WLAN



On entering https://my.ruckus when connected over an Open or WEP WLAN, the diagnostic information is restricted for security reasons.

FIGURE 393 Viewing Diagnostic Information in Open WLAN





© 2024 CommScope, Inc. All rights reserved.
350 West Java Dr., Sunnyvale, CA 94089 USA
https://www.commscope.com