CONFIGURATION GUIDE

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

Supporting SmartZone Release 7.0.0

Part Number: 800-73597-001 Rev B
Publication Date: August 2024

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

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

About This Guide

The RUCKUS SmartZone Network Administration Guide explains how to optimally configure your RUCKUS access points and WLAN services, from managing firewall options and traffic policies, to quality of service and administrative tasks in the access points. Additionally, this guide explains how to effectively manage your RUCKUS ICX switches and the available services for your wired network.

New In This Document

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

Feature	Description	Reference
Adding Icons.	Throughout the guide.	-
Adding Animated GIFs	Throughout the guide.	-
6G Outdoor and Indoor Channel Range Separation	Allows you to use channel options for indoor and outdoor channels.	• Creating an AP Group on page 30 • Creating an AP Zone on page 43 • Configuring Access Points on page 125
Cybersecurity	The Cybersecurity feature enhances the existing password security feature, ensuring compliance with stricter password configuration and usage rules that adhere to higher security standards.	• Cybersecurity on page 29 • Creating an AP Zone on page 43

License Requirements to Manage Access Points and Switches

There are certain licenses required for the SmartZone controller to operate network-managed equipment, including capacity licenses for onboarding the AP and switch devices and support licenses for entitling software upgrades and support services.

AP and Switch Capacity Licenses

Onboarding fully operational access points and switches to the SmartZone controller requires one capacity license per device (meaning, one AP Capacity License per access point and one Switch Capacity License per switch). When all applicable capacity licenses have been consumed, attempting to onboard new devices to the controller will fail and be reported with an error, such as: “AP onboarding failed due to not enough capacity licenses” or "Switch registration rejected by SZ due to license capacity".

NOTE
The Virtual SmartZone controllers come with default permanent Capacity licenses for one Access Point and one ICX Switch. If you plan to manage additional AP or switch devices, then licenses for additional devices must be acquired separately.

NOTE
Beginning with SmartZone release 6.1.0, the SZ-144 platform supports 25 permanent AP Capacity licenses. You may upgrade your SZ-144 firmware from earlier versions to release 6.1.0 or later to get the 25 permanent AP licenses.

NOTE
For SmartZone controllers operating in cluster mode, the capacity license availability is shared across all the nodes in the cluster. Refer to the *RUCKUS SmartZone Controller Administration Guide* for more details about cluster definition.

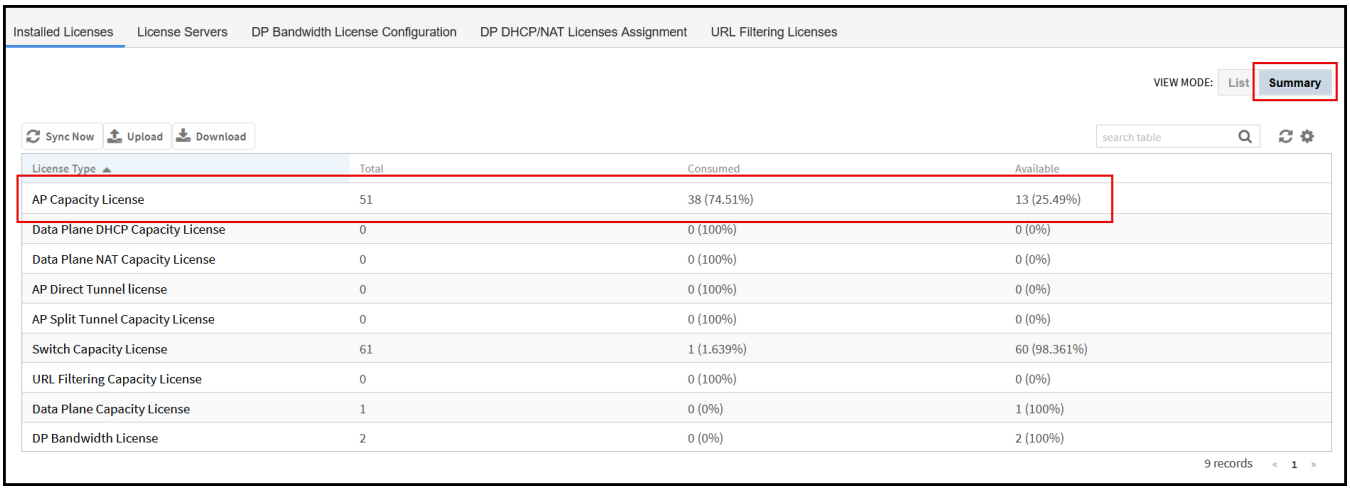
Verifying the Available AP Capacity Licenses in the Controller

SmartZone provides AP capacity license information in two locations, each providing slightly different amounts of information.

1. Navigate the main menu, clicking **Administration** > **Licenses** > **Installed Licenses**.
2. Change the view mode to **Summary**.

3. Check the number of avaliable and consumed AP capacity licences.

FIGURE 1 Checking the Available AP Capacity Licenses Using the Installed Licenses Menu Option

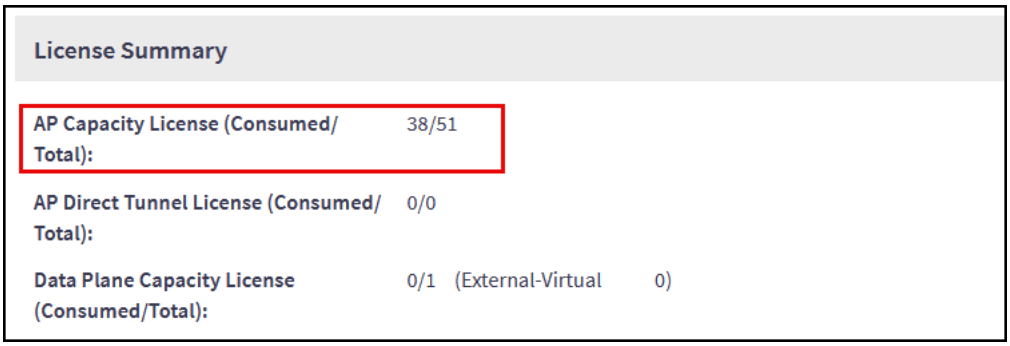


License Type	Total	Consumed	Available
AP Capacity License	51	38 (74.51%)	13 (25.49%)
Data Plane DHCP Capacity License	0	0 (100%)	0 (0%)
Data Plane NAT Capacity License	0	0 (100%)	0 (0%)
AP Direct Tunnel license	0	0 (100%)	0 (0%)
AP Split Tunnel Capacity License	0	0 (100%)	0 (0%)
Switch Capacity License	61	1 (1.639%)	60 (98.361%)
URL Filtering Capacity License	0	0 (100%)	0 (0%)
Data Plane Capacity License	1	0 (0%)	1 (100%)
DP Bandwidth License	2	0 (0%)	2 (100%)

To view the number of total and consumed AP capacity licenses, execute the following steps:

1. Navigate the main menu, clicking **Administration** > **System** > **System Info**. In the *About* tab scroll to the *License Summary* section to view the tally of consumed AP Capacity licenses out of the total licenses obtained.

FIGURE 2 Available AP Capacity Licenses

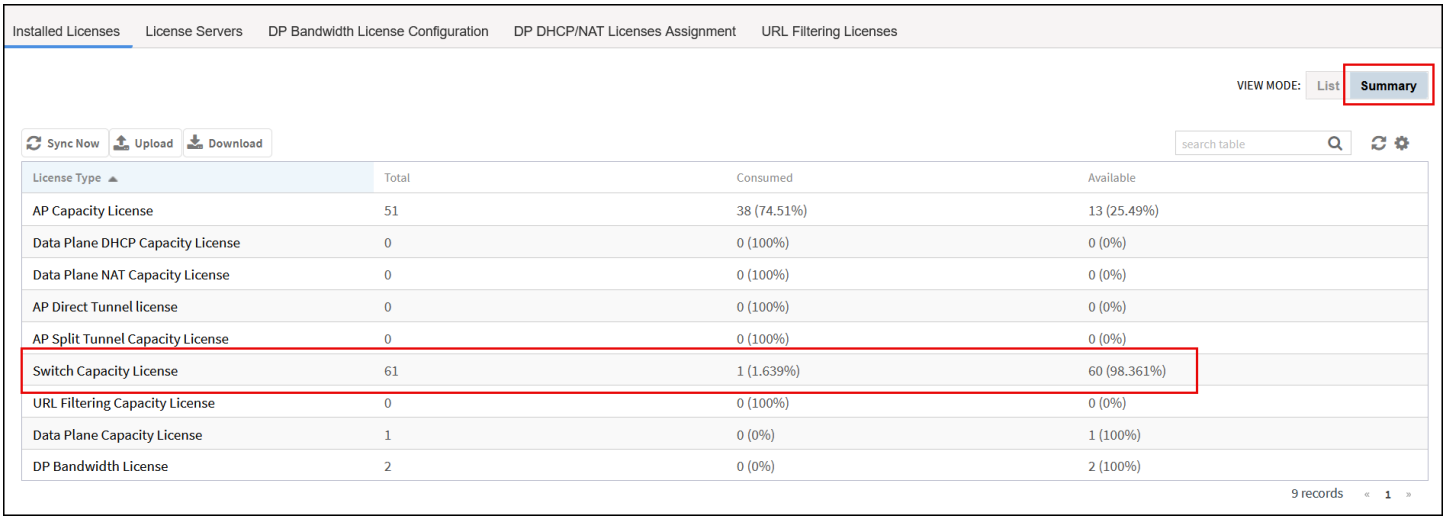


Verifying the Available Switch Capacity Licenses in the Controller

Follow these steps to access a summary of total, consumed, and available Switch Capacity licenses: Navigate to the main menu by clicking **Administration** > **Licenses** > **Installed Licenses**.

1. Change the view mode to **Summary**.
2. Check the number of available and consumed Switch Capacity licenses.

FIGURE 3 Available Switch Capacity Licenses



License Type	Total	Consumed	Available
AP Capacity License	51	38 (74.51%)	13 (25.49%)
Data Plane DHCP Capacity License	0	0 (100%)	0 (0%)
Data Plane NAT Capacity License	0	0 (100%)	0 (0%)
AP Direct Tunnel license	0	0 (100%)	0 (0%)
AP Split Tunnel Capacity License	0	0 (100%)	0 (0%)
Switch Capacity License	61	1 (1.639%)	60 (98.361%)
URL Filtering Capacity License	0	0 (100%)	0 (0%)
Data Plane Capacity License	1	0 (0%)	1 (100%)
DP Bandwidth License	2	0 (0%)	2 (100%)

AP Support Licenses

Apart from the AP Capacity licenses, which are for onboarding and managing the APs, AP Support licenses are required to complete any AP software upgrades using the controller. The AP Support license entitles 100% of your onboarded APs to software upgrades and RUCKUS Support assistance.

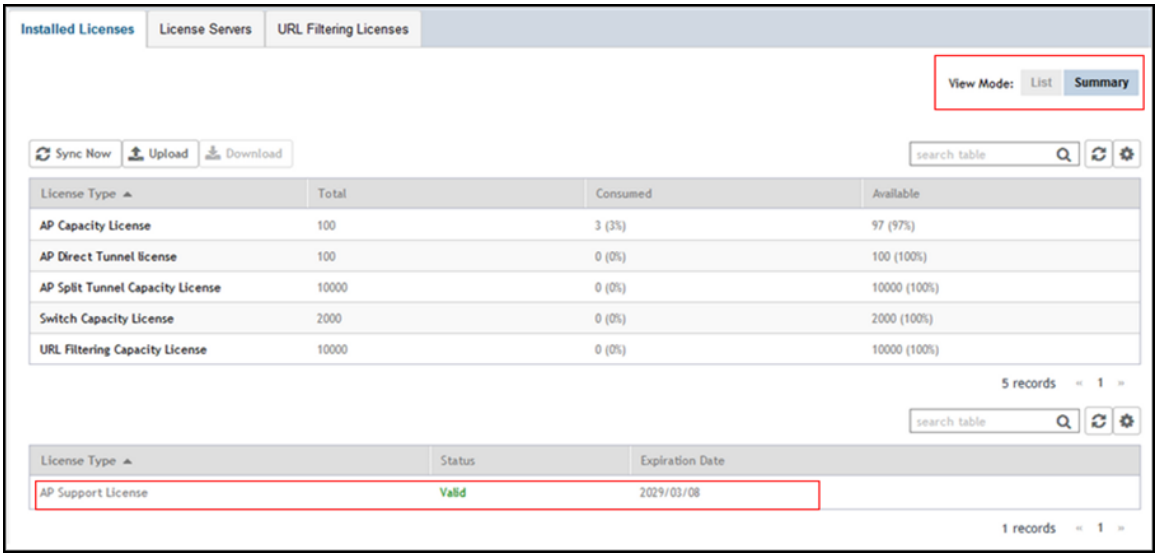
Verifying the AP Support Licenses

In the previous controller 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 Licenses** retrieved from the license server at any given point of time.

To view the AP license status and validity click **View** > **Summary** tab.

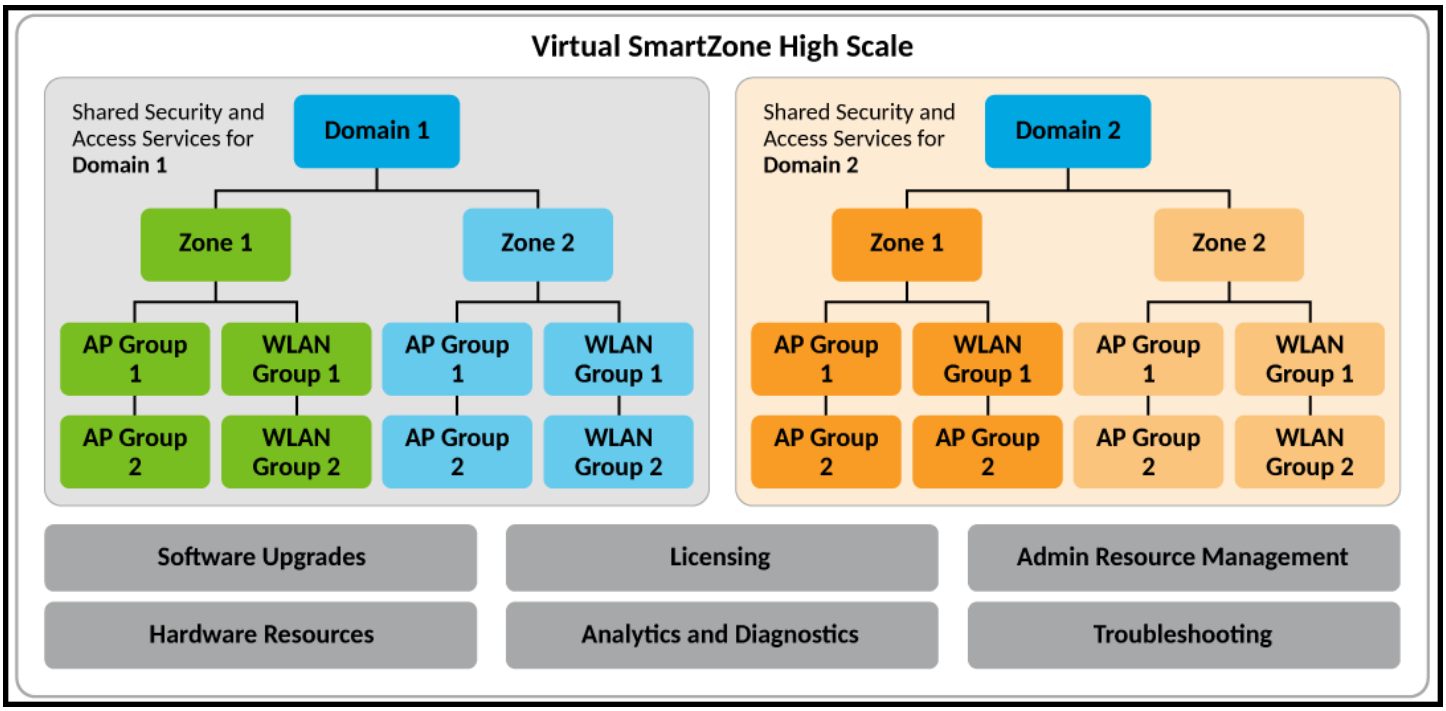
FIGURE 4 Installed AP License Summary



SmartZone Network Hierarchy

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

FIGURE 5 SmartZone Network Hierarchy



SmartZone Domains

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

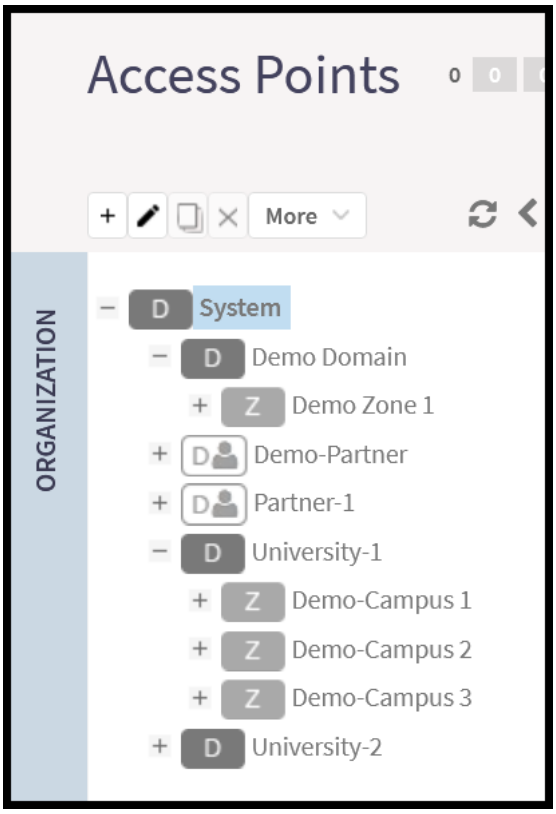
RUCKUS recommends utilizing Domains specifically when there is a need to establish distinct administrative boundaries within a network environment. In essence, Domains are employed to segregate different administrative realms, ensuring that each administrator is responsible for managing only a designated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

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

Partner Domains

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

FIGURE 6 Domains and Partner Domains



AP Zones

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

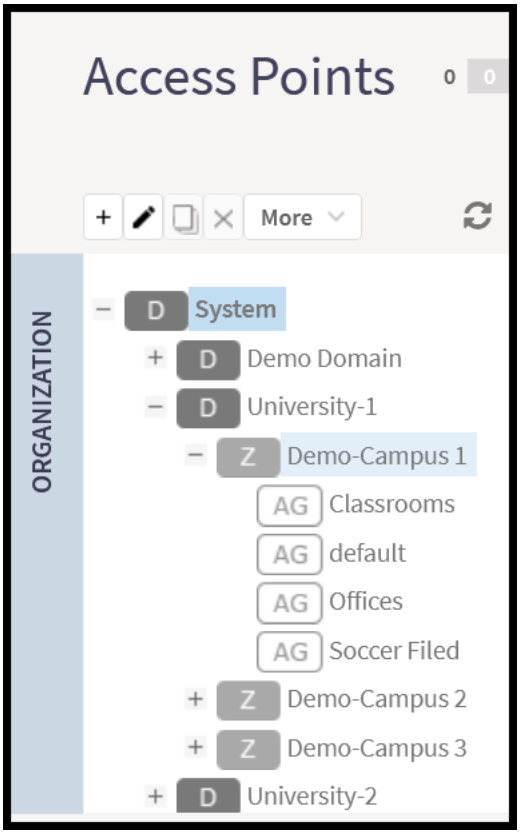
Furthermore, AP Zones share resources such as WLAN Groups and services like RADIUS authentication, guest access, and others, providing administrative flexibility and centralized management capabilities for each of the zones.

AP Groups

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

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

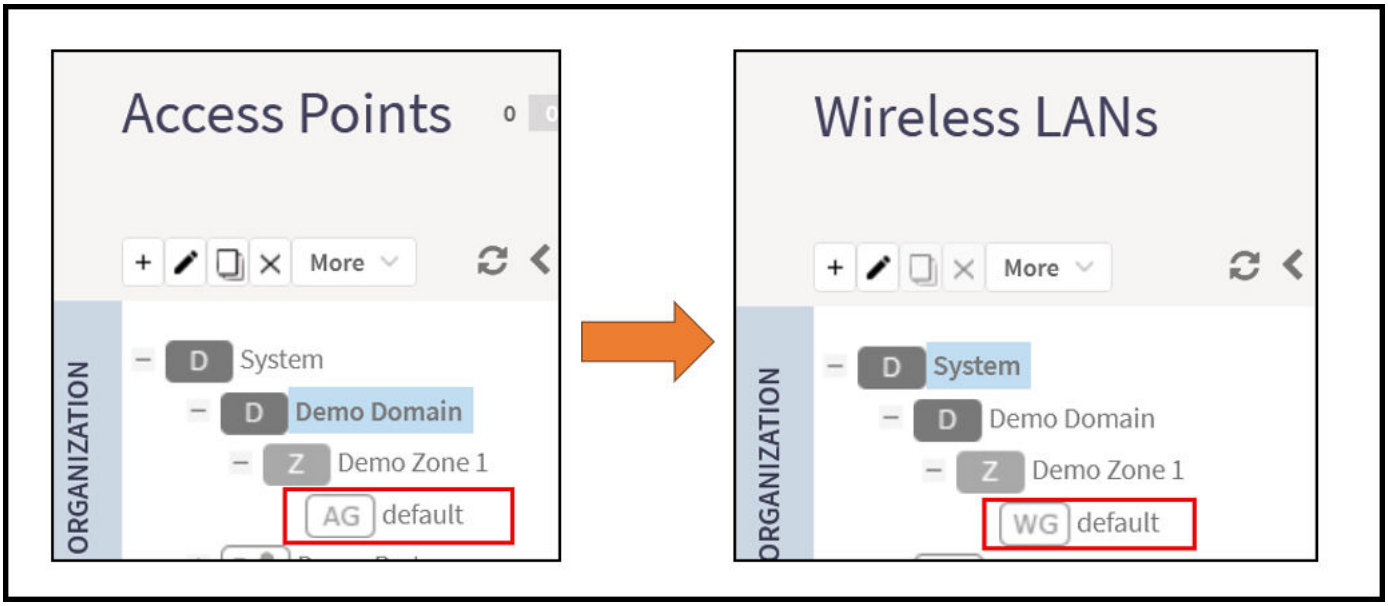
FIGURE 7 AP Domains, Zones, and Groups



WLAN Groups

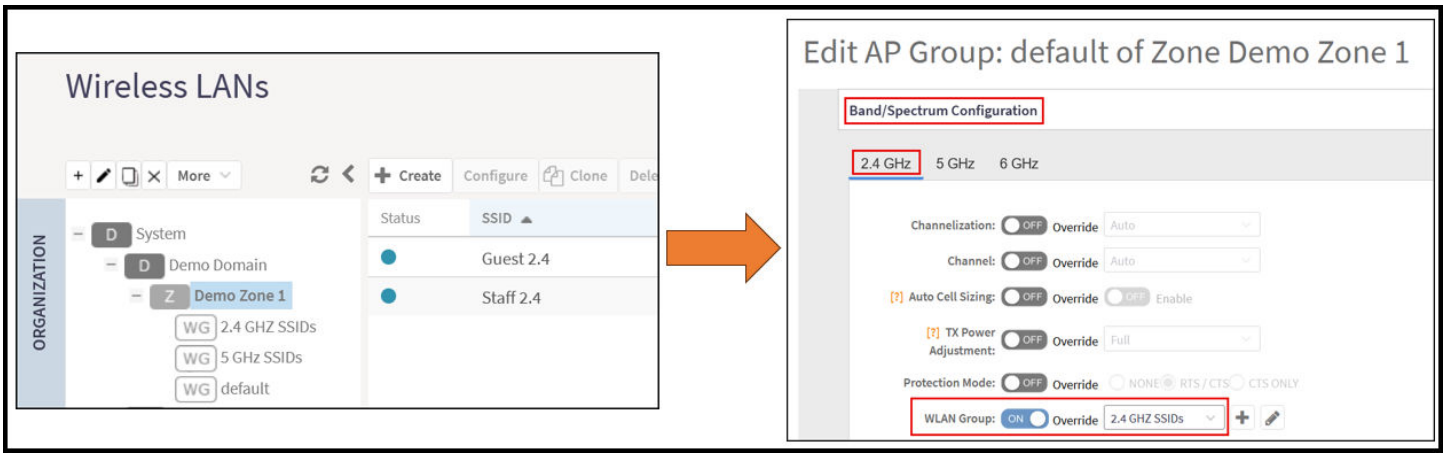
By default, when an AP Zone is created, a default WLAN Group is automatically created and assigned to the AP Zone and any AP Group within it; however, a new WLAN Group can be created on demand, and the administrator can override the default assignment at the AP Group level or at the individual AP level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

FIGURE 8 Automatic Creation of the Default AP Group and WLAN Group



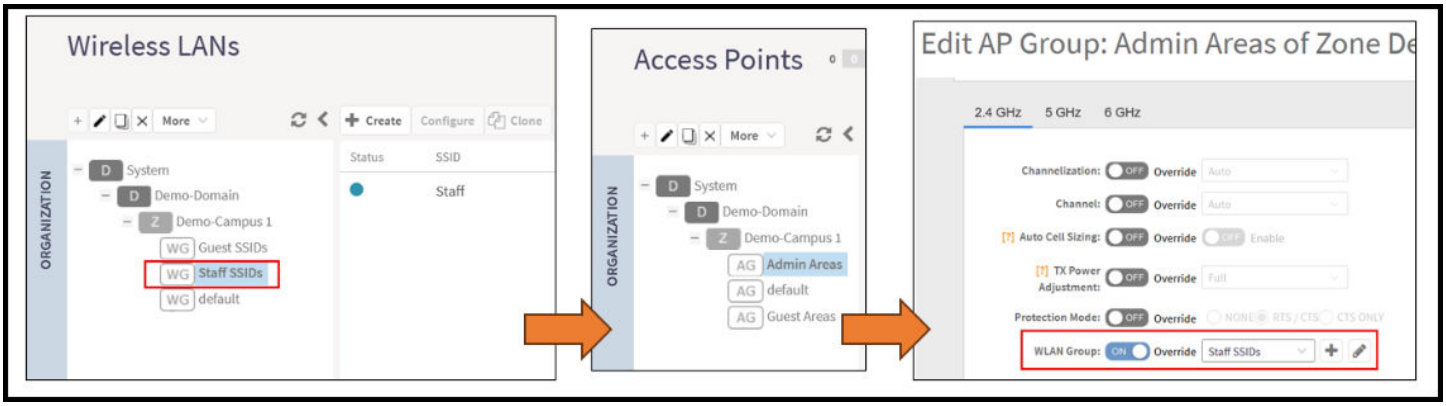
Grouping the SSIDs (WLANs) helps the administrator to assign WLAN Groups to different segments of the network, as necessary, by binding the WLAN Groups to AP Groups. Refer to the below use case example where the administrator has assigned a different WLAN Group to each radio band (2.4 GHz or 5 GHz).

FIGURE 9 Assigning a different WLAN Group to each radio band of an AP Group



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

FIGURE 10 Assigning a different WLAN Group to each AP Group

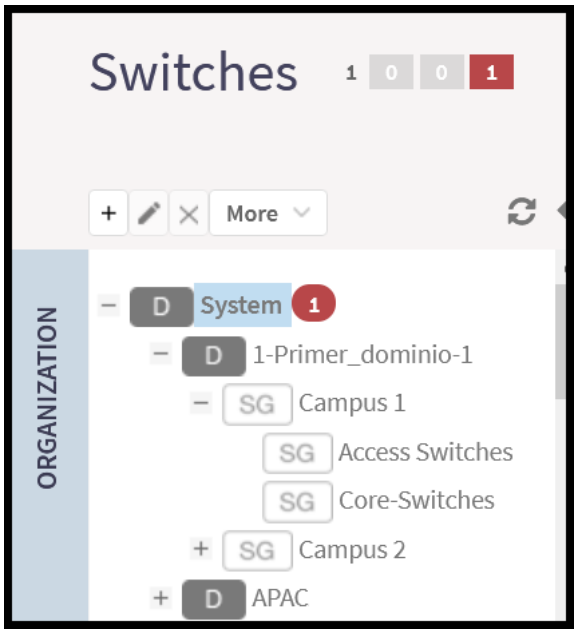


NOTE
For more information, refer to how to create or modify WLANs, WLAN Groups, and AP Groups, and all possible configuration options related to them.

Switch Groups

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

FIGURE 11 SmartZone Switch Groups



Creating an AP Domain

Limiting the Number of APs in a Domain or Zone

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

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.

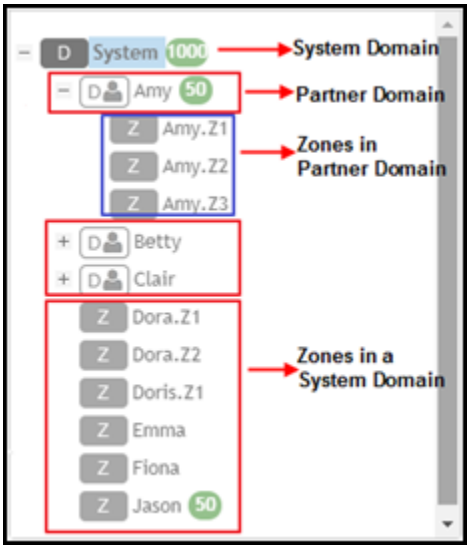
A scheduler task in the background periodically checks the AP number limitation against the number of APs connected. To avoid occupying the license capacity, the APs will be rejected in the following situations:

- 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 12 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.

2. Create a user group and configure the access permissions, resources and administrator account.

   NOTE
   Refer to *RUCKUS SmartZone Controller Administration Guide* for instructions on creating administrative accounts.

   NOTE
   While creating user groups, in step 4 (I) c, for **Permission**, select Super Admin from the drop-down.

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.

AP Groups

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.

Cybersecurity

The Cybersecurity feature enhances the existing password security feature, ensuring compliance with stricter password configuration and usage rules that adhere to higher security standards.

However, the factory-provided password is exempt from these compliance requirements because it is used only once during the initial login.

Requirements

This feature has no special hardware or software requirements for feature enablement or usage.

Prerequisites

This feature has no prerequisites to feature enablement or usage.

When setting up an AP for the first time, use these default credentials:

- **User**: super
- **Password**: sp-admin

For a factory reset, log in through the AP UI or AP CLI using the default credentials and change the password to comply with the following requirements:

- **Blank Spaces**: The password must not contain any blank spaces.
- **Character Complexity**: The password must be a minimum of 8 characters in length and include at least one lowercase letter, one uppercase letter, one number, and one special character.
- **Special Characters Allowed**: You can use the following special characters: **~!@#$%^&*()-=_+[]{}|;':",./<>?**

NOTE

- The password must not begin with the special character "**~**"
- The password cannot contain the special characters **$** and **(** consecutively
- Password for SNMP configuration must not include special characters **$;&()|<>'`**

- **Device-Specific Credentials**: Each device must have a unique password. Avoid using the initial factory setting credentials across all devices to prevent unauthorized access.

Remember that all passwords used to log in to an AP terminal or AP UI must comply with these requirements. Once you set a new password, use it for subsequent logins. The default password "sp-admin" is only for changing the password and cannot be used to configure or monitor the AP.

Considerations

- **Resetting Factory Settings**: When an AP is reset to its initial factory settings, also reset any passwords indicated on the product label or equipment enclosure.

Limitations

The controller upgrade process does not include validation of the current passwords, for APs in existing zones, against the cybersecurity requirements.

Meaning, after controller upgrade, the current passwords for the zone and APs will be retained until further user action prompts validation:

AP Password Validation:

- - Initially set AP passwords are stored as hashes, making the actual password unretrievable from the stored value.
  - Updates to AP password validation rules will not affect existing AP passwords due to the hash storage.

After the first login using the sp-admin user name, the AP will prompt the user to change the default password. Use the new password for subsequent logins. This behavior is already present in AP solo software and is now being used in the controller profile.

Best Practices

This feature has no special recommendations for feature enablement or usage.

Creating an AP Group

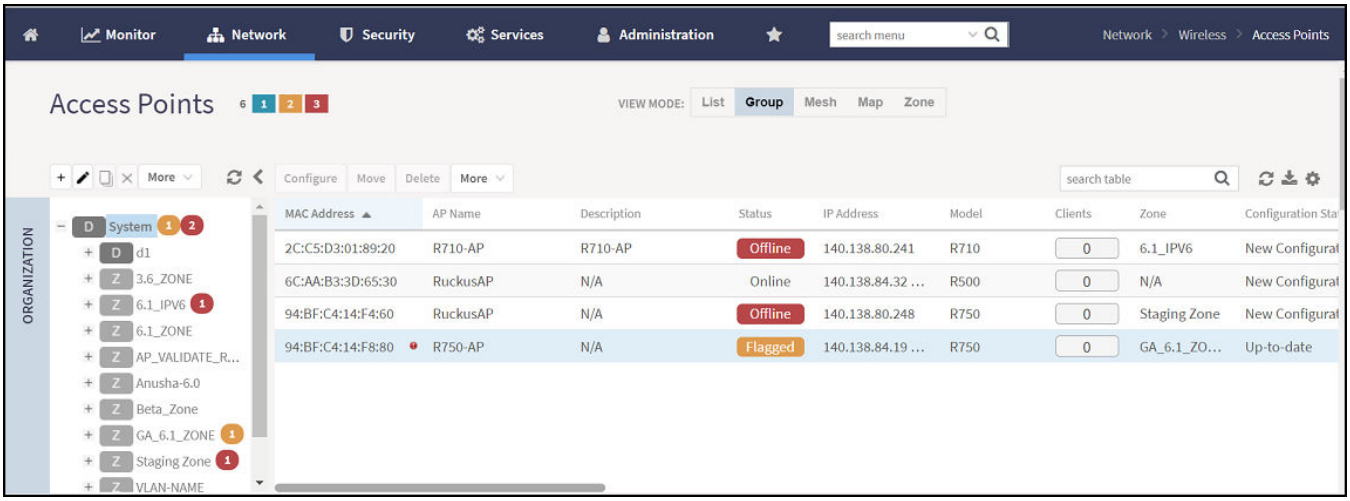
By creating an AP group, you can configure a profile that defines the channels, radio settings, Ethernet ports and other configurable fields for all members of the group or for all APs of a specific model in the group.

To create an AP Group, perform the following:

1. Click **Network** > **Wireless** > **Access Point**.

   This displays **Access Points** page.

FIGURE 13 Access Point Page



2. From the System tree hierarchy, select the zone and click . The **Create AP Group** page is displayed.
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 3 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.
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**
Radio Options		

TABLE 3 AP Group Details (continued)

Field	Description	Your Action
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.
Band/Spectrum Configuration > **2.4 GHz**		
Channelization	Helps manage and allocate radio frequency resources. A lower channel width allows the zone to potentially serve more clients, whereas a higher channel width improves throughput, but potentially serves fewer clients and increases the possibility of interference. The Auto setting defaults to 20 MHz channelization.	Set the channel bandwidth used during transmission to either 20 or 40 (MHz), or select Auto to set it automatically. **NOTE** By default, for the **Country Code** Indonesia, the **Channelization** width is set to 20 MHz only for outdoor APs.
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.
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 maintaining mesh links and to discover AP neighbors.	Enter the duration in seconds. Range: 1 through 65535.

TABLE 3 AP Group Details (continued)

Field	Description	Your Action
Auto Channel Selection	Automatically adjusts the channel for network self-healing and performance optimization. **ChannelFly** is set as the default option. For the **ChannelFly** option, you may also modify the default settings for the **Channel Change Frequency** and **Full Optimization Period**. The **Channel Change Frequency** slidebar allows you to specify the responsiveness of ChannelFly to interference (with consideration for the impact on associated clients), ranging from Minimal to Very Often. The **Full Optimization Period** timeslot bar allows you to specify one or more periods of time when ChannelFly is allowed to fully optimize the channel plan, ignoring the impact of channel changes on associated clients. Select time periods when the wireless network is servicing the fewest clients.	Select the required option. • **Background Scanning**: Changes the AP channel when there is an interference. • **ChannelFly**: Monitors potential throughput and will change channels to learn each channel's capacity, optimize throughput, and to avoid interference.
Band/Spectrum Configuration > **5 GHz**		
Channelization	Helps manage and allocate radio frequency resources. A lower channel width allows the zone to potentially serve more clients, whereas a higher channel width improves throughput, but potentially serves fewer clients and increases the possibility of interference. Prior to SmartZone release 7.0.0, the Auto setting defaulted to 80 MHz channelization. Beginning in SmartZone release 7.0.0, the Auto setting defaults to 40 MHz channelization.	Set the channel bandwidth used during transmission: Auto, 20, 40, 80 and 160. **NOTE** By default, for the **Country Code** Indonesia, the **Channelization** width is set to 20 MHz only for outdoor APs.
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 3 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 maintaining mesh links and to discover AP neighbors.	Enter the duration in seconds. Range: 1 through 65535.
Auto Channel Selection	Automatically adjusts the channel for network self-healing and performance optimization. **ChannelFly** is set as the default option. For the **ChannelFly** option, you may also modify the default settings for the **Channel Change Frequency** and **Full Optimization Period**. The **Channel Change Frequency** slidebar allows you to specify the responsiveness of ChannelFly to interference (with consideration for the impact on associated clients), ranging from Minimal to Very Often. The **Full Optimization Period** timeslot bar allows you to specify one or more periods of time when ChannelFly is allowed to fully optimize the channel plan, ignoring the impact of channel changes on associated clients. Select time periods when the wireless network is servicing the fewest clients.	Select the required option. • **Background Scanning**: Changes the AP channel when there is an interference. • **ChannelFly**: Monitors potential throughput and will change channels to learn each channel's capacity, optimize throughput, and to avoid interference.
Band/Spectrum Configuration > **6 GHz** **NOTE** This tab is available only if the **Tri-band Dual-5G Mode** option is not enabled.		
Channelization	Helps manage and allocate radio frequency resources. A lower channel width allows the zone to potentially serve more clients, whereas a higher channel width improves throughput, but potentially serves fewer clients and increases the possibility of interference. The Auto setting defaults to 160 MHz channelization.	Set the channel bandwidth used during transmission: Auto, 20, 40, 80 and 160.

TABLE 3 AP Group Details (continued)

Field	Description	Your Action
Channel	Indicates the channel to use.	• In countries where only 6 GHz Indoor channels are permitted, the 6 GHz Outdoor channels are disabled. • If a country permits the use of 6GHz Indoor and Outdoor channels, the controller will provide the available channel ranges for both the channels. For example, in the US, the available channel ranges are - – Indoor APs can operate in UNII-5,6,7,8 – Outdoor APs can operate in UNII-5,7 • You can choose channel options for Indoor and Outdoor channels. The default setting for both Indoor and Outdoor channels is **Auto**.
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.
Enable AFC	The Enable AFC function acts as a communication agent between the controller and the AP. RUCKUS APs supporting the 6GHz band require AFC support to switch to Standard Power Mode. The Enable AFC button can be toggled when the country of the zone supports AFC. If AFC is enabled, the AP would send an AFC request to acquire permission to turn to standard power in the 6GHz band. If AFC permission is granted, then the AP could switch to Standard Power mode. Otherwise, indoor APs should remain in Low Power Mode, and outdoor APs will turn off the 6GHz band.	Click the button.
Background Scan	Allows the AP radio to scan other channels in the band for accessing channel health and capacity, detecting rogue devices, optimizing and maintaining mesh links and to discover AP neighbors.	Enter the duration in seconds. Range: 1 through 65535.

TABLE 3 AP Group Details (continued)

Field	Description	Your Action
Auto Channel Selection	Automatically adjusts the channel for network self-healing and performance optimization. **ChannelFly** is set as the default option. For the **ChannelFly** option, you may also modify the default settings for the **Channel Change Frequency** and **Full Optimization Period**. The **Channel Change Frequency** slidebar allows you to specify the responsiveness of ChannelFly to interference (with consideration for the impact on associated clients), ranging from Minimal to Very Often. The **Full Optimization Period** timeslot bar allows you to specify one or more periods of time when ChannelFly is allowed to fully optimize the channel plan, ignoring the impact of channel changes on associated clients. Select time periods when the wireless network is servicing the fewest clients.	Select the required option. • **Background Scanning**: Changes the AP channel when there is an interference. • **ChannelFly**: Monitors potential throughput and will change channels to learn each channel's capacity, optimize throughput, and to avoid interference.
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 options: • 6 mbps • 9 mbps • 12 mbps • 18 mbps • 24 mbps
6G Mgmt Tx Rate	Sets the transmit rate for management frame types such as beacon and probes.	Select one of the following options: • 6 mbps • 9 mbps • 12 mbps • 18 mbps • 24 mbps
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%, for example: 3.00Mbps to 4.00Mbps traffic passes. This limit is only for downlink and is not affected by BSS Min Rate setting. **NOTE** SSID Rate Limit always takes 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** The Multicast Rate Limit value cannot exceed SSID Rate Limit values for respective **Uplink** and **Downlink** direction.
Band/Spectrum Configuration > **Lower 5 GHz**		

TABLE 3 AP Group Details (continued)

Field	Description	Your Action
Channelization	Helps manage and allocate radio frequency resources. A lower channel width allows the zone to potentially serve more clients, whereas a higher channel width improves throughput, but potentially serves fewer clients and increases the possibility of interference. Prior to SmartZone release 7.0.0, the Auto setting defaulted to 80 MHz channelization. Beginning in SmartZone release 7.0.0, the Auto setting defaults to 40 MHz channelization.	Set the channel bandwidth used during transmission: Auto, 20, 40, 80 and 160. **NOTE** By default, for the **Country Code** Indonesia, the **Channelization** width is set to 20 MHz only for outdoor APs.
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 maintaining mesh links and to discover AP neighbors.	Enter the duration in seconds. Range: 1 through 65535.

TABLE 3 AP Group Details (continued)

Field	Description	Your Action
Auto Channel Selection	Automatically adjusts the channel for network self-healing and performance optimization. **ChannelFly** is set as the default option. For the **ChannelFly** option, you may also modify the default settings for the **Channel Change Frequency** and **Full Optimization Period**. The **Channel Change Frequency** slidebar allows you to specify the responsiveness of ChannelFly to interference (with consideration for the impact on associated clients), ranging from Minimal to Very Often. The **Full Optimization Period** timeslot bar allows you to specify one or more periods of time when ChannelFly is allowed to fully optimize the channel plan, ignoring the impact of channel changes on associated clients. Select time periods when the wireless network is servicing the fewest clients.	Select the required option. • **Background Scanning**: Changes the AP channel when there is an interference. • **ChannelFly**: Monitors potential throughput and will change channels to learn each channel's capacity, optimize throughput, and to avoid interference.
Band/Spectrum Configuration > **Upper 5 GHz**		
Channelization	Helps manage and allocate radio frequency resources. A lower channel width allows the zone to potentially serve more clients, whereas a higher channel width improves throughput, but potentially serves fewer clients and increases the possibility of interference. Prior to SmartZone release 7.0.0, the Auto setting defaulted to 80 MHz channelization. Beginning in SmartZone release 7.0.0, the Auto setting defaults to 40 MHz channelization.	Set the channel bandwidth 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 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.

TABLE 3 AP Group Details (continued)

Field	Description	Your Action
TX Power Adjustment	Configures the power transmitted on the upper 5ghz, manually 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 power transmitted power is set to 0dBm (1mW) per chain for 11n APs, and 2dBm per chain for 11ac APs. If you choose Max, the power transmitted 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 maintaining mesh links and to discover AP neighbors.	Enter the duration in seconds. Range: 1 through 65535.
Auto Channel Selection	Automatically adjusts the channel for network self-healing and performance optimization. **ChannelFly** is set as the default option. For the **ChannelFly** option, you may also modify the default settings for the **Channel Change Frequency** and **Full Optimization Period**. The **Channel Change Frequency** slidebar allows you to specify the responsiveness of ChannelFly to interference (with consideration for the impact on associated clients), ranging from Minimal to Very Often. The **Full Optimization Period** timeslot bar allows you to specify one or more periods of time when ChannelFly is allowed to fully optimize the channel plan, ignoring the impact of channel changes on associated clients. Select time periods when the wireless network is servicing the fewest clients.	Select the required option. • **Background Scanning**: Changes the AP channel when there is an interference. • **ChannelFly**: Monitors potential throughput and will change channels to learn each channel's capacity, optimize throughput, and to avoid interference.
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 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**.

TABLE 3 AP Group Details (continued)

Field	Description	Your Action
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**.
Model Specific Options **NOTE** Select the **Override** check box for each setting to change its default configuration.		
AP Model	Indicates AP model for which the configuration is done.	Select the option.
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.
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.
PoE Operating Mode	PoE Operating Mode allows manual control of power negotiation between the AP and the power source. Default is Auto, allowing the correct power requirement to be negotiated between the AP and the power source **NOTE** You can set the PoE operating mode from the **AP Configuration** tab on the controller or using the **get power-mode** CLI command. The R730 AP is supported only in SZ6.1.0 firmware zone.	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.

TABLE 3 AP Group Details (continued)

Field	Description	Your Action
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.
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.
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.
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**

TABLE 3 AP Group Details (continued)

Field	Description	Your Action
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 **Override** 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**
Venue Code	Indicates the venue code.	You can choose to override this setting and enter the code in the field provided.
BSS Coloring	Indicates the BSS coloring settings.	• Select the **Override zone configuration** check box. • Select the **Enable BSS Coloring** check box.

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.

NOTE

Starting with the 7.0 release, the support for **Cellular Options** while configuring or creating an AP Group is removed from the controller web interface.

Working with AP Zones

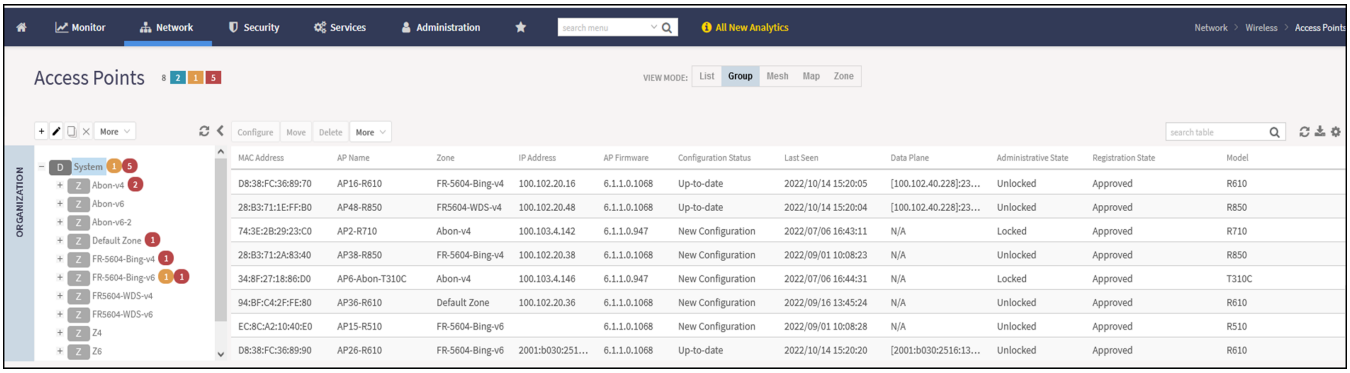
Creating an AP Zone

An AP zone functions as a way of grouping RUCKUS wireless APs and applying settings and WLAN services to these groups.

To create an AP zone, complete the following steps:

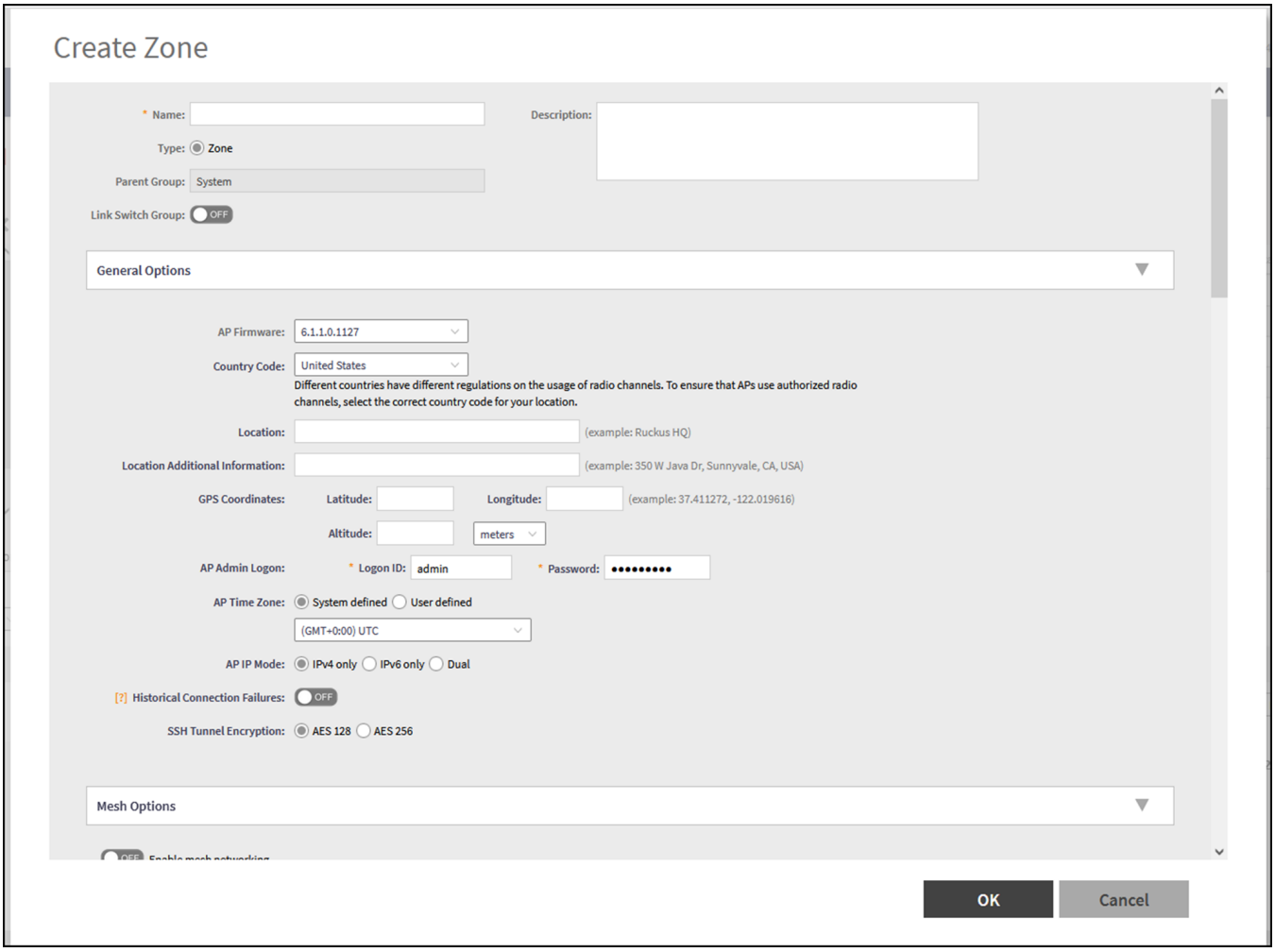
1. On the menu, click **Network** > **Wireless** > **Access Point**.

   FIGURE 14 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 15 Create Zone Page



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

TABLE 4 AP Zone Details for SZ300 and vSZ-H platforms

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.

TABLE 4 AP Zone Details for SZ300 and vSZ-H platforms (continued)

Field	Description	Your Action
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.
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.	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.Use the newly created password in accordance with the cybersecurity requirement. **NOTE** Password for SNMP configuration must not include special characters **$;&()|<>'`**	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 4 AP Zone Details for SZ300 and vSZ-H platforms (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**
Mesh Options		
NOTE Regardless of Single or Dual band, APs mesh with only there channel of radio which is in range.		
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.	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/6 GHz.
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.
Band/Spectrum Configuration > **2.4 GHz**		
Channelization	Helps manage and allocate radio frequency resources. A lower channel width allows the zone to potentially serve more clients, whereas a higher channel width improves throughput, but potentially serves fewer clients and increases the possibility of interference. The Auto setting defaults to 20 MHz channelization.	Set the channel bandwidth used during transmission to either **20** or **40** (MHz), or select **Auto** to set it automatically. **NOTE** By default, for the **Country Code** Indonesia, the **Channelization** width is set to 20 MHz only for outdoor APs.
Channel	Indicates the channel to use.	Select one of the options: **Auto**, **1**, **6** or **11**.

TABLE 4 AP Zone Details for SZ300 and vSZ-H platforms (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 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 maintaining mesh links and to discover AP neighbors.	Enter the duration in seconds. Range: 1 through 65535.
Auto Channel Selection	Automatically adjusts the channel for network self-healing and performance optimization. **ChannelFly** is set as the default option. For the **ChannelFly** option, you may also modify the default settings for the **Channel Change Frequency** and **Full Optimization Period**. The **Channel Change Frequency** slidebar allows you to specify the responsiveness of ChannelFly to interference (with consideration for the impact on associated clients), ranging from Minimal to Very Often. The **Full Optimization Period** timeslot bar allows you to specify one or more periods of time when ChannelFly is allowed to fully optimize the channel plan, ignoring the impact of channel changes on associated clients. Select time periods when the wireless network is servicing the fewest clients.	Select the required option. ● **Background Scanning**: Changes the AP channel when there is interference. ● **ChannelFly**: Monitors potential throughput and will change channels to learn each channel's capacity, optimize throughput, and to avoid interference.
Band/Spectrum Configuration > **5 GHz**		

TABLE 4 AP Zone Details for SZ300 and vSZ-H platforms (continued)

Field	Description	Your Action
Channelization	Helps manage and allocate radio frequency resources. A lower channel width allows the zone to potentially serve more clients, whereas a higher channel width improves throughput, but potentially serves fewer clients and increases the possibility of interference. Prior to SmartZone release 7.0.0, the Auto setting defaulted to 80 MHz channelization. Beginning in SmartZone release 7.0.0, the Auto setting defaults to 40 MHz channelization.	Set the channel bandwidth used during transmission: Auto, 20, 40, 80 and 160. **NOTE** By default, for the **Country Code** Indonesia, the **Channelization** width is set to 20 MHz only for outdoor APs.
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.
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.

TABLE 4 AP Zone Details for SZ300 and vSZ-H platforms (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 maintaining mesh links and to discover AP neighbors.	Enter the duration in seconds. Range: 1 through 65535.
Auto Channel Selection	Automatically adjusts the channel for network self-healing and performance optimization. **ChannelFly** is set as the default option. For the **ChannelFly** option, you may also modify the default settings for the **Channel Change Frequency** and **Full Optimization Period**. The **Channel Change Frequency** slidebar allows you to specify the responsiveness of ChannelFly to interference (with consideration for the impact on associated clients), ranging from Minimal to Very Often. The **Full Optimization Period** timeslot bar allows you to specify one or more periods of time when ChannelFly is allowed to fully optimize the channel plan, ignoring the impact of channel changes on associated clients. Select time periods when the wireless network is servicing the fewest clients.	Select the required option. ● **Background Scanning**: Changes the AP channel when there is interference. ● **ChannelFly**: Monitors potential throughput and will change channels to learn each channel's capacity, optimize throughput, and to avoid interference.
Band/Spectrum Configuration > **6 GHz** **NOTE** This tab is available only if the **Tri-band Dual-5G Mode** option is not enabled.		
Channelization	Helps manage and allocate radio frequency resources. A lower channel width allows the zone to potentially serve more clients, whereas a higher channel width improves throughput, but potentially serves fewer clients and increases the possibility of interference. The Auto setting defaults to 160 MHz channelization.	Set the channel bandwidth used during transmission: **Auto**, **20**, **40**, **80**, **160** and **320**. **NOTE** The 320 MHz-radio frequency is available only for the R770 AP 6 GHz radio frequency.
Channel	Indicates the channel to use.	● In countries where only 6 GHz Indoor channels are permitted, the 6 GHz Outdoor channels are disabled. ● If a country permits the use of 6GHz Indoor and Outdoor channels, the controller will provide the available channel ranges for both Indoor and Outdoor channels. For example, in the US, the available channel ranges are - – Indoor APs can operate in UNII-5,6,7,8 – Outdoor APs can operate in UNII-5,7 ● You can choose channel options for Indoor and Outdoor channels. The default setting for both Indoor and Outdoor channels is **Auto**.

TABLE 4 AP Zone Details for SZ300 and vSZ-H platforms (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 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.
Enable AFC	The Enable AFC function acts as a communication agent between the controller and the AP. RUCKUS APs supporting the 6GHz band require AFC support to switch to Standard Power Mode. The Enable AFC button can be toggled when the country of the zone supports AFC. If AFC is enabled, the AP would send an AFC request to acquire permission to turn to standard power in the 6GHz band. If AFC permission is granted, then the AP could switch to Standard Power mode. Otherwise, indoor APs should remain in Low Power Mode, and outdoor APs will turn off the 6GHz band. Refer to Automated Frequency Coordination System on page 74 for a comprehensive understanding of this feature.	For the newly created zone, AFC will be enabled by default if the country permits it. For an existing zone, the **Enable AFC** feature will be disabled. You will need to manually select it.
Background Scan	Allows the AP radio to scan other channels in the band for accessing channel health and capacity, detecting rogue devices, optimizing and maintaining mesh links and to discover AP neighbors.	Enter the duration in seconds. Range: 1 through 65535.

TABLE 4 AP Zone Details for SZ300 and vSZ-H platforms (continued)

Field	Description	Your Action
Auto Channel Selection	Automatically adjusts the channel for network self-healing and performance optimization. **ChannelFly** is set as the default option. For the **ChannelFly** option, you may also modify the default settings for the **Channel Change Frequency** and **Full Optimization Period**. The **Channel Change Frequency** slidebar allows you to specify the responsiveness of ChannelFly to interference (with consideration for the impact on associated clients), ranging from Minimal to Very Often. The **Full Optimization Period** timeslot bar allows you to specify one or more periods of time when ChannelFly is allowed to fully optimize the channel plan, ignoring the impact of channel changes on associated clients. Select time periods when the wireless network is servicing the fewest clients.	Select the required option. • **Background Scanning**: Changes the AP channel when there is interference. • **ChannelFly**: Monitors potential throughput and will change channels to learn each channel's capacity, optimize throughput, and to avoid interference.
Band/Spectrum Configuration > **Lower 5 GHz**		
Channelization	Helps manage and allocate radio frequency resources. A lower channel width allows the zone to potentially serve more clients, whereas a higher channel width improves throughput, but potentially serves fewer clients and increases the possibility of interference. Prior to SmartZone release 7.0.0, the Auto setting defaulted to 80 MHz channelization. Beginning in SmartZone release 7.0.0, the Auto setting defaults to 40 MHz channelization.	Set the channel bandwidth used during transmission: Auto, 20, 40, 80 and 160. **NOTE** By default, for the **Country Code** Indonesia, the **Channelization** width is set to 20 MHz only for outdoor APs.
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.

TABLE 4 AP Zone Details for SZ300 and vSZ-H platforms (continued)

Field	Description	Your Action
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 maintaining mesh links and to discover AP neighbors.	Enter the duration in seconds. Range: 1 through 65535.
Auto Channel Selection	Automatically adjusts the channel for network self-healing and performance optimization. **ChannelFly** is set as the default option. For the **ChannelFly** option, you may also modify the default settings for the **Channel Change Frequency** and **Full Optimization Period**. The **Channel Change Frequency** slidebar allows you to specify the responsiveness of ChannelFly to interference (with consideration for the impact on associated clients), ranging from Minimal to Very Often. The **Full Optimization Period** timeslot bar allows you to specify one or more periods of time when ChannelFly is allowed to fully optimize the channel plan, ignoring the impact of channel changes on associated clients. Select time periods when the wireless network is servicing the fewest clients.	Select the required option. • **Background Scanning**: Changes the AP channel when there is interference. • **ChannelFly**: Monitors potential throughput and will change channels to learn each channel's capacity, optimize throughput, and to avoid interference.
Band/Spectrum Configuration > **Upper 5 GHz**		
Channelization	Helps manage and allocate radio frequency resources. A lower channel width allows the zone to potentially serve more clients, whereas a higher channel width improves throughput, but potentially serves fewer clients and increases the possibility of interference. Prior to SmartZone release 7.0.0, the Auto setting defaulted to 80 MHz channelization. Beginning in SmartZone release 7.0.0, the Auto setting defaults to 40 MHz channelization.	Set the channel bandwidth 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 4 AP Zone Details for SZ300 and vSZ-H platforms (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 maintaining mesh links and to discover AP neighbors.	Enter the duration in seconds. Range: 1 through 65535.

TABLE 4 AP Zone Details for SZ300 and vSZ-H platforms (continued)

Field	Description	Your Action
Auto Channel Selection	Automatically adjusts the channel for network self-healing and performance optimization. **ChannelFly** is set as the default option. For the **ChannelFly** option, you may also modify the default settings for the **Channel Change Frequency** and **Full Optimization Period**. The **Channel Change Frequency** slidebar allows you to specify the responsiveness of ChannelFly to interference (with consideration for the impact on associated clients), ranging from Minimal to Very Often. The **Full Optimization Period** timeslot bar allows you to specify one or more periods of time when ChannelFly is allowed to fully optimize the channel plan, ignoring the impact of channel changes on associated clients. Select time periods when the wireless network is servicing the fewest clients.	Select the required option. ● **Background Scanning**: Changes the AP channel when there is interference. ● **ChannelFly**: Monitors potential throughput and will change channels to learn each channel's capacity, optimize throughput, and to avoid interference.
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.
Syslog Options		
Enable external syslog server for APs	Enables the AP to send syslog data to the syslog server on the network.	Select the option.

TABLE 4 AP Zone Details for SZ300 and vSZ-H platforms (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. › **Protocol**: 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. › **Protocol**: 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.
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 4 AP Zone Details for SZ300 and vSZ-H platforms (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. **Auth Pass Phrase**: Use the newly created password in accordance with the cybersecurity requirement. **NOTE** Password for SNMP configuration must not include special characters **$;&()|<>'`** 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**.
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.
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.

TABLE 4 AP Zone Details for SZ300 and vSZ-H platforms (continued)

Field	Description	Your Action
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.

TABLE 4 AP Zone Details for SZ300 and vSZ-H platforms (continued)

Field	Description	Your Action
Load Balancing	Balances the number of clients or the available capacity across APs.	Select the required option: ● Based on Client Count: If this option is selected, **Steering Mode** and **Sticky Client** options are enabled. – **Steering Mode** - Controls the APs' steering behavior for load 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. – **Sticky Client Steering**: Some client devices connect to an AP and stay connected to the same servicing AP, and does not change its association to the closer APs. These clients are referred as sticky clients. These clients may experience degradation in service because of lower throughput resulting in poor user experience. The purpose of the sticky client steering functionality is to identify these clients and assist in transition to a better AP. Click on the toggle button to enable the options. › SNR Threshold - Signal-to-Noise (SNR) ratio value evalutes signal based on the noise. Enter the value between 5db to 30db. › NBRAP % Threshold - NBRAP (Neighbor AP) percentage is used to calculate a base SNR and compare it to the SNR received from a neighbor AP. Enter the percentage (%) range between 10-40.

TABLE 4 AP Zone Details for SZ300 and vSZ-H platforms (continued)

Field	Description	Your Action
		• **Based on Capacity**: This option performs the similar functionality as **Based on Client Count** the difference is Limit 2.4Ghz Client to is disabled. • **Disabled** - By default, **Disabled** option is selected. **NOTE** The band change is applicable only for those connected clients that support the 802.11v standard.
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.
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.

TABLE 5 AP Zone Details for SZ100 and vSZ-E platforms

Field	Description	Your Action
Name	Indicates the name of the zone or 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.

TABLE 5 AP Zone Details for SZ100 and vSZ-E platforms (continued)

Field	Description	Your Action
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.
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.	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.	Click the button.
SSH Tunnel Encryption	Specifies the encryption that reduces the load on controller control of SSH traffic.	Select the required option: • **AES 128** • **AES 256**
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.	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/6 GHz.
Radio Options		

TABLE 5 AP Zone Details for SZ100 and vSZ-E platforms (continued)

Field	Description	Your Action
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.
Band/Spectrum Configuration > 2.4 GHz		
Channelization	Helps manage and allocate radio frequency resources. A lower channel width allows the zone to potentially serve more clients, whereas a higher channel width improves throughput, but potentially serves fewer clients and increases the possibility of interference. The Auto setting defaults to 20 MHz channelization.	Set the channel bandwidth used during transmission to either 20 or 40 (MHz), or select Auto to set it automatically. **NOTE** By default, for the **Country Code** Indonesia, the **Channelization** width is set to 20 MHz only for outdoor APs.
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.
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 maintaining mesh links and to discover AP neighbors.	Enter the duration in seconds. Range: 1 through 65535.

TABLE 5 AP Zone Details for SZ100 and vSZ-E platforms (continued)

Field	Description	Your Action
Auto Channel Selection	Automatically adjusts the channel for network self-healing and performance optimization. **ChannelFly** is set as the default option. For the **ChannelFly** option, you may also modify the default settings for the **Channel Change Frequency** and **Full Optimization Period**. The **Channel Change Frequency** slidebar allows you to specify the responsiveness of ChannelFly to interference (with consideration for the impact on associated clients), ranging from Minimal to Very Often. The **Full Optimization Period** timeslot bar allows you to specify one or more periods of time when ChannelFly is allowed to fully optimize the channel plan, ignoring the impact of channel changes on associated clients. Select time periods when the wireless network is servicing the fewest clients.	Select the required option. • **Background Scanning**: Changes the AP channel when there is interference. • **ChannelFly**: Monitors potential throughput and will change channels to learn each channel's capacity, optimize throughput, and to avoid interference.
Band/Spectrum Configuration > **5 GHz**		
Channelization	Helps manage and allocate radio frequency resources. A lower channel width allows the zone to potentially serve more clients, whereas a higher channel width improves throughput, but potentially serves fewer clients and increases the possibility of interference. Prior to SmartZone release 7.0.0, the Auto setting defaulted to 80 MHz channelization. Beginning in SmartZone release 7.0.0, the Auto setting defaults to 40 MHz channelization.	Set the channel bandwidth used during transmission: Auto, 20, 40, 80 and 160. **NOTE** By default, for the **Country Code** Indonesia, the **Channelization** width is set to 20 MHz only for outdoor APs.
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 5 AP Zone Details for SZ100 and vSZ-E platforms (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 maintaining mesh links and to discover AP neighbors.	Enter the duration in seconds. Range: 1 through 65535.
Auto Channel Selection	Automatically adjusts the channel for network self-healing and performance optimization. **ChannelFly** is set as the default option. For the **ChannelFly** option, you may also modify the default settings for the **Channel Change Frequency** and **Full Optimization Period**. The **Channel Change Frequency** slidebar allows you to specify the responsiveness of ChannelFly to interference (with consideration for the impact on associated clients), ranging from Minimal to Very Often. The **Full Optimization Period** timeslot bar allows you to specify one or more periods of time when ChannelFly is allowed to fully optimize the channel plan, ignoring the impact of channel changes on associated clients. Select time periods when the wireless network is servicing the fewest clients.	Select the required option. • **Background Scanning**: Changes the AP channel when there is interference. • **ChannelFly**: Monitors potential throughput and will change channels to learn each channel's capacity, optimize throughput, and to avoid interference.
Band/Spectrum Configuration > **6 GHz** **NOTE** This tab is available only if the Tri-band Dual-5G Mode option is not enabled.		

TABLE 5 AP Zone Details for SZ100 and vSZ-E platforms (continued)

Field	Description	Your Action
Channelization	Helps manage and allocate radio frequency resources. A lower channel width allows the zone to potentially serve more clients, whereas a higher channel width improves throughput, but potentially serves fewer clients and increases the possibility of interference. The Auto setting defaults to 160 MHz channelization.	Set the channel bandwidth used during transmission: **Auto**, **20**, **40**, **80**, **160** and **320**. **NOTE** The 320 MHz-radio frequency is available only for the R770 AP 6 GHz radio frequency.
Channel	Indicates the channel to use.	• In countries where only 6 GHz Indoor channels are permitted, the 6 GHz Outdoor channels are disabled. • If a country permits the use of 6GHz Indoor and Outdoor channels, the controller will provide the available channel ranges for both Indoor and Outdoor channels. For example, in the US, the available channel ranges are - – Indoor APs can operate in UNII-5,6,7,8 – Outdoor APs can operate in UNII-5,7 • You can choose channel options for Indoor and Outdoor channels. The default setting for both Indoor and Outdoor channels is **Auto**.
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.
Background Scan	Allows the AP radio to scan other channels in the band for accessing channel health and capacity, detecting rogue devices, optimizing and maintaining mesh links and to discover AP neighbors.	Enter the duration in seconds. Range: 1 through 65535.

TABLE 5 AP Zone Details for SZ100 and vSZ-E platforms (continued)

Field	Description	Your Action
Auto Channel Selection	Automatically adjusts the channel for network self-healing and performance optimization. **ChannelFly** is set as the default option. For the **ChannelFly** option, you may also modify the default settings for the **Channel Change Frequency** and **Full Optimization Period**. The **Channel Change Frequency** slidebar allows you to specify the responsiveness of ChannelFly to interference (with consideration for the impact on associated clients), ranging from Minimal to Very Often. The **Full Optimization Period** timeslot bar allows you to specify one or more periods of time when ChannelFly is allowed to fully optimize the channel plan, ignoring the impact of channel changes on associated clients. Select time periods when the wireless network is servicing the fewest clients.	Select the required option. • **Background Scanning**: Changes the AP channel when there is interference. • **ChannelFly**: Monitors potential throughput and will change channels to learn each channel's capacity, optimize throughput, and to avoid interference.
Band/Spectrum Configuration > **Lower 5 GHz**		
Channelization	Helps manage and allocate radio frequency resources. A lower channel width allows the zone to potentially serve more clients, whereas a higher channel width improves throughput, but potentially serves fewer clients and increases the possibility of interference. Prior to SmartZone release 7.0.0, the Auto setting defaulted to 80 MHz channelization. Beginning in SmartZone release 7.0.0, the Auto setting defaults to 40 MHz channelization.	Set the channel bandwidth used during transmission: Auto, 20, 40, 80 and 160. **NOTE** By default, for the **Country Code** Indonesia, the **Channelization** width is set to 20 MHz only for outdoor APs.
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.

TABLE 5 AP Zone Details for SZ100 and vSZ-E platforms (continued)

Field	Description	Your Action
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 maintaining mesh links and to discover AP neighbors.	Enter the duration in seconds. Range: 1 through 65535.
Auto Channel Selection	Automatically adjusts the channel for network self-healing and performance optimization. **ChannelFly** is set as the default option. For the **ChannelFly** option, you may also modify the default settings for the **Channel Change Frequency** and **Full Optimization Period**. The **Channel Change Frequency** slidebar allows you to specify the responsiveness of ChannelFly to interference (with consideration for the impact on associated clients), ranging from Minimal to Very Often. The **Full Optimization Period** timeslot bar allows you to specify one or more periods of time when ChannelFly is allowed to fully optimize the channel plan, ignoring the impact of channel changes on associated clients. Select time periods when the wireless network is servicing the fewest clients.	Select the required option. • **Background Scanning**: Changes the AP channel when there is interference. • **ChannelFly**: Monitors potential throughput and will change channels to learn each channel's capacity, optimize throughput, and to avoid interference.
Band/Spectrum Configuration > **Upper 5 GHz**		
Channelization	Helps manage and allocate radio frequency resources. A lower channel width allows the zone to potentially serve more clients, whereas a higher channel width improves throughput, but potentially serves fewer clients and increases the possibility of interference. Prior to SmartZone release 7.0.0, the Auto setting defaulted to 80 MHz channelization. Beginning in SmartZone release 7.0.0, the Auto setting defaults to 40 MHz channelization.	Set the channel bandwidth 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 5 AP Zone Details for SZ100 and vSZ-E platforms (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 maintaining mesh links and to discover AP neighbors.	Enter the duration in seconds. Range: 1 through 65535.

TABLE 5 AP Zone Details for SZ100 and vSZ-E platforms (continued)

Field	Description	Your Action
Auto Channel Selection	Automatically adjusts the channel for network self-healing and performance optimization. **ChannelFly** is set as the default option. For the **ChannelFly** option, you may also modify the default settings for the **Channel Change Frequency** and **Full Optimization Period**. The **Channel Change Frequency** slidebar allows you to specify the responsiveness of ChannelFly to interference (with consideration for the impact on associated clients), ranging from Minimal to Very Often. The **Full Optimization Period** timeslot bar allows you to specify one or more periods of time when ChannelFly is allowed to fully optimize the channel plan, ignoring the impact of channel changes on associated clients. Select time periods when the wireless network is servicing the fewest clients.	Select the required option. ● **Background Scanning**: Changes the AP channel when there is interference. ● **ChannelFly**: Monitors potential throughput and will change channels to learn each channel's capacity, optimize throughput, and to avoid interference.
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	Indicates 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 list.
Syslog Options		
Enable external syslog server for APs	Enables the AP to send syslog data to the syslog server on the network.	Select the option.

TABLE 5 AP Zone Details for SZ100 and vSZ-E platforms (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. › **Protocol**: 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. › **Protocol**: 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.
AP SNMP Options		
Enable AP SNMP	Indicates if the AP SNMP option is enabled.	Select the check box.
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**.

TABLE 5 AP Zone Details for SZ100 and vSZ-E platforms (continued)

Field	Description	Your Action
SNMPv3 Agent	Indicates 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**.
DHCP Service for Wi-Fi Clients		
Enable DHCP Service in this zone	Enables the DHCP service for this zone.	Select the check box.
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.
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.

TABLE 5 AP Zone Details for SZ100 and vSZ-E platforms (continued)

Field	Description	Your Action
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.

TABLE 5 AP Zone Details for SZ100 and vSZ-E platforms (continued)

Field	Description	Your Action
Load Balancing	Balances the number of clients or the available capacity across APs.	Select the required option: ● Based on Client Count: If this option is selected, **Steering Mode** and **Sticky Client** options are enabled. – **Steering Mode** - Controls the APs' steering behavior for load 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. – **Sticky Client Steering**: Some client devices connect to an AP and stay connected to the same servicing AP, and does not change its association to the closer APs. These clients are referred as sticky clients. These clients may experience degradation in service because of lower throughput resulting in poor user experience. The purpose of the sticky client steering functionality is to identify these clients and assist in transition to a better AP. Click on the toggle button to enable the options. › SNR Threshold - Signal-to-Noise (SNR) ratio value evalutes signal based on the noise. Enter the value between 5db to 30db. › NBRAP % Threshold - NBRAP (Neighbor AP) percentage is used to calculate a base SNR and compare it to the SNR received from a neighbor AP. Enter the percentage (%) range between 10-40.

TABLE 5 AP Zone Details for SZ100 and vSZ-E platforms (continued)

Field	Description	Your Action
		• **Based on Capacity**: This option performs the similar functionality as **Based on Client Count** the difference is Limit 2.4Ghz Client to is disabled. • **Disabled** - By default, **Disabled** option is selected. **NOTE** The band change is applicable only for those connected clients that support the 802.11v standard.
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.
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. • **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**

TABLE 5 AP Zone Details for SZ100 and vSZ-E platforms (continued)

Field	Description	Your Action
Recovery SSID	Allows you to enable or disable the Recovery (Island) SSID broadcast on the controller.	Enable **Recovery SSID Broadcast**. **NOTE** The Recovery SSID is available when an AP does not get a reply back for unicast ARP to its configured gateway.
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.

NOTE
Starting with 7.0 release, the support for **Cellular Options** while configuring or creating a zone is removed from the controller web interface.

Automated Frequency Coordination System

The Automated Frequency Coordination (AFC) system is a spectrum sharing mechanism developed for license-exempt (LE) devices to securely share spectrum with licensed operators. It is a regulatory requirement aimed at maximizing spectrum access and minimizing interference in the 6 GHz band between unlicensed Wi-Fi 6e/7 devices and licensed devices in various services such as fixed services, satellite services, television/broadcast services, and ultra-wide band services.

To prevent interference with licensed devices, unlicensed Standard Power devices that operate in 6 GHz spectrum must consult an AFC system before operation. In the United States, the AFC system uses data from the Federal Communications Commission (FCC) agency's Universal Licensing System (ULS) and Equipment Authorization System (EAS), which includes all licensed users currently operating in the 6 GHz band, to coordinate the shared use of the spectrum between these incumbents and the unlicensed operators. The interaction with these databases is read-only, where the AFC can retrieve data but cannot modify it.

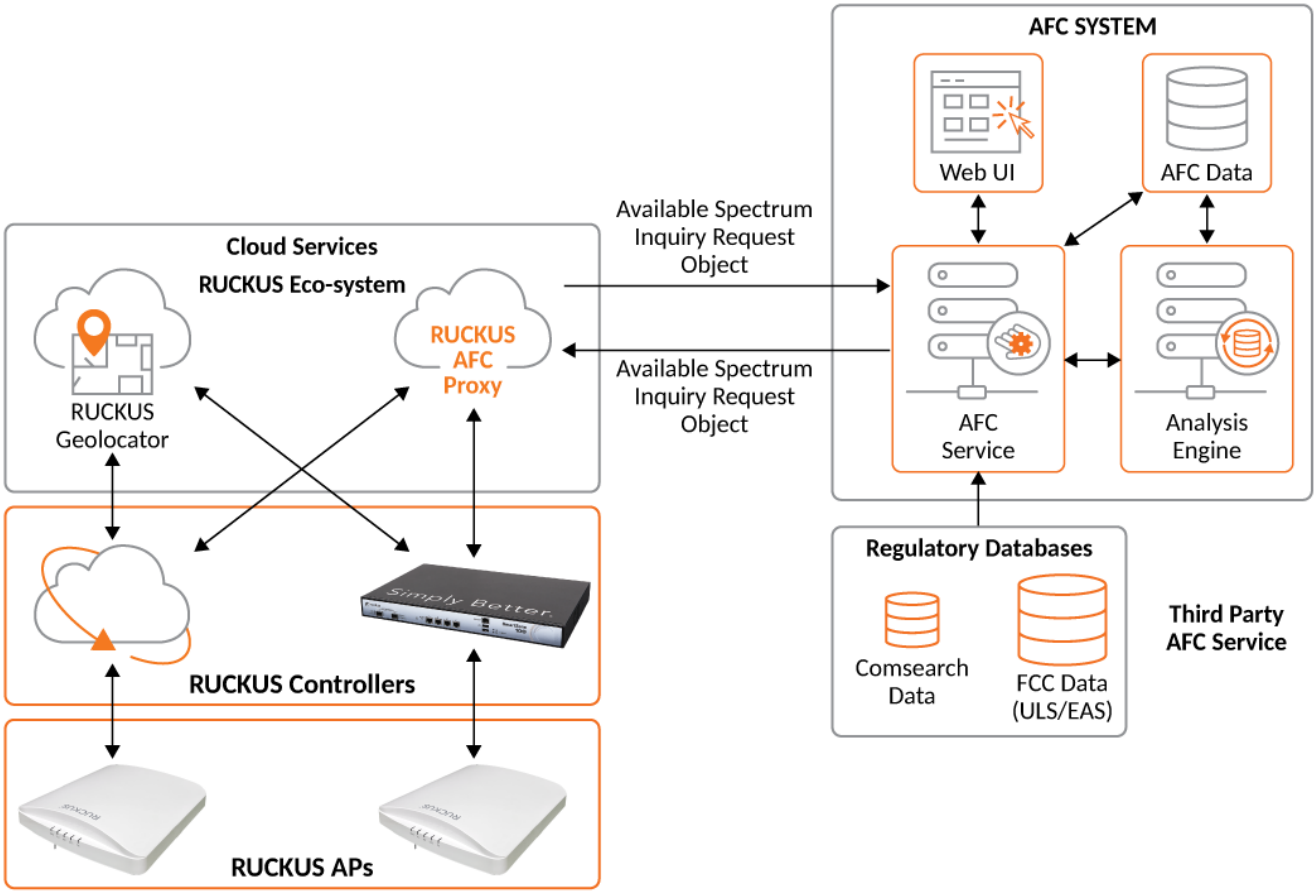
APs are required to register with the AFC system, and thereafter must check in with the system every 24 hours to obtain a current list of available channels. If an AP fails to connect with the AFC, it is allowed to continue operating until 11:59 p.m. on the following day. However, if the AP still fails to connect after this period, it must cease Standard Power operation: Indoor APs revert to Low Power Indoor (LPI) limits, while outdoor APs cease operating in the 6 GHz band.

The AFC system authenticates each AP using its serial number and regulatory ID, which are unique identifiers for the AP. This ensures that only authorized APs are allowed to operate within the specified frequency bands. The AFC system is required to store the registered information of each AP for a period of three months. This includes the registration details and connection history for each AP. This data can be used for troubleshooting, auditing, and ensuring compliance with regulations.

APs must automatically self-geolocate their own geographical position in terms of latitude, longitude, and height above ground level. The geographical position is used to derive a Location Uncertainty Volume within which the AP has a 95% probability of being located.

The following image illustrates services offered by RUCKUS in the AFC System.

FIGURE 16 RUCKUS AFC Architecture



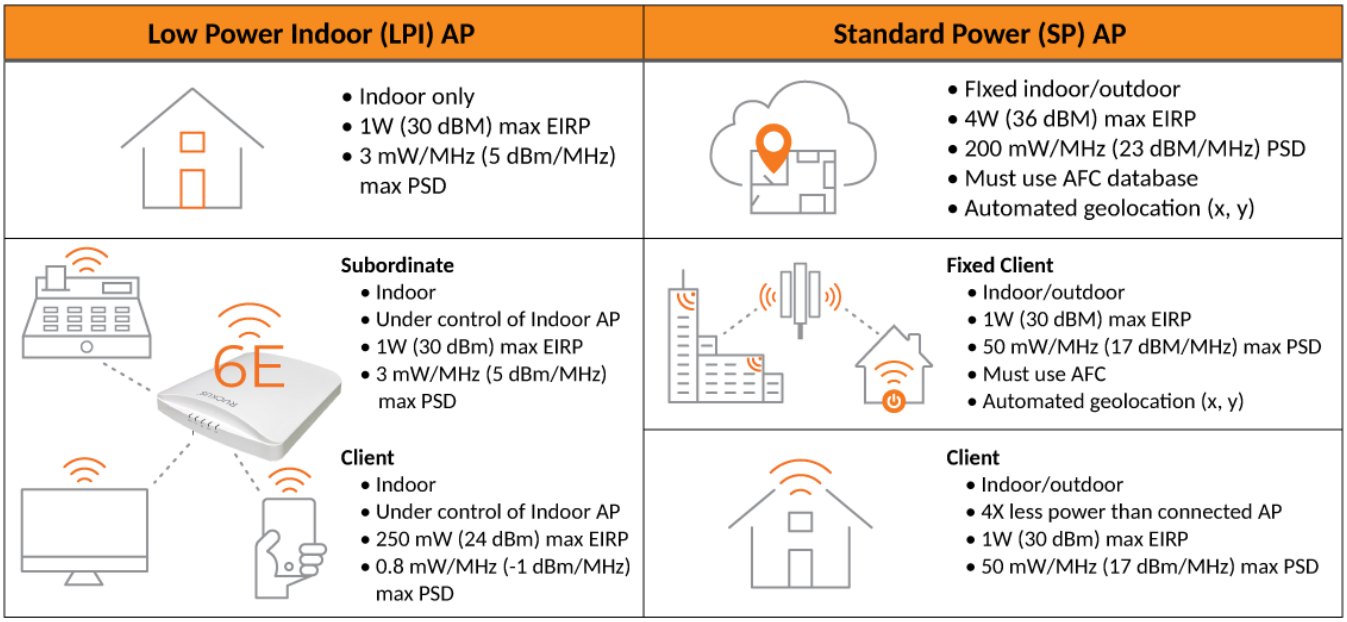
AFC Power Modes

Outdoor APs supporting the 6 GHz spectrum operate in Standard Power mode only.

Indoor APs supporting the 6 GHz spectrum can operate in one of two different power modes:

- Low power indoor (LPI) operation
- Standard power (SP) operation

FIGURE 17 Types of 6 GHz Devices



Low Power Indoor

Low Power Indoor (LPI) operation is specific to indoor access points operating in the 6 GHz spectrum. LPI mode limits these indoor APs to a maximum equivalent isotropic radiated power (EIRP) of 30 dBm and a maximum power spectral density (PSD) of 5 dBm/MHz. These APs can operate on all four 6 GHz frequency bands (U-NII-5 through U-NII-8) without the use of AFC.

FIGURE 18 Low Power Indoor Devices

Device Type	Max EIRP	Max PSD	Geolocation Required?	AFC Required?	Limitations	Bands
Indoor AP (Low Power Indoor) 	1W (30 dBm)	3 mW/MHz (5 dBm/MHz)	No	No	• Indoor only • Integrated antenna (not external) • No weatherized enclosure • Wired power (no battery) • Must be labeled: **"FCC regulations restrict operation of this device to indoor use only"**	U-NII-5 to U-NII-8 5925-7125 MHz
Subordinate (Mesh extender) 	1W (30 dBm)	3 mW/MHz (5 dBm/MHz)	No	No	• Indoor only • Under control of Indoor AP • Integrated antenna (not external) • No weatherized enclosure • Wired power (no battery) • Can't be used to connect devices between separate building or structures • Must be labeled: **"FCC regulations restrict operation of this device to indoor use only"** • Must be certified separately	U-NII-5 to U-NII-8 5925-7125 MHz
Client 	250 mW (24 dBm)	0.8 mW/MHz (-1 dBm/MHz)	No	No	• Indoor only • Under control of Indoor AP • Integrated antenna (not external) • No weatherized enclosure • Wired power (no battery) • Operating power must be 6 dB below associated SP AP transmit power	U-NII-5 to U-NII-8 5925-7125 MHz

Standard Power

Standard power (SP) operation is applicable to both indoor and outdoor APs in the 6 GHz spectrum, specifically within the U-NII-5 and U-NII-7 sub-bands. When AFC is enabled, these APs are allowed to operate at a higher power, with a maximum EIRP of 36 dBm and a maximum PSD of 23 dBm/MHz. Outdoor APs may only operate in Standard Power mode.

FIGURE 19 Standard Power Devices

Device Type	Max EIRP	Max PSD	Geolocation Required?	AFC Required?	Limitations	Bands
Standard Power AP 	4W (36 dBm)	200 mW/MHz (23 dBm/MHz)	Yes	Yes	• Antenna elevation angle requirements	U-NII-5 & U-NII-7 5925-6425 MHz & 6525-6875 MHz
Fixed Client 	4W (36 dBm)	200 mW/MHz (23 dBm/MHz)	Yes	Yes	• Can only connect to a SP AP • Client device intended as CPE • Permanently attached to a structure • Antenna elevation angle requirements	U-NII-5 & U-NII-7 5925-6425 MHz & 6525-6875 MHz
Client 	1W (30 dBm)	50 mW/MHz (17 dBm/MHz)	No	No	• Operating power must be 6 dB below associated SP AP transmit power	U-NII-5 & U-NII-7 5925-6425 MHz & 6525-6875 MHz

Effective Isotropic Radiated Power

Effective Isotropic Radiated Power (EIRP) is a measure of the output power radiated from an ideal isotropic antenna in a single direction. It is used to quantify the maximum amount of power that could be radiated from an antenna, considering its antenna gain and the transmitter power of the RF system. EIRP is commonly measured in decibel-milliwatts (dBm).

TABLE 6 Low Power Indoor vs Standard Power Modes for APs

Power Modes	Max EIRP	Max PSD	Does it require AFC	Indoor or Outdoor	Note
Low Power Indoor (LPI)	30 dBm	5 dBm/MHz	No	Only indoor	Maximum EIRP increases with Bandwidth
Standard Power (SP)	36 dBm	23 dBm/MHz	Yes	Both indoor and outdoor	Maximum EIRP stays constant with Bandwidth

TABLE 7 Maximum EIRP for Various Bandwidths

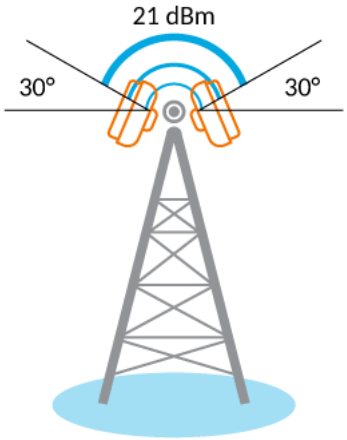
	Power Mode	EIRP	20 MHz	40 MHz	80 MHz	160 MHz	320 MHz
Access Point	Standard Power	Max EIRP	36 dBm				
		SNR Penalty due to increase in noise floor compared to 20 MHz	-	3 dB	6 dB	9 dB	12 dB
	Low Power	Max EIRP	18 dBm	21 dBm	24 dBm	27 dBm	30 dBm
		SNR Penalty due to increase in noise floor compared to 20 MHz	0 dB				
Client	Standard Power	Max EIRP	30dBm				
		SNR Penalty due to increase in noise floor compared to 20 MHz	-	3 dB	6 dB	9 dB	12 dB
	Low Power	Max EIRP	12 dBm	15 dBm	18 dBm	21 dBm	24 dBm
		SNR Penalty due to increase in noise floor compared to 20 MHz	0 dB				

Limitations

Limitations in Standard Power Usage:

- Client devices operating in the 160 MHz bandwidths are limited to an EIRP of 21 dBm (125 mW).
- Client devices operating in the 320 MHz bandwidths are limited to an EIRP of 24 dBm (251 mW).
- Fixed client devices may not emit more than 21 dBm at an angle greater than 30° relative to the horizon. Refer to Figure 20 for a visual representation.

FIGURE 20 Limitations in Standard Power Usage



Usage Prohibition of 6 GHz band

The use of the 6 GHz band is prohibited in certain areas, such as oil platforms, automobiles, trains, and aircraft. However, large aircrafts flying above 10,000 feet can utilize APs operating in the 5925-6425 MHz band (for example: U-NII-5 radio band).

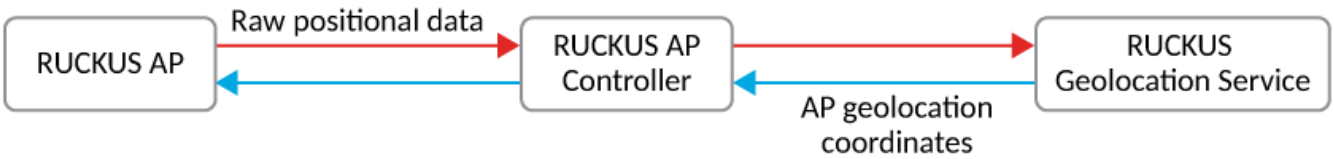
FIGURE 21 Usage Prohibition

RUCKUS AFC System Architecture

RUCKUS employs a cloud-based architecture to deliver Automated Frequency Coordination (AFC) support across its product lines of enterprise Wi-Fi Access Points (APs). Within the RUCKUS cloud, an AFC Proxy Server and a Geolocation Service Server are hosted, both of which are exclusively accessible to registered RUCKUS client devices.

The Geolocation Service Server acts as a centralized hub for processing location data from APs at a venue. APs, through their respective AP Controllers, supply the Geolocation Service Server with raw positional data, which consists of RF-based observations about their neighboring APs. From its overarching view of the entire Wi-Fi network, the Geolocation Service Server collectively analyzes the raw positional data from all APs to infer the geolocation coordinates of each AP, formatted appropriately for AFC inquiries.

FIGURE 22 Geolocation Flow

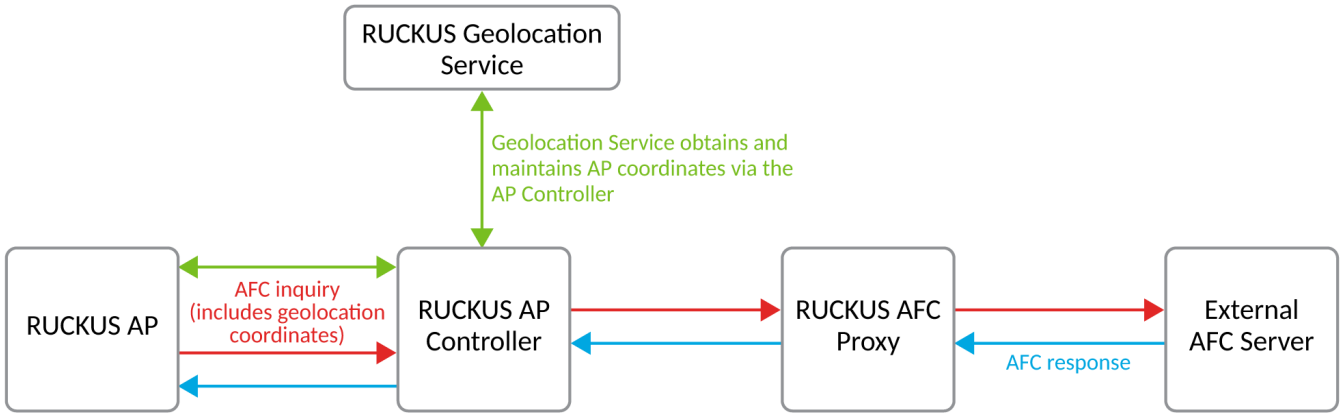


To conduct an AFC available spectrum inquiry, a RUCKUS AP first determines its geolocation coordinates (latitude, longitude, height above ground level, lateral and vertical uncertainty) with the aid of the RUCKUS Geolocation Service Server. It then formulates the AFC inquiry, incorporating its geolocation coordinates, and forwards this inquiry to the RUCKUS AFC Proxy Server via its Controller. The AFC Proxy Server subsequently relays the AP AFC inquiry to an external AFC service provider's server for processing and waits for the response, which is then sent back to the AP. Refer to Figure 23 for a visual representation of these messaging paths.

The APs communicate with the AFC Proxy Server and Geolocation Service Server through their respective AP controllers, not directly. RUCKUS has the following types of AP controllers:

- SmartZone 144 and SmartZone 300 are hardware-based AP controllers.
- Virtual SmartZone is a virtualized AP controller (distributed as a virtual machine).

FIGURE 23 AFC Inquiry Flow



How RUCKUS AP Geolocation Works

The Geolocation Service Server aids APs in pinpointing their geolocation coordinates. In any given venue, APs are categorized into two distinct groups. The first is a small group of Reference APs, for which geolocation coordinates are initially established. The second is a larger group of Non-Reference APs, for which geolocation coordinates are inferred based on their relative distance to each other and to the Reference APs. Geolocation coordinates of any Non-Reference AP can be determined only when there is a distance connection to a Reference AP, either directly or indirectly.

Initiating the geolocation process, the network administrator selectively designates strategically located APs at a specific venue as Reference APs. These APs could be positioned near a window or at opposite ends of the building, for instance. Interaction with the geolocation process is facilitated through a companion RUCKUS app on a mobile device, used by the network administrator. This app displays a list of all APs at the venue, enabling the network administrator to select the APs that will serve as Reference APs.

The geolocation coordinates of the selected Reference APs can be ascertained using one of three methods:

- Using the built-in AP GPS receiver (if available and able to receive the appropriate GPS signals).

  NOTE
  All outdoor APs would be equipped with built-in GPS and thus, will be using this method for geolocation directly.

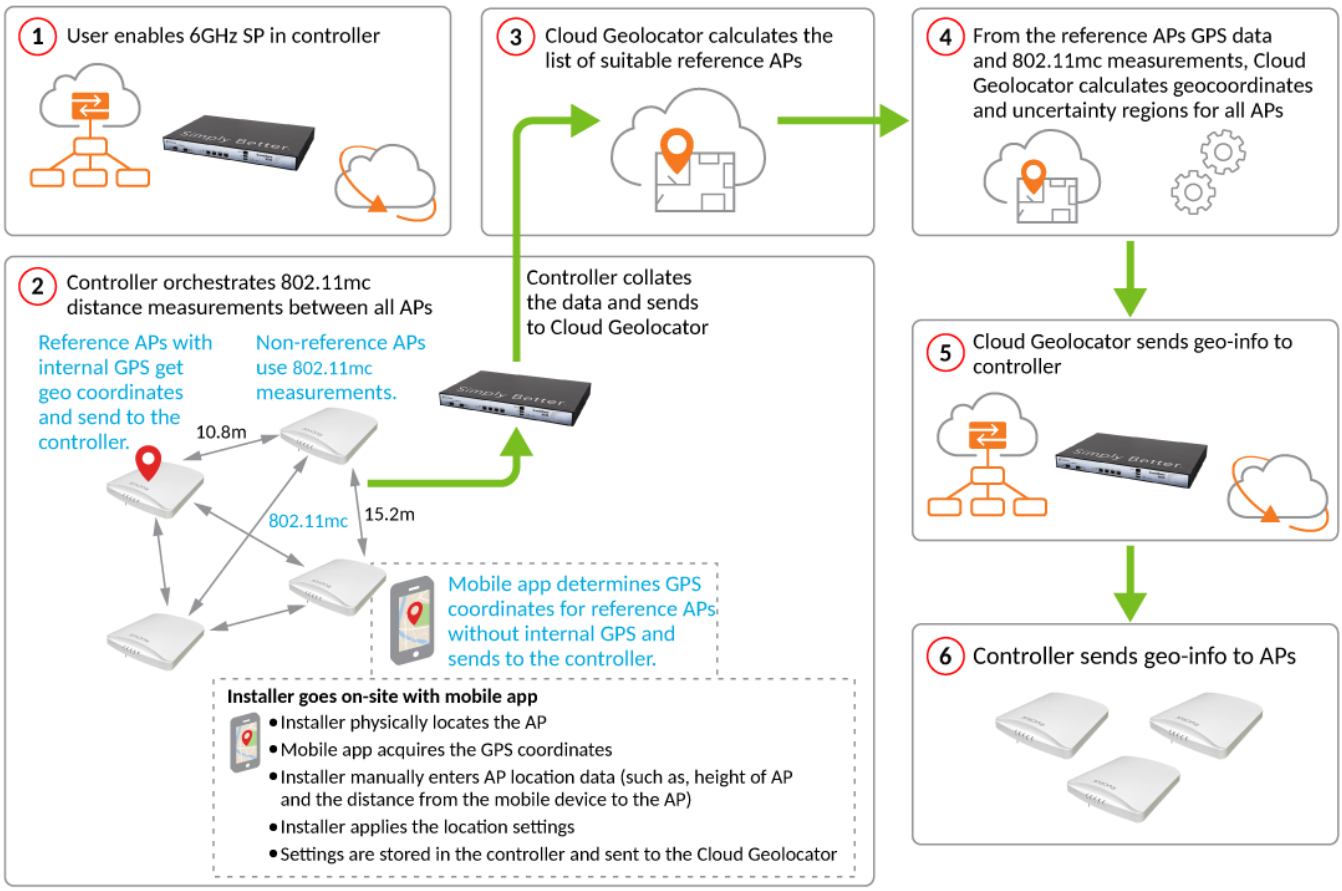
- Accessing a cloud-based geolocation database, such as the Google Geolocation API, which can identify an AP location based on the MAC addresses of other Wi-Fi devices within its observable range. For more information, you can refer to the official documentation of the Google Geolocation API.
- A network administrator, equipped with a mobile device that has the RUCKUS mobile app installed, stands directly beneath the AP. The network administrator prompts the mobile app, which then automatically collects the geolocation coordinates of the mobile device using its built-in location service. This information is used to estimate the AP geolocation coordinates.

The optimal method is selected based on the specific deployment scenario. The resulting geolocation coordinates are transmitted to the Geolocation Service Server. Any systematic inaccuracies inherent in the selected method are factored into the calculation of the accompanying lateral uncertainty. A less accurate source would necessitate a larger value for lateral uncertainty.

Subsequently, all APs, both Reference and Non-Reference, relay information about the neighboring APs they can observe to their respective AP Controllers. These controllers then forward this information to the Geolocation Service Server. This information primarily consists of standard-based 802.11mc Round Trip Time (RTT) distance values, which may be supplemented by Received Signal Strength (RSS) measurements, if necessary. These values can be used to estimate the pairwise distances between APs. The Geolocation Service Server utilizes this information to construct an AP Graph of the venue, where the edges of the graph represent the estimated distances between APs.

With the geolocation coordinates of the Reference APs and the spatial relationships among APs as depicted by the AP Graph, the Geolocation Service Server is equipped to geometrically infer the geolocation coordinates of the Non-Reference APs.

FIGURE 24 RUCKUS Geolocation Workflow



Mobile Applications

Using a mobile application at the installation site, the user is provided a list of Access Points (APs) for which no geolocation coordinates are available. This list is sourced from the cloud-based Geolocator. For each AP without geolocation data, the user manually inputs the AP location data as prompted by the mobile application. The mobile application then retrieves the GPS coordinates based upon the location of the mobile device. The GPS coordinates and other location-related data are transmitted to the controller, which in turn forwards it to the Cloud Geolocator for further processing.

Enabling Automated Frequency Coordination from SmartZone

To set the geolocation of the APs and to verify their status, it is essential to enable the AFC feature in the controller.

Download and install the RUCKUS SWIPE app on your mobile phone. iOS users can download the app from the Apple App Store, and Android users can download the app from the Google Play Store.

> **NOTE**
> Ensure you have a valid RUCKUS Cloud account and log in to access your account.

The AFC feature is disabled by default. The AFC feature is available only if the country of the selected zone allows AFC and RUCKUS obtains the AFC certificate from the prevailing government authority, such as the US Federal Communications Commission (FCC). Otherwise, the **Enable AFC** option is grayed out.

To enable the AFC feature, perform the following:

1. Ensure that RUCKUS Cloud Authentication is enabled for your account. To enable the RUCKUS **Cloud Authentication**, click **Administration** > **External Services** > **Ruckus Services** > **Ruckus Cloud Services** and toggle the **Cloud Authentication** button.

   This displays the login screen.
2. Enter the login credentials and click **Sign In**.

   You can now configure AFC at the Zone, AP Group, or AP level.
3. From the system-tree hierarchy, select the required Zone, AP group, or AP for which you want to enable AFC and click **Configure**.
4. In the **Band/Spectrum Configuration** section, select the **6 GHz** tab.

   If the selected country or the zone allows AFC and if RUCKUS has obtained the AFC certificate from the Federal Communications Commission (FCC) or government authority, the **Enable AFC** toggle button is available for selection.

   If the above condition is not met, then the **Enable AFC** is grayed out.
5. Toggle the **Enable AFC** button to **ON**.

6. If the zone of the country allows AFC, but the **Enable AFC** button is still grayed out, upload the required AP patch file (*.patch).

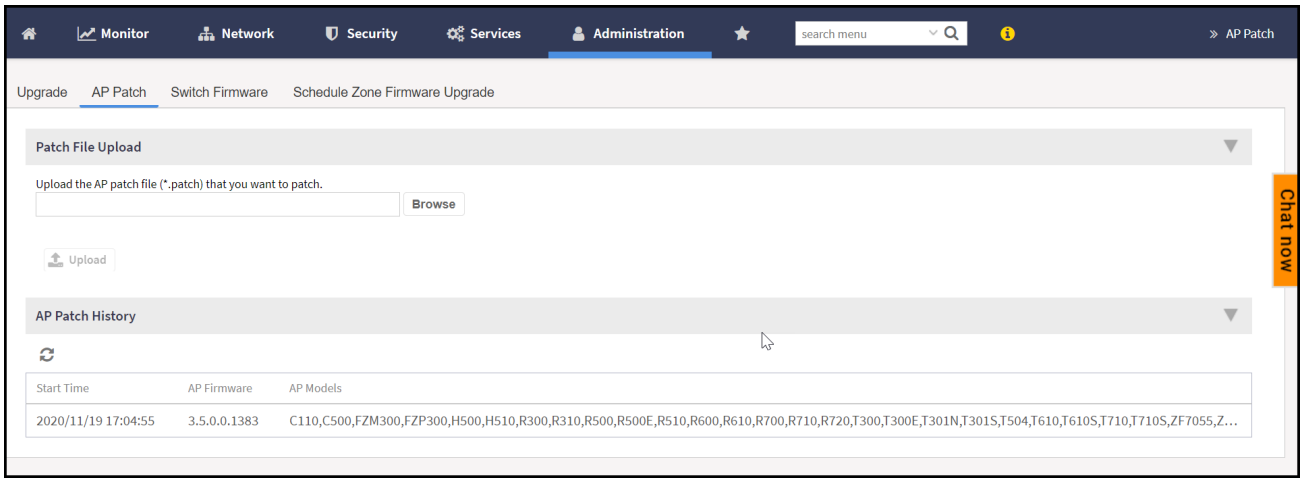
   Prerequisites:

   - The necessary AP patch is available only if the country's regulatory body has issued the AFC certificate to RUCKUS AP models.
   - Download the necessary AP patch file from the RUCKUS Support website to your local computer.

   To upload the patch file, perform the following:

   a) In the main menu, click **Administration** > **Administration** > **Upgrade** > **AP Patch**. This displays **Patch File Upload** screen.

   FIGURE 25 AP Patch File Upload



   b) Click on the **Browse** button. Select the **.patch** file from your local computer and click **Upload**. Now the **AFC Enable** toggle button is active and ready to enable the AFC functionality (perform Steps 3-5 in this procedure).

Checking Automated Frequency Coordination Status

The AFC Status and additional AFC-related information for a specific AP can be viewed on the Access Points page. Logged in to your SmartZone controller, perform the following steps:

1. Navigate the main menu, clicking **Network** > **Wireless** > **Access Points**.
2. Click the Table Settings icon and ensure that the **AFC Status** and **Power Mode (6G)** table columns are checked for inclusion on the **Access Points** screen.
3. Use the **Access Points** screen search function, or navigate through the network hierarchy, such that the desired AP appears in the table. The **AFC Status** column reflects the current status for the AP.
4. View additional AFC-related information by selecting a specific AP, scrolling to the **DETAILS** portion of the page, and clicking the **General** tab. The **AFC Info** section reflects **AFC Status**, as well as additional AFC-related information.

AFC statuses and their meanings are as follows:

- **AFC NOT REQUIRED**: At least one of the following conditions occurred:
  - **Enable AFC** is not enabled.
  - The selected country in the zone config is not in the allowed AFC country list.
  - The AP does not support the 6 GHz band.
  - The AP model has not obtained the certificate, or the AP firmware version is not updated to the latest version.

- **WAIT FOR LOCATION**: At least one of the following conditions occurred:
  - The AFC Geolocation for the AP has not been set using the RUCKUS SWIPE mobile app (applies to RUCKUS Wi-Fi 6E APs only).
  - The RUCKUS Wi-Fi 7 AP GPS module cannot detect its geolocation.
  - The AP location has not been calculated by the RUCKUS GeoLocator cloud service.
- **WAIT FOR RESPONSE**: The AFC request has been sent to the AFC Proxy; the AP is waiting for the AFC Proxy server to respond.
- **AFC SERVER FAILURE**: An error occurred in the AFC Proxy server.
- **REJECTED**: The AFC Proxy server determined that there are no available channels for this location and returned an AFC Reject response. If this is an indoor AP, it automatically switches to low power mode. If this is an outdoor AP, it automatically turns off the 6 GHz radio.
- **PASSED**: The AFC Proxy server determined that there are available channels for this location. The AP is allowed to operate in Standard Power mode within the expiration time of 1 day.
- **N/A**: The AP is Offline.

Radio Band Features

Band or Spectrum Configuration

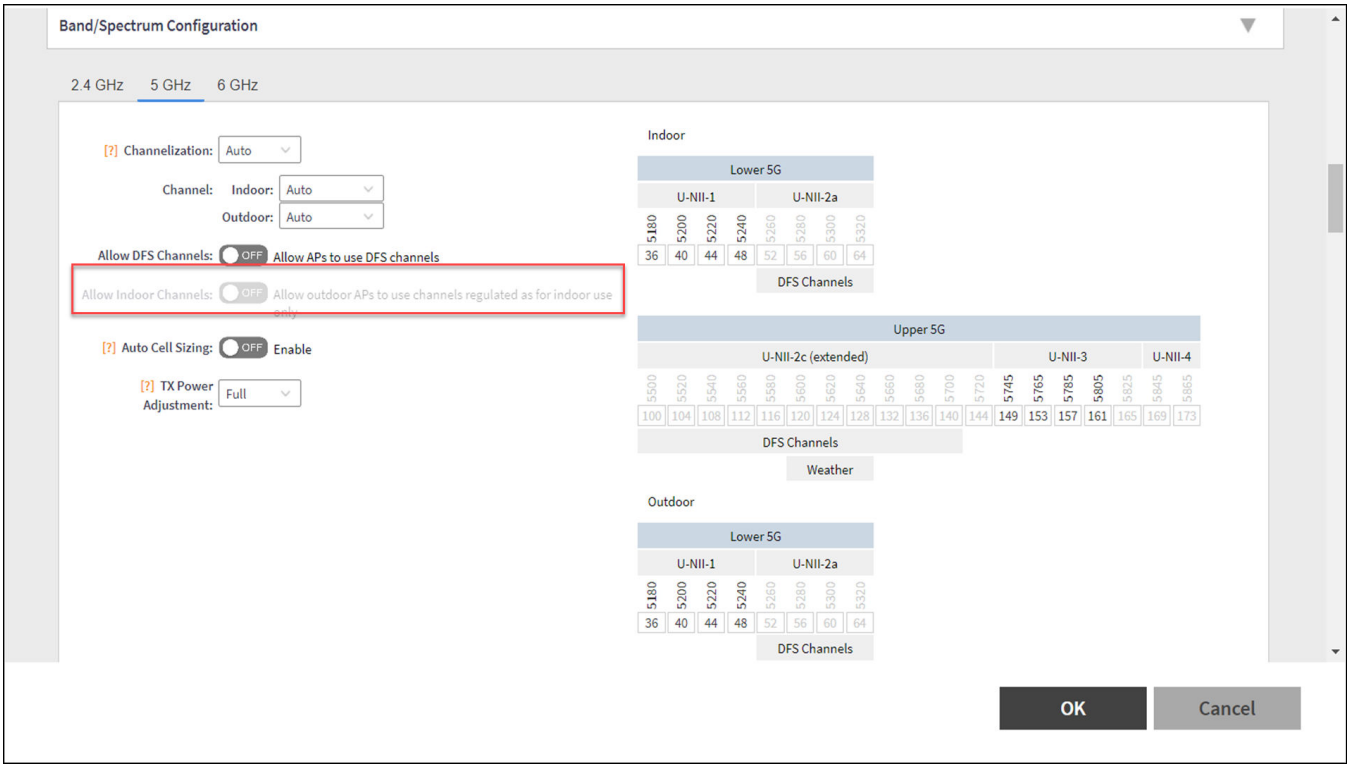
Band or spectrum configuration is a method of statistically picking the most potent channel for an AP.

> **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 26 Band or Spectrum Configuration



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.

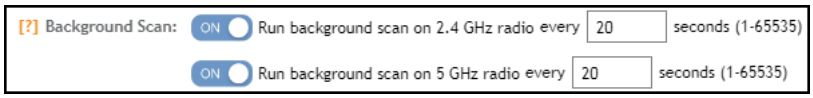
TABLE 8

Channel Selection Method	When to Use
ChannelFly	Recommended method for most deployments.

TABLE 8 (continued)

Channel Selection Method	When to Use
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.

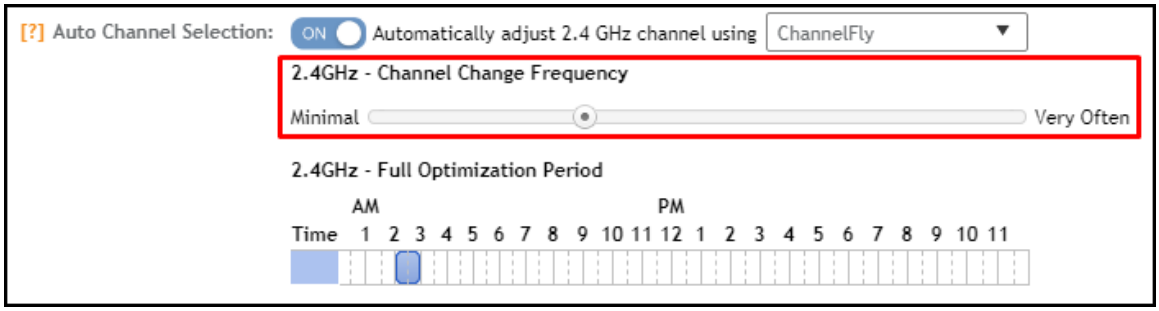


ChannelFly

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 9.



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 9 Client Threshold Table

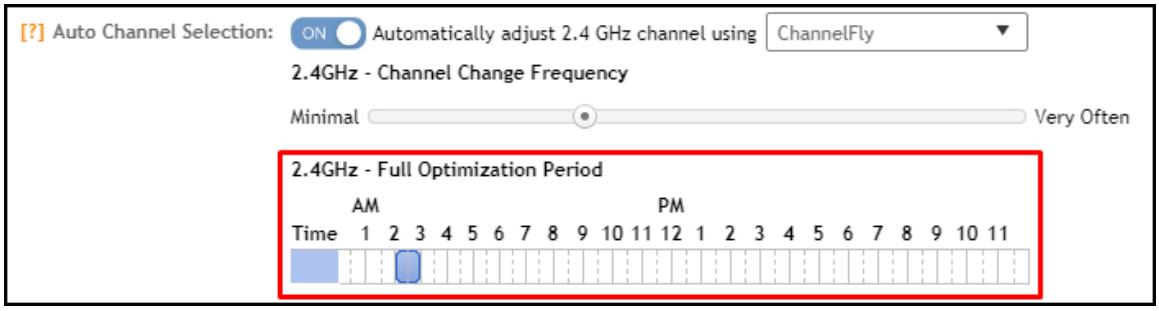
CCF	100	90	80	70	60	50	40	30	20	10	1
Client Threshold	10	9	8	7	6	5	4	3	2	1	0

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 10 ChannelFly State and its Behavior

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

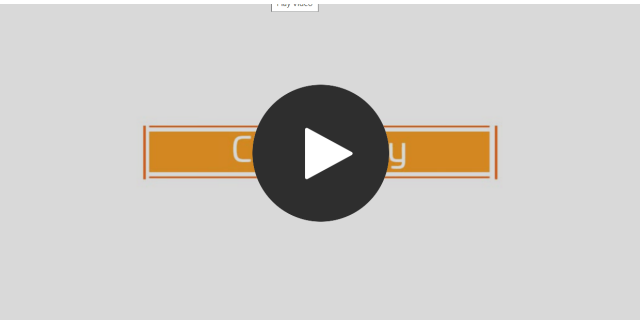
Background Scanning uses Background Scan to collect information on the presence of neighboring APs. Background Scanning focuses on finding a channel with the fewest number of neighbors.

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.

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.

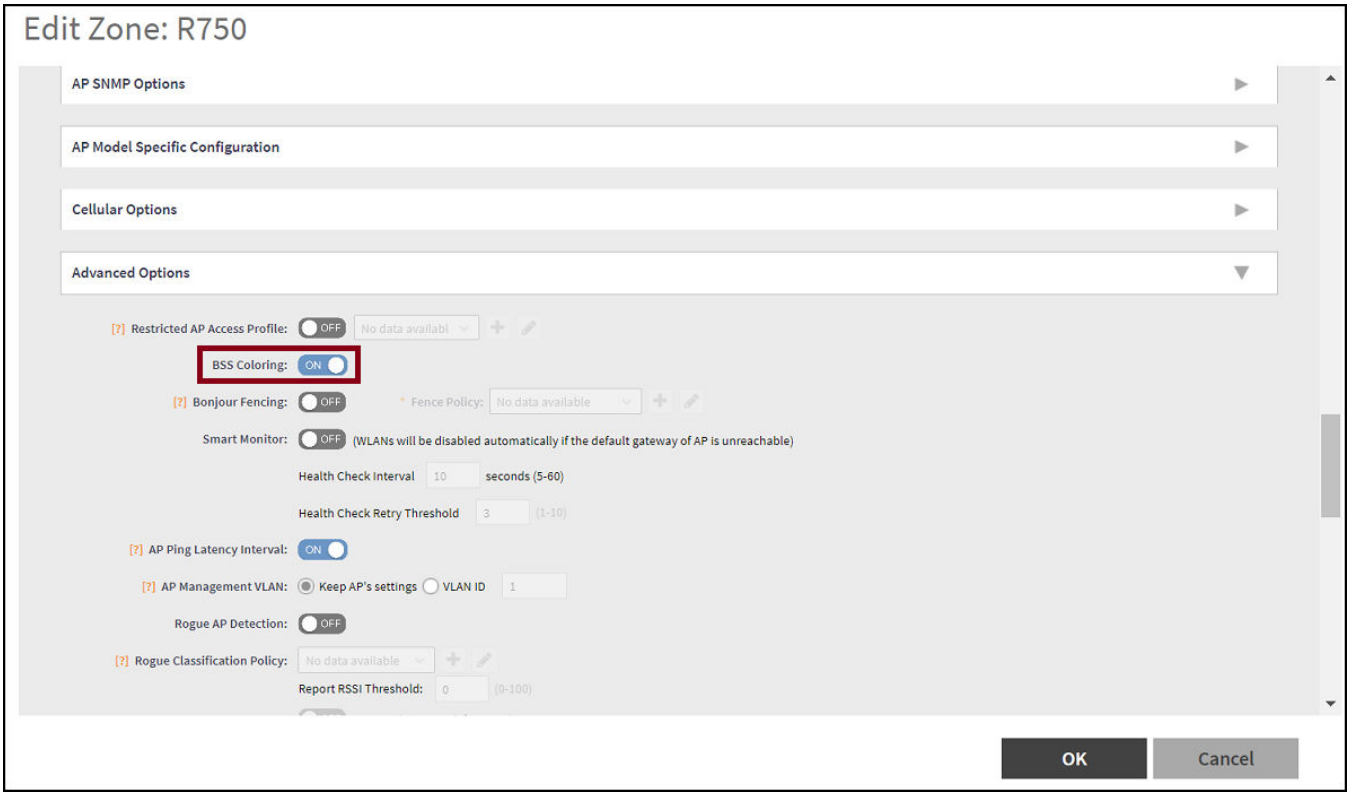
Complete the following steps to configure BSS Coloring for a zone.

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

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

   The **Configure Zone** page is displayed.

   FIGURE 27 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.

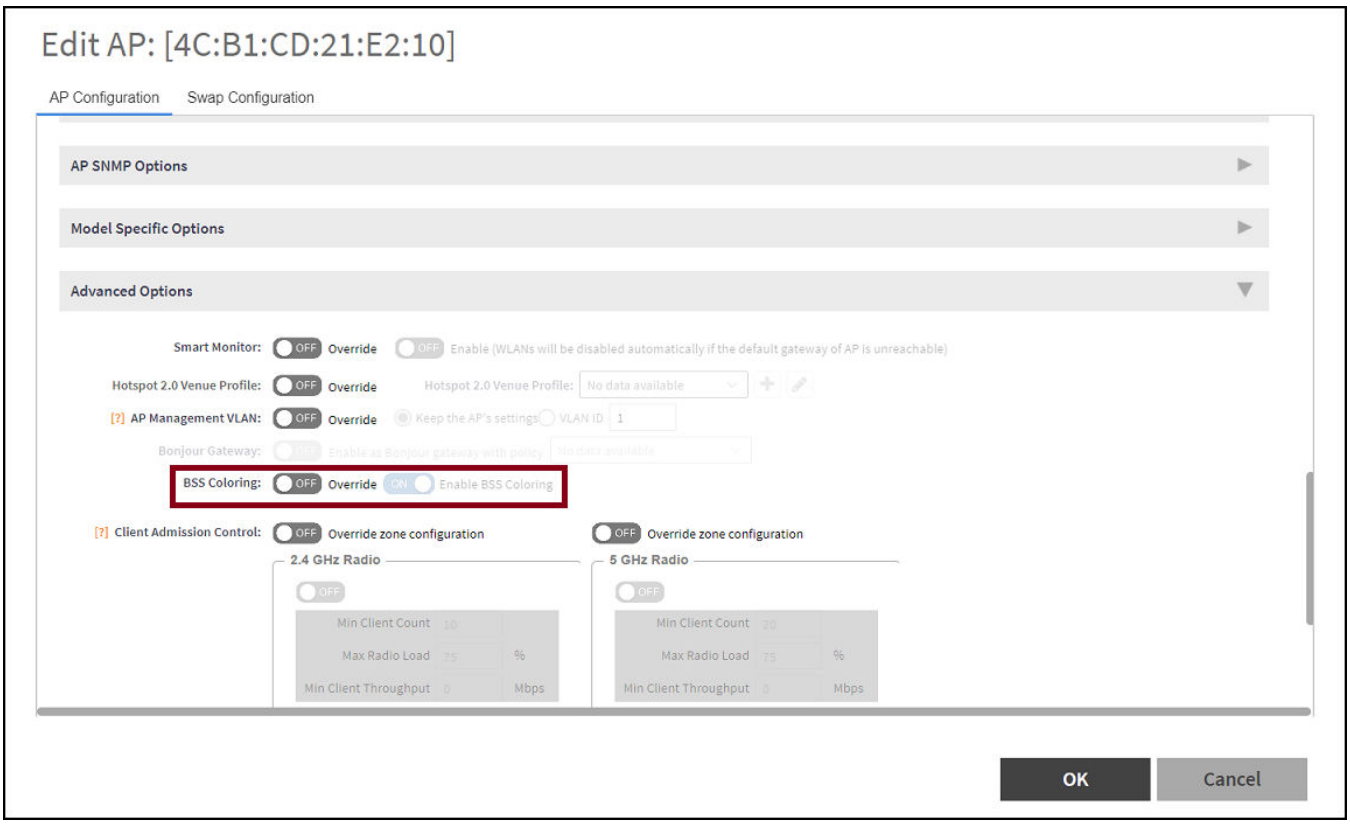
NOTE
BSS Coloring for individual access points is available for 802.11ax APs only.

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 28 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

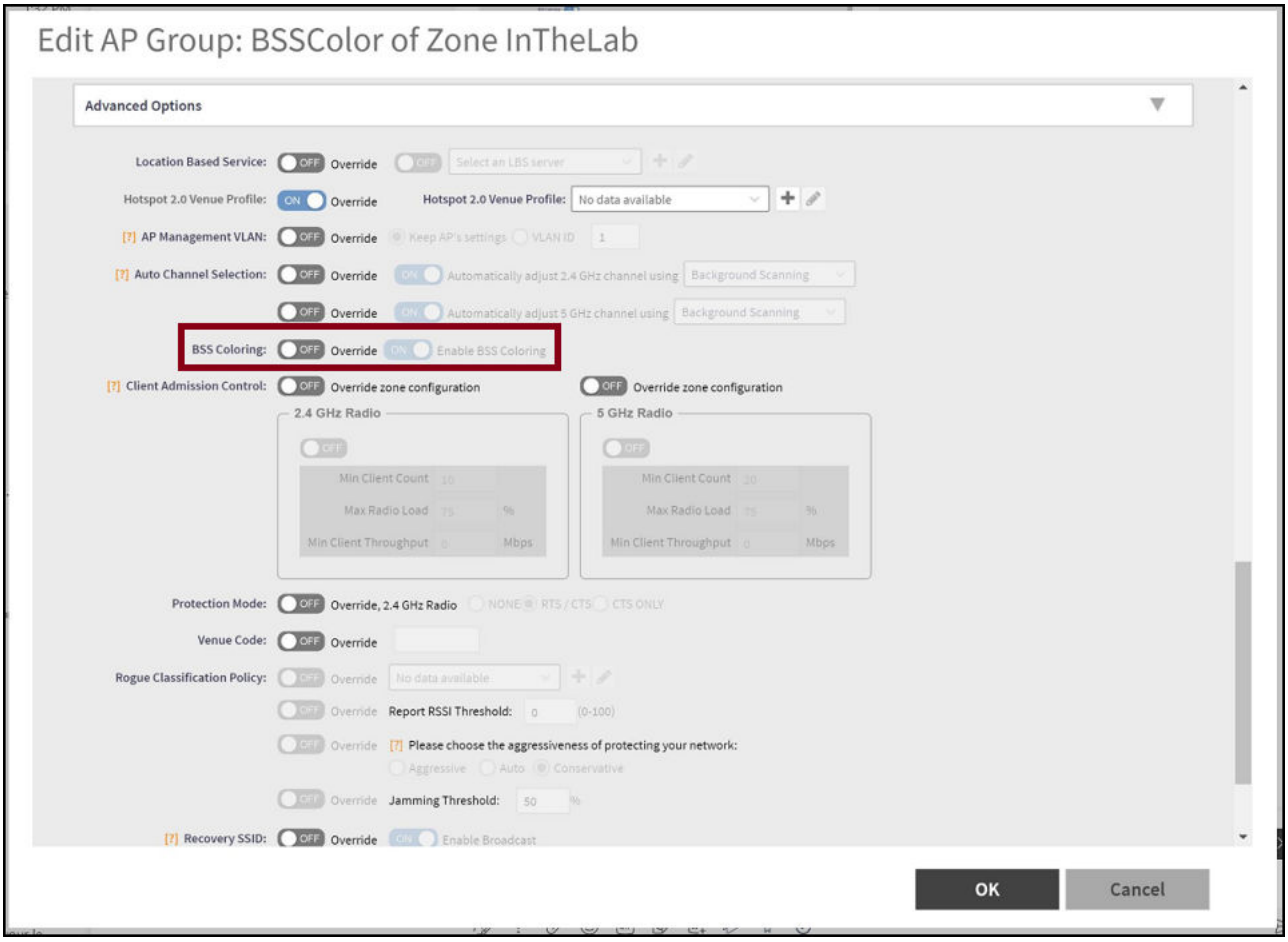
Complete the followings steps to configure the BSS Coloring within an AP group.

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 29 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.

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.

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 11 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.
WLAN	Displays details of the respective WLAN and WLAN group. You can create or configure a WLAN and a WLAN group. Refer to *RUCKUS SmartZone Controller Administration Guide*.
Hotspots and Portals	Displays details of the respective hotspots and portals. Refer to *RUCKUS SmartZone Access and Security Services Guide*.
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 *RUCKUS SmartZone Access and Security Services Guide*
Bonjour	Displays details of the respective Bonjour services. Refer to Bonjour on page 257.
Tunnels & Ports	Displays details of the respective tunnels and ports. Refer to *RUCKUS SmartZone Tunnel and Data Plane Guide*.
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 *RUCKUS SmartZone Access and Security Services Guide*.

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.

Configuring Templates

Creating Zone Templates

A zone template contains configuration settings (radio, AP GRE tunnel, channel mode, and background scanning) that you can apply to all access points that belong to a particular AP zone. Applying a zone template to an AP zone will overwrite all settings on all access points that belong to the AP zone.

To create a zone template:

1. Go to **Administration** > **System** > **Templates** > **Zone Templates**.
2. Click **Create**, the Create Zone Template form is displayed.
3. Enter the template details as explained in the following table.

TABLE 12 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**

TABLE 12 Zone Template Details (continued)

Field	Description	Your Action
AP Admin Logon	Indicates the admin logon credentials. For the Default Zone, the controller's cluster name is used as the default login ID and password.	Enter the **Logon ID** and **Password**.
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.

TABLE 12 Zone Template Details (continued)

Field	Description	Your Action
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.
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.

TABLE 12 Zone Template Details (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 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**.
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		

TABLE 12 Zone Template Details (continued)

Field	Description	Your Action
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.
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.

TABLE 12 Zone Template Details (continued)

Field	Description	Your Action
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 rougues 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.
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**

TABLE 12 Zone Template Details (continued)

Field	Description	Your Action
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.

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**.

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.

Moving a Single Access Point to a Different AP Zone

Follow these steps to move a single access point from its current AP zone to a different one.

> **NOTE**
> This feature is applicable only for SZ100 and vSZ-E platforms.

> **NOTE**
> The AP that you move will inherit the configuration of the new AP zone.

1. From the Access Points page, locate the access point that you want to move to a different AP zone.
2. Click **Move**, the Select Destination AP Zone form appears.
3. Select the AP zone to which you want to move the access point.
4. Click **OK**.

You have completed moving an access point to a new AP zone.

Working with Maps

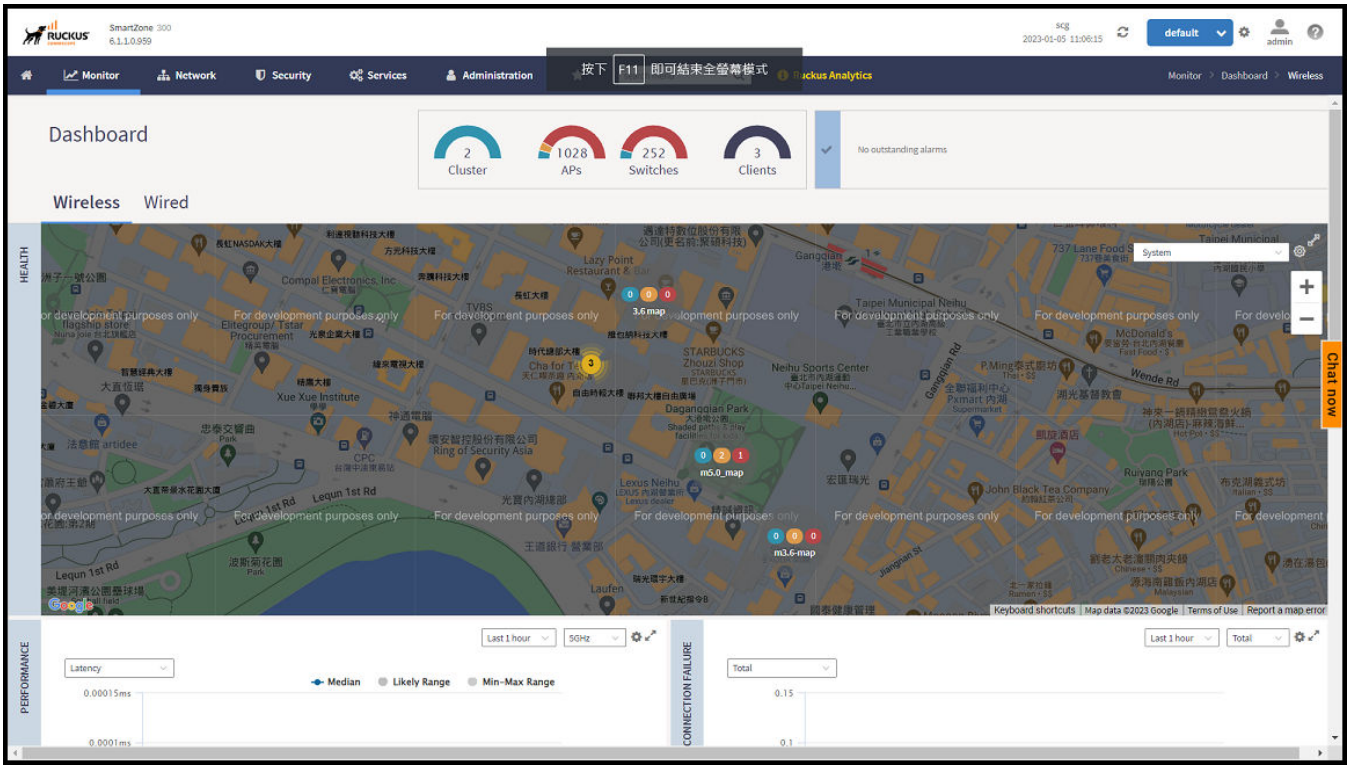
Importing floorplan maps into SmartZone allows you to further customize the information displayed on the Dashboard and Access Points pages, and monitor your APs, zones, groups, clients and traffic statistics all within the world map view on the Dashboard.

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 30 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:

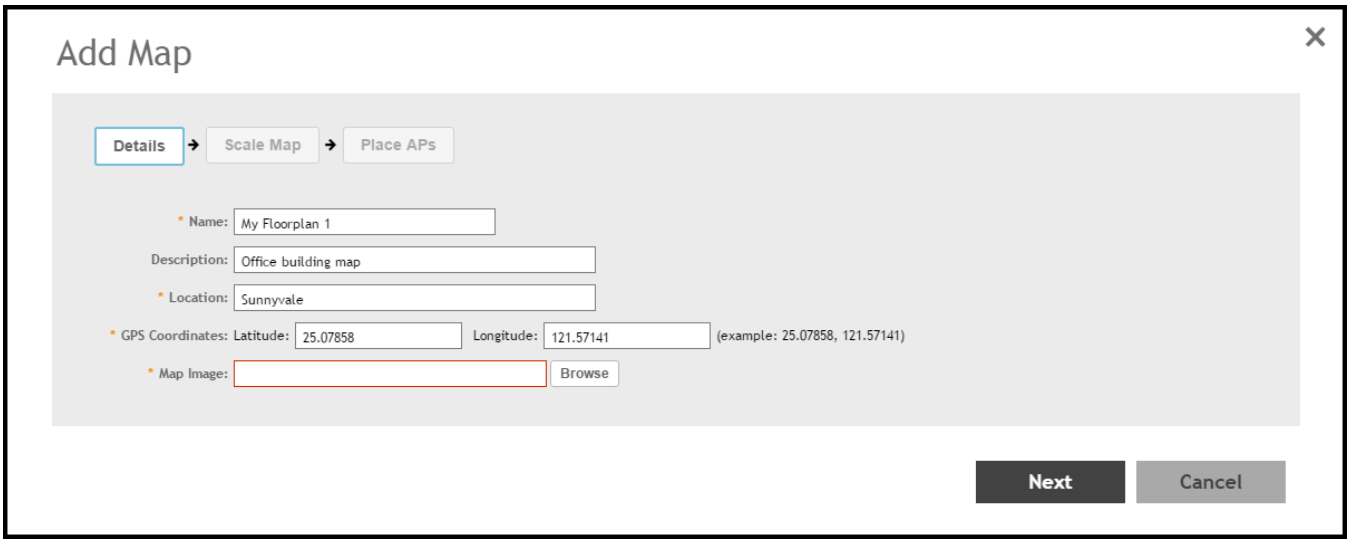
- AP status, performance, and health conditions
- Client connections to an AP
- Location-specific trouble spots related to AP or client connectivity

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 31 Creating the Add Map form



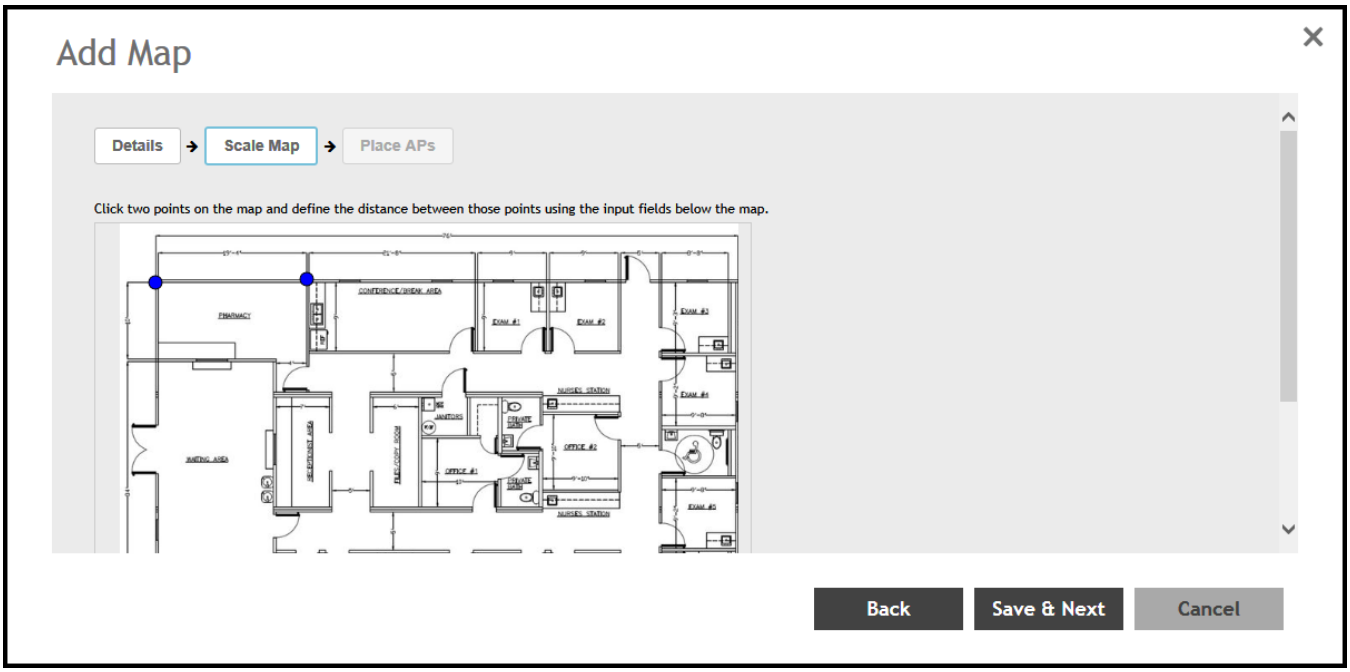
6. To add a **Map Image**, click **Browse** and select a site, venue, or floor map in jpg, jpeg, png, bmp or svg file formats.

   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.

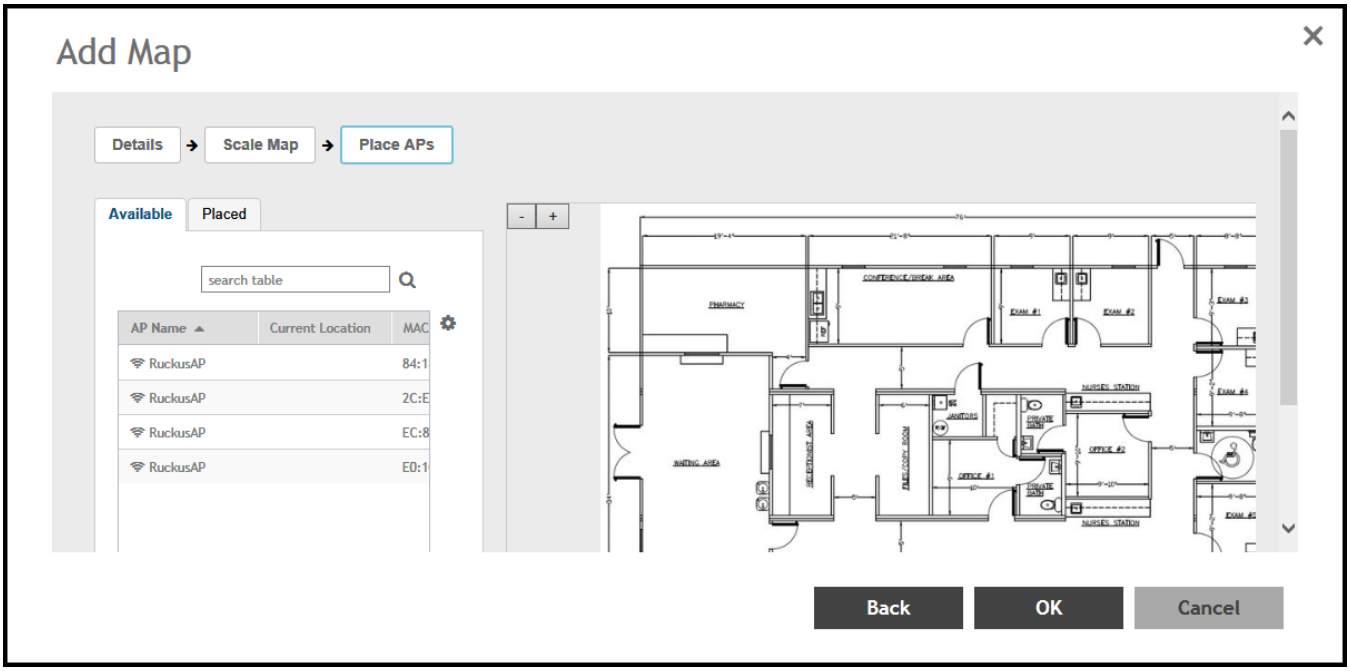
FIGURE 32 Indicating the Selected Points on the Map



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.

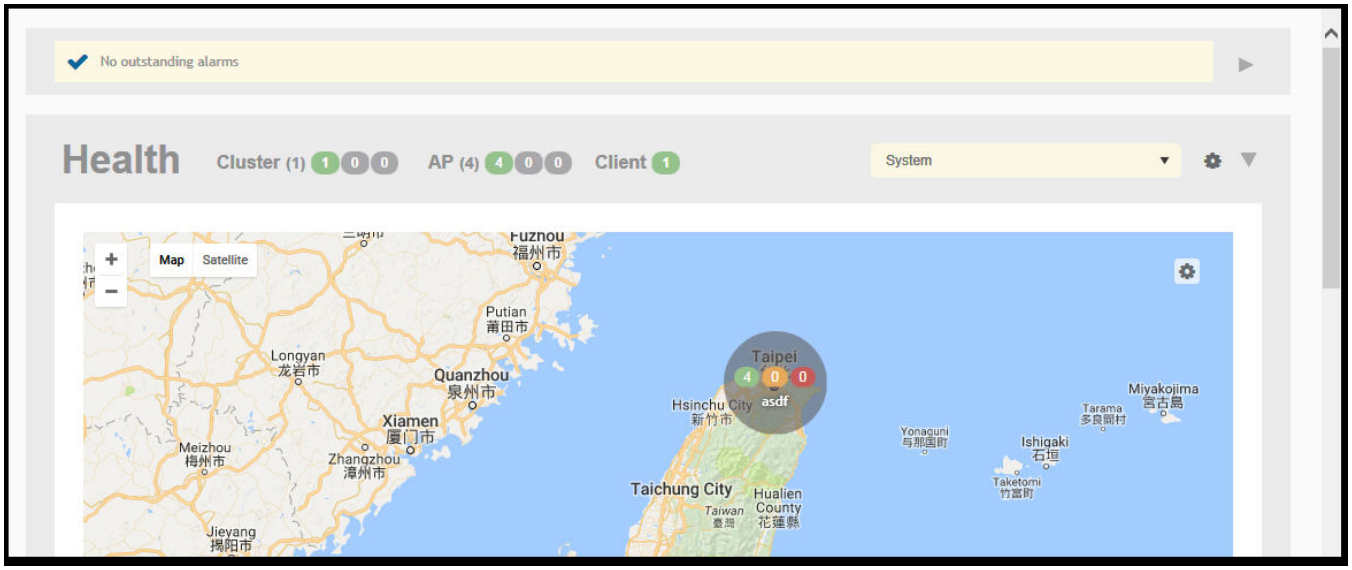
    FIGURE 33 Dragging and dripping to place APs on the Floorplan



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 34 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.

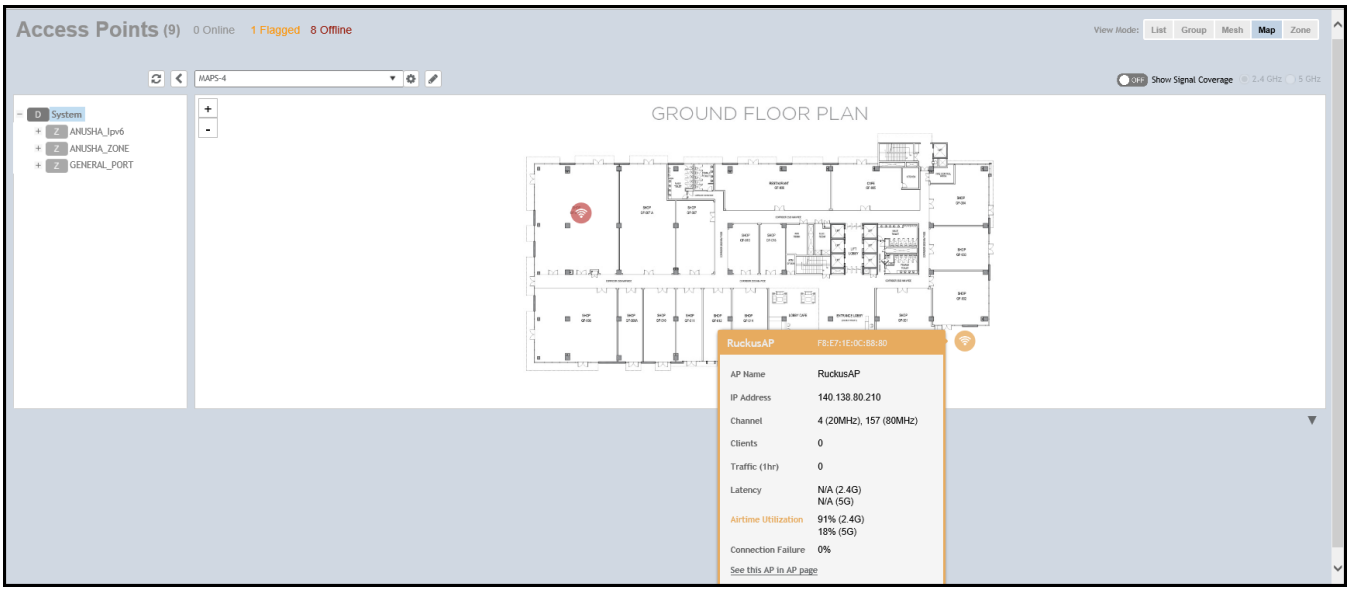
FIGURE 35 RF Coverage Heat Map

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 36 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.

AP Provisioning and Swapping

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.

Approving Access Points

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

NOTE
This feature is applicable only for SZ100 and vSZ-E platforms.

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**.

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.
2. To view the list of APs pending for approval, click the **Unapproved APs** below the left pane.
3. 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.
4. From the **AP Zone** drop-down, select the zone.
5. In **Last 4 digit of AP S/N**, enter the last four digit serial number of the AP.
6. 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.

Viewing Mesh APs

Mesh APs are wireless access points. They provide consistent transmission of data, any failures do not disrupt the data transmision.

To view the Mesh APs on the controller, perform the following steps.

1. From the main menu, click the **Network** tab.

2. Click **Access Point**, the **Access Point** page appears. On the upper-right corner of the page, select the **Mesh** option from **View** mode.

   The below table describes the fields for Mesh AP, and the description.

   FIGURE 37 Viewing Mesh APs

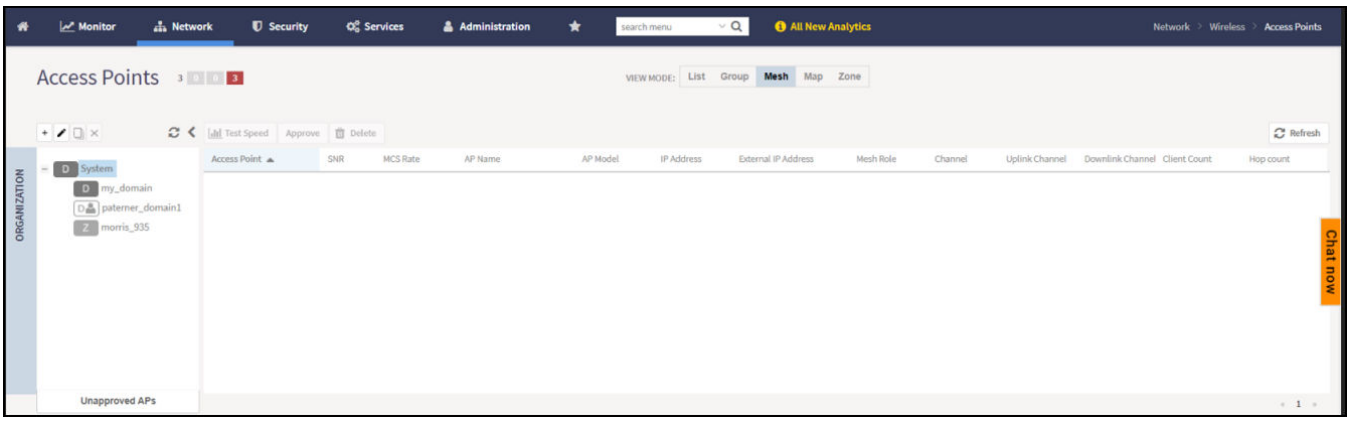


TABLE 13 Access Point Details

Field Name	Description
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.
MCS Rate (Tx) (Rx)	Displays the median of MCS rate Tx/Rx for both client and AP in there respective pages. These values are updated every 180 seconds (Highscale) and 90 seeconds (Essentials).
AP Name	Displays the name assigned to the access point
AP Model	Displays the model name.
IP Address	Displays the IP address assigned to the wireless client
External IP Address	Displays the APs external IP address
Mesh Role	Displays the status of APs
Channel	Displays the wireless channel (and channel width) that the wireless client is using
Traffic (Uplink)	Displays the total uplink traffic (in KB/MB/GB/TB) for this client in this session
Traffic (Downlink)	Displays the total downlink traffic (in KB/MB/GB/TB) for this client in this session
Client Count	Displays the number of client in theAP
Hop Count	Displays the number of hop counts

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
For SZ300 and vSZ-H platforms, 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.

NOTE
For SZ100 and vSZ-E platforms, 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 Default 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.

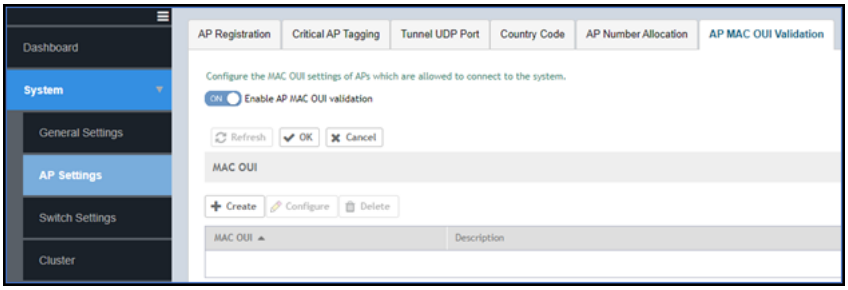
1. Go to **Network** > **Wireless** > **AP Settings** > **AP Registration** .
2. Select the rule from the list and click.
   - **Up**—To give a rule higher priority, move it up the table
   - **Down**—To give a rule lower priority, move it down the table
3. Click **Update Priorities** to save your changes.

Creating an AP MAC OUI Address

To create the MAC OUI address for an AP, perform the following -

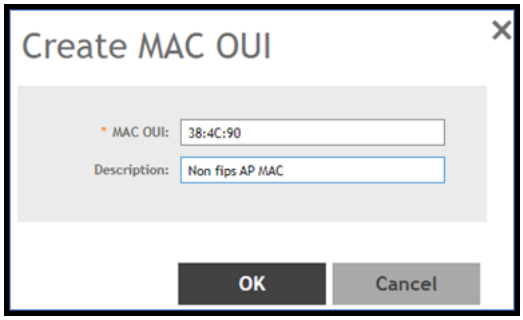
1. Go to **System** > **AP Settings** > **AP MAC OUI Validation**.
2. To turn **ON**, click **Enable AP MAC OUI Validation** radio button.

   FIGURE 38 AP MAC OUI Validation



3. Under **MAC OUI** section, click **Create**. This displays **Create MAC OUI** window.

   FIGURE 39 Create MAC OUI



4. Enter the **MAC OUI**.

5. Click **OK**.

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 SmartZone controller deployments. You can migrate ZoneDirector AP configuration information to SmartZone controllers from the controller itself, using a migration tool.

The AP models must be supported by the controller.

NOTE
Not more than 50 APs will be migrated from ZoneDirector to SmartZone.

TABLE 14 Migration Support Matrix

SmartZone Version	ZoneDirector Version
3.5.x	9.13x
3.6.x	9.13.x, 10.0.x, 10.1.x
5.0.x	9.13.x, 10.0.x, 10.1.x
5.1.x	9.13.x, 10.0.x, 10.1.x, 10.2.x
5.2.x	9.13.x, 10.0.x, 10.1.x, 10.2.x, 10.3.x, 10.4.x
6.x	9.13.x, 10.0.x, 10.1.x, 10.2.x, 10.3.x, 10.4.x, 10.5.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 to the release notes.

AP Switchover

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.

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)

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

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.

Rehoming Managed APs

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

AP Auto Rehome

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

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

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

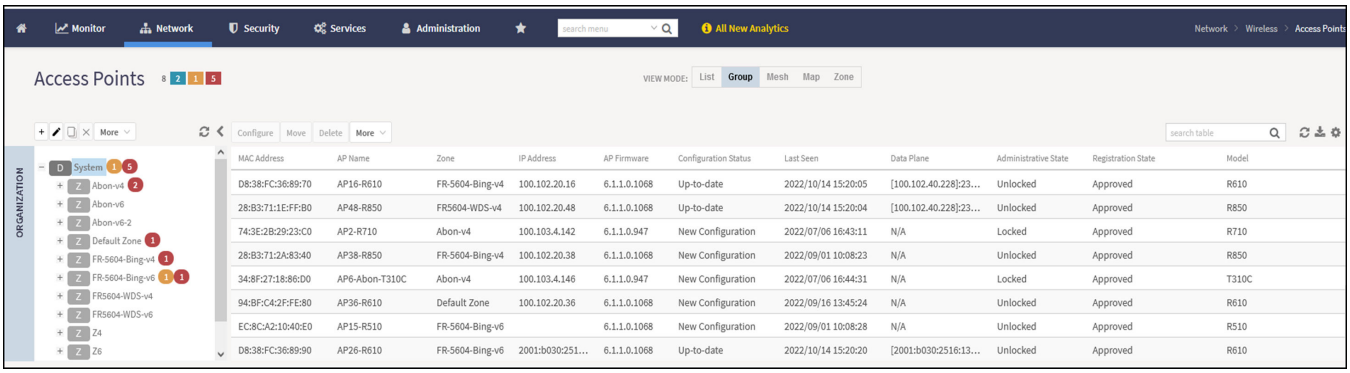
NOTE
AP Auto Rehome is supported only on SZ300 and vSZ platforms.

NOTE
AP Auto Rehome is configurable only at the zone level.

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

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

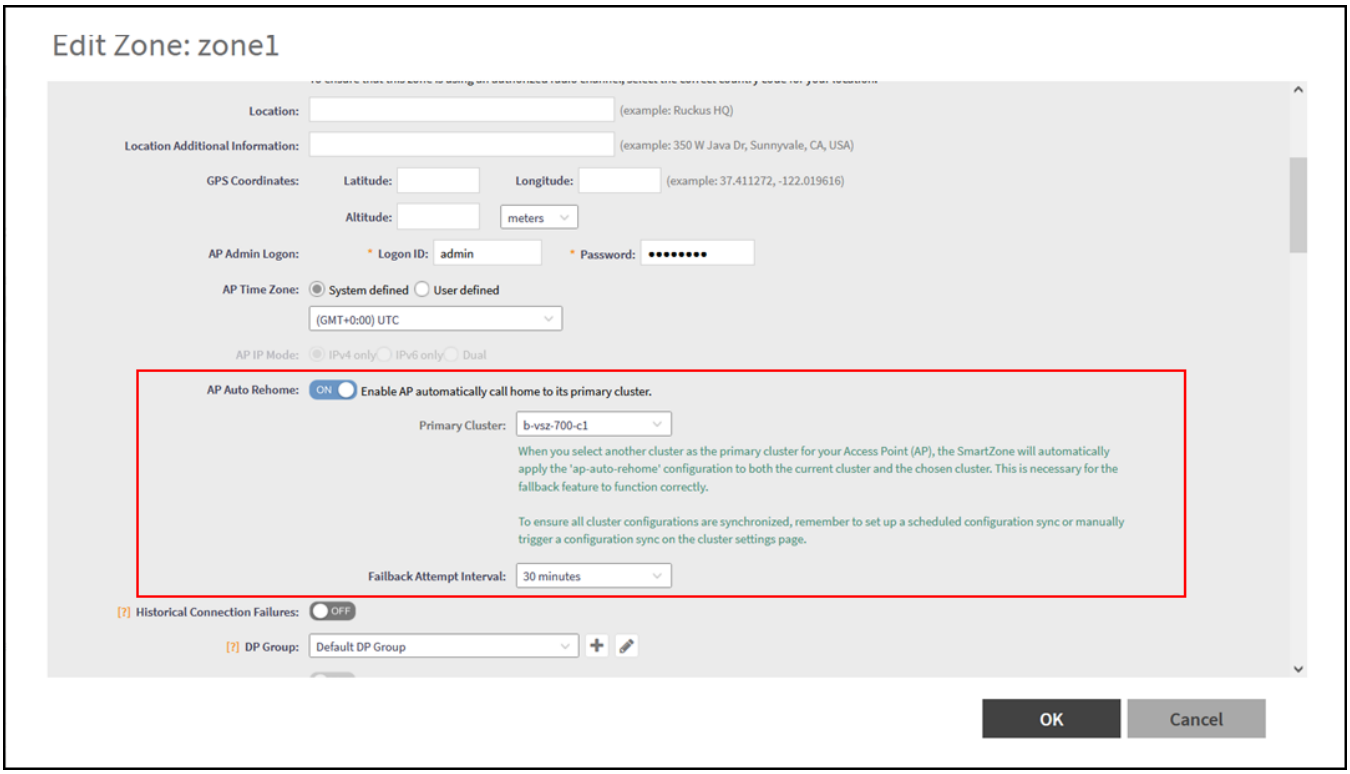
FIGURE 40 Access Points Page



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

   The **Edit Zone** page is displayed.

   FIGURE 41 Editing a Zone



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

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

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:

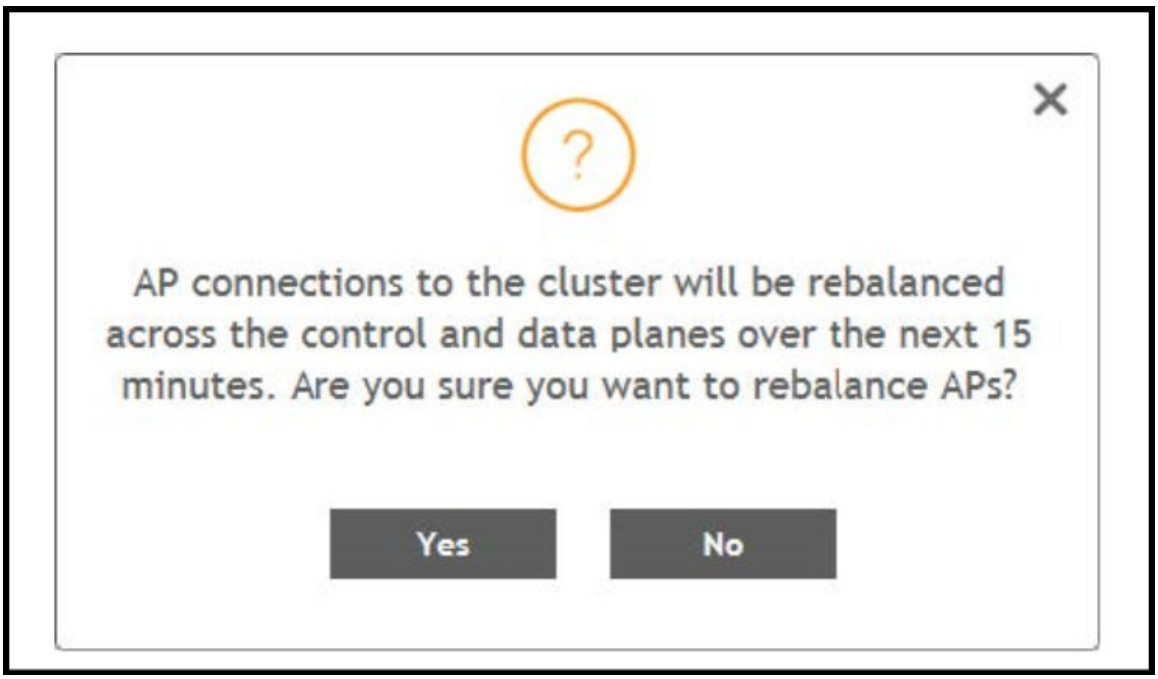
   - **Event 770: Generate ApConfig for plane load rebalance succeeded.**
   - **Event 771: Generate ApConfig for plane load rebalance failed.**

   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 42 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.

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.

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

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.

Reports

Report Generation

Creating Reports

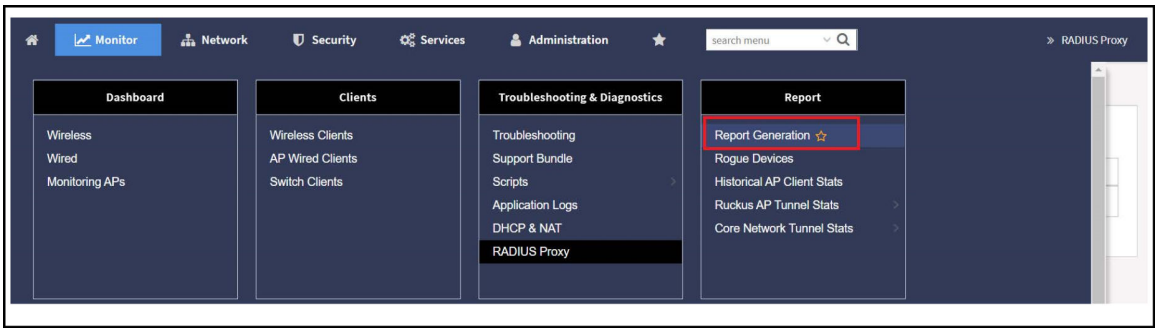
You can create reports to obtain a historical view of the maximum and minimum number of clients connected to the system, the number of clients connected at different time intervals, and the traffic statistics for the switches.

Complete the following steps to create a new report.

1. From the main menu, go to **Monitor**>**Report** >**Report Generation**.

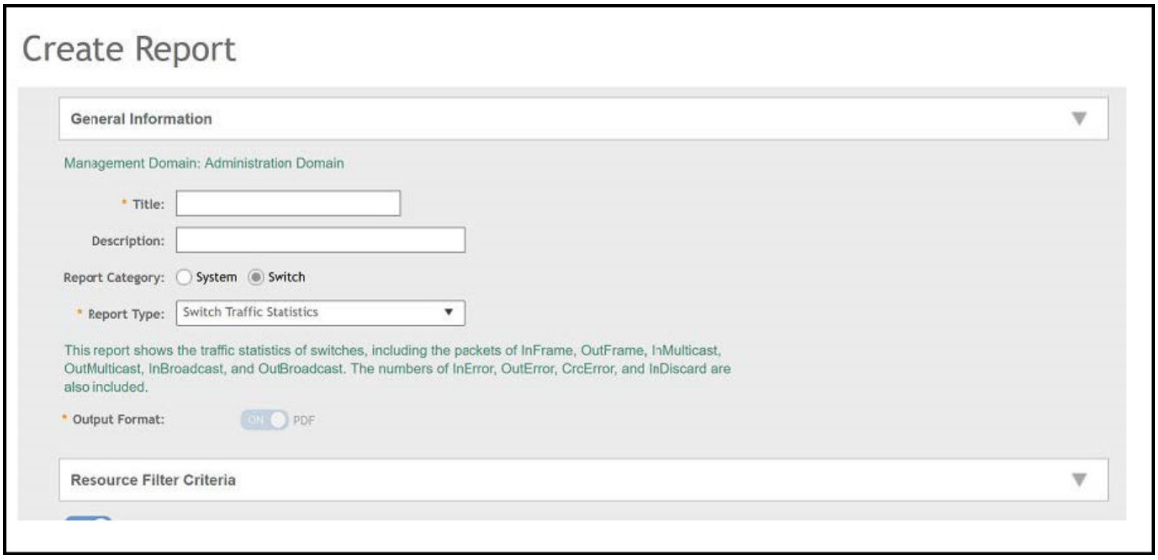
   The **Report Generation** page is displayed.

   FIGURE 43 Report Generation Screen



2. Click **Create**. The **Create Report** dialog box is displayed.

FIGURE 44 Create Report Dialog Box



3. Enter the required parameters as described in the following table.

TABLE 15 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 type.
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 the System option), and Switch.	Enter the device or switch name or select the device or switch from the list and select the option.
SSID	Indicates the SSID for which you want to generate the report.	Select the check box and select 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 because 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 select the required frequency: • **2.4G** • **5G** • **6GHz/5GHz**
Time Filter		
Time Interval	Defines the time interval at which to generate the report.	Select the required time interval.

TABLE 15 Report Parameters (continued)

Field	Description	Your Action
Time Filter	Defines the time duration for which to generate the report.	Select the required time filter.
Schedules		
Enable/Disable	Specifies the scheduled time when a report must be generated. By default, the current system time zone is also displayed.	By default, this option is disabled. Select **Enable** and **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, this option is disabled. Select **Enable**, click **Add New**, and enter the email address. You can add multiple email addresses.
Export Report Results		
Enable/Disable	Automatically uploads the reports to an FTP server.	By default, this option is disabled. Select **Enable**, and select the FTP server from the drop-down list and click **Test**.

4. Click **OK**.

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

Generating Reports

Complete the following steps to generate a report.

1. From the main menu, go to **Monitor** > **Report** > **Report Generation**.

   The **Report Generation** page is displayed.

2. Select the required report from the list, and click **Generate**. The **Report Generated** form is displayed.
3. Click **OK**. The report is generated and listed in the **Report Results** pane.
4. From the **Result Links** column, select the required format, and click **Open** to view the report.

Global AP Settings

Configuring APs

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.

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 **Access Point Edit Parameters** table below.
3. Click **OK**.

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

TABLE 16 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.

TABLE 16 Access Point Edit Parameters (continued)

Field	Description	Your Action
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	Helps manage and allocate radio frequency resources. A lower channel width allows the zone to potentially serve more clients, whereas a higher channel width improves throughput, but potentially serves fewer clients and increases the possibility of interference. The Auto setting defaults to 20 MHz channelization.	Set the channel bandwidth used during transmission to either 20 or 40 (MHz), or select Auto to set it automatically. **NOTE** By default, for the **Country Code** Indonesia, the **Channelization** width is set to 20 MHz only for outdoor APs.
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.
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.

TABLE 16 Access Point Edit Parameters (continued)

Field	Description	Your Action
Protection Mode	Allows to manually override the protection mode and select from the options - • None • RTS/CTS • CTS Only	Select the preferred protection mode.
WLAN Group	Allows to manually configure the WLAN Group. To add a WLAN group, refer to Creating a WLAN Group on page 268.	Add a WLAN group to the AP Group.
WLAN Service	By default it is ON.	
Background Scan	Allows the AP radio to scan other channels in the band for accessing channel health and capacity, detecting rogue devices, optimizing and maintaining mesh links and to discover AP neighbors.	Enter the duration in seconds. Range: 1 through 65535.
Auto Channel Selection	Automatically adjusts the channel for network self-healing and performance optimization. **ChannelFly** is set as the default option. For the **ChannelFly** option, you may also modify the default settings for the **Channel Change Frequency** and **Full Optimization Period**. The **Channel Change Frequency** slidebar allows you to specify the responsiveness of ChannelFly to interference (with consideration for the impact on associated clients), ranging from Minimal to Very Often. The **Full Optimization Period** timeslot bar allows you to specify one or more periods of time when ChannelFly is allowed to fully optimize the channel plan, ignoring the impact of channel changes on associated clients. Select time periods when the wireless network is servicing the fewest clients.	Select the required option. • **Background Scanning**: Changes the AP channel when there is an interference. • **ChannelFly**: Monitors potential throughput and will change channels to learn each channel's capacity, optimize throughput, and to avoid interference.
AP Configuration > **Band/Spectrum Configuration** > **5 GHz**		
Channelization	Helps manage and allocate radio frequency resources. A lower channel width allows the zone to potentially serve more clients, whereas a higher channel width improves throughput, but potentially serves fewer clients and increases the possibility of interference. Prior to SmartZone release 7.0.0, the Auto setting defaulted to 80 MHz channelization. Beginning in SmartZone release 7.0.0, the Auto setting defaults to 40 MHz channelization.	Set the channel bandwidth used during transmission: Auto, 20, 40, 80 and 160. **NOTE** By default, for the **Country Code** Indonesia, the **Channelization** width is set to 20 MHz only for outdoor APs.
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.

TABLE 16 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.
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 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.
Protection Mode	Allows to manually override the protection mode and select from the options - • None • RTS/CTS • CTS Only	Select the preferred protection mode.
WLAN Group	Allows to manually configure the WLAN Group.	Add a WLAN group to the AP Group.
WLAN Service	By default it is ON.	

TABLE 16 Access Point Edit Parameters (continued)

Field	Description	Your Action
Auto Channel Selection	Automatically adjusts the channel for network self-healing and performance optimization. **ChannelFly** is set as the default option. For the **ChannelFly** option, you may also modify the default settings for the **Channel Change Frequency** and **Full Optimization Period**. The **Channel Change Frequency** slidebar allows you to specify the responsiveness of ChannelFly to interference (with consideration for the impact on associated clients), ranging from Minimal to Very Often. The **Full Optimization Period** timeslot bar allows you to specify one or more periods of time when ChannelFly is allowed to fully optimize the channel plan, ignoring the impact of channel changes on associated clients. Select time periods when the wireless network is servicing the fewest clients.	Select the required option. • **Background Scanning**: Changes the AP channel when there is an interference. • **ChannelFly**: Monitors potential throughput and will change channels to learn each channel's capacity, optimize throughput, and to avoid interference.
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	Helps manage and allocate radio frequency resources. A lower channel width allows the zone to potentially serve more clients, whereas a higher channel width improves throughput, but potentially serves fewer clients and increases the possibility of interference. The Auto setting defaults to 160 MHz channelization.	Set the channel bandwidth used during transmission: Auto, 20, 40, 80 and 160.
Channel	Indicates the channel to use.	• In countries where only 6 GHz Indoor channels are permitted, the 6 GHz Outdoor channels are disabled. • If a country permits the use of 6GHz Indoor and Outdoor channels, the controller will provide the available channel ranges for both Indoor and Outdoor channels. For example, in the country US, the available channel ranges are - – Indoor APs can operate in UNII-5,6,7,8 – Outdoor APs can operate in UNII-5,7 • You can choose channel options for Indoor and Outdoor channels. The default setting for both Indoor and Outdoor channels is **Auto**.
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 16 Access Point Edit Parameters (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.
Background Scan	Allows the AP radio to scan other channels in the band for accessing channel health and capacity, detecting rogue devices, optimizing and maintaining mesh links and to discover AP neighbors.	Enter the duration in seconds. Range: 1 through 65535.
Auto Channel Selection	Automatically adjusts the channel for network self-healing and performance optimization. **ChannelFly** is set as the default option. For the **ChannelFly** option, you may also modify the default settings for the **Channel Change Frequency** and **Full Optimization Period**. The **Channel Change Frequency** slidebar allows you to specify the responsiveness of ChannelFly to interference (with consideration for the impact on associated clients), ranging from Minimal to Very Often. The **Full Optimization Period** timeslot bar allows you to specify one or more periods of time when ChannelFly is allowed to fully optimize the channel plan, ignoring the impact of channel changes on associated clients. Select time periods when the wireless network is servicing the fewest clients.	Select the required option. • **Background Scanning**: Changes the AP channel when there is an interference. • **ChannelFly**: Monitors potential throughput and will change channels to learn each channel's capacity, optimize throughput, and to avoid interference.
AP Configuration > **Band/Spectrum Configuration** > **Lower 5 GHz**		
Channelization	Helps manage and allocate radio frequency resources. A lower channel width allows the zone to potentially serve more clients, whereas a higher channel width improves throughput, but potentially serves fewer clients and increases the possibility of interference. Prior to SmartZone release 7.0.0, the Auto setting defaulted to 80 MHz channelization. Beginning in SmartZone release 7.0.0, the Auto setting defaults to 40 MHz channelization.	Set the channel bandwidth used during transmission: Auto, 20, 40, 80 and 160. **NOTE** By default, for the **Country Code** Indonesia, the **Channelization** width is set to 20 MHz only for outdoor APs.
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.

TABLE 16 Access Point Edit Parameters (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 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 maintaining mesh links and to discover AP neighbors.	Enter the duration in seconds. Range: 1 through 65535.
Auto Channel Selection	Automatically adjusts the channel for network self-healing and performance optimization. **ChannelFly** is set as the default option. For the **ChannelFly** option, you may also modify the default settings for the **Channel Change Frequency** and **Full Optimization Period**. The **Channel Change Frequency** slidebar allows you to specify the responsiveness of ChannelFly to interference (with consideration for the impact on associated clients), ranging from Minimal to Very Often. The **Full Optimization Period** timeslot bar allows you to specify one or more periods of time when ChannelFly is allowed to fully optimize the channel plan, ignoring the impact of channel changes on associated clients. Select time periods when the wireless network is servicing the fewest clients.	Select the required option. • **Background Scanning**: Changes the AP channel when there is an interference. • **ChannelFly**: Monitors potential throughput and will change channels to learn each channel's capacity, optimize throughput, and to avoid interference.
AP Configuration > **Band/Spectrum Configuration** > **Upper 5 GHz**		
Channelization	Helps manage and allocate radio frequency resources. A lower channel width allows the zone to potentially serve more clients, whereas a higher channel width improves throughput, but potentially serves fewer clients and increases the possibility of interference. Prior to SmartZone release 7.0.0, the Auto setting defaulted to 80 MHz channelization. Beginning in SmartZone release 7.0.0, the Auto setting defaults to 40 MHz channelization.	Set the channel bandwidth 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 16 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 maintaining mesh links and to discover AP neighbors.	Enter the duration in seconds. Range: 1 through 65535.
Auto Channel Selection	Automatically adjusts the channel for network self-healing and performance optimization. **ChannelFly** is set as the default option. For the **ChannelFly** option, you may also modify the default settings for the **Channel Change Frequency** and **Full Optimization Period**. The **Channel Change Frequency** slidebar allows you to specify the responsiveness of ChannelFly to interference (with consideration for the impact on associated clients), ranging from Minimal to Very Often. The **Full Optimization Period** timeslot bar allows you to specify one or more periods of time when ChannelFly is allowed to fully optimize the channel plan, ignoring the impact of channel changes on associated clients. Select time periods when the wireless network is servicing the fewest clients.	Select the required option. • **Background Scanning**: Changes the AP channel when there is an interference. • **ChannelFly**: Monitors potential throughput and will change channels to learn each channel's capacity, optimize throughput, and to avoid interference.

TABLE 16 Access Point Edit Parameters (continued)

Field	Description	Your Action
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
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 overrides 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.
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**		

TABLE 16 Access Point Edit Parameters (continued)

Field	Description	Your Action
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		
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 AP to send syslog data to the syslog server on the network.	Select the option.

TABLE 16 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. › **Protocol**: 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. › **Protocol**: 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.

TABLE 16 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 **Override** 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 **Administration** > **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**.

Swap Configuration

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.

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 17 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

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.

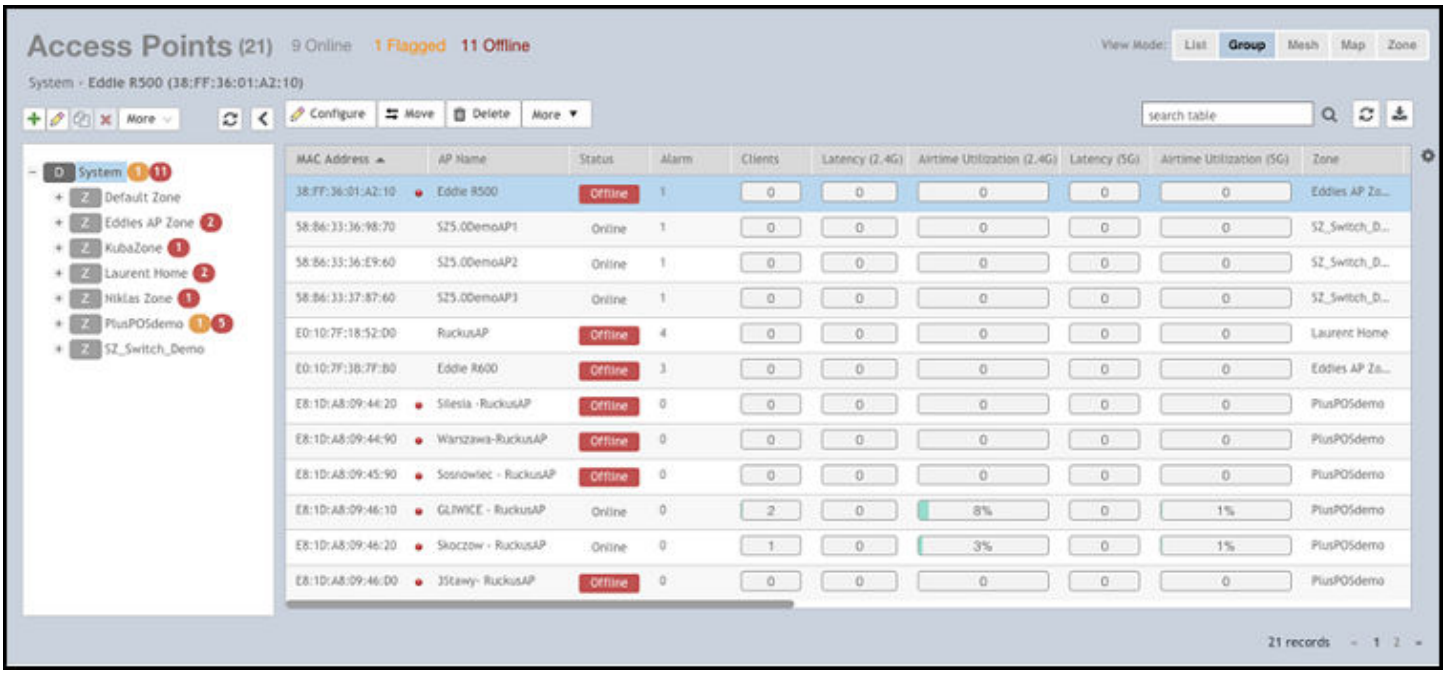
Follow these steps to tag critical APs (APs that exceed the data traffic threshold you have defined) automatically:

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 45 APs Tagged as Critical



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**.

Configuring the Tunnel UDP Port

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

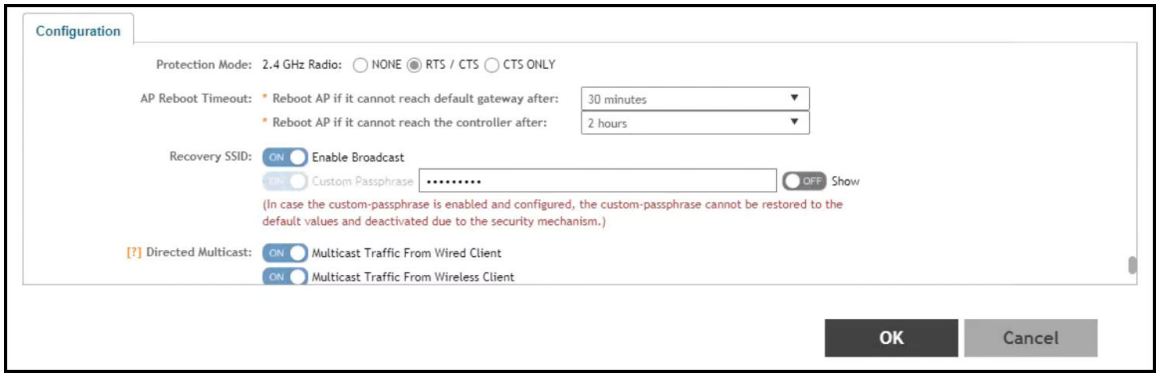
To configuring the tunnel UDP port:

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

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:

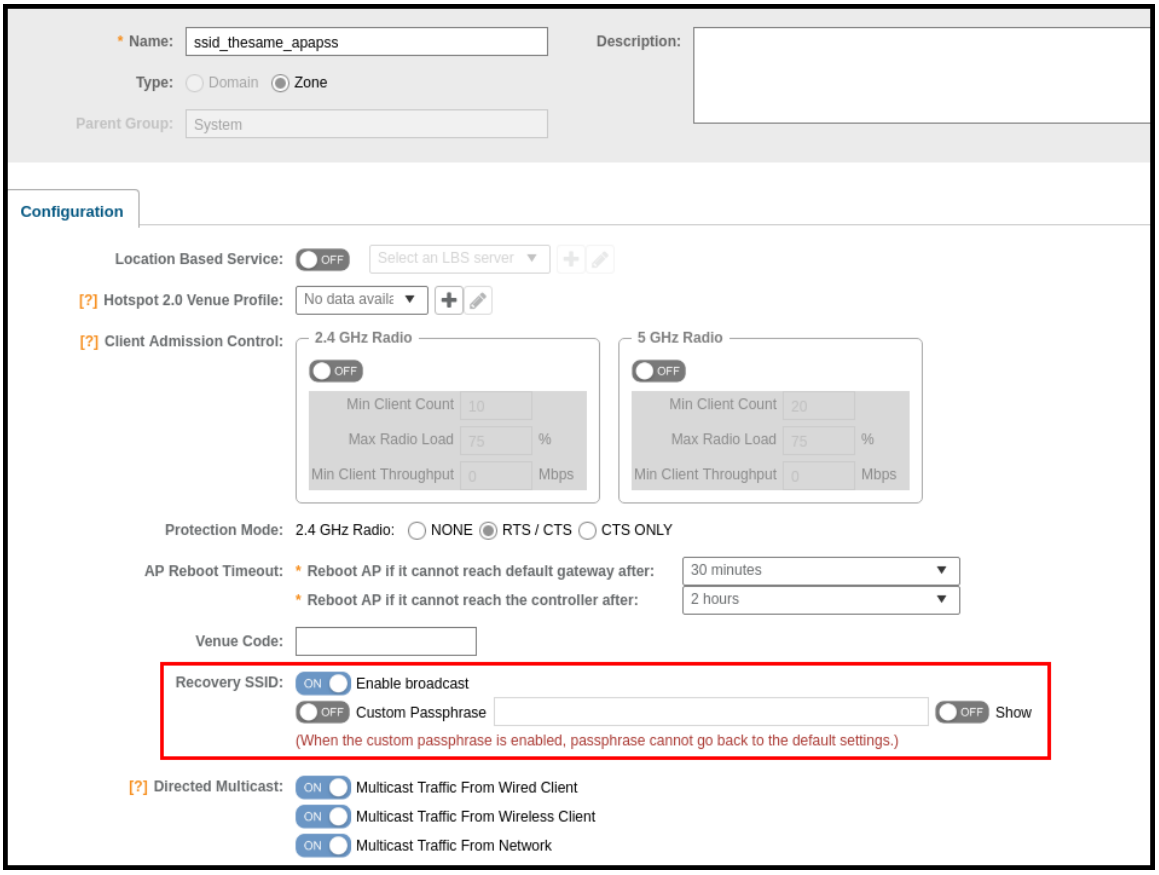
- The default of this Recovery SSID feature is enabled. The default passphrase is AP admin password in clear text format.
- If the user wants to change it, input the passphrase while enabling.
- The validation of passphrase, apply the same rule of WLAN passphrase.
- The passphrase can be clear text stored 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

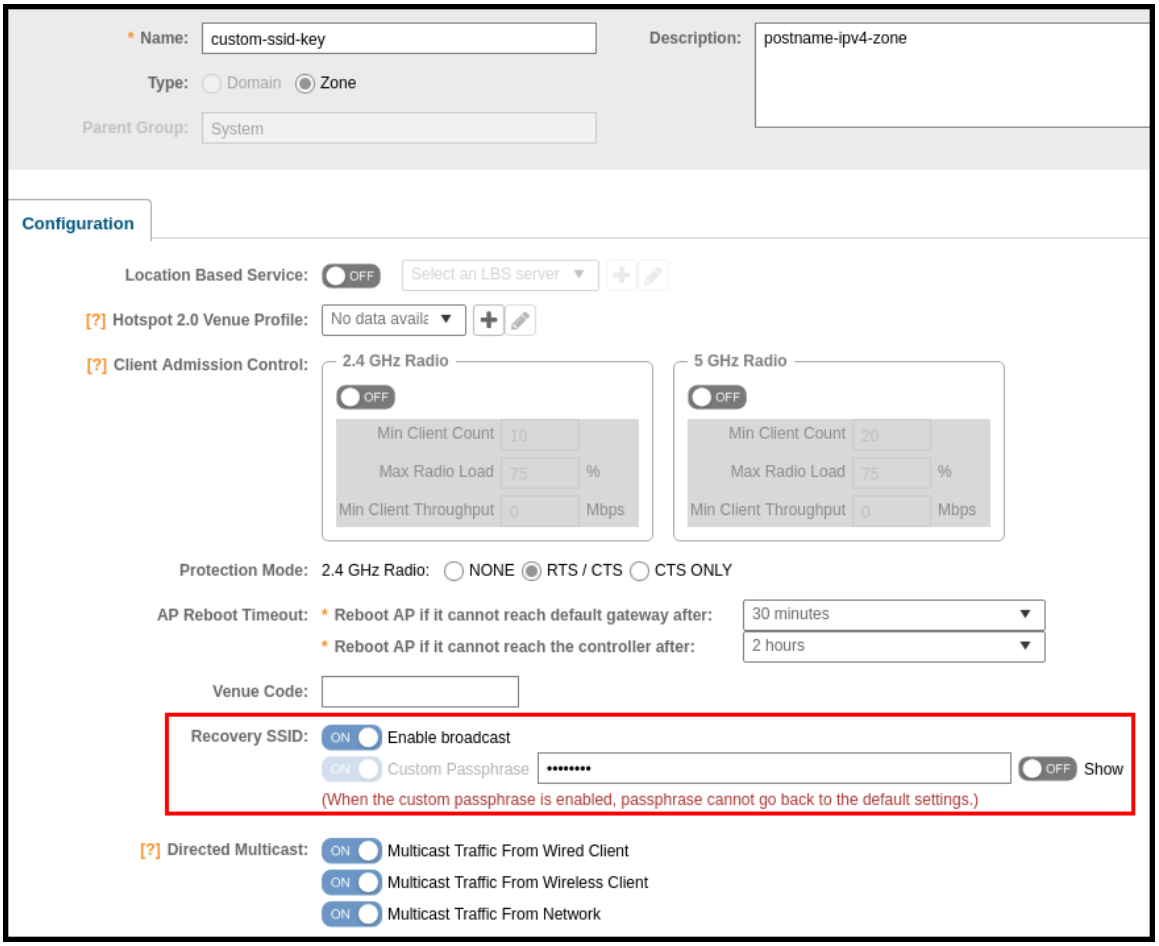
When the Custom passphrase is disabled, the Custom passphrase filed is empty.

FIGURE 46 Custom Passphrase Disabled



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

FIGURE 47 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 18 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 19 Non-Standard High Power Solution Summary

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

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

TABLE 20 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 Access Point

TABLE 21 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 22 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 23 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

TABLE 23 R720 (continued)

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 the controller GUI

TABLE 24 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 Access Point

TABLE 25 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 through the controller 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 the controller GUI

TABLE 26 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 27 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

TABLE 27 T750 (continued)

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 28 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 29 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

POE tables for different 11AT/ BT5 Access Point

For 3-radio APs starting R760, the power mode table will support another power mode within bt5. When the LLDP module is loaded the power negotiation starts from 40W (BT5) in auto or BT5 mode and stops negotiation when it reaches 25.5W (AT).

NOTE
WLAN services are available only if the power negotiation is completed. Hence, there may be a delay in availability for WLAN services.

TABLE 30 R760

Power Mode	Power Source	2G/5G/6G Radio Chains (Tx/Rx)	(Use R9 CC) 2G/5G/6G Tx power (dBm)	10GE eth	1GE eth	USB (3W)	IOT	Power Consumption From estimate (W@50C)	LLDP Request
Full Power	DC	4x4/4x4/4x4	22/20/22	Yes	Yes	Yes	Yes	38.3	N/A
POE 802.3bt5	POE Switch	4x4/4x4/4x4	22/20/22	Yes	Yes	Yes	Yes	36.08	40
POE 802.3bt5	POE Switch	4x4/4x4/4x4	22/20/22	Yes	Yes	No	Yes	33.83	35
POE 802.3at	POE Switch or POE Injector	4x4/4x4/4x4	Mode: 2-5-5 15/16/15 Mode: 2-5-6 13/14/14	Yes	No	No	Yes	25.48	25.5
POE 802.3af	POE Switch	Not supported, used only for LLDP power negotiation. 802.3af mode WLANs are disabled, and TX power set to 1.							

Link Layer Discovery Protocol (LLDP)

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 31 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

Viewing LLDP Neighbors

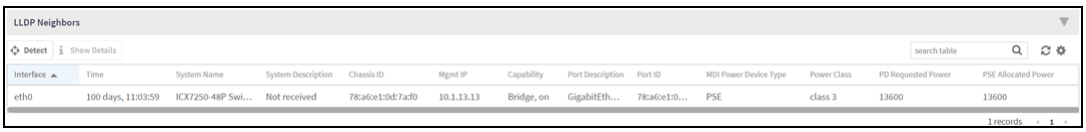
You can view basic information, and detailed information about the LLDP neighbor of an AP form the controller interface.

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 48 Neighbor LLDP APs for a Non-Mesh Zone

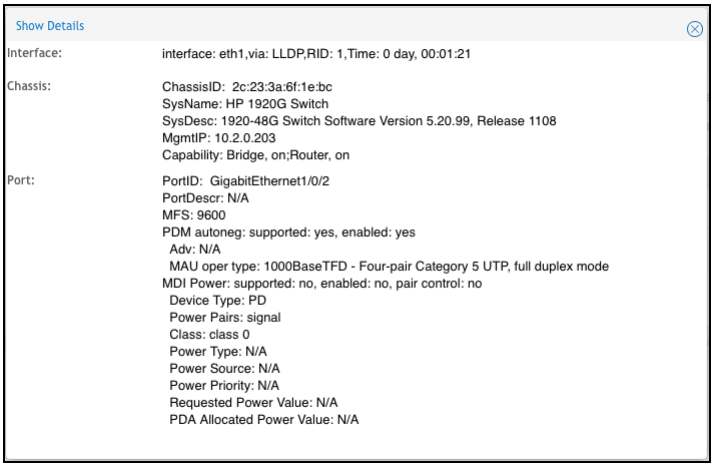


   You can view basic information about the LLDP AP neighbor such as:

   - 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 49 Additional LLDP AP Neighbor Details



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

Link Aggregation Protocol (LACP)

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.

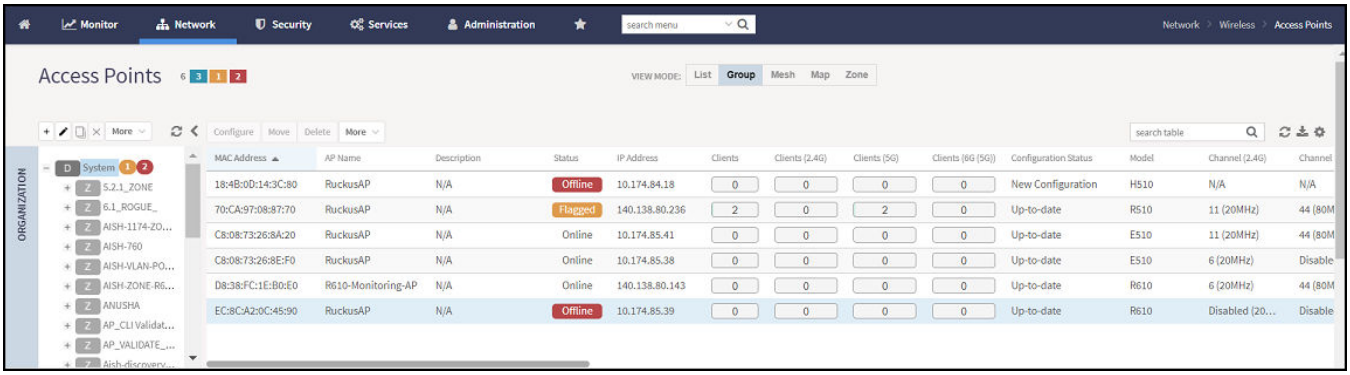
Enabling the LACP Support for a Zone

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.

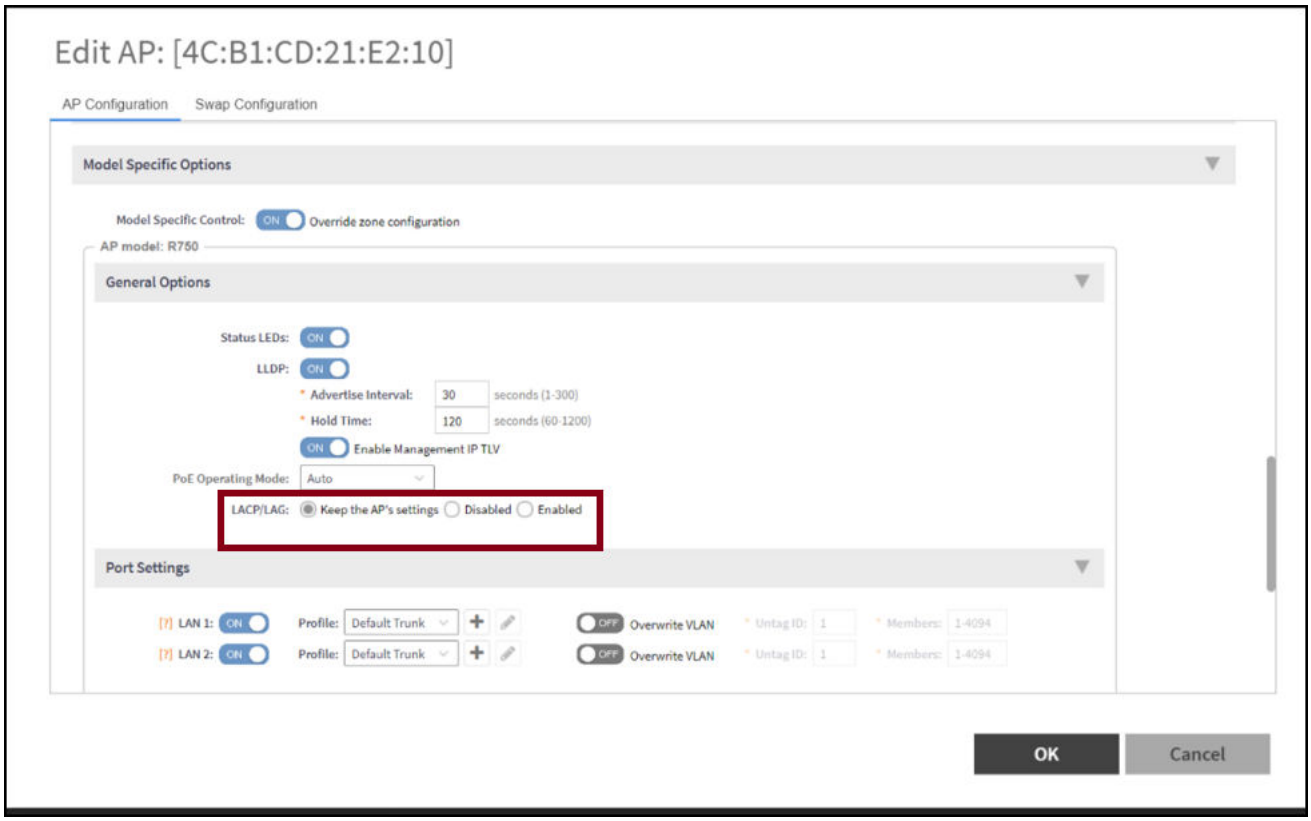
   FIGURE 50 Viewing the Access Points



2. Select a zone and click .

   The **Configure Group** page is displayed.

   FIGURE 51 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

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.

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**.

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, the link speed must be downgraded and should be 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 follow these steps.

1. From the main menu 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**.

AP Ethernet Ports

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.

Follow the below steps to create an **Ethernet Port** profile.

1. From the main menu go to **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.

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:
       - Default WAN: Enables default WAN configuration
       - Local Subnet(LAN): Enables DHCP service on ethernet ports. In the **VLAN Options**, select the **VLAN Untag ID** in the ethernet profile which is similar to 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 Address Resolution Protocol (ARP) limits the rate of ARP requests from the connected clients to prevent ARP flooding. Enter the number of packets to be reviewed for 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 limits the rate 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.
     - User Side Port: User Side Port is by default enabled when 802.1x is enabled.
       - 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.
   - Wired Client Isolation
     - Client Isolation: Prevents wired clients from communicating with each other. This option isolates wired client traffic from all hosts on the same VLAN/subnet. By default, this option is disabled. Enable the following options as approriate:
       - Isolate unicast packets: Isolates only unicast packets between a wired client enabled with client isolation and other clients of the AP. By default, this option is enabled.
       - Isolate multicast/broadcast packets: Isolates only multicast/broadcast packets between a wired client enabled with client isolation and other clients of the AP. By default, this option is disabled.
       - Automatic support for VRRP: Isolates packets in Virtual Router Redundancy Protocol (VRRP) deployment. By default, this option is disabled indicating the AP is not in VRRP deployment.

VIDEO

Client Isolation. Defines wired destinations on the local subnet that can be reached, even if client isolation is enabled.

Click to play video in full screen mode.

- Authentication Options
  - 802.1X: Select to enable 802.1X authentication.
  - 802.1X Role: Select the authenticator role from the menu.
    - Supplicant: You can customize the user name and password to authenticate as a supplicant role or use the credentials of the AP MAC address.
    - MAC-based Authenticator: Each MAC address host is individually authenticated. Each newly learned MAC address triggers an Extensible Authentication Protocol over LAN (EAPoL) request-identify frame.
    - Port-based Authenticator: Only a single MAC address host must be authenticated for all hosts to be granted access to the network.
  - 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: Select this option if you want to limit the device access to internal network resources only.
- 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:
- Port Type: Must be Access Port
- Access Network: Must be Tunnel Ethernet Port traffic
- 802.1x Role: Enabled with Mac Based
- DVLAN: Enabled
- Q in Q (Client Visibility and User Side Port are by default enabled): 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 wired clients.
  - L2 Access Control Policy: Select the Layer 2 policy for wired ports. When the User Side Port is not enabled, 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 of the firewall profile. Click  to create a new policy. Refer to the **Creating a L2 Access Control Service** section of the *Network Administrative Guide* for more information.
- 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.

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 32 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.

Model Specific Settings

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 33 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 33 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 34 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**.

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*.

AP Services

DHCP & NAT

Viewing DHCP and NAT Information

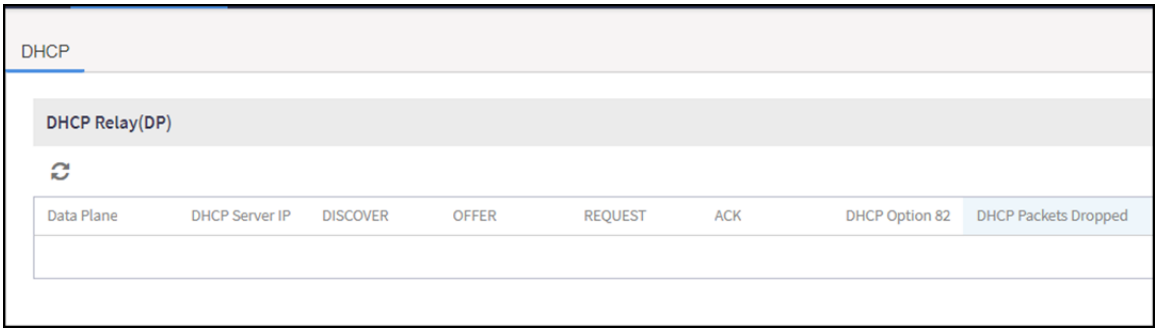
DHCP or NAT functionality on controller managed APs and DPs (data planes) allows customers to reduce costs and complexity by removing the need for DHCP server or NAT router to provide IP addresses to clients. For data traffic aggregation and services delivery, choose the appropriate user profile for DHCP and NAT services on the virtual controllers.

Complete the following steps to view DHCP servers and NAT router information.

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

1. From the main menu go to **Monitor** > **Troubleshooting&Diagnostics** > **DHCP&NAT** in High or Enterprise virtual controllers or **Monitor** > **Troubleshooting&Diagnostics** > **DHCP** in SZ300 or SZ100 controller platforms.
2. Select **DHCP** to monitor **DHCP Relay (DP)** of the data planes. It displays information pertaining to relay packets, server packets and the number of IP addresses assigned when **DHCP Relay** is enabled in **Core Network Tunnel** > **Bridge or L2oGRE**.

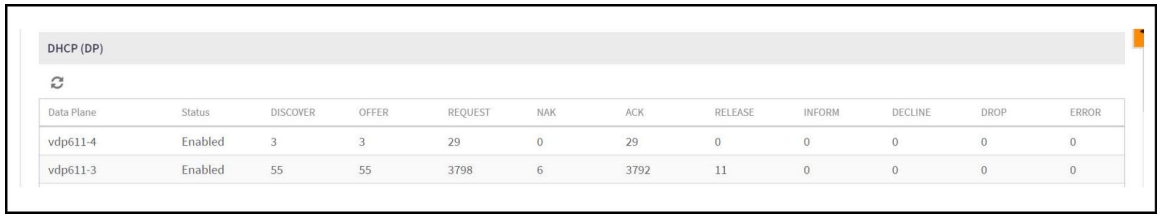
FIGURE 52 DHCP Relay



The following options are seen on virtual controllers.

3. From the main menu go to **Monitor** > **Troubleshooting&Diagnostics** > **DHCP&NAT** > > **DHCP (DP)** to monitor data planes. It displays information pertaining to data planes, status and other related information to data planes

FIGURE 53 DHCP DP

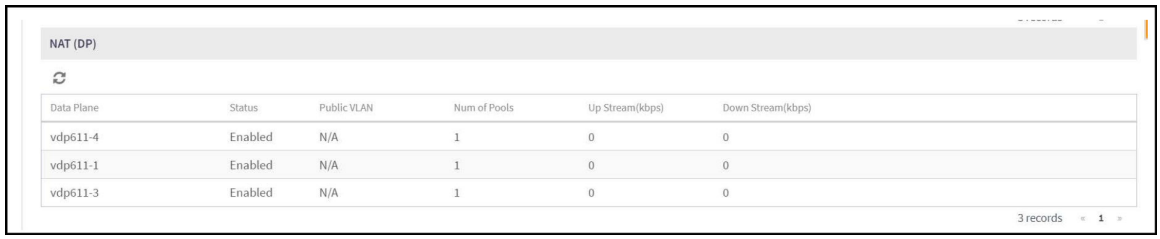


DHCP (DP)

Data Plane	Status	DISCOVER	OFFER	REQUEST	NAK	ACK	RELEASE	INFORM	DECLINE	DROP	ERROR
vdp611-4	Enabled	3	3	29	0	29	0	0	0	0	0
vdp611-3	Enabled	55	55	3798	6	3792	11	0	0	0	0

4. Select **NAT (DP)** to monitor the NAT router information of the data planes. It displays information the server packets and the number of used ports.

FIGURE 54 NAT DP



NAT (DP)

Data Plane	Status	Public VLAN	Num of Pools	Up Stream(kbps)	Down Stream(kbps)
vdp611-4	Enabled	N/A	1	0	0
vdp611-1	Enabled	N/A	1	0	0
vdp611-3	Enabled	N/A	1	0	0

3 records « 1 »

Working with DHCP

DHCP Server or NAT Router

DHCP or NAT functionality on controller managed APs and DPs (data planes) allows customers to reduce costs and complexity by removing the need for DHCP server or NAT router to provide IP addresses to clients. For data traffic aggregation and services delivery, choose the appropriate user profile for DHCP and NAT services on the Virtual SmartZone Data Plane (vSZ-D).

AP Based DHCP or 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 or 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 through 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 or NAT functions. Therefore, DHCP or NAT service will not be running on any APs (they will serve clients only), while the DHCP or 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 and out of Wi-Fi 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 address assignment and management with minimal impact on forwarding latency. The DHCP server allows IP address assignment only when a DHCP license assignment policy is created for a specific vSZ-D. A maximum of 101k IP address assignments are allowed for each vSZ-D. Additional IP address assignments require additional licensing.

NOTE
DHCP server or NAT router if enabled, is supported only for wireless client IPv4 address assignment.

Profile-based NAT

With NAT service enabled, all the Wi-FI client traffic is NAT routed by the vSZ-D before forwarding to the core network. The NAT license assignment policy for the 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 reduces the network overhead significantly since it reduces the MAC-table considerations on the UP-stream switches significantly. This feature is very useful in high density deployments.

Network Topology

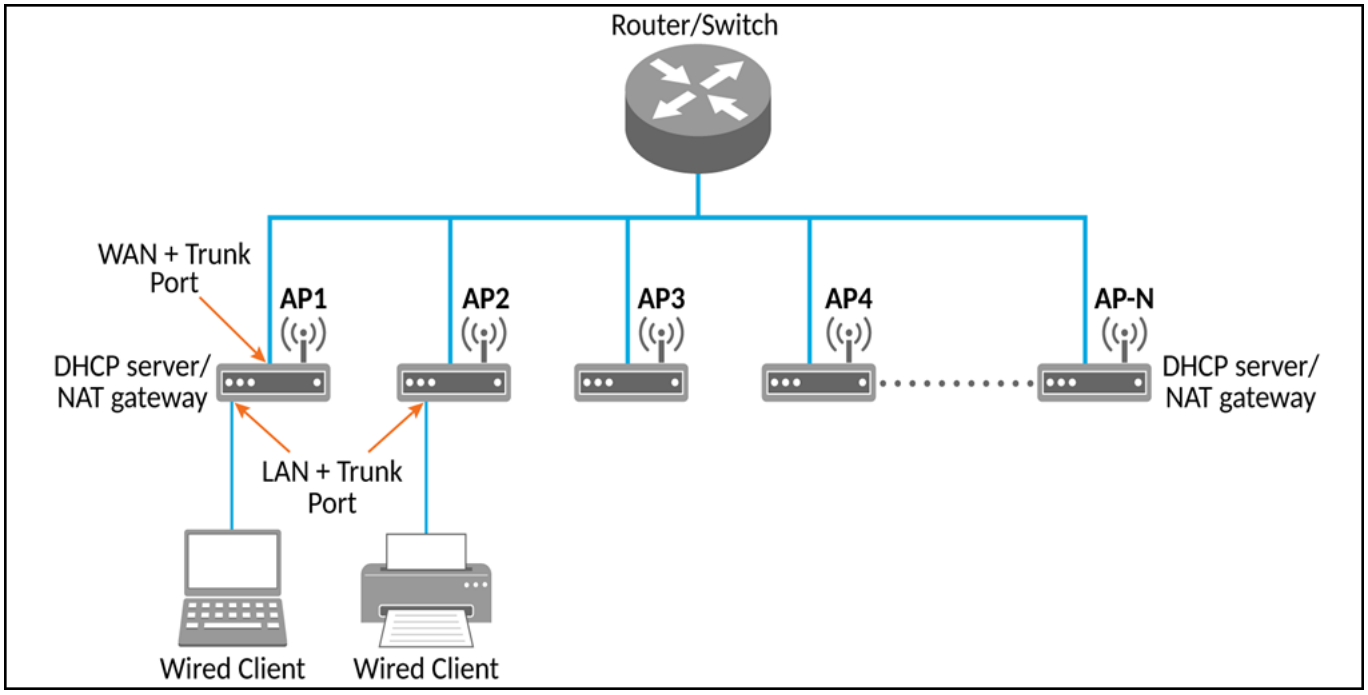
Access Points (APs) can be deployed in three types of topologies.

- Single AP Topology
- Multiple AP (Flat Network) Topology
- Hierarchical AP Topology

Single AP Topology

All the APs in the zone get their IP addresses from the WAN router and provides the DHCP or NAT service. For example,AP H510 or H320 is configured as GAP (Generation Application Protocol) as a manual port selection, then LAN1 and LAN2 configuration is pushed to Ethernet1 and Ethernet2 ports of the APs instead of Ethernet0 and Ethernet1 ports.

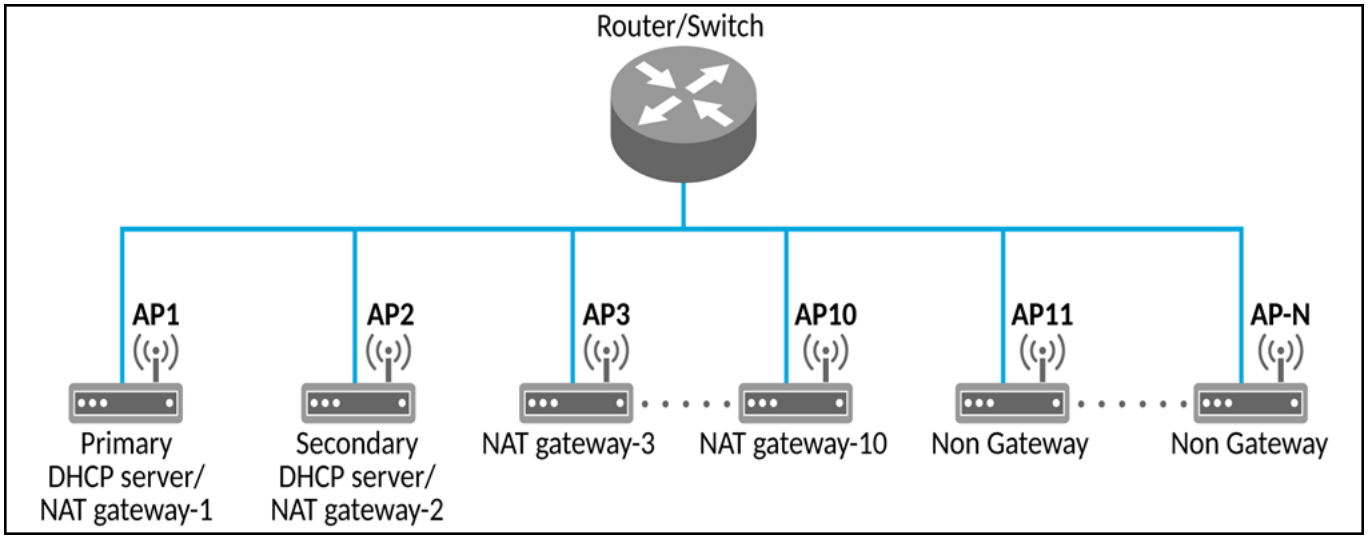
FIGURE 55 Single AP Topology



Multiple AP (Flat Network) Topology

All the APs in the zone get their IP address from the WAN router and designated APs provide the DHCP or NAT service. A maximum of two APs is selected for DHCP service (primary and secondary) and ten APs for NAT Gateway.

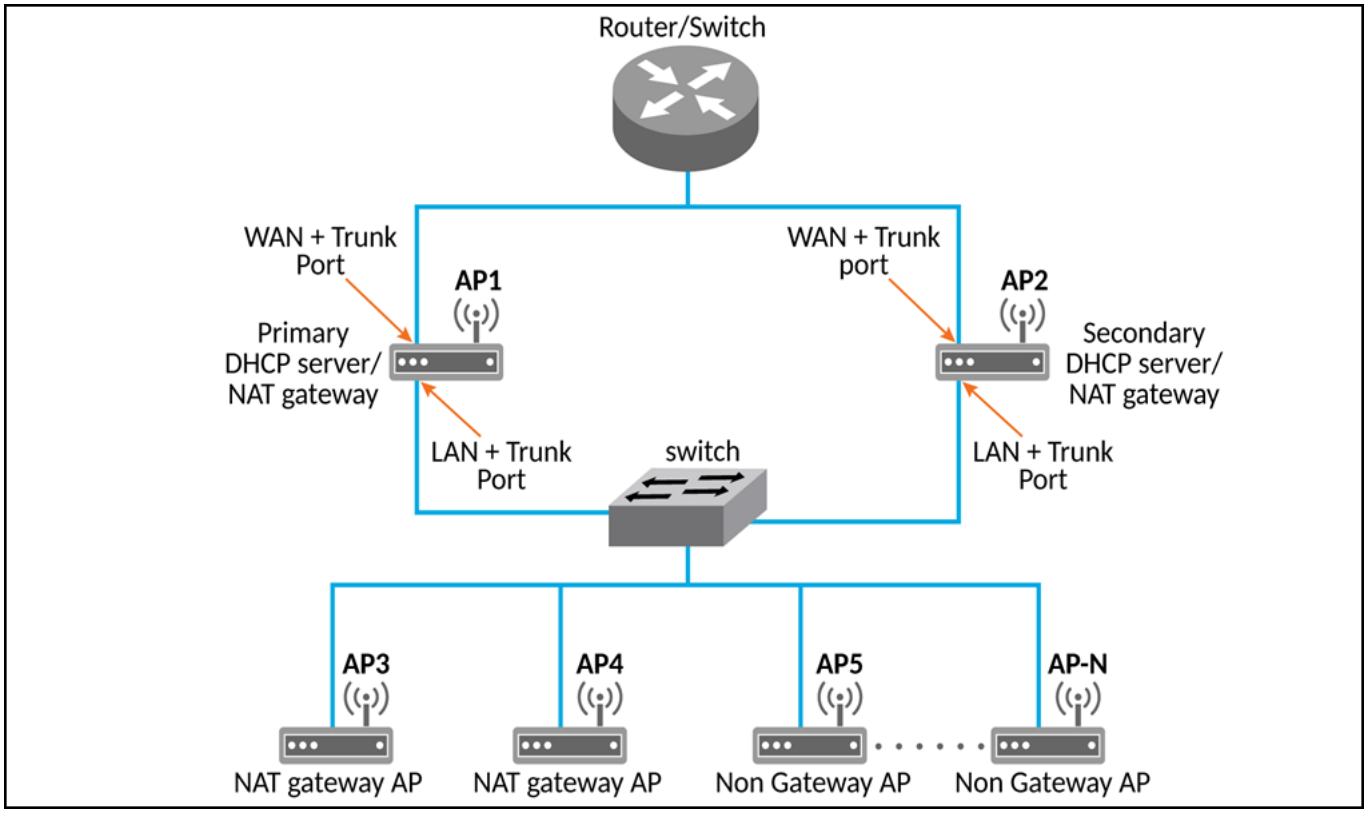
FIGURE 56 Multiple AP (Flat Network) Topology



Hierarchical AP Topology

Designated APs provide the DHCP or NAT service. Gateway APs get the IP address from the WAN router and non-gateway APs get the IP address from the Gateway APs. For example, AP H510 or H320 is configured as GAP by manual port selection, then LAN1 and LAN2 configuration is pushed of the APs to Ethernet1 and Ethernet2 ports instead of Ethernet0 and Ethernet1 ports. If Ethernet0 port needs to be configured, then LAN5 or LAN3 ports need to be configured.

FIGURE 57 Hierarchical AP Topology



Hierarchical Network Topology

Hierarchical network topology along with DHCP or NAT runs on single and multiple APs.

Gateway APs are directly connected to the service providers' router or switch to get the public IP addresses. The Non-Gateway APs (NGAP) gets the private IP addresses from the Gateway APs (GAP) through the DHCP or NAT service. Wired client such as printers and laptops are directly connected to the LAN port of the GAP or WAN ports of NGAP and are operational without the external DHCP or NAT. Basic Mesh topology is supported where GAP is the root AP and all other NGAPs are Mesh APs.

The Dynamic WAN Port Detection (DWPD) algorithm detects the WAN port among Ethernet0/Ethernet1/Ethernet2 of the APs, and marks only one port of the AP as WAN. LAN port selection is based on the availability of wired port with tunnel enabled. All other wired ports on the AP are marked as LAN.

Expected behavior of a three port APs are as follows:

- Ethernet0: Connected to WAN

  Result after DWPD: Ethernet0=WAN, Ethernet1=LAN, Ethernet2=WAN
- Ethernet1: Connected to WAN

Result after DWPD: Ethernet0=LAN, Ethernet1=WAN, ETH2=WAN

- Ethernet2: Connected to WAN

  Result after DWPD: Ethernet0=LAN, Ethernet1=WAN, Ethernet2=WAN

Using DWPD a user can plug-n-play without configuring WAN or LAN ports. Wired client connectivity for each AP is possible where all the APs in the zone run DHCP or NAT service. All Ethernet ports can be configured as LAN ports allowing wired clients to connect.

LAN port profile enables APs with multiple Ethernet ports to be configured as LAN ports and a separate switch is not required if the multi-port AP is a GAPs. All the required wired and NGAPs are connected directly to the number of available Ethernet ports.

While using DHCP NAT-HN (Network Address Translation) with DWPD, the AP ignores the Ethernet port configuration, which is pushed from the interface. The AP selects the WAN and LAN ports, dynamically and on detecting the WAN port successfully, it marks the other port as a LAN port. When it marks an Ethernet port as a LAN port, the DWPD chooses the untagged VLAN ID as one (1) by default.

NOTE
The LAN port configuration cannot be changed.

Wired client gets the IP address from DHCP Pool VLAN ID 1. To configure Ethernet port VLAN ID to 100 through the interface, manually select WAN port and apply the appropriate Ethernet port profile to Ethernet0 and Ethernet1 ports of the AP.

NOTE
If APs or clients connected to a LAN switch come before the DWPD process completes on the GAPs, the clients or NGAPs get the IP addresses from WAN VLANS (the default VLAN or non-default VLAN, which is part of WAN).

Configuring AP-based DHCP Service Settings

Using DHCP service settings, 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:

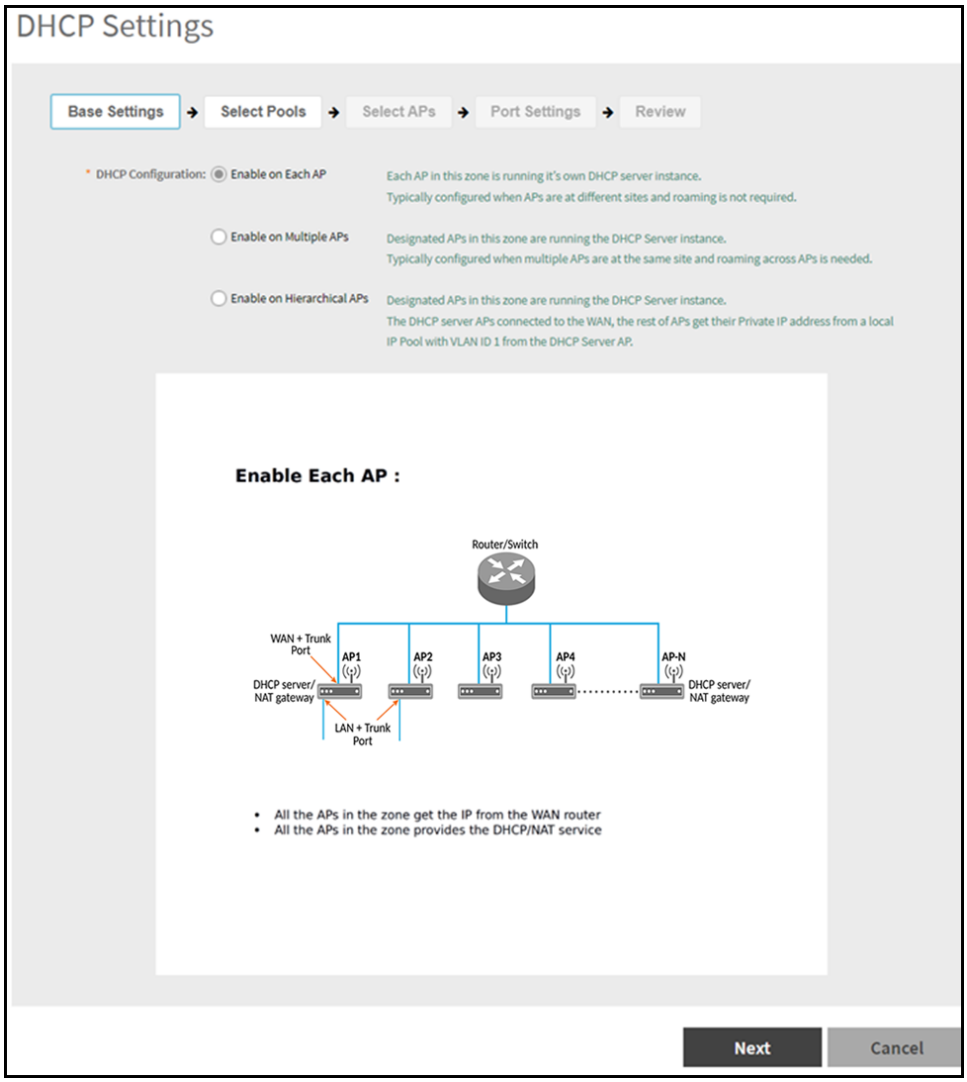
- There must be a minimum of one and a maximum of 10 APs acting as Gateway AP (GAP) based on the topology when configuring DHCP server and NAT router. There is no count on the number of APs acting as Non-Gateway APs (NGAP).
- For a single NGAP, connect Ethernet0 of NGAP to LAN port (usually Ethernet1) of GAP.
- For more than one NGAP, Layer2 switch is required to connect the LAN port of GAPs to all the NGAPs.
- For APs having more than two Ethernet ports, all the Ethernet ports except the WAN backhaul (usually Ethernet0) is configured as LAN ports. In such cases, a separate switch is not required.

To configure DHCP services:

1. From the main menu go to **Services** > **DHCP** > **DHCP Setting (AP)**.

2. Select a Zone from the zone list on the left side of the screen, and click **Enable DHCP Service**.

FIGURE 58 DHCP Settings Wizard

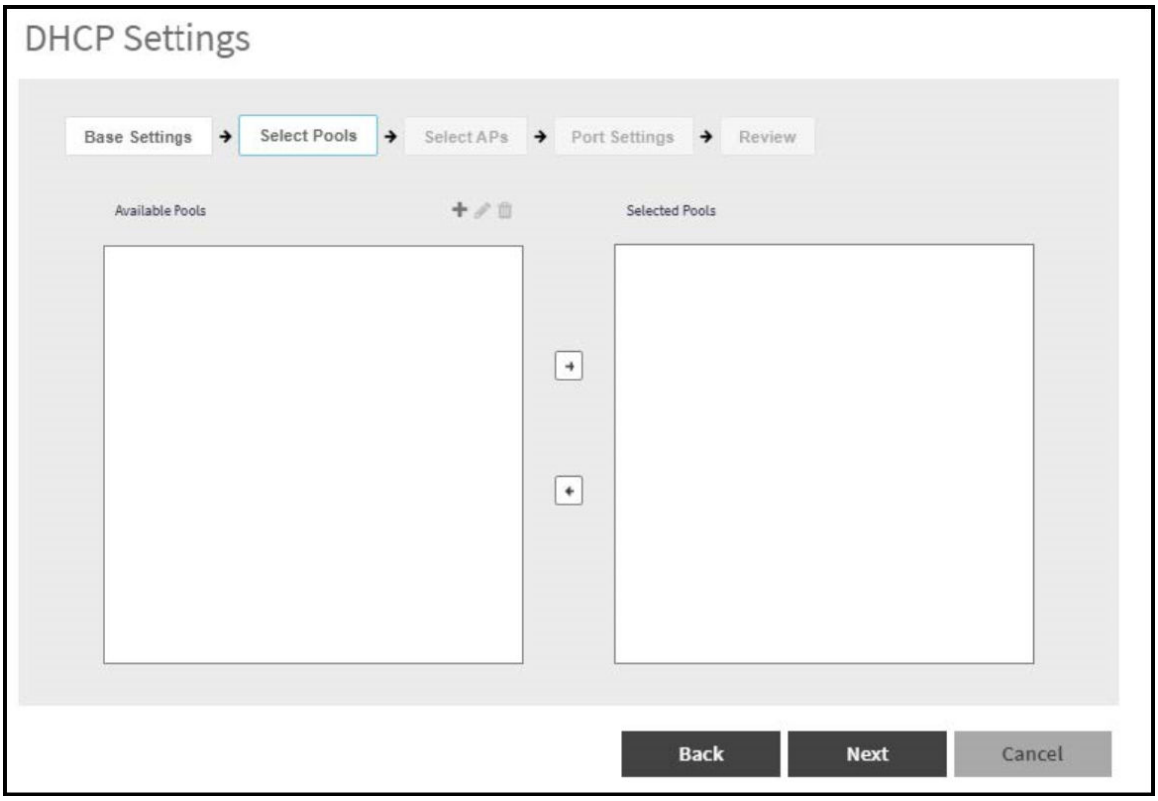


3. On the first page of the wizard (**Base Settings**), configure the **DHCP Configuration** as follows:
   - **Enable on Each AP**: Each AP in this zone gets the IP address from the WAN router and runs its own DHCP server instance. This option is typically used when APs are at different sites and roaming is not required.
   - **Enable on Multiple APs**: Designate, which APs provide DHCP or NAT service. This option is typically used when multiple APs are at the same site and roaming is required. This option also allows whether to automatically or manually specify which APs provide DHCP service.
   - **Enable on Hierarchical APs**: Designate, which APs provide DHCP or NAT service. The DHCP server connects to the WAN AP and the other APs get their private IP address from the local IP address 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 to assign client IP addresses.

NOTE
For the **Enable on Hierarchical APs** DHCP configuration, one of the pools must be VLAN ID 1.

FIGURE 59 Selecting Pools



NOTE

If DHCP pools are not created, it can be done from the wizard. Click the Plus icon and configure the IP address pool as described in the Creating an AP DHCP Pool on page 169.

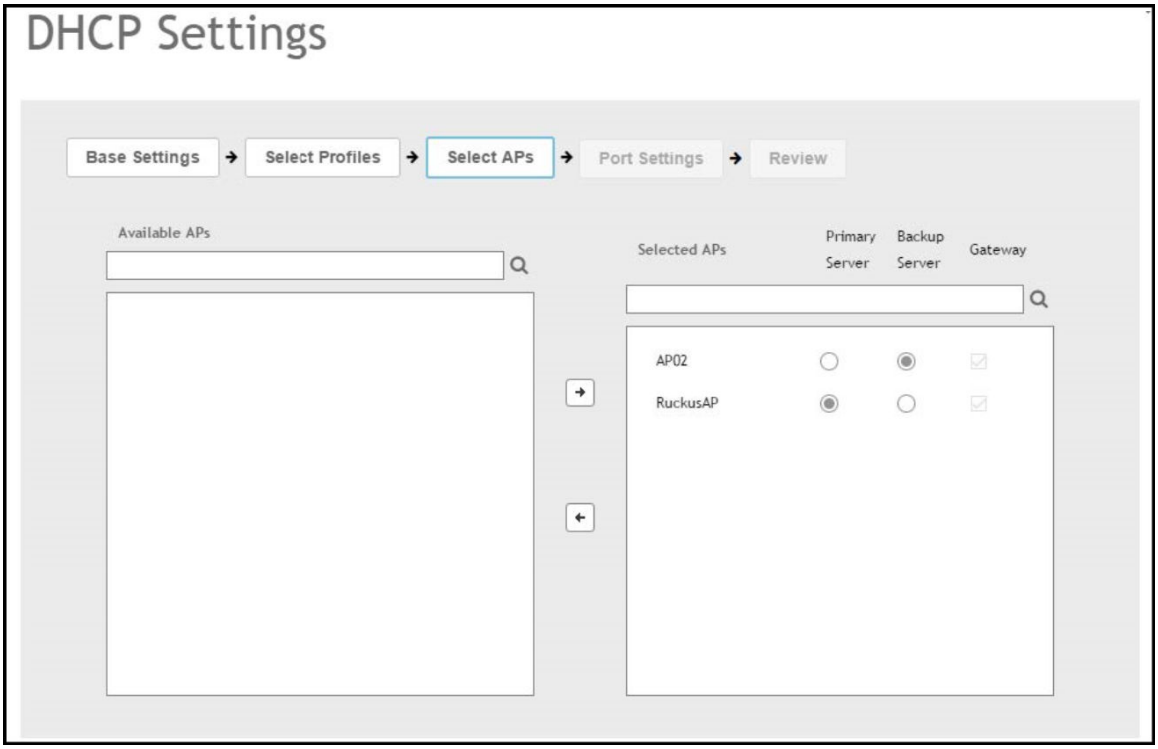
6. Click **Next**. The **Select APs** screen appears.

NOTE
If **Auto Select AP** is selected on the first wizard screen, this configuration screen is 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, select a maximum of two APs for DHCP service (primary and secondary) and a maximum of 10 APs for NAT Gateway.

FIGURE 60 Selecting APs



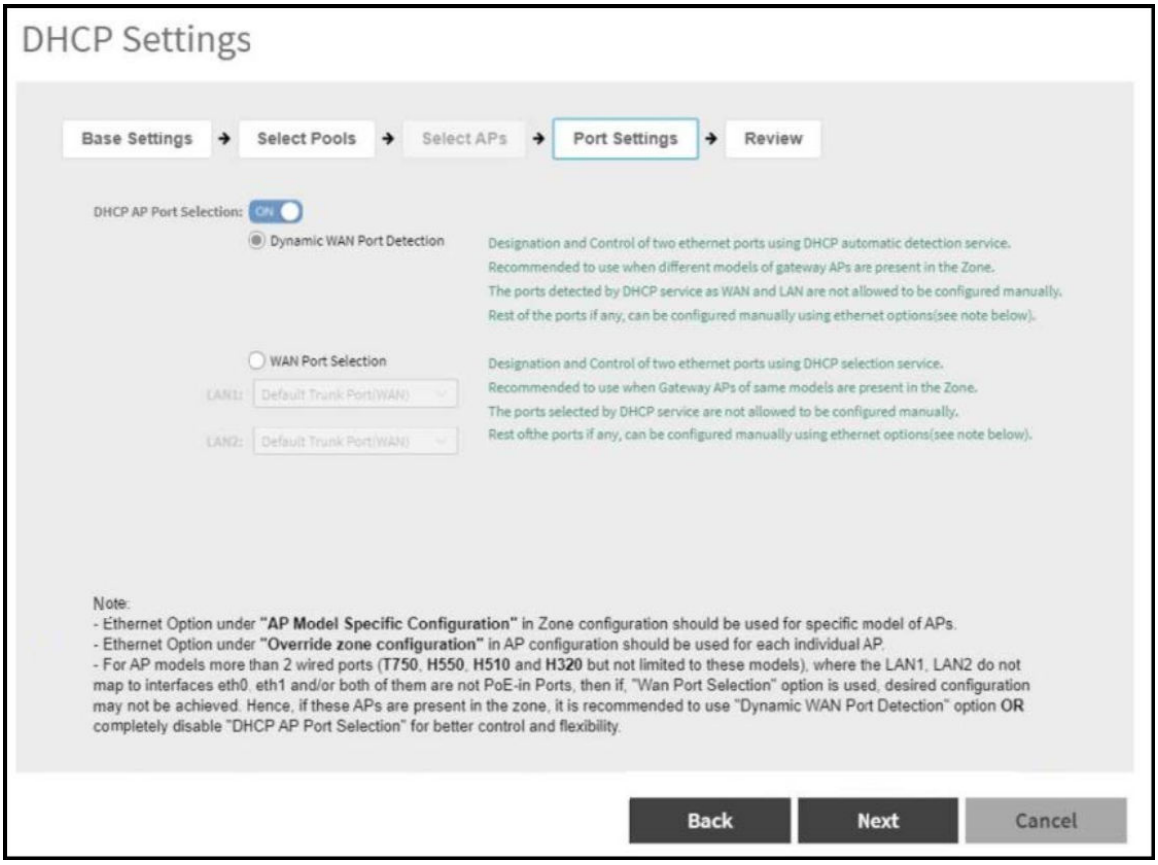
8. Click **Next**. The **Port Settings** screen is displayed.

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**
> It is recommended to use **Dynamic WAN Port Detection** option or disable **DHCP AP Port Selection** for AP models with more than two wired ports, where LAN1 and LAN2 do not map to Ethernet0 and Ethernet1 interfaces respectively, and where both are not PoE in ports.

- **Dynamic WAN Port Detection**(DWPD): By default, WAN is identified, LAN selected and the non-DWPD ports are 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 cannot be configured manually. Remaining ports, if any, can be configured as follows:
  - For specific models of APs, use the Ethernet option in **AP Model Specific Configuration**.
  - For each individual AP, use the Ethernet option in **Override zone configuration**.
- **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 GAP of the same model are present in the zone. The ports selected by the DHCP service cannot 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. Remaining ports, if any, can be configured as follows:
  - For specific models of APs, use the Ethernet option in **AP Model Specific Configuration**.
  - For each individual AP, use the Ethernet option in **Override zone configuration**.

FIGURE 61 Port Settings



10. Click **Next**.
11. On the **Review** screen, review the 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 or NAT functionality and assign IP addresses to wireless clients from the DHCP address pools 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 164.

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 is configured and accessed through Virtual SmartZone Data Plane (vSZ-D). The vSZ-D server assigns the IP address to the user equipment based on the profile rule. Different pools with the same subnet are created without overlapping the IP address range.

You must configure the following settings to create a DHCP profile.

NOTE
DHCP supports only access-side network.

- Configuring DHCP Global Settings on page 170
- Configuring DHCP Pool Settings on page 171

Configuring DHCP Global Settings

A DHCP profile can be used simultaneously by multiple segments and gateways in the network.

To configure Profile-based DHCP Global settings follow these steps:

1. In the controller virtual platform web interface go to **Services** > **DHCP & NAT** > **DHCP Profiles (DP)**.
2. Click **Create**. The **Create DHCP Profile** page is displayed.
3. Configure the following:
   - **Profile Name**: Type a name for the DHCP profile. AP supports 32 bytes.
   - **Description**: Type a description of the settings.
   - **Domain Name**: Type the domain name.
   - **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** is displayed. 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 is displayed. 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

For any *DHCP pool*, you can *configure* a primary subnet and any number of secondary subnets.

To configure DHCP pool settings follow these steps:

1. In the controller virtual platform web interface go to **Services** > **DHCP & NAT** > **DHCP Profiles (DP)**.
2. Select the DHCP profile from the list 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.
   - **Assigning Options**
     - **Subnet**: Type the IP address.
     - **Subnet Mask**: Type the network IP address.
     - **Broadcast Address**: Type the broadcast IP address.
     - **Pool Range**: Type the IP address range for the pool.
     - **Exclude Pool**: Type the IP 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 is displayed. Configure the following:
       - Choose the **Space Name** or click **Create** to add the Option 43 Space name.
       - Type a **Description**.
     - Click **OK**. You have configured **Option43 Value**.
5. Click **OK**.

   You have created DHCP pool configuration.

Creating Profile-based NAT

A NAT router profile is configured and accessed through Virtual SmartZone Data Plane (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 172
- Configuring NAT Pool Setting on page 172

Configuring NAT Global Settings

Network Address Translation (NAT) is a process in which one or more local IP address is translated into one or more Global IP address and vice versa in order to provide Internet access to the local hosts.

To create a NAT global setting follow these steps:

1. In the controller virtual platform web interface go to **Services** > **DHCP & NAT** > **NAT Profiles (DP)**.
2. Click **Create**. The **Create NAT Profile** page is displayed.
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 follow these steps.

1. In the controller virtual platform web interface 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 is displayed.

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 one of the following:
       - Update the VLAN range.
       - Update the QinQ VLAN range.
       - Leave both the fields blank for RADIUS NAT server setup.
     - **Private VLAN Range**: Type the VLAN range and click **Add**. Range: 1 through 4095. For example: 1 or 1-2.
   - **Translation Options**
     - **Port Range**: Type the port range. Range: 10000 through 65534. For example: 10000-20000.
     - **Public Address Range**: Type the public IP address range.

       NOTE
       This public address must not be a duplicate of the other public addresses 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 Server or NAT Router with Mesh Options

DHCP or NAT functionality on controller managed APs and DPs (data planes) allows customers to reduce costs and complexity by removing the need for DHCP server or NAT router to provide IP addresses to clients.

To configure DHCP or NAT with mesh option follow these steps.

1. To configure DHCP or NAT with mesh enable the Mesh option at the Zone level.
2. From the Access Points page, select the AP to be assigned as the root AP.
3. Click **Configure**.
4. Select the Mesh specific options and the root AP mode.
5. Create multiple address pools and assign it to the APs, which are on DHCP services. Refer to Creating an AP DHCP Pool on page 169.
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 164.

Domain Name System (DNS)

Creating a DNS Server Profile

A DNS server profile allows you to specify the primary and secondary address of the DNS server for devices to identify the host name within the specified zone.

To create a DNS Server Profile, perform the following:

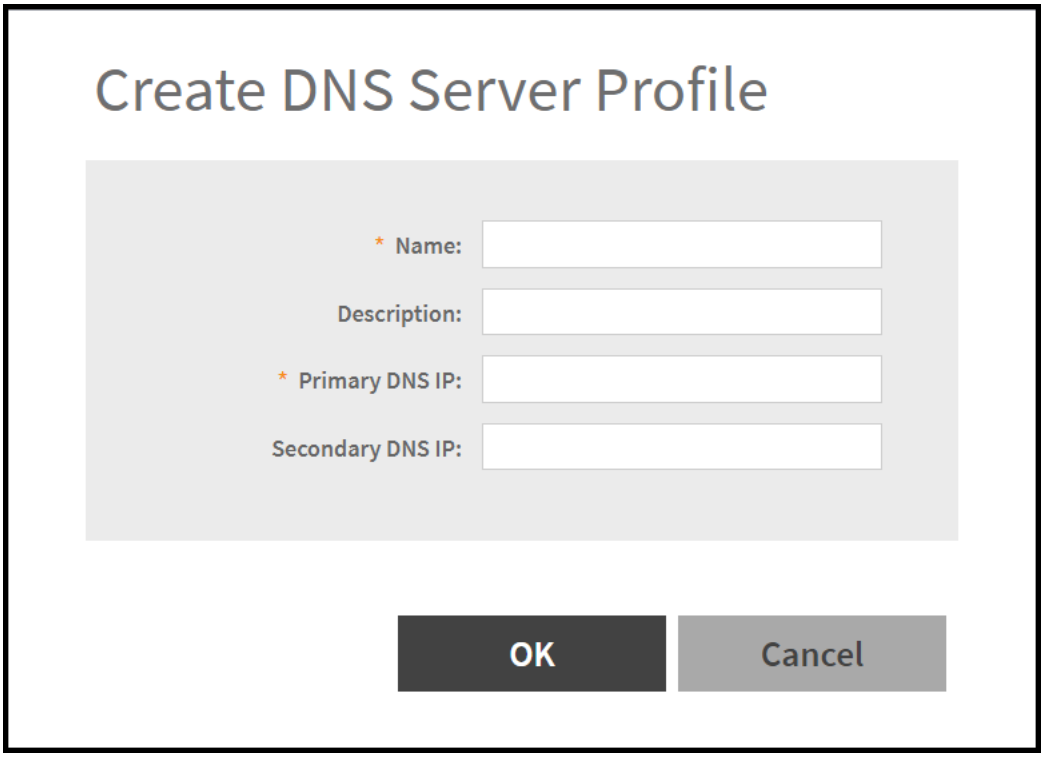
1. Click **Administration** > **System** > **DNS Servers**.

   This displays the **DNS Servers** page.

2. Click **Create**.

   This displays the **Create DNS Server Profile** page.

   FIGURE 62 Create DNS Server Profile



3. Enter the following:
   a. Name: Type a name to identify the DNS server profile.
   b. Description: Enter a short description for profile.
   c. Primary DNS IP: Enter the primary DNS IP address.

      NOTE
      This feature supports IPv4 address format.

   d. Secondary DNS IP: Enter the secondary DNS IP address.

      NOTE
      This feature supports IPv4 address format.

   e. Click **OK**.

You have created a DNS Server Profile.

NOTE
You can also edit, clone and delete the profile by selecting the options **Configure**, **Clone** and **Delete** from the **DNS Servers** page.

Creating a DNS Spoofing Profile

A DNS spoofing profile allows you to specify individual Fully Qualified Domain Name (FQDN) entries to bypass DNS resolution and provide clients with the result specified in the associated rules.

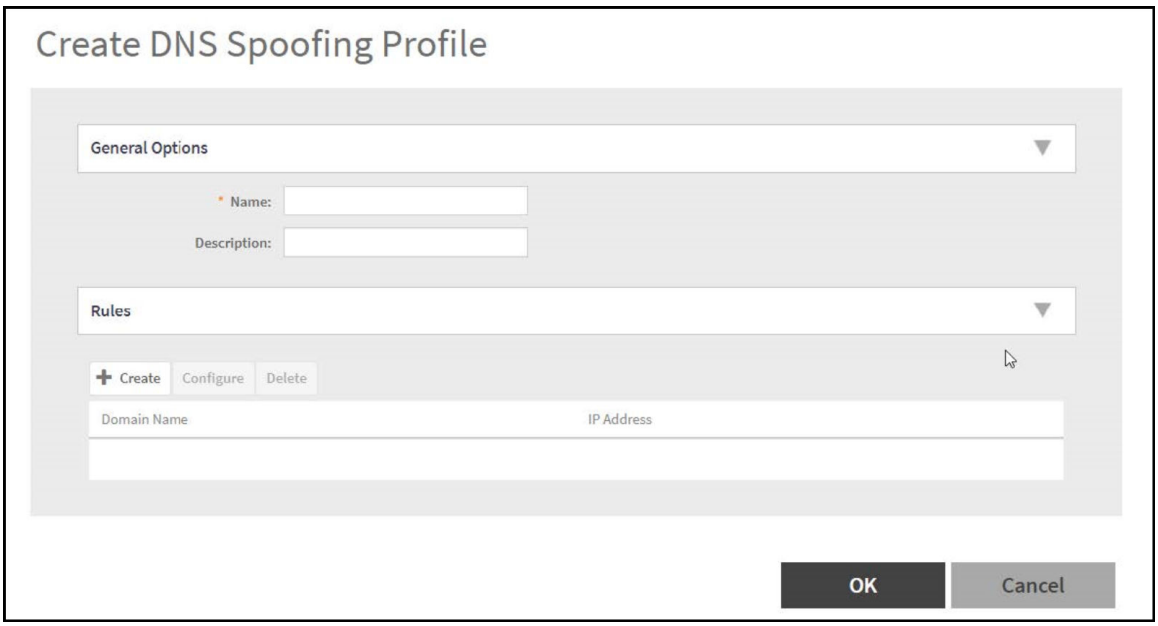
To create a DNS Spoofing Profile, Perform the following:

1. Click **Services** > **Others** > **DNS Spoofing**

2. Select a zone to create a DNS spoofing profile and click **Create**.

   This displays **Create DNS Spoofing Profile** page.

   FIGURE 63 Create DNS Spoofing Profile



3. Configure the following:
   a) **General Options**
      1. Name: Enter a name to identify the DNS spoofing profile.
      2. Description: Enter a short description for the profile.
   b) **Rules**
      1. Click **Create**, and the **Create Rules** dialog box is displayed.
      2. Domain Name : Enter the FQDN of an individual host entry.
      3. **IP List**: *IP Address*: Enter the and IP Address to resolve the domain name and click **Add**. If the user sends rule 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.
      4. e
   c) 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** from the **DNS Spoofing** page.

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:

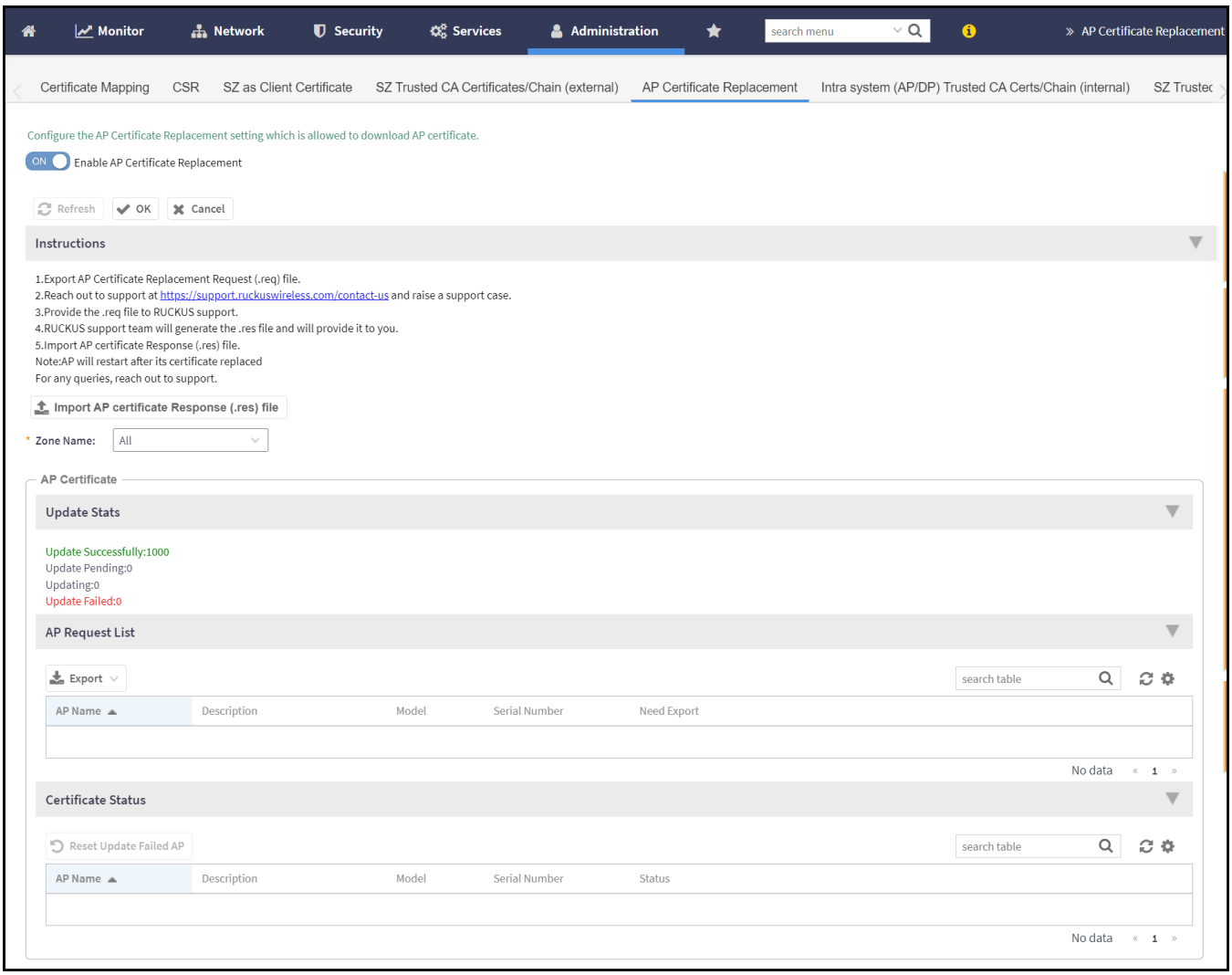
- All APs with expired certificates need to be replaced with a new valid certificate.
- Manually enable certificate check using `ap-cert-expired-check` CLI command in the configuration mode.

You must get AP certificate replacement before your AP certificate expires. The system generates an *apCertificateExpireSystem* alarm and event when an AP certificate expires.

For AP Certificate replacement, perform the following:

1. Click **Administration** > **System** > **Certificates** > **AP Certificate Replacement**. This displays the **AP Certificate Replacement** page.

FIGURE 64 AP Certificate Replacement



2. By default, the Enable AP Certificate Replacement is disabled. Click the **Enable AP Certificate Replacement** button to enable the AP certificate replacement and follow the instructions on the screen.
3. From the AP Certificate Replacement page of the application, click **Import AP certificate Response (.res) file**. The Import AP certificate for replacement form appears.
4. Click **Browse** and select the file.
5. Click **OK**.

   NOTE
   All APs included in the imported response (.res) file reboot after their certificate is refreshed.

6. Select the **Zone Name** from the drop-down list.

AP Certificate

In the **AP Certificate** section, the following details are displayed.

- **Update Stats**: Displays the status of the AP certificate.
- **AP Request List**: Displays the list of requested APs.
- **Certificate Status**: Displays the certificate status.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.

  After 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

AP Restricted Access

The Restricted Access profile can be created without having any blocked ports or enabling well known and additional entries in the whitelist ports. The 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. The 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 inherent security of the AP.

NOTE
A maximum of five *Restricted Access* profiles can be created per zone.

The AP currently has the following categories of open ports:

TABLE 35 Well known ports on Access Points

Sl. No.	Port	Use	Protocol
1	80	HTTP	TCP - IPv4 & IPv6
2	22	SSH	TCP - IPv4 & IPv6

TABLE 35 Well known ports on Access Points (continued)

Sl. No.	Port	Use	Protocol
3	443	HTTPS	TCP - IPv4 & IPv6
4	161	SNMP	UDP - IPv4 & IPv6
5	23	TELNET	TCP - IPv4 & IPv6

NOTE
Refer to *RUCKUS SmartZone Access and Securiy Services Guide* for comprehensive information on configuring *AP Restricted Access*.

AP CLI Scripts

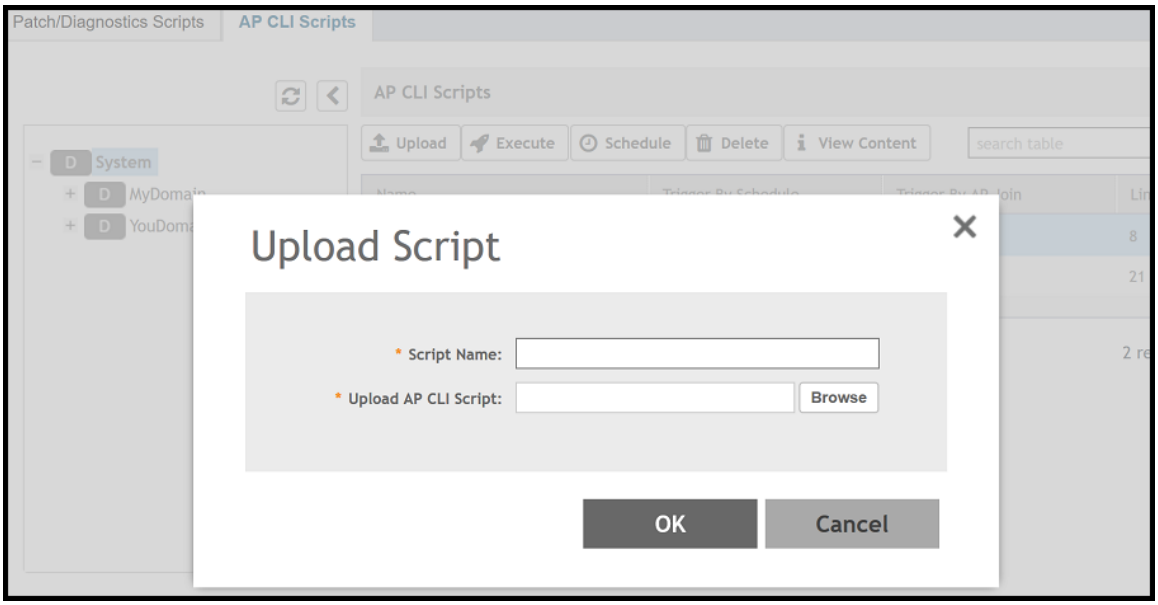
Uploading AP CLI Scripts

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

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, select the AP zone to apply the script.
5. Click **Upload**.

   The **Upload Script** dialog box is displayed.

   FIGURE 65 Uploading Scripts



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

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. 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, select the domain in which the AP is present.
5. From the **AP CLI Scripts** tab, select the script from the list of scripts.
6. Click **Execute**.

   The **Execute Script** dialog box is displayed.

   FIGURE 66 Executing a Script

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

The controller runs the selected script on the specified zone.

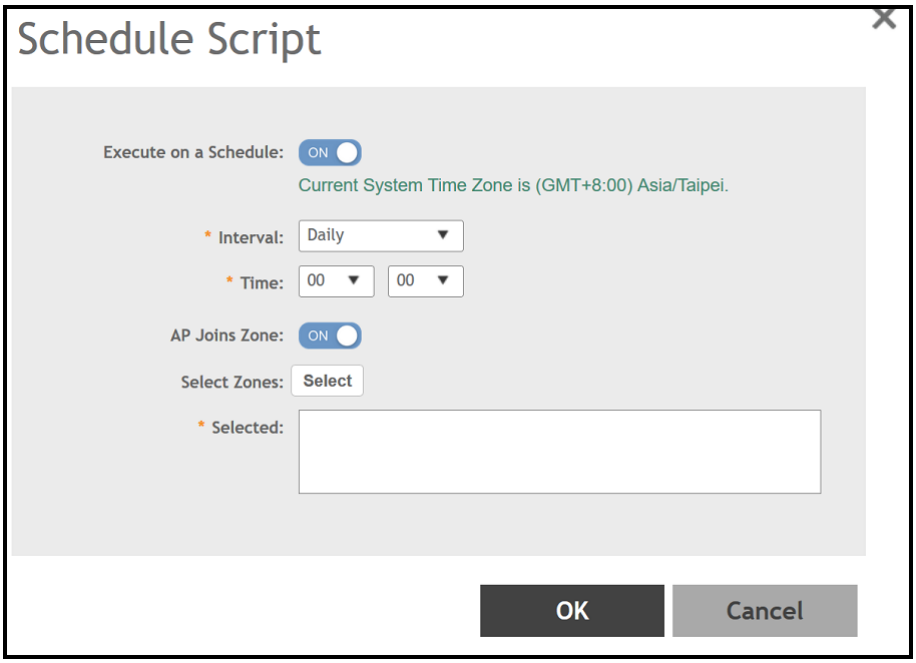
Scheduling AP CLI Scripts

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. 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.
6. Click **Schedule**.

   The **Schedule Script** dialog box is displayed.

   FIGURE 67 Scheduling a Script



7. Configure the following options:
   - **Execute on a Schedule**: Enable this option to execute the script based on the current system time.
   - **Interval**: Schedule the script execution in multiple events. Options are Daily, Weekly and Monthly.
   - **Time**: Select the time from the drop-down menu to execute the script.
   - **AP Joins Zone**: By default this option is disabled. Enable this option to make sure the script runs on the AP when it joins a particular zone.
8. To select the zone, click **Select**.

   This displays the **Select Zone** page . Identify and select the zone. The selected zone is populated in the **Selected** area.
9. 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.

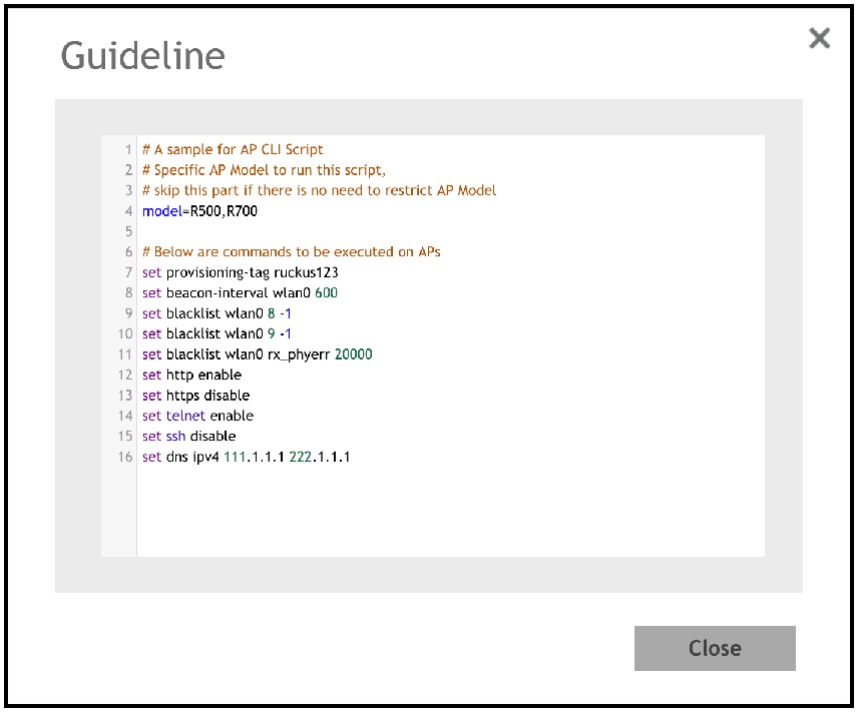
1. From the main menu, click **Monitor**.
2. Under **Troubleshooting & Diagnostics**, hover over the **Scripts**, and click **Patch/Diagnostic Scripts**.
3. Select the **AP CLI Scripts** tab.
4. From the domain tree, choose the domain in which the AP is present.
5. From the **AP CLI Scripts** tab, select 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 68 Viewing Script Details



7. Click **Close**.

Viewing the Script Execution Summary

After an AP CLI script is executed on-demand or as scheduled, you can view the details in the **History** tab.

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.

   The **History** tab displays the list of scripts that were executed.

5. From the **AP CLI Scripts** tab, select the script from the list of scripts.
6. Select a script from the **History** tab, and click **View Execution Summary**.

   The **Script Execution Summary** displays the script name, the number of successful, failed, and skipped APs, the start and end times of the execution process, the MAC address of the AP, the AP and zone names, the execution status, and the last execution line.

   FIGURE 69 Script Execution Summary

7. Click **Close**.

AP Status

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:

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

NOTE
APs that exceed their health threshold and that require your attention are flagged. Refer to the Understanding Cluster and AP Health Icons on page 193 section for more information.

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 36 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

Tagging Critical APs

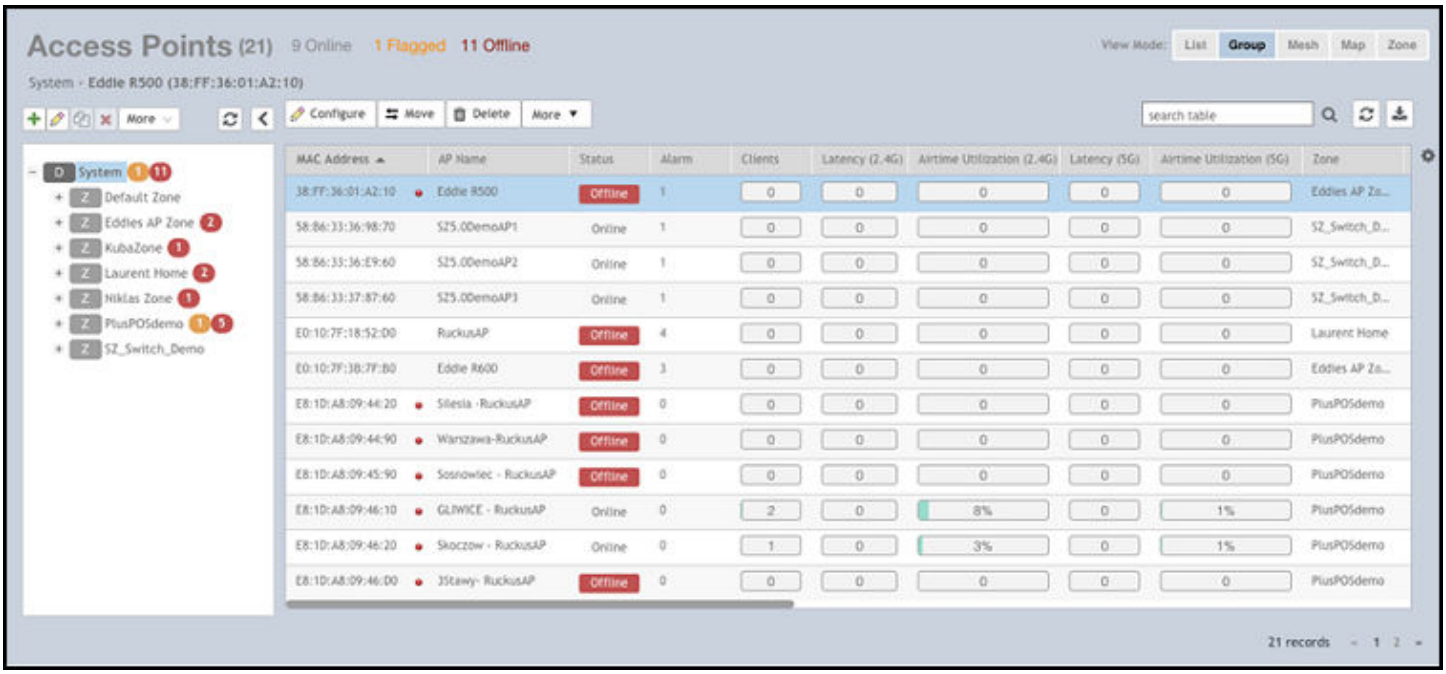
A critical AP is an AP that exceeds the daily traffic threshold (sum of uplink and downlink) data bytes configured on the controller web interface.

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 70 APs Tagged as Critical



Monitoring the Network

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

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

TABLE 37 System, Domain, Zone, and AP Groups Monitoring Tabs for SZ300 and vSZ-H platforms

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

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

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

TABLE 38 System, Zone, and AP Groups Monitoring Tabs for SZ100 and vSZ-E platforms

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

TABLE 38 System, Zone, and AP Groups Monitoring Tabs for SZ100 and vSZ-E platforms (continued)

Tabs	Description	System	Zone	AP Groups
WLANs	Displays WLAN information.	Yes	Yes	NA
Services	Displays information on the list of services.	Yes	Yes	NA
Troubleshooting	Displays client connection and spectrum analysis	Yes	Yes	Yes
Administrators	Displays administrator account information.	Yes	NA	NA

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

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

Viewing Managed APs

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.

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.

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

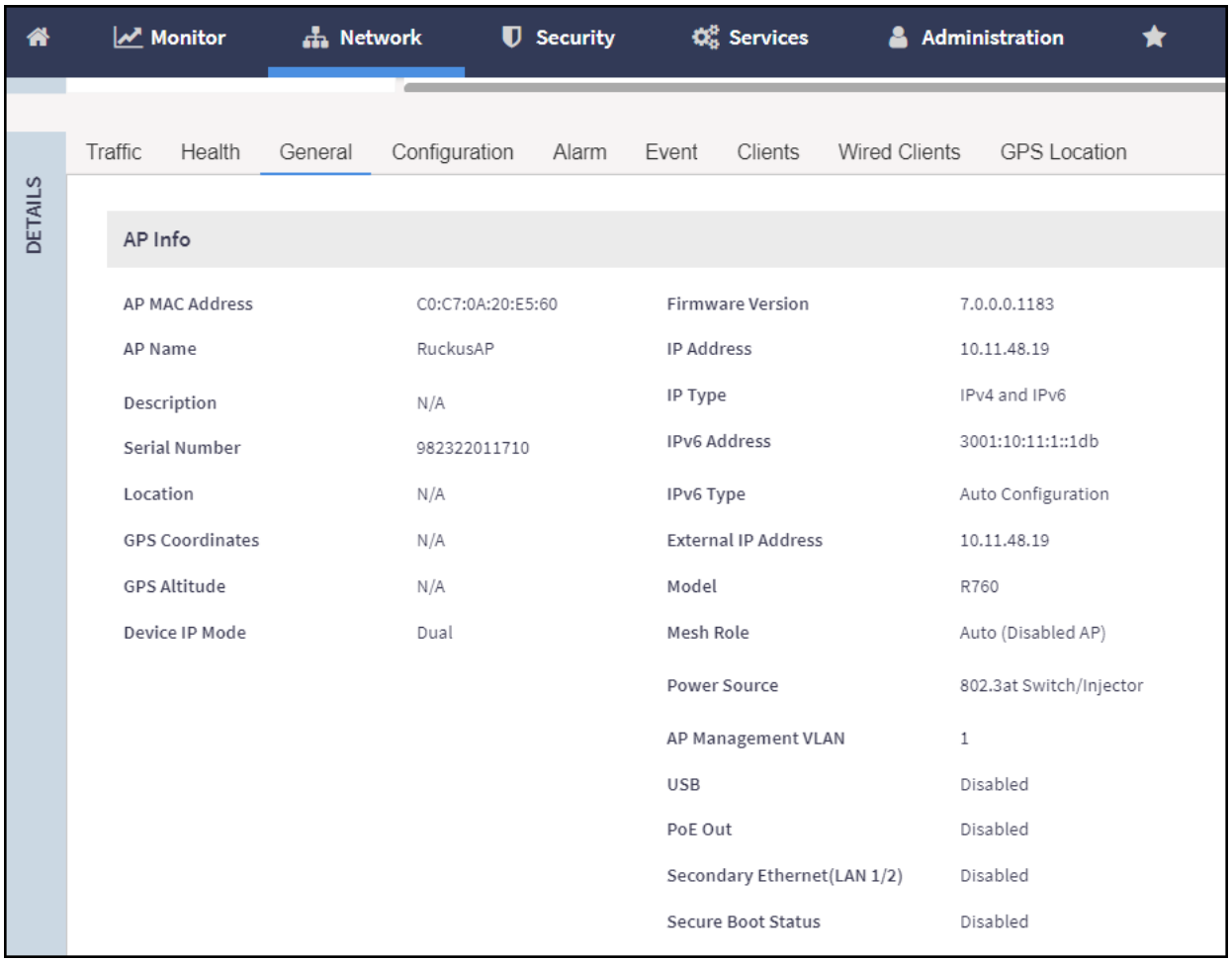
- **Select ALL** - Selects all the APs in the list.
- **Deselect All**- Clears all selection from the list.
- **Troubleshooting > Client Connection** - Connects to client devices and analyze network connection issues in real-time. See, *Troubleshooting Client Connections*.
- **Troubleshooting > Spectrum 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*.
- **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 107
- **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 107
- **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 107
- **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 107
- **Download Support Log** - Downloads support log.
- **Trigger AP Binary Log** - Triggers binary log for the selected AP.
- **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 137.
- **Swap** - Swaps current AP to swap-in AP. See, Editing Swap Configuration on page 137
- **Switch Over Clusters** - Moves APs between clusters. See Configuring AP Switchover on page 114.
- **Approve** - Approves AP and completes registering. See, Working with AP Registration Rules on page 110.

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.

FIGURE 71 General AP Information



NOTE
For 6.1.1 and later releases, the **Onboard IoT Radio** status is removed.

Viewing AP Health Indicators

You can monitor the AP performance and connection failures at the domain, zone, AP group, or specific AP level from the **Health** tab on the **Access Points** page. For all health metrics, the maximum, average, and minimum values are displayed for the AP group, followed by the specific value for each of the top APs. You can customize the number of individual APs displayed for the selected domain, zone, and AP group.

AP health indicators are divided into two categories: **Performance** and **Connection Failure**.

Performance

- Latency - It is the measurement of average delay required to 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 measurement of potential data throughput based on recent airtime efficiency and the performance potential of the AP and its currently connected clients.

Connection Failure

- Total - It is a measurement of unsuccessful connectivity attempts by clients.
- Authentication - It is 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 measurement of client connection attempts that failed during an Extensible Authentication Protocol (EAP) exchange.
- RADIUS - It is a measurement of RADIUS exchange failures due to AAA client/server communication issues or errors
- DHCP - It is a measurement of failed IP address assignment to client devices.
- User Authentication - It is a measurement of post authentication attempts that failed at the application layer such as Web Authentication, Guest Access, and Hotspot (WISPr) login.

You can customize the information displayed in the **Performance** and **Connection Failure** section:

1. From the **Access Points** page, select the required domain, zone, AP group, or AP.
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 top number of APs for which you want to see all three Performance metrics (default is 10). When you select a domain or zone from the network heirarchy, the **Show top** field filters the display to only the top number of APs that you specified in that domain or zone.
   - **Display Channel Change**: Select the required options. For example: **2.4G**, **5G**, and **6G/5G**.

     This option is available only when a single AP is selected.
   - **AP**: Choose the unique identifier displayed for each AP. For example: **Name**, **MAC**, **IP**.
4. Click **OK**.

   You can also customize the Performance metrics display using the following:
   - **Historical Health** versus **Real Time Health** view drop-down list (this option is available only when a single AP is selected; when a domain or zone is selected, the only view available is Historical Health).
   - The **Last 1 hour** versus **Last 24 hours** drop-down list (The vSZE and SZ100 web interfaces additionally have **Last 7 days** and **Last 14 days** options).
   - The radio band drop-down list.

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

5. On the **Connection Failure** bar, select the Setting icon. The **Settings - Connection Failure** pop-up appears. Customize the following:
   - **Show top**: Enter the top number of APs for which you want to see all three Performance metrics (default is 10). When you select a domain or zone from the network heirarchy, the **Show top** field filters the display to only the top number of APs that you specified in that domain or zone.
   - **AP**: Choose the unique identifier displayed for each AP. For example: **Name**, **MAC**, **IP**.

   You can also customize the Connection Failure metrics display using the following:
   - The **Access Points** versus **Failure Types** drop-down list.
   - The **Last 1 hour** versus **Last 24 hours** drop-down list (The vSZE and SZ100 web interfaces additionally have **Last 7 days** and **Last 14 days** options).
   - The radio band drop-down list.

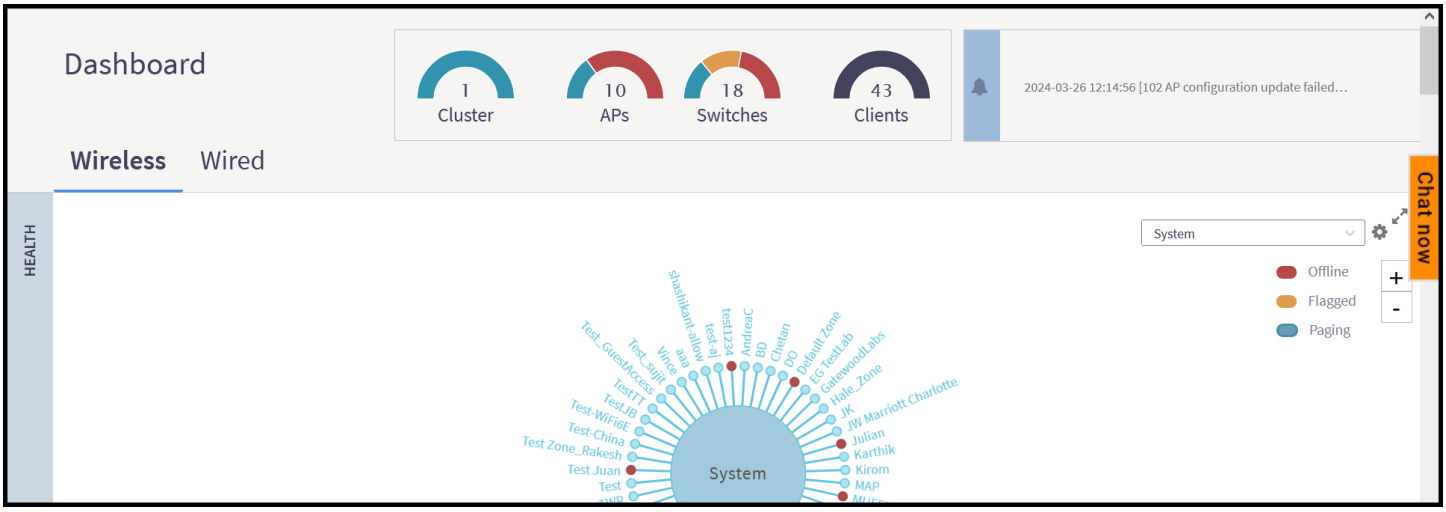
   Connection Failure details of the AP are listed according to the settings.

Health

Health

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

FIGURE 72 Dashboard Main Panel

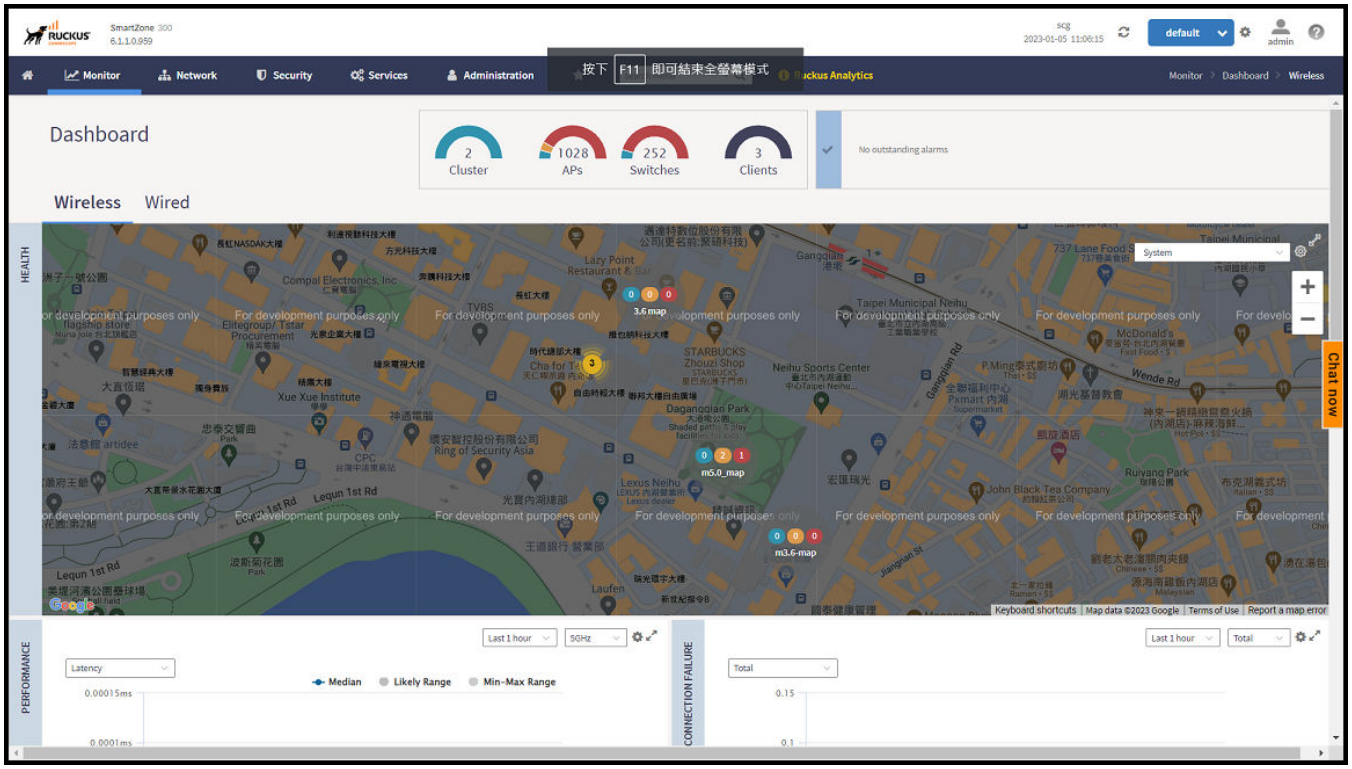


p

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

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

FIGURE 73 Health Workspace Area



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

Understanding Cluster and AP Health Icons

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

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

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

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

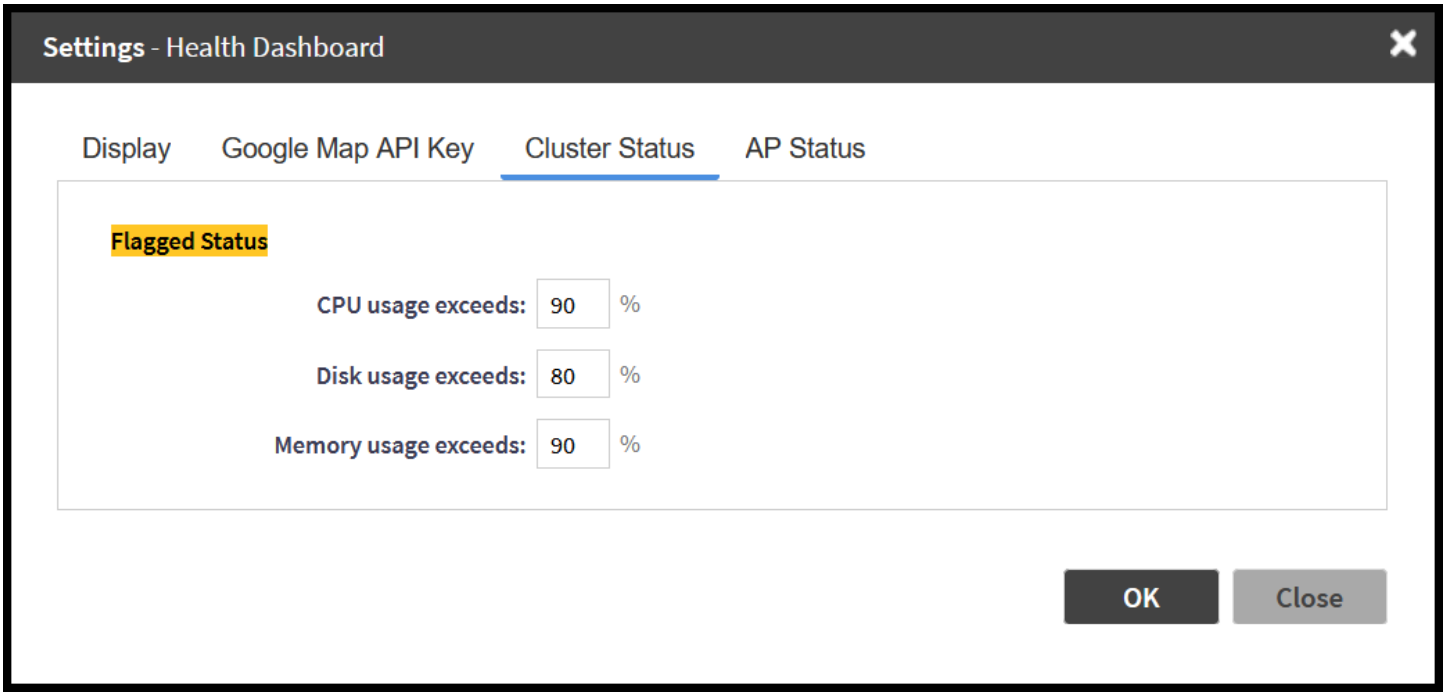
Customizing Health Status Thresholds

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

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

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

FIGURE 74 Setting Cluster Health Status Thresholds



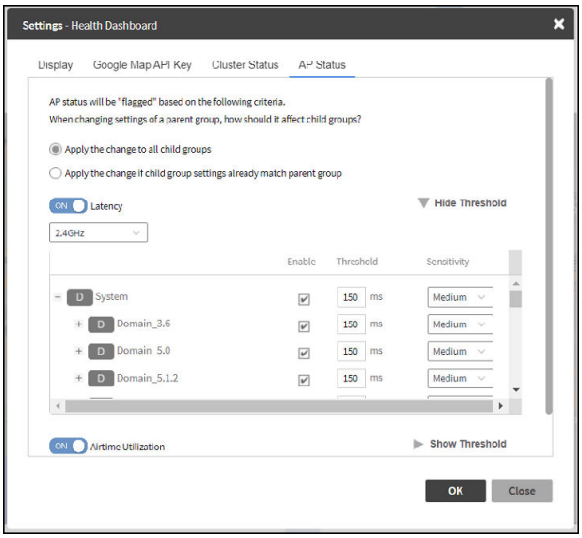
Customizing AP Flagged Status Thresholds

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

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

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

FIGURE 75 Configuring AP Flagged Status Thresholds



Using the Health Dashboard Map

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

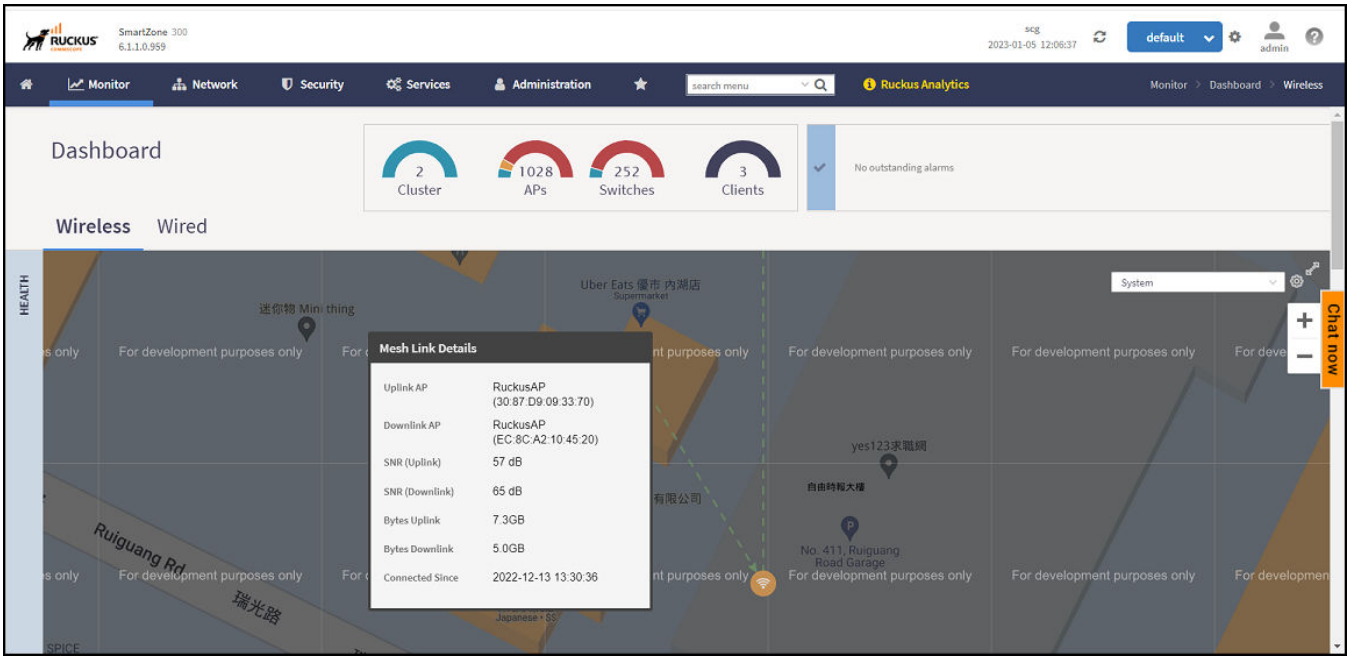
For SZ100 and vSZ-E platforms, use the **AP Status** pull-down menu to configure which AP health parameters will be displayed on the AP icons on the map. Use the Display menu to display the client count or radio channel in use.

Use the **Settings** icon to configure the information displayed in tooltips when hovering over an AP on the map. You can also change the view mode altogether, from map view to Groups, Control Planes or Data Planes view mode using the settings menu. Additionally, you can also select the 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.

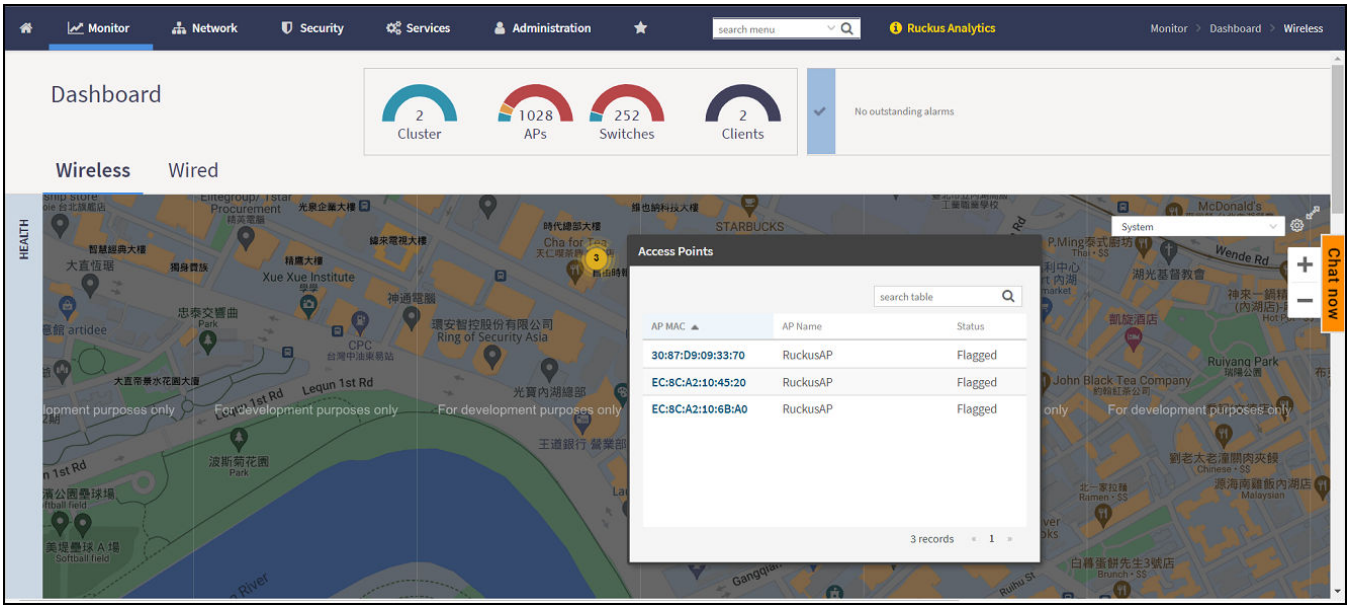
FIGURE 76 Mesh Link Details



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:

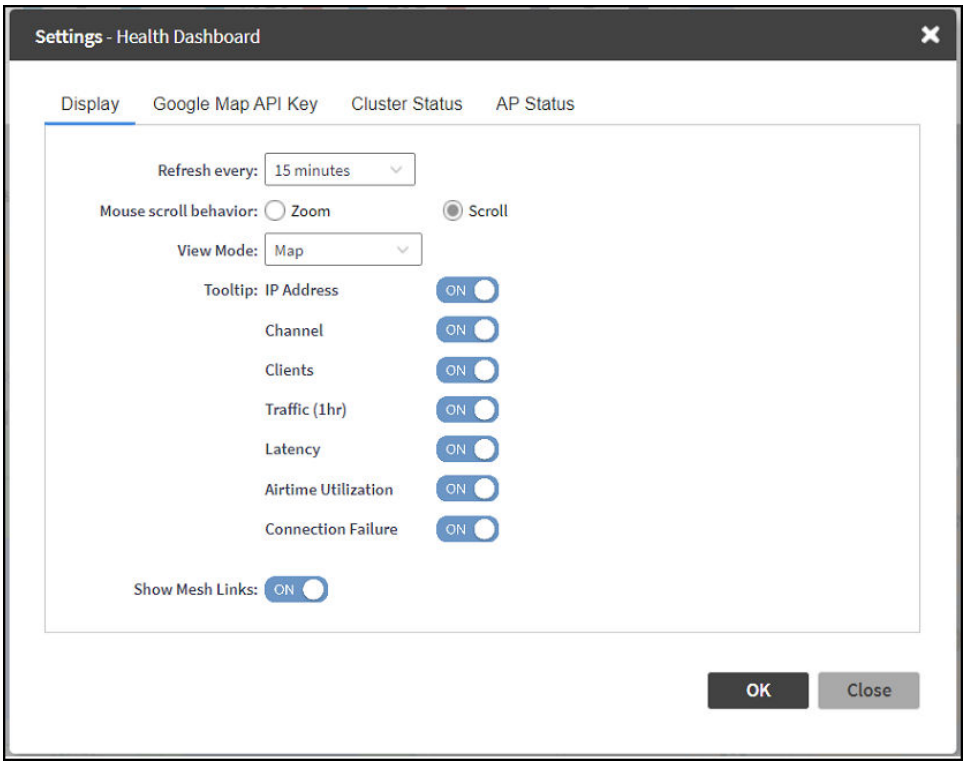
- AP MAC: Displays the MAC address of the AP
- AP Name: Displays the name assigned to the access point
- Status: Displays the status of the AP such as Online or Offline

FIGURE 77 AP Details



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

FIGURE 78 Configuring Map Settings



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

Configuring the Google Map API Key Behavior

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

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. Following are the statistics that are evaluated:

TABLE 39 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

TABLE 39 Airtime Utilization Statistics (continued)

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

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:

- **SZ300 and vSZ-H platforms**: Duration: 1 hour and 24 hours
- **SZ100 and vSZ-E platforms**: Duration: 1 hour, 24 hours, 7 days, and 14 days
- 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.

AP Traffic Indicators

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.

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.

Customizing Traffic Analysis

You can customize the traffic analysis page to display specific traffic information.

> **NOTE**
> This feature is applicable only for SZ100 and vSZ-E platforms.

1. From **Monitor**>**Dashboard** > **Traffic Analysis**, click the settings button. The Settings - Traffic Analysis form appears.
2. In the **Refresh every** drop-down, select the refresh interval.
3. Select the required check boxes from the following options:
   - **Traffic Trend**
   - **Client Trend**
   - **Access Points**
   - **WLANs**
   - **Clients**
4. Click **OK**. You have customized the traffic analysis page.

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).

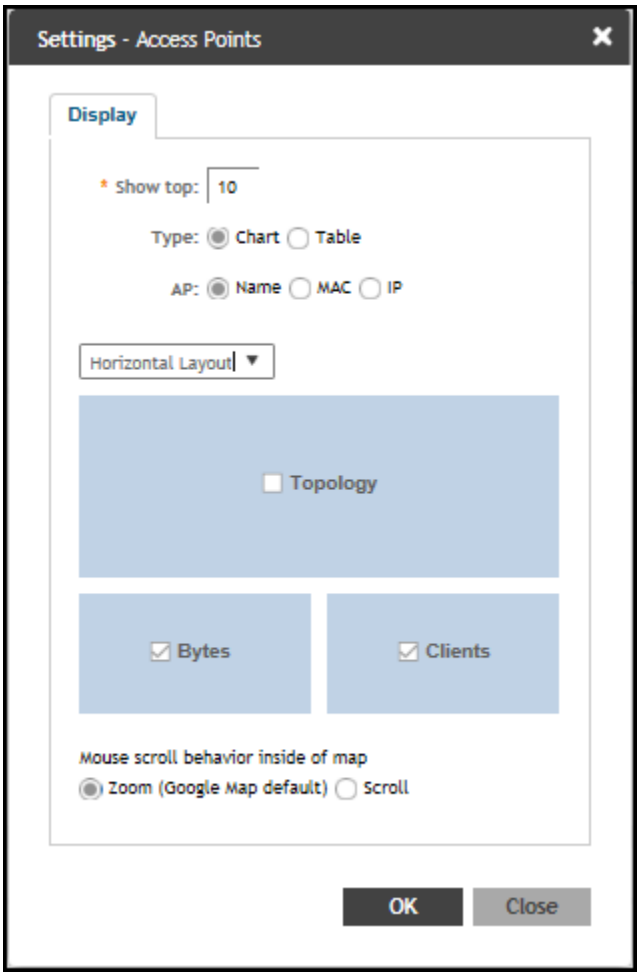
You can view historical and real-time data of the AP. Throughput and the number of clients connected to the AP are displayed in a bar chart. You can view the count of AP model details supported on the system in a pie chart. You must configure the AP settings to view its traffic analysis.

To configure the AP settings:

1. From the Access Points area, click settings .

   The AP setting form displays.

   FIGURE 79 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 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 setting . The Settings - Clients form displays.
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

The controller 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, the controller 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

The controller 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

Neighbor APs

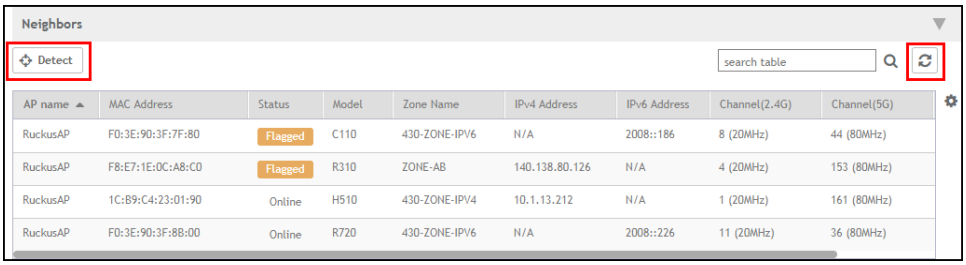
Viewing Neighbor APs in a Non-Mesh Zone

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 80 Neighbor APs for a Non-Mesh Zone



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

Reports

Rogue Devices

Viewing Rogue Devices

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

If the user has enabled rogue AP detection, a zone is configured for monitoring (refer to Configuring Monitoring APs), click **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 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

The administrator 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.

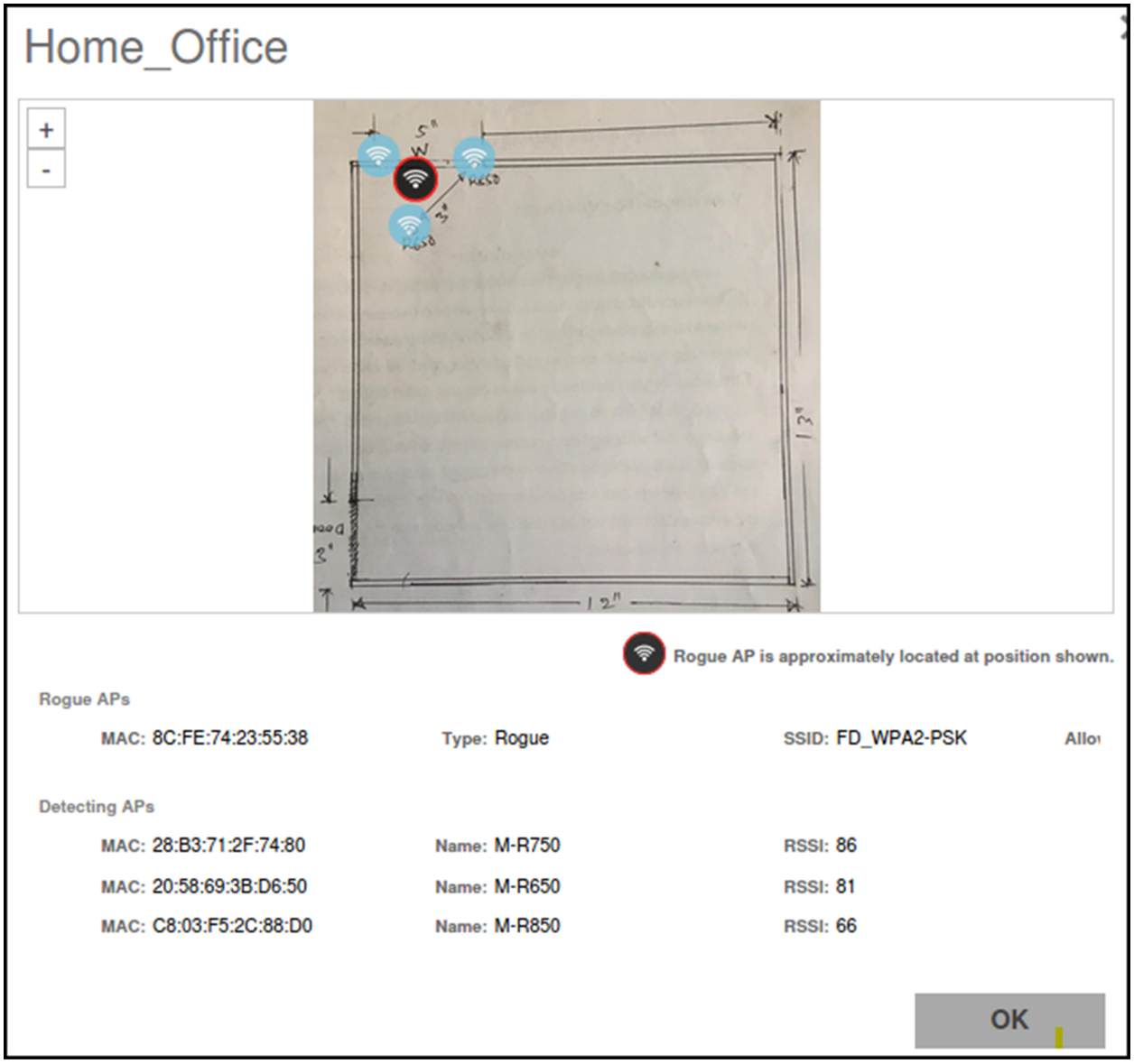
1. From the left pane, select **Report** > **Rogue Devices**.
2. Under **Device Type**, select **Access Point** or **Client**.

3. Click **Locate Rogue**.

   This displays **Rogue AP Location** page with rogue AP or rogue client. You can select from the following options:

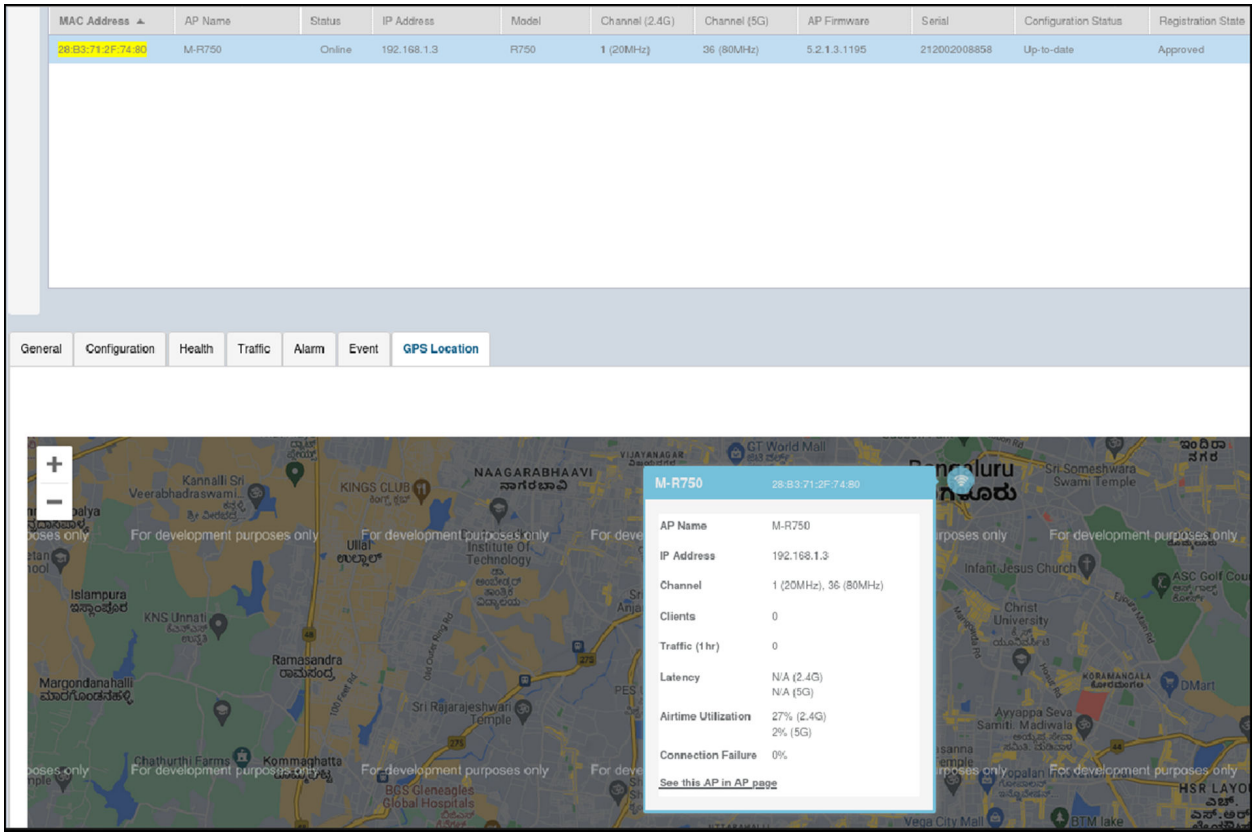
   - **Map**: Displays the monitor APs and rogue AP/UE detected on the floor map that is uploaded.

     FIGURE 81 Map View



   - **Satellite**: Displays the location as satellite imagery.

FIGURE 82 Satellite View



Click **+** to zoom in and **-** to zoom out.

You can find the following information about rogue and detected 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 40.

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

TABLE 40 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 41 contains historical client statistics report based on the UE session statistics.

TABLE 41 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.

External Syslog Server

External Syslog Server

This feature extracts the external syslog server setting as a profile, which will be regulated by the MSP (Managed Service Provider). The customers can select the partner domain-level profile while setting up a zone or an AP.

As a partner-domain customer needs only the AP or UE logs and events, the zone-level syslog setting could help to redirect log or events to different partner-domain external syslog per zone.

The MSP can create a maximum 16 profiles per partner domain.

Secure Boot

Overview

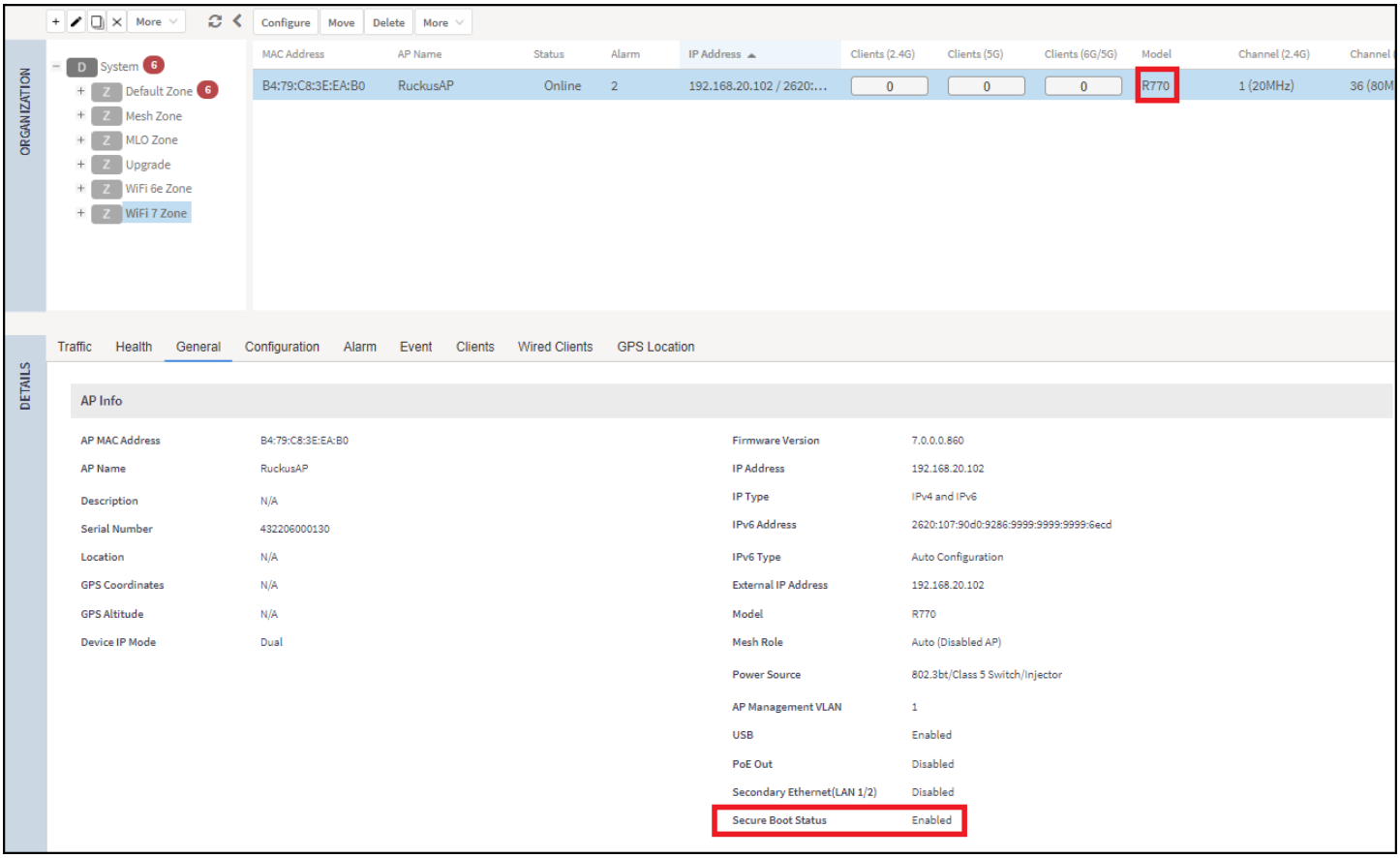
Secure Boot is a security technology that safeguards against the unauthorized modification of software binaries. The objective of this feature is to implement a secure boot process that includes digital signatures and verification for all bootloader images, up to and including u-boot. The Secure Boot functionality is applicable to AP models that minimally support Wi-Fi 7 and later APs incorporate this protection to ensure that only software, specifically bootloader images, which is properly signed and authorized by RUCKUS, can operate on the AP. This helps prevent unauthorized hacking or tampering of the device.

The Secure Boot feature is not configurable; the factory default setting is **Enabled**.

Requirements

Wi-Fi 7 and later AP models support Secure Boot.

FIGURE 83 Status of Secure Boot on Wi-Fi 7 AP



Considerations

The RUCKUS AP uses two features for signing and verification of software:

- **Image signing**: The AP image signing feature signs and verifies the entire AP software image, including the Kernel and Root File System. However, it does not cover the signing and verification of the bootloader images stored in NOR flash.
- **Secure Boot**: Secure Boot performs the signing and verification of the bootloader images in NOR flash memory.

AP Clients

Wireless

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.

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 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 setting . The Settings - Clients form displays.
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

The controller 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, the controller 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

The controller 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

Deauthorizing a Wireless Client

You can 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 by deauthorizing them. Deauthorized wireless clients remain connected to the wireless network, but are redirected to the authentication portal whenever they attempt to access network resources.

To deauthorize a wireless client, complete the following steps.

1. From the dashboard, click **Monitor** > **Wireless Clients** > **Clients**

   The **Wireless Clients** tab is displayed.
2. 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 field. Press **Enter** to search for the client.
3. Select the client and click the **Deauthorize** button.

   The table refreshes, and the client that you deauthorized is removed 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.

You might consider blocking a wireless client device for the following reasons:

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

To block a wireless client from accessing he SmartZone network, complete the following steps.

1. From the dashboard, click **Monitor** > **Clients** > **Wireless Clients**.

   The **Wireless Clients** tab is displayed.
2. 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 field. Press **Enter** to search for the client.
3. Select the client and click the **Block** button.

Unblocking a Wireless Client

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

To unblock a wireless client, complete the following steps.

1. From the dashboard, click **Security** > **Access Control** > **Blocked Client**.
2. 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 field. Press **Enter** to search for the client.
3. Select the client and click the **Delete** button.

Disconnecting a Wireless Client

Wireless clients can be temporarily disconnected from the wireless network through the web interface. For example, when troubleshooting problematic network connections, wireless clients may need to be manually disconnected as part of the troubleshooting process.

To disconnect a wireless client from the WLAN to which it is connected, complete the following steps.

1. From the dashboard, click **Monitor** > **Clients** > **Wireless Clients.**
2. 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 field. Press **Enter** to search for the client.
3. Select the client and click the **Disconnect** button.

   The table refreshes, and the client that you disconnected is removed from the list.

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 42 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

TABLE 42 Wireless Client Details (continued)

Column Name	Description
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
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

Viewing Wireless Client Information

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

To view information about a wireless client, complete the following steps.

1. From the dashboard, 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 displays general information about the wireless client:

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

Wired

Wired Clients

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

Deauthorizing a Wired Client

You can force wired clients that joined the wired network through an authentication portal to reauthenticate themselves by deauthorizing them. Deauthorized wired clients remain connected to the wired network, but are redirected to the authentication portal whenever they attempt to access network resources.

To deauthorize a wired client, complete the following steps.

1. From the dashboard, go to **Monitor** > **Clients** > **AP Wired Clients.**

   The **AP Wired Clients** tab is displayed.
2. 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 field. Press **Enter** to search for the client.
3. Select the client and click the **Deauthorize** button.

   The table refreshes, and the client that you deauthorized is removed from the list.

Viewing a Summary of Wired Clients

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

From the dashboard, go to **Monitor** > **Clients** > **AP Wired Clients**.

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

NOTE
To view wired clients that belong to a specific zone, click the zone name in the zone tree. The table refreshes, displaying only the clients that belong to the zone you selected.

NOTE
For more information about how the 802.1X configuration works for the port refer to Creating an Ethernet Port Profile on page 150.

TABLE 43 Wired Client Details

Column Name	Description
MAC Address	Displays the MAC address of the wired client
Username	Displays the name of the user logged in to the wired client
IP Address	Displays the IP address assigned to the wired client
AP MAC	Displays the MAC address of the access point
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 to access the WLAN service

AP Upgrade

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.

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.

Traffic Policies, Firewall and QoS

Understanding Wi-Fi Calling

Mobile service providers offer services where you can make voice calls or send and receive text messages from their mobile phones using a Wi-Fi 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 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.

Due to increasing use of Wi-Fi for device connections, Wi-Fi Calling is seeing high demand by many service providers worldwide, which allows them to differentiate their Wi-Fi 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.

Wi-Fi calling supports Wi-Fi calling traffic recognition and prioritization above other network traffic, with visibility for Wi-Fi calling statistics for the network operator.

Analyzing Wi-Fi Calling Statistics

Wi-Fi calls are tunneled to the carrier's Evolved Packet Data Gateway (EPDG), which eliminates dropped calls when switching from Wi-Fi to LTE and vice versa. Multiple carriers' EPDGs can be supported on a single WLAN. Wi-Fi Calling coexists seamlessly with RUCKUS CBRS (Citizens Band Radio Service) APs.

Follow the below steps to view Wi-Fi Calling Summary to view statistics, client details and quality chart.

From the main menu, go to **Services** > **Others** > **Wi-Fi Calling** > **Summary**.

The summary displays statistics of the top ten SSIDs (Service Set Identifier) and Evolved Packet Data Gateway (ePDGs) by traffic in the last one or twenty four hour interval. Choose the Zone or Domain and the corresponding WLAN to view the relevant statistics.

The **Wi-Fi Calling Clients** provides the following information.

- **Hostname**: The name of the user equipment or device that is connected to 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 Verizon, 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**: Data that is transmitted during the Wi-Fi call.

- **Traffic (uplink/downlink)**: The speed with which data is transmitted during the Wi-Fi call.

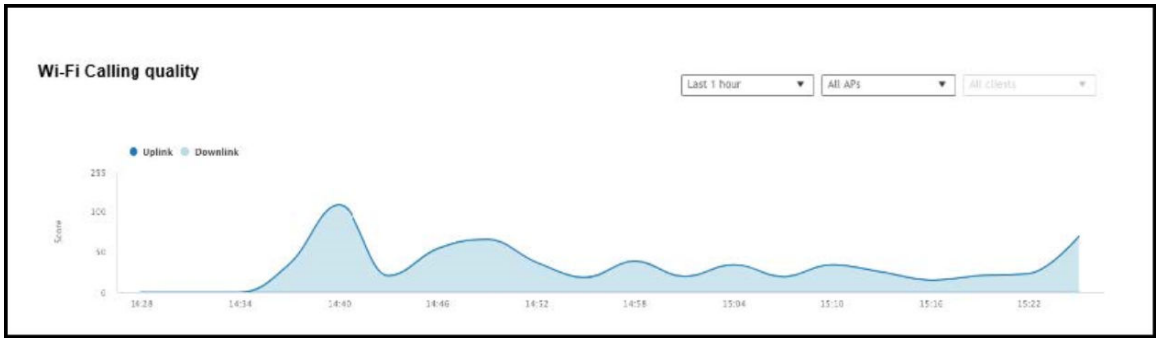
FIGURE 84 Wi-Fi Calling Client Details

The **Clients Detail** provides the following information.

- **AP MAC:** The MAC address of the AP.
- **Client IP:** The IP address of the client.
- **Carrier Name:** The name of the carrier, such as Verizon, AT&T, Sprint, T-Mobile.
- **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.

The **Wi-Fi Calling quality** chart displays the uplink and downlink quality. Call quality can be filtered based on time, the AP list, and the client MAC address list.

FIGURE 85 Wi-Fi Calling Quality Chart



Creating a Wi-Fi Calling Profile

You can classify the voice packets in a Wi-Fi call based on the carrier by creating a Wi-Fi calling profile.

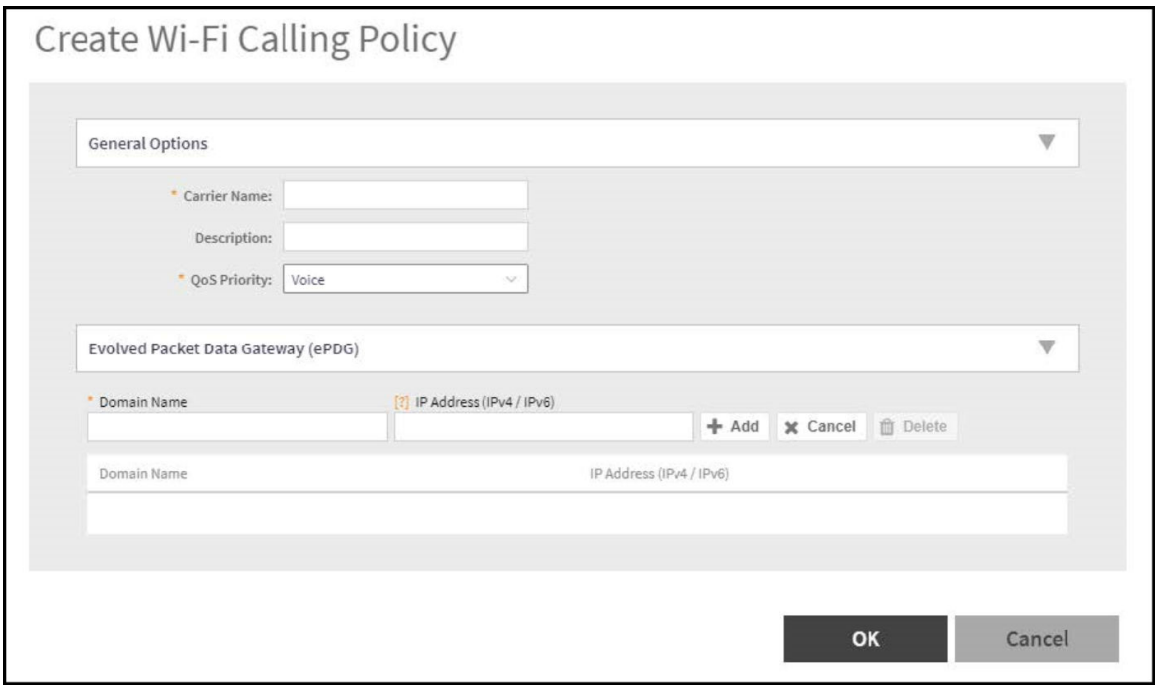
Follow the below steps to create a **Wi-Fi Calling** profile.

1. From the main menu go to **Services** > **Others** > **Wi-Fi Calling** > **Profiles**.

2. Click **Create**.

   The **Create Wi-Fi Calling Policy** dialog box is displayed.

   FIGURE 86 Creating a Wi-Fi Calling Policy



3. Under **General Options**, configure the following options:
   - **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 o the profile.
   - **QoS Priority**: Select the prioritization for the calls from the list such as Voice, Video, Best Effort and Background.
4. Under **Evolved Packet Data Gateway (ePDG)**, configure the following options:
   - **Domain Name**: Enter the domain name, for example, epdg.epc.att.net.
   - (Optional) **IP Address (IPv4/IPv6)**: Enter the IP address for the domain. Providing the IP address enables better Wi-Fi calling QoS during roaming.
5. Click **Add** to include the domain.

   The AP verifies the domain IP address before qualifying the Wi-Fi call.
6. Click **OK** .

The Wi-Fi 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 selecting **Configure**, **Clone**, and **Delete** options respectively.

Configuring Wi-Fi Calling in a WLAN

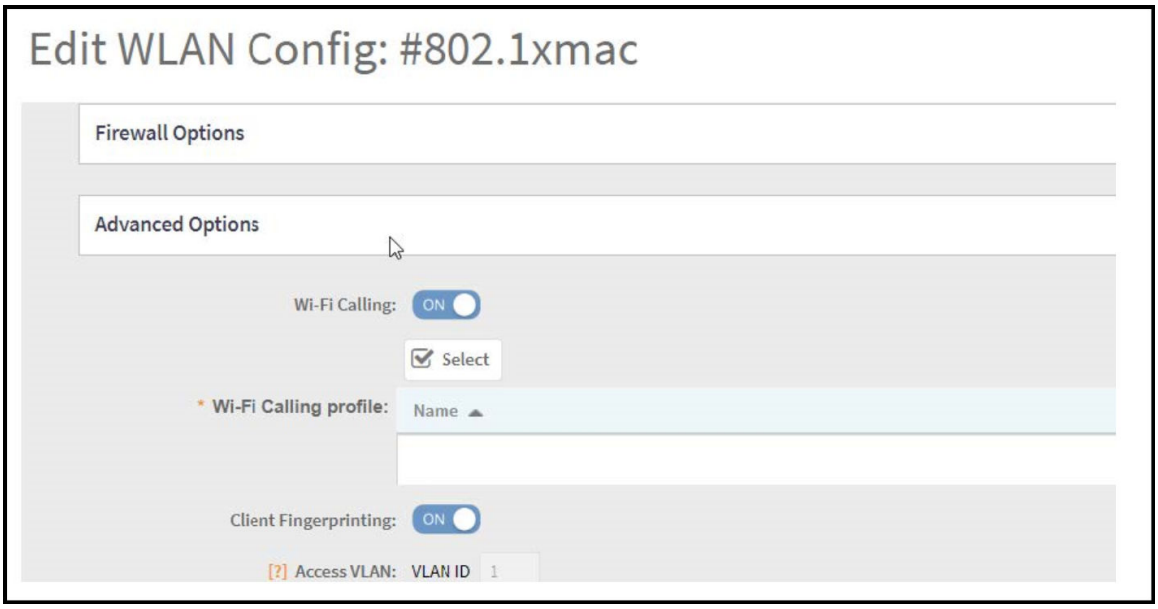
Use the configuration option to create the Wi-Fi policies.

Follow the steps below to edit the WLAN configuration for selecting a Wi-Fi calling profile.

1. From the main menu navigate to **Network** > **Wireless LANS**.
2. Select the WLAN to enable Wi-Fi calling and click **Configure**.

   The **Edit WLAN Configuration** dialog box is displayed. You can also enable Wi-Fi calling when you create a fresh WLAN configuration, by clicking **Create**.

   FIGURE 87 Configuring Wi-Fi Calling in a WLAN



3. Under **Advanced Options**, set **Wi-Fi Calling** to **ON**.
4. Click **Select**.

   The **Wi-Fi Calling Policies** dialog box is displayed.
5. From the **Available Profiles** list, identify the profiles you want and click the **->** icon. The profiles move to **Selected Profiles**. You can use the **<-** icon to remove the profile for the WLAN.
6. Click **OK**.

   The profiles selected are displayed in the **Wi-Fi Calling Profile** page.

URL Filtering

You 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 98304 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.

AP-to-AP communication provides client roaming support with Application Visibility Control (AVC) features such as Application Recognition Control (ARC) and URL Filtering. URL-filtering, based on category and threat level (web reputation) will work on the destination AP depending on the URL domain.

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

Enabling URL Filtering on the WLAN

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.

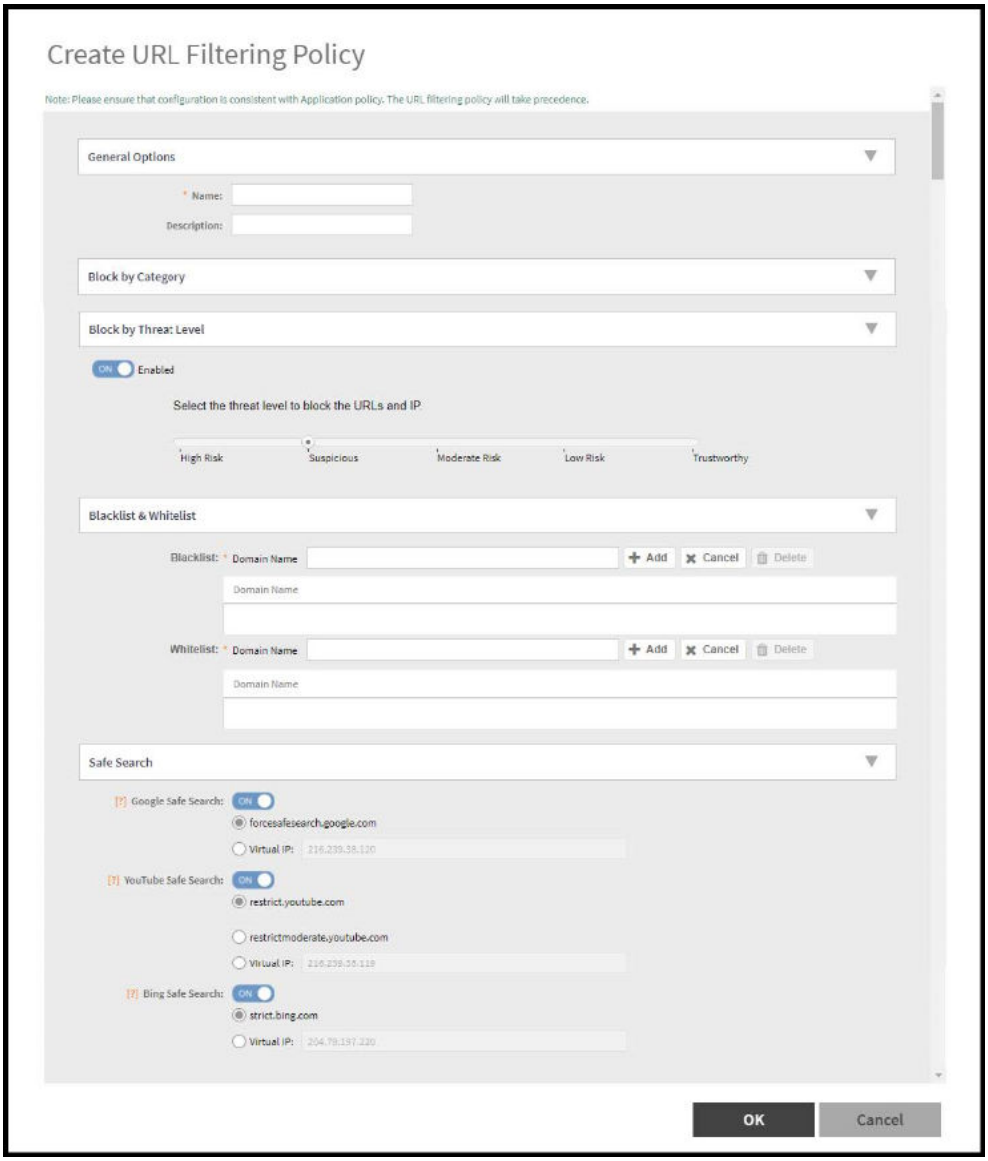
Complete the following steps to create a URL filtering policy.

1. From the main menu 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.

   FIGURE 88 Creating URL Filtering Policy



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 categorization, 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. From R5.2 onwards, the wildcard (*) character is supported in middle and on either start or end, for example, "*.ruckus*.com", www.ruckus*.co*). This only allows a maximum of two wildcards (*).

  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 (IPv4 and IPv6) address, select the **Virtual IP** option and enter the IP address. If safe search is enabled before uprading to release 6.1, 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
- Threat Level

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.

Follow these steps to enable URL filtering on the controller for an available WLAN.

1. From the main menu go to **Network** > **Wireless LANs** to select a domain or zone.
2. 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.

3. 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 Enabling URL Filtering on the WLAN on page 225.

   FIGURE 89 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, navigate to **Administration** > **Administration** > **Licenses** > **Installed Licenses**.

For more information on importing installed licenses, synchronizing the controller with the license server, and downloading license files, refer *RUCKUS SmartZone Software Licensing Guide*.

When the license capacity is exhausted, event code 1281 is triggered. When the license period expires, alarm code 8003 is generated, indicating that the URL filtering server is unreachable. For more information, refer *RUCKUS SmartZone Alarms and Events Guide*.

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.

NOTE
The R730 AP is supported on Zones running R6.1.0.

TABLE 44 List of APs that have a RAM size of 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	

Application Control

Viewing an Application Control Summary

You can view an application-specific or port-specific summary in a chart or table format.

Complete the following steps to view the application control summary.

1. From the main menu, go to **Security** > **Application Control** > **Summary**.

   The **Summary** page is displayed.
2. The **Summary** page can be viewed with following options:
   - Top Applications by: Choose Application or Port from the menu.
   - Click to view by Chart or Table.
   - **Count:** Select **10** or **25**.
   - Total, 2.4 GHz, 5GHz, and 6GHz.
   - **Duration:** Select **Last 1 hour** or **Last 24 hours**.
   - APs: Select a specific AP or **All APs**.
   - 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.

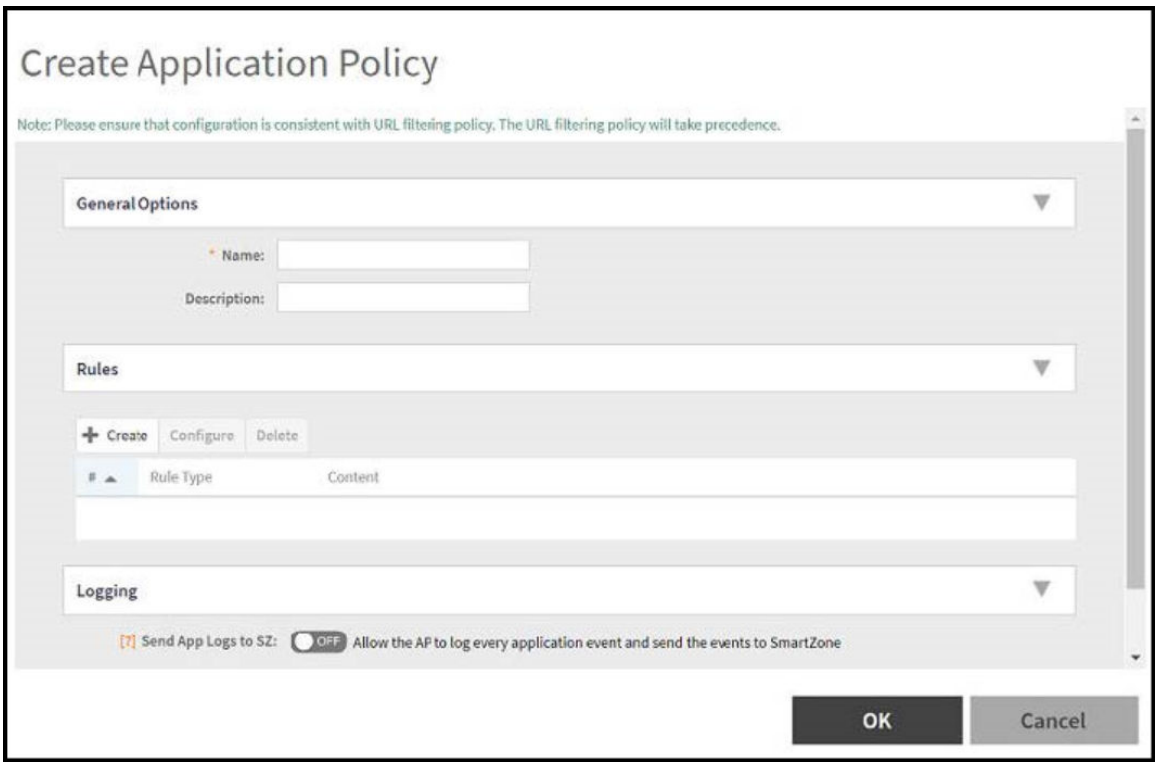
1. From the main menu, go to **Security** > **Application Control** > **Application Policy**.

   The **Application Policy** page is displayed.

2. Click **Create**.

   The **Create Application Policy** dialog box is displayed.

   FIGURE 90 Creating an Application Policy



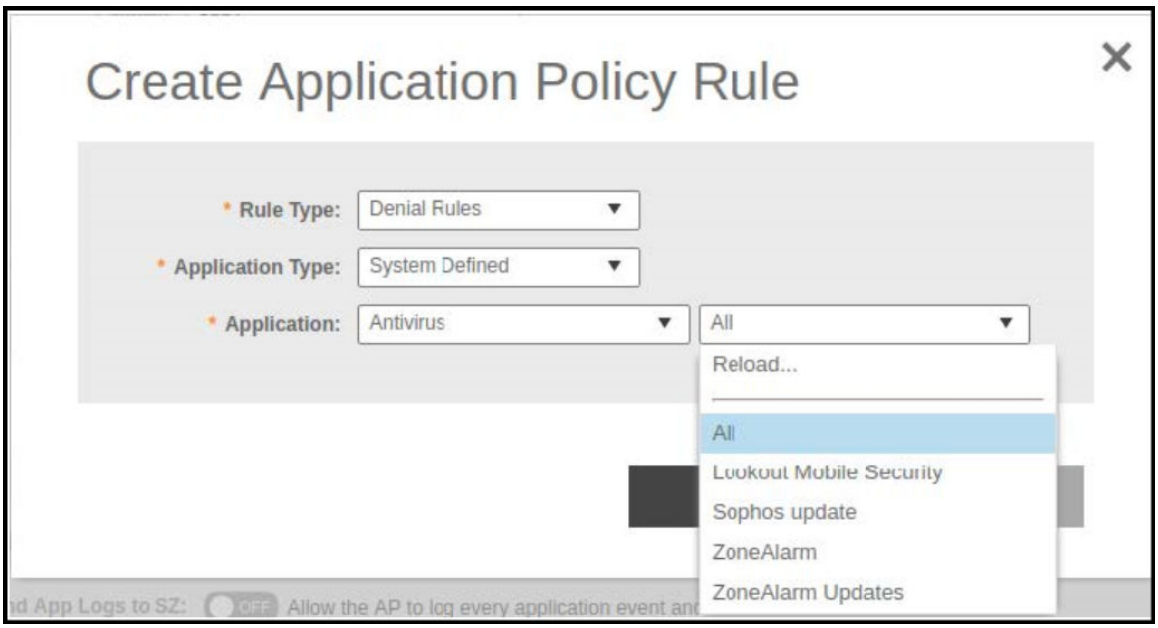
3. Under **General Options**, enter the policy name and description.

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 91 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.

Application Signature Packages

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

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

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

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

Creating a User-Defined Application

When an application is unrecognized and generically (or incorrectly) categorized, the controller is unable to monitor its traffic, unless you configure an explicit application identification policy based on IP address or mask, port, and protocol.

Complete the following steps to configure a user-defined application.

1. From the main menu, go to **Security** > **Application Control** > **User Defined Applications**.
2. Click **Create**.

   The **Create User Defined Application** dialog box is displayed.
3. Configure the following options:
   - **Name**: Enter a name for the application. This name that will identify this application on the dashboard.
   - **Type**: Select **Default** or **Port Mapping.**
   - **IP Mode**: Select **IPv4** or **IPv6** address.
   - **Destination IP/Netmask**: Enter the destination IP address of the application and the netmask of the destination IP address.
   - **Destination Port**: Enter the destination port for the application.
   - **Protocol**: Select the protocol used by the application. Options include **TCP** and **UDP**.
4. Click **OK**.

   NOTE
   You can also edit, clone, and delete the user-defined application by selecting the options **Configure**, **Clone**, and **Delete** respectively from the **User Defined** tab.

Creating a Traffic Class Profile

A traffic class allows you to classify traffic according to a set of criteria that you define, such as source and destination IP addresses.

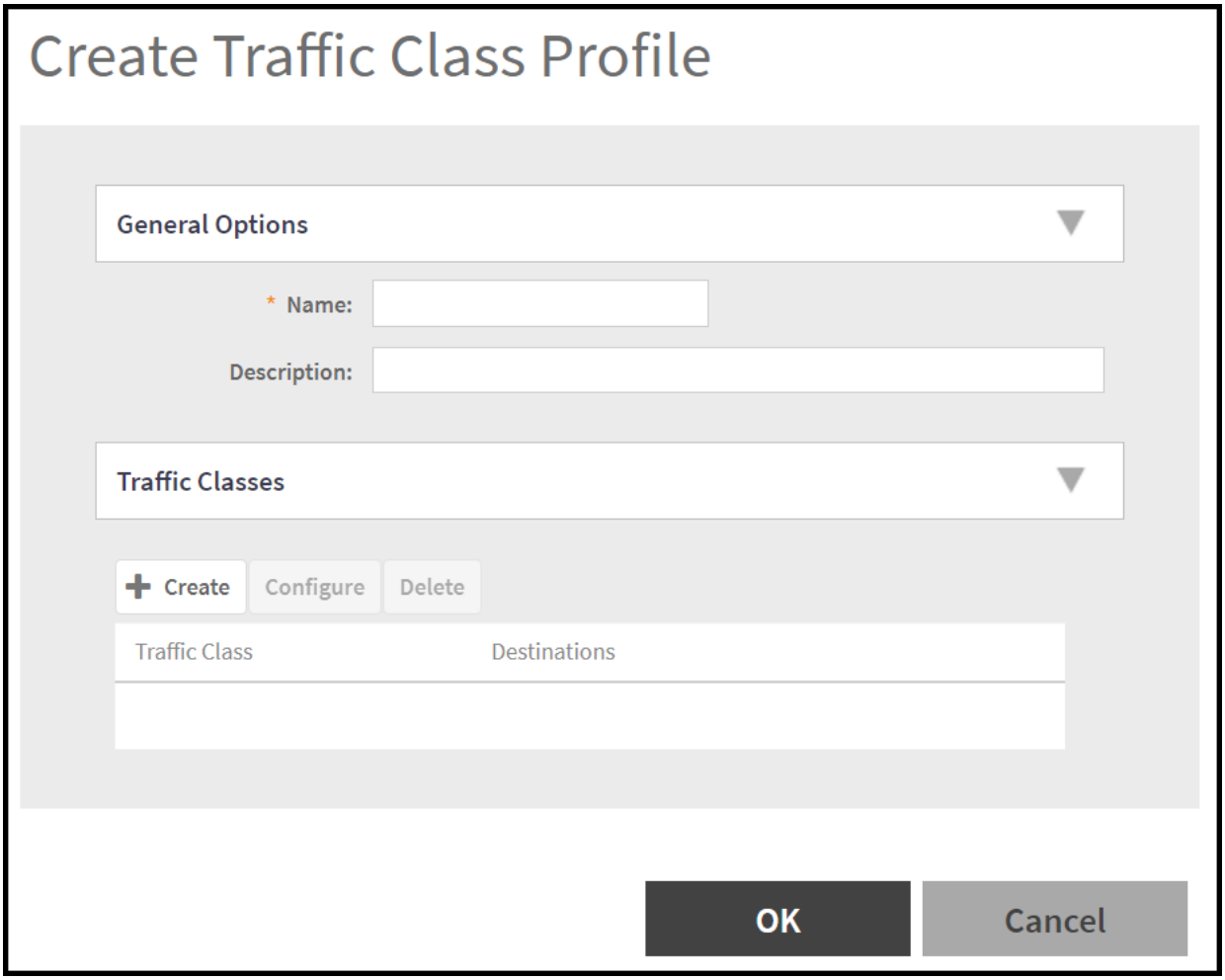
To create a Traffic Class Profile, perform the following:

1. Click **Security** > **Access Control** > **Traffic Classes**.

2. Select the zone from the system tree and click **Create**.

   This displays **Create Traffic Class Profile** page.

   FIGURE 92 Create Traffic Class Profile



3. **General Options**
   a. Name: Enter a name to identify the traffic class profile.
   b. Description: Enter a short description for traffic class profile.

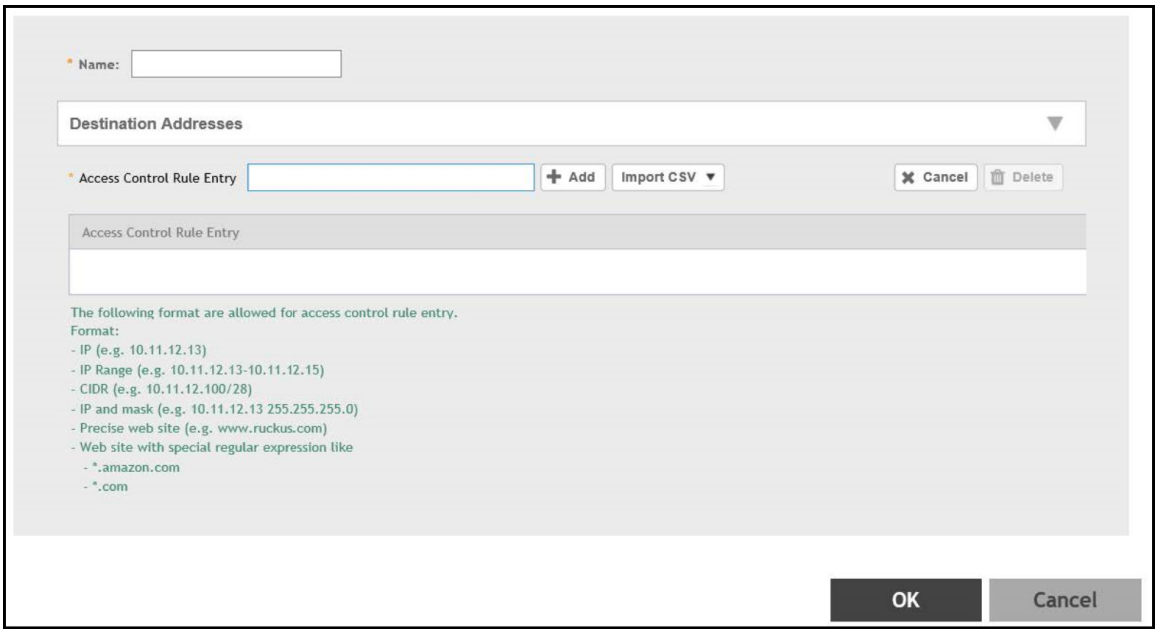
4. **Traffic Classes**
   a. Click **Create**. This displays **Destination Addresses** window.

      Enter a name to identify the destination address.

   b. **Destination Addresses** - *Access Control Rule Entry*: Enter an access control rule as shown in the format section under the field and click **Add**. The access control address is displayed in the **Access Control Rule Entry** table.

      Import CSV Format: Click this field to import a CSV format file from your local computer.

FIGURE 93 Destination Addresses



5. Click **OK**.

NOTE
Only four traffic classes can be added in a single **Traffic Class** profile.

You have created a Traffic Class Profile.

NOTE
The IP destination is reachable only when the IP is not part of traffic class but is present under Split Tunnel. The Split Tunnel policy is effective only when both **Split Tunnel** and **Traffic Class** features are enabled together.

Managing a Firewall Profile

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.

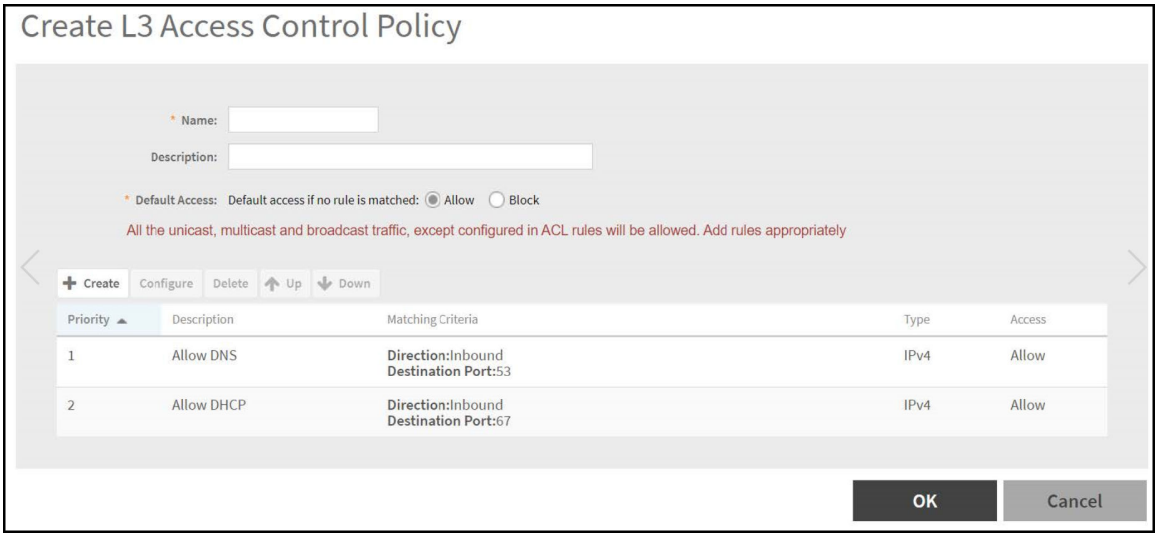
1. Select **Security** > **Access Control** > **L3 Access Control**.

   The **L3 Access Control** page is displayed.

2. Click **Create**.

   This displays the **L3 Access Control Policy** page.

   FIGURE 94 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 238 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.

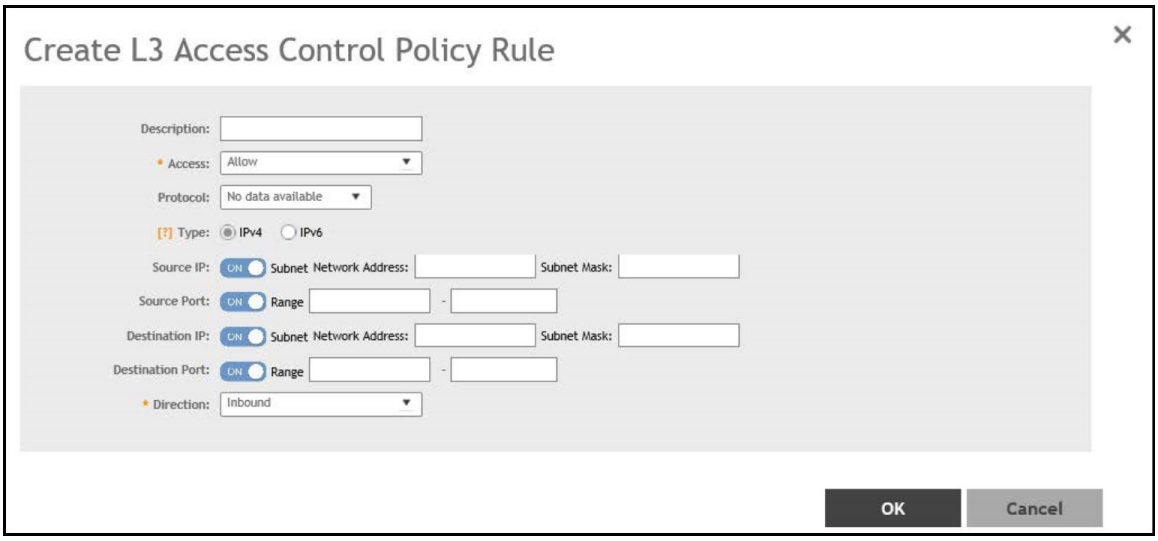
Create an L3 Access Control Policy Rule

An L3 Access Control consists of 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 95 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 Policy

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.

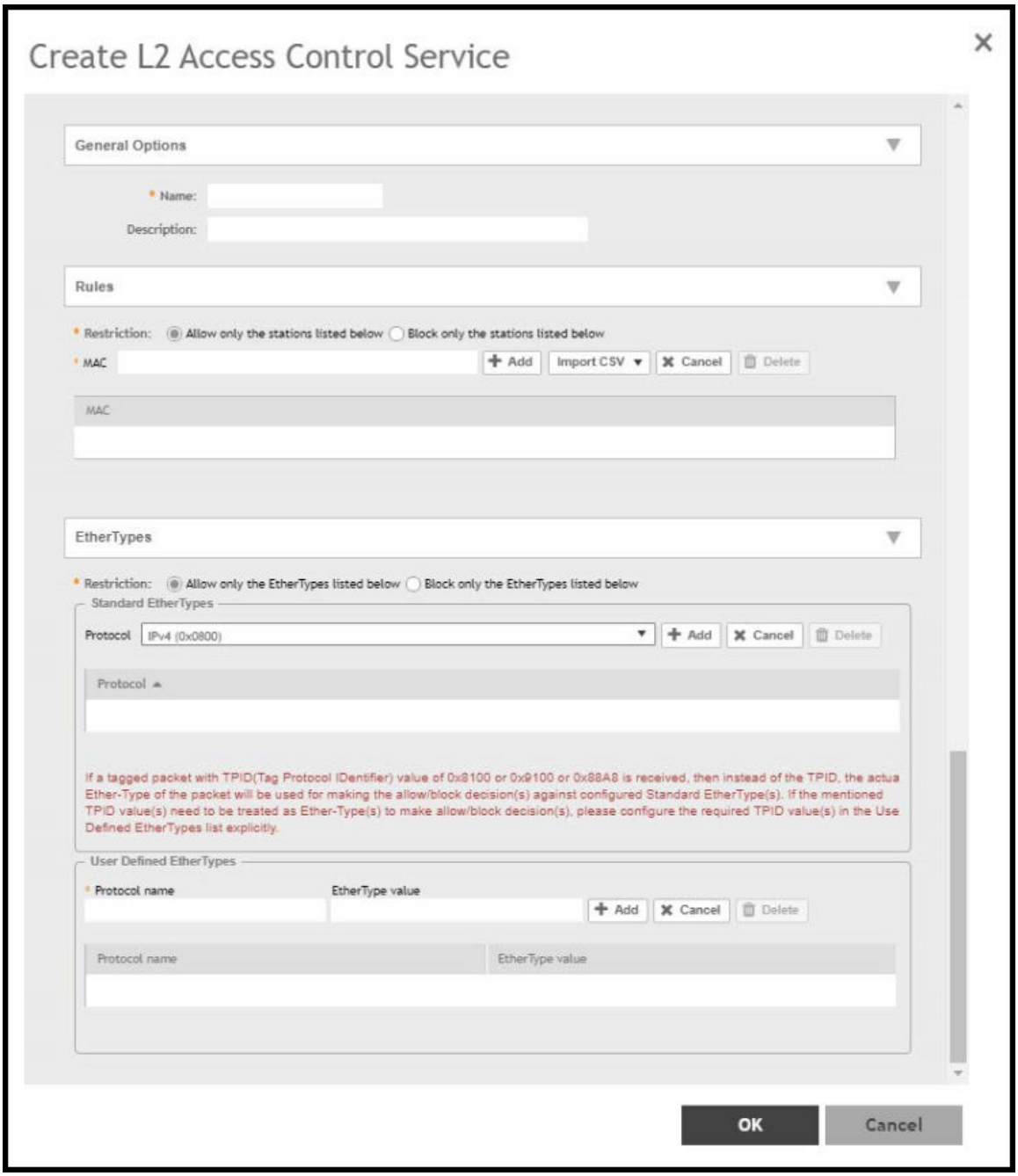
NOTE
If a tagged packet with Tag Protocol Identifier (TPID) value of 0x8100, 0x9100, or 0x88A8 is received, then instead of the TPID, the actual Ether-Type of the packet will be used for making the allow or block decision against the configured Ether-Types. If the mentioned TPID values need to be treated 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 96 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.

Configuring Application Controls

Using the **Application Control** screen, you can identify, control, and monitor applications that are running on wireless and wired clients associated with managed APs, and you can also apply filtering policies to prevent users from accessing certain applications.

Additionally, you can create your own user-defined applications, import an updated application signature package, and configure rate limiting and QoS traffic shaping policies based on system-defined or user-defined applications.

AP-to-AP communication provides client roaming support with Application Visibility Control (AVC) features such as Application Recognition Control (ARC) and URL Filtering. ARC will work on the destination AP based on its app-id.

Viewing an Application Control Summary

You can view an application-specific or port-specific summary in a chart or table format.

Complete the following steps to view the application control summary.

1. From the main menu, go to **Security** > **Application Control** > **Summary**.

   The **Summary** page is displayed.

2. The **Summary** page can be viewed with following options:
   - Top Applications by: Choose Application or Port from the menu.
   - Click to view by Chart or Table.
   - **Count:** Select **10** or **25**.
   - Total, 2.4 GHz, 5GHz, and 6GHz.
   - **Duration:** Select **Last 1 hour** or **Last 24 hours**.
   - APs: Select a specific AP or **All APs**.
   - 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.

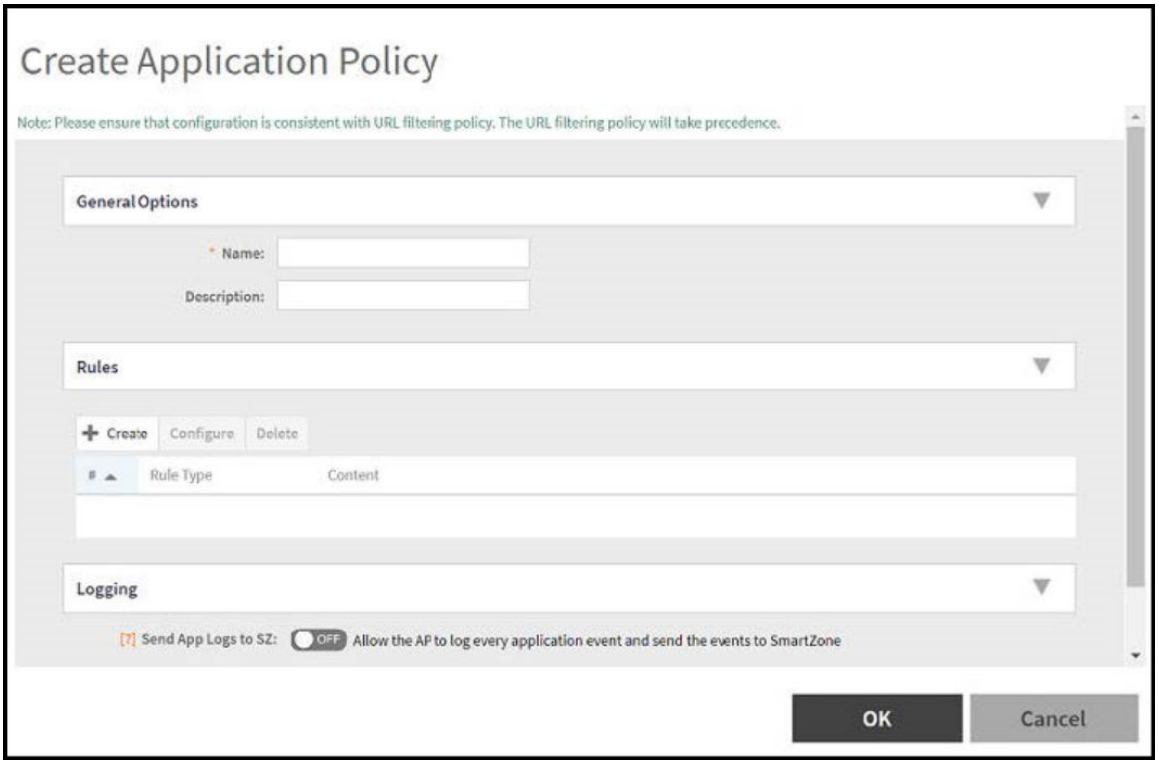
Complete the following steps to create an application control policy.

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 97 Creating an Application Policy



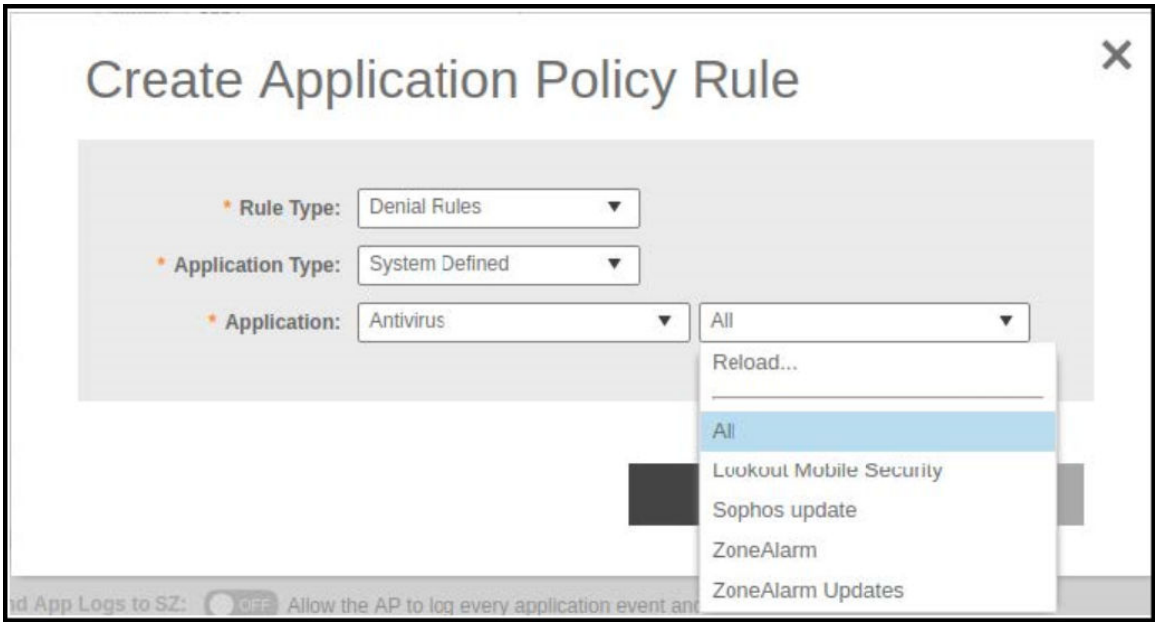
3. Under **General Options**, enter the policy name and description.

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 98 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.

Implementing an Application Control Policy

Deploying an application control policy involves configuring a Firewall Profile with the policy, and then applying that profile to a WLAN.

To implement an Application Control Policy:

1. Go to **Security** > **Application Control** > **Application Policy**.

   Refer to Creating an Application Control Policy on page 231 for more information.

   NOTE
   For SmartZone 5.2.1 or earlier releases, go to **Firewall** > **Application Control**.

2. Go to **Wireless LANs**.
3. Locate the WLAN for which you want to apply the application policy, and select it from the list.
4. Click **Configure**. The **Edit WLAN [WLAN Name]** page appears.
5. Under **Firewall Options**, select the **Enable WLAN specific** option.
6. From **Application Control**, select an application control policy you created from the drop-down list. Alternatively, click **Create** to create a new application control policy.

7. Click **OK** to save your WLAN changes.

FIGURE 99 Select an Application Policy to apply to the Firewall Profile

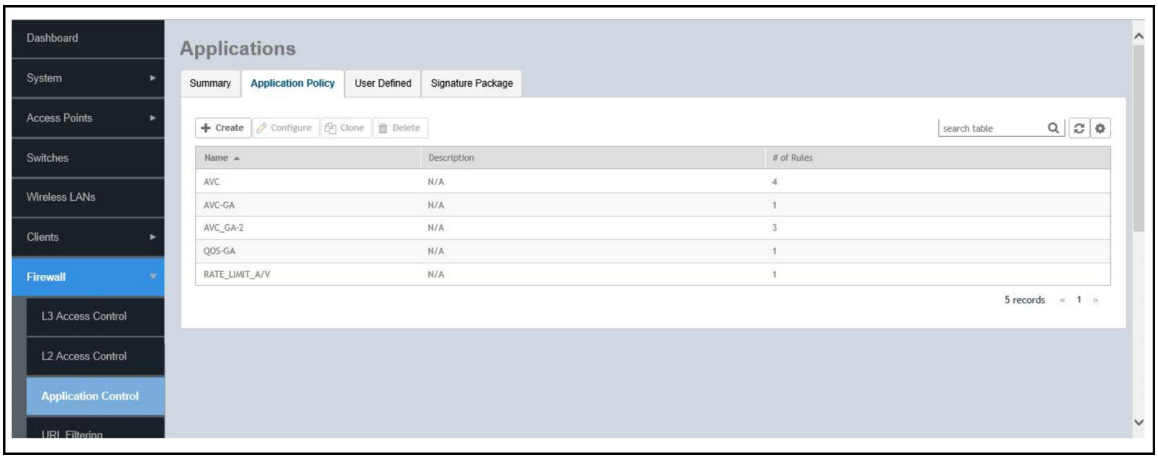
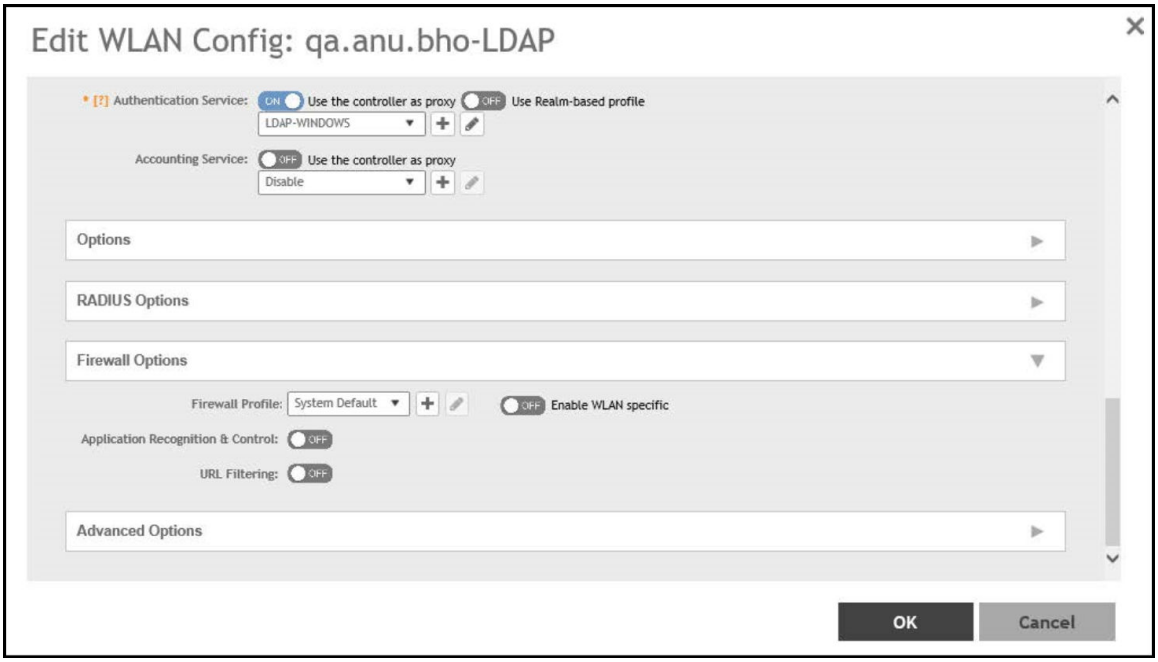


FIGURE 100 Apply the Application Control Policy to a WLAN



Creating a User-Defined Application

When an application is unrecognized and generically (or incorrectly) categorized, the controller is unable to monitor its traffic, unless you configure an explicit application identification policy based on IP address or mask, port, and protocol.

Complete the following steps to configure a user-defined application.

1. From the main menu, go to **Security** > **Application Control** > **User Defined Applications**.

2. Click **Create**.

   The **Create User Defined Application** dialog box is displayed.
3. Configure the following options:
   - **Name**: Enter a name for the application. This name that will identify this application on the dashboard.
   - **Type**: Select **Default** or **Port Mapping.**
   - **IP Mode**: Select **IPv4** or **IPv6** address.
   - **Destination IP/Netmask**: Enter the destination IP address of the application and the netmask of the destination IP address.
   - **Destination Port**: Enter the destination port for the application.
   - **Protocol**: Select the protocol used by the application. Options include **TCP** and **UDP**.
4. Click **OK**.

NOTE
You can also edit, clone, and delete the user-defined application by selecting the options **Configure**, **Clone**, and **Delete** respectively from the **User Defined** tab.

Application Signature Packages

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

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

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

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

URL Filtering

You 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 98304 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.

AP-to-AP communication provides client roaming support with Application Visibility Control (AVC) features such as Application Recognition Control (ARC) and URL Filtering. URL-filtering, based on category and threat level (web reputation) will work on the destination AP depending on the URL domain.

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

Enabling URL Filtering on the WLAN

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.

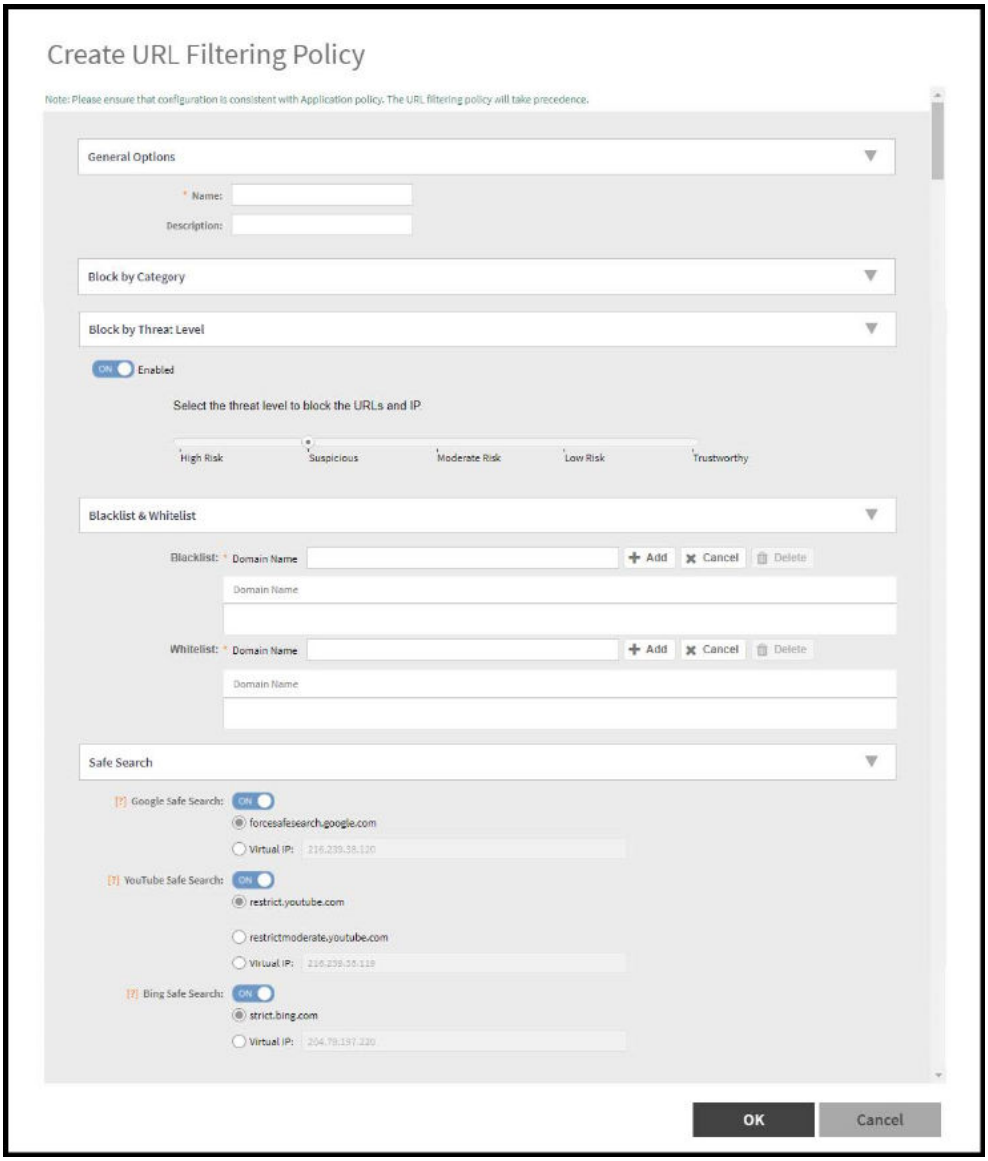
Complete the following steps to create a URL filtering policy.

1. From the main menu 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.

   FIGURE 101 Creating URL Filtering Policy



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 categorization, 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. From R5.2 onwards, the wildcard (*) character is supported in middle and on either start or end, for example, "*.ruckus*.com", www.ruckus*.co*). This only allows a maximum of two wildcards (*).

  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 (IPv4 and IPv6) address, select the **Virtual IP** option and enter the IP address. If safe search is enabled before uprading to release 6.1, 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
- Threat Level

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.

Follow these steps to enable URL filtering on the controller for an available WLAN.

1. From the main menu go to **Network** > **Wireless LANs** to select a domain or zone.
2. 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.

3. 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 Enabling URL Filtering on the WLAN on page 225.

   FIGURE 102 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, navigate to **Administration** > **Administration** > **Licenses** > **Installed Licenses**.

For more information on importing installed licenses, synchronizing the controller with the license server, and downloading license files, refer *RUCKUS SmartZone Software Licensing Guide*.

When the license capacity is exhausted, event code 1281 is triggered. When the license period expires, alarm code 8003 is generated, indicating that the URL filtering server is unreachable. For more information, refer *RUCKUS SmartZone Alarms and Events Guide*.

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.

NOTE
The R730 AP is supported on Zones running R6.1.0.

TABLE 45 List of APs that have a RAM size of 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**.

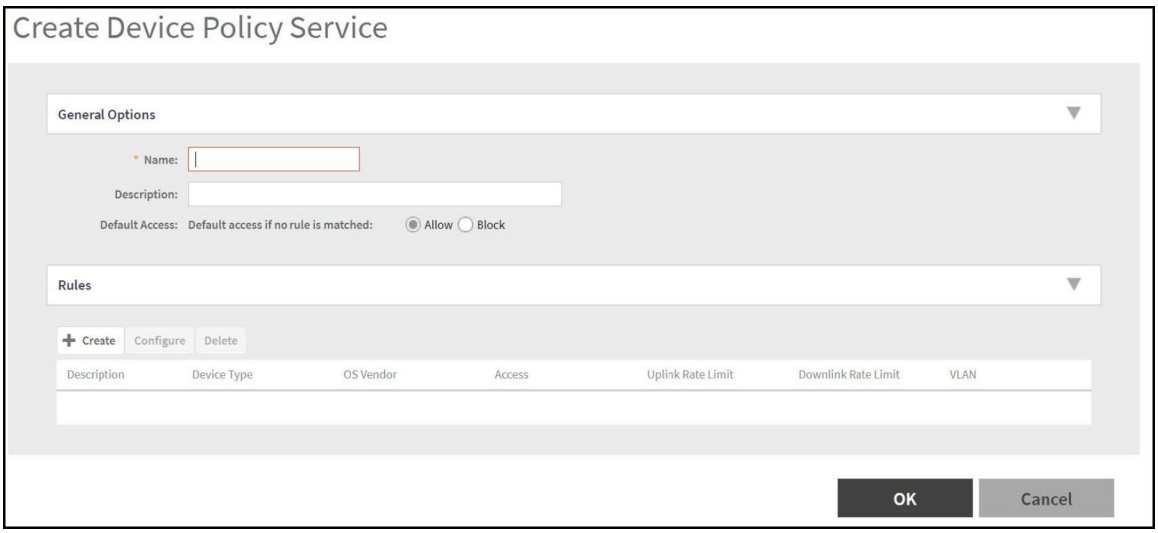
   This displays **Summary** and **Profiles** options.

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 103 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 the Device Policy Rules on page 254.
   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.

Creating the Device Policy Rules

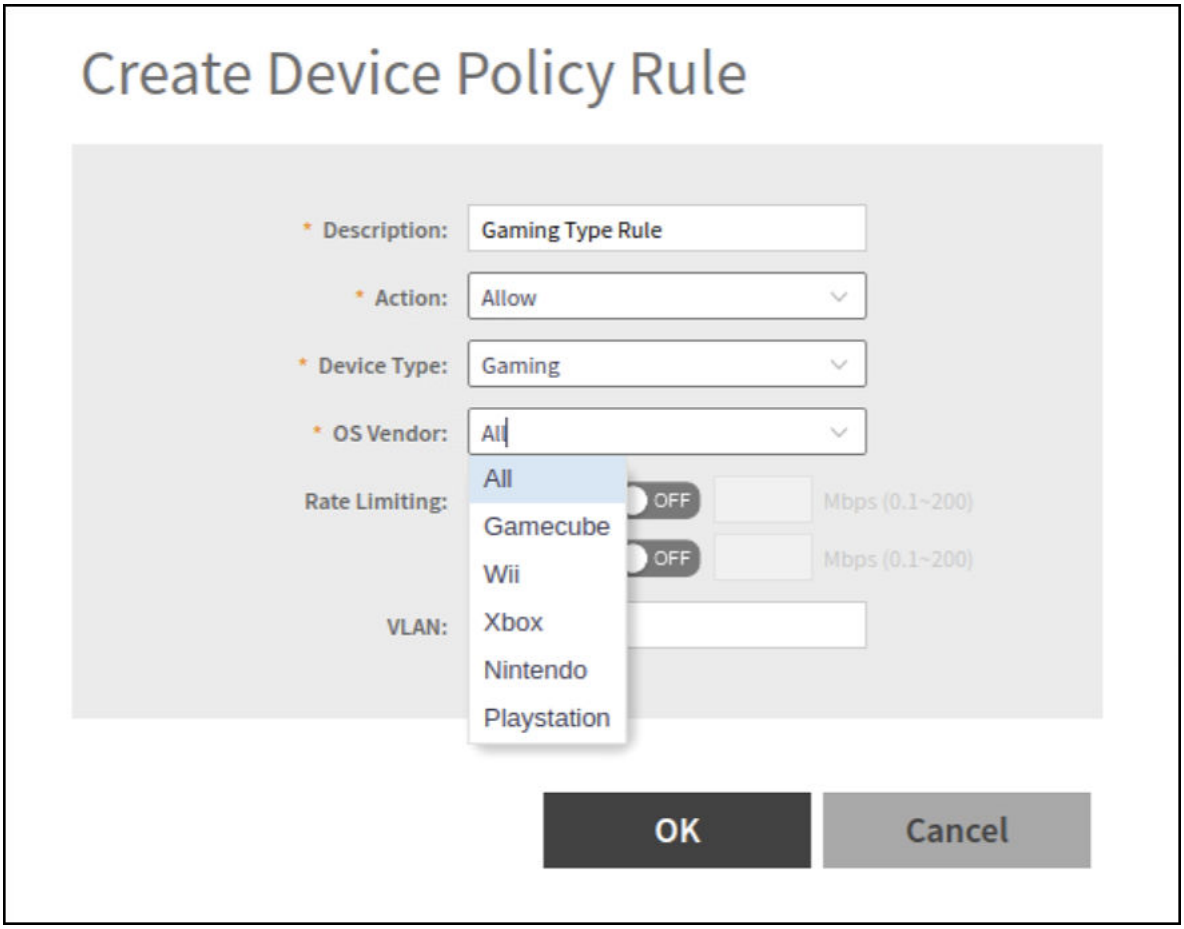
Complete the following steps to create a device policy rule.

1. From the main menu, go to **Security** > **Access Control** > **Device Policy**.

   The **Summary** and **Profiles** tabs are displayed on page.
2. Click the **Profiles** tab.
3. Click **Create** to open the **Create Device Policy Service** page.
4. In the **Rules** section, click **Create**.

   The **Create Device Policy Rule** page is displayed.

   FIGURE 104 Creating a Device Policy Rule



5. Configure the following.
   a) **Description**: Enter a short description for this device policy.
   b) **Action**: Select **Allow** or **Block**. This is the action that the system takes if the client matches any of the attributes in the rule.
   c) **Device Type**: Select the device type from the list.

      NOTE
      The **Device Type** feature is also supported on 11 AX APs.

   d) **OS Vendor**: Select the OS type from the list.

      NOTE
      Starting with the 7.0 release, the original supported **Gaming** device type OS vendors have been merged. The **XBOX 360** is merged with **XBOX**, **PlayStation 2** and **PlayStation 3** are merged into **PlayStation**.

   e) **Rate Limiting**: Enable the uplink and downlink rate limiting, and enter a rate limit value for each.

      NOTE
      The Rate limit supports a maximum of 100 clients per WLAN per radio. After the threshold, the system displays client failure (203) error.

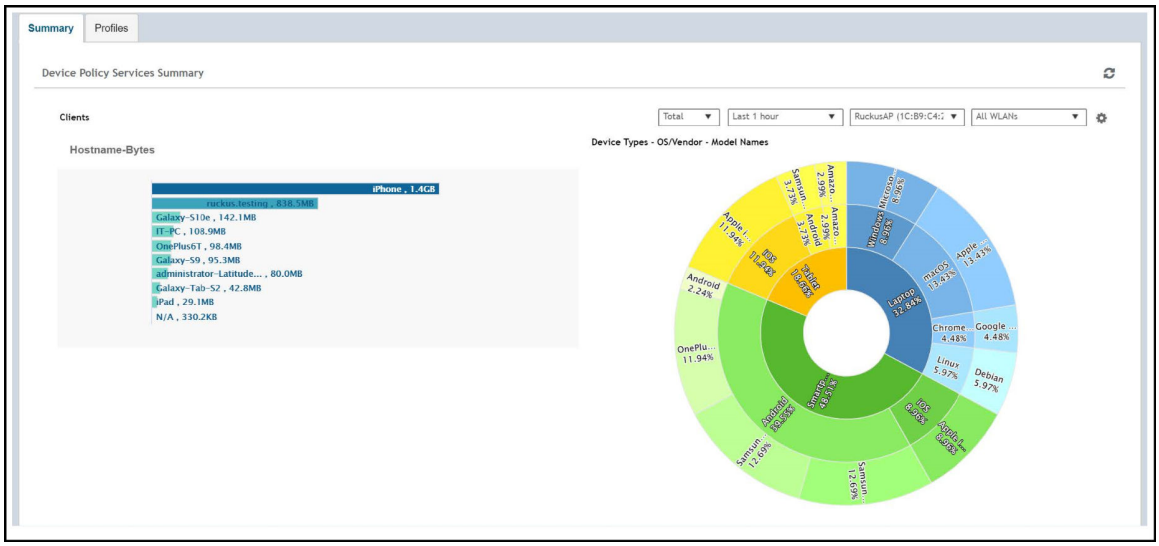
   f) **VLAN** : Enter the VLAN number for segmenting the client type. The value ranges from 1 through 4094. If no value is entered, this policy will not affect device VLAN assignment.
   g) Click **OK**.

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 105 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 46 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.

Configuring Traffic Analysis Display for WLANs

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

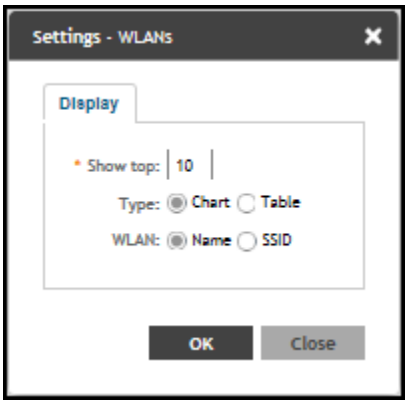
You can view historical and real-time data of the WLANs. Throughput and the number of clients connected to the WLANs are displayed in a bar chart. You must configure the WLAN settings to view its traffic analysis.

Complete the following steps to configure the WLAN settings.

1. From the WLAN area, click settings .

   The WLAN settings form displays.

   FIGURE 106 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**.

Bonjour

Bonjour is the Apple 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, you may want to offer Bonjour services from one VLAN to another.

The controller provides two features for controlling how and where Bonjour services are available to clients:

- Bonjour Gateway on page 257: Bridges Bonjour services from one VLAN to another.
- Bonjour Fencing on page 259: Limits 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.

Bonjour Gateway on the controller provides an multicast DNS (mDNS) proxy service configurable from the web interface to allow administrators to specify which types of Bonjour services can be accessed from and to which VLANs.

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 Bonjour Gateway are on separate subnets, the network must be configured to route traffic between them.

Creating Bonjour Gateway Policies

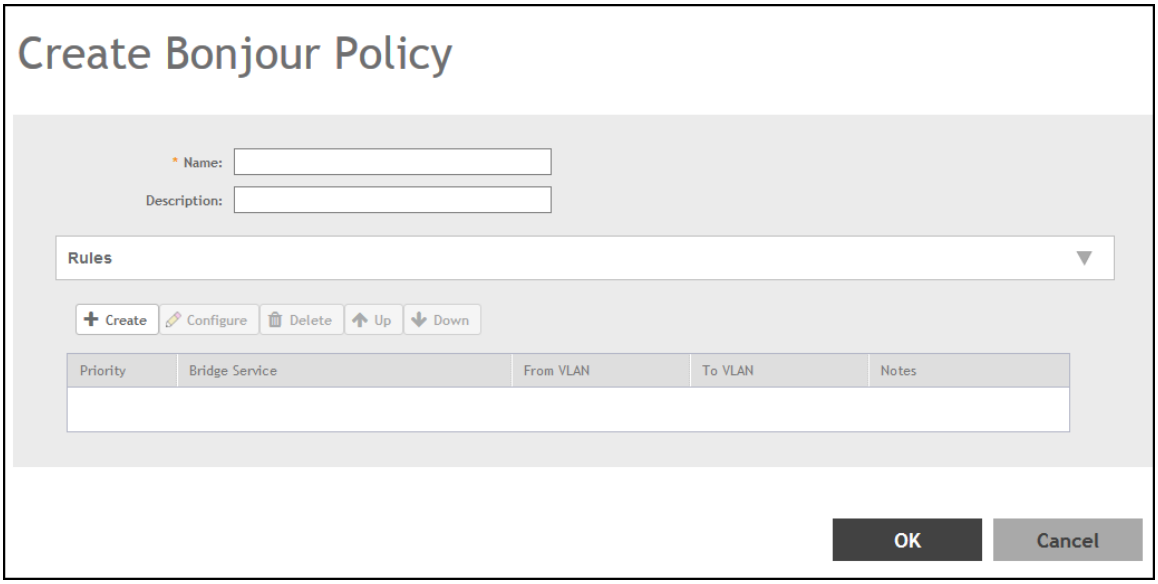
A Bonjour Gateway policy must be created for an AP zone before the policy can be deployed to an AP or group of APs.

Complete the following steps to create a Bonjour Gateway policy.

1. From the main menu, 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.
4. Click **Create**.

   The **Create Bonjour Policy** dialog box is displayed.

   FIGURE 107 Creating a Bonjour Gateway Policy



5. Configure the following options:
   - **Name**: Enter a name for the policy.
   - **Description**: Enter a description for the policy.
   - **Rules**: Create the policy rule by configuring the following
6. Under **Rules**, click **Create**. The **Create Bonjour Policy Rule** dialog box is displayed.
7. 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 will be made available.

     NOTE
     Add optional notes for this rule.

8. Click **OK**.
9. Click **OK** to save your Bonjour policy rule.

You have created a Bonjour policy with a rule.

> **NOTE**
> You can also edit, clone, and delete the policy by selecting the **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 259.

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.

Complete the following steps to apply a Bonjour Gateway policy to an AP.

1. From the main menu, 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. Go to **Advanced Options**
5. Under **Bonjour Gateway**, select the check box next to **Enable as Bonjour Gateway with policy**, and select the policy you created from the list.
6. 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 and spatial domain.

While Bonjour Fencing is related to Bonjour Gateway, they are designed for different purposes. Bonjour Gateway bridges mDNS services across VLANs, and is useful because mDNS or Bonjour packets are restricted to the same VLAN or subnet and cannot be routed to other VLANs. Bonjour Fencing limits the range of Bonjour service discovery within a physical space, which is useful because logical network boundaries (for example, VLANs) do not always correlate well to physical boundaries within a building or 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.
- For a wired fencing policy to work properly, wireless fencing for the same mDNS service must 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 is wired or wireless.
- Bonjour Fencing works for local breakout scenarios, but does 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, the AP will always give priority to the hop 1 service record. Because tagging occurs 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 > Bonjour** page.

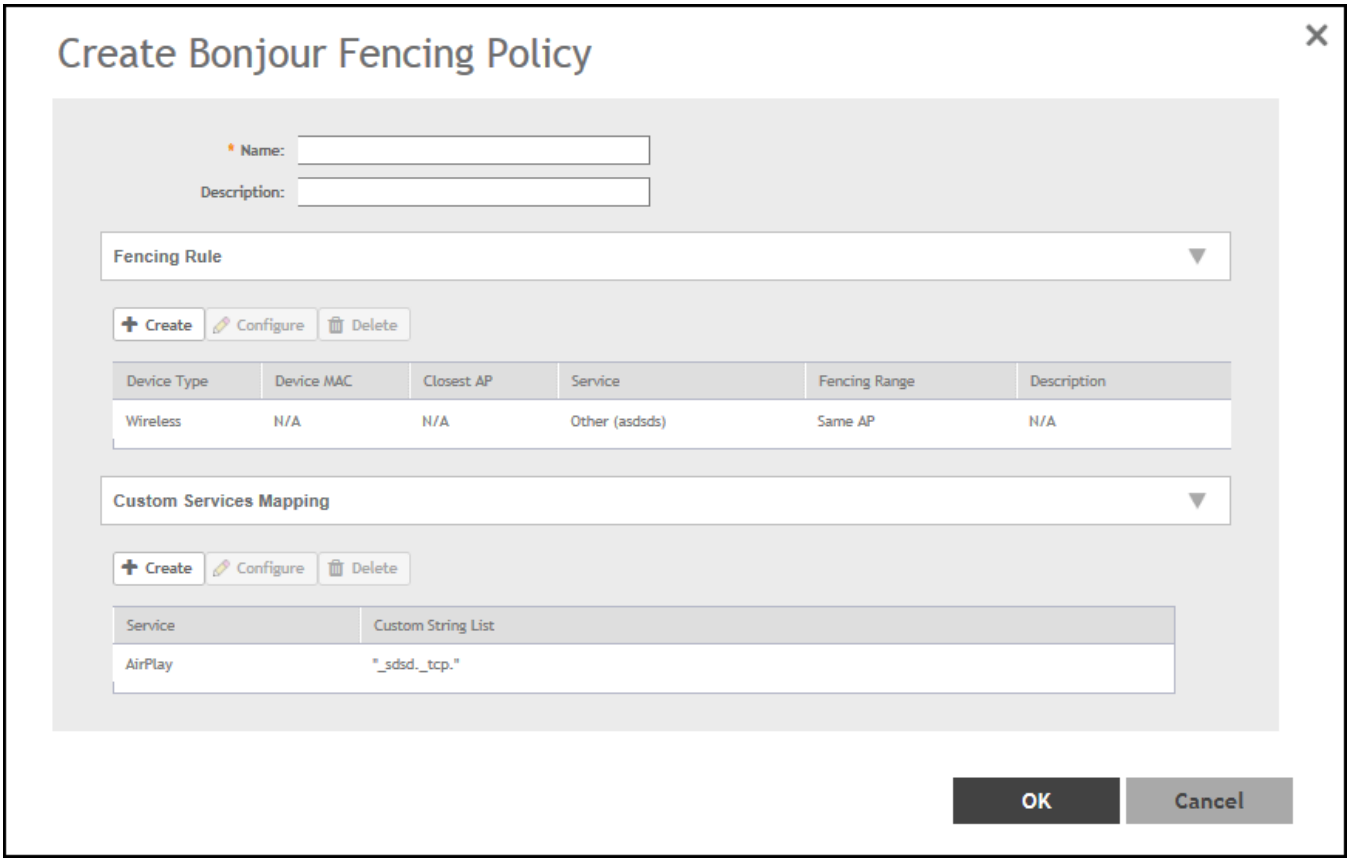
> **NOTE**
> Bonjour Fencing for a particular service does not work if another service from the same server, which is not fenced, is enabled simultaneously.

Complete the following steps to create a Bonjour Fencing policy.

1. From the main menu, 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** dialog box is displayed.

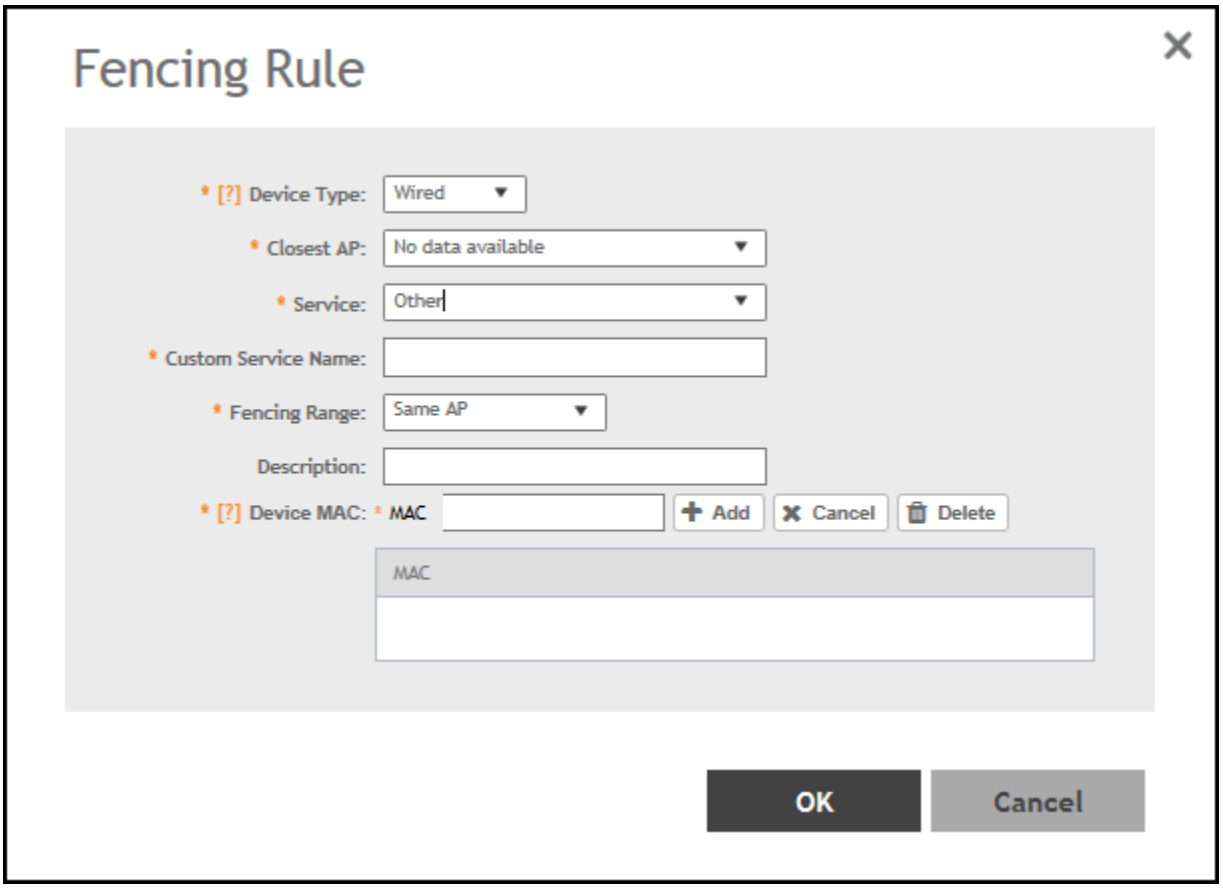
   FIGURE 108 Creating a Bonjour Fencing Policy



4. Configure the following options:
   - **Name**: Enter a name for the policy.
   - **Description**: Type a description for the policy.
   - **Fencing Rule**: Create the policy rule by configuring the following:

5. Under **Fencing Rule**, click **Create**. The **Fencing Rule** dialog box is displayed.

FIGURE 109 Creating a Fencing Rule



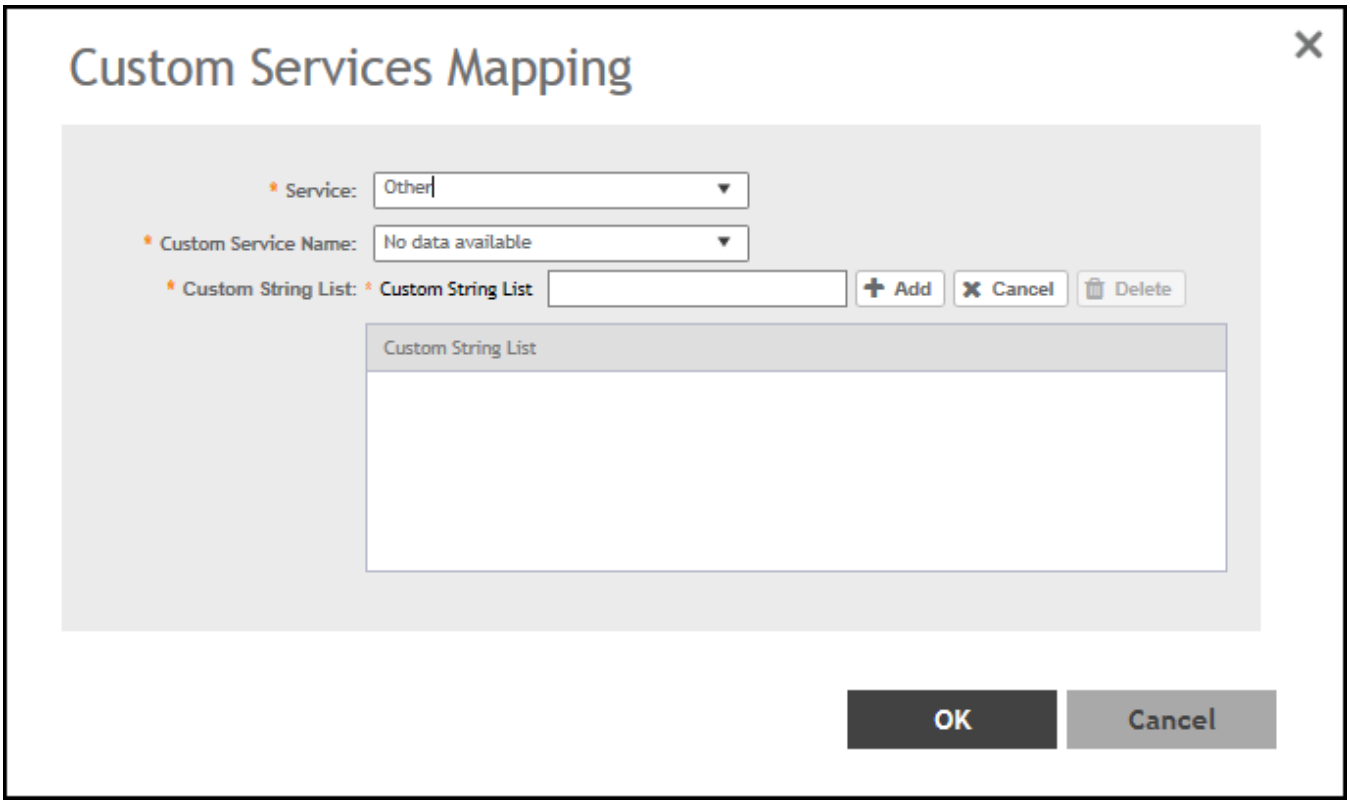
6. Configure the following options:
   - **Device Type**: Select **Wireless** or **Wired** network connection method for the device advertising Bonjour services.
   - **Closest AP**: Select the closest AP to create a physical anchor point for fencing; the closest AP is auto-detected for wireless devices, based on the AP association.
   - **Service**: Select one of the Bonjour services from the list. In SmartZone 5.0, two new services, **Chromecast** and **Other** were added. Chromecast behaves as the standard service. If you select **Other**, the custom service name that is used for service mapping is displayed. Regardless of the selected device type, only three services with the same custom service name can be created.
   - **Custom Service Name**: Enter a name for mapping services other than the custom services regardless of the device type. You can create a maximum of three services with the same custom service name.
   - **Fencing Range**: Select Same AP or 1-Hop AP Neighbors as the fencing range.
   - **Description**: Enter any description you may have for the fencing rule.
   - **Device MAC**: Enter the MAC address of the device advertising Bonjour services. This option is available only for the Wired device type; it supports up to four wired MAC addresses.
7. Click OK to save the Bonjour Fencing rule.

NOTE
Each policy can contain up to 32 rules.

8. Under **Custom Services Mapping**, click **Create**.

   The **Custom Services Mapping** dialog box is displayed.

   FIGURE 110 Creating a Custom Services Mapping



9. Configure the following options:
   - **Service**: Select one of the Bonjour services from the 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 the **Other** type has one entry with custom strings (three at most) because it allows three other rules.

   - This field is available only if you select the **Other** option from the **Service** list. **Custom Service Name** lists all the custom service names with the service type **Other** created in the fencing rule.
   - **Custom String List**: Enter the name of the string list in the format **_xxxx._xtcp** or **_xxxx._xudp**. You can create only one entry for Custom service and three entries for an **Other** service.
10. Click **OK** to save the services mapping policy.
11. Click **OK** to save the policy.

NOTE
You can also edit or delete the policy by selecting the **Configure** or **Delete** respectively, from the **Fencing** tab.

Quality of Service (QoS)

Quality of Service (QoS) classifies each traffic type entering a device into access category (Voice, Video, Best Effort or Background) and treats it with the priorities assigned to that access category.

> **NOTE**
> The order of precedence applied for QoS priority is Application Recognition and Control (ARC) (app-specific QoS) > QoS Map Set > SmartCast > MSCS > RUCKUS Unilateral. The ARC, QoS Map Set, and RUCKUS Unilateral features apply only when they are enabled. The SmartCast and MSCS features are enabled by default.

RUCKUS SmartCast™

RUCKUS SmartCast™ is a Quality of Service (QoS) engine that provides QoS classification and directed multicast features to maximize the reliability and performance of delay-sensitive applications, such as IP-based voice and video over 802.11 networks.

SmartCast provides packet inspection, automatic traffic classification, prioritization, advanced queuing, and scheduling.

Comprising the IEEE 802.11e/WMM hardware-based queuing standard, SmartCast is enabled by default on every RUCKUS access point and requires no GUI configuration.

Quality of Service (QoS) Mapping

When the QoS Map Set feature is enabled, the AP maps the DSCP of each packet to the user priority TID automatically before sending the packet to the wireless client. Beginning with release 7.0, SmartCast supports all 64 DSCP values and all 8 TID values (0-8), ensuring application of the appropriate access category queue (best effort, background, video, or voice) to each packet. The following table depicts how SmartCast handles DSCP to TID mapping.

TABLE 47 DSCP to TID Mapping

SmartCast (for SmartZone release until 6.1.2)				SmartCast (for SmartZone release 7.0 and onward)			
Access Category	**ToS (Hexadecimal)**	**DSCP (Decimal)**	**TID/UP**	**Access Category**	**ToS (Hexadecimal)**	**DSCP (Decimal)**	**TID/UP**
Voice	0xE0	56	6				
Voice	0xC0	48	6	**Voice**	0xC0 to 0xFC	48 to 63	7
Voice	0xB8	46	6	**Voice**	0xA8 to 0xBC	42 to 47	6
Video	0xA0	40	5	**Video**	0xA0 to 0xA4	40 to 41	5
Video	0x80	32	5	**Video**	0x5C to 0x9C	23 to 39	4
Best Effort (Data)	0x60	24	0	**Background**	0x44 to 0x40	17 to 22	3
Background	0x40	16	1	**Best Effort (Data)**	0x24 to 0x40	9 to 16	0
Background	0x20	8	1	**Background**	0x4 to 0x20	1 to 8	1
Best Effort (Data)	0x00	0	0	**Best Effort (Data)**	0x0	0	0

Quality of Service (QoS) Mirroring

The Quality of Service (QoS) Mirroring feature enables the AP to apply identical traffic priorities (Voice, Video, Best Effort or Background) to downlink flows so that they correspond to their respective uplink flows. Due to either deliberate or unintentional factors, downlink packets frequently lack priority markings. With QoS Mirroring, the AP gives precedence to real-time flows, such as voice, video conferencing, and gaming, over asynchronous flows like file downloads and movie streaming, in accordance with the associated upstream traffic flows within the WLAN.

The following QoS mirroring modes are implemented:

- Mirrored Stream Classification Service (MSCS) implemented as per IEEE standards
- RUCKUS Unilateral QoS mirroring implemented as a RUCKUS Proprietary

Mirrored Stream Classification Service

The Mirrored Stream Classification Service (MSCS) is a WI-FI CERTIFIED QoS Management™ technology that allows each client device to request the AP to assign priorities to specified downlink traffic flows, aligning the priorities with what the client initially assigned to the corresponding uplink traffic flows. In this operational mode, the client prompts the AP to initiate mirroring by sending the AP an MSCS request.

The AP performs QoS treatment for certain uplink IP flows that results in reduced latency and a better end-user experience with real-time applications. For example, a client can request that gaming traffic has a higher priority on the network than other traffic associated with watching streaming content or browsing the web. Even if there are other clients using the same network to the maximum, the game traffic is given the highest priority, resulting in reduced latency and a better gaming experience.

MSCS begins only when the downlink packet from the server is tagged as differentiated services code point (DSCP) 0x00 (in other words, the packet is not classified). The client devices use a dedicated frame exchange to trigger the MSCS process. The MSCS functionality works only for client devices that support MSCS.

RUCKUS Unilateral Mirroring

Unilateral Mirroring is an exclusive RUCKUS feature that provides QoS mirroring without requiring signaling between the AP and the client, extending the advantages of mirroring to legacy clients that lack support for MSCS. When QoS Mirroring is enabled for all clients, the AP automatically assigns an equivalent priority to each downlink flow for a legacy client, mirroring each of its flow with the priority of its corresponding uplink flow. Clients with MSCS support explicitly initiate mirroring by sending an MSCS request to the AP.

The Unilateral mirroring feature mirrors the downlink user priority (UP) or traffic identifier (TID) corresponding to its uplink UP/TID, and the AP does not expect any request from the station (STA). The AP mirrors uplink UP/TID to downlink UP/TID when the downlink packets from the server are DSCP 0x00. The client devices do not use a dedicated frame exchange to trigger the Unilateral QoS process. This mode supports both MSCS clients and non-MSCS clients.

WLAN Management

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:

- 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 Service Provider (MSP) manages and assumes a defined set of responsibilities. You can create an MSP managed domain, to manage all their settings within that domain.

> **NOTE**
> This feature is applicable only for RUCKUS SZ300 physical controller and Virtual SmartZone-High Scale (vSZ-H) platforms.

To create a WLAN Domain for an MSP, perform the following:

1. Click **Network** > **Wireless** > **Wireless LANs** .

   This displays **Wireless LANs** page.
2. Select **System** as parent group and click the **Create Domain/Zone/Group (+)** image button.

   This displays **Create Domain** page.

   FIGURE 111 Create MSP Domain

3. Enter the following details:
   a) Name: Type a name to identify the domain.
   b) Description: Enter a short description for the domain.
   c) Parent Group: Displays the selected parent group name.
   d) Managed by Partner: Click to enable the Managed Service Provider (MSP).
4. Click **OK**, the newly created MSP domain is displayed in the left pane.

Managing WLANs

This section explains how to maintain a robust wireless network for your organization.

On the Wireless LANs page select a system, domain, zone, or WLAN group from the hierarchy tree, respective contextual tabs appear at the bottom of the page. The tabs are used to monitor the selected group. The following table lists the tabs that appear for system, zone, and WLAN group.

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

Tabs	Description	System	Domain (Only for SZ300 and vSZ-H)	Zone	WLAN Groups
Configuration	Displays the respective configuration information.	Yes	Yes	Yes	Yes

TABLE 48 System, Domain, Zone, and WLAN Groups Monitoring Tabs (continued)

Tabs	Description	System	Domain (Only for SZ300 and vSZ-H)	Zone	WLAN Groups
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 (applicable only for SZ300 and vSZ-H)
- Extract a WLAN Template
- Apply a WLAN Template
- Change the AP Firmware
- Switch over a Cluster
- Trigger a preferred node (applicable only for SZ300 and vSZ-H)

NOTE
WLANs can be disabled or enabled at the AP. For more information, refer *Configuring Access Points*.

Moving a WLAN to a different WLAN Zone

You can move a wireless network from one zone to another.

NOTE
The WLAN that you move inherits the configuration of the new WLAN zone. This feature is applicable only for SZ300 and vSZ-H platforms.

To move a WLAN from its current WLAN zone to a different zone, perform the following:

1. Click **Network** > **Wireless** > **Wireless LANs**, and select the WLAN zone from the list to move another WLAN zone.
2. Click **More** and select **Move**.

   This displays the **Select Destination Management Domain** dialog box.
3. Select the destination WLAN zone and click **OK**.

   A confirmation message is displayed.
4. Click **Yes**.

   The WLAN is moved to the destination location.

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.

Complete the following steps to create a WLAN group.

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 269.

     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 **Create 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.

WLAN Configuration

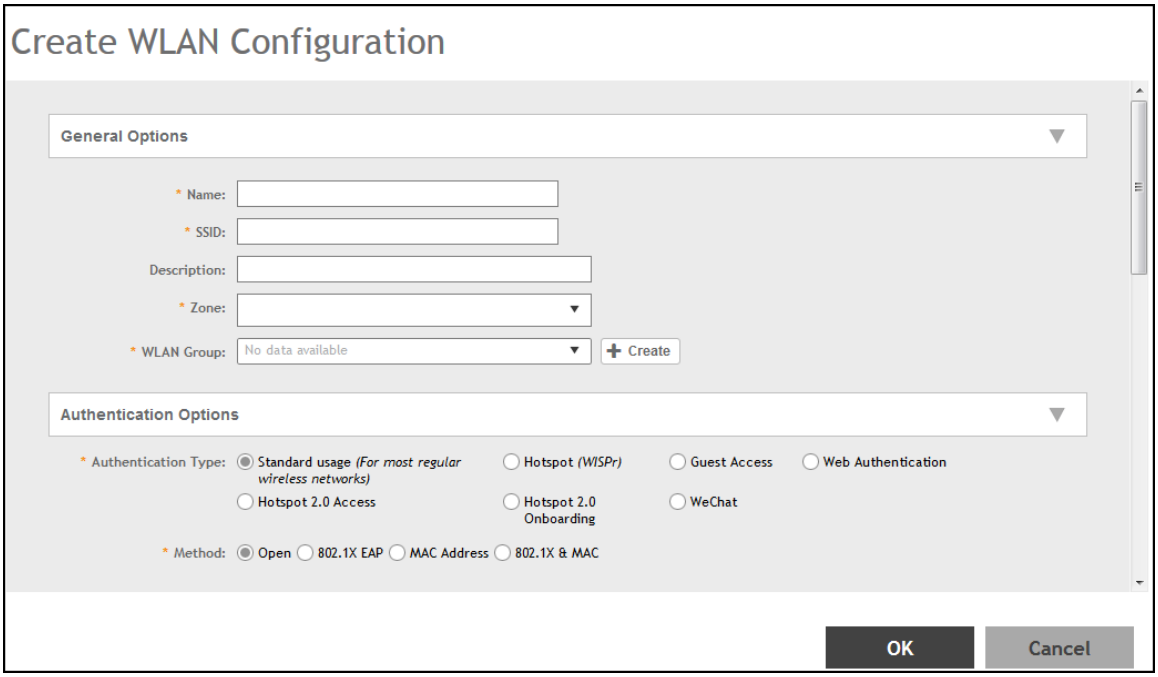
Creating a WLAN Configuration

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** to create a WLAN.
2. Click **Create**. The **Create WLAN Configuration** page is displayed.

FIGURE 112 Create WLAN Configuration Page



3. Set the required configurations as detailed in the following table.

TABLE 49 WLAN Configuration for SZ100 and vSZ-E

Field	Description	Your Action
General Options		
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 settings or function.	Enter a short description.
Zone	Indicates the zone to which the WLAN belongs.	Select the zone to which the WLAN settings apply.
WLAN Group	Indicates the WLAN groups to which the WLAN applies.	Select the WLAN groups.
Authentication Options		

TABLE 49 WLAN Configuration for SZ100 and vSZ-E (continued)

Field	Description	Your Action
Authentication Type	Defines the type of authentication flow for the WLAN. **NOTE** Authentication types such as Web Authentication, and Guest Access except WeChat are 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, refer to 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. Refer to 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. Refer to 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.

TABLE 49 WLAN Configuration for SZ100 and vSZ-E (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) also 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. ● **MAC Address**—Authenticates 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.

TABLE 49 WLAN Configuration for SZ100 and vSZ-E (continued)

Field	Description	Your Action
		• **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 passes, 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.
Reserve SSID	The Reserve SSID is broadcasted in case the AP loses its SSH Control connection to the controller, or Dataplane if it is tunneling traffic. The Reserve SSID will typically become operational within 3 minutes, depending upon when the lost heartbeat is detected. This allows Open, WPA2/WPA3, WPA2/WPA3 mixed or WPA-mixed mode to be used as back up SSID. Reserve SSID is limited to only one WLAN per Zone.	By default it is disabled.
Encryption Options		
Method	Specifies the encryption method. WPA, WPA2, WPA3, WPA2/WPA3-Mixed and OWE (Opportunistic Wireless Encryption) are the encryption methods certified by the Wi-Fi Alliance; WPA2, WPA3, WPA2/WPA3-Mixed and OWE 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. Choose the following: – **AES**: a. Enter **PassPhrase**. b. Select or clear **Show**. c. Select the **Enable 802.11r Fast BSS Transition** check box and enter the **Mobility Domain ID**. d. Select the required **802.11w MFP** option. – **AUTO**: a. Enter **Passphrase**. b. Enter **SAE Passphrase** c. Select or clear **Show**.

TABLE 49 WLAN Configuration for SZ100 and vSZ-E (continued)

Field	Description	Your Action
		• **WPA3**—Enhanced WPA3 encryption using AES encryption algorithm. Enable this option for 6G radio. Choose the **Algorithm**: – **AES**: a. Enter **Passphrase**. b. Select or clear **Show** c. 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** - Allows mixed networks of WPA2 and WPA3-compliant devices using AES algorithm. By default the **Algorithm** is **AES** – a. Enter **Passphrase** b. Enter **SAE Passphrase** c. Select or clear **Show** d. Select **802.11r Fast Roaming** toggle button. If **On**, enter the **Mobility Domain ID**. e. In the **802.11w MFP** field, select **Capable** or **Required** options. f. In the **DPSK3** , toggle button **On** - no need to configure passphrase or SAE passphrase. The DPSK sets as external at both intermediate and service WLAN. **Off** - Enter the Passphrase and SAE Passphrase. g. In the **Transition Disable Indication**, toggle button, if the **DPSK3** is enabled then by default, this option is **On**. When this option is enabled, the WiFi client connected to this AP should use the most secure algorithm that the client supports to associate with the AP. If the **DPSK3** is **Off** client has the option to connect with WPA2/WPA3 security protocol by enabling this option.

TABLE 49 WLAN Configuration for SZ100 and vSZ-E (continued)

Field	Description	Your Action
		• **Opportunistic Wireless Encryption(OWE)** - Allows the encryption without the manual input the passphrase using AES algorithm. Enable this option for 6G radio. Choose the **Algorithm** – **AES**: In the **802.11w MFP** field, " Required" is the default selected option.
		Opportunistic Wireless Encryption(OWE) - Transition - Allows the AP to create two WLANs. One is **OPEN** WLAN and another is **OWE** WLAN with SSID.
		• **WPA-Mixed**—Allows mixed networks of WPA- and WPA2-compliant devices. Use this setting if your network has a mixture of older clients that only support WPA and TKIP, and newer client devices that support WPA2 and AES. a. Choose **Algorithm**: **AES** or **AUTO** b. Enter **PassPhrase**. c. Select or clear **Show**. d. Select **Enable 802.11r Fast BSS Transition**. e. Enter the **Mobility Domain ID**
		• **None**
Reserve SSID	Is a limited to only one WLAN per Zone. The Reserve SSID option is displayed only when standard + open + (WPA2/ WPA3 or WPA2/ WPA3-Mixed or WPA mixed is enabled.	By default it is disabled.
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. **NOTE** RuckusGRE or SoftGRE must be enabled on the WLAN before mapping it to a Split Tunnel Profile.
vSZ-D DHCP/NAT	Enables tunneling option for DHCP/NAT.	Select the required check boxes: • **Enable Tunnel NAT** • **Enable Tunnel DHCP**

TABLE 49 WLAN Configuration for SZ100 and vSZ-E (continued)

Field	Description	Your Action
RADIUS based DHCP/NAT	Enables RADIUS-based DHCP/NAT settings. 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**
Authentication & Accounting Server (for WLAN **Authentication Type**: **Standard**)		
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. Beginning with SmartZone 7.0.0, the **User controller as proxy** option can be disabled to allow non-proxy AAA service. b. Select the server from the menu. c. Select the **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.
Authentication Server	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 Controller as Proxy** check box. 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** For WISPr survivability, the customer portal must use the AP WISPr ZD-Style API/Backup AAA authentication to continue the WISPr service.

TABLE 49 WLAN Configuration for SZ100 and vSZ-E (continued)

Field	Description	Your Action
Accounting Server	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. 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** For WISPr survivability, the customer portal must use the AP WISPr ZD-Style API/Backup AAA authentication to continue the WISPr service.
Guest Access Portal (for WLAN **Authentication Type**: **Guest Access**)		
Guest Portal 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.
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 be authenticated.
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.
Authentication & Accounting Server (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 drop-down menu.
Bypass CNA	Bypasses the Apple CNA feature on iOS and OS X devices that connect to this WLAN.	Select the **Enable** check box.
Authentication Server	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 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.
Hotspot 2.0 Profile (for WLAN **Authentication Type**: **Hotspot 2.0 Access**)		
Hotspot 2.0 Profile	Indicates the profile, which includes operator and identify provider profiles.	Choose the profile.

TABLE 49 WLAN Configuration for SZ100 and vSZ-E (continued)

Field	Description	Your Action
Authentication Server RFC 5580	Supports RFC 5580 location delivery on the WLAN, which carries location information in RADIUS exchanges.	Select the check box.
Accounting Server Updates	Indicates the frequency to send interim updates. Configure 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.
Wireless Client Isolation		
Client Isolation	Prevents wireless clients from communicating with each other. By default this option is disabled.	Enable **Client Isolation** to separate wireless client traffic from all hosts on the same VLAN/subnet. When **Client Isolation** is enabled the below options are available to enable or disable as appropriate: • **Isolate unicast packets:** Isolates only unicast packets between a client isolation-enabled WLAN and other clients of the AP. • **Isolate multicast/broadcast packets:** By default, this option is disabled, when enabled, only multicast packets between a client isolation and other clients of the AP are separated. • **Automatic support for VRRP/HSRP:** By default, this option is disabled, when enabled, allows you to have isolation without adding physical MAC addresses of VRRP/HSRP routers. Client isolation only discovers virtual IP and MAC in VRRP/HSRP.
Isolation Whitelist	Isolation whitelist allows you to manually specify a list of **MAC** and **IP Addresses** that override the blocked list.	Click on the **Add** icon corresponding to the field to manually enter the MAC and IP addresses to the isolation whitelist. **NOTE** Specify a default gateway that splits IP address into the host and network addresses in the whitelist.
RADIUS Option		

TABLE 49 WLAN Configuration for SZ100 and vSZ-E (continued)

Field	Description	Your Action
NAS ID	Defines the ID sent to the RADIUS server, which will identify the AP.	Choose the option: • **WLAN BSSID** • **AP MAC** • **User-defined**
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** • **NONE**
Single Session ID Accounting	Enabling this feature 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 statistics are also reset, essentially resetting the accounting.	Select the **Enable** check box to use this feature.
NAS IP	Indicates the NAS IP address.	Select the option: • **Disabled** • **SZ Control IP** • **SZ Management IP** • **User-defined**

TABLE 49 WLAN Configuration for SZ100 and vSZ-E (continued)

Field	Description	Your Action
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. c. Select the **L2 Access Control Policy** from the drop-down list or click to create a new policy. d. Select the **Application Policy** from the drop-down list or click to create a new policy. e. Select the **URL Filtering Profile** from the drop-down list or click to create a new profile. f. Select the **Device Policy** from the drop-down list or click to create a new policy.
Application Recognition and Control (ARC)	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.

TABLE 49 WLAN Configuration for SZ100 and vSZ-E (continued)

Field	Description	Your Action
Advanced Options		
BSS Priority	Determines the traffic transmit preference of one WLAN compared to another. Traffic for the high priority WLANs are always sent before the low priority WLANs in the same QoS category (background, best effort, video, voice).	Choose the priority: • **High**—Enabled by default. • **Low**
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.
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**.
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 Onboarding 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 you toggle the switch to **OFF** (enabled by default).	Click the **Client Load Balancing** toggle switch to **OFF** to disable this feature.
Proxy ARP	Enables proxy ARP. When proxy ARP is enabled on a WLAN, the AP provides proxy service for stations when receiving neighbor discovery packets (for example, ARP request and ICMPv6 Neighbor Solicitation messages), and acts on behalf of the station in delivering ARP replies. When the AP receives a broadcast ARP/Neighbor Solicit request for a known host, the AP replies on behalf of the host. If the AP receives a request for an unknown host, it forwards the request.	Select the check box.
DGAF	Disables AP from forwarding downstream group-addressed frames. This option is available only when proxy ARP is enabled.	Select the option.
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 802.11d is helpful for many devices that cannot independently determine their operating country.	Select the check box to enable this option.

TABLE 49 WLAN Configuration for SZ100 and vSZ-E (continued)

Field	Description	Your Action
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.	Select the check box.
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 are automatically enabled with default values (in packets per minute, or ppm) that 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 to which 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.

TABLE 49 WLAN Configuration for SZ100 and vSZ-E (continued)

Field	Description	Your Action
DHCP Option 82	Enables an AP to encapsulate additional information (such as VLAN ID, AP name, SSID, and MAC address) into the DHCP request packets before forwarding them to the DHCP server. The DHCP server can then use this information to allocate an IP address to the client from a particular DHCP pool based on these parameters.	Select the option.
DHCP Option 82 Format	Enables an AP to encapsulate additional information (such as VLAN ID, AP name, SSID, MAC address, IF name, AP model, Location, Privacy type and Area name) into the DHCP request packets before forwarding them to the DHCP server. The DHCP server can then use 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. • **Subopt-2 with format** and select the option. • **Subopt-150 with VLAN-ID**. • **Subopt-151 with format** and select the option.
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.
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 APs' 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.
Inactivity Timeout	Indicates the duration after which idle clients will be disconnected.	Enter the duration. Range: 60 through 86400 seconds

TABLE 49 WLAN Configuration for SZ100 and vSZ-E (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 (SSID).	Enter the duration. Range: 120 to 864000 seconds (10 days). Default Value: 172800 seconds (2 days). **NOTE** The 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.
WiFi 6/7	Controls how the Wi-6/7 AP radios operate to support clients of various capabilities on a specific WLAN. By default, this feature enabled (**ON**), allowing Wi-Fi 6/7 client devices and legacy Wi-Fi 5 client devices to interoperate with the Wi-Fi 6/7 APs and utilize Wi-Fi 6/7 features (such as OFDMA, TWT, 6GHz operation, Preamble Puncturing, 320MHz bandwidth, and MLO) available on the WLAN. When disabled (**OFF**), the Wi-Fi 6/7 APs are downgraded to support Wi-Fi 4/5 capabilities. This allows Wi-Fi 6/7 and legacy client devices to interoperate with the Wi-Fi 6/7 APs on the WLAN; however, the Wi-Fi 6/7 features are not available for use. Disabling this feature is recommended when client drivers are not up to date or if the client device drivers have bugs Refer to Wi-Fi 6 or Wi-Fi 7 Support on page 317 for further feature information and the Wi-Fi support matrix. **NOTE** From releases 5.2.1 through 6.1.2, this option was labeled as Wi-Fi 6. Beginning with release 7.0.0, this option is renamed as Wi-Fi 6/7.	Default setting: Enabled (toggled **ON**). Click the toggle button to **OFF** to downgrade the Wi-Fi 6/7 AP functionality, allowing support for Wi-Fi 6/7 and legacy client devices.
MLO (Multi Link Operation)	Allows client devices to seamlessly associate across multiple bands and facilitates smooth switch between these links. The Multi-Link Operation (MLO) feature enhances peak throughput by efficiently sending packets from the same flow across multiple links. It also minimizes latency due to increased channel access opportunities through these multiple links. Furthermore, it enables swift and seamless traffic routing based on channel capacity for load balancing without the need for disassociation and reassociation.	Default radio frequency: 2.4GHz + 5GHz You can also select a combination of two radio frequency. For example, 2.4 GHz + 5 GHz, 2.4 GHz + 6 GHz or 5 GHz + 6 GHz.

TABLE 49 WLAN Configuration for SZ100 and vSZ-E (continued)

Field	Description	Your Action
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 option.
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 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
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 checked 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 controller and AP using 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.

TABLE 49 WLAN Configuration for SZ100 and vSZ-E (continued)

Field	Description	Your Action
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.	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 **Uplink** and **Downlink** check boxes and enter the limiting rates in mbps respectively. Range: 1 mbps through 1000 mbps.
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 percent of the traffic, a maximum of 3.00Mbps to 4.00Mbps traffic passes per second. 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 drop-down menu. Select Disable from the drop-down 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.

TABLE 49 WLAN Configuration for SZ100 and vSZ-E (continued)

Field	Description	Your Action
DNS Spoofing Profile	When an AP receives a DNS packet all the fields in the packet are validated. **NOTE** Only A/AAAA DNS query packets are considered. When same domain name is present in both DNS spoofing profile and walled garden table in WISPr WLAN then AP DNS cache is updated with the IP address present in the DNS spoofing profile. If DNS spoof and URL filtering with safe search is enabled, URL filtering(safe search) takes the precedence for "goggle", "You Tube", "Bing" domain names. If safe search is not enabled, DNS-Spoof 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 drop-down menu. Select Disable from the drop-down 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.
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 required option. Click to add a new profile or click to edit a profile.
Client Flow Data Logging	Sends a log message with source MAC, destination MAC, source IP, destination IP, source port, destination port, L4 protocol, and AP MAC of each packet session to the external syslog server. This function is provided by the AP syslog client (not the controller 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 the **Enable Transient Client Management** check box 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.

TABLE 49 WLAN Configuration for SZ100 and vSZ-E (continued)

Field	Description	Your Action
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.
AP Host Name Advertisement in Beacon	AP host name is included in beacon. By default this feature is disabled.	Enable this option to view the AP host name.
QOS Mirroring	This feature allows an AP to use a client's uplink Quality of Service (QoS) classification (Voice, Video, Best Effort or Background) to classify the client device's downlink packets in the mirrored (reverse direction) stream. The AP assigns the downlink packets to the same QoS category as the uplink packets.	• **Disabled** - QoS mirroring is disabled for all the clients. • **Enabled via Protocol** - QoS mirroring is enabled only for clients that send Mirrored Stream Classification Service (MSCS) requests. Legacy clients are not supported with QoS preference. This is the default setting. • **Enabled for All** - Unilateral mirroring is applied for this option and QoS mirroring is enabled for all the clients.

TABLE 50 WLAN Configuration for SZ300 and vSZ-H

Field	Description	Your Action
General Options		
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		

TABLE 50 WLAN Configuration for SZ300 and vSZ-H (continued)

Field	Description	Your Action
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.

TABLE 50 WLAN Configuration for SZ300 and vSZ-H (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 passes, 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 50 WLAN Configuration for SZ300 and vSZ-H (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.	• **WPA2/WPA3-Mixed** - Allows mixed networks of WPA2 and WPA3-compliant devices using AES algorithm. By default the **Algorithm** is **AES** – a. Enter **Passphrase** b. Enter **SAE Passphrase** c. Select or clear **Show** d. Select **802.11r Fast Roaming** toggle button. If **On**, enter the **Mobility Domain ID**. e. In the **802.11w MFP** field, select **Capable** or **Required** options. f. In the **DPSK3** , toggle button **On** - no need to configure passphrase or SAE passphrase. The DPSK sets as external at both intermediate and service WLAN. **Off** - Enter the Passphrase and SAE Passphrase. g. In the **Transition Disable Indication**, toggle button, if the **DPSK3** is enabled then by default, this option is **On**. When this option is enabled, the WiFi client connected to this AP should use the most secure algorithm that the client supports to associate with the AP. If the **DPSK3** is **Off** client has the option to connect with WPA2/WPA3 security protocol by enabling this option.
		• **Opportunistic Wireless Encryption (OWE)** - Allows the encryption without the manual input the passphrase using AES algorithm. Enable this option for 6G radio. a. Choose **Algorithm** – **AES**: In the **802.11w MFP** field, " Required" is the default selected option. • **WPA-Mixed**—Allows mixed networks of WPA- and WPA2-compliant devices. Use this setting if your network has a mixture of older clients that only support WPA and TKIP, and newer client devices that support WPA2 and AES. a. Choose **Algorithm**: **AES** or **AUTO**. b. Enter **Passphrase**. c. Select or clear **Show**. d. Select **Enable 802.11 Fast BSS Transition**. e. Enter the **Mobility Domain ID**. f. **Dynamic PSK** – **Disable** – **Internal** 1. Enter **DPSK Length** 2. Choose **DPSK Type** 3. Select **DPSK Expiration** – **External**—Enables **Authentication Service** • **None**
		Opportunistic Wireless Encryption(OWE) - Transition - Allows the AP to create two WLANs. One is **OPEN** WLAN and another is **OWE** WLAN SSID.

TABLE 50 WLAN Configuration for SZ300 and vSZ-H (continued)

Field	Description	Your Action
Reserve SSID	The Reserve SSID is broadcasted in case the AP loses its SSH Control connection to the controller or Dataplane if it is tunneling traffic. The Reserve SSID will typically become operational within 3 minutes, depending upon when the lost heartbeat is detected. This allows Open, WPA2/WPA3, WPA2/WPA3 mixed or WPA-mixed mode to be used as back up SSID. Reserve SSID is limited to only one WLAN per Zone.	By default it is disabled.
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 approved, the controller limits the 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. Beginning with SmartZone 7.0.0, the **User controller as proxy** option can be disabled to allow a non-proxy AAA service. b. Select the server from the menu. c. Select **Enable RFC Location Delivery Support**.

TABLE 50 WLAN Configuration for SZ300 and vSZ-H (continued)

Field	Description	Your Action
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.
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.

TABLE 50 WLAN Configuration for SZ300 and vSZ-H (continued)

Field	Description	Your Action
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.
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.
Wireless Client Isolation		

TABLE 50 WLAN Configuration for SZ300 and vSZ-H (continued)

Field	Description	Your Action
Client Isolation	Prevents wireless clients from communicating with each other.	Enable **Client Isolation** to separate wireless client traffic from all hosts on the same VLAN/subnet. When client isolation is enabled the below options are available to enable or disable as appropriate: ● **Isolate unicast packets:** Isolates only unicast packets between a client isolation-enabled WLAN and other clients of the AP. ● **Isolate multicast/broadcast packets:** By default, this option is disabled, when enabled, only multicast packets between a client isolation and other clients of the AP are separated. ● **Automatic support for VRRP/HSRP:** By default, this option is disabled, when enabled, allows you to have isolation without adding physical MAC addresses of VRRP/HSRP routers. Client isolation only discovers virtual IP and MAC in VRRP/HSRP.
Isolation Whitelist	Isolation whitelist allows you to manually specify a list of **MAC** and **IP Addresses** that override the blocked list.	Click on the **Add** icon corresponding to the field to manually enter the MAC and IP addresses to the isolation whitelist. **NOTE** Specify a default gateway that splits IP address into the host and network addresses in the whitelist.
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**
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** ● **NONE**

TABLE 50 WLAN Configuration for SZ300 and vSZ-H (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. c. Select the **L2 Access Control Policy** from the drop-down list or click to create a new policy. d. Select the **Application Policy** from the drop-down list or click to create a new policy. e. Select the **URL Filtering Profile** from the drop-down list or click to create a new profile. f. Select the **Device Policy** from the drop-down list or click to create a new policy.
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.

TABLE 50 WLAN Configuration for SZ300 and vSZ-H (continued)

Field	Description	Your Action
Client Virtual ID Extraction	Extracts the Virtual IDs of the users who login into the social media , public email such as WeChat, Whats App, 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		
BSS Priority	Determines the traffic transmit preference of one WLAN compared to another. Traffic for the high priority WLANs are always sent before the low priority WLANs in the same QoS category (background, best effort, video, voice).	Choose the priority: • **High**—Enabled by default. • **Low**
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.
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**.
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 Onboarding 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 you toggle the switch to **OFF** (enabled by default).	Click the **Client Load Balancing** toggle switch to **OFF** to disable this feature.
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.
DGAF	Disables AP from forwarding downstream group-addressed frames. This option is available only when proxy ARP is enabled.	Select the option.

TABLE 50 WLAN Configuration for SZ300 and vSZ-H (continued)

Field	Description	Your Action
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 50 WLAN Configuration for SZ300 and vSZ-H (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 50 WLAN Configuration for SZ300 and vSZ-H (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 50 WLAN Configuration for SZ300 and vSZ-H (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 : – **AP-MAC** – **AP-MAC ESSID** – **AP-NAME ESSID** ● **Subopt-2 with format** and select the option. The options are: – **Client-MAC** – **AP-MAC** – **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.
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.

TABLE 50 WLAN Configuration for SZ300 and vSZ-H (continued)

Field	Description	Your Action
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.
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 6/7	Controls how the Wi-6/7 AP radios operate to support clients of various capabilities on a specific WLAN. By default, this feature enabled (**ON**), allowing Wi-Fi 6/7 client devices and legacy Wi-Fi 5 client devices to interoperate with the Wi-Fi 6/7 APs and utilize Wi-Fi 6/7 features (such as OFDMA, TWT, 6GHz operation, Preamble Puncturing, 320MHz bandwidth, and MLO) available on the WLAN. When disabled (**OFF**), the Wi-Fi 6/7 APs are downgraded to support Wi-Fi 4/5 capabilities. This allows Wi-Fi 6/7 and legacy client devices to interoperate with the Wi-Fi 6/7 APs on the WLAN; however, the Wi-Fi 6/7 features are not available for use. Disabling this feature is recommended when client drivers are not up to date or if the client device drivers have bugs Refer to Wi-Fi 6 or Wi-Fi 7 Support on page 317 for further feature information and the Wi-Fi support matrix. **NOTE** From releases 5.2.1 through 6.1.2, this option was labeled as Wi-Fi 6. Beginning with release 7.0.0, this option is renamed as Wi-Fi 6/7.	Default setting: Enabled (toggled **ON**). Click the toggle button to **OFF** to downgrade the Wi-Fi 6/7 AP functionality, allowing support for Wi-Fi 6/7 and legacy client devices.

TABLE 50 WLAN Configuration for SZ300 and vSZ-H (continued)

Field	Description	Your Action
MLO (Multi Link Operation)	Allows client devices to seamlessly associate across multiple bands and facilitates smooth switch between these links. The Multi-Link Operation (MLO) feature enhances peak throughput by efficiently sending packets from the same flow across multiple links. It also minimizes latency due to increased channel access opportunities through these multiple links. Furthermore, it enables swift and seamless traffic routing based on channel capacity for load balancing without the need for disassociation and reassociation.	Default radio frequency: 2.4GHz + 5GHz You can also select a combination of two radio frequency. For example, 2.4 GHz + 5 GHz, 2.4 GHz + 6 GHz or 5 GHz + 6 GHz.
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
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

TABLE 50 WLAN Configuration for SZ300 and vSZ-H (continued)

Field	Description	Your Action
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 controller 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 1000 Mbps. **NOTE** Rate limit supports maximum of 100 clients per WLAN per radio. After the threshold, the system displays client failure (203) error.

TABLE 50 WLAN Configuration for SZ300 and vSZ-H (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%, .for example. 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, URL filtering (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 50 WLAN Configuration for SZ300 and vSZ-H (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, the controller limits the user to use the CALEA feature.
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 controller 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.

TABLE 50 WLAN Configuration for SZ300 and vSZ-H (continued)

Field	Description	Your Action
QOS Mirroring	This feature allows an AP to use a client's uplink Quality of Service (QoS) classification (Voice, Video, Best Effort or Background) to classify the client device's downlink packets in the mirrored (reverse direction) stream. The AP assigns the downlink packets to the same QoS category as the uplink packets.	• **Disabled** - QoS mirroring is disabled for all the clients. • **Enabled via Protocol** - QoS mirroring is enabled only for clients that send Mirrored Stream Classification Service (MSCS) requests. Legacy clients are not supported with QoS preference. This is the default setting. • **Enabled for All** - Unilateral mirroring is applied for this option and QoS mirroring is enabled for all the clients.

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.

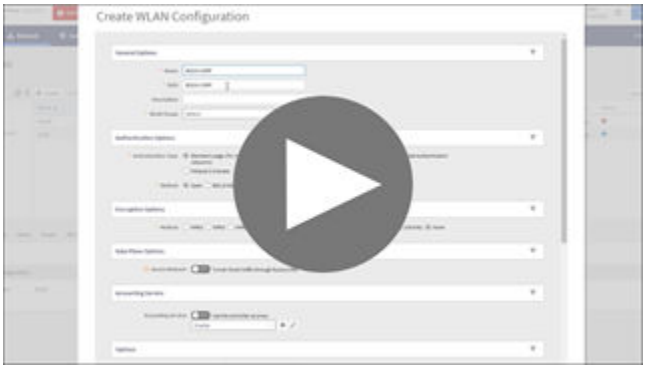
NOTE
You can edit, clone, and delete WLANs by selecting the options **Configure**, **Clone**, and **Delete** respectively, from the **Wireless LANs** page.

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.

VIDEO
Creating 802.1X WLAN. 802.1X WLAN Configuration.



Click to play video in full screen mode.

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 51 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

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.

WLAN Types

External DPSK without having a proxy RADIUS

Creating a User Role with Active Directory Authentication

Configuring user roles using AD authentication provides broad range of directory-based identity-related services.

To create a User Role with AD authentication:

1. Create a new UTP for a particular Role. Refer to Create an L3 Access Control Policy on page 237.
2. Create a role. Refer to *User Roles* in *RUCKUS SmartZone Access and Security Services Guide*.
3. **NOTE**
   Non-proxy Auth servers are not supported.

   Create a new Proxy AD server and apply the UTP. Refer to *Creating Proxy Authentication AAA Servers* in *RUCKUS SmartZone Access and Security Services Guide*.
4. **NOTE**
   In step 4 of the authentication test, for the **Service Protocol** option, choose **Active Directory** and proceed.

   Perform an authentication test to ensure that the user gets assigned the correct Role. Refer to *Testing AAA Servers* in *RUCKUS SmartZone Access and Security Services Guide*.
5. Create a web authentication portal WLAN configuration and assign the Non-proxy AD server to it. Refer to *RUCKUS SmartZone Network Administration Guide*.
   a) Choose **WLAN Usage** > **Authentication Type** > **Web Authentication**.
   b) Configure the following for **Authentication & Accounting Server**:

      Web Authentication Portal: Choose the option from the drop-down.

      Authentication Server: Select the Use the Controller Proxy check box and choose the authentication service from the drop-down.

Encryption Options

WPA3 R3 Support

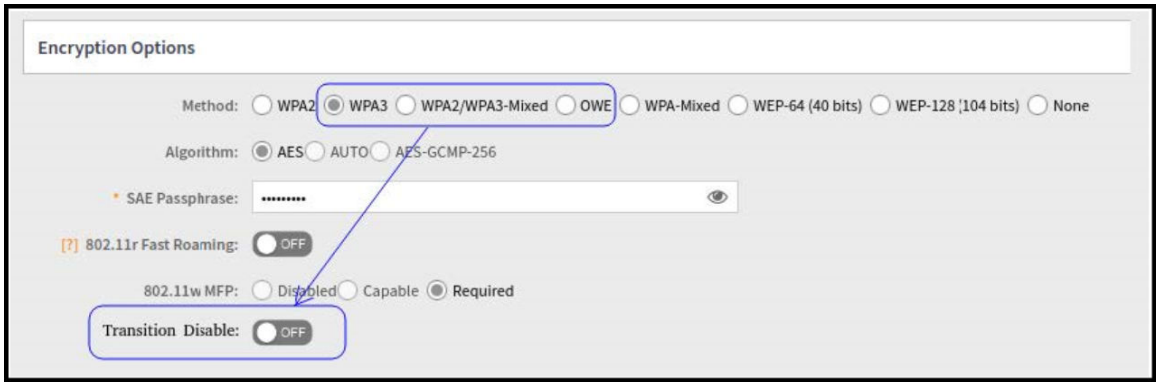
SAE Hash to Element (H2E)

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

Tansition 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.

Wireless Services

Configuring Traffic Analysis Display for WLANs

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

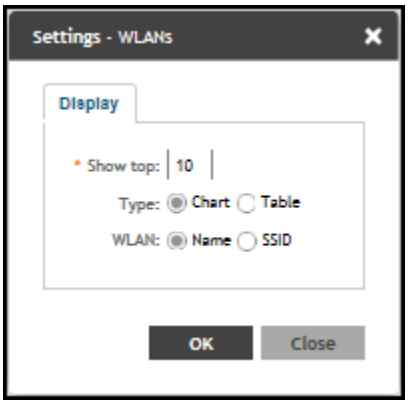
You can view historical and real-time data of the WLANs. Throughput and the number of clients connected to the WLANs are displayed in a bar chart. You must configure the WLAN settings to view its traffic analysis.

Complete the following steps to configure the WLAN settings.

1. From the WLAN area, click settings .

   The WLAN settings form displays.

   FIGURE 113 WLAN Settings Form



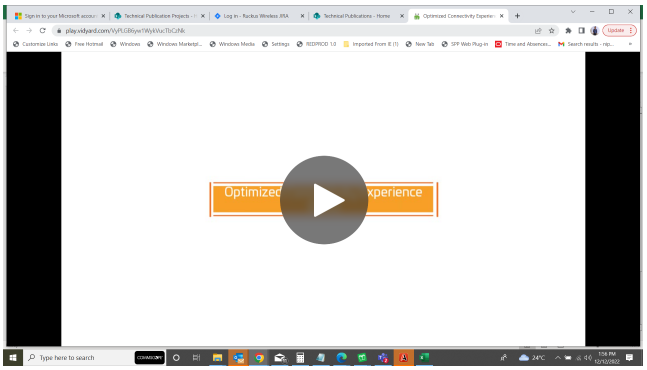
2. In the **Show top** box, enter the number of WLANs for which the traffic must be analyzed. Range: 5 through 20.
3. Select the **Type** radio button for the type of display you want to view. The choices are **Chart** or **Table**.
4. Select the **WLAN** identification option to be displayed. The choices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

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.

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.

Multicast Rate Filter

All the controller managed APs support this feature. The GUI for rate limit control is designed as:

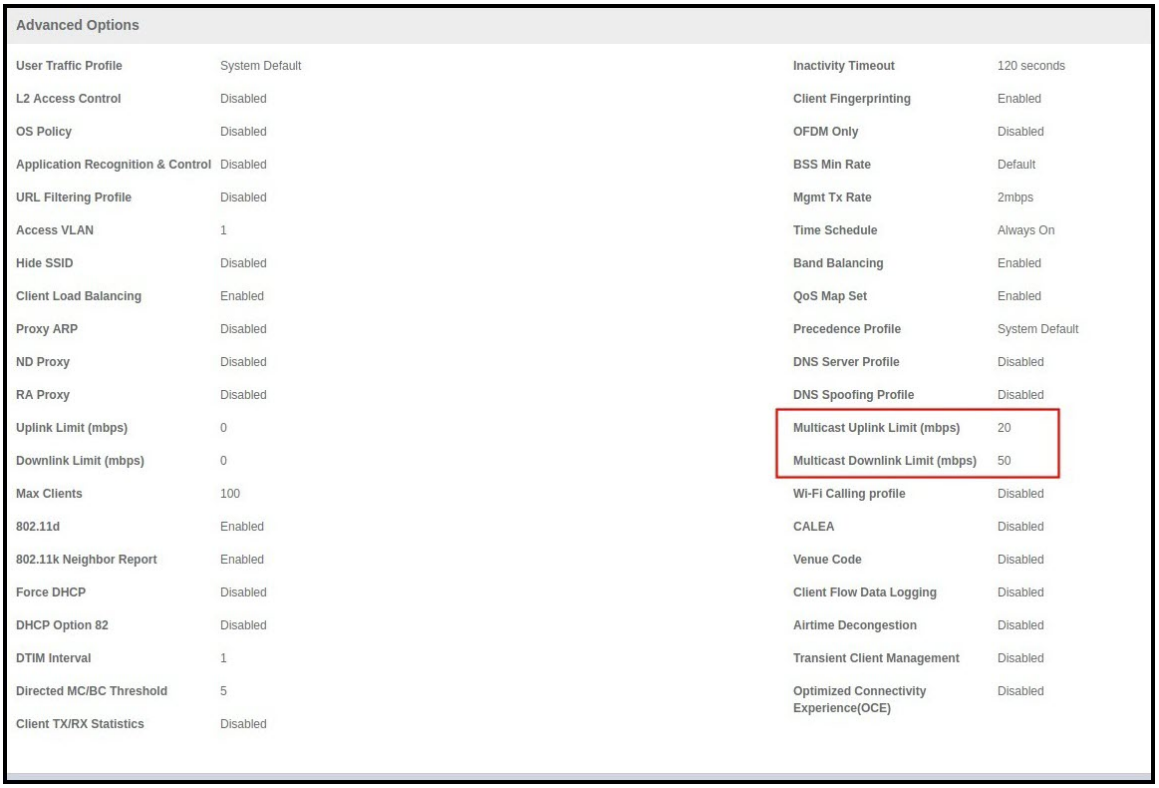
- **FIGURE 114** Multicast Rate Limiting

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 115 Configuring the Multicast Rate Limit



Advanced Options

User Traffic Profile	System Default	Inactivity Timeout	120 seconds
L2 Access Control	Disabled	Client Fingerprinting	Enabled
OS Policy	Disabled	OFDM Only	Disabled
Application Recognition & Control	Disabled	BSS Min Rate	Default
URL Filtering Profile	Disabled	Mgmt Tx Rate	2mbps
Access VLAN	1	Time Schedule	Always On
Hide SSID	Disabled	Band Balancing	Enabled
Client Load Balancing	Enabled	QoS Map Set	Enabled
Proxy ARP	Disabled	Precedence Profile	System Default
ND Proxy	Disabled	DNS Server Profile	Disabled
RA Proxy	Disabled	DNS Spoofing Profile	Disabled
Uplink Limit (mbps)	0	Multicast Uplink Limit (mbps)	20
Downlink Limit (mbps)	0	Multicast Downlink Limit (mbps)	50
Max Clients	100	Wi-Fi Calling profile	Disabled
802.11d	Enabled	CALEA	Disabled
802.11k Neighbor Report	Enabled	Venue Code	Disabled
Force DHCP	Disabled	Client Flow Data Logging	Disabled
DHCP Option 82	Disabled	Airtime Decongestion	Disabled
DTIM Interval	1	Transient Client Management	Disabled
Directed MC/BC Threshold	5	Optimized Connectivity Experience(OCE)	Disabled
Client TX/RX Statistics	Disabled		

User can check multicast uplink and downlink fields in WLAN preview.

FIGURE 116 WLAN Preview

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.

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 117 Load Balancing

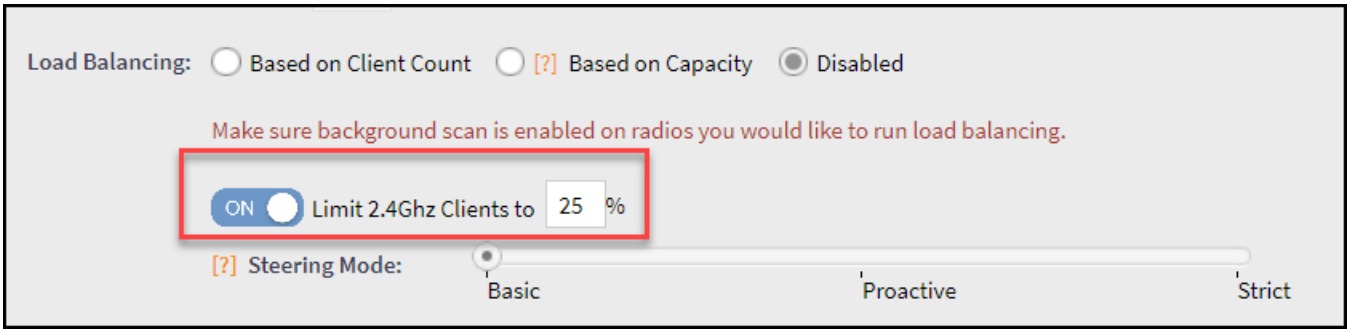
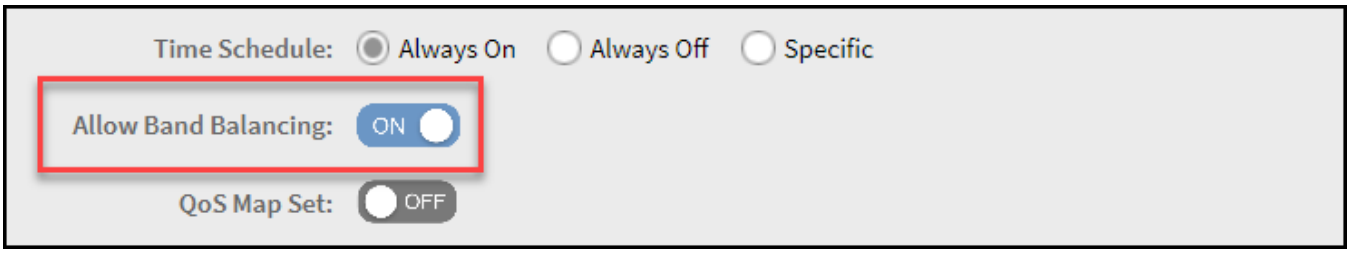


FIGURE 118 Band Balancing



Load Balancing

Load balancing is a solution used to distribute traffic across the application servers. This feature helps to control and direct traffic.

Enabling load balancing improves the WLAN performance by directing the wireless client load between the access points. 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 Received Signal Strength Indicator (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.

After the controller is aware of which APs are adjacent to each other, it begins to manage 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:

- Client signal is weak and cannot support a link with another AP.
- Client signal is strong and belongs to this AP.

The APs maintain these configured client limits and enforce them after 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.

NOTE
Load balancing and Steering mode configuration are at Zone level and Client Load Balancing is at WLAN level.

To enable **Load Balancing** following are the considerations:

- 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.

Enable Load Balancing

By default the Load Balancing is disabled, enable the feature by choosing the appropriate functionalities:

- **Based on Client Count**: Access points are set to a client threshold. If a client wants to associate with an AP whose current count is less, then the client is allowed to associate with the AP. If not then client evalutes the neighbouring APs.
- **Based on Capacity**: The capacity quantifies the maximum data transmitted over a network. Capacity determination is based on bandwidth, data rate and number of streams.
- **Limit 2.4Ghz Clients to**: By default, the functionality is disabled, click the toggle button to enable and set the percentage.

Steering Mode

Steering mode allows the access point to disable lower bandwidth from probing the client device. This allows the access point to respond to only one bandwidth. This helps in reducing congestion and take advantage of the higher bandwidth and improves user experience.

There are three modes in Steering Mode, choose the approriate mode by clicking on the functionality:

- **Basic**: Withold probe and authentication responses at connection time in heavily loaded band to balance clients to the other band.
- **Proactive**: Uses **Basic** functionality and actively rebalances clients through 802.11v BSS Transition Management (BTM).
- **Strict**: Uses **Proactive** functionality and forcefully rebalances clients through 802.11v BSS Transition Management (BTM).

Sticky Client Detection

There are instances where some client devices connects to an AP and stay connected to the same servicing AP, and does not change its association to the closer APs. These clients are referred as sticky clients.

These clients may experience degradation in service because of lower throughput resulting in poor user experience. The purpose of the sticky client detection is to identify these clients and assist in transition to a better AP.

By default, the sticky client steering is disabled, click the toggle button to enable and enter the following:

- **SNR Threshold**: Signal-to-Noise (SNR) ratio value evalutes signal based on the noise. Enter the value between 5db to 30db.
- **NBRAP % Threshold**: Network Based Application Recognition Protocol (NBRAP) is used to calculate a base SNR and compare it to the SNR received from a neighboring AP. The percentage range is between 10-40.

Airtime Decongestion

NOTE
Before enabling airtime decongestion you must enable **Background Scan**.

Airtime Decongestion optimizes the Wi-Fi management traffic in a network where the amount of management traffic can potentially consume a significant portion of airtime, and thereby reduce the amount of time available for traffic. The Airtime Decongestion controls the RSSI threshold setting for Transient Client Management. Enabling Airtime Decongestion disables the RSSI threshold configuration.

VIDEO
Airtime Decongestion Overview. This video provides a brief overview of Airtime Decongestion.

Click to play video in full screen mode.

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 to 100 (To set the minimum client control to 0, select the Client Admission Control threshold.)
- Maximum radio load (%) - 50 to 100
- Minimum client throughput (Mbps) - 0 to 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 or band balancing (or both) is enabled.

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.

Wi-Fi 6 or Wi-Fi 7 Support

The Wi-Fi 6/7 feature controls how the Wi-6/7 AP radios operate to support clients of various capabilities on a specific WLAN.

When the Wi-Fi 6/7 option is enabled on the WLAN (default setting), the Wi-Fi 6/7 AP radios operate in their normal Wi-Fi 6 or Wi-Fi 7 modes. Wi-Fi 6/7 features (such as OFDMA, TWT, 6GHz operation, Preamble Puncturing, 320MHz bandwidth, and MLO) are available to all client devices that support Wi-Fi 6/7. However, legacy Wi-Fi 5 client devices that have outdated or problematic drivers cannot interoperate with the Wi-Fi 6/7 APs.

When the Wi-Fi 6/7 option is disabled on the WLAN, then all Wi-Fi 6/7 AP radios are downgraded to operate in accordance with legacy Wi-Fi 4 and Wi-Fi 5 standards. The Wi-Fi 6/7 features are no longer available to any clients on the network. However, legacy Wi-Fi 5 client devices that have outdated or problematic drivers can interoperate with the Wi-Fi 6/7 APs.

You may configure multiple WLANs on an AP. So you could have one WLAN that supports Wi-Fi 6/7 clients and another WLAN that supports legacy clients. Table 52 provides a side-by-side comparison of the Wi-Fi standards version supported by each radio band, based on the Wi-Fi 6/7 option setting.

TABLE 52 Wi-Fi and Radio Support Matrix

Radio	Wi-Fi 7 AP		Wi-Fi 6E AP		Wi-Fi 6 AP	
Wi-Fi 6/7 option	On	Off	On	Off	On	Off
2.4 GHz	Wi-Fi 7	Wi-Fi 4	Wi-Fi 6	Wi-Fi 4	Wi-Fi 6	Wi-Fi 4
5 GHz	Wi-Fi 7	Wi-Fi 5	Wi-Fi 6	Wi-Fi 5	Wi-Fi 6	Wi-Fi 5
6 GHz	Wi-Fi 7	OFF	Wi-Fi 6E	OFF	N/A	N/A

Virtual LAN

How Dynamic VLAN Works

Dynamic VLAN can be used to automatically and dynamically assign wireless clients to different VLANs based on RADIUS attributes. The maximum number of VLANs supported in Dynamic VLAN per 11ax Virtual AP (VAP) is increased to 128 VLANs.

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 119 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 53 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.

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.

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. Allocating thousands of clients into a single, large subnet or VLAN can result in degraded performance due to factors such as broadcast and multicast traffic. VLAN pooling is adopted to address this problem.

VLAN pooling allows administrators to deploy a 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.

NOTE
The 802.11ac wave 2AP models support maximum of 64 VLANs. Other AP models support upto 32 VLANs.

Creating a VLAN Pooling Profile

To create VLAN a Pooling Profile, perform the following:

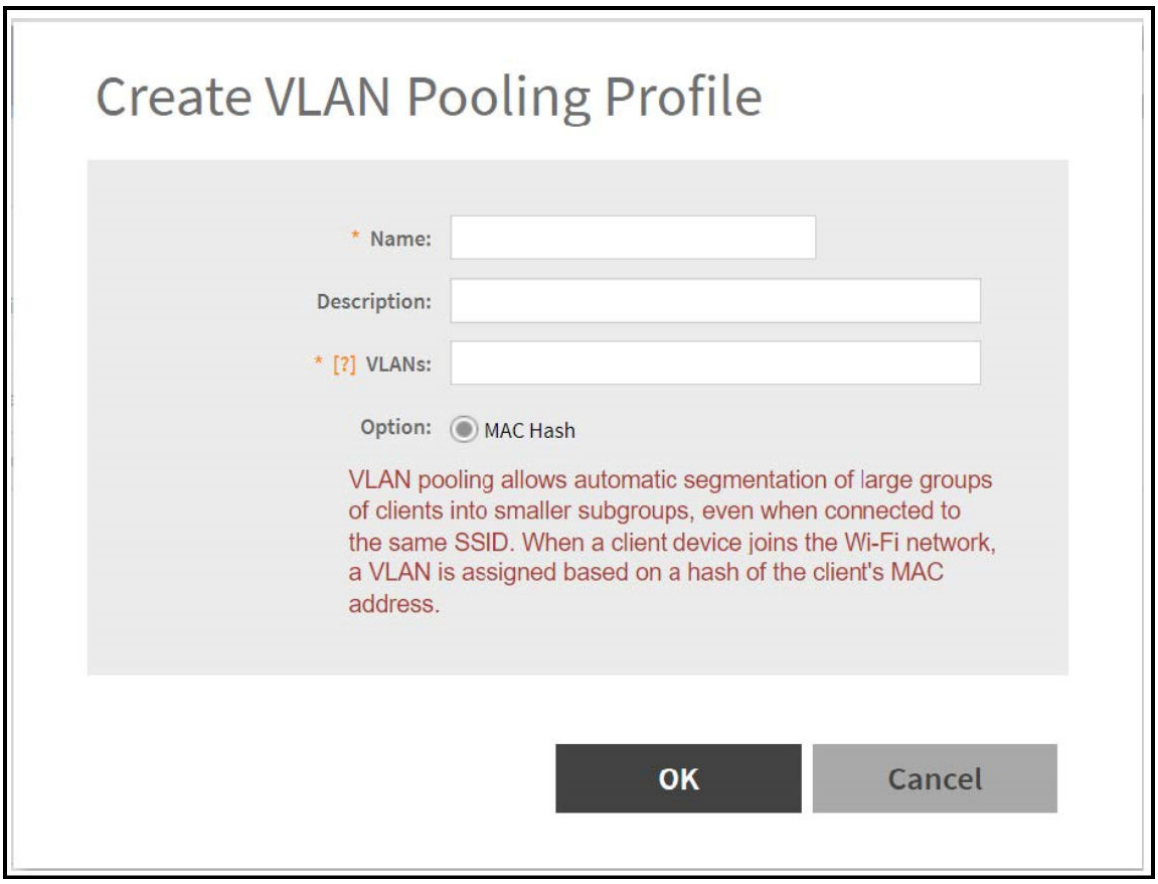
1. Click **Security** > **Access Control** > **VLAN** and select **VLAN Pooling**.

   The **VLAN Pooling** screen is displayed.

2. Select the zone and Click **Create**.

   The **Create VLAN Pooling Profile** page is displayed.

   FIGURE 120 Create VLAN Pooling Profile



3. Enter the following details:
   a. Name: Type a name to identify the VLAN profile.
   b. Description: Type a short description for the VLAN profile.
   c. VLANS: Type the VLAN IDs to be assigned to this pool. VLAN IDs can be separated by hyphens, commas, or a combination (for example, 7-10,13,17,20-28).
   d. Click **OK**.
4. You have created the **VLAN Pooling profile**.

   You can also edit, clone and delete a profile by selecting the options **Configure**, **Clone** and **Delete** respectively, from the **VLAN Pooling** tab.

   NOTE
   Each VLAN pool can contain up to 64 VLANs, and a maximum of 64 VLAN pools can be created. Each WLAN can be configured with a single VLAN pool. For 802.11ac Wave 1, the dynamic VLAN number is 32. For 802.11ac Wave 2 AP/802.11ax AP, dynamic VLAN number is 64.

VLAN Precedence

Clients are assigned to VLANs by various methods, and there is an order of precedence by which VLANs are assigned and rate limiting is applied. The assignment is commonly from lowest to highest precedence. However, you can create a VLAN Precedence Profile where you can change the order of these precedences.

VLAN Precedence

To create a VLAN Precedence, perform the following:

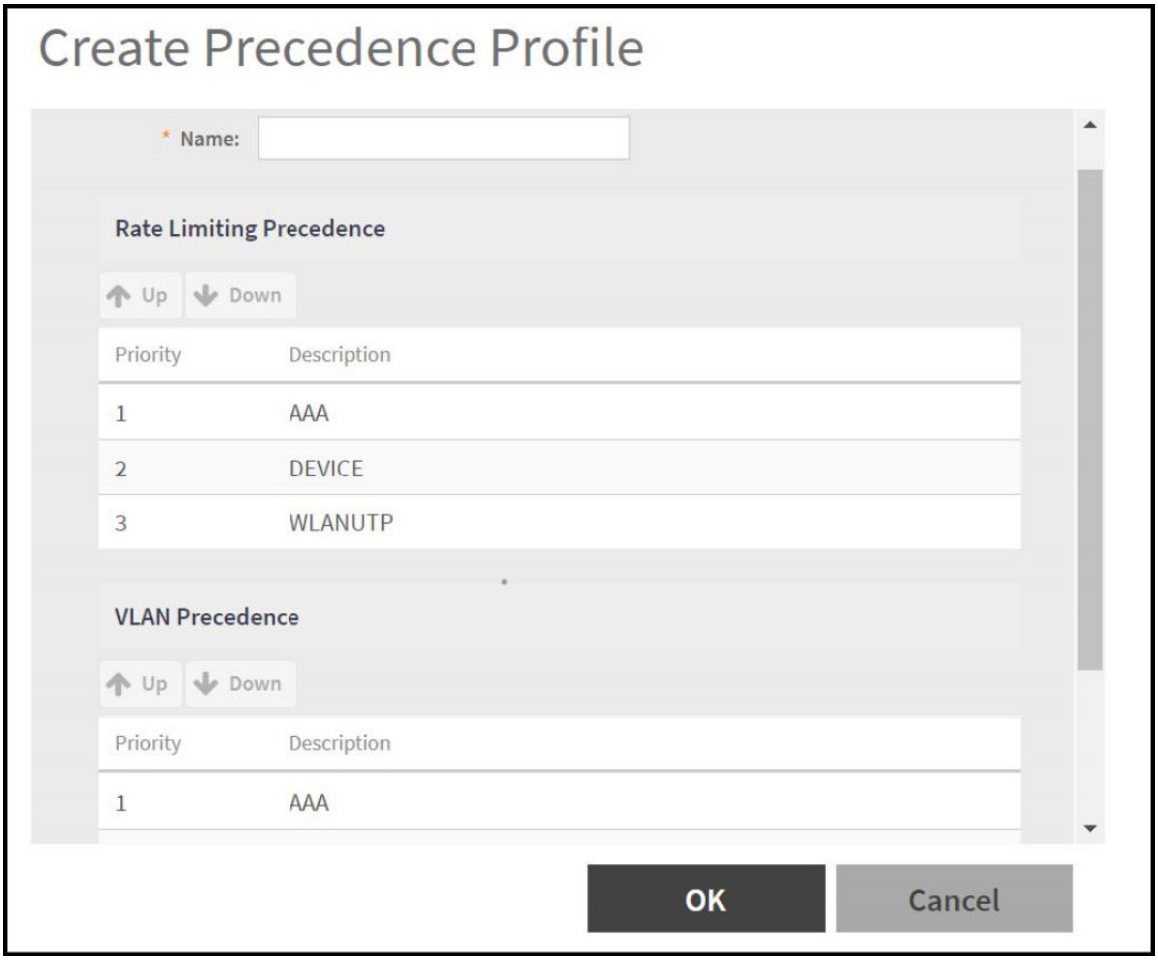
1. Click **Security** > **Access Control** > **VLAN** and select **VLAN Precedence**.

   The **`VLAN Precedence`** page is displayed.

2. Click **Create**.

   The **Create Precedence Profile** page is displayed.

   FIGURE 121 Create Precedence Profile



3. Configure the following:
   a. Name: Enter a name to identify 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**.

      NOTE
      Each VLAN has a default precedence.

You have created a VLAN Precedence profile.

NOTE
You can also edit, clone and delete a profile by selecting the options **Configure**, **Clone** and **Delete** from the **VLAN Precedence** tab.

VLAN Name

Virtual LAN (VLAN) is a logical network segmented by function or application without a regard to physical location. A VLAN breaks single network into multiple sections thus effectively creating multiple stand alone networks out of the same network. This is secure and reduces number of broadcasts received on individual device.

VLAN name can be 32 characters in length. You can configure upto 4094 port-based VLANs on a layer 2 and 3 switches. The default VLAN (VLAN1) uses default values and you cannot create, modify, delete or suspend activities on the default VLAN.

TABLE 54 VLAN Ranges

VLAN Numbers	Range	Description
1	Normal	Default
2-1005	Normal	Configurable VLANs
1006-4094	Extended	Configurable but with parameters

Creating VLAN Name Profile

To create VLAN Name Profile, perform the following:

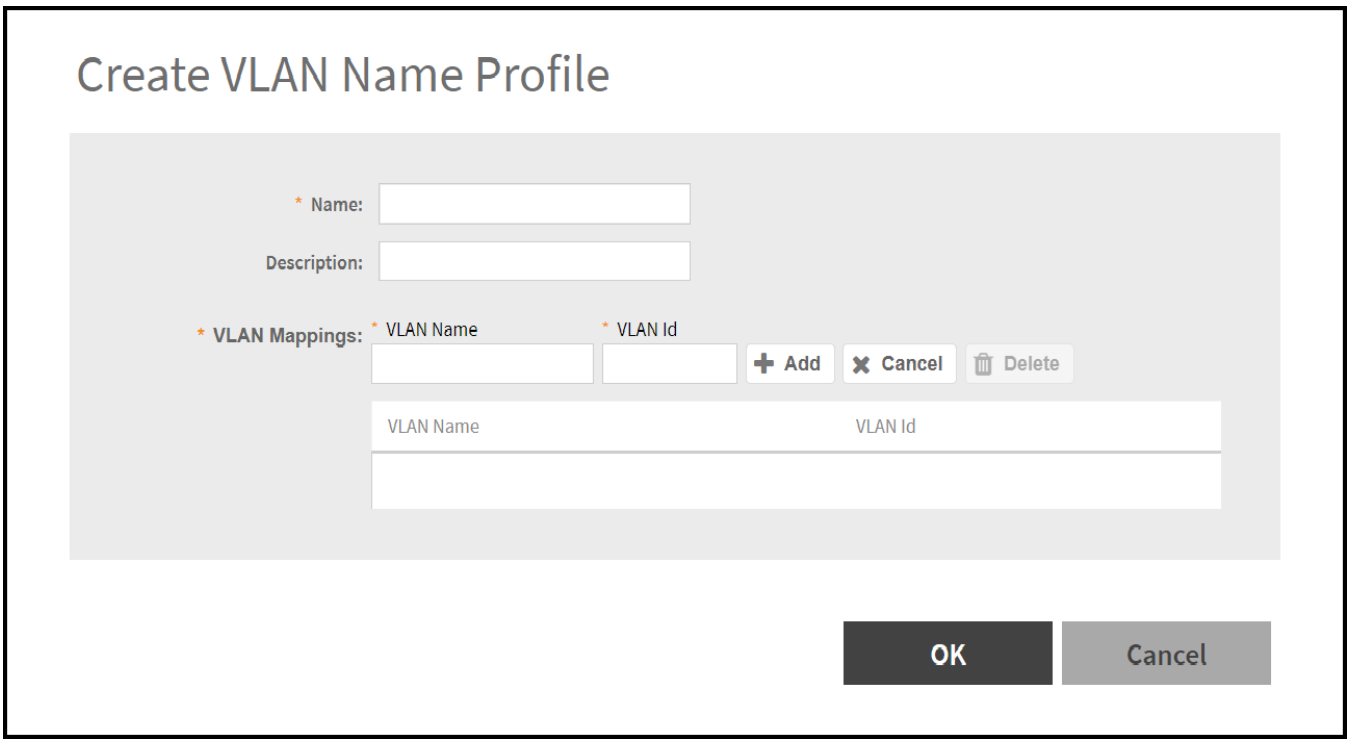
1. Click **Security** > **Access Control** > **VLAN** > **VLAN Name**.

   The **VLAN Name** page is displayed.

2. Select a zone from the hierarchy and click **Create**.

   The **Create VLAN Name Profile** page is displayed.

   FIGURE 122 Create VLAN Name Profile



3. Enter the following fields:
   a. Name: Enter a name to identify 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 .

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 55 WLAN Templates: Contextual Tabs

Tab	Description
General	Displays details of the respective WLAN template.

TABLE 55 WLAN Templates: Contextual Tabs (continued)

Tab	Description
WLAN	Displays details of the respective WLAN. You can create or configure a WLAN. Refer to Creating a WLAN Configuration on page 269.
Hotspots and Portals	Displays details of the respective hotspots and portals. Refer to *RUCKUS SmartZone Access and Security Services Guide*.
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 *RUCKUS SmartZone Access and Security Services Guide*.
Tunnels & Ports	Displays details of the respective tunnels and ports. Refer to *RUCKUS SmartZone Tunnel and Data Plane Guide*.
Radius	Displays details of the respective VSA profiles. You can create or configure a VSA profile. Refer to *RUCKUS SmartZone Access and Security Services Guide*.

Creating WLAN Templates

To create a WLAN template:

1. Go to **Administration** > **System** > **Templates** > **WLAN Templates**.
2. Click **Create**, the Create WLAN Template form is displayed.
3. Enter a **Template Name**.
4. Enter a **Description**.
5. Select the **Template Firmwar**e.
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**.
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.

Switch Management

Supported ICX Models

The following ICX switch models can be managed from SmartZone:

TABLE 56 ICX Firmware Versions Compatible with SmartZone

ICX Model	First Supported FastIron Release	Last Supported FastIron Release
ICX 7150	08.0.80a	09.0.10a and subsequent patches
ICX 7150-C08P, -C08PT, -24F, -10ZP	08.0.92	09.0.10a and subsequent patches
ICX 7250	08.0.80a	09.0.10a and subsequent patches
ICX 7450	08.0.80a	09.0.10a and subsequent patches
ICX 7550	08.0.95a	-
ICX 7650	08.0.80a	-
ICX 7750	08.0.80a	08.0.95 and subsequent patches
ICX 7850	08.0.90	-
ICX 7850-48C	09.0.10a	-
ICX 8200	10.0.00	-
ICX 8200-24ZP, -48ZP2, -24FX, -24F, -48F, -C08ZP	10.0.10	-

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
FastIron 09.0.10a and later releases support management by SmartZone 6.1 and later.

NOTE
ICX switches with FIPS mode enabled do not support management by SmartZone.

TABLE 57 ICX and SmartZone Release Compatibility Matrix

	SmartZone 5.1[1]	SmartZone 5.1.1	SmartZone 5.1.2	SmartZone 5.2	SmartZone 5.2.1 / 5.2.2	SmartZone 6.0	SmartZone 6.1	SmartZone 6.1.1	SmartZone 6.1.2	SmartZone 7.0.0
FastIron 08.0.80	Yes	Yes[1]	No	No	No	No	No	No	No	No
FastIron 08.0.90a	No	Yes	Yes	Yes	Yes	Yes	No	No	No	No
FastIron 08.0.91	No	Yes	Yes	Yes	No	No	No	No	No	No
FastIron 08.0.92	No	No	Yes	Yes	Yes	Yes	Yes	No	No	No
FastIron 08.0.95 and subsequent patches	No	No	No	No	No	Yes	Yes	Yes	Yes	No
FastIron 09.0.10a and subsequent patches	No	No	No	No	No	No	Yes	Yes	Yes	Yes
FastIron 10.0.00 and subsequent patches	No	No	No	No	No	No	No	Yes	Yes	Yes
FastIron 10.0.10 and subsequent patches	No	No	No	No	No	No	Yes	Yes	Yes	Yes

The following table provides details on switch management feature compatibility between ICX and SmartZone releases.

TABLE 58 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

[1] Does not support ICX configuration.

TABLE 58 Switch Management Feature Compatibility Matrix (continued)

Feature	SmartZone Release	ICX FastIron Release
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	08.0.92 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 and later[3]
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
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
Network Segmentation	6.1.1 and later	09.0.10d and later[4]
Breakout Port Support	7.0.0 and later	09.0.10h and later
Enhancement in Firmware Upgrade Status	7.0.0 and later	09.0.10h and later
SmartZone Usernames in ICX Syslogs	7.0.0 and later	09.0.10h and later, 10.0.10c and later
Configuring Separate Authentication and Accounting in AAA server	7.0.0 and later	09.0.10h and later

[2] To download system logs from SmartZone for a particular ICX switch, TFTP must be enabled.
[3] FastIron 10.0.00 and later releases do not support management VLANs.
[4] As an exception, FastIron release 10.0.00 does not support this feature.

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
- CLI templates and provisioning

NOTE
Refer to the Supported ICX Models on page 327 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 can be managed by SmartZone. The following items are required to manage ICX devices:

NOTE
Refer to the Supported ICX Models on page 327 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 ICX 7250, ICX 7450, and ICX 7750 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 123 Command Required to Disable Certificate Check

```
SZ# conf
SZ(config)# non-tpm-switch-cert-validate
Successful operation

SZ(config)# end
SZ#
```

- 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 59 Virtual Platform Requirements for Supporting ICX Devices

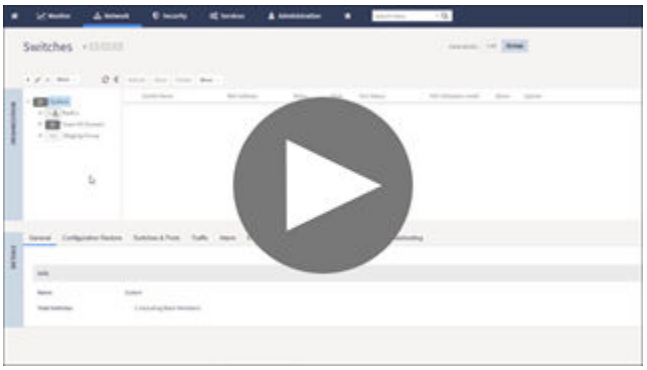
Platform	Maximum Number of Switches Per Node	RAM	vCPU	Disk Storage
vSZ-E	200	18 GB	4	100 GB
vSZ-H	2000	30 GB	12	300 GB

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.

Supported ICX Firmware and Models

TABLE 60 ICX Firmware Versions Compatible with SmartZone

ICX Model	First Supported FastIron Release	Last Supported FastIron Release
ICX 7150	08.0.80a	09.0.10a and subsequent patches
ICX 7150-C08P, -C08PT, -24F, -10ZP	08.0.92	09.0.10a and subsequent patches
ICX 7250	08.0.80a	09.0.10a and subsequent patches
ICX 7450	08.0.80a	09.0.10a and subsequent patches
ICX 7550	08.0.95a	-
ICX 7650	08.0.80a	-
ICX 7750	08.0.80a	08.0.95 and subsequent patches
ICX 7850	08.0.90	-
ICX 7850-48C	09.0.10a	-
ICX 8200	10.0.00	-
ICX 8200-24ZP, -48ZP2, -24FX, -24F, -48F, -C08ZP	10.0.10	-

The Follwing 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.

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.

ICX Release Compatibility Matrix

TABLE 61 ICX and SmartZone Release Compatibility Matrix

	SmartZone 5.11	SmartZone 5.1.1	SmartZone 5.1.2	SmartZone 5.2	SmartZone 5.2.1 / 5.2.2	SmartZone 6.0	SmartZone 6.1	SmartZone 6.1.1	SmartZone 6.1.2	SmartZone 7.0.0
FastIron 08.0.80	Yes	Yes	No	No	No	No	No	No	No	No
FastIron 08.0.90a	No	Yes	Yes	Yes	Yes	Yes	No	No	No	No
FastIron 08.0.91	No	Yes	Yes	Yes	No	No	No	No	No	No
FastIron 08.0.92	No	No	Yes	Yes	Yes	Yes	Yes	No	No	No

TABLE 61 ICX and SmartZone Release Compatibility Matrix (continued)

	SmartZone 5.11	SmartZone 5.1.1	SmartZone 5.1.2	SmartZone 5.2	SmartZone 5.2.1 / 5.2.2	SmartZone 6.0	SmartZone 6.1	SmartZone 6.1.1	SmartZone 6.1.2	SmartZone 7.0.0
FastIron 08.0.95 and subsequent patches	No	No	No	No	No	Yes	Yes	Yes	Yes	No
FastIron 09.0.10a and subsequent patches	No	No	No	No	No	No	Yes	Yes	Yes	Yes
FastIron 10.0.00 and subsequent patches	No	No	No	No	No	No	No	Yes	Yes	Yes
FastIron 10.0.10 and subsequent patches	No	No	No	No	No	No	Yes	Yes	Yes	Yes

Switch Management Feature Compatibility Matrix

TABLE 62 ICX and SmartZone Release Compatibility Matrix

	SmartZone 5.11	SmartZone 5.1.1	SmartZone 5.1.2	SmartZone 5.2	SmartZone 5.2.1 / 5.2.2	SmartZone 6.0	SmartZone 6.1	SmartZone 6.1.1	SmartZone 6.1.2	SmartZone 7.0.0
FastIron 08.0.80	Yes	Yes	No	No	No	No	No	No	No	No
FastIron 08.0.90a	No	Yes	Yes	Yes	Yes	Yes	No	No	No	No
FastIron 08.0.91	No	Yes	Yes	Yes	No	No	No	No	No	No
FastIron 08.0.92	No	No	Yes	Yes	Yes	Yes	Yes	No	No	No
FastIron 08.0.95 and subsequent patches	No	No	No	No	No	Yes	Yes	Yes	Yes	No

TABLE 62 ICX and SmartZone Release Compatibility Matrix (continued)

	SmartZone 5.11	SmartZone 5.1.1	SmartZone 5.1.2	SmartZone 5.2	SmartZone 5.2.1 / 5.2.2	SmartZone 6.0	SmartZone 6.1	SmartZone 6.1.1	SmartZone 6.1.2	SmartZone 7.0.0
FastIron 09.0.10a and subsequent patches	No	No	No	No	No	No	Yes	Yes	Yes	Yes
FastIron 10.0.00 and subsequent patches	No	No	No	No	No	No	No	Yes	Yes	Yes
FastIron 10.0.10 and subsequent patches	No	No	No	No	No	No	Yes	Yes	Yes	Yes

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.

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.

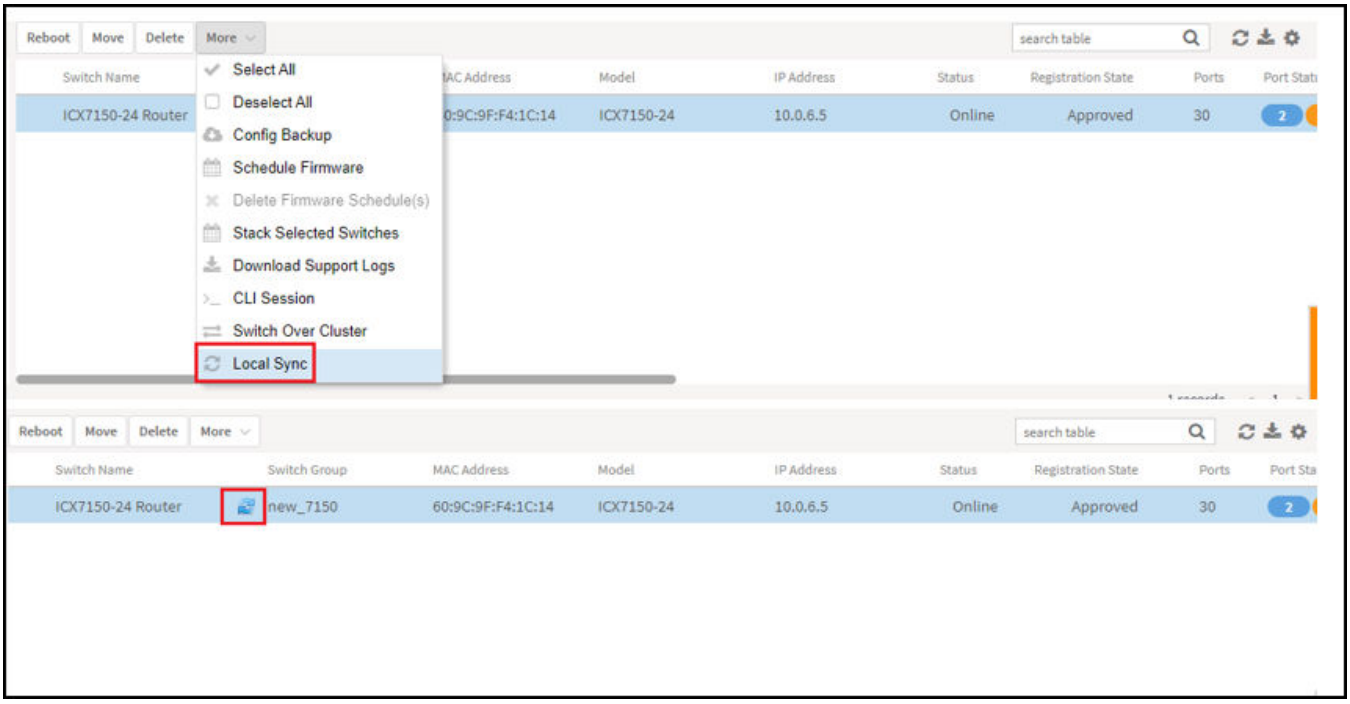
Data Synching on the Switch Table

When a switch running FastIron 08.0.90 or later joins the controller, the controller runs the Local Sync operation every 5 minutes. If the changes are made on the switch console or any configuration changes are deployed on the controller, the controller syncs those corresponding changes to the switch or port table five minutes later, which causes a delay. Therefore, beginning with SmartZone 6.1.1, the Local Sync time is reduced from 5 minutes to 3 minutes to speed up the process.

When a CLI session is closed, Local Sync is triggered automatically to update the changes on the controller. Similarly, the controller can trigger Local Sync manually for a selected switch.

1. On the menu, click **Network** > **Wired** > **Switches** to display the **Switches** window.
2. In the **Organization** tab, select a **Domain** > **Switch Group** or **Switch Group** and select the **Switch**. Click **More** > **Local Sync** .

FIGURE 124 Selecting LocalSync on the Controller UI



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.

Beginning with 09.0.10h, access to the ICX device through web management may change when the device is connected to SmartZone.

- When **WebAuth** is not configured on the ICX switch and then is connected to SmartZone, web management is disabled and the CLI command **web-management disable** is then added to the running configuration. To enable web-management, enter **no web-management disable** on the ICX device.
- When an ICX device is configured with **WebAuth** on any VLAN and then is connected to SmartZone there is no change in the web management behavior. If **WebAuth** is disabled later, access to web management will stay enabled until the next time the device is connected to SmartZone.
- When an ICX device is connected to SmartZone and then **WebAuth** is enabled on any VLAN, enter **no web-management disable** on the ICX device to enable web management.

- When a device has web management disabled, if a user enabled the **WebAuth** configuration, it will not work until **no web-management disable** is entered on the device.

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 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.

Configuring a Custom Port Number for Connection to SmartZone

By default, ICX switches use TCP destination port 22 to connect with SmartZone. Use the **manager ssh-port** command to configure a different port number for connecting with SmartZone.

The following example configures an ICX switch to connect to SmartZone over SSH port 25. A warning message is displayed as shown if a session is already established. You must confirm the configuration update when prompted before the new connection is established. Check configuration status with the **show manager status** command.

```
device# configure terminal
device(config)# manager ssh-port
  DECIMAL   Enter a decimal value (Default 22)
device(config)# manager ssh-port 25

device(config)# manager ssh-port 25  <-- Warning message -->
Current session if established will be dropped to establish a new session with port 25.
Are you sure? (enter 'y' or 'n'): y  <-- You must confirm the configuration.
!
!
device(config)# exit

device# 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             : 10.176.160.115
Active List IPV6        : None
DHCP Option 43          : No
DHCP Opt 43 List        : None
Backup List             : None
Backup List IPV6        : None
Merged List             : 10.176.160.115

SZ IP Used              : 10.176.160.115
Port List               : 987
Server Port Used        : 443
Query Status            : APPROVED

SSH Tunnel Status -:
Tunnel Status           : Established
SSH Port                : 25          <-- configuration confirmed
CLI IP/Port             : 127.255.255.253/22866
SNMP IP/Port            : 127.255.255.254/63989
Syslog IP/Port          : 127.0.0.1/20514
HTTP CLIENT IP/Port     : 127.0.0.1/5080
HTTP SERVER IP/Port     : 127.255.255.252/40042
Timer Status            : Not Running
```

NOTE

If you configure a custom port on an ICX switch, the SmartZone controller settings must also be updated. Refer to the appropriate version of the RUCKUS SmartZone administration guide for details.

Connecting the ICX to the SmartZone Controller

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 in privileged EXEC or global configuration mode:

- **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.

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
   ```

Approving and Registering switches

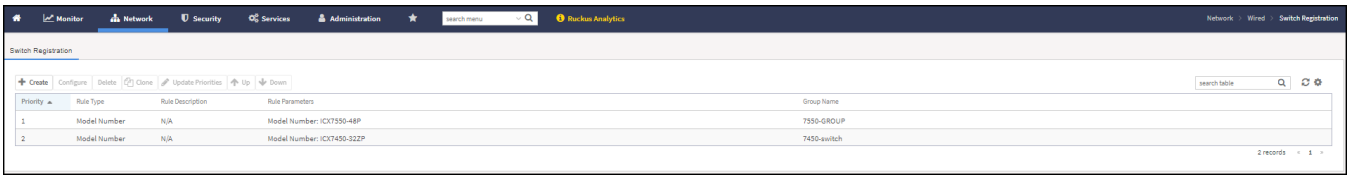
Creating Switch Registration Rules

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. On the menu, click **Network** > **Wired** > **Switch Registration** to display the **Switch Registration** window.

   FIGURE 125 Switch Registration



2. Click 

icon to display the **Switch Registration Rule** dialog box.

   Complete the following fields:

   - **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 from the drop down list.

FIGURE 126 Creating Switch Registration Rules - IP Address Range

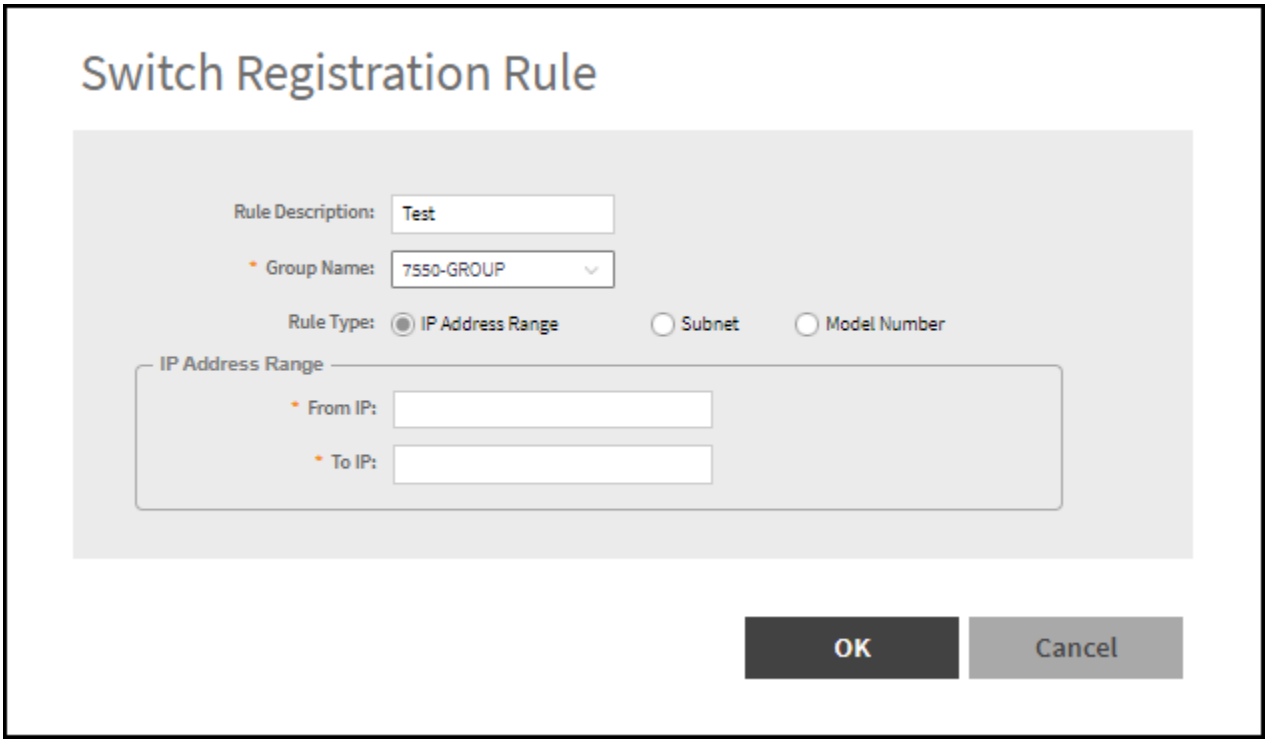


FIGURE 127 Creating Switch Registration Rules - Subnet

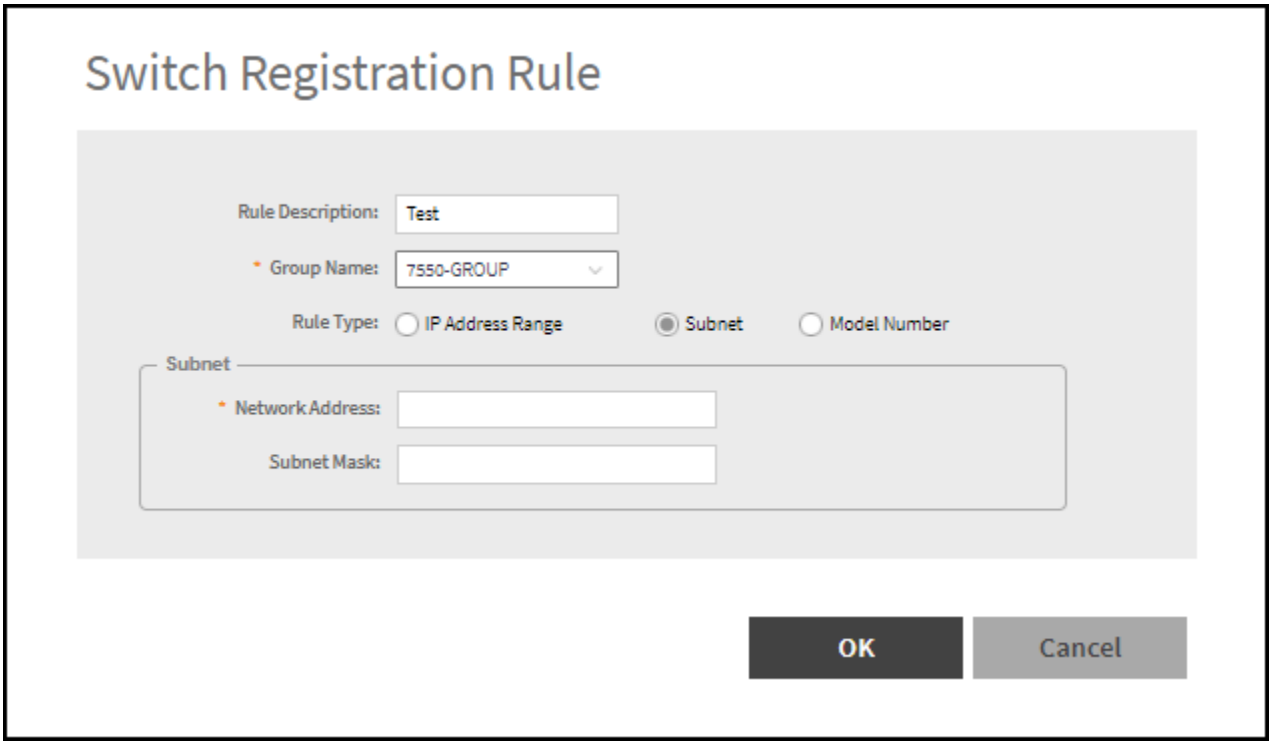
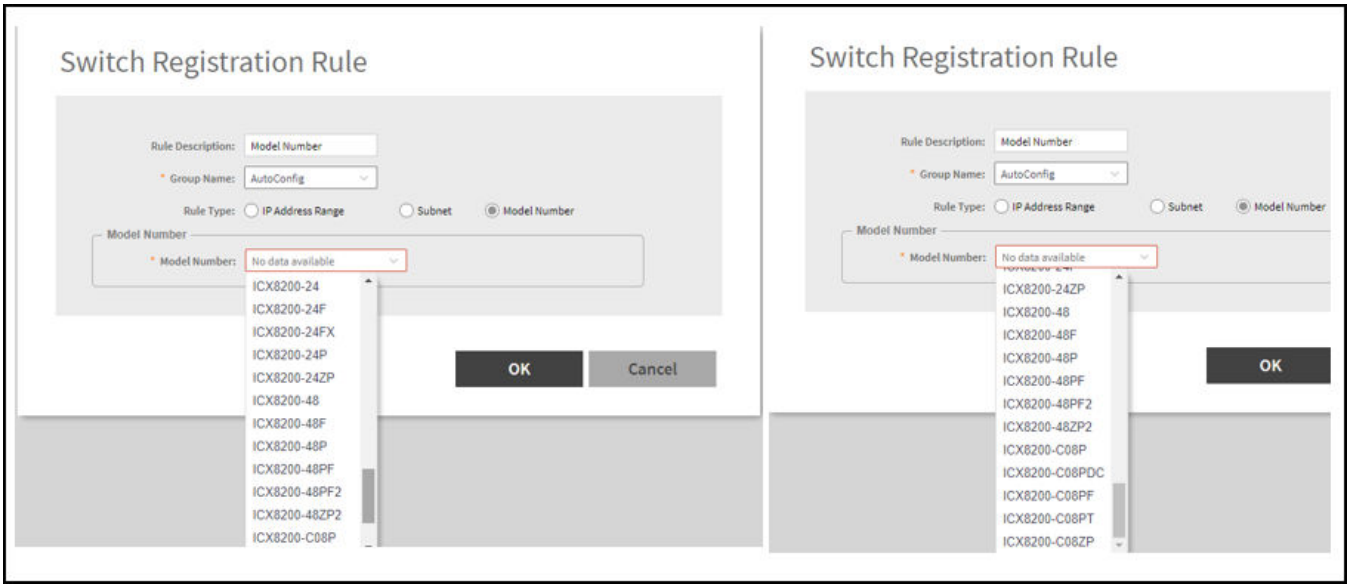


FIGURE 128 Creating Switch Registration Rules - Model Number



3. Click **OK**.

   You can edit, copy and delete the rule by selecting the rule and clicking **Configure**, **Clone**, and **Delete**, respectively.

   After 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 344 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.

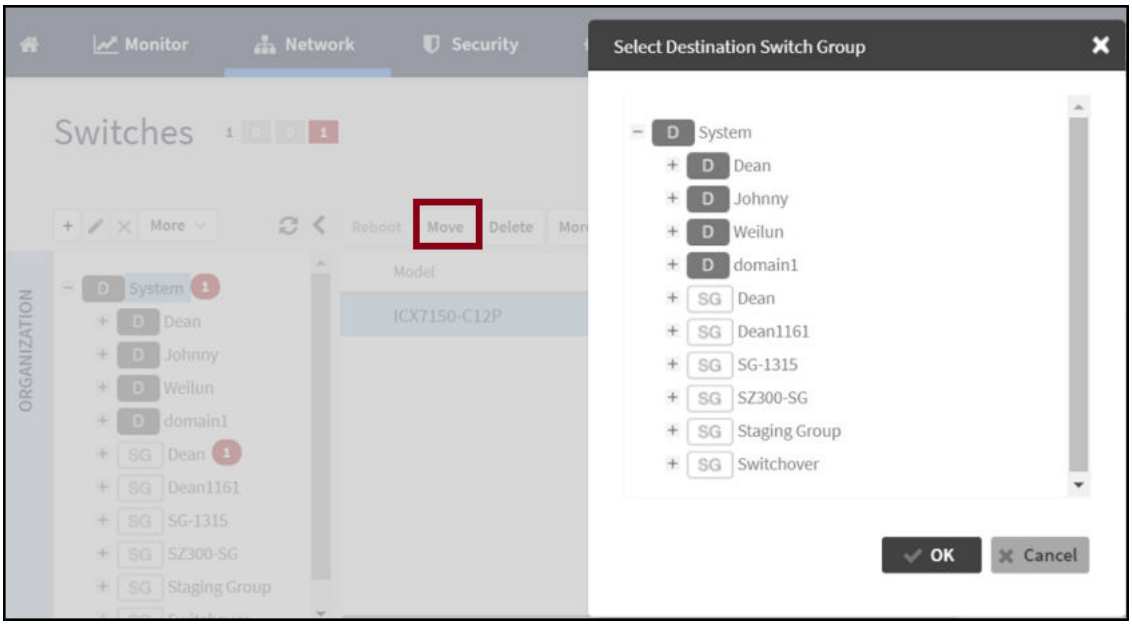
Moving the Switches between Groups

You can move the switch to any group or sub-group within the system tree hierarchy.

1. On the menu, click **Network** > **Wired** > **Switches** to display the **Switches** window.
2. From the system tree, select a **Domain** > **Switch Group** or **Switch Group** and select the **Switch** that you want to move.

3. Click the **Move** tab.

FIGURE 129 Moving the switch



The **Select Destination Switch Group** dialog box is displayed showing the system tree hierarchy.

4. Select a **Domain** > **Switch Group** or **Switch Group** to which you want to move the selected switch.
5. Click **OK**.

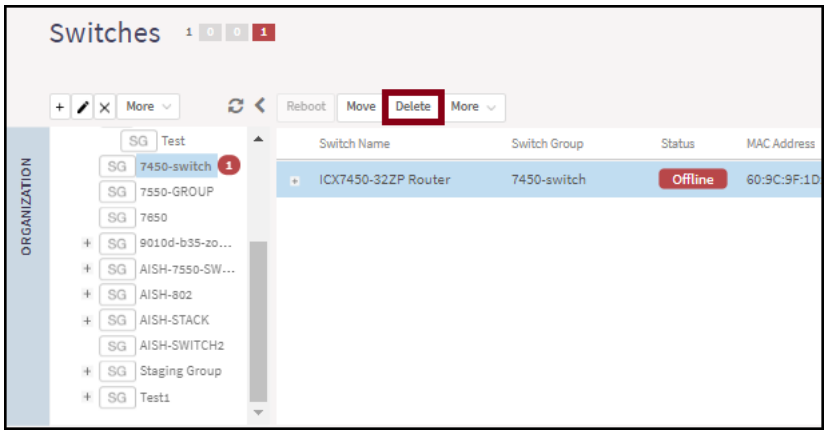
Deleting Switches

The **Delete** enables you to remove the switches that are no longer needed.

1. On the menu, click **Network** > **Wired** > **Switches** to display the **Switches** window.

2. From the system tree, select a **Domain** > **Switch Group** or **Switch Group** and select the **Switch** that you want to delete.

   FIGURE 130 Clicking the Delete Tab



3. Click the **Delete** tab.

   After deletion, the selected switch will no longer be managed by the controller interface.

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 the topic Creating Switch Registration Rules on page 341.

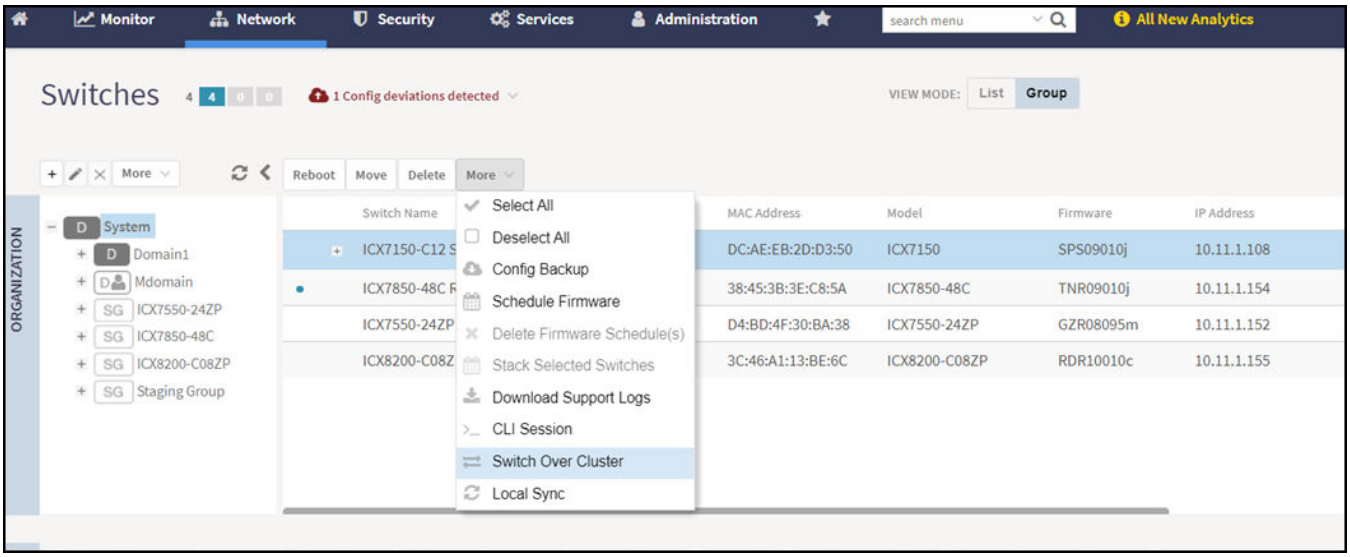
NOTE
Depending on the switch High Availability license on the standby cluster switches must be approved so that it can be discovered and monitored by the controller. For more information, refer to Approving Switches on page 344 .

Complete the following steps to switch over from one cluster to another.

1. On the menu, click **Network** > **Switches** > **Switches** to display the **Switches** window.

2. From the system tree, select a **Domain** > **Switch Group** or **Switch Group** and select the **Switch**.

   FIGURE 131 Switch Over Cluster



3. Click **More**. Select **Switch Over Cluster** from the list.

   The **Switch Over Cluster** dialog box is displayed.
4. In the **Control IP** field, enter the control IP address of the switchover target cluster.
5. Click **OK**. A **Confirmation** dialog box is displayed.
6. Click **YES** to confirm.

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. On the menu, click **Network** > **Wired** > **Switches** to display the **Switches** window.
2. From the system tree, select a **Domain** > **Switch Group** or **Switch Group** and select the **Switch** to rehome.
3. In the **System Domain**, click **More** > **Rehome Active Cluster** to display the **Confirmation** dialog box.
4. Click **Yes**.

ICX to SmartZone Connection Status

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.

```
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
```

Disconnecting the ICX Switch from SmartZone

Use the **manager disconnect** command in privileged exec or global configuration mode 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 in privileged exec or global configuration mode.

This command can be executed on the local terminal.

```
ICX# manager disconnect
SZ Disconnect initiated...

ICX# configure terminal
ICX(config)# 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
```

Working with Switches

Viewing Switch Information

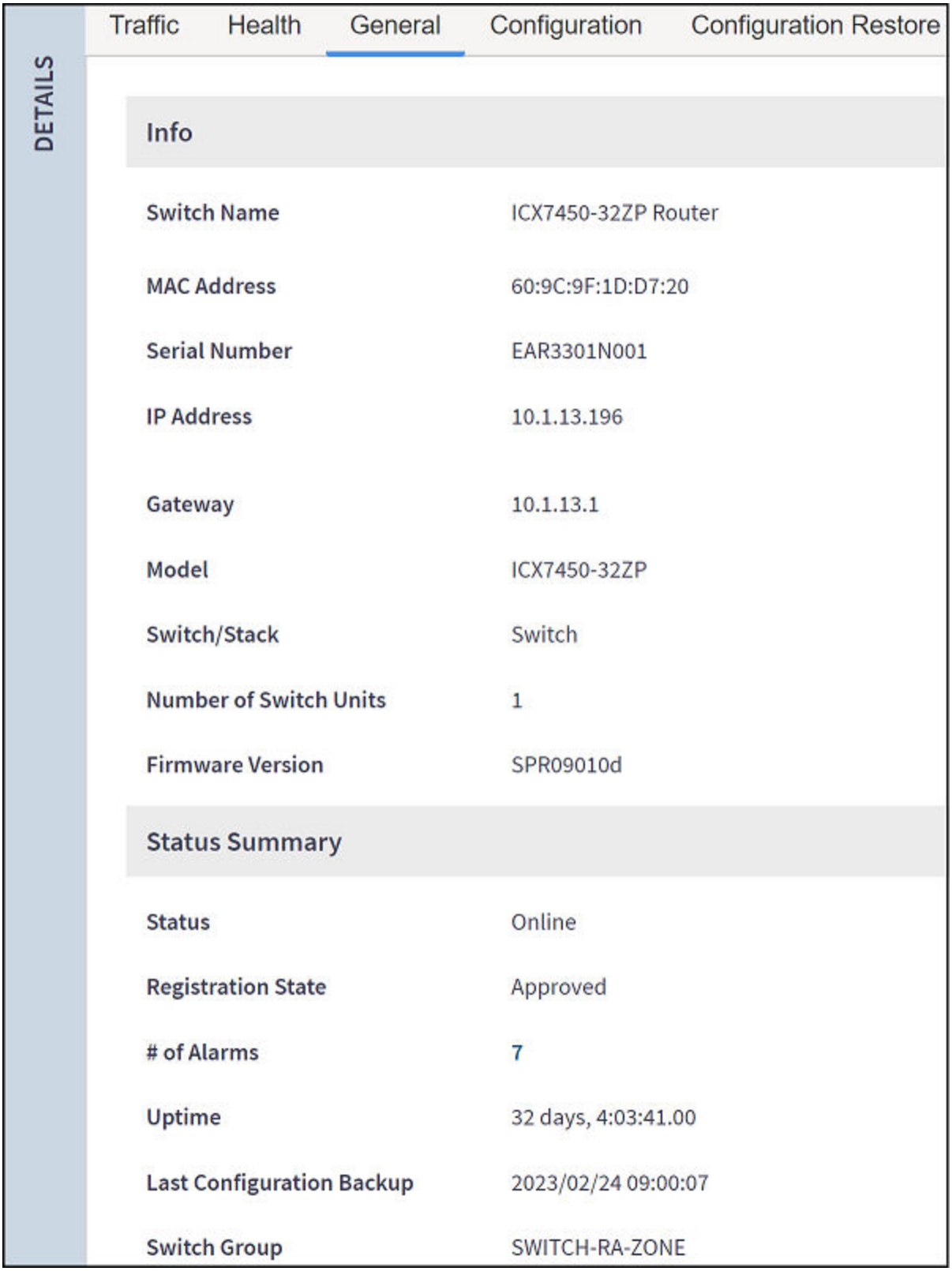
Details such as switch status, firmware version, and IP address are available for individual switches, stacks, and switch groups.

To view information on a switch, a stack, or a switch group, perform these steps.

1. On the menu, click **Network** > **Wired** > **Switches** to display the **Switches** window.

2. In the **Organization** tab, Select the **Domain** > **Switch Group** or **Switch Group** and select the **Switch** to display information specific to it. In the **Details** tab, click **General** tab to display the switch information.

FIGURE 132 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).
- # 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.

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 352 and Creating Switch Registration Rules on page 341 for additional information.

Creating Switch Groups

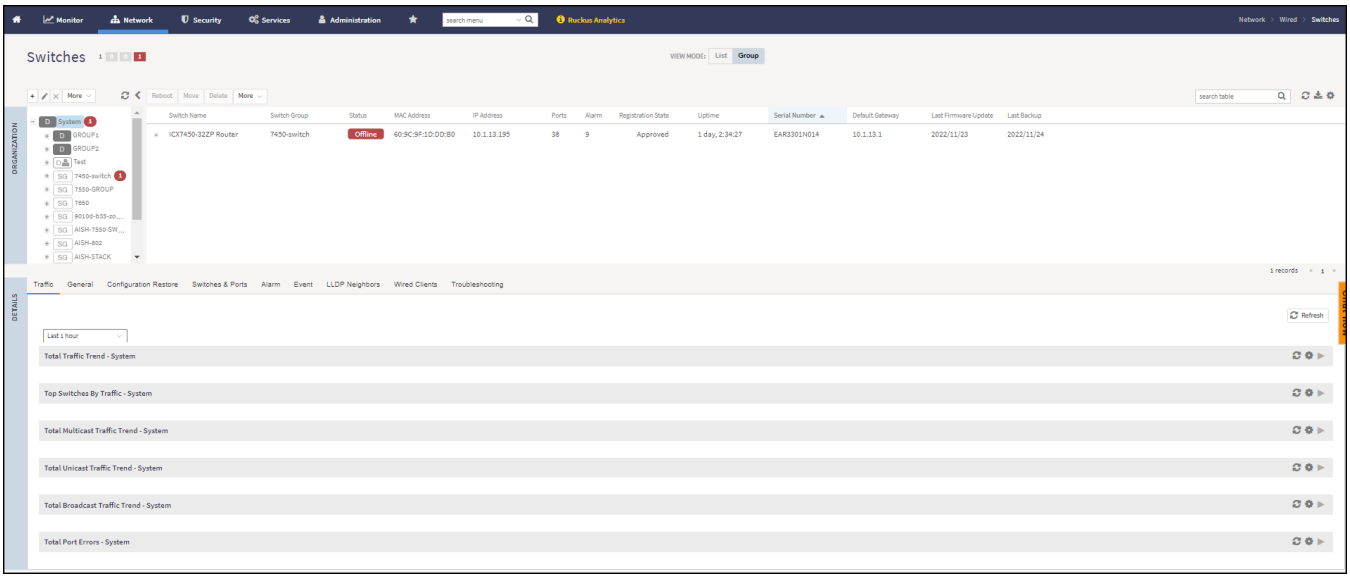
You can group switches based on your need, for example, you can group switches based on their size or their location.

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.

1. On the menu, click **Network** > **Wired** > **Switches** to display the **Switches** window.

   FIGURE 133 Switches

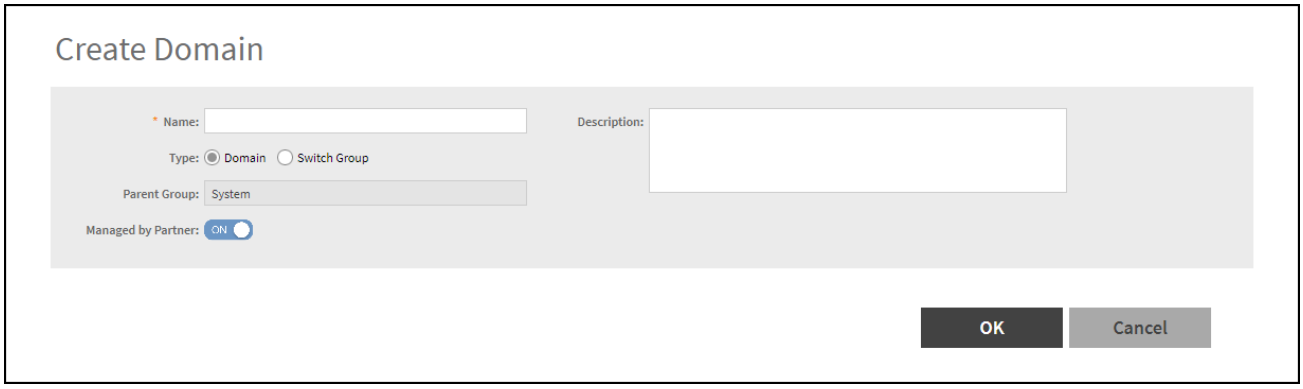


   You can create a switch group or you can create a domain and add the switch group to that domain.

2. Complete the following steps to create a domain.

   a) In the **Organization** tab, click  to display the **Create Domain** dialog box.

   FIGURE 134 Create Domain



   b) Complete the following fields:

   - **Name**: Enter the domain name.
   - **Description**: Enter a brief description for the domain.
   - **Type**: Domain
   - **Parent Group**: Displays the parent group under which the switch group resides. By default **System** is selected.
   - **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.

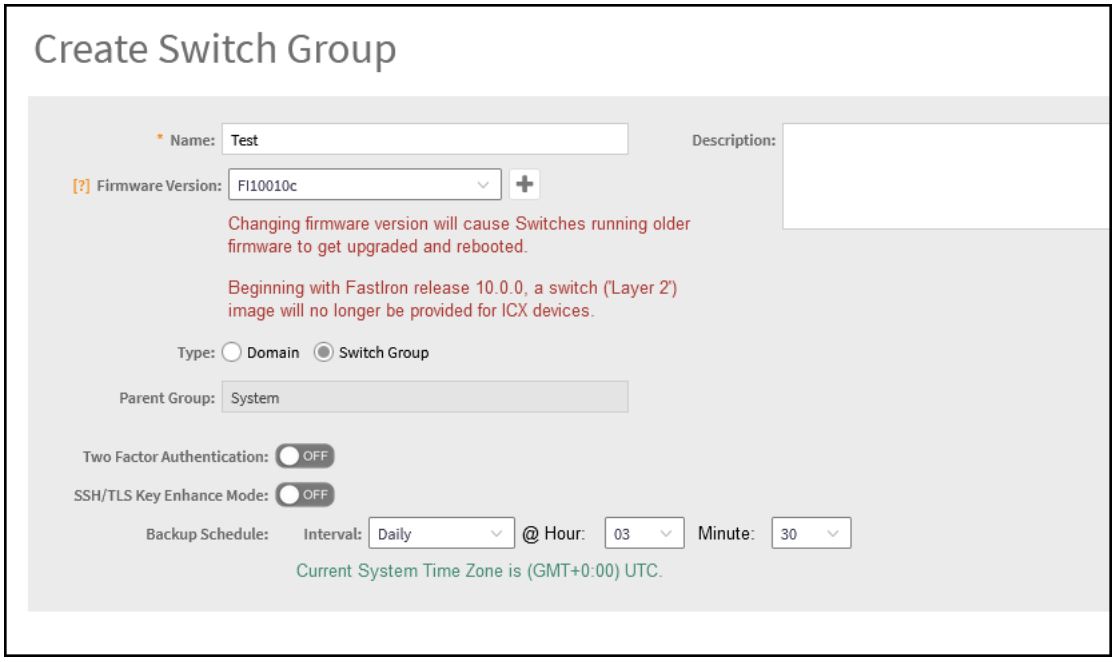
   c) Click **OK**.

   The domain is created under the selected parent group in the **Organization** tab. The domain is identified with "D" symbol.

3. To create a individual switch group, in the **Organization** tab select the **System** and follow from the Step 5.
4. To create a switch group within a domain, in the **Organization** tab select the **Domain** from the list and follow from the Step 5.

5. In the **Organization** tab, click icon to display the **Create Switch Group** dialog box. You can also edit or configure the switch group by clicking icon.

FIGURE 135 Creating Switch Group



Complete the following fields:

- **Name**: Type the name of the switch group that you want to create.
- **Description**: Enter a brief description for the switch group.
- **Firmware Version**: Select the Firmware version (optional) which will automatically upgrade the switches (running an older version) joining the group.
- **Type**: Select **Switch Group**. For enterprise devices such as SZ-300 and vSZ-H.
- **Parent Group**: Displays the parent group under which the switch group resides
- **Two Factor Authentication**: Switch **ON** to use the **Console CLI** or **Remote CLI** to access the **Switches**.

  NOTE
  Turning ON this feature will disable the SSH access to the switches.

  NOTE
  Beginning with the SZ 7.0 release, when **Two Factor Authentication** is enabled on the controller, the ICX System log displays the SZ administrator name associated with the configuration activity performed on the controller. In the earlier releases, the ICX System log showed a generic message indicating that the network controller made the change.

  A **message** dialog box is displayed, click **OK**.
- **Backup Schedule**: Allows you to schedule the backup. From the **Interval** drop-down list, select the type of backup such as **Daily**, **Weekly**, or **Monthly**. If the backup selected is **Daily**, you can configure **@Hour** , and **Minute** fields. If the backup selected is **Weekly**, you can configure the **Every** (day of the week), **@Hour** , and **Minute** fields. If the backup selected is **Monthly**, you can configure **Every** (date), **@Hour** , and **Minute** fields.

NOTE
The default backup time for scheduling a **Daily** backup is 3:30 a.m. The backup schedule is configured on the level one switch group.

- **SSH/TLS Key Enhance Mode**: Allows you to enable or disable ECDSA Certificate.

  NOTE
  If the administrator wants to turn on **SSH/TLS Key Enhance Mode** of the Switch Group, the **Firmware Version** setting must be configured first, and it must be the following.
  - 10.0.10c and later versions
  - 9010j and 9010j patch

6. Click **OK**.

   The switch group is created under the selected parent group in the **Organization** tab. The switch group is identified with "SG" symbol.

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. On the menu, click **Network** > **Wired** > **Switches** to display the **Switches** window.
2. In the **Organization** tab, select a **Domain** > **Switch Group** or **Switch Group** and in the **Details** tab, click **Configuration** tab.
3. In the **Model Configuration** tab, select the **Switch Model** and click 

icon to display the **Feature Configuration** dialog box.

4. Configure the Switch settings.
   a) Click **Switch** tab.

   FIGURE 136 Switch Configuration

   b) Complete the following fields:
   - **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.
5. Configure the switch ACL settings, refer to *Configure the ACL settings* in the Creating Switch Model-Based Configurations on page 390.

6. Configure the switch **VLAN** settings.

   NOTE
   You can create a new VLAN and set it as the default VLAN.

   a) Click **VLAN** tab.

   b) Click 

icon to display the **VLAN** fields.

FIGURE 137 VLAN Configuration

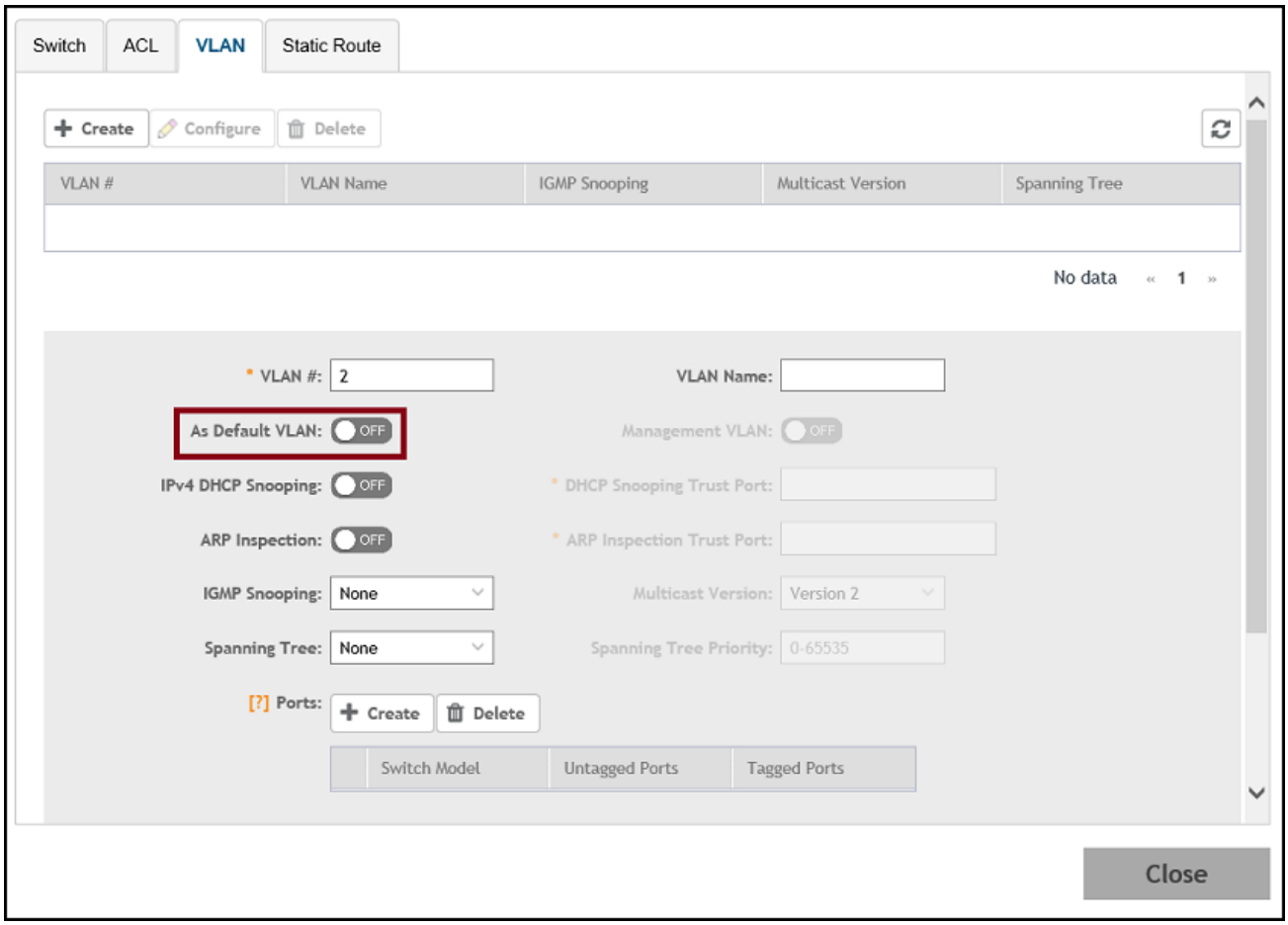
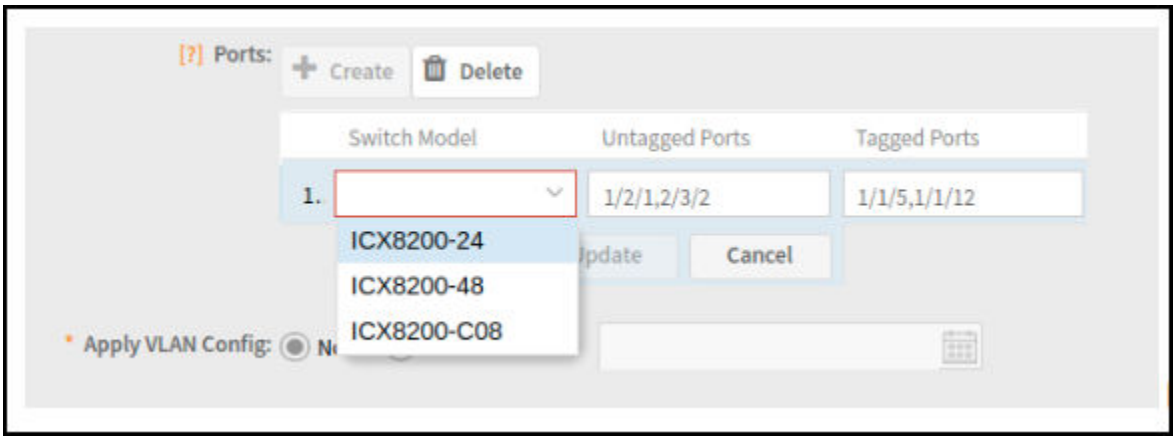


FIGURE 138 Creating Port and Adding Port Details



c) Complete the following fields:

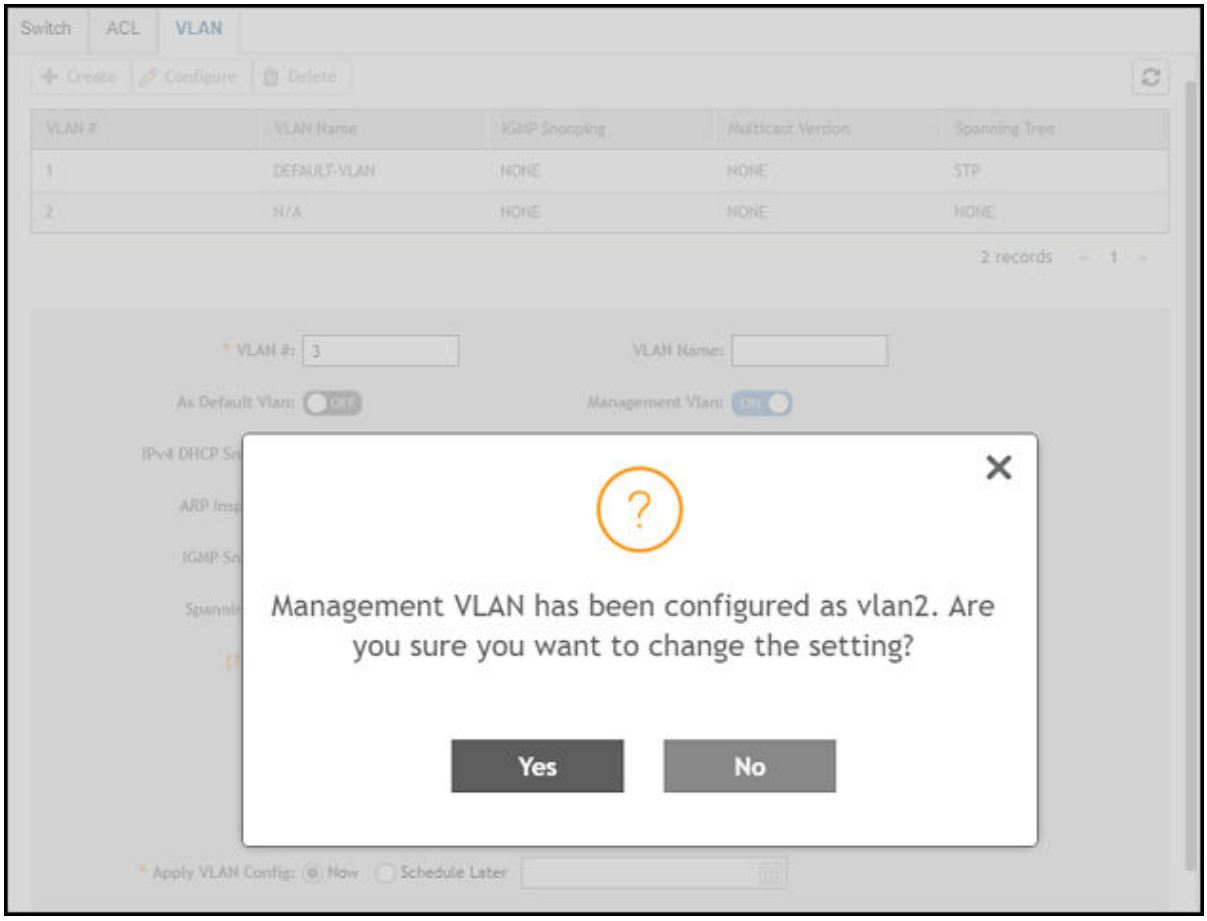
- **VLAN#**: Enter a unique number for VLAN.
- **VLAN Name** is changed to **DEFAULT-VLAN** and the Management settings correspond to the previous VLAN settings.

  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.

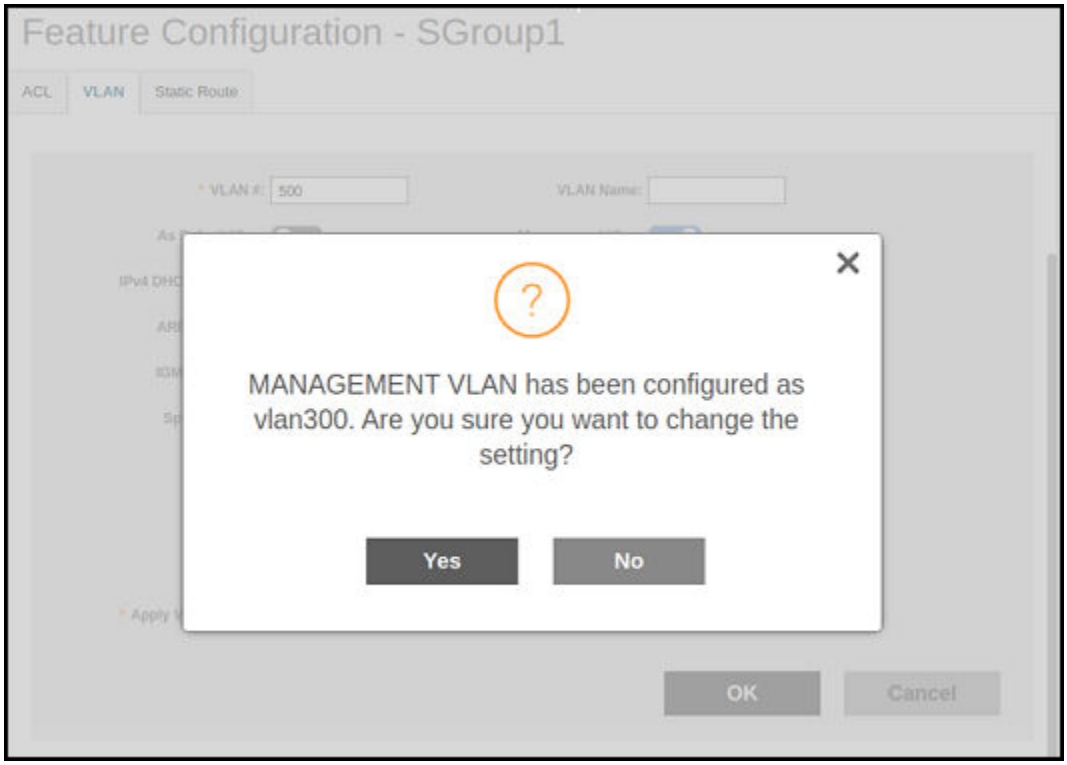
FIGURE 139 Management VLAN Confirmation

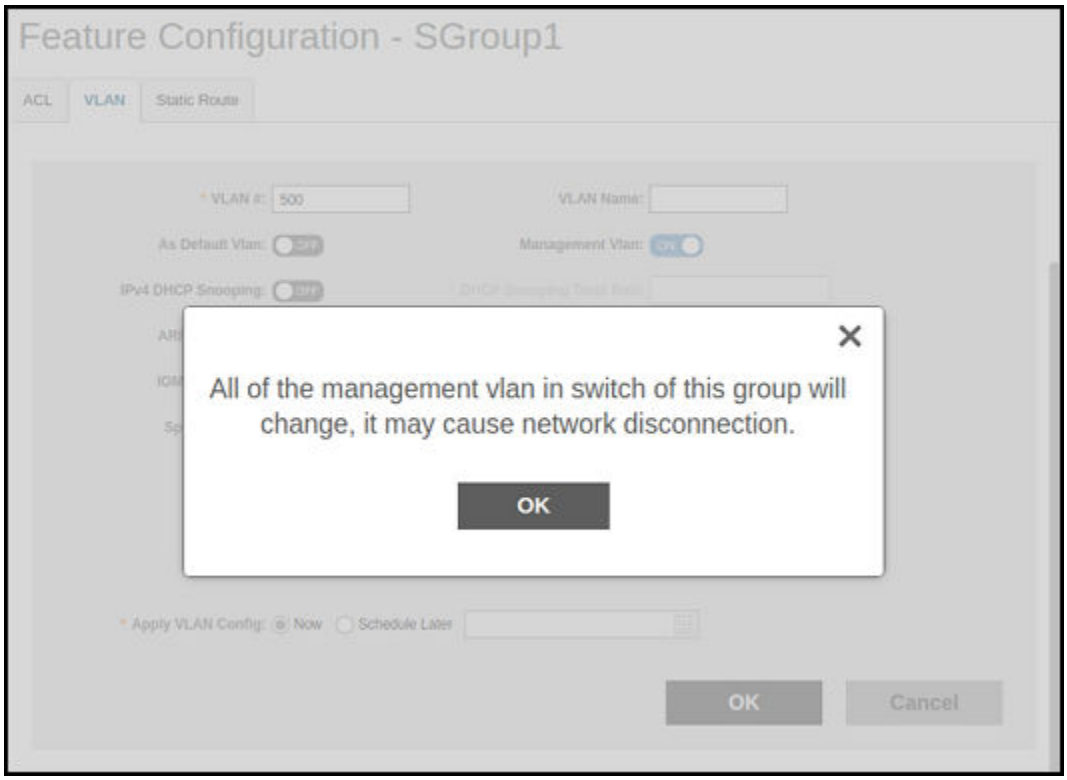


If **Management VLAN** is enabled on a VLAN and you try to enable it on another VLAN, the controller displays a dialogue box showing the VLAN ID that has been configured as the Management VLAN. If you click **Yes**, the controller overwrites the settings.

- For a switch group, the controller displays a dialogue box, as shown in the following figure.

FIGURE 140 Management VLAN Confirmation Dialogue Box





- **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**.
- **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.

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

7. Configure the switch Static Route settings, refer to *Configure the Static Route settings* in the Creating Switch Model-Based Configurations on page 390.
8. 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.

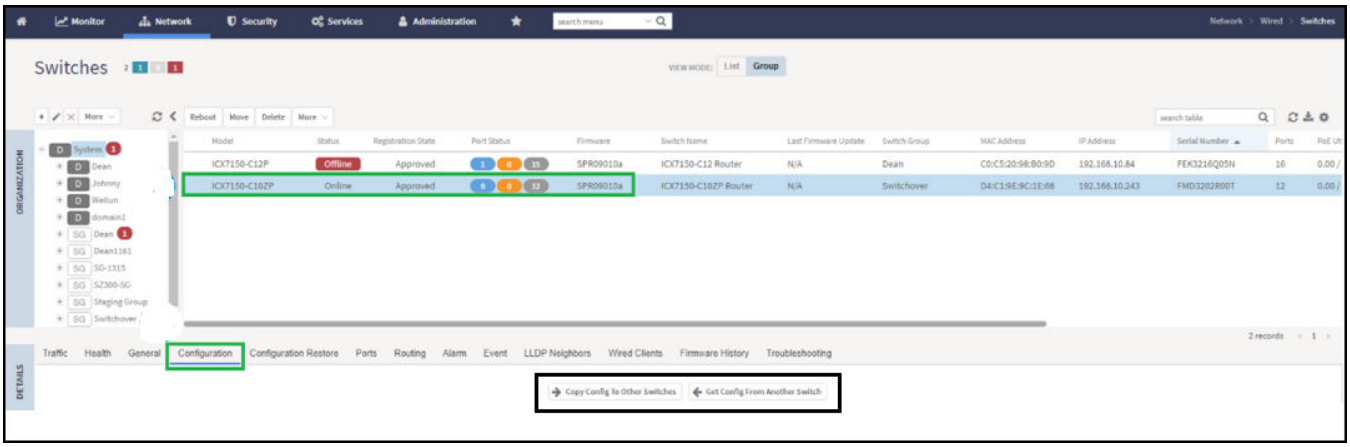
Complete the following steps to copy configuration to one or more target switches.

1. From the main menu, go to **Network** > **Wired** > **Switches.**

   The **Switches** page appears.

2. Select the switch and then the **Configuration** tab.

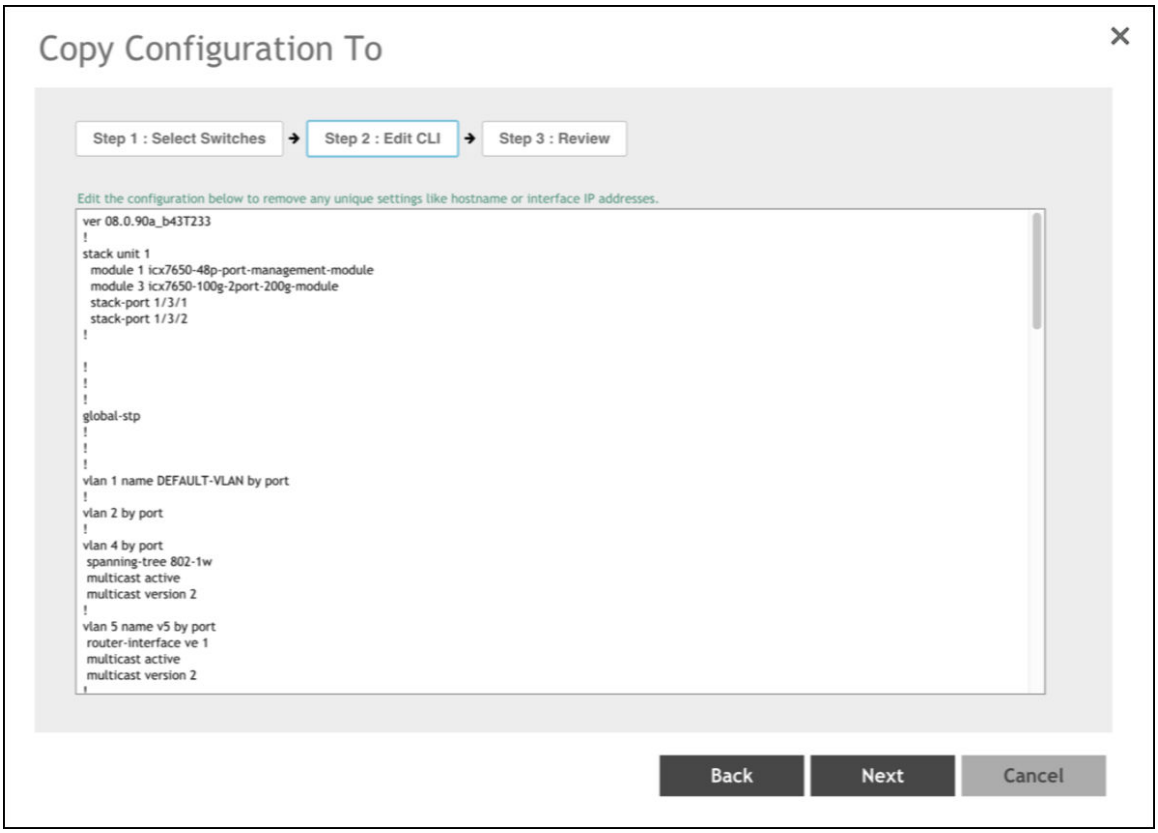
FIGURE 141 Switch Group Configuration Tab



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 142 Copy Configuration To - Edit CLI Page



6. Review CLI config and click **OK**.

Configuring the Switch

SmartZone 5.1.1 introduces the switch configuration capabilities. The following features are added:

- **Zero Touch Provisioning**: Simplifies the initial deployment of switches. Allows you to define switch configuration at a switch group level. If a new switch joins the group automatically, it gets provisioned.
- **Ongoing Configuration Changes**: You can modify the switch configuration as a part of network maintenance. This includes modifying switch group level settings, port settings, and routing interfaces.
- **Stack formation**: You can configure individual switches to be formed into a stack directly from the controller.
- **Configuration copy**: You 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 through CLI/Telnet/SSH or 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.

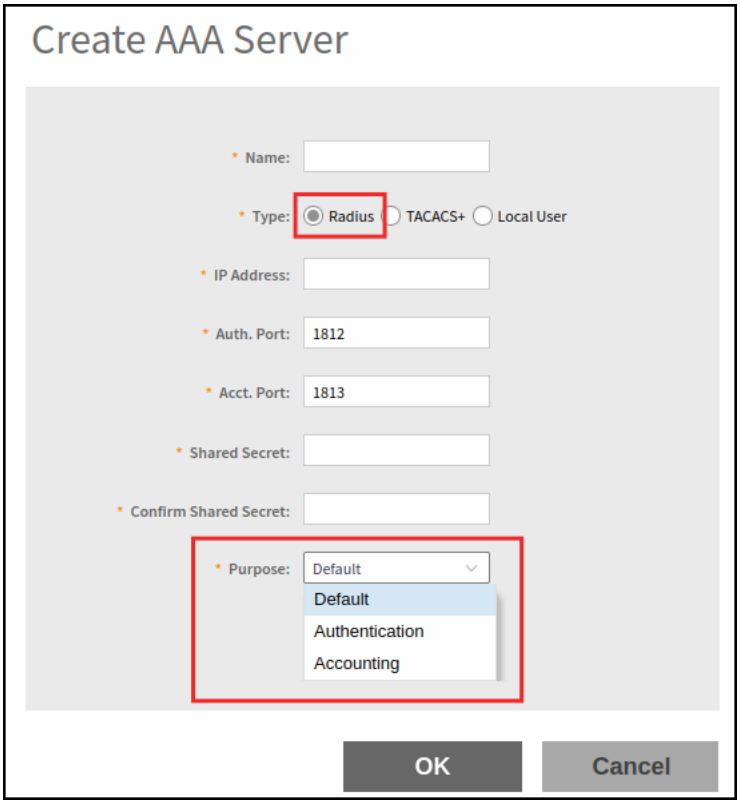
Configuring Switch AAA Servers

To add and manage Authentication, Authorization, and Accounting (AAA) servers that the controller can use for authentication, follow these steps.

1. Select **Network** > **Wired** > **Switches** The **Switches** window is displayed.
2. Select a **Domain** > **Switch Group** and scroll down to view the details.
3. In the **Common Configuration** tab, click the **Configure** icon to display the **Common Configuration** dialog box.
4. Click the **AAA** tab.
5. Expand the **AAA Servers** section.
6. Click the **[+Create]** icon.

   The **Create AAA Server** page is displayed.
7. Enter the AAA server name.
8. For **Type**, select **RADIUS**, **TACACS+** or **Local User** type of AAA server to authenticate user.

   FIGURE 143 Creating a Switch AAA Server with Type as RADIUS



9. **IP Address**: Enter the IP address of the AAA server.

10. **Auth. Port**: Enter the authentication port that the server is using.

    NOTE
    The default port number is 1812. If you need to enter any other value for the port number, it must be within the range of 0 to 65535.

11. **Acct. Port**: Enter the accounting port that the server is using.

    NOTE
    The default port number is 1813. If you need to enter any other value for the port number, it must be within the range of 0 to 65535.

12. **Shared Secret**: Enter the shared secret.
13. **Confirm Shared Secret**: Re-enter the shared secret to confirm.
14. **Purpose**: When Type=RADIUS, select the purpose for the RADIUS AAA server being created. Values are **Default**, **Authentication** and **Accounting** from the list.

    NOTE
    Starting with 7.0 release, you can set up multiple RADIUS servers with different options such as **Authentication** and **Accounting**. In earlier releases, the controller could only configure a RADIUS server for a switch with the **Default** option.

    NOTE
    The switch supports this setting on FastIron release 08.0.90 and later versions.

    When Type=TACACS+, select the purpose for the TACACS+ AAA server being created. Values are **Default**, **Authentication**, **Authorization**, and **Accounting**. When Type = Local User, select the privilege for the Local User server being created. Values are **Port Config** , **Read Only** and **Read Write**.

15. Click **OK**.

    You can subsequently edit or delete a AAA server by selecting the server from the list in the **AAA Servers** section and selecting **Configure** or **Delete**, respectively.

    NOTE
    The ICX switch fails to delete the TACACS+ and RADIUS AAA servers when pushed from SmartZone or Virtual SmartZone if SNMP query is disabled in the switch or if the switch is pre-configured before joining SmartZone or Virtual SmartZone.

Configuring Switch AAA Server Settings

To configure and manage AAA servers, complete the following steps.

1. Select **Network** > **Wired** > **Switches** > **AAA** .

2. Select **Switch AAA Setting**Select **Switch GroupConfigurationCommon ConfigurationConfigureAAA**, 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**.

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.

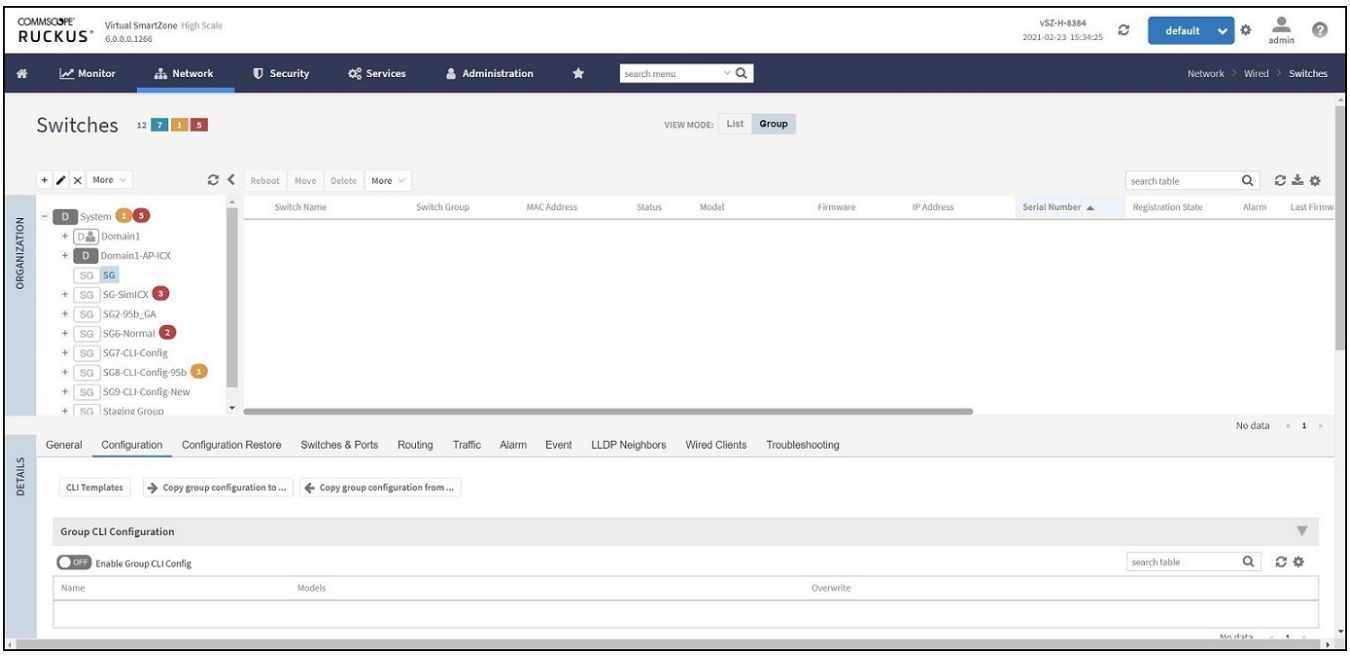
- After selecting the Group CLI configuration option, the existing GUI options at the switch group level are disabled, including common settings, model family based configurations, the **Copy configuration** to, and **Get configuration** from functions.
- If the Group CLI configuration is selected, only 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.

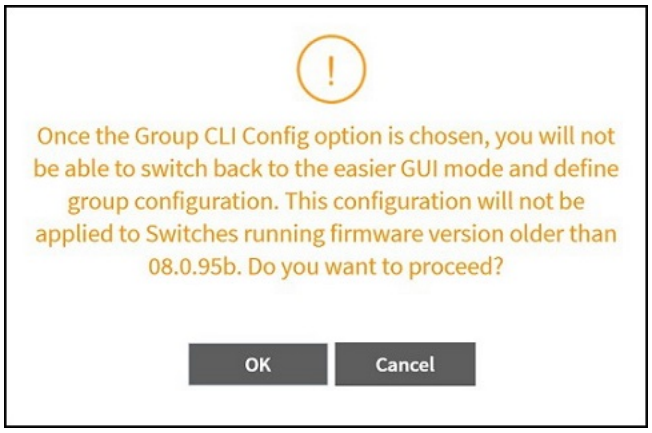
1. On the menu, click **Network** > **Wired** > **Switches** to display the **Switches** window.
2. In the **Organization** tab, select a **Domain** or **Switch Group** and in the **Details** tab, click **Configuration** tab.

   FIGURE 144 Enabling Group CLI Config setup



3. In the **Group CLI Configuration** tab, switch ON **Enable Group CLI Config** to display the **Confirming Group CLI Configuration Setup** dialog box.

   FIGURE 145 Confirming Group CLI Configuration Setup



4. Click **OK** to display the **Group CLI Configuration** dialog box.

5. In the **Choose Model**, select one or more ICX models to create a new Group CLI Configuration template and click **Next** to display the **CLI Configuration** tab. You can also select an existing ICX model and click **Next** to modify the Group CLI configuration.

   NOTE
   The RUCKUS ICX devices that have already been selected in the Group CLI Configuration will not be available.

FIGURE 146 Choosing ICX Models

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 147 Entering the Name in the new Group CLI Configuration

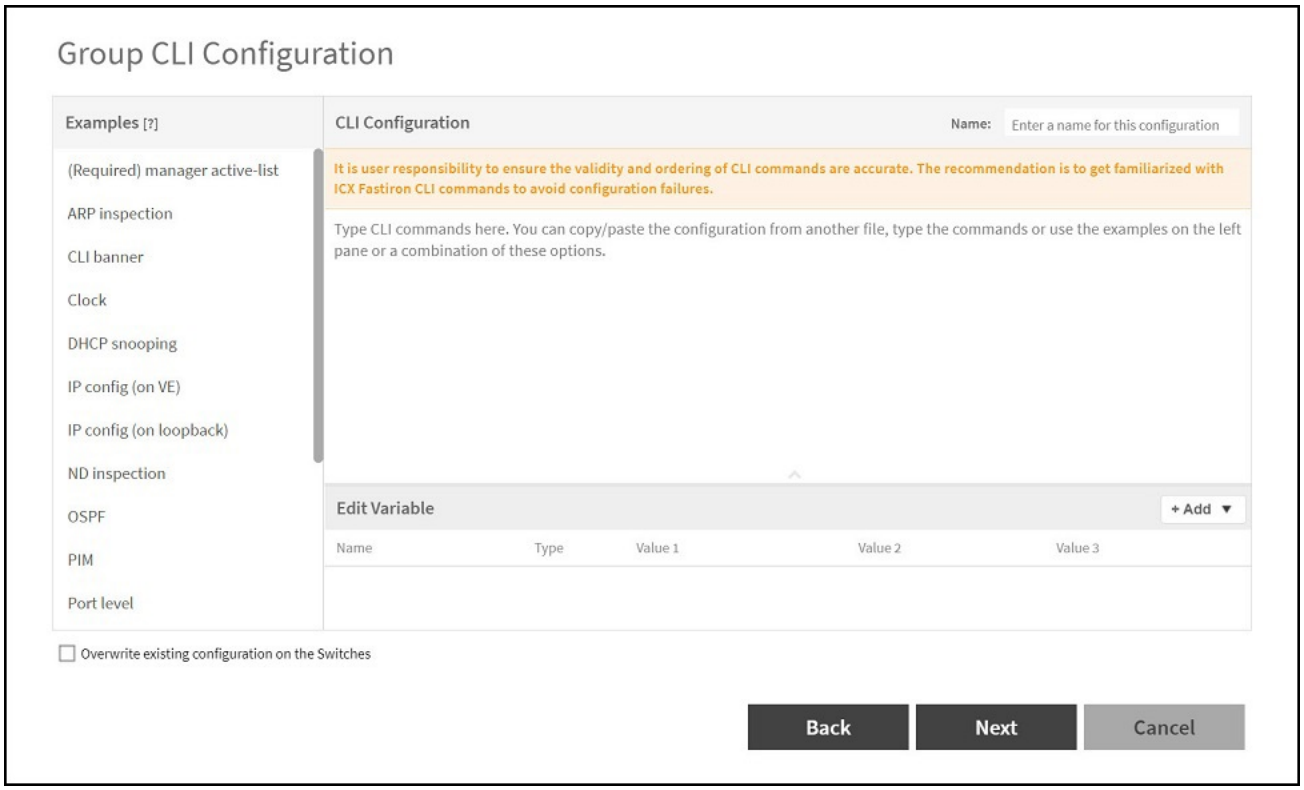


FIGURE 148 Inserting Command Lines in the New Group CLI Configuration

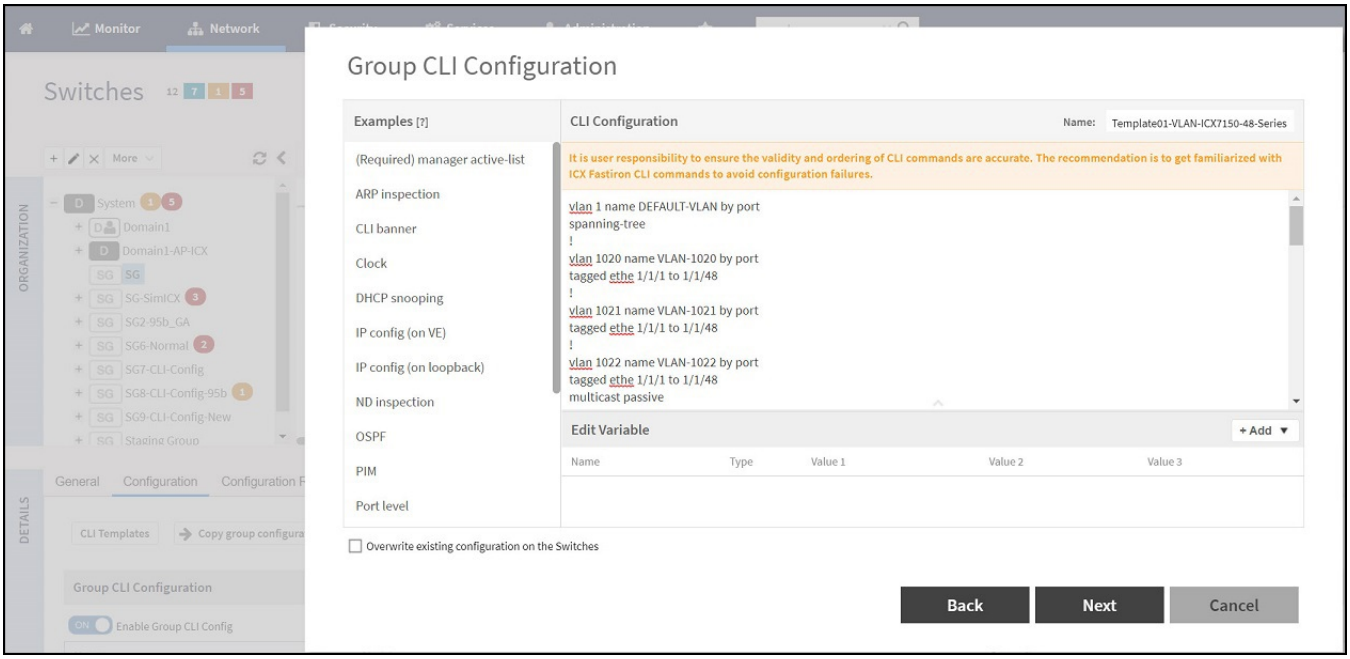


FIGURE 149 Support for space in variable string

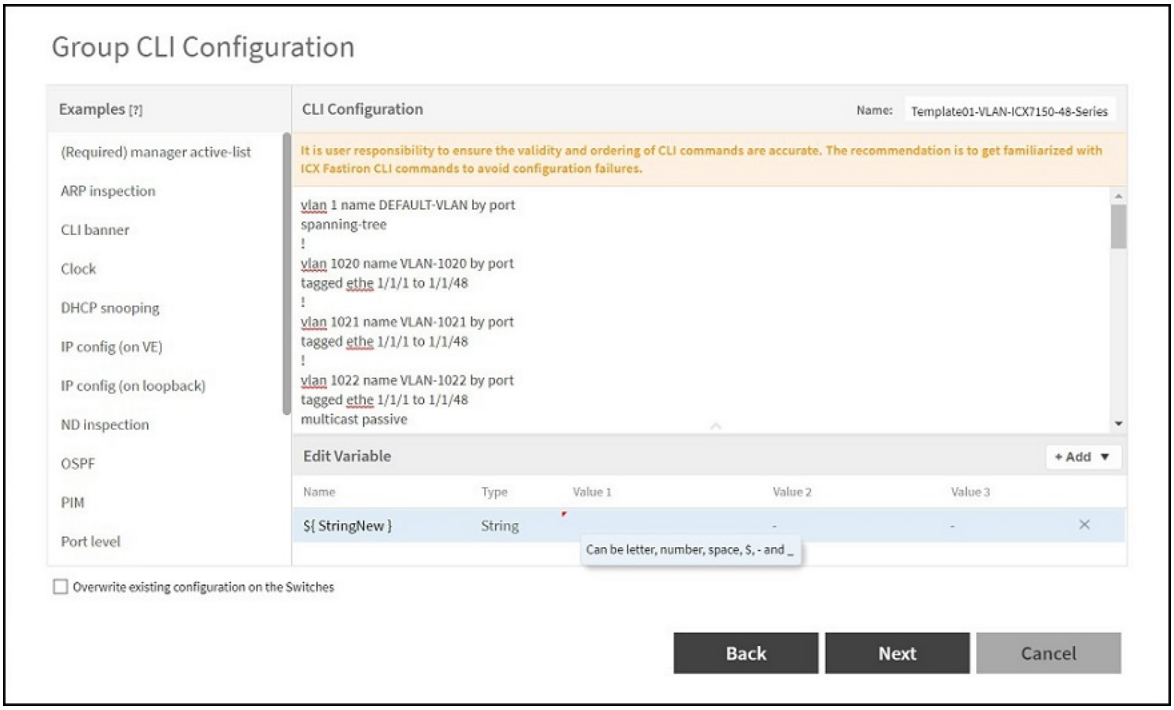


FIGURE 150 Support for dollar sign in variable string

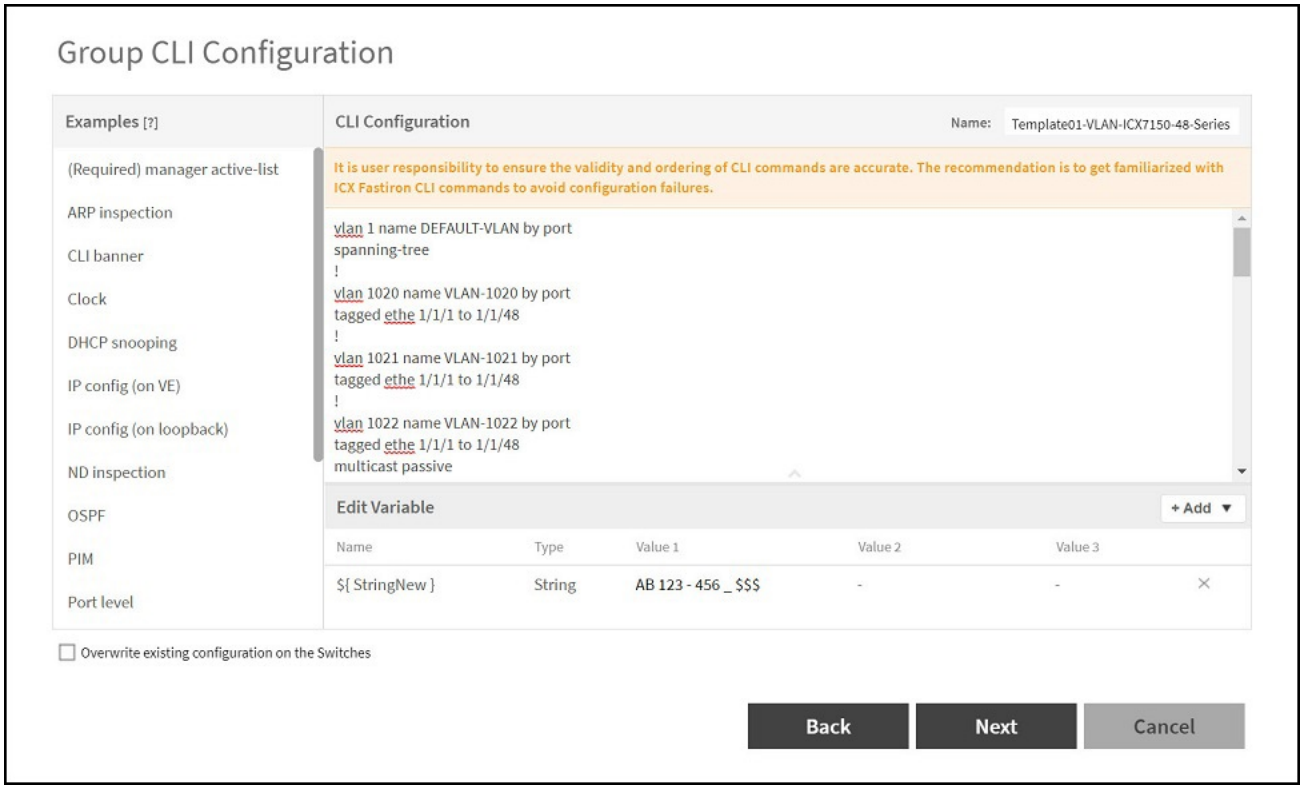


FIGURE 151 Example Template

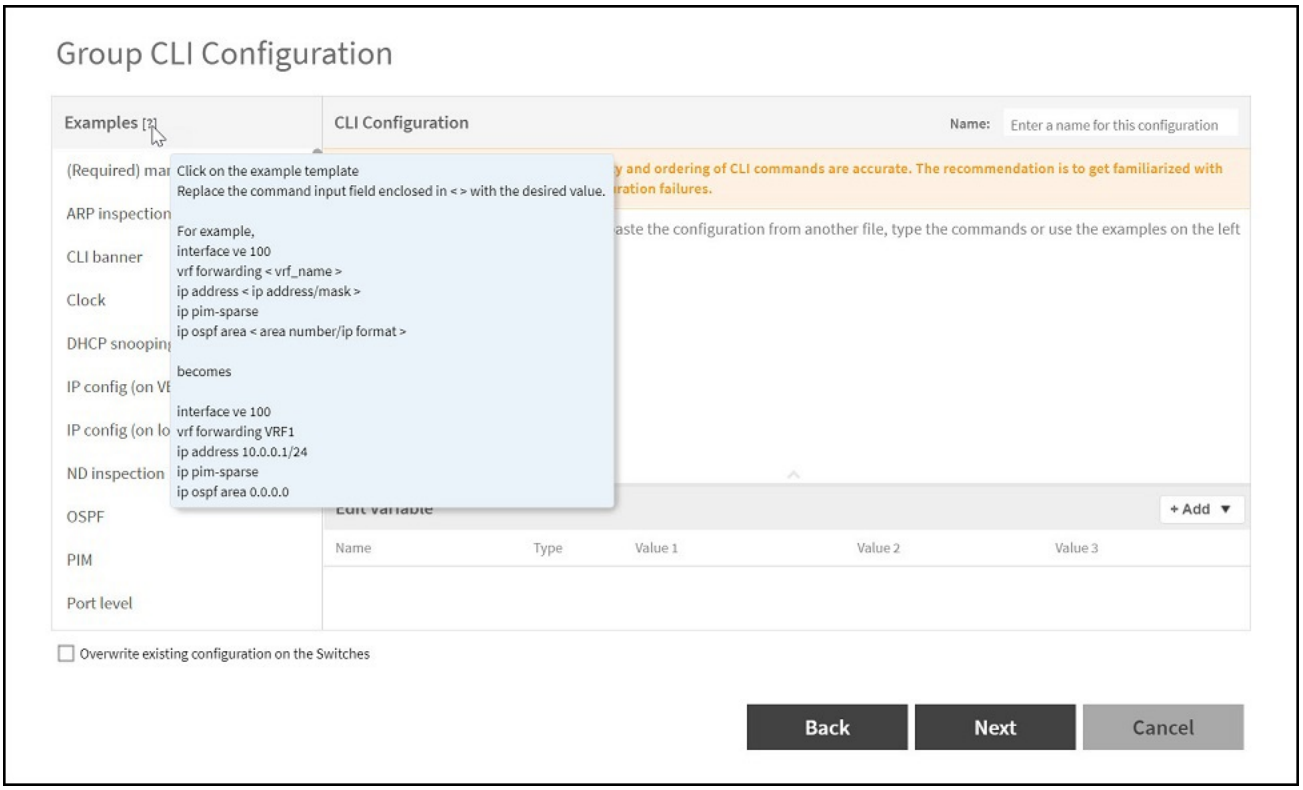


FIGURE 152 Support for IP address in Variable

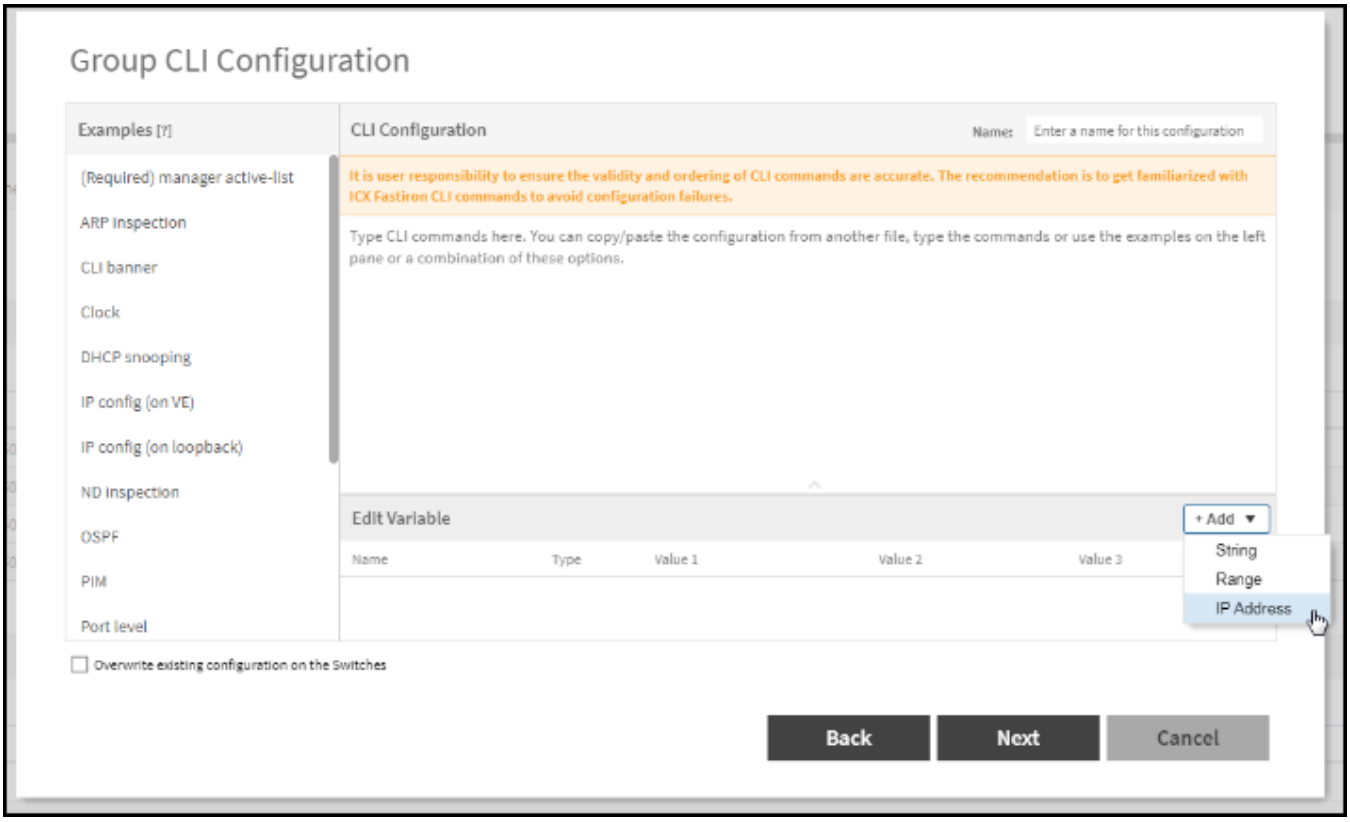


FIGURE 153 Details of fields in IP address in Variable

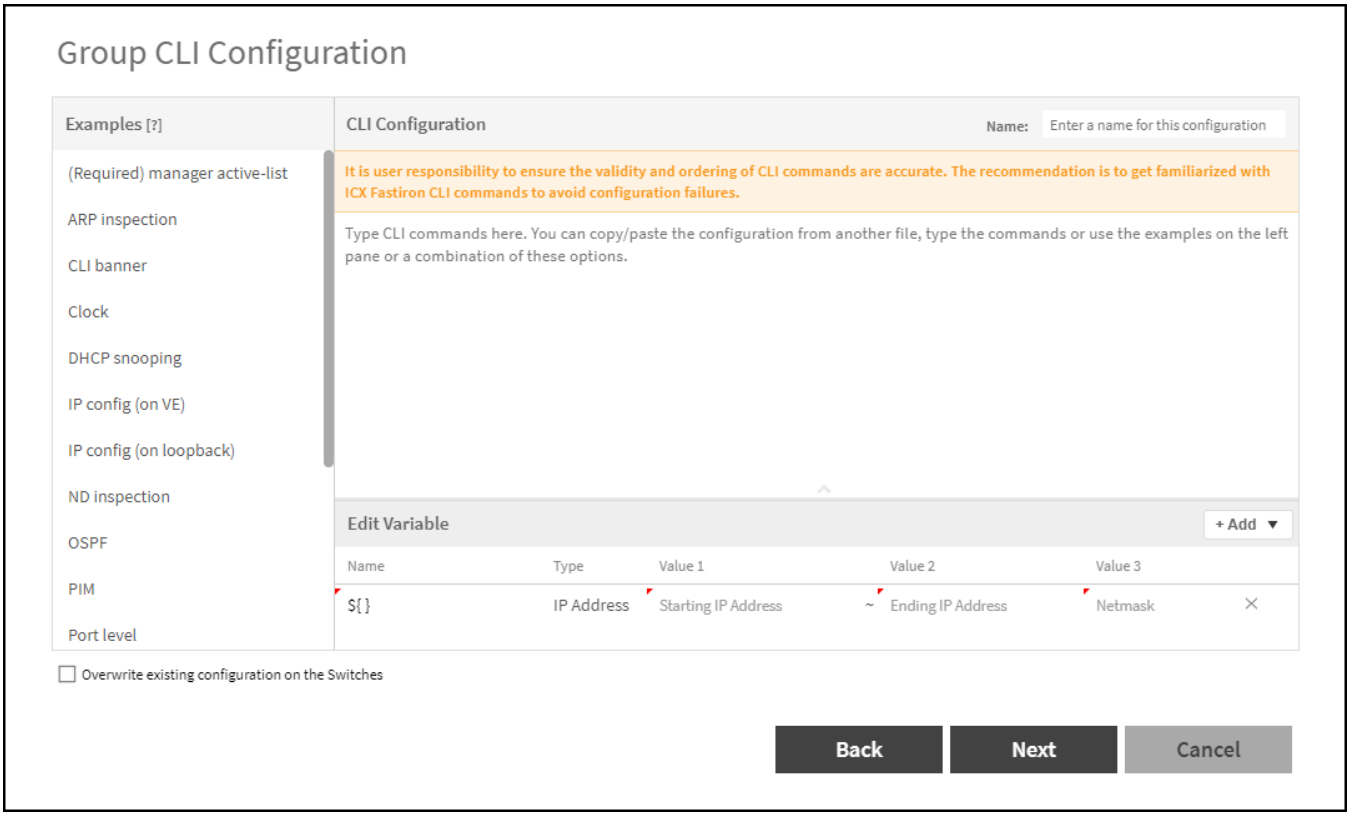
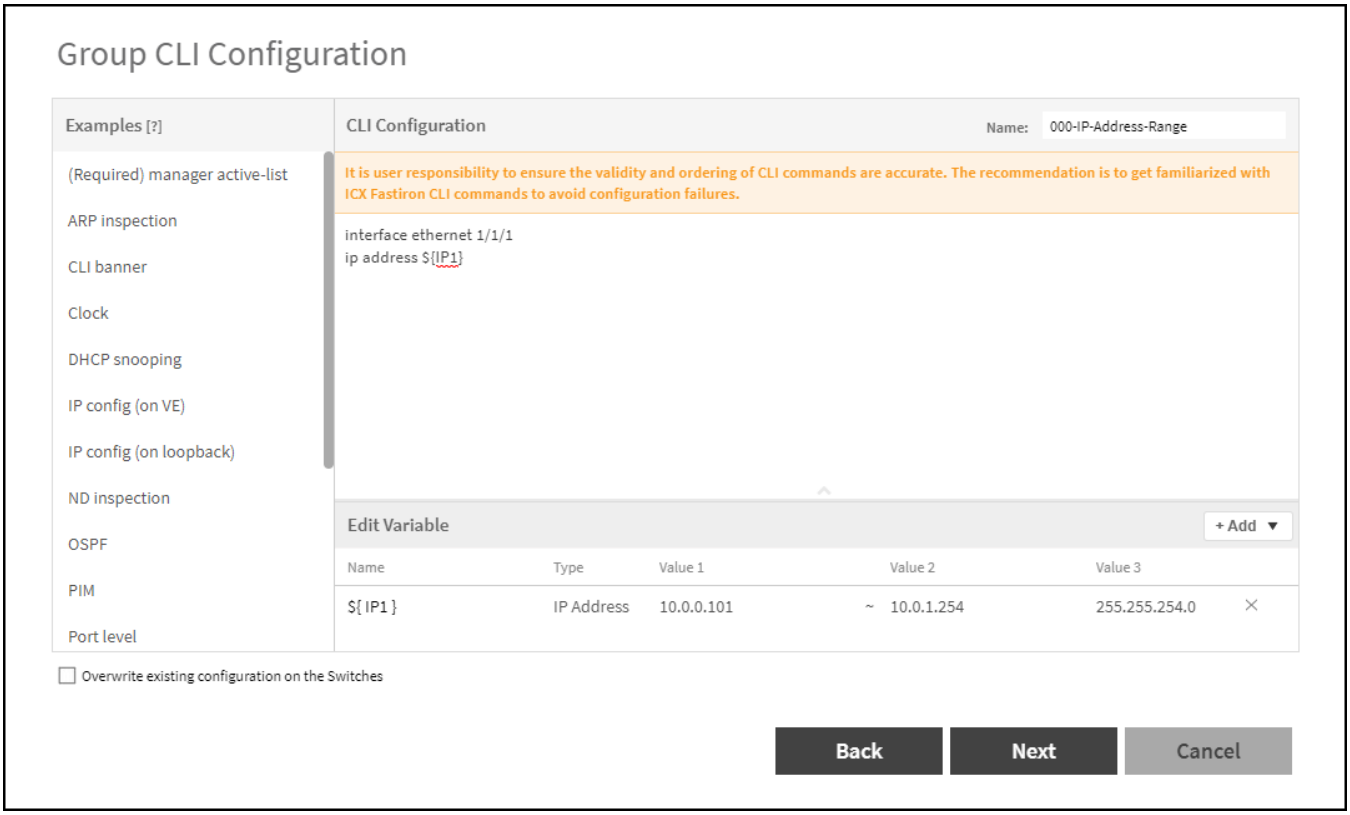


FIGURE 154 Example for IP address in variable



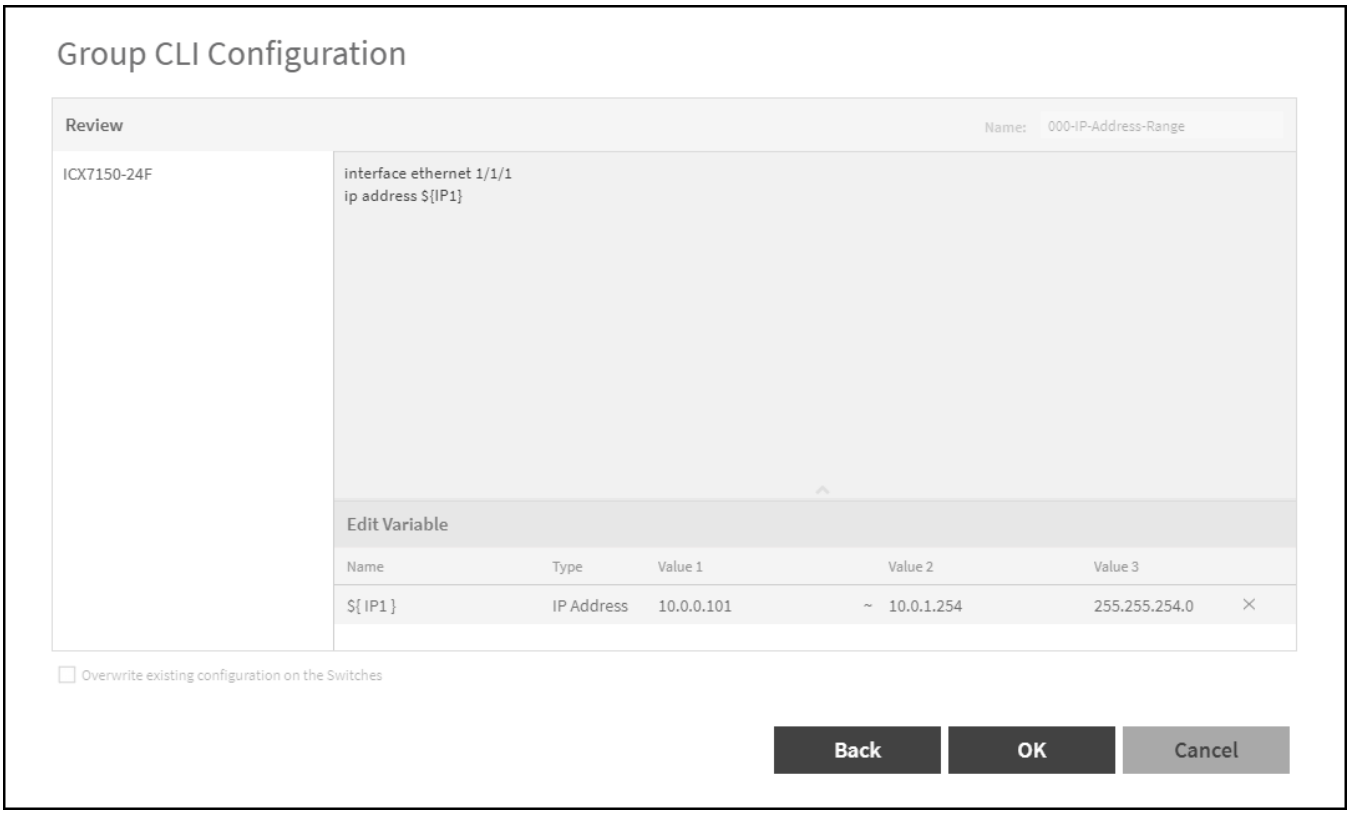
7. Variables asists in applying unique configuration to the switches. For example, IP address can be defined as a variable so that each switch gets assigned a unique IP address . In the **Edit Variable** field, enter the **Name**, **Type**, **Value 1**, **Value 2** and **Value 3** of the variables, where **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, the controller will replace the existing configuration of the switch with the configuration defined for the group.

8. After reviewing the Group CLI Configuration, click **OK**.

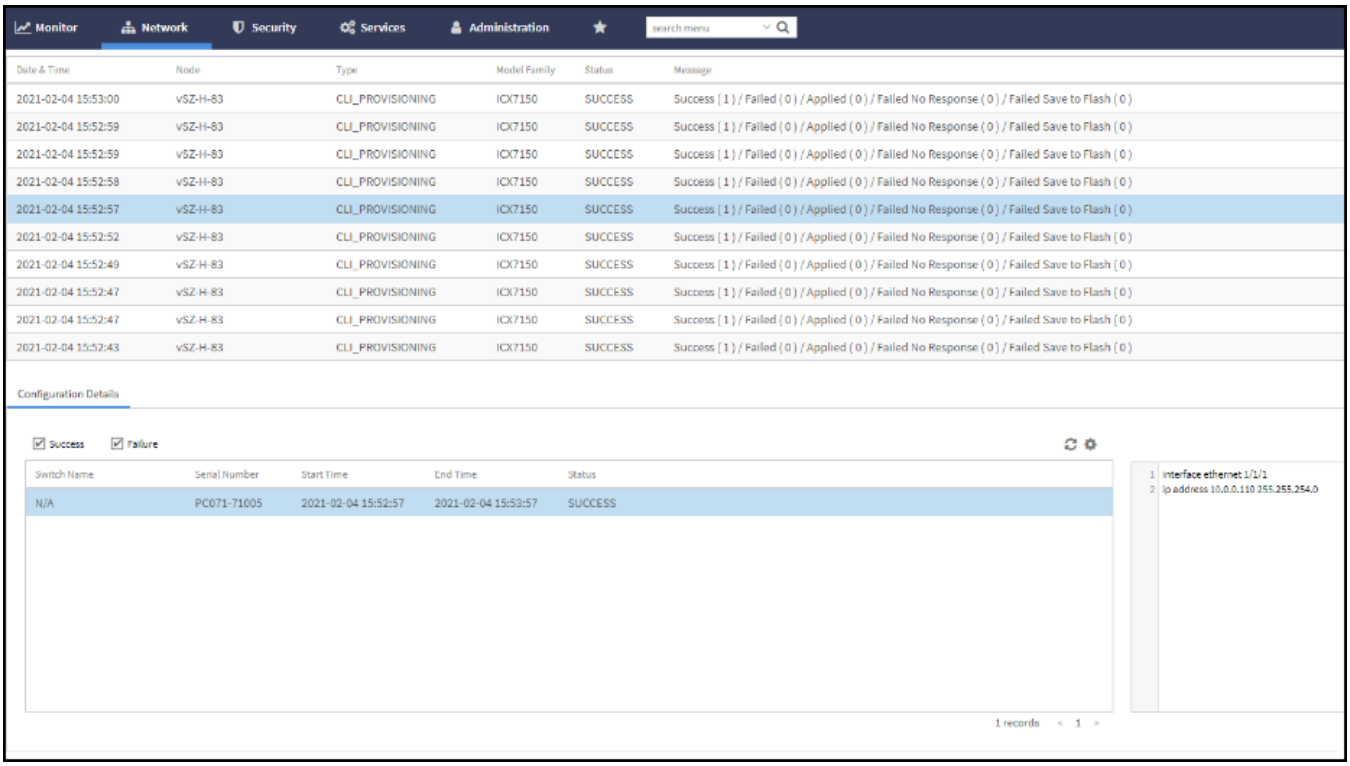
FIGURE 155 Reviewing the Group CLI Configuration



9. A confirmation dialog box is displayed, click **OK**.

10. The switch group is now Group CLI Configuration enabled and is available for provisioning.

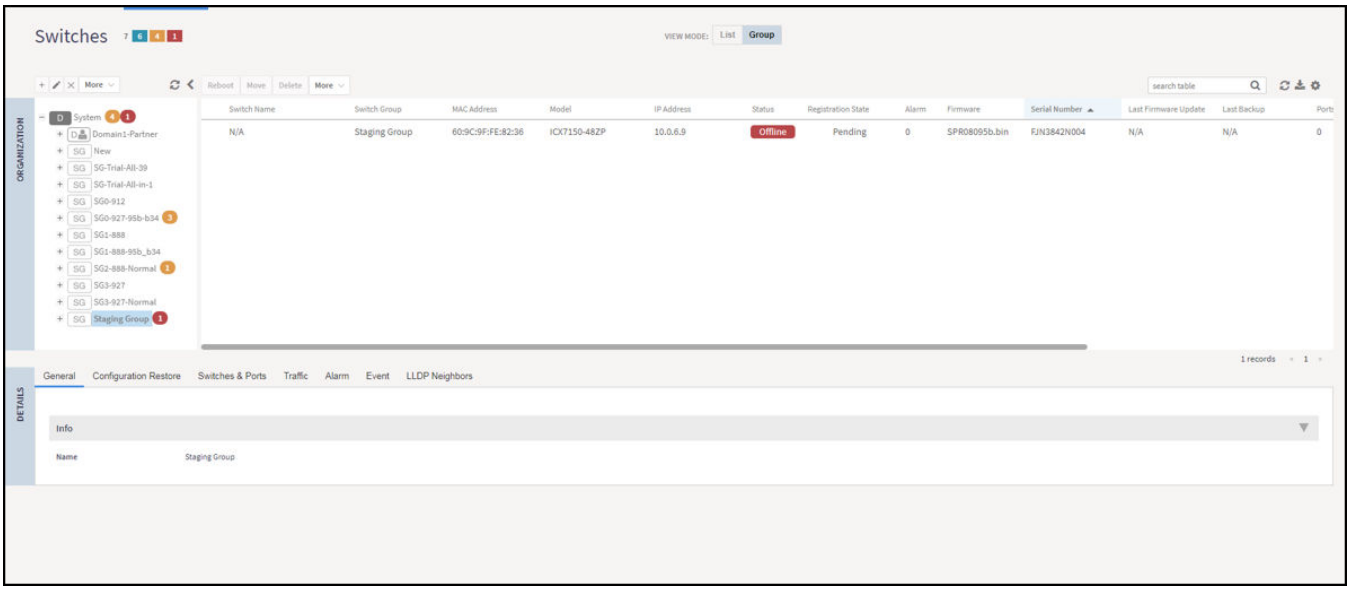
FIGURE 156 Provisioning the Group CLI Configuration Setup



11. After the configuration is setup, any factory default switch joining the group will have the configuration applied and will be rebooted for the changes to take effect.

12. In the **Organization** tab, select a **Domain** or **Switch Group** and select the **Switches** .

FIGURE 157 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.

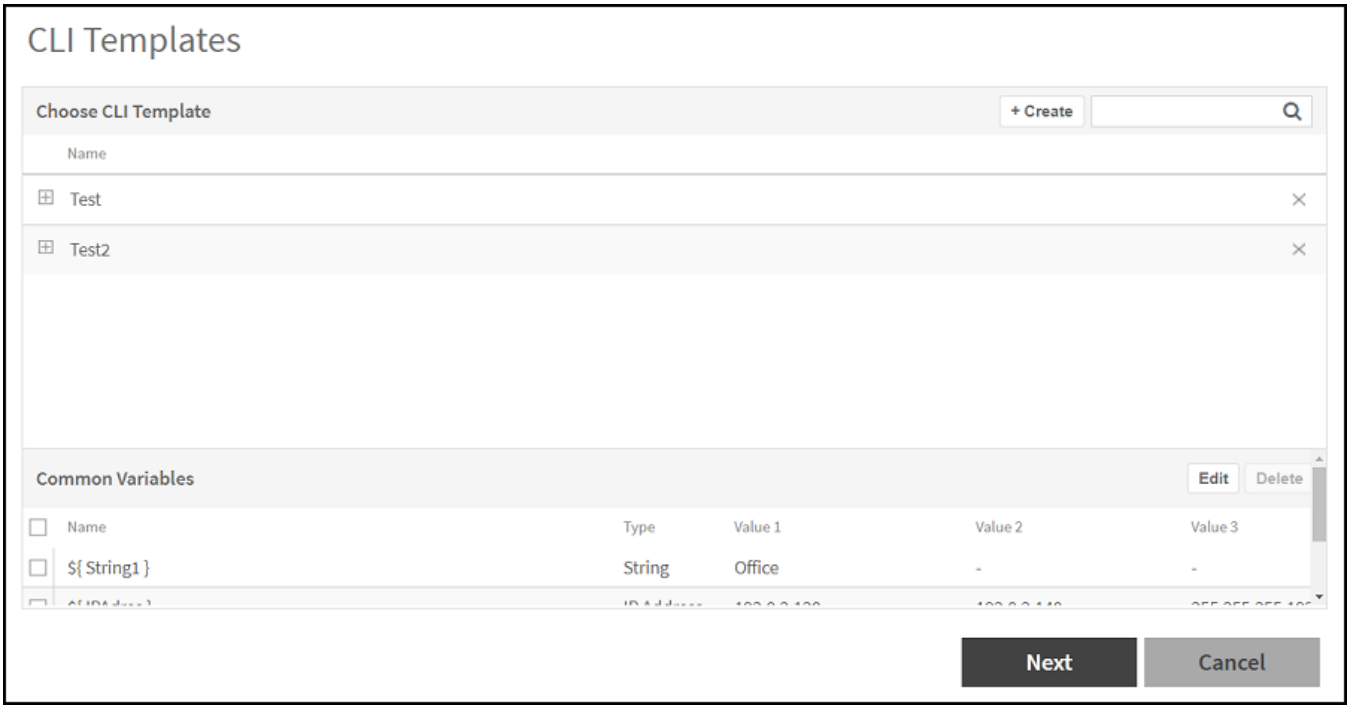
Using CLI templates

1. On the menu, click **Network** > **Wired** > **Switches** to display the **Switches** window.
2. In the **Organization** tab, select a **Domain** > **Switch Group** or **Switch Group** and in the **Details** tab, click **Configuration** tab.

3. Click **CLI template** icon to display the **CLI Templates** dialog box. You can select an existing CLI template with an existing common variables or create a new CLI template with a new common varibles.

   NOTE
   To edit existing common variables or add common variables. Click **Edit** icon, modify the common variables or add common variables and then click **Save**. For more information, see *Step 4 b Edit Variable*.

FIGURE 158 CLI Template

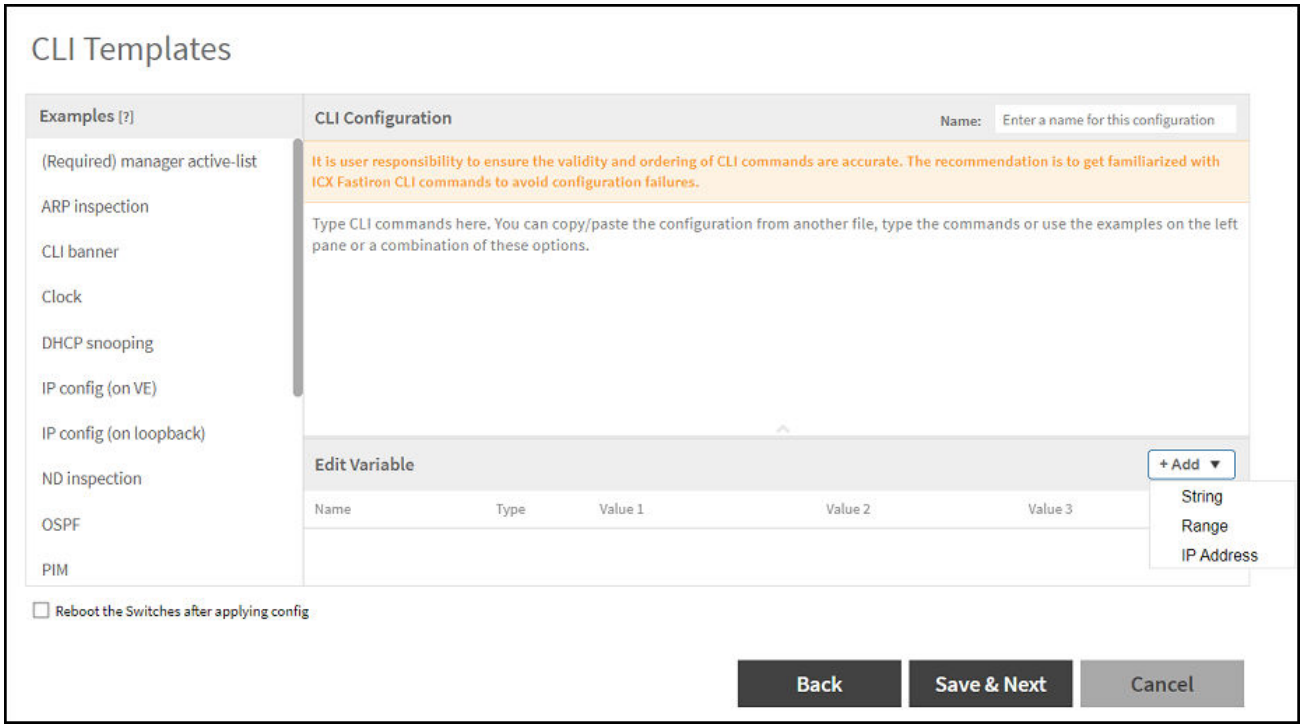


4. Complete the following steps to create a new CLI template.

   a) Click 

icon to display the **CLI Templates** dialog box.

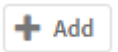
   FIGURE 159 CLI Templates Dialog Box



   b) Complete the following fields:

   - **Name**: Enter the name of the CLI template.
   - **Command Lines**: Insert or edit 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.

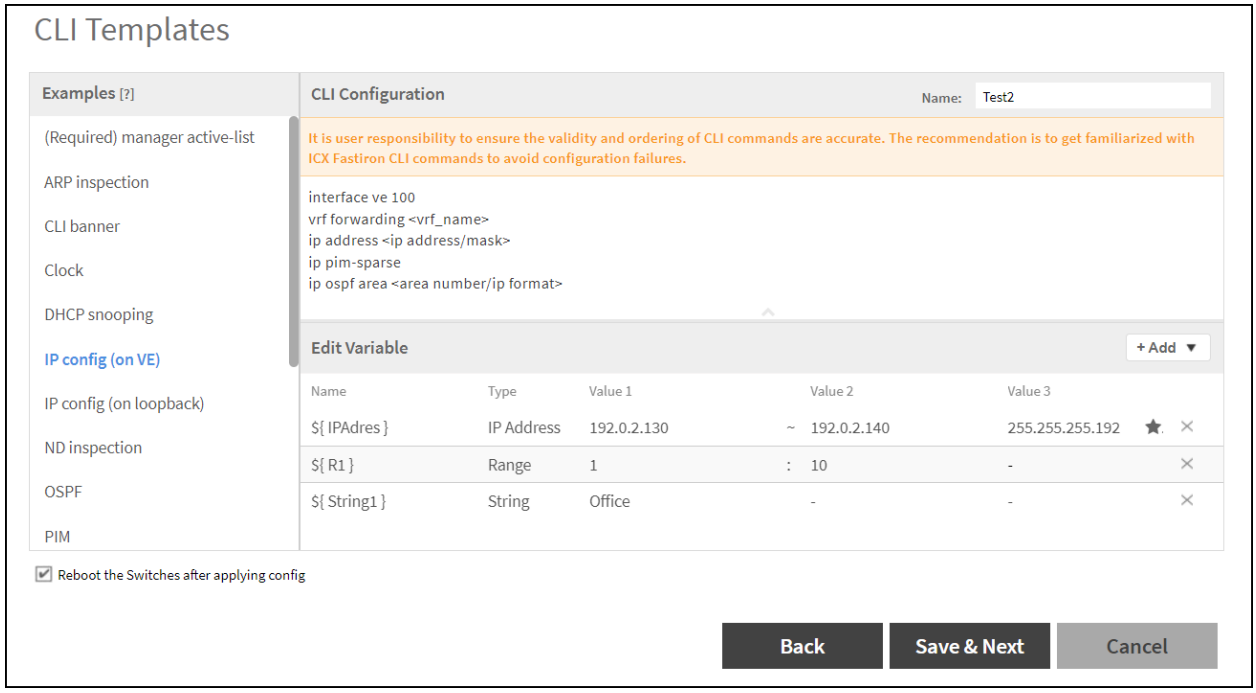
     NOTE
     It is recommended that users get familiarized with FastIron commands and their ordering to avoid any issues with applying the configuration.

   - **Edit Variable**: Click 

icon and select the **String** or **Range** or **IP Address** variable to add the **String** or **Range** or **IP Address** variable to the table. 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". Click  icon to add a new variables setting to the Common Variables.

     NOTE
     The **Edit Variable** field is optional.

FIGURE 160 Adding Common Variables

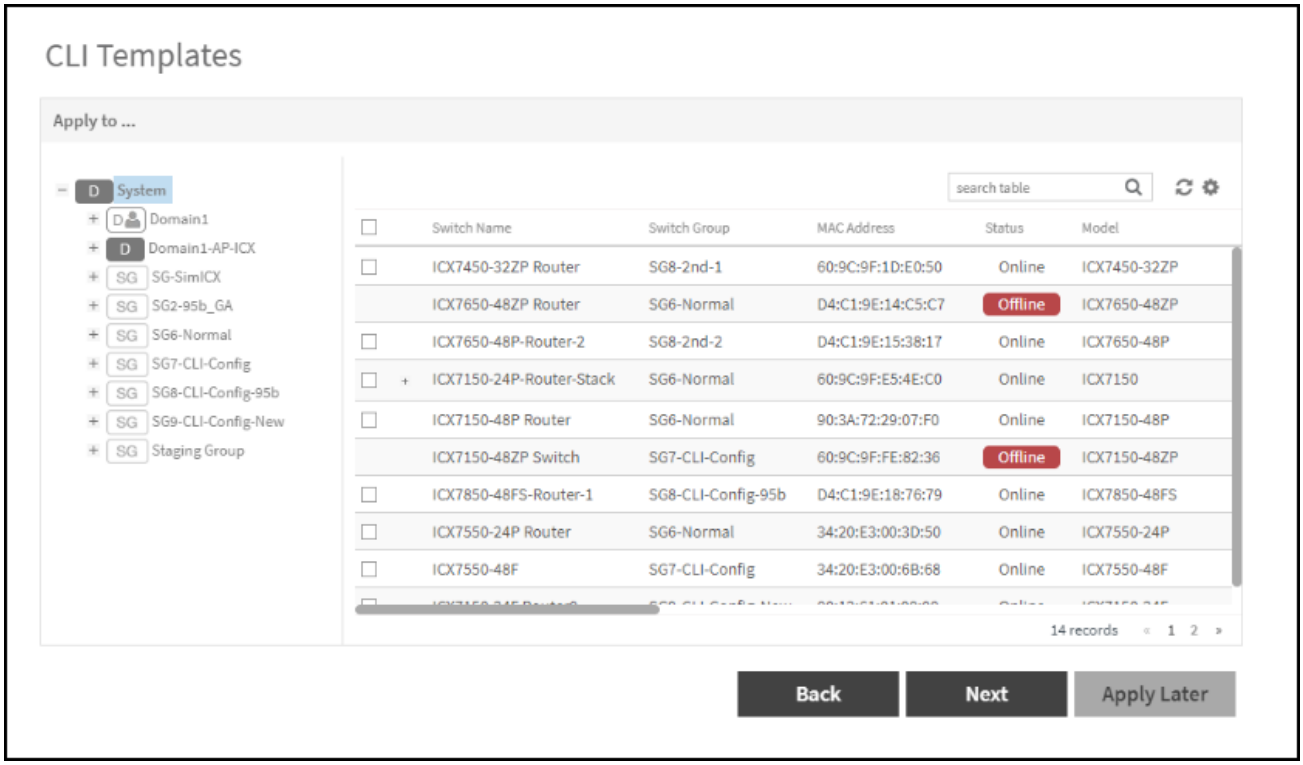


c) Select **Reboot Switches after applying config** check box if you want the switch to reload after the configuration update. If you do not select this option, the switch will not reload after the configuration update.

d) Click **Save & Next**.

e) Select the target switches check box and click **Next** to display the **Review** dialog box.

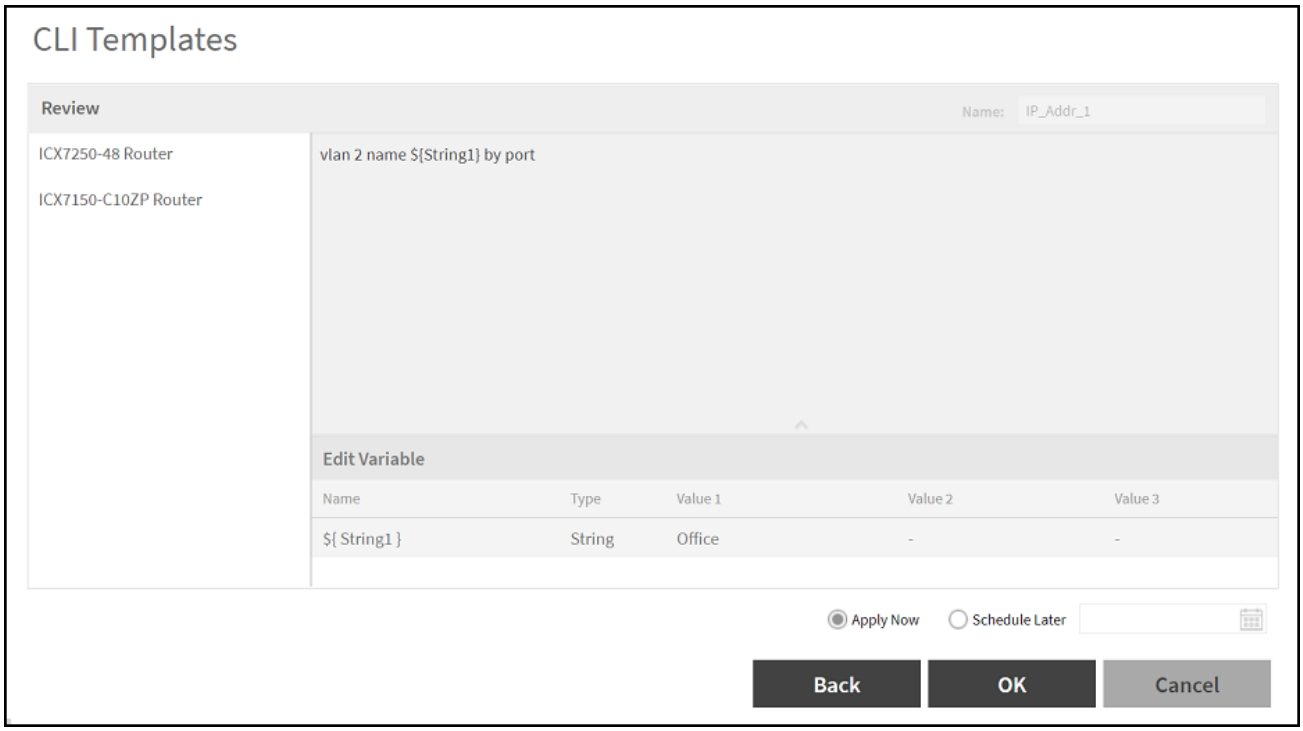
FIGURE 161 Selecting Switches



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.

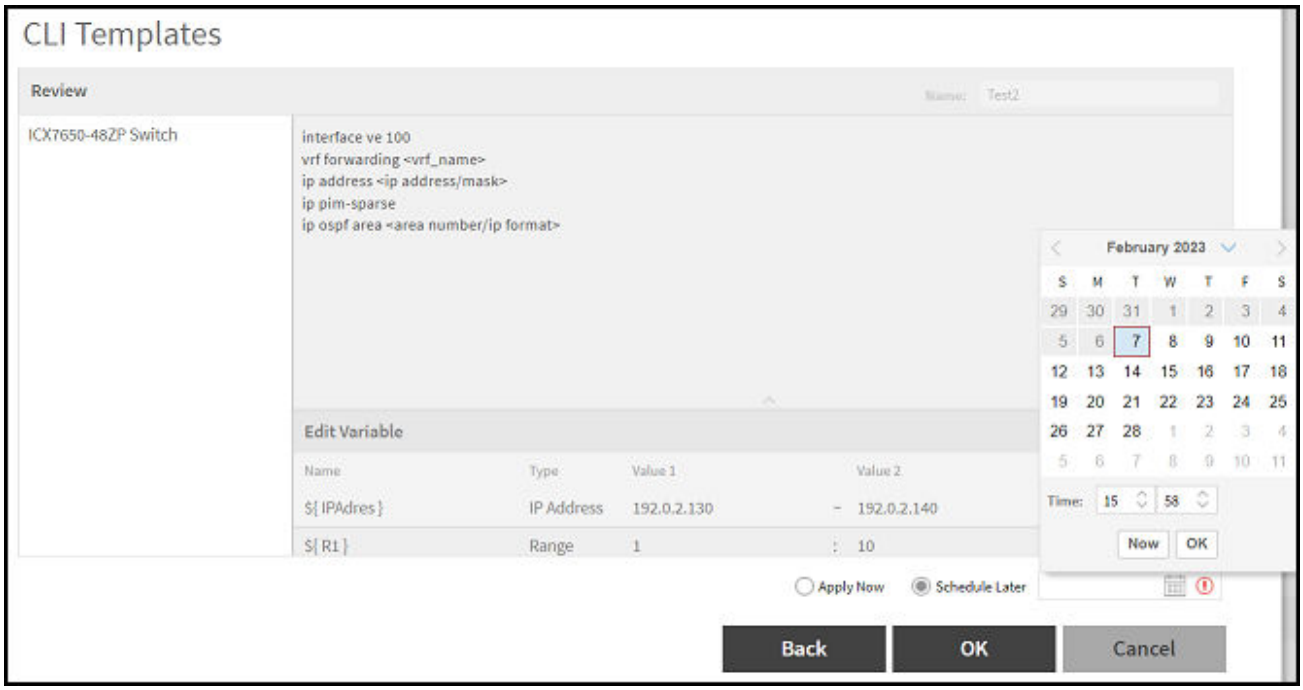
f) Review the CLI template.

FIGURE 162 Reviewing the CLI Template



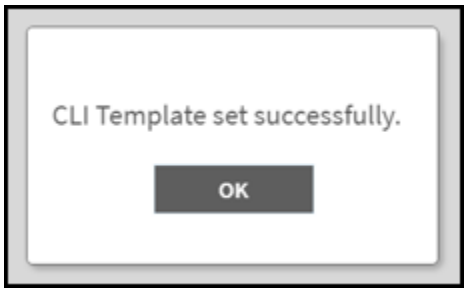
g) Select **Apply now** or **Schedule Later** to save the created template and apply to the selected switches. If you select the **Schedule Later** then select the **Date** and **Time** to apply the configuration.

FIGURE 163 Schedule Later Dialog Box



h) Click **OK** to display the **CLI Template Set Successfully** message.

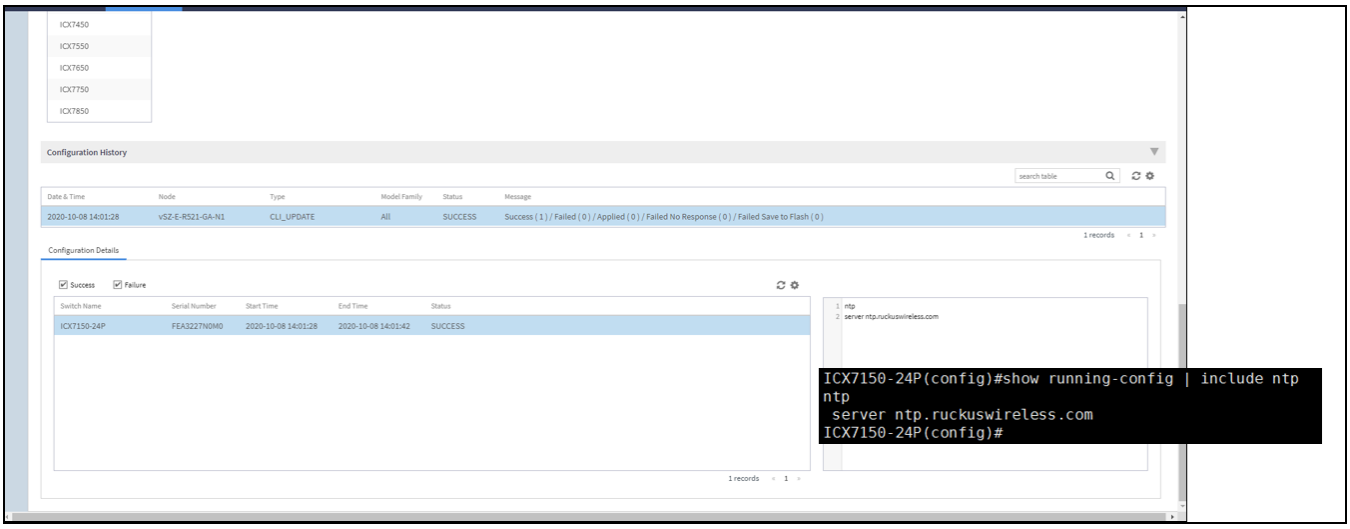
FIGURE 164 Applying the CLI Template



i) Click **OK**.

5. In the **Organization** tab, select a **Domain** > **Switch Group** or **Switch Group** and in the **Details** tab, click **Configuration** tab.
6. In the **Configuration History** tab, select the **Switch** to display the **Configuration Details** tab. Make sure that the CLI template is successfully added to the switch.

FIGURE 165 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.

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.

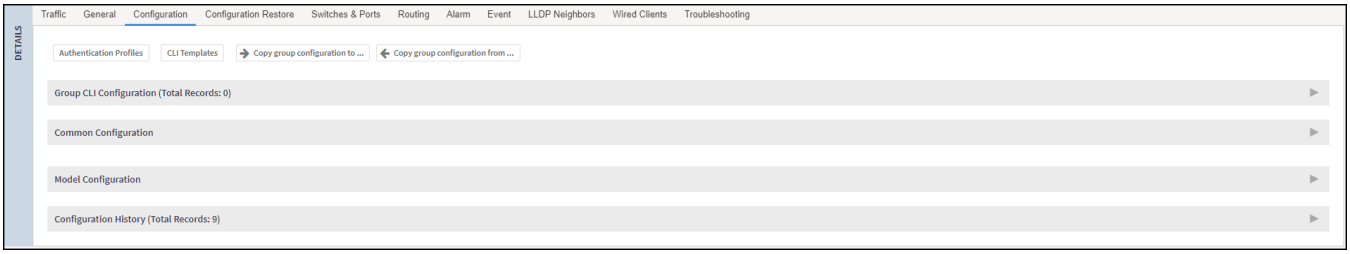
NOTE
ICX switches must run FastIron 08.0.90a or later release to take advantage of the switch configuration capabilities of the controller.

Creating a Common Configuration

You can create, view, and edit the configuration settings for a group of switches.

1. On the menu, click **Network** > **Wired** > **Switches** to display the **Switches** window.
2. From the system tree, select a **Domain** > **Switch Group** or **Switch Group** and in the **Details** tab, click the **Configuration** tab.

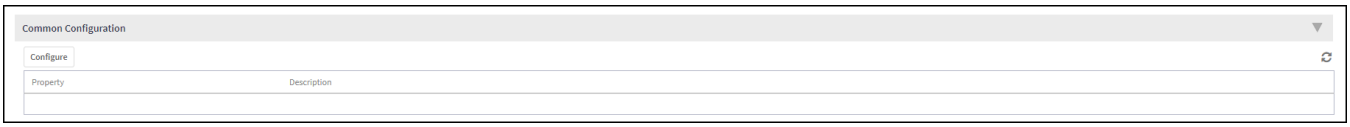
FIGURE 166 Configuration



3. In the **Common Configuration** tab, click **Configure** to display the **Common Configuration** dialog box.

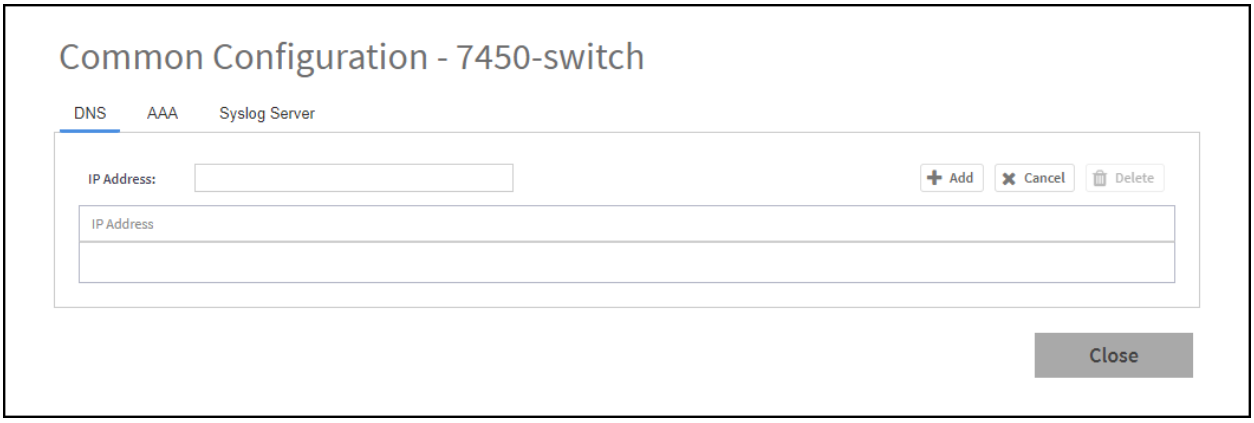
   NOTE
   In the following example, the Switch Group is the Default Group.

FIGURE 167 Common Configuration



a) Configure the **DNS** settings.
   1. Click the **DNS** tab.

      FIGURE 168 DNS Settings

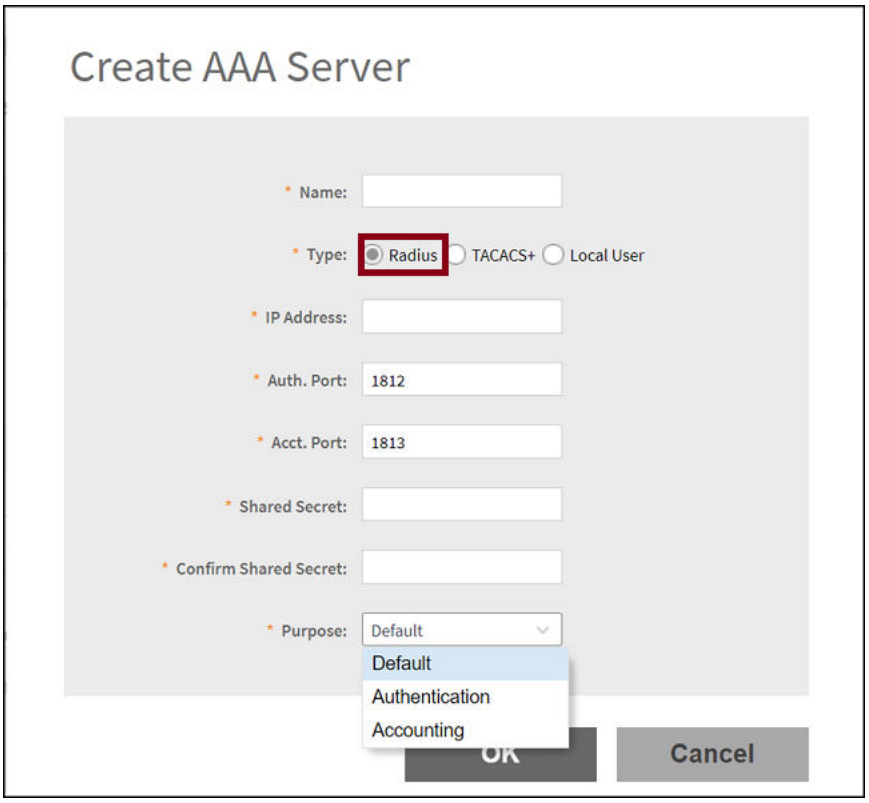


   2. Enter the **IP address** and click **Add**.

   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.

b) Configure the **AAA** settings.
   1. Click the **AAA** tab.
   2. Expand the **AAA Servers** section and configure one or more AAA servers.
      a. Click the  icon to display the **Create AAA Server** dialog box and complete the AAA server configuration, refer to *Configuring Switch AAA Servers* in the *RUCKUS SmartZone Management Guide*.

         FIGURE 169 Creating AAA Server

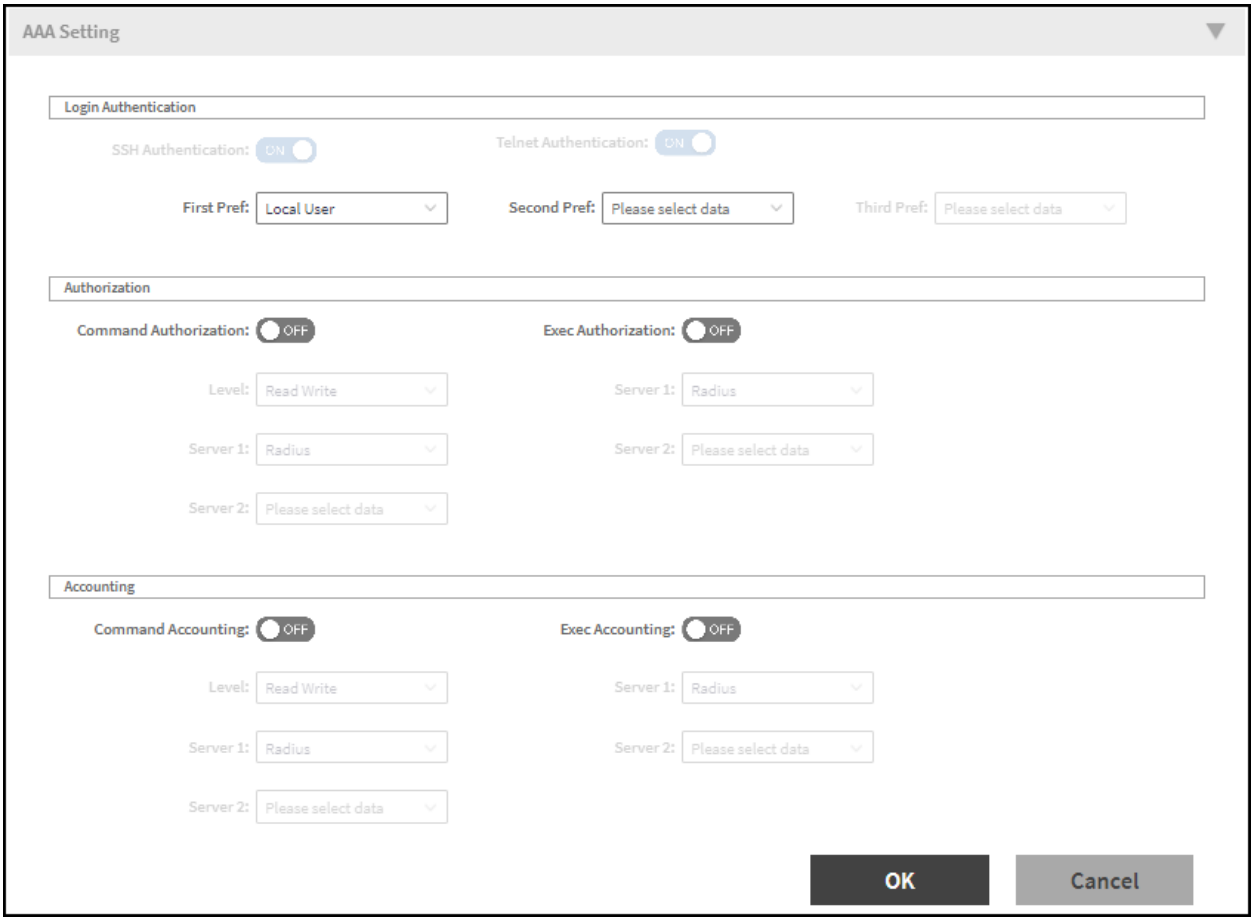


b. Click **OK**.

NOTE
You can subsequently edit or delete a AAA server by selecting the server from the list in the **AAA Servers** section and selecting **Configure** or **Delete**, respectively.

3. Configure the **AAA Setting**.

FIGURE 170 AAA Setting



a. Complete the **AAA Settings**. For more information on configuring and managing AAA servers for user authentication, refer to Configuring Switch AAA Server Settings in the *RUCKUS SmartZone Management Guide*.

b. Click **OK**.

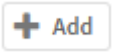
c) Configure the **Syslog Server** settings.

1. Click the **Syslog Server** tab.

NOTE
This feature is supported on FastIron 08.0.95 and later releases.

2. Complete the following fields:
   - **IP address**: Enter the **IP address** of the remote syslog server. Click **Cancel** to erase the entry in the field.
   - **Port**: Enter the port number in the **Port** field.

     NOTE
     The default setting is UDP port 514, but this can be changed as per your network requirements.

3. Click the  icon.

   NOTE
   Select the IP Address and click the **Delete** icon to delete the syslog server **IP Address**.

d) Click **Close**.

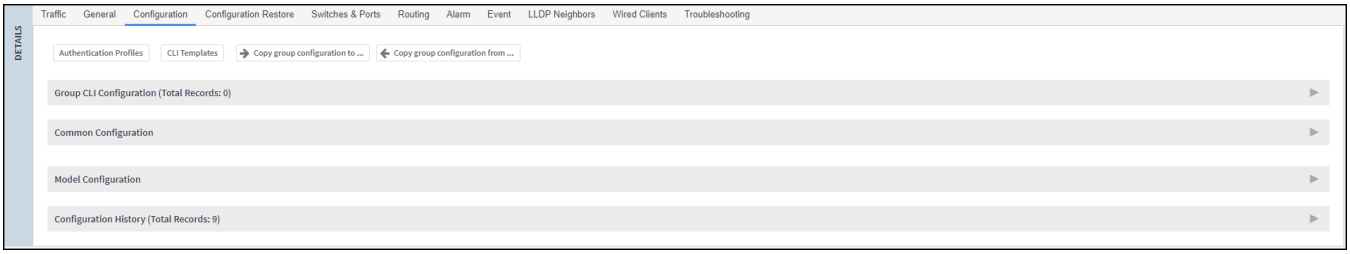
Creating Switch Model-Based Configurations

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. On the menu, click **Network** > **Wired** > **Switches** to display the **Switches** window.
2. Select **Domain** > **Switch Group** or **Switch Group** and click the **Configuration** tab.

FIGURE 171 Configuration



3. In the **Model Configuration**, select the **Switch Model** from the drop down list and click **Configure** to display the **Feature Configuration** dialog box.

FIGURE 172 Model Configuration

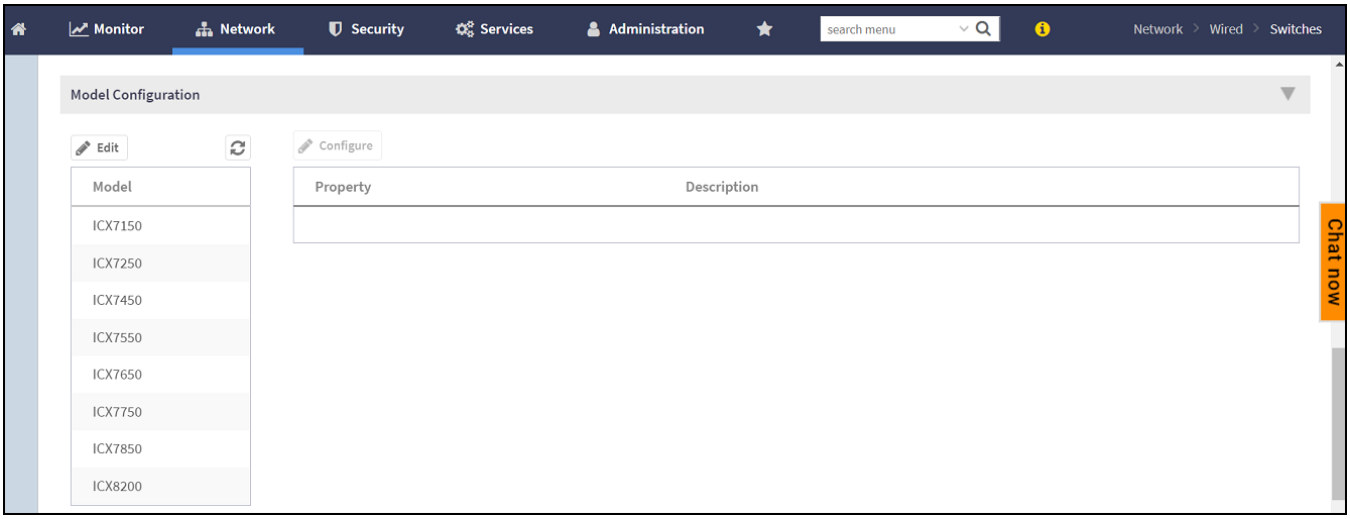
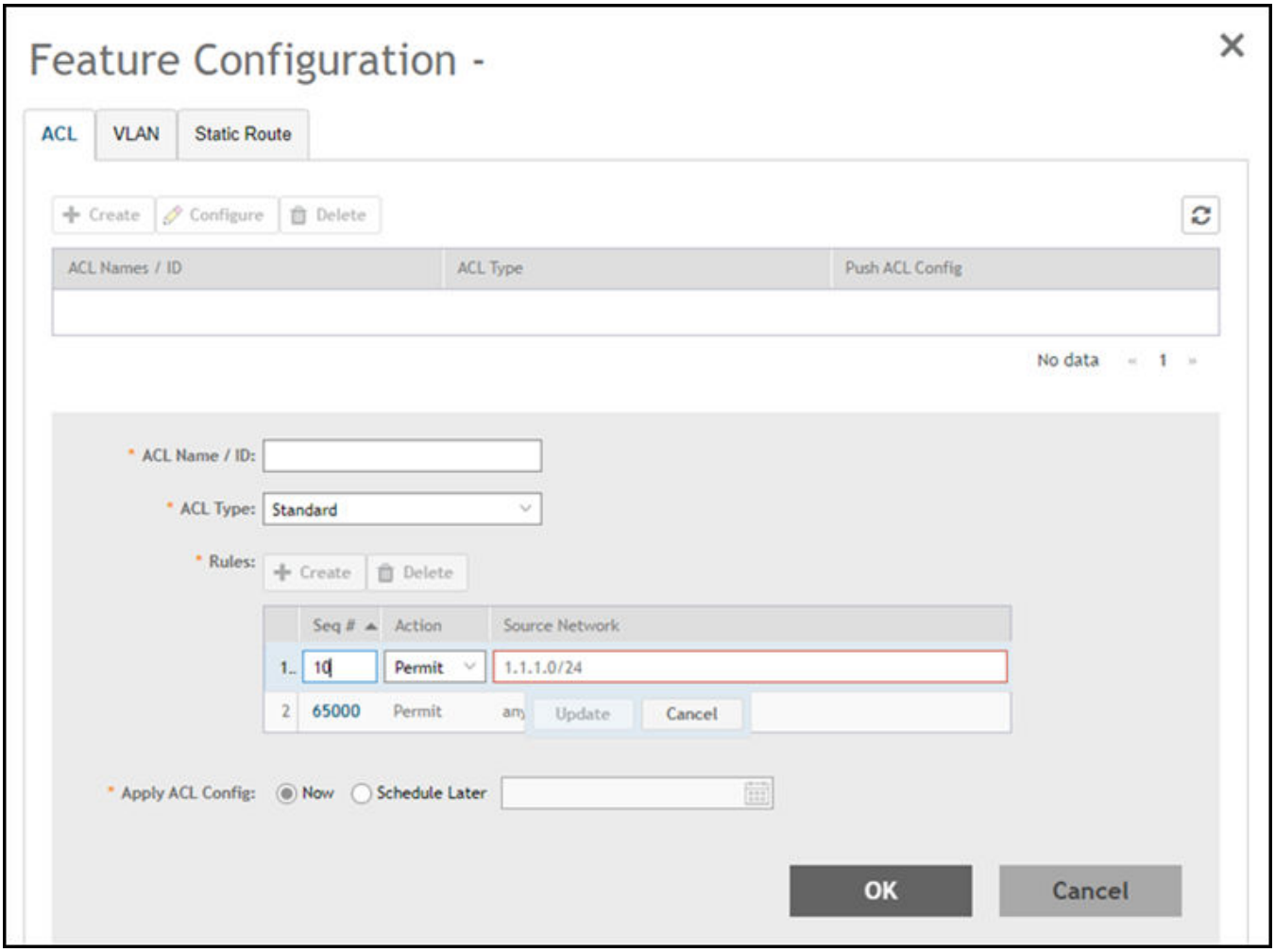


FIGURE 173 Feature Configuration

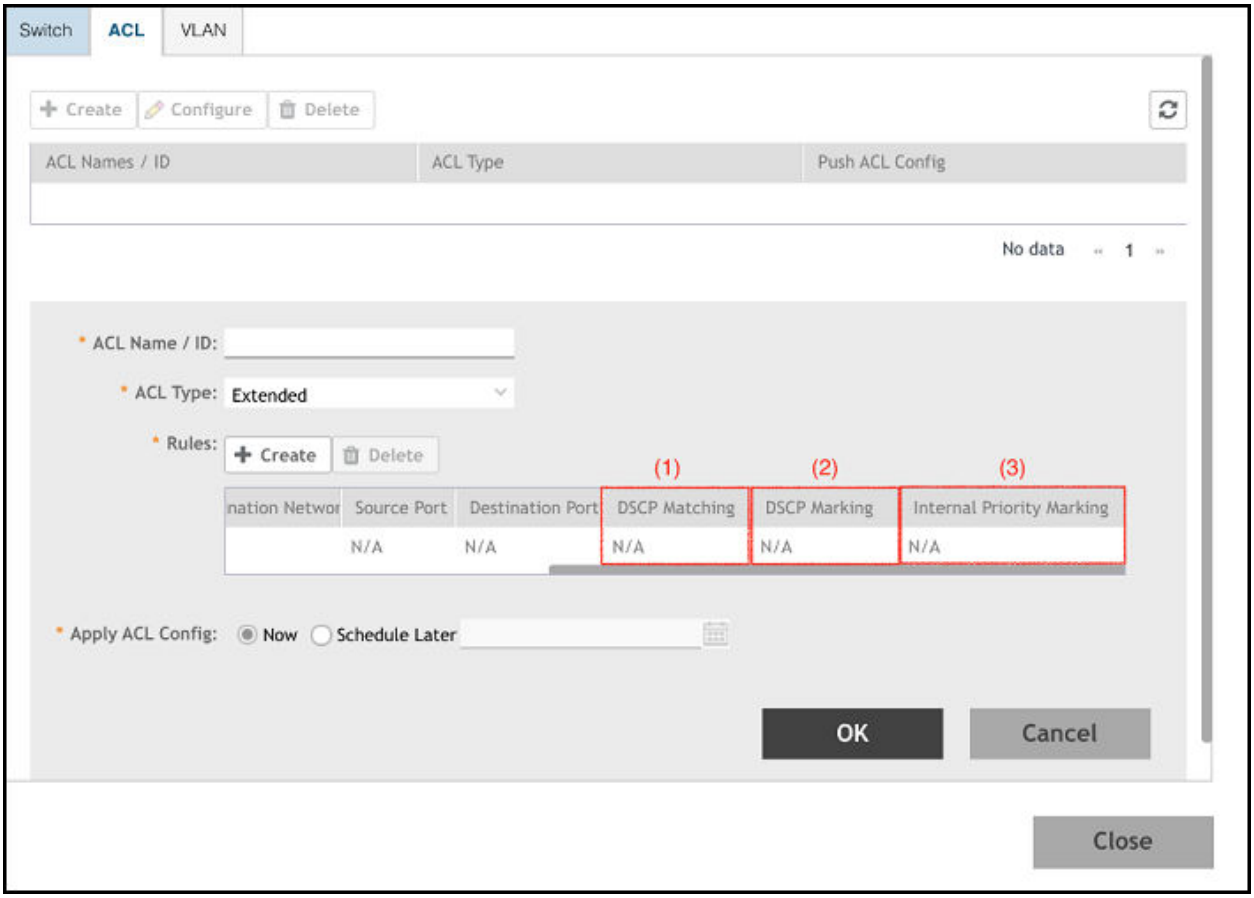


NOTE
The **Feature Configuration** page displays details about the ACL, VLAN, and static route. You can create, edit, and delete these configurations as necessary.

a) Configure the **ACL** settings.

1. Click the **ACL** tab.
2. Click the  icon to display the **ACL** fields.

FIGURE 174 ACL Configuration with ICX Firmware version 08.0.95 - Extended ACL Type



3. Complete the following fields:
   - **ACL Name/ID**: Enter the name of the access control list or provide the list identifier.
   - **ACL Type**: Select Standard or Extended from the drop down list.
   - **Rules**: Click **Create** to create an ACL rule.
     - Complete the following fields to configure the following ACL rule for the Standard ACL type:

       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.

     - Complete the following fields to configure the following ACL rule for the Extended ACL type:
       - **Seq#**: Enter the sequence.
       - **Action**: Select Permit or Deny.

- **Source Network**: Enter the source network.
- **Destination Network**: Enter the destination network.
- **Source Port**: By default port 22 is selected.
- **Destination Port**: By default port 22 is selected.
- **DSCP Matching**: Enter the DSCP matching.
- **DSCP Marking**: Enter the DSCP marking.
- **Internal Priority Marking**: Enter the internal priority marking.

- **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 the configuration by selecting **Configure**.

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

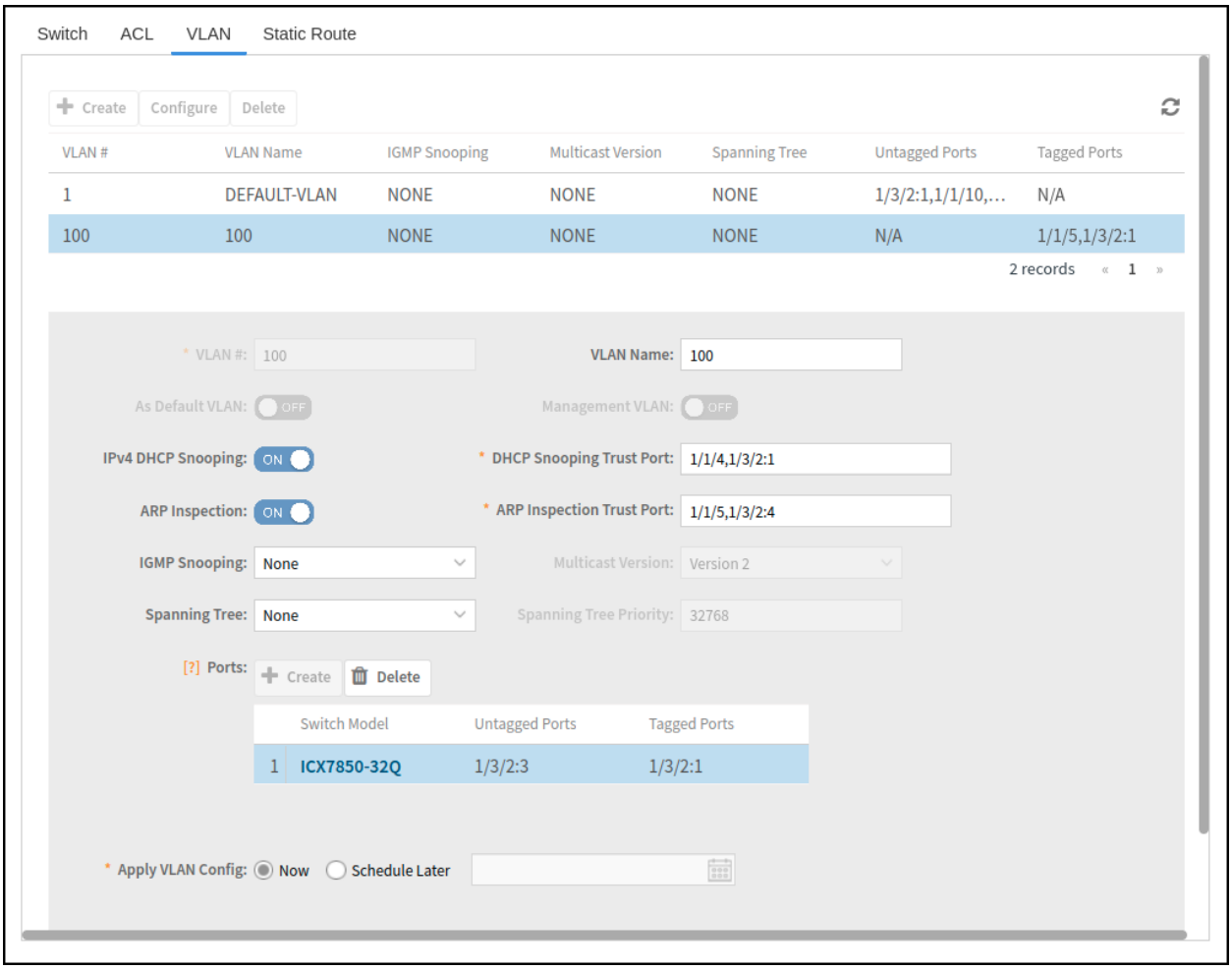
NOTE
Beginning with the 7.0 release, when you **Delete** an ACL, the ICX System log displays the SZ Administrator name associated with this activity. In the earlier releases, the ICX System log showed a generic message indicating that the network controller made the change.

b) Configure the **VLAN** settings.

1. Click the **VLAN** tab.
2. Click the 

icon to display the **VLAN** fields.

FIGURE 175 VLAN Configuration



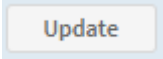
3. Complete the following VLAN fields:
   - **VLAN #**: Enter the number of the VLAN.
   - **VLAN Name**: Enter the name of the Layer 2 VLAN.
   - **As Default VLAN**: If you enable the **As Default VLAN** the **VLAN Name** is changed to **DEFAULT-VLAN** and the Management settings correspond to the previous VLAN settings.
   - **Management VLAN**: By enabling this, you can configure Management VLAN for the switches or switch groups.
   - **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 breakout 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 breakout 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 the 

icon and complete the following fields:

  NOTE
  Different set of ports can be entered for each switch model.

  - **Switch Model**: Select the switch model from the drop down list.
  - **Untagged Ports**: Enter the breakout port.
  - **Tagged Ports**: Enter the breakout port.
  - Click the 

icon.
- **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.

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

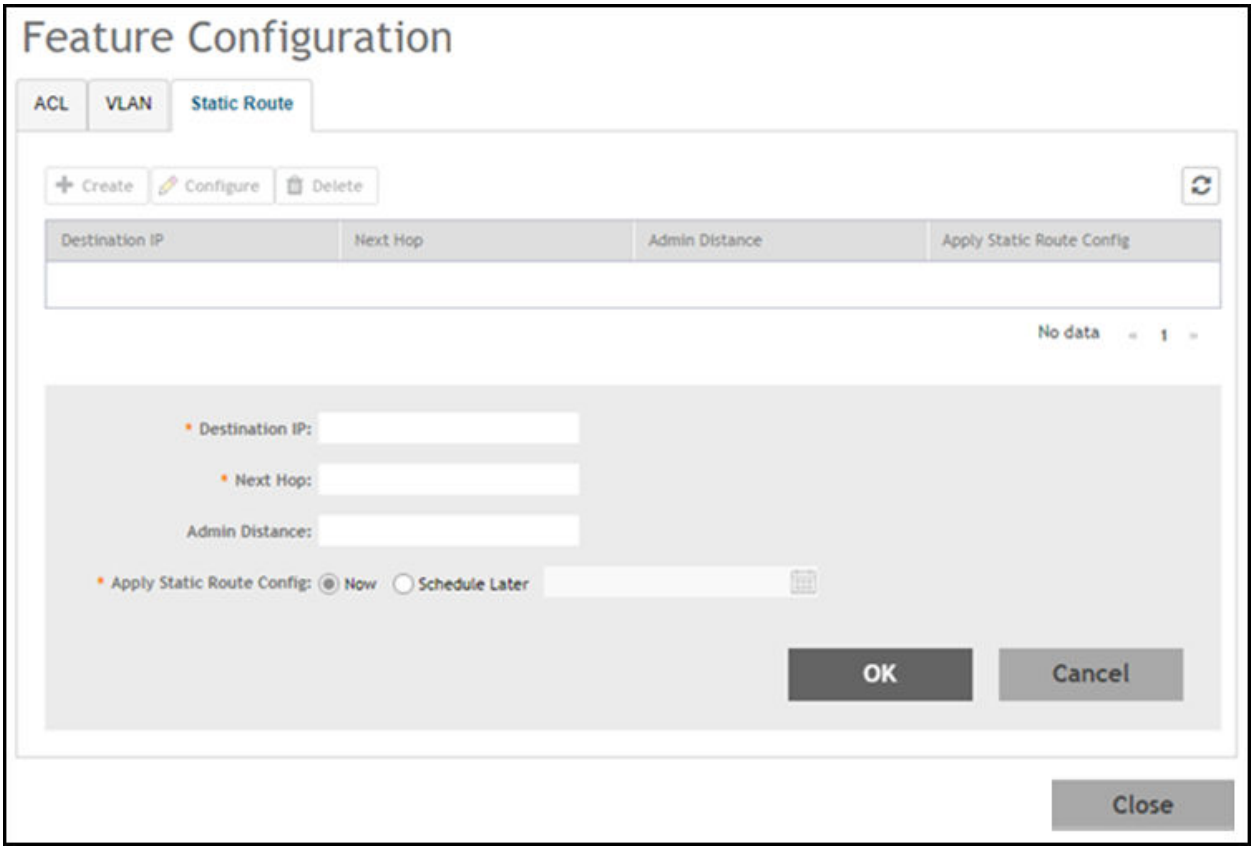
  NOTE
  Beginning with the 7.0 release, when you modify the **VLAN #** and **VLAN Name** , the ICX System log displays the SZ Administrator name associated with this configuration activity. In the earlier releases, the ICX System log showed a generic message indicating that the network controller made the change.

c) Configure the **Static Route** settings.

1. Click the **Static Route** tab.
2. Click the 

icon to display the **Static Route** fields.

FIGURE 176 Static Route Configuration



3. Complete the following Static Route fields:
   - **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.

     NOTE
     You can also edit and delete the Static Route configuration by selecting the options **Configure** and **Delete** respectively, from the **Static Route** tab.

d) 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.

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 356.

Creating and Managing Port Templates

The controller allows you to configure switch port settings. However, there are many advanced port settings that are not supported by the controller. You must configure these advanced port settings on the switch console.

The controller introduced with a port template facilitates the deployment of advanced port settings.

You can apply a port template to joined (or online) switch ports for which the firmware version is FastIron 08.0.95b or later. If the switch port is newly added, you must apply the port template again.

NOTE
You cannot apply a port template to ports that belong to offline switches.

NOTE
Apply the new untag VLAN to selected ports. Make sure to untag the default VLAN from these ports before applying the Port Template.

Creating a Port Template and Assigning Target Ports

Complete the following steps to create a port template and assign ports to the template.

1. On the menu, click **Network** > **Wired** > **Switches** to display the **Switches** window.
2. Either select a switch group and click the **Switches & Ports** tab, or select a switch and click the **Ports** tab.
3. In the **Port Details** tab, click **Port Templates** to display the **Port Templates** dialog box.

4. In the **Port Templates** following actions are available to create new and manage existing port templates:
   - Expand the list of existing port templates. Click "+".
   - Create a new port template. Click + Create.
   - Delete an existing port template. Click ×
   - Close the dialog box without applying any changes. Click Cancel.
   - Update the selected port template. Click Next.

FIGURE 177 Port Templates Dialog Box Showing all the Actions

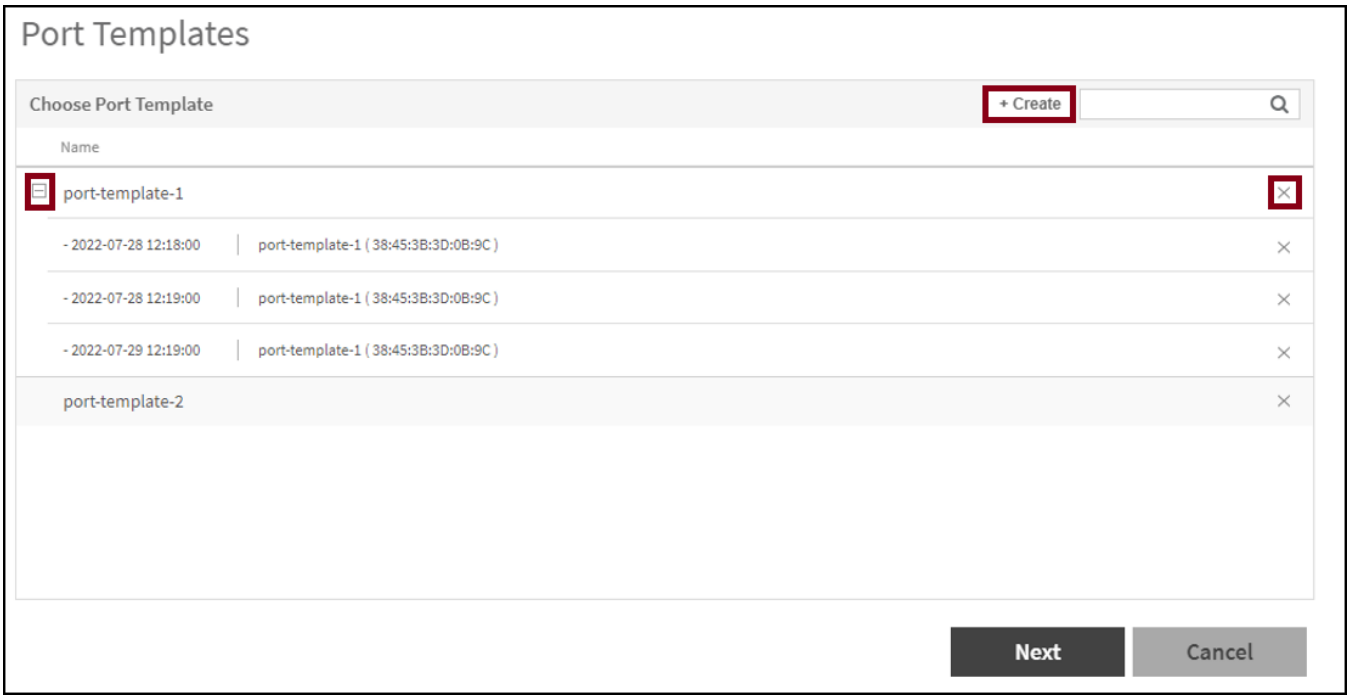
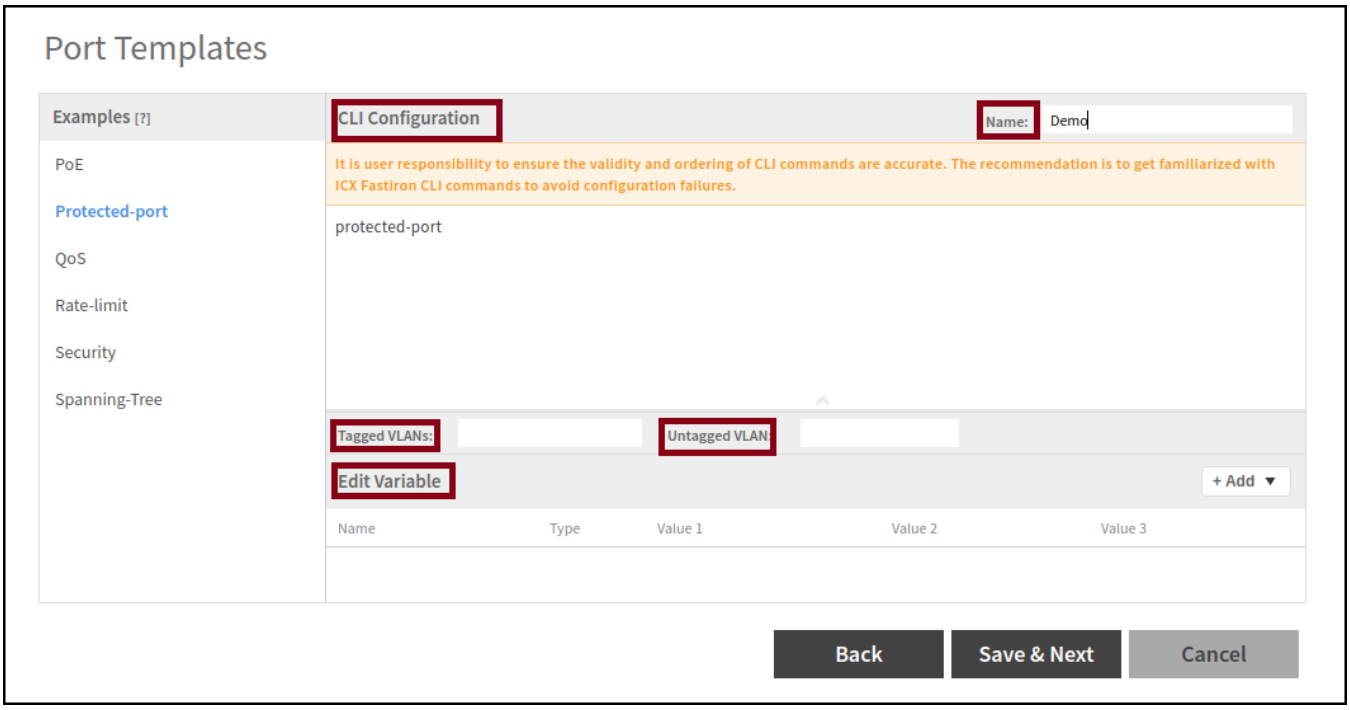


FIGURE 178 Creating a Port Template



5. To create a port template, complete the following steps:
   a) In the **Name** field, enter the name of the port template.
   b) Enter VLAN IDs in the **Tagged VLANs** field, separating multiple IDs with commas and no spaces. When you apply the port template to selected ports, the controller will automatically add the needed VLAN CLI commands to the template.

      NOTE
      If the **Tagged VLANs** field is empty, the controller will not add any tagged VLAN CLI commands.

   c) Enter a VLAN ID in the **Untagged VLAN** field. When the port template is applied to the selected ports, the controller will automatically add the necessary VLAN CLI commands to the template.

      NOTE
      If the **Untagged VLANs** field is empty, the controller will not add any untagged VLAN CLI commands.

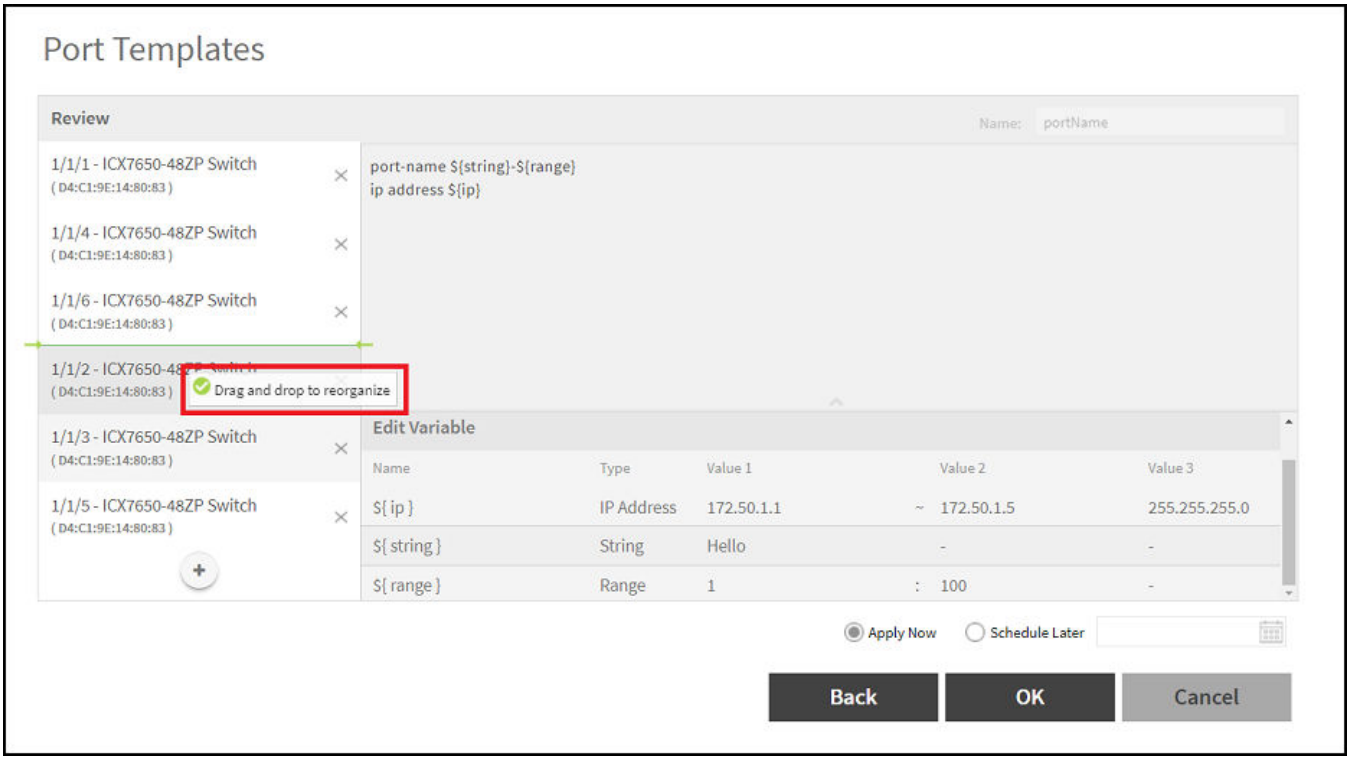
   d) In the **Edit Variable** field, enter the **Name**, **Type**, **Value 1**, **Value 2**, and **Value 3** for IP address variables. Value1 denotes the “Starting IP Address”, Value 2 denotes the “Ending IP Address”, and Value 3 denotes the “Netmask". Variables help to apply unique configurations to the switches. If you want to use a variable in the **CLI Configuration** editor, it must begin with a dollar sign ($) and use a pair of curly braces, for example, ${VARIABLE_NAME}. An IP address can be defined as a variable so that each switch gets assigned a unique IP address.
   e) In the **CLI Configuration** field, enter command types for the template, including variables.
6. After creating, click **Save & Next** to save the port template. You can click **Back** to view the previous step, or click **Cancel** to close the page.

7. Click "+" on the left pane of the **Review** page to add more ports to the list. Select **Apply Now** to apply the port template. Select **Schedule Later** to apply the port template at the date and time specified by clicking the calendar icon. After selecting either **Apply Now** or **Schedule Later**, click **OK**.

   NOTE
   Before the SZ 7.0 release, as a preliminary step, you must select a port and then apply the port template. With the 7.0 release, you can apply a port template without initially selecting a port.

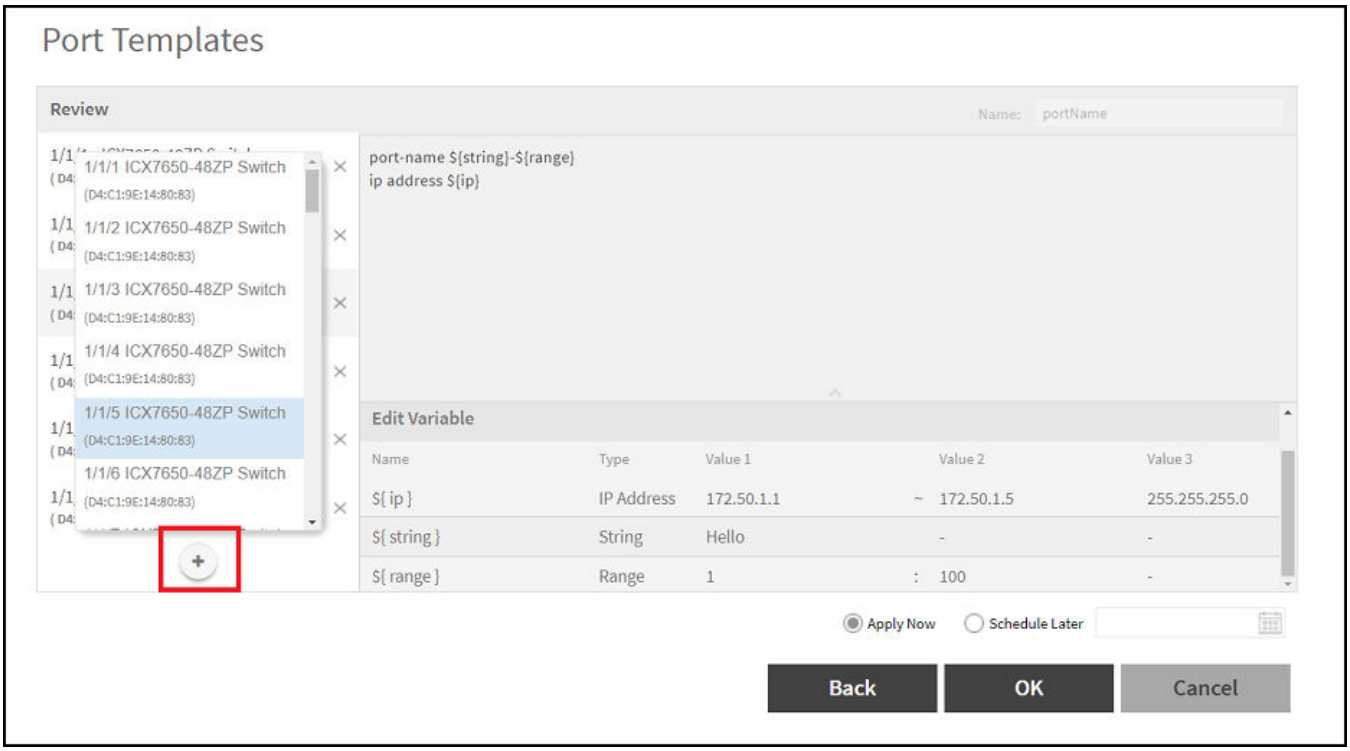
You can also organize the port list by selecting a port and dragging it above or below.

FIGURE 179 Organizing the Port List



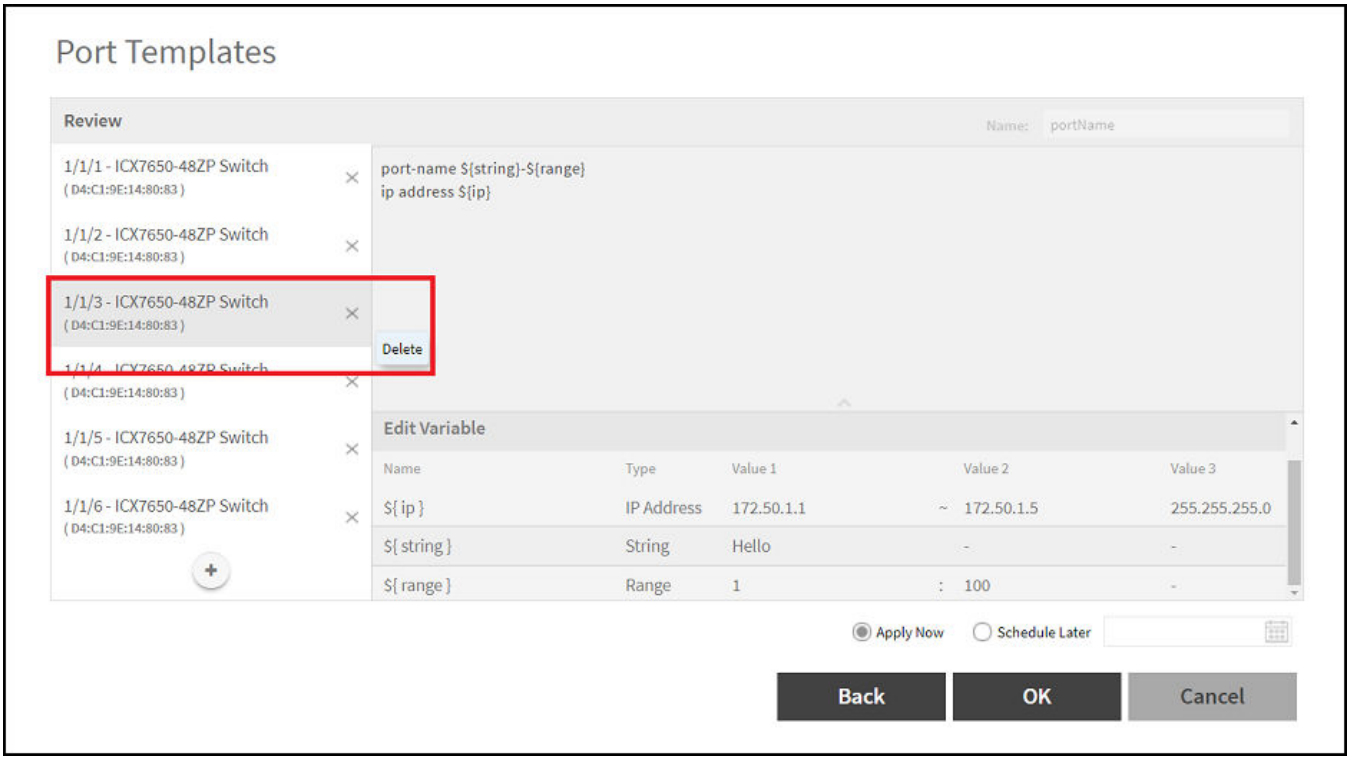
You can also add port to the list.

FIGURE 180 Adding Ports to the List



You can also delete a port from the list.

FIGURE 181 Deleting Port from the List



8. After applying the port template to the selected ports, a dialog box with the message **Port Template applied successfully** is displayed, click **OK**.

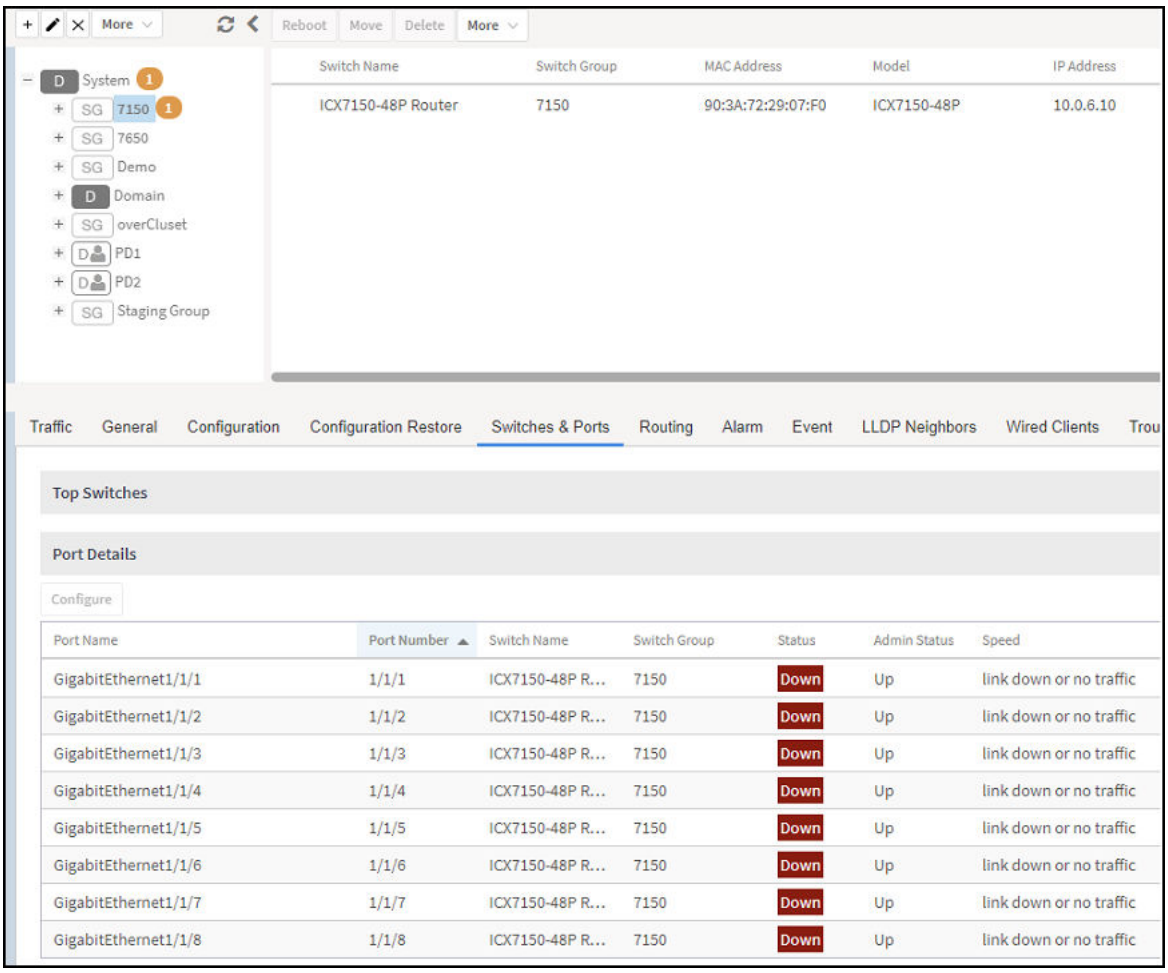
Configuring Port Settings for a Switch

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. On the menu, click **Network** > **Wired** > **Switches** to display the **Switches** window.
2. In the **Organization** tab, select a **Domain** > **Switch Group** or **Switch Group** and in the **Details** tab, click the **Switches and Ports** tab.

FIGURE 182 Switch Port Page



3. In the **Port Details** tab, select the port that must be updated and click **Configure** to display the **Port Settings** window.

FIGURE 183 Port Settings Showing Single Update

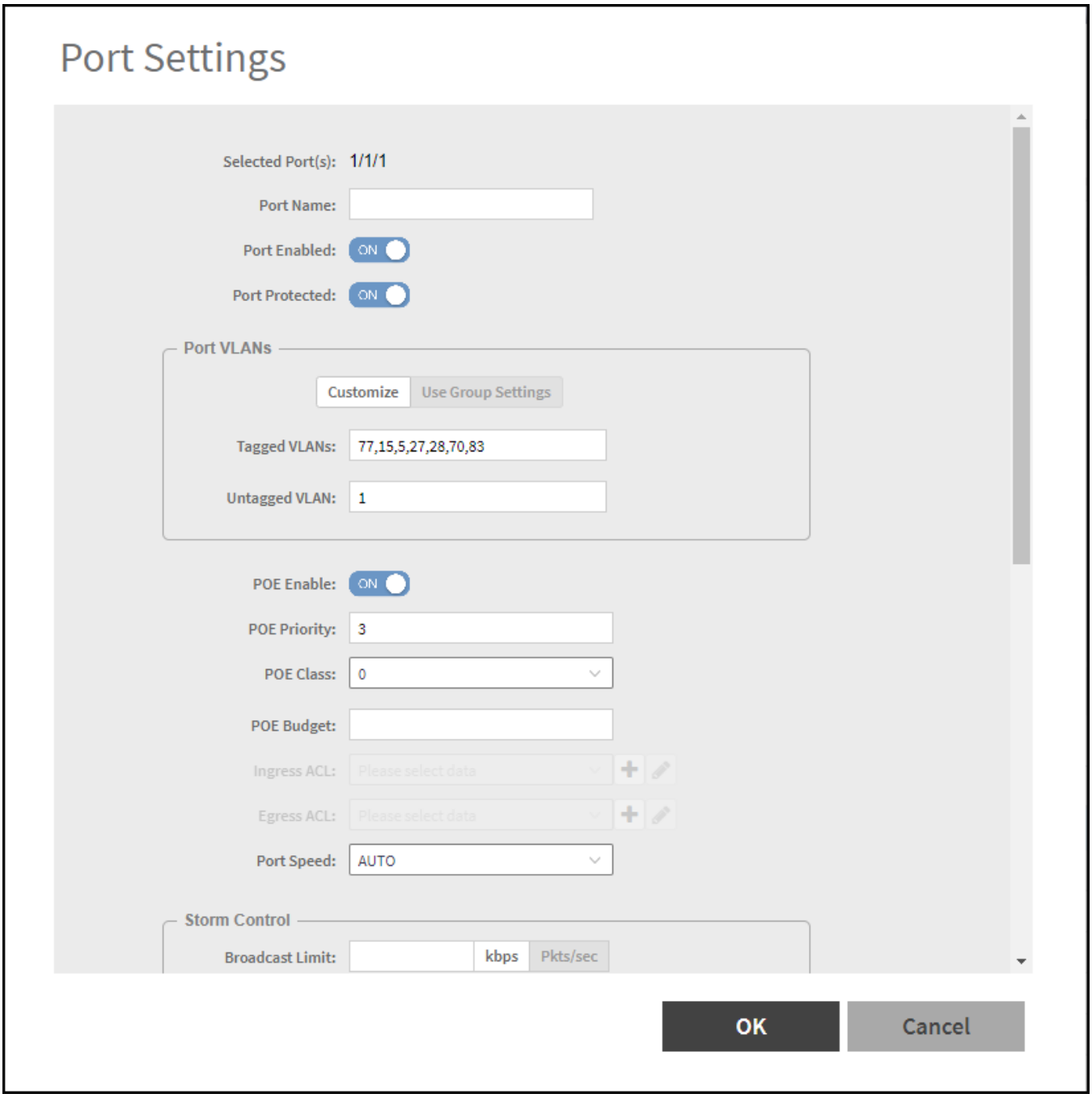


FIGURE 184 Poret Settings Showing Multiple Update

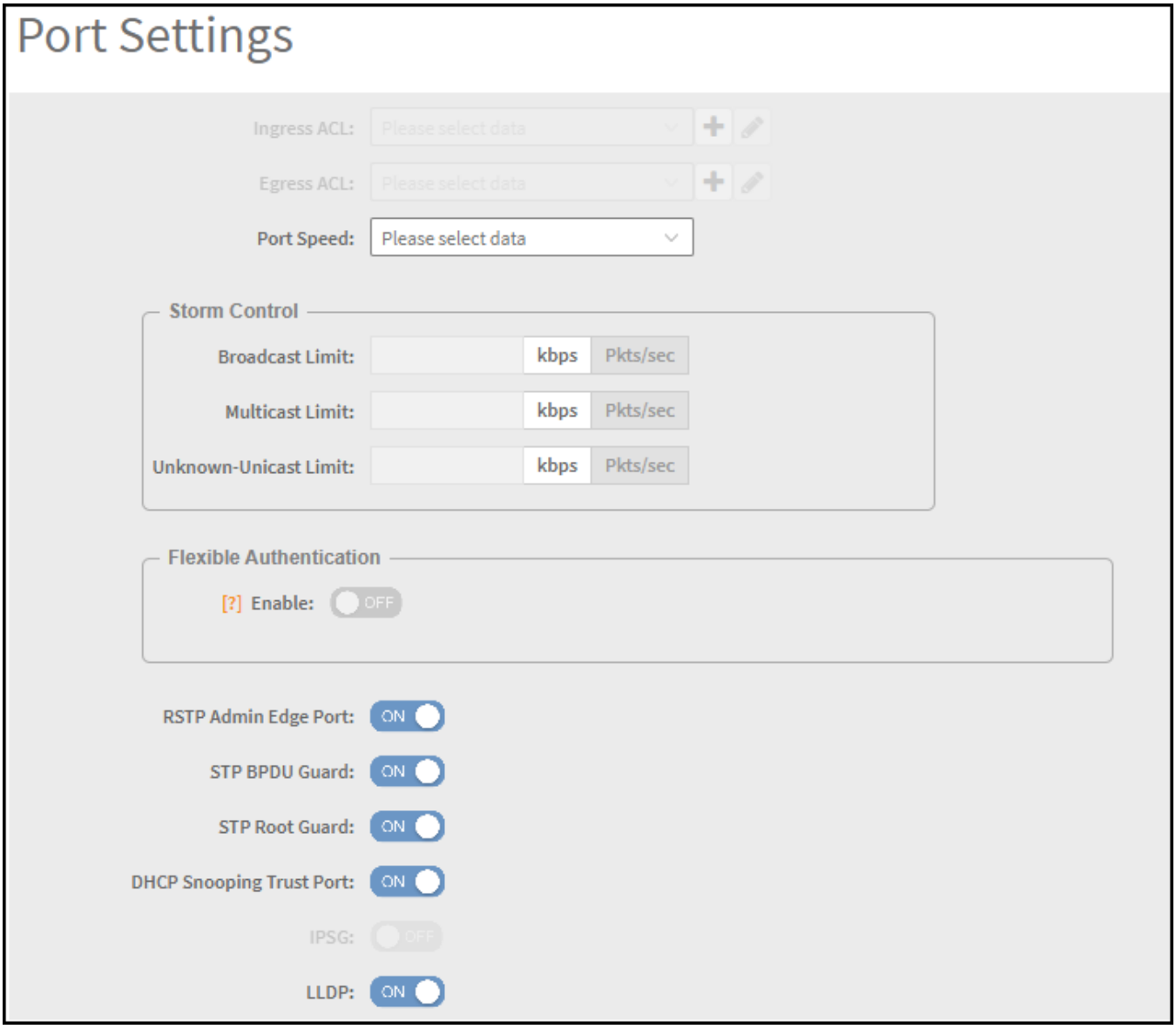
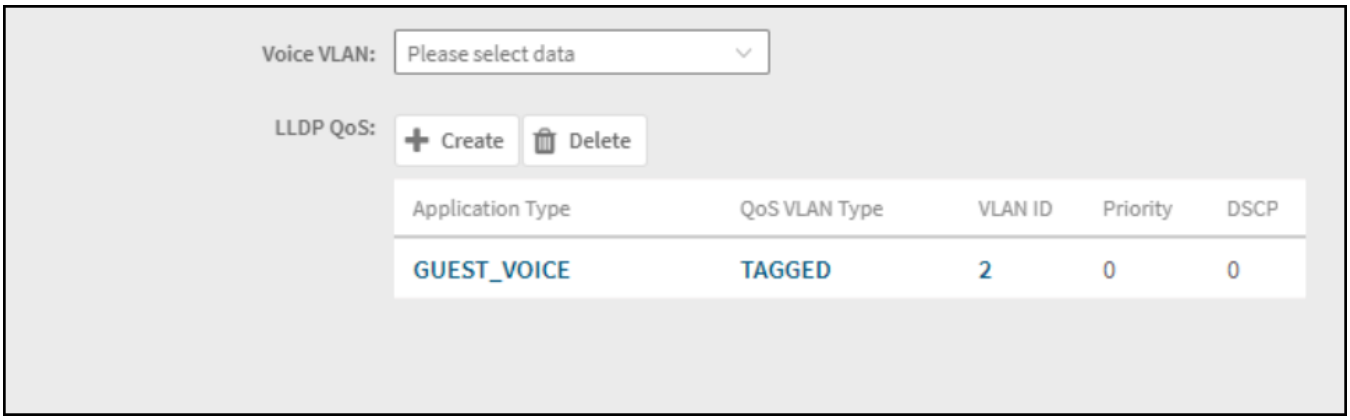


FIGURE 185 Port Settings for QoS


Voice VLAN:
Please select data
LLDP QoS:
Create
Delete
Application Type
QoS VLAN Type
VLAN ID
Priority
DSCP
GUEST_VOICE
TAGGED
2
0
0

4. Complete the following fields:
   - **Port Name**: Enter the port name.
   - **Port Enabled**: Click to enable the port.
   - **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.

   - **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.
   - **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.

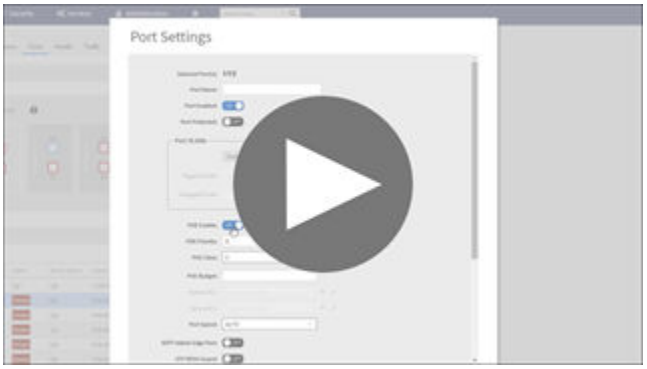
     NOTE
     The value 0 pkts/sec and 0 kbps indicates storm control is disabled.

   - **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.

5. 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 the 5.2.1 release, you could edit ports for one switch at a time. After the 5.2.1 release, you can edit ports for multiple switches in the same switch group.

For instance, if you need to disable ports 1/1/11 and 1/1/12 on multiple switches, the controller lets you filter the ports list by typing your search criteria.

The search criteria is based on the following:

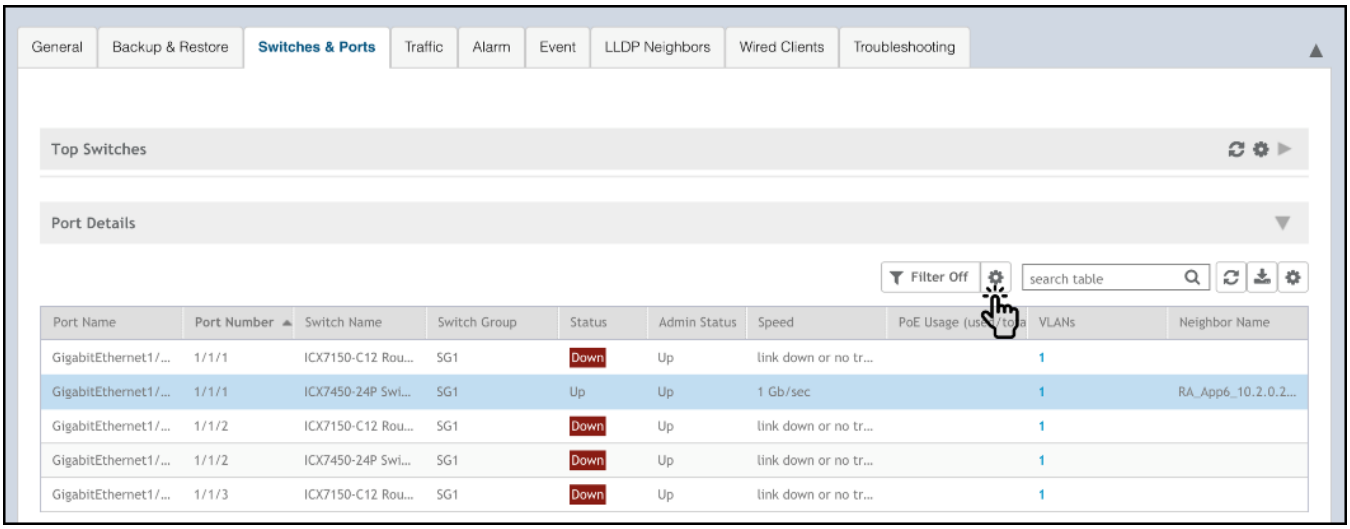
- Switch Name
- Port Numbers - comma separated values (1/1/1,1/1/11,1/1/24), (or) Range of ports (1/1/1 to 1/1/20)
- VLAN Membership
- PoE Detected Ports
- Port Status
- Admin Status

Complete the following steps to edit ports across multiple switches.

1. On the menu, click **Network** > **Wired** > **Switches** to disaply the **Switches** window.
2. From the system tree, select a **Domain** > **Switch Group** or **Switch Group**.

3. In the **Details** pane, click the **Switches and Ports** tab.

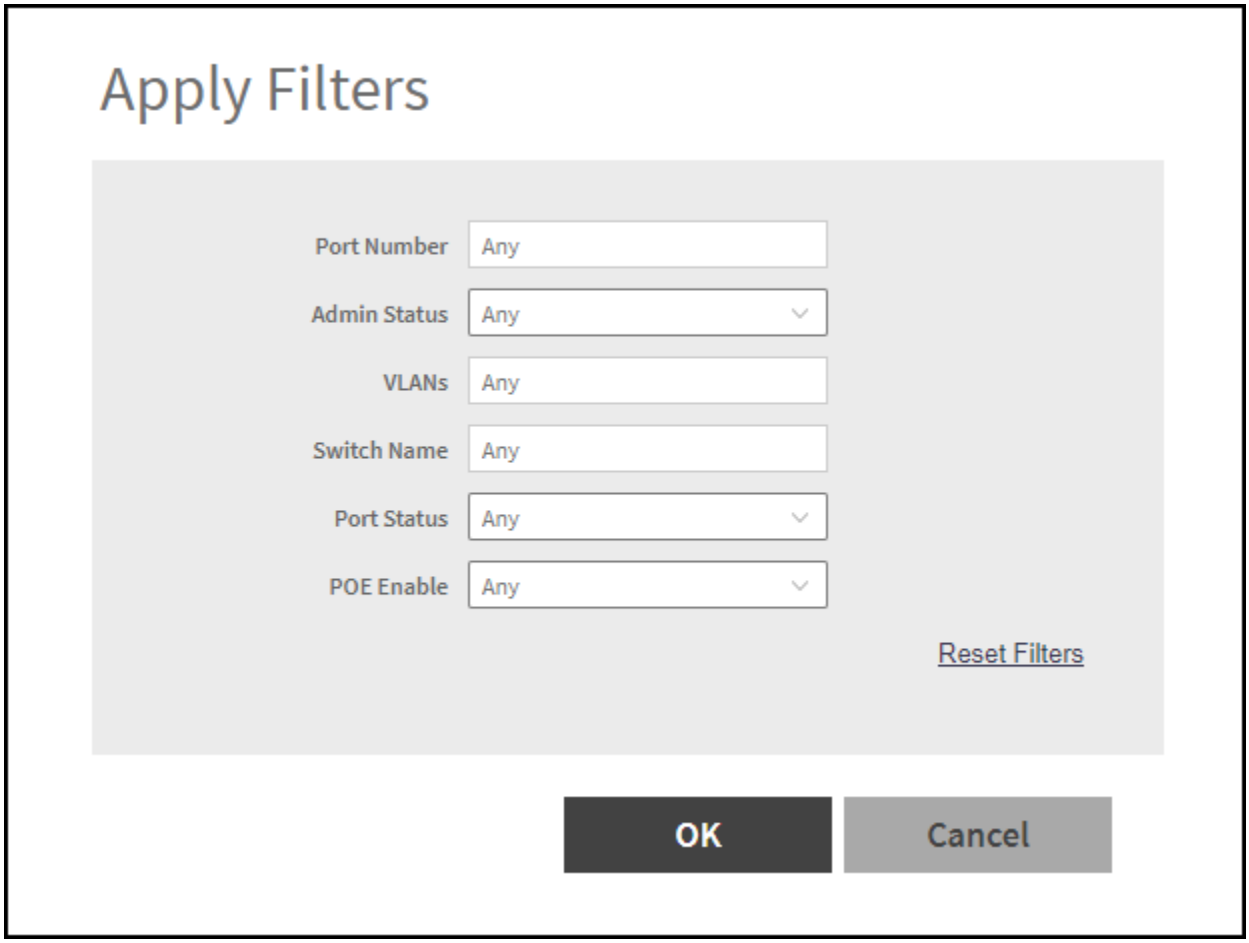
FIGURE 186 Viewing the Switches and Ports Page



4. In the **Port Details** section, 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 187 Applying Filter to Edit the Ports



   NOTE
   The **Reset Filters** allows you to clear the search conditions.

5. Click **OK**.

   The controller applies the above filters to return ports that meet the search criteria.

Creating Routing Configurations

You can create, edit, and delete routing configurations for a switch.

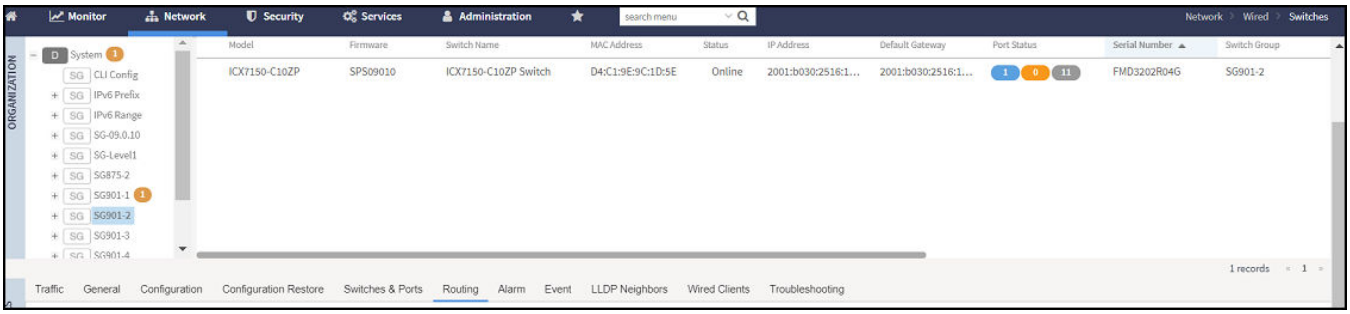
1. From the main menu, go to **Network** > **Wired** > **Switches** to display the window.

   The **Switches** page is displayed.

2. Select the **Domain** > **Switch Group** or specific **Switch Group**, and then choose the switch.

3. In the **Details** pane, click the **Routing** tab.

FIGURE 188 Switch Routing Tab

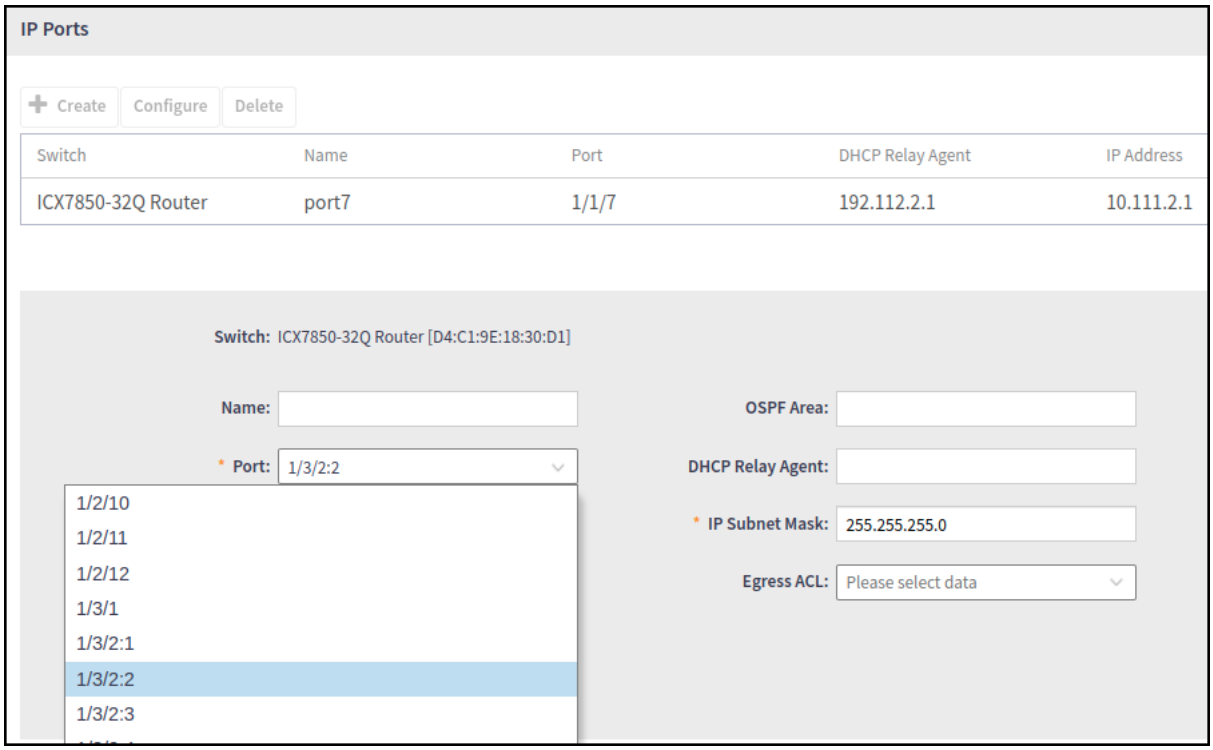


4. In the **IP Ports** section, click the 

icon.

5. The **IP Ports** page is displayed.

FIGURE 189 IP Ports Page



Complete the following fields:

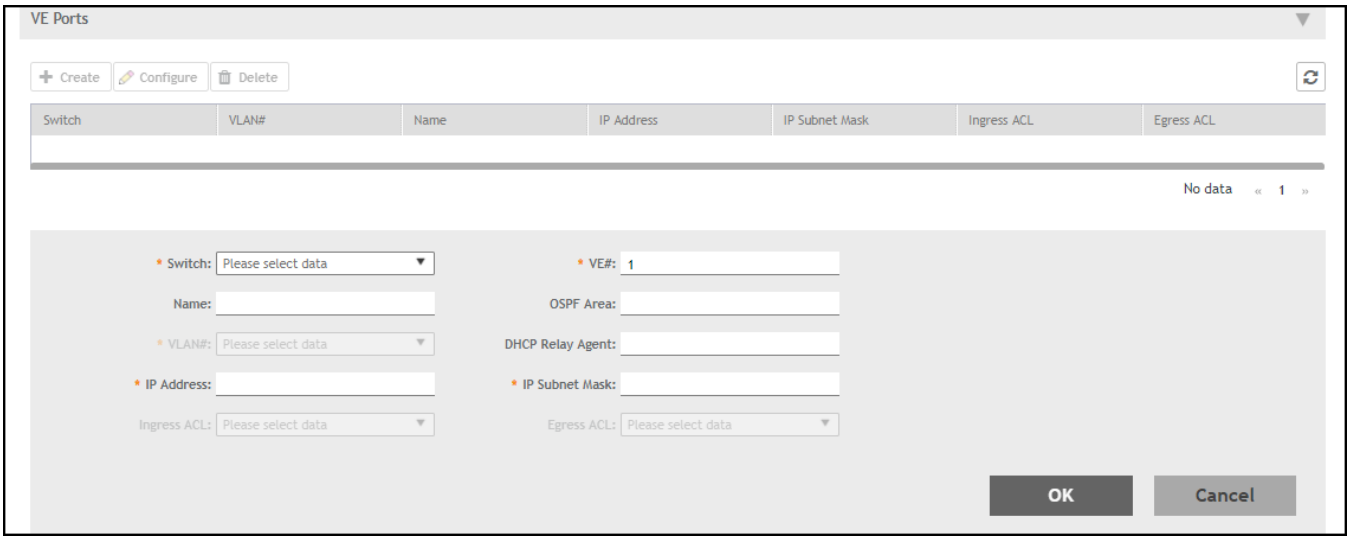
- **Switch**: Select the switch from the drop down list.
- **Name**: Enter a name.
- **OSPF Area**: Enter the OSPF area IPv4 address.
- **Port**: Select the breakout port number from the list.
- **DHCP Relay Agent**: Enter the DHCP relay agent IP address.
- **IP Address**: Configure the IP address on the selected breakout port.
- **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**.

7. In the **VE Ports** section, click the 

icon.

FIGURE 190 VE Ports Page



Complete the following fields:

- **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.

8. The **VE Ports** ports page is displayed.
9. Click **OK**.

Managing Link Aggregation Groups (LAGs)

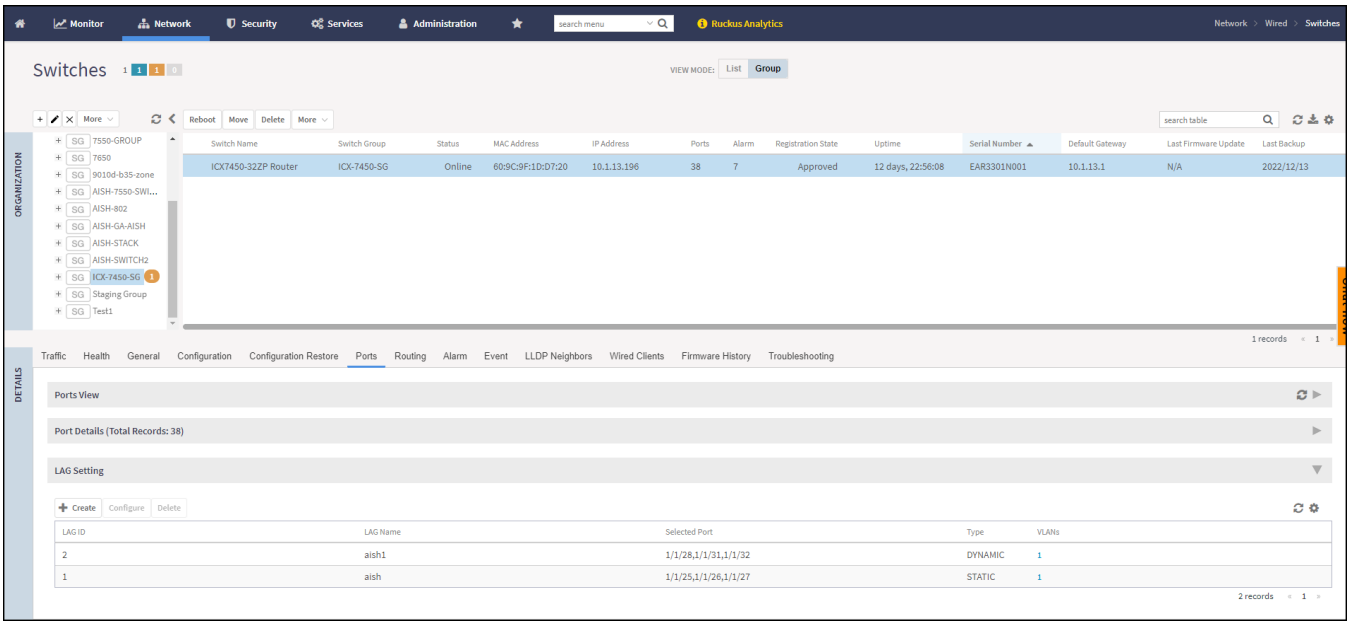
Controller provides an option to define LAGs at an individual switch level.

1. From the main the menu, go to **Network** > **Wired** > **Switches**.

   The **Switches** page is displayed.
2. Select a **Domain** > **Switch Group** or specific **Switch Group**, and then choose the **Switch**.

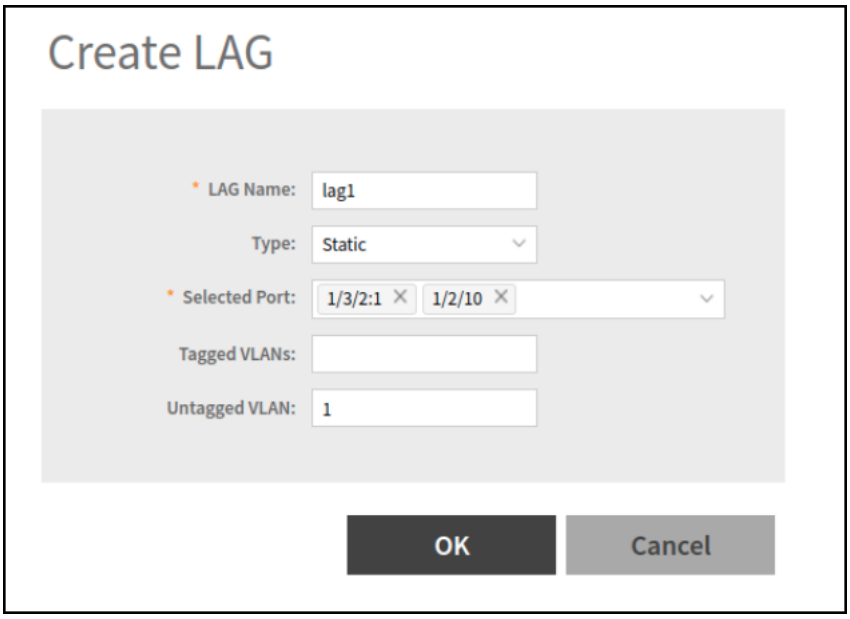
3. In the **Details** pane, click the **Ports** tab.

FIGURE 191 Ports



4. In the **LAG Setting** section, click the  icon to display the **Create LAG** dialog box.

FIGURE 192 Creating LAG



5. Complete the following fields:
   a) **LAG Name**: Enter a name.
   b) **Type**: Select either **Static** or **Dynamic** from the list.
   c) **Selected Port**: Add a breakout port to the selected port.

      NOTE
      You are required to manually configure breakout ports on the switches.

   d) **Tagged VLANs**: Enter the tagged VLAN ID or VLAN ID range.
   e) **Untagged VLANs**: Enter an untagged VLAN ID.
6. Click **OK**.

Creating a Switch Stack

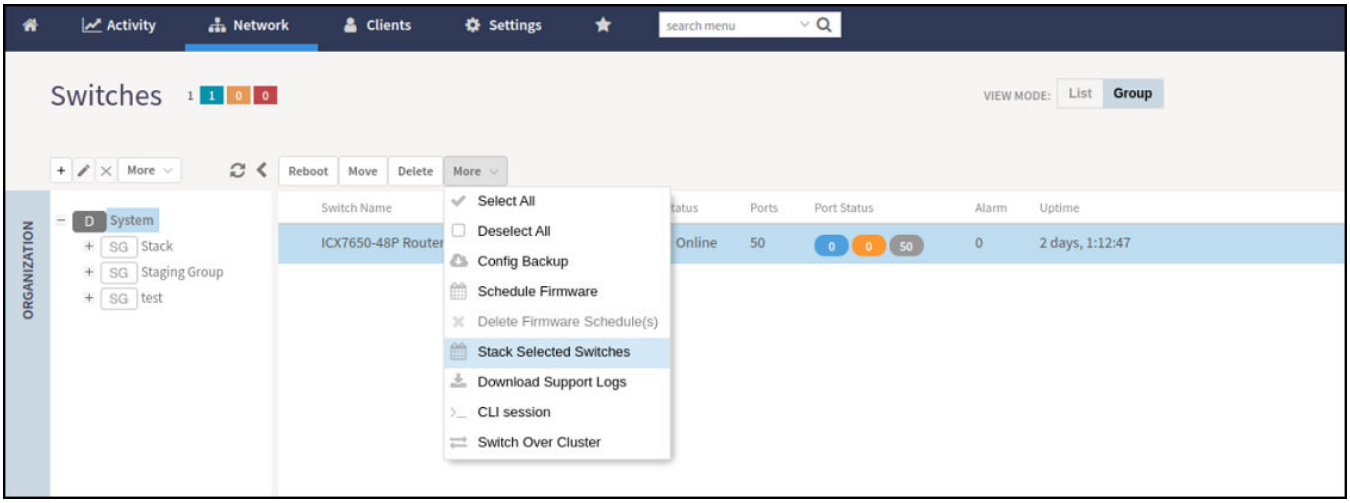
You can create a stack by selecting individual switches that are connected to the controller.

As a prerequisite, before you connect the switch cables ensure to configure switch stacking from the controller.

Complete the following steps to create a stack of switches.

1. On the menu, click **Network** > **Wired** > **Switches** to display the **Switches** window.
2. In the **Organization** tab, select a **Domain** > **Switch Group** or **Switch Group** and select the **Switch** that are to be stacked. Click **More** > **Stack Selected Switches** to display the **Create Stack** page.

   FIGURE 193 Creating a Stack



3. Enable **Active Role** and click **OK** to create the stack.

   NOTE
   The stack creation process takes 15 minutes.

4. To view a switch in the created stack, from the system tree, click **Domain** > **Switch Group** or **Switch Group** and select the stacked **Switch**.

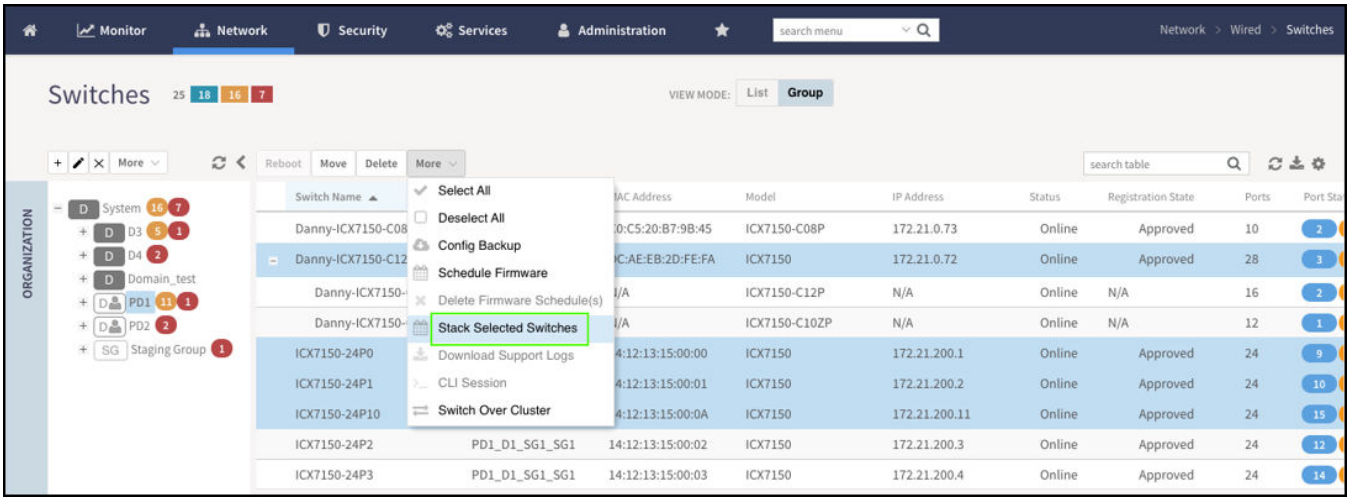
Ability to Convert Standalone Switch to Stack

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.

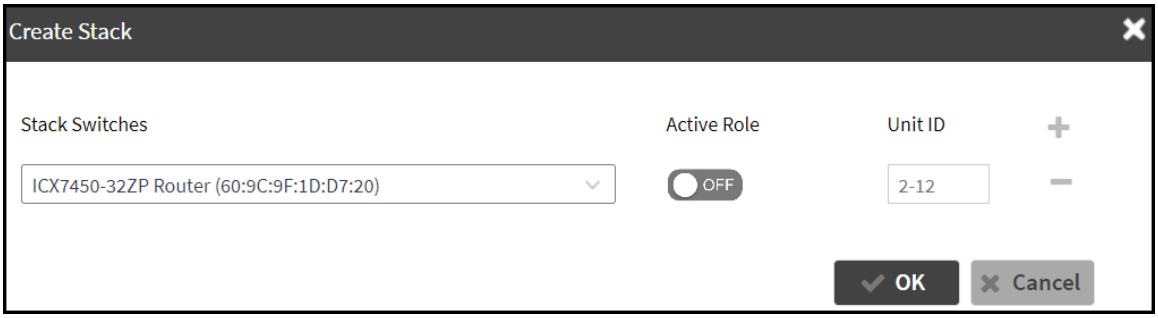
1. On the menu, click **Network** > **Wired** > **Switches** to display the **Switches** window.
2. In the **Organization** tab, click a **Domain** > **Switch Group** or **Switch Group** and select the **Switch**.
3. To add standalone switch to the stack, click **More** > **Stack Selected Switches**

FIGURE 194 Stack Selected Switches



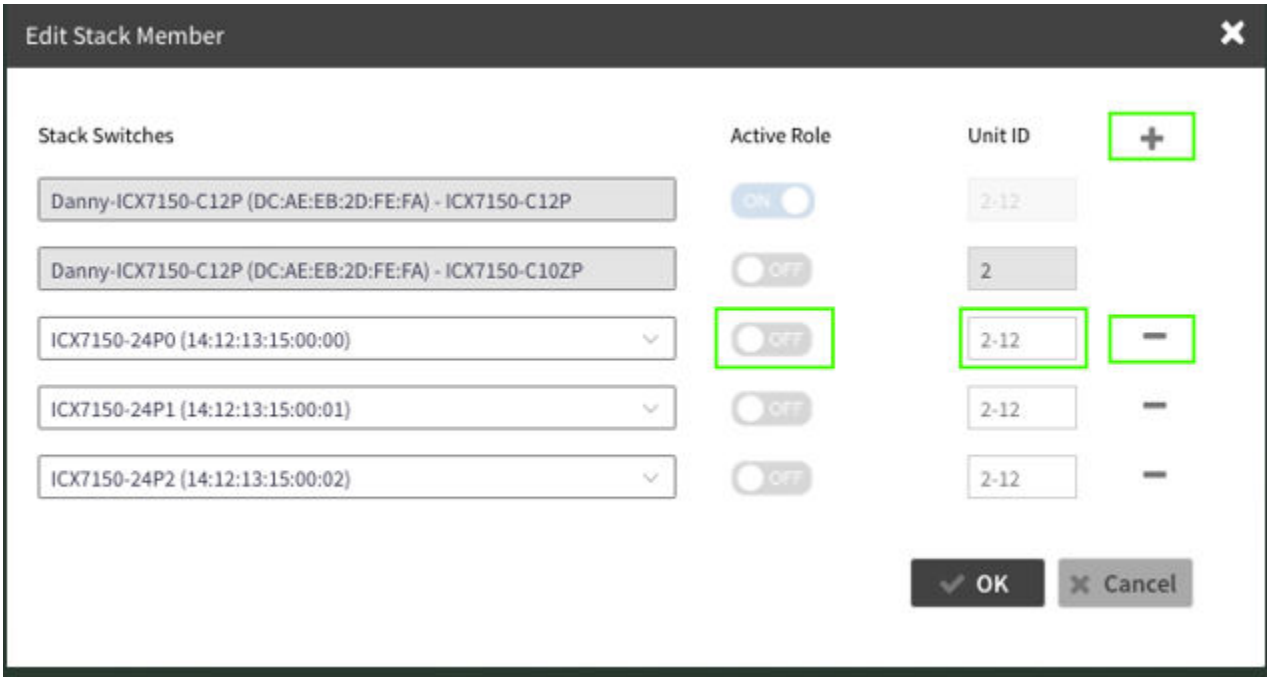
The **Create Stack** dialog box is displayed. Turn **Active Role** ON.

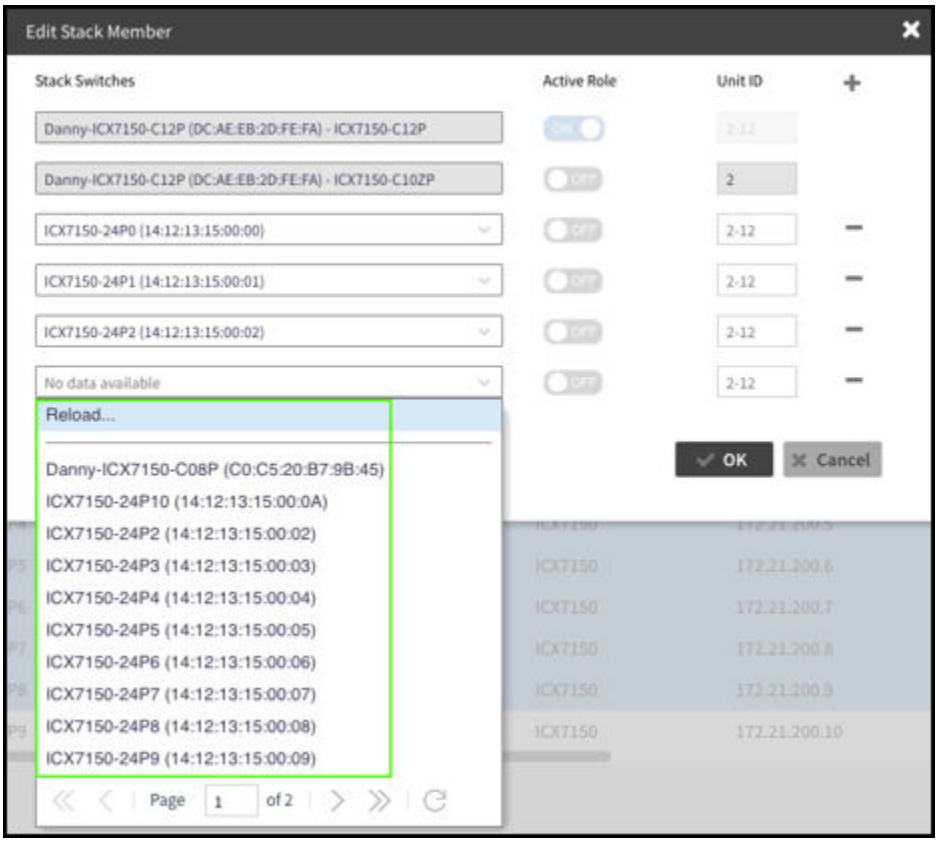
FIGURE 195 Create Stack Dialog Box



4. 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; for example, 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.

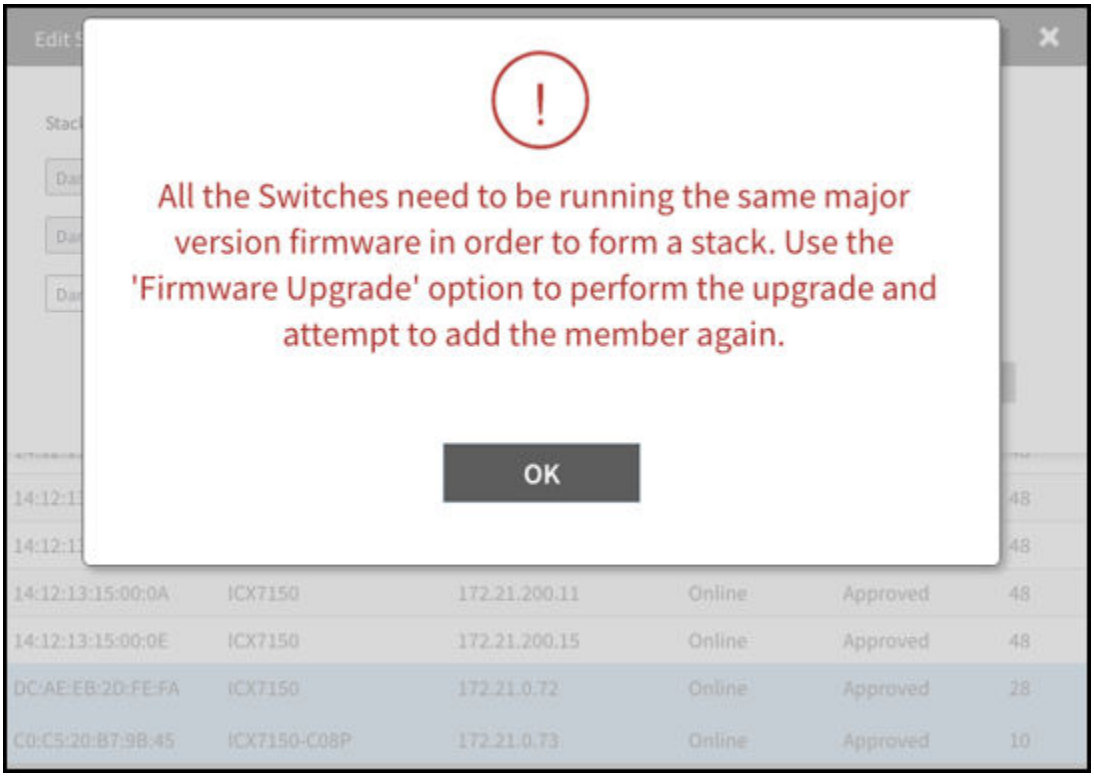
   NOTE
   From FI 09.0.00, the maximum stack size for ICX 7150 and ICX 7250 devices are limited to eight units in a stack.




Edit Stack Member
Stack Switches
Active Role
Unit ID
Danny-ICX7150-C12P (DC:AE:EB:2D:FE:FA) - ICX7150-C12P
Danny-ICX7150-C12P (DC:AE:EB:2D:FE:FA) - ICX7150-C10ZP
2
ICX7150-24P0 (14:12:13:15:00:00)
ICX7150-24P1 (14:12:13:15:00:01)
ICX7150-24P2 (14:12:13:15:00:02)
No data available
2-12
Reload...
Danny-ICX7150-C08P (C0:C5:20:B7:9B:45)
ICX7150-24P10 (14:12:13:15:00:0A)
ICX7150-24P2 (14:12:13:15:00:02)
ICX7150-24P3 (14:12:13:15:00:03)
ICX7150-24P4 (14:12:13:15:00:04)
ICX7150-24P5 (14:12:13:15:00:05)
ICX7150-24P6 (14:12:13:15:00:06)
ICX7150-24P7 (14:12:13:15:00:07)
ICX7150-24P8 (14:12:13:15:00:08)
ICX7150-24P9 (14:12:13:15:00:09)
Page 1 of 2
OK
Cancel

5. Click **OK**.

NOTE
If stack and switch are running different version of an image, an error message is displayed.



Viewing Port Details

Details on port use are available for individual switches, stacks, and switch groups.

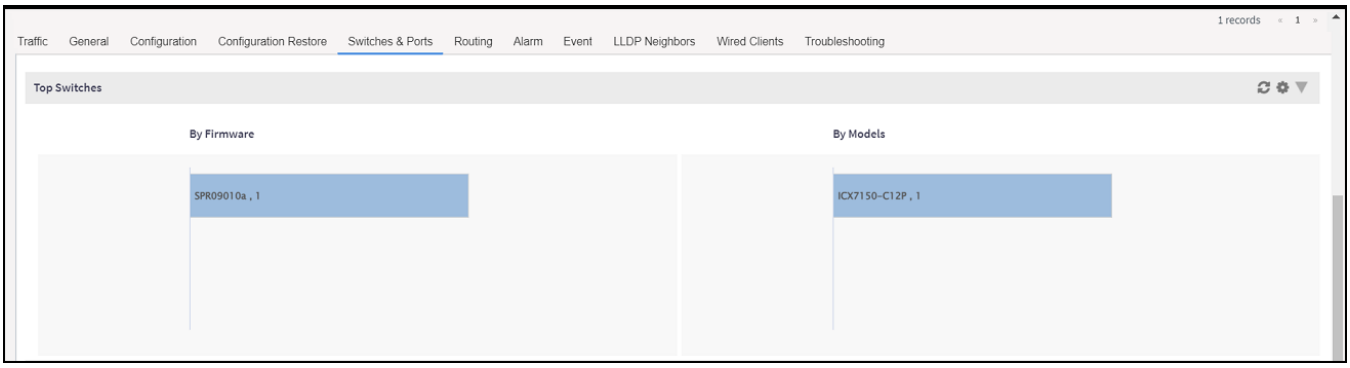
Perform these steps to display information on ports for a switch, stack, or switch group.

1. On the menu, click **Network** > **Wired** > **Switches** to display the **Switches** window.

2. From the system tree, select the **Domain** > **Switch Group** or **Switch Group** and in the **Details** tab, click **Switches and Ports** tab.

   For a switch group, a **Top Switches** tab similar to the following figure is displayed. The graphs provide information on top switches based on firmware and model.

   FIGURE 196 Top Switches Page

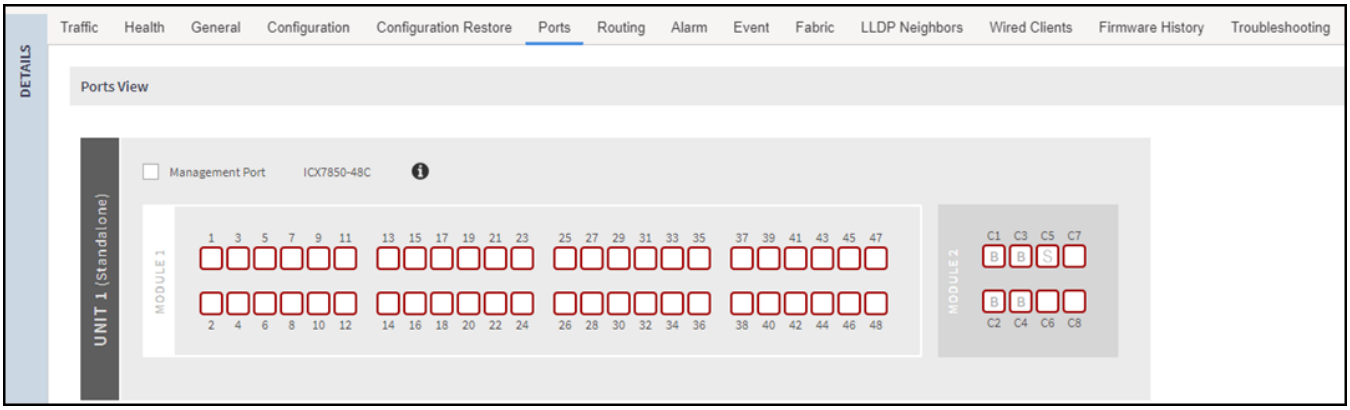


3. In the **Switch Group**, select the **Switch** and click **Ports** tab to view the **Front Panel View** in the **Ports View** tab for additional port information as shown in the following figure.

   The **Front Panel View** provides information on the state of all ports in each switch module, for example port Up, Down, or Administratively Down.

   When you hover over the breakout port, a popup window will appear, stating, `The 40Gbps port breaks out into four 10Gbps sub-ports respectively`

FIGURE 197 Front Panel View



The following figure shows the diagram legend used in the Front Panel View page.

FIGURE 198 Diagram Legend

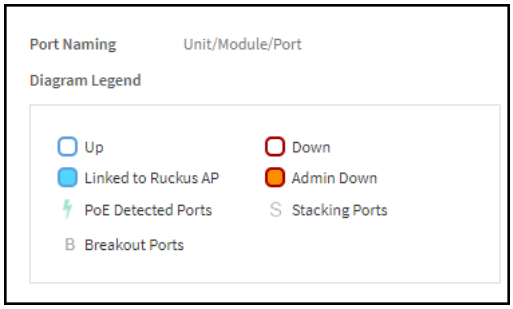
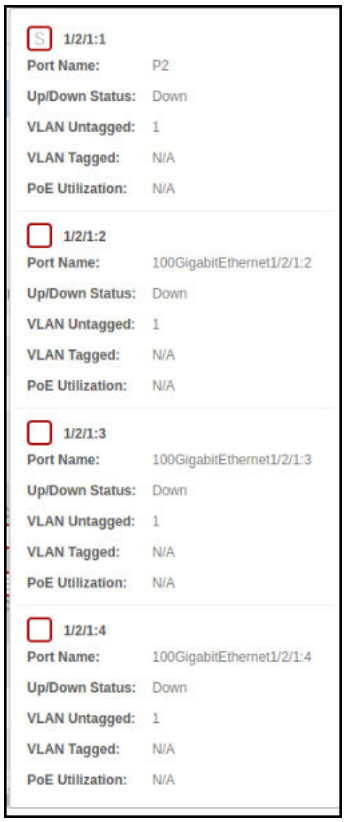


FIGURE 199 Viewing the Breakout Ports



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.
- Linked to Ruckus AP: Ports that are linked to RUCKUS AP.
- Admin Down: Ports that have been manually disabled by the network administrator.
- PoE Detected Ports: Ports that are PoE detected.
- Stacking Ports: Ports that are stacked.
- Breakout Ports: The 40G/100G port can be divided into 4x10G or 4x25G .

4. Click the switch name to view the **Port Details** page as shown in the following figure.

FIGURE 200 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.

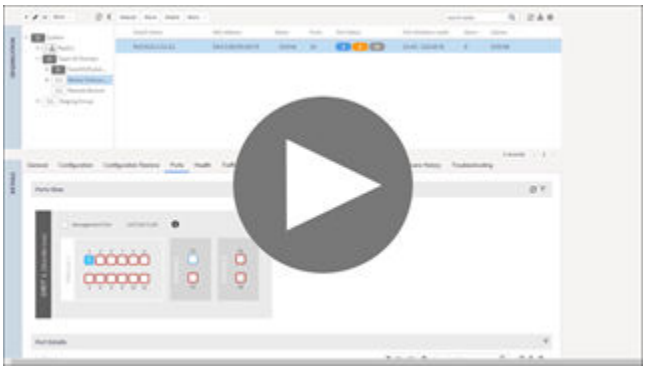
- **Port Name**: Displays the port name.
- **Port Number**: Displays the breakout port number
- **Status**: Whether the port is operationally up or down.
- **Admin Status**: Whether the port has been set to Up or Down by the network administrator.
- **Speed**: The speed of the port.
- **PoE Device Type**: 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**
> 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.

Accessing the Switch CLI through Controller (Remote CLI)

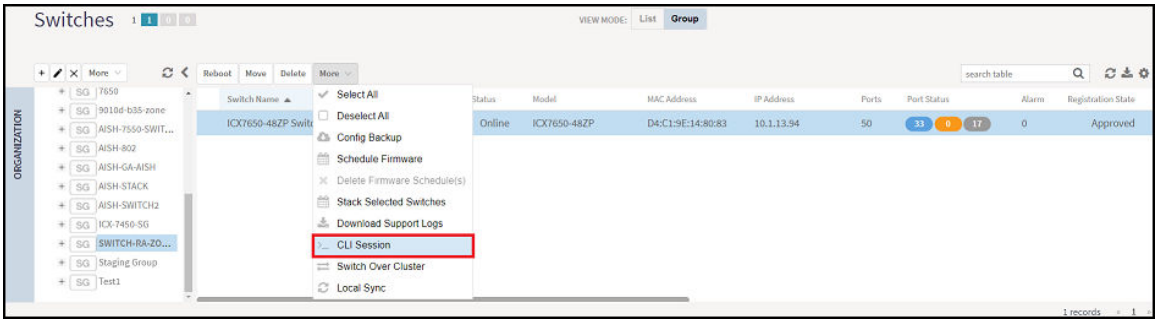
SmartZone 5.2.1 introduces this essential feature that allows you to directly access the Switch CLI prompt from the controller web interface. The Remote CLI allows you to establish a secured connection between controller and switch that can span over Internet, and eliminate the need to open VPN connection 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 and later releases.

The administrator must complete the following steps to access a CLI session.

1. On the menu, click **Network** > **Wired** > **Switches** to display the **Switches** window.
2. In the **Organization** tab, select a **Domain** > **Switch Group** or **Switch Group** and select the **Switch**.
3. Click **More** > **CLI session** to display the **CLI command** window.

FIGURE 201 Selecting CLI Session

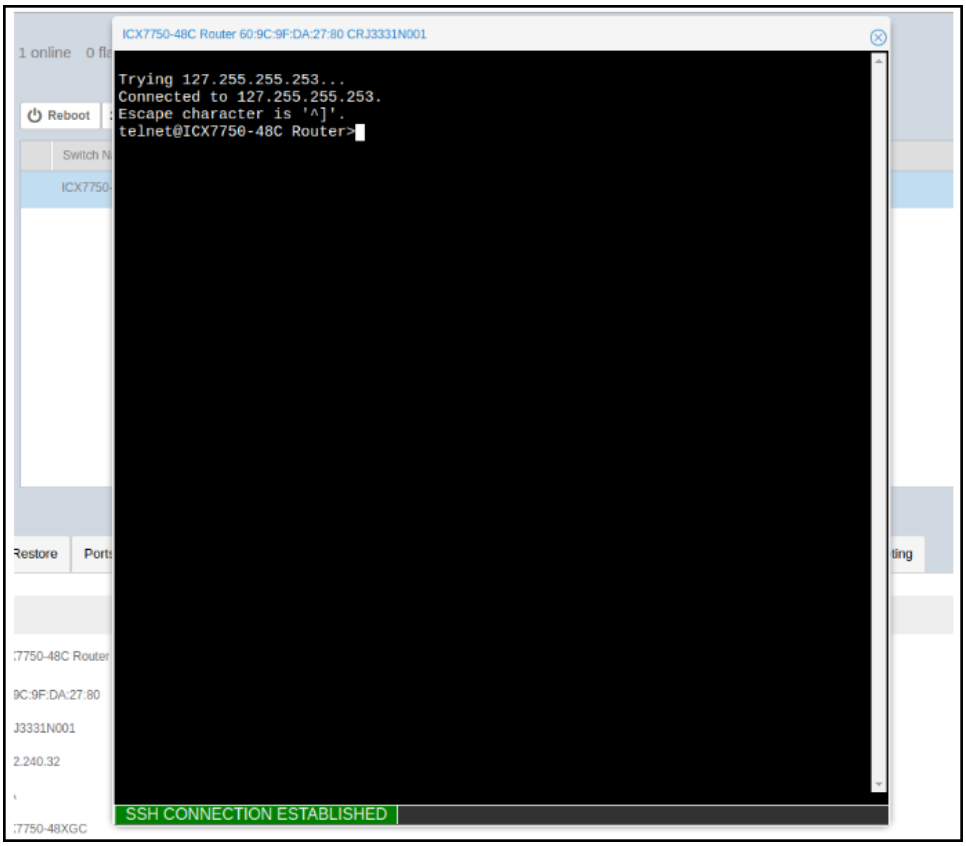


4. Enter the administrator password.

   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.

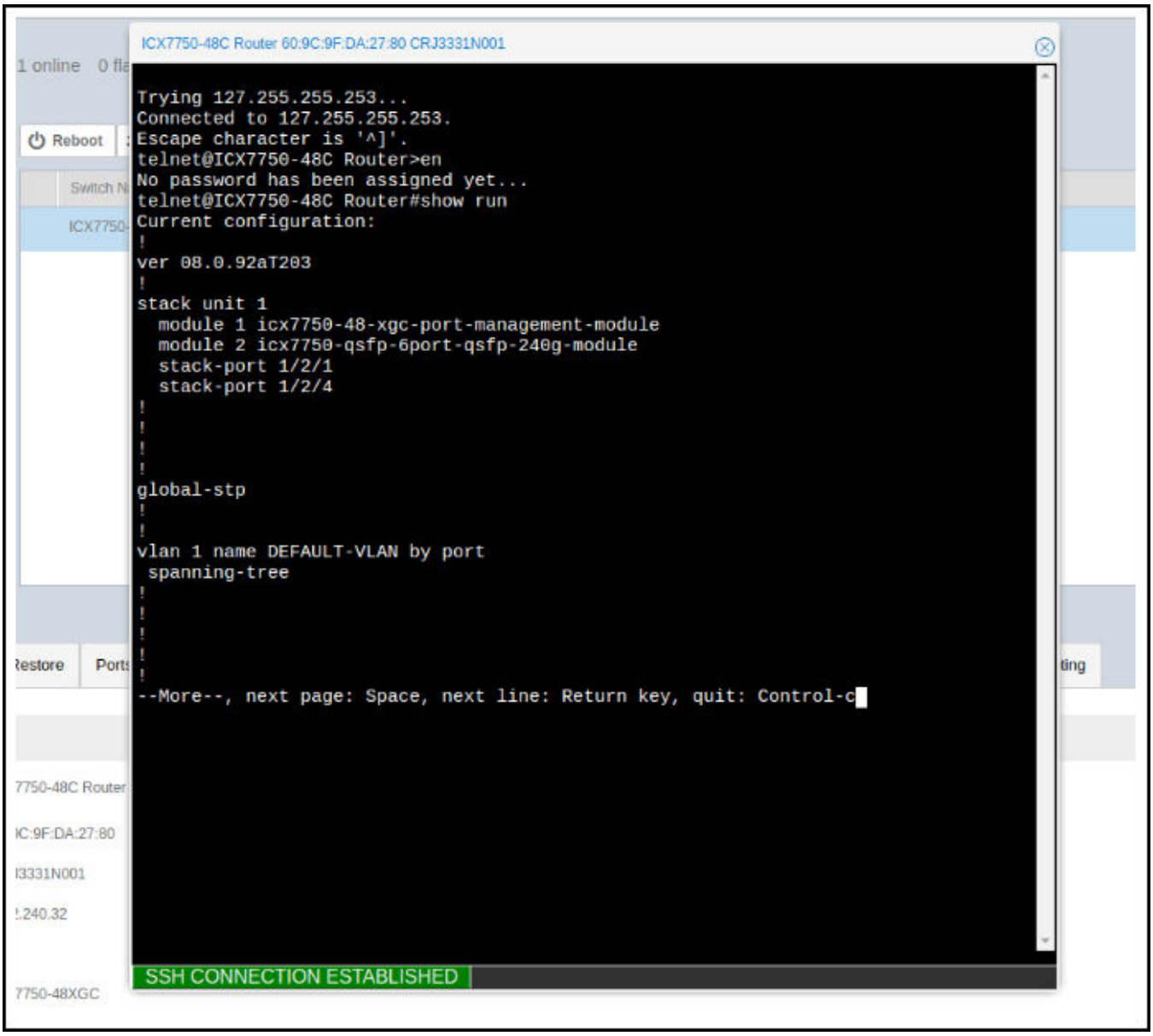
   NOTE
   You do not need to enable telnet server on ICX switches to use Remote CLI.
   However, if telnet authentication is enabled on the switch, you will be prompted to enter the credentials when opening CLI session via SmartZone. The credentials depend on the type of authentication defined on the switch (local user, RADIUS etc.).

FIGURE 202 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 203 Example of Paging Display



6. Enter the **exit** command to quit the CLI session.

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.

Prerequisites: Ensure the controller is synched to the NTP server.

Complete the following steps to configure the switch backup.

1. On the menu, click **Network** > **Wired** > **Switches** to display the **Switches** window.
2. From the system tree, select a **Domain** > **Switch Group** or **Switch Group** to perform switch group configuration backup or select a **Switch** to perform a switch configuration backup.

FIGURE 204 Switch Group Configuration Backup

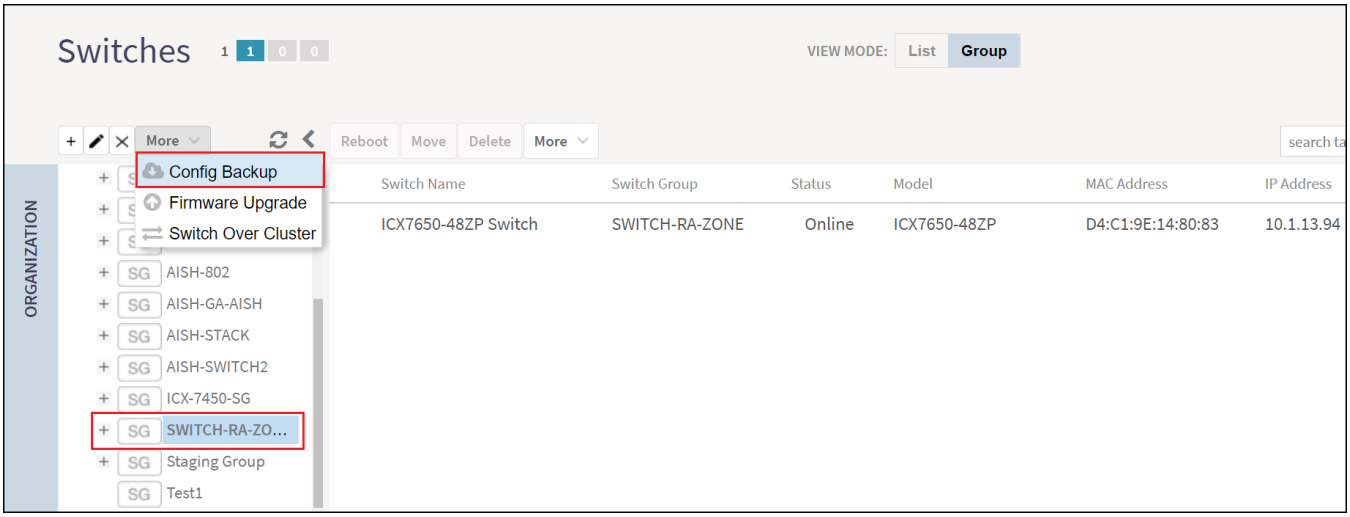
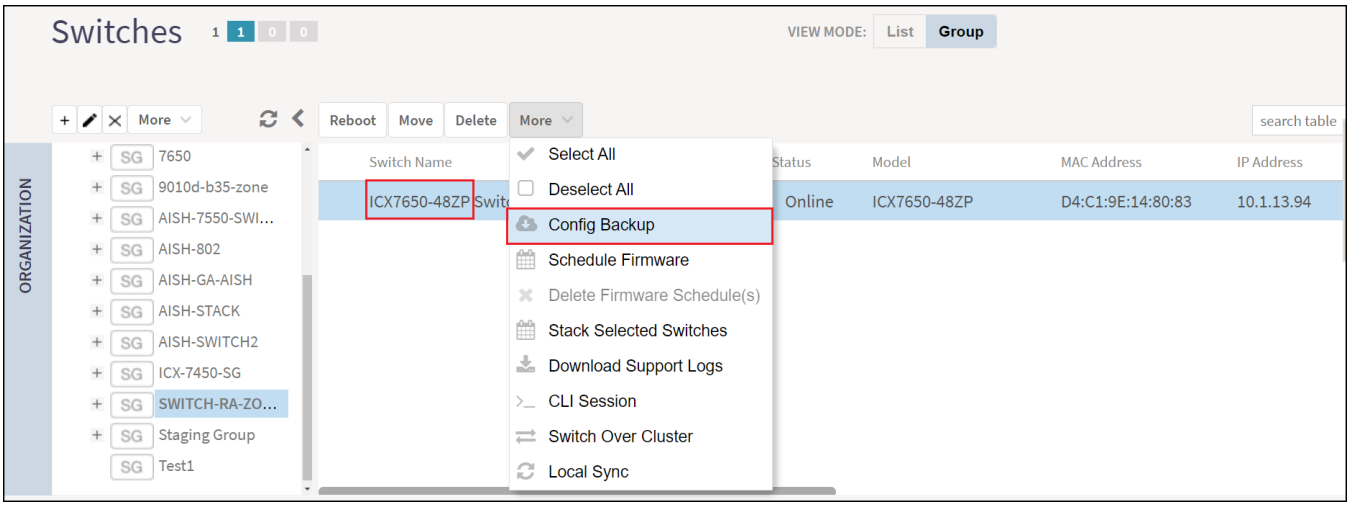
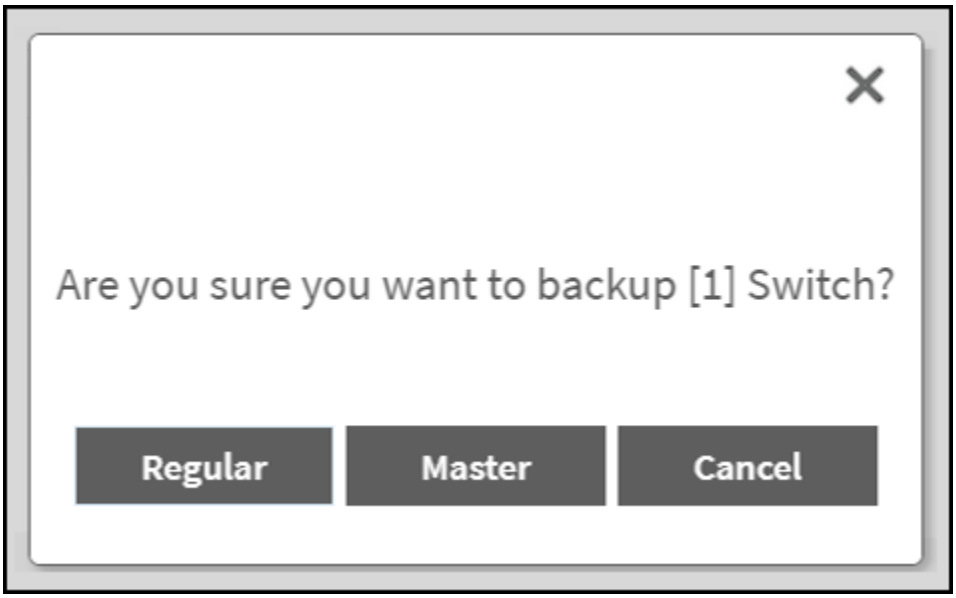


FIGURE 205 Switch Configuration Backup



3. Click **More** > **Config Backup** to display the **Configuration Backup** dialog box.

FIGURE 206 Configuring Backup



A confirmation message is displayed asking the type of backup that must be carried such as **Regular** or **Master**.

The master configuration backup is for the configuration change alert feature. It allows you to select a switch configuration backup to serve as the master configuration backup. If the latest regular configuration backup differs from the master configuration backup, the controller will automatically display an alert indicating a configuration change. The regular configuration backup are the scheduled configuration backup that can be triggered by the user at any time.

NOTE
It is recommended to use master configuration backup, as the regular configuration backup will be removed if there are more than seven different configuration backups. The master configuration backup will not be removed in this case.

4. Click **Master**. A message is displayed confirming that the backup process has been initiated. Click **OK**.

   After the backup is completed, the status is recorded in the **Configuration 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.

   Complete the below steps to restore an individual switch configuration.

   a. From the system tree, select a **Domain** > **Switch Group** or **Switch Group** and select the **Switch** for which you want to perform configuration restore.
   b. In the **Details** tab, click the **Configuration Restore** tab to display the listed configurations in the table.
   c. Select a **Configuration** and click **Config Restore**. A message is displayed stating "Are you sure you want to restore this backup configuration to the Switch?"
   d. Click **Yes** to display the message "Switch Configuration restore operation has started and it will take up to two minutes to complete. Refer to the configuration table to know the status."
   e. Click **OK**.

   Complete the below steps to view the switch configuration differences.

   a. On the **Configuration Restore** tab, select the configurations for which you want to view the differences. Press **Ctrl** key to select more than one configuration.
   b. Click the **Config Diff** tab. The **Configuration Details** table is displayed showing the configurations of the selected switches.

   On the **Configuration Restore** tab, select the configuration to perform the following actions.

   - Click the **Config View** tab to display the **Switch Config View** dialog box to see the configuration details.
   - Click the **Config Download** tab to download the copy of the configuration file.
   - Click the **Master Backup** tab to backup the switch configuration.
   - Click the **Delete** tab to delete the configuration file.

Creating Config Backup for Switch Group

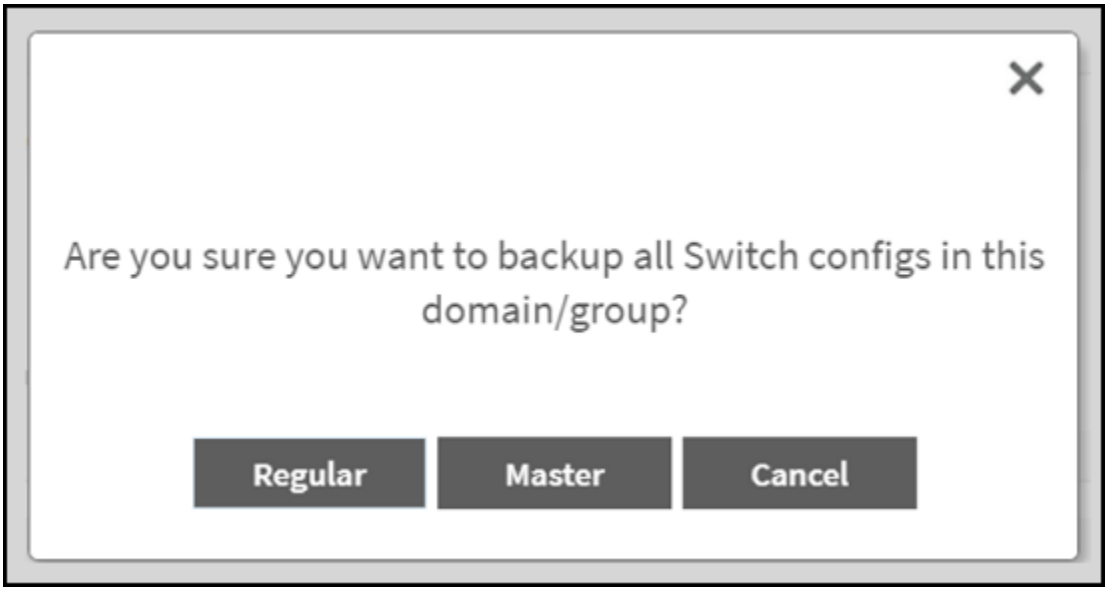
The Master configuration backup allows you to initate a backup of a switch group or domain.

1. On the menu, click **Network** > **Wired** > **Switches** to display the **Switches** window.
2. From the system tree, select the **Domain** > **Switch Group** or **Switch Group**.

3. Click **More** > **Config Backup**.

   A dialog box is displayed asking the type of backup to be performed such as **Regular** or **Master**.

   FIGURE 207 Backing up Switch group or Domain



4. Click **Master** to create master backup for switch groups.

   The **Switch config backup operation is triggered successfully** dialog box is displayed ensuring the backup operation is completed.

5. Click **OK**.

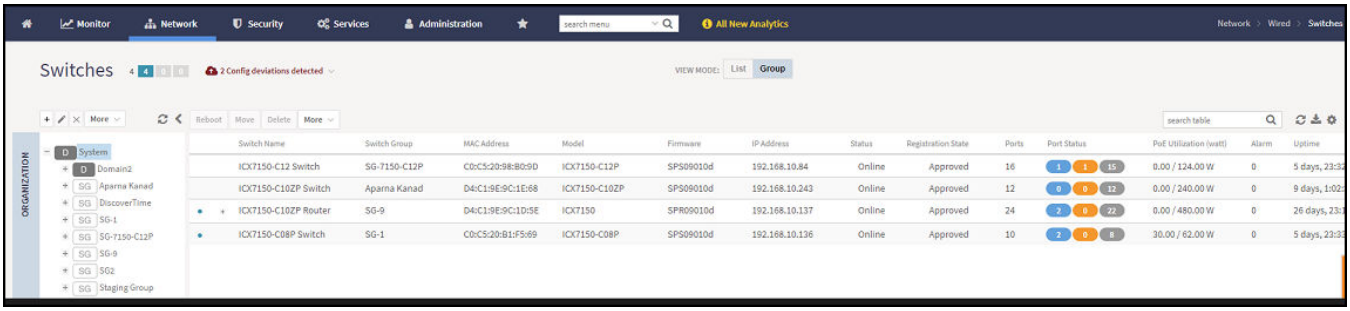
Viewing Configuration Alerts

If you select a config backup as a master config backup, then you will receive an alert if there are any changes in the later backups containing different content. For more information on config backup settings, refer the topics Backing up and Restoring Switch Configuration on page 426 and Creating Config Backup for Switch Group on page 429.

1. On the menu, click **Network** > **Wired** > **Switches** to display the **Switches** window.

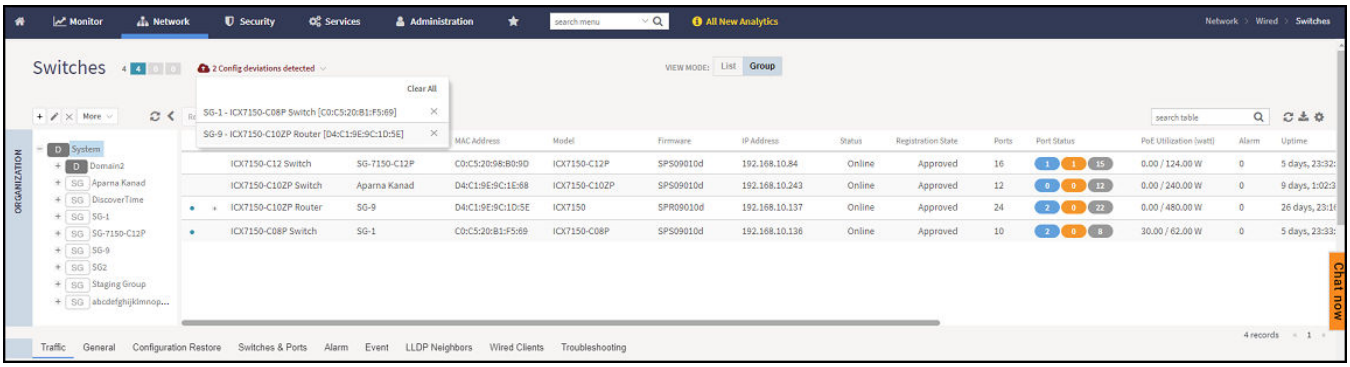
   The alert is displayed at the top of the switch page.

   FIGURE 208 Master Backup Alert



2. You can select switch or switch groups from the alert list to view the last updated backup configurations.

FIGURE 209 Expanding the drop-down list of Alert



3. You can click Clear All to clear all of the alerts from the list, or you can individually remove each switch by clicking ✕.

NOTE

The icon in the switch table announces that the backup in the switch configuration is changed. The icon and the alert are cleared automatically when the latest config is same as master backup config.

Firmware Upgrade

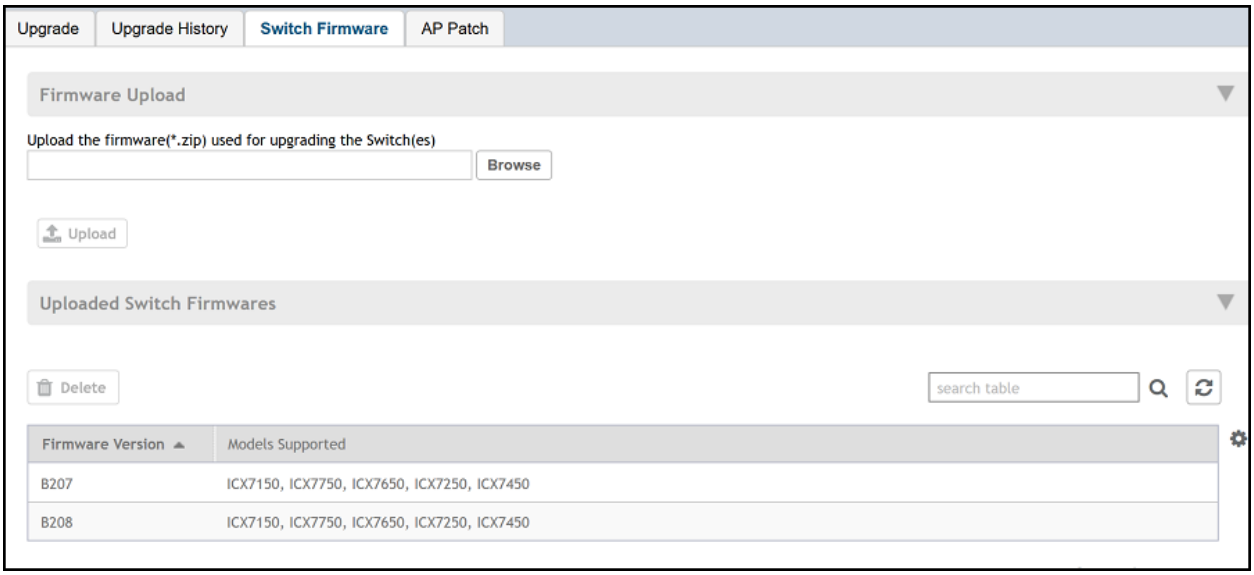
Uploading the Switch Firmware to the Controller

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 210 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.

Configuring the Group Firmware Settings

The Group Firmware Settings allows you to select default firmware for the switch group.

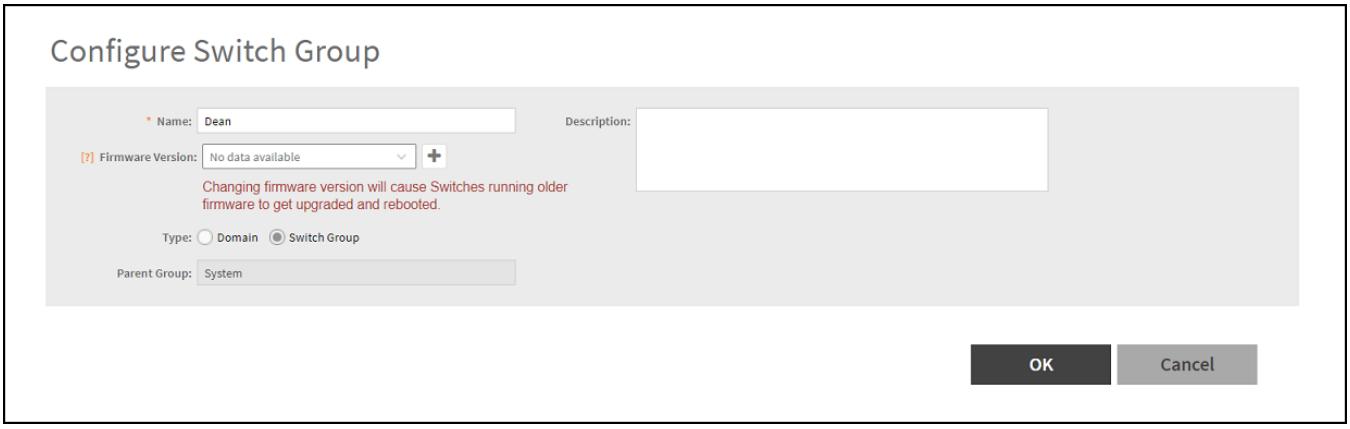
NOTE
The default firmware selection at group level does not trigger upgrade for the existing switches in the switch group, it only triggers upgrade for newly joined switches. The newly joined switches are upgraded to the selected firmware in the switch group.

Complete the following steps to perform the firmware upgrade of newly added switch in the switch group to the default firmware version.

1. On the menu, click **Network** > **Wired** > **Switches** to display the **Switches** window.

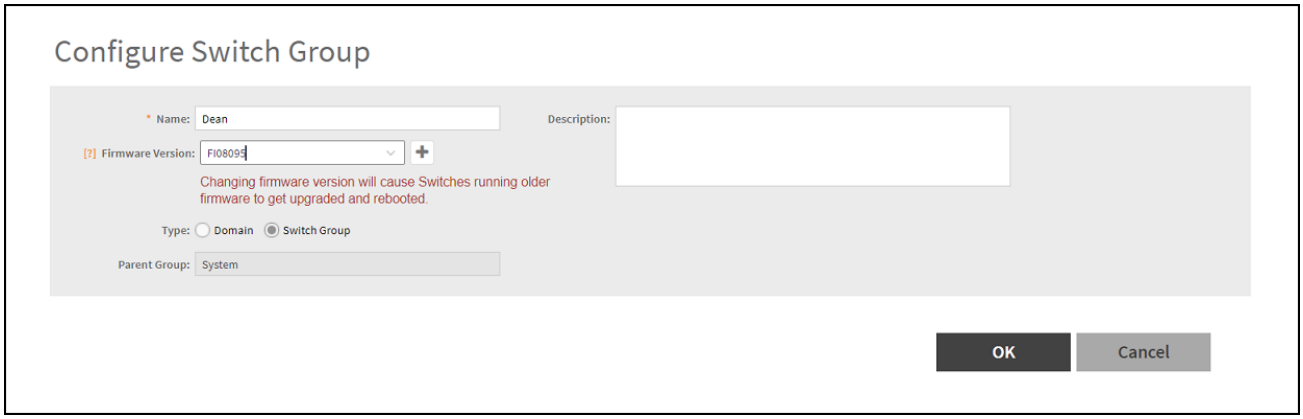
2. From the system tree, select a **Domain** > **Switch Group** or **Switch Group** that you want to configure, and click icon to display the **Configure Switch Group** page.

FIGURE 211 Configuring the Switch with Default Version



3. Complete the following details:
   - **Name**: Enter the name for the switch group.
   - **Description**: Enter a brief description about the switch group .
   - **Firmware version**: Select a firmware version from the list or retain the default firmware version.

     FIGURE 212 Configuring the Switch Group with Firmware Version



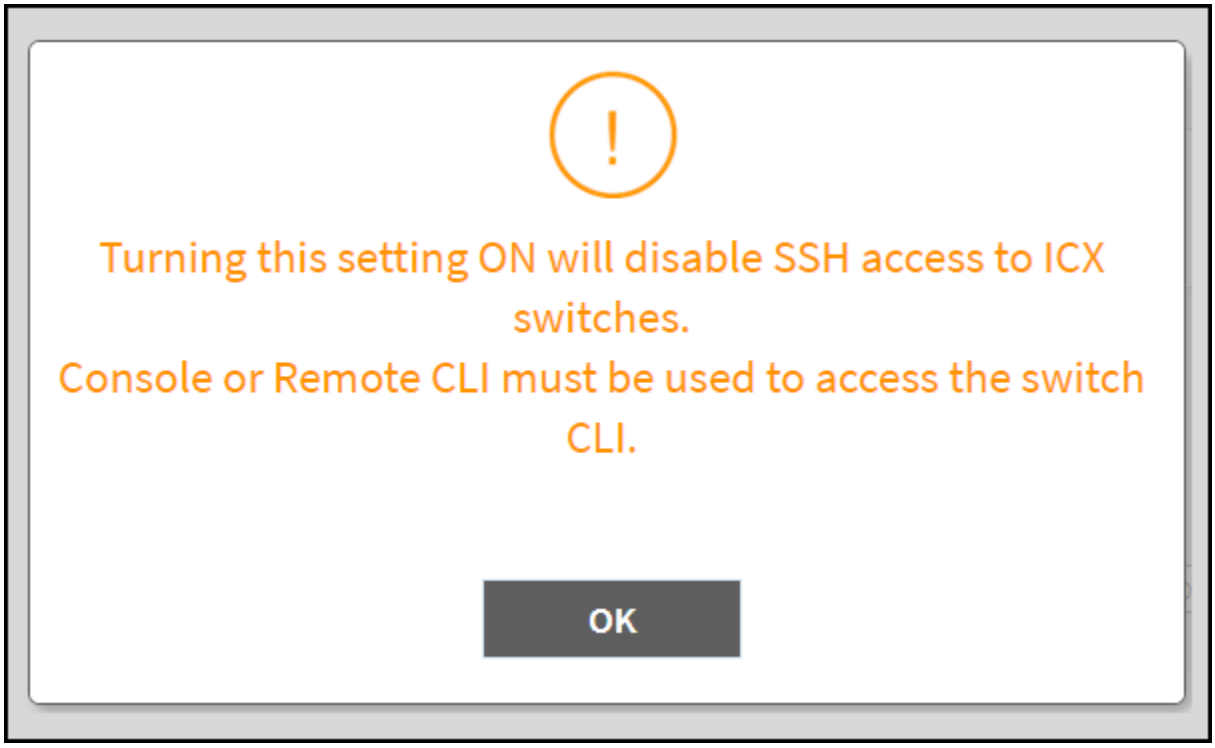
     NOTE
     The Group Firmware Settings requires switches to be running on SmartZone 5.2.1 or later.

   - **Type**: Choose **Switch Group**.
   - **Parent Group**: Displays the parent group under which the switch group resides.
   - **Two Factor Authentication**: Switch **ON** to use the **Console CLI** or **Remote CLI** to access the **Switches**.

     NOTE
     Turning ON this feature will disable the SSH access to the switches.

     A **Message** dialog box is displayed, click **OK**.

FIGURE 213 Two Factor Authentication Message



- **Backup Schedule**: Allows you to schedule the backup. From the **Interval** drop-down list, select the type of backup such as **Daily**, **Weekly**, or **Monthly**. If the backup selected is **Daily**, you can configure **@Hour** , and **Minute** fields. If the backup selected is **Weekly**, you can configure the **Every** (day of the week), **@Hour** , and **Minute** fields. If the backup selected is **Monthly**, you can configure **Every** (date), **@Hour** , and **Minute** fields.

  NOTE
  The default backup time for scheduling a **Daily** backup is 3:30 a.m. The backup schedule is configured on the level one switch group.

4. 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.

NOTE
Beginning with FastIron release 10.0.0, a switch ("Layer 2") image will no longer be provided for ICX devices. Only the router ("Layer 3") image will be available. On Upgradeto FastIron 10.0.00, the configuration of any ICX devices operating with the switch image will automatically be translated to the equivalent router image configuration.The target upgrade to 10.0.0 supports only router code.
The following features are deprecated as a result of this change:

- The IP default gateway
- The management VLAN
- Global configuration of the IP address (Going forward, the IP address must be configured at the interface level for each port.)

Refer to the RUCKUS FastIron Software Upgrade Guide for additional details.

Complete the following steps to perform a firmware upgrade on the switch group.

1. On the menu, click **Network** > **Wired** > **Switches** to display the **Switches** window.
2. In the **Organization** tab, select a **Domain** > **Switch Group** or **Switch Group**.

3. Click **More** > **Firmware Upgrade** to display the **Upgrade Firmware (Group)** dialog box.

FIGURE 214 Selecting Firmware Upgrade for a Switch Group

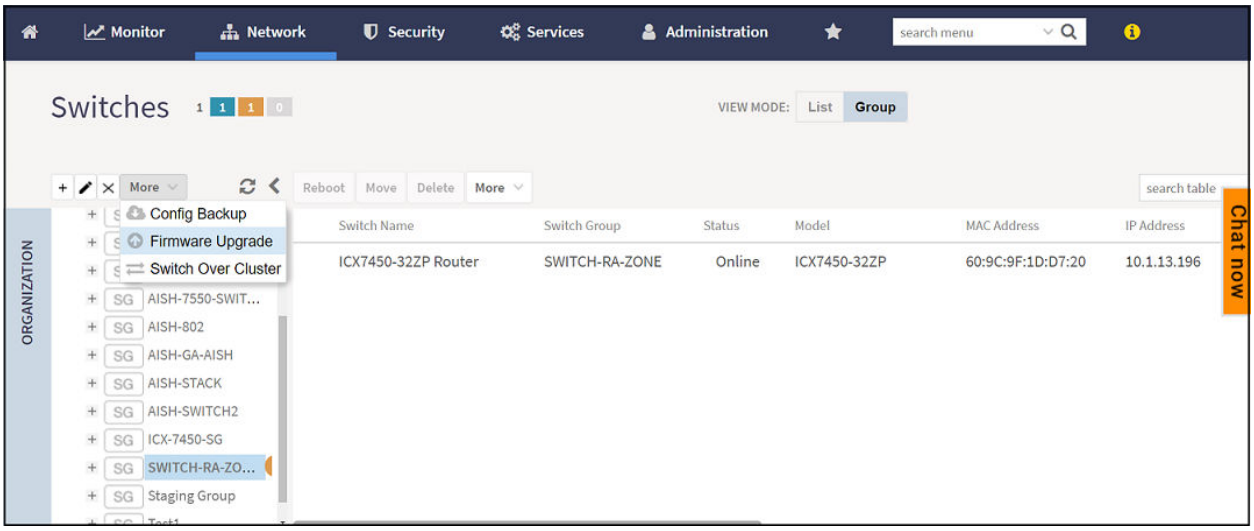
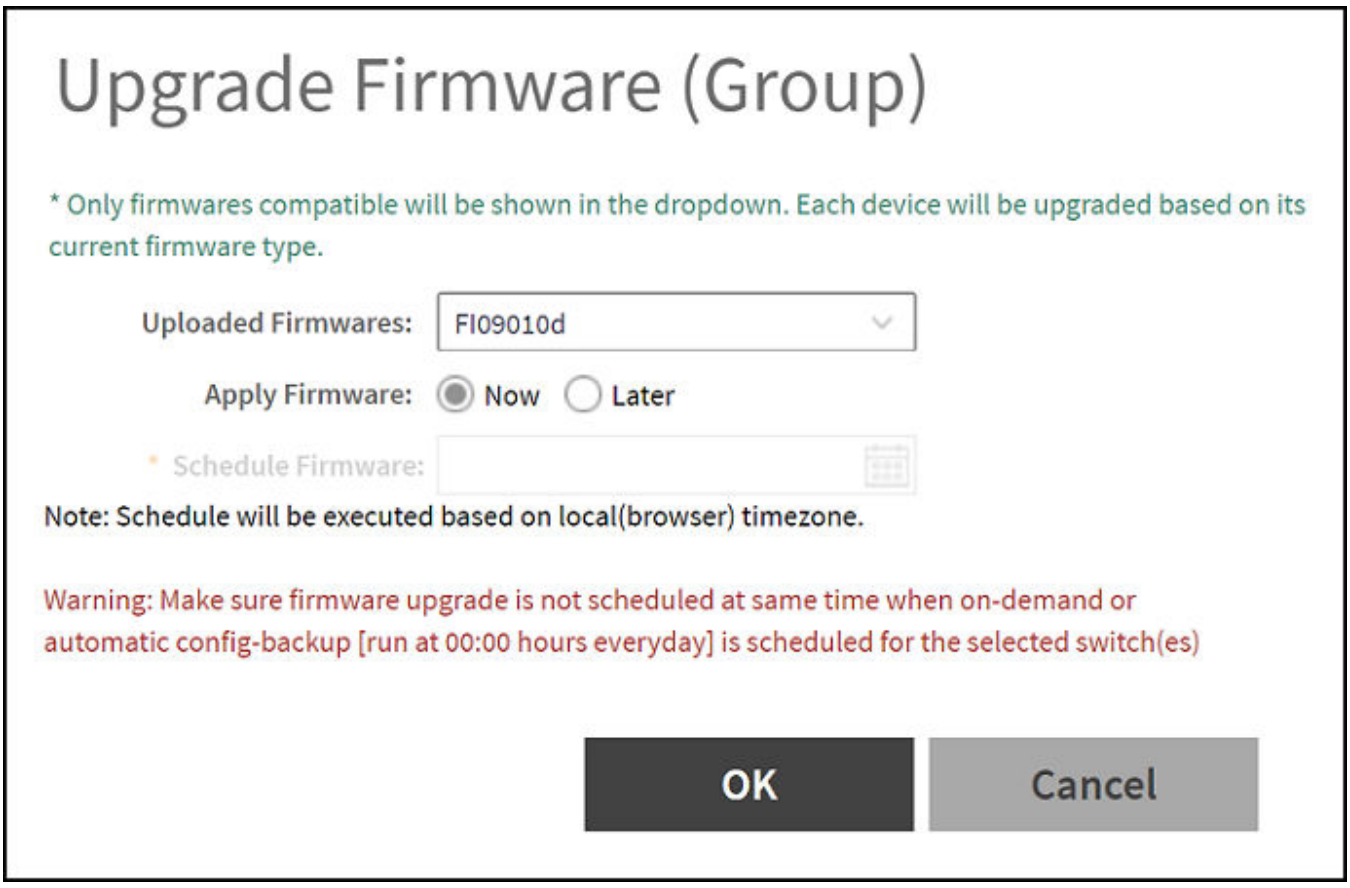


FIGURE 215 Scheduling the Upgrade for a Switch Group



4. Complete the following fields:
   - **Uploaded Firmwares**: Select firmware from the list.
   - **Apply Firmware**: Select Now or Later to set the new firmware version to the switch group.
   - **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.

Prerequisites

- Upload a valid FastIron firmware version (newer than version 8.0.80) to the controller.
- Sync the controller with the NTP server. On the controller user interface, navigate to **Administration** > **System** > **Time** then click **Sync Server**.

Scheduling Firmware Upgrade

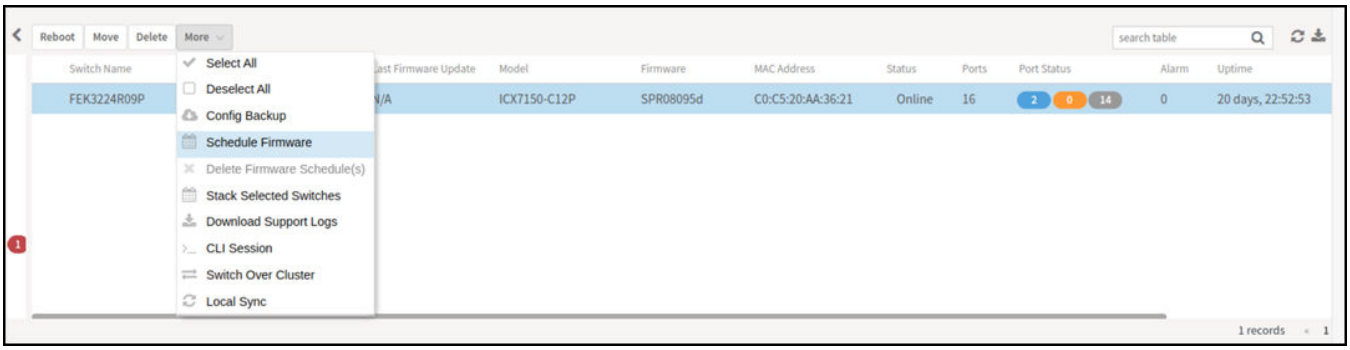
1. From the main menu, click **Network** > **Wired** > **Switches**.

   The **Switches** page is displayed.
2. Select a **Domain** > **Switch Group** or specific **Switch Group** and select the **Switch** that you want to upgrade.

   NOTE
   To upgrade the firmware for multiple switches simultaneously, hold down the **Ctrl** key as you select the desired switches.

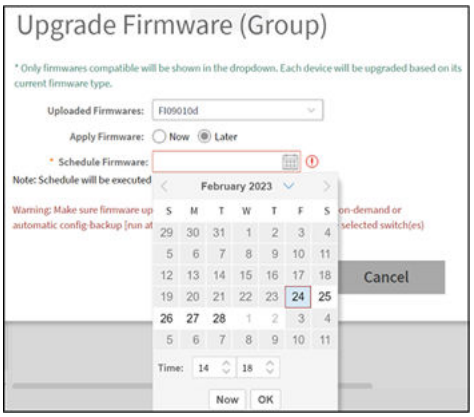
3. Click **More** > **Schedule Firmware**.

FIGURE 216 Selecting Schedule Firmware



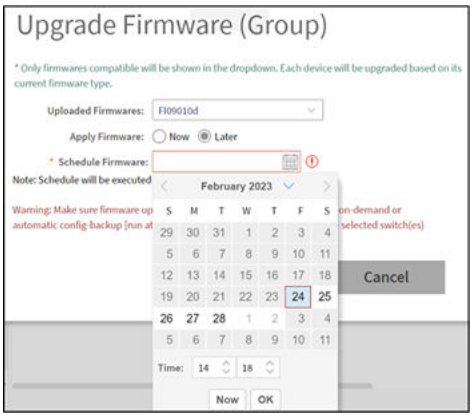
The **Upgrade Firmware** dialog box is displayed.

FIGURE 217 Scheduling Firmware Upgrade



4. Complete the following fields:
   - **Uploaded Firmwares**: Select the firmware version that you want the switch to be upgraded to.
   - **Firmware Type**: Select type of firmware you want to upload to the switch. Options include **Switch** and **Router** images.
   - **Apply Firmware**: Set when you want to apply the new firmware version to the switch. You can select **Now** or **Later** to schedule your upgrade. If you select **Later**, then you must select the date and time from the **Schedule Firmware** field.

FIGURE 218 Scheduling Firmware Upgrade



The switch upgrade request success message is displayed.

FIGURE 219 Switch Upgrade Request Success

5. Click **OK**.

6. To monitor the firmware upgrade progress, select the target switch and click the **Firmware History** tab. Hover your cursor over any message in the **Status** field for a tooltip providing additional information regarding that stage of the upgrade process.

   The images of six stages of completion along with their tooltips are shown below.

FIGURE 220 Preparing Phase with Tooltip

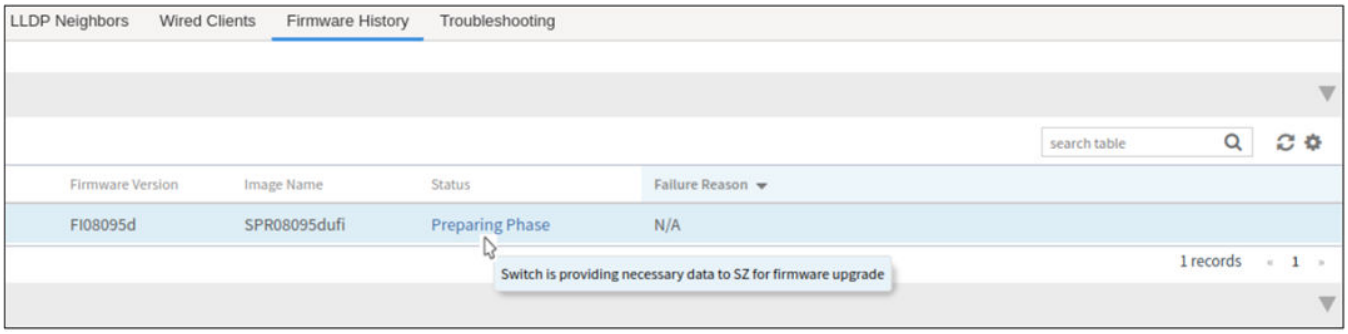


FIGURE 221 Backup Image Start with Tooltip

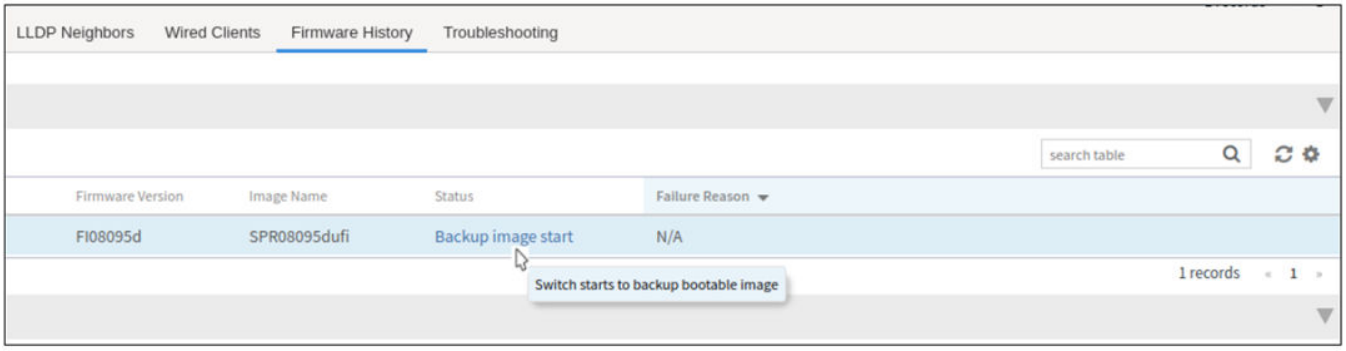


FIGURE 222 Backup Image Complete with Tooltip

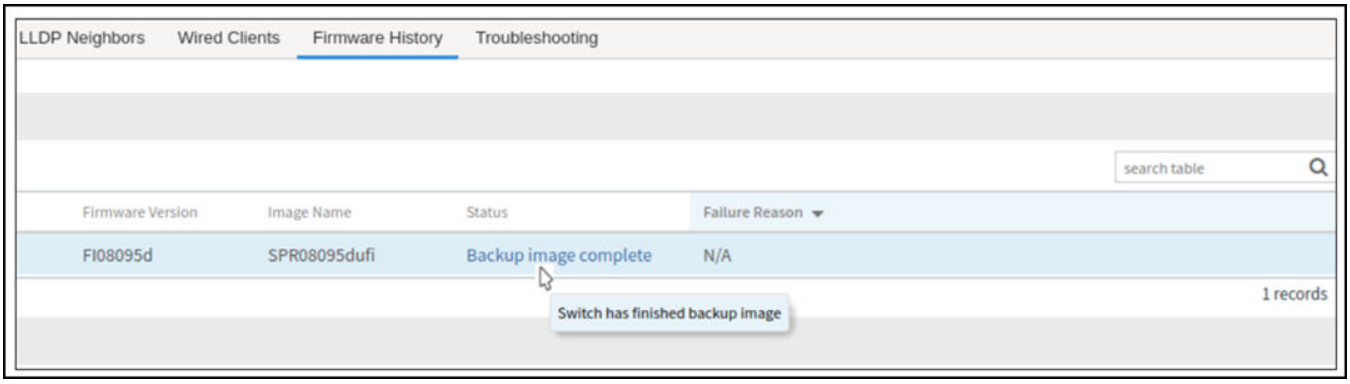


FIGURE 223 Download Image Start with Tooltip

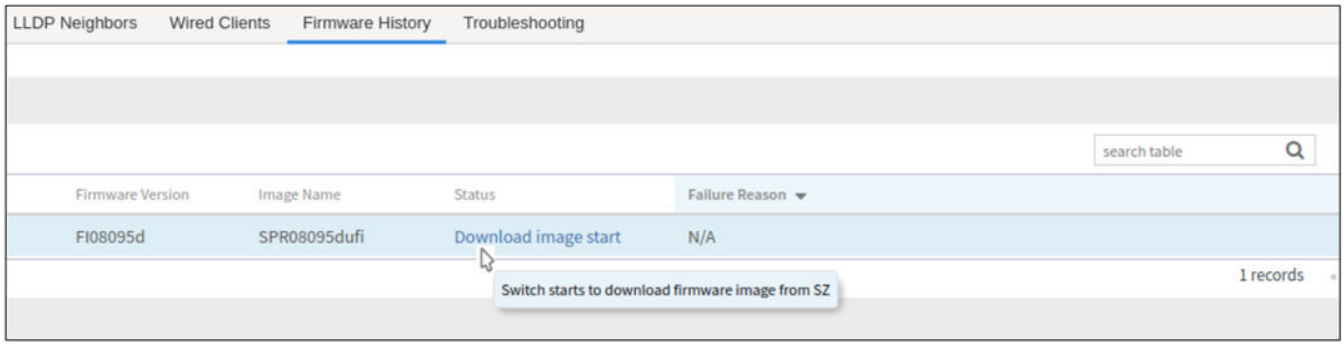


FIGURE 224 Download Image Complete with Tooltip

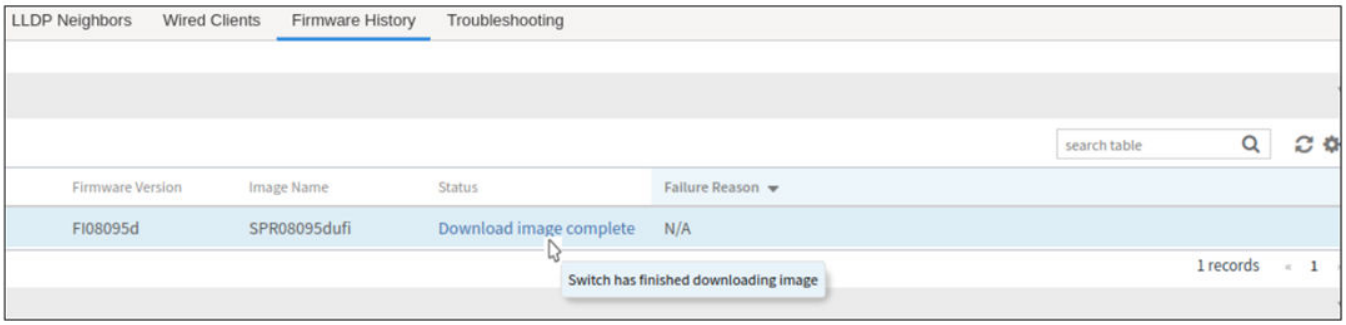
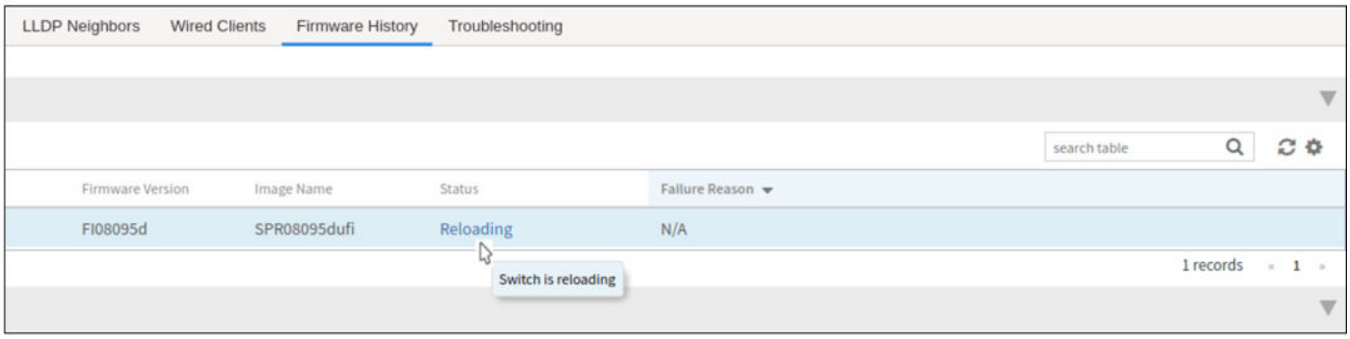


FIGURE 225 Reloading phase with tooltip



Deleting the Firmware Upgrade Schedules

If you schedule a firmaware upgrade, and if the firmware upgrade is not executed or is in progress then this feature allows you to cancel the firmware upgrade. However, it must be noted that if the switch is copying or downloading the firmware, the controller will not be able to cancel the process.

To delete the firmware upgrade process, perform the following steps.

1. On the menu, click **Network** > **Wired** > **Switches** to display the **Switches** window.

2. In the **Organization** tab, select a **Domain** > **Switch Group** or **Switch Group** and select the **Switch**. In the **Details** tab, click **More** > **Delete Firmware Schedules**.

FIGURE 226 Upgrade in Progress

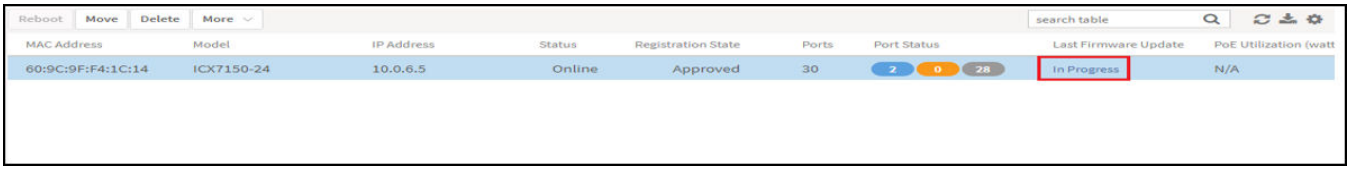
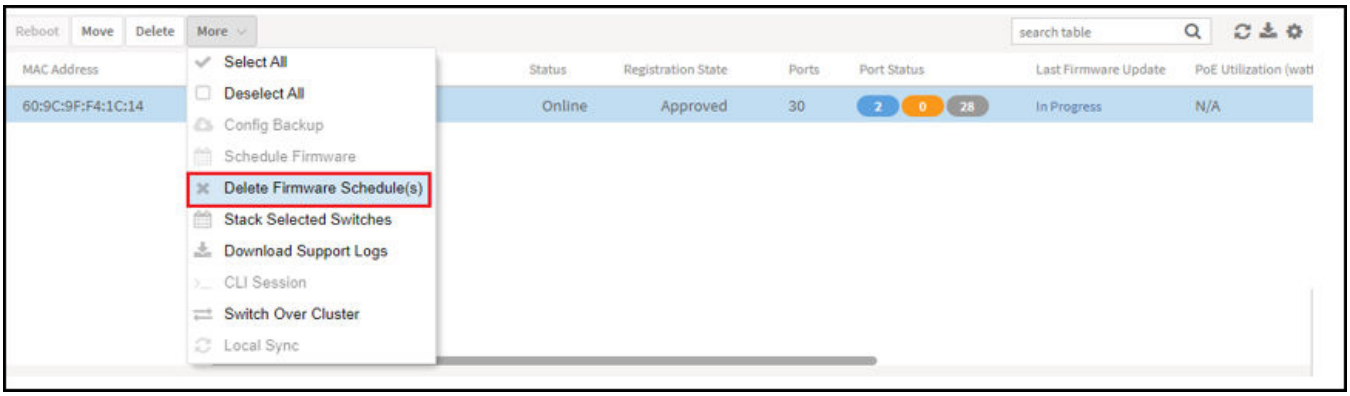
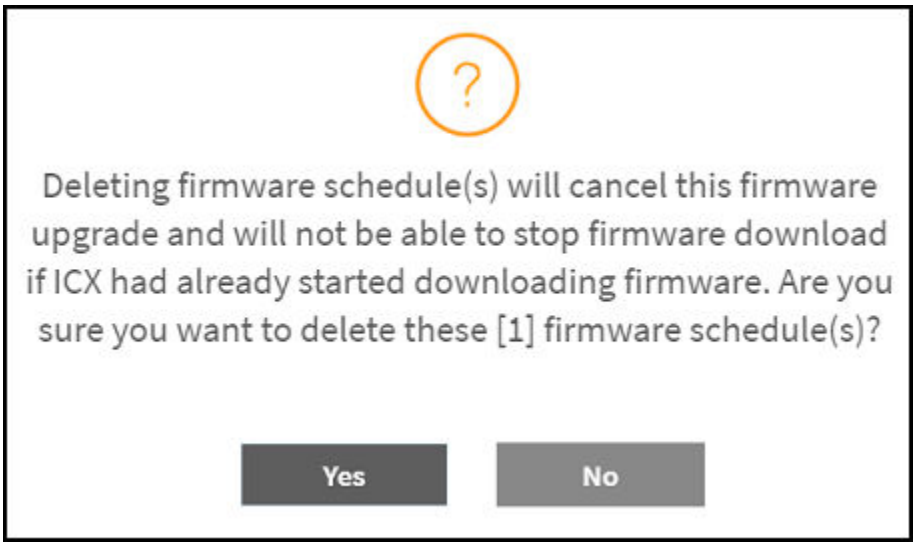


FIGURE 227 Deleting Firmware Upgrade Schedule(s)



A warning message is displayed before you cancel the upgrade.

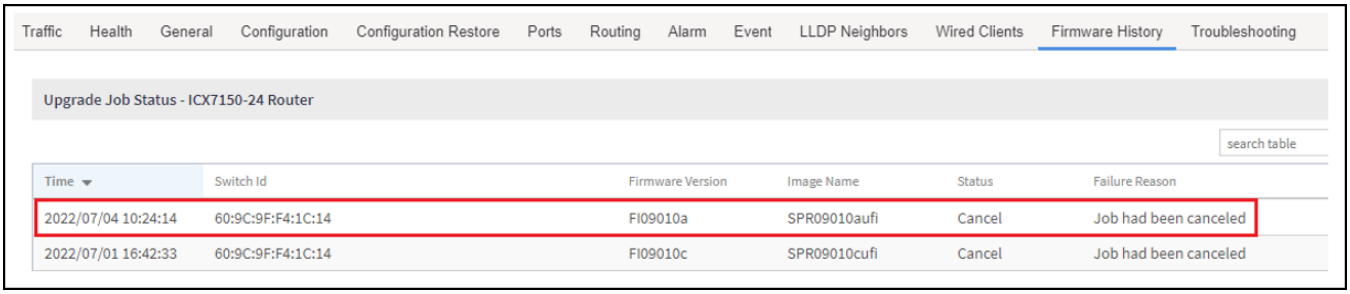
FIGURE 228 Warning Message before deleting



3. Click **Yes** to delete the firmware schedule.
4. A **Switch firmware schedule(s) deleted successfully** message dialog box is displayed, click **OK**.

5. In the **Organization** tab, select the **Switch** and in the **Details** tab, select the **Firmware History** tab. In the **Upgrade Job Status** tab confirm that the schedule is canceled.

FIGURE 229 Confirming the deletion



Monitoring Switch Status

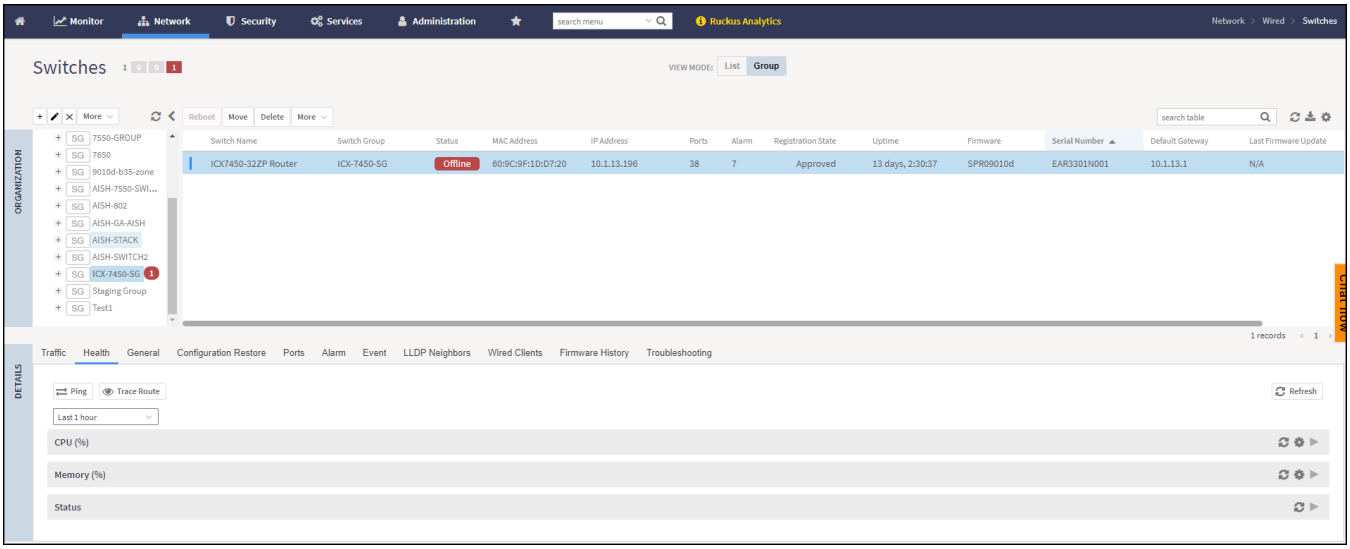
Viewing Switch Health

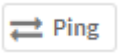
Health information displayed for a switch is based on memory usage and CPU usage statistics.

To view information on the health of a switch or the active controller of a stack, perform the following steps.

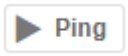
1. On the menu, click **Network** > **Wired** > **Switches** to display the **Switches** window.
2. In the **Organization** tab, select a **Domain** > **Switch Group** or **Switch Group** and select the **Switch**.
3. In the **Details** tab, click **Health** tab.

FIGURE 230 Health



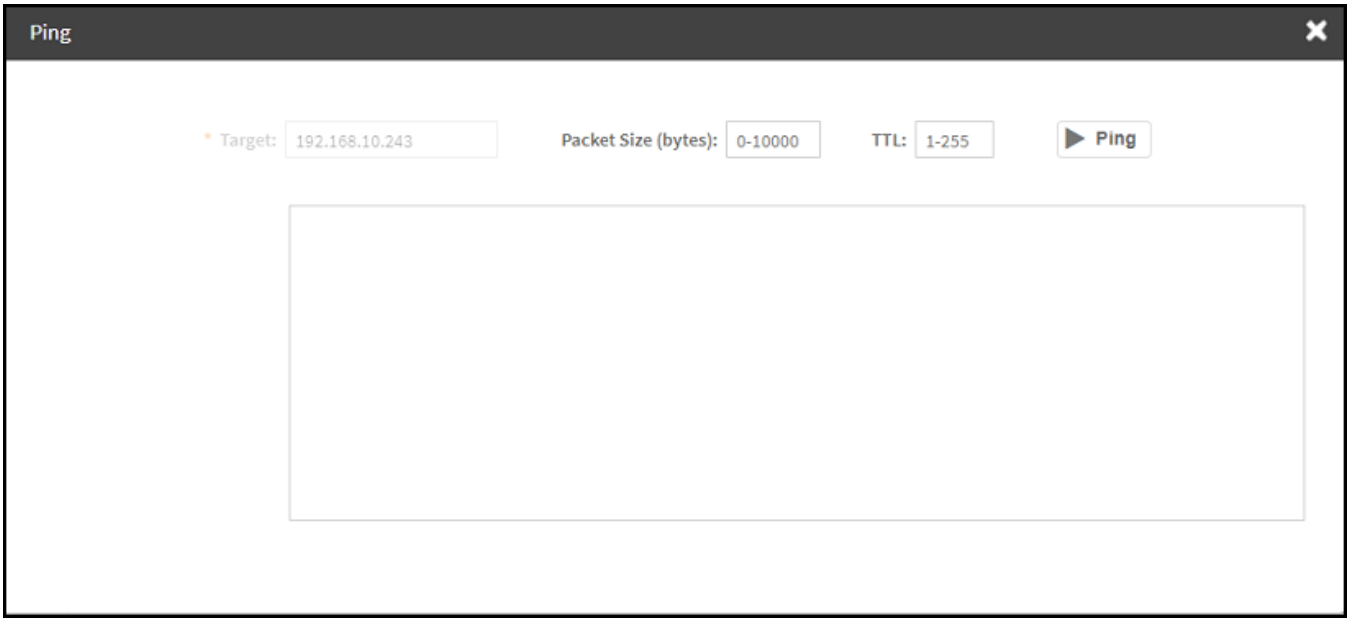
4. Click 

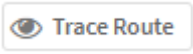
icon to display the **Ping** dialog box.

5. In the **Ping** dialog box, enter the IP address of the target switch, packet size, and TTL (Time to Live) value. Click 

icon. In the below display window you can view that 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 231 Pinging the switch



6. Click 

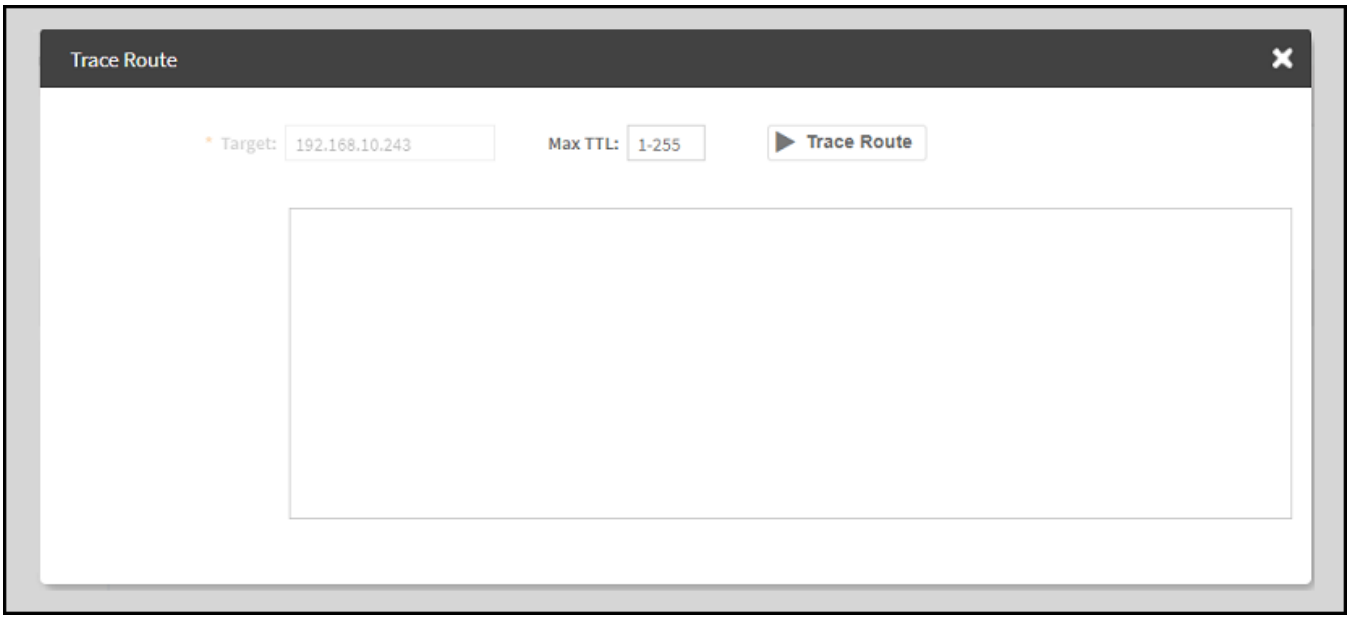
icon to display the **Trace Route** dialog box.

7. On the **Trace Route** dialog box, enter the TTL (Time to Live) value. Click 

icon. In the below display window you can view that a 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 232 Tracing the packet route through the network

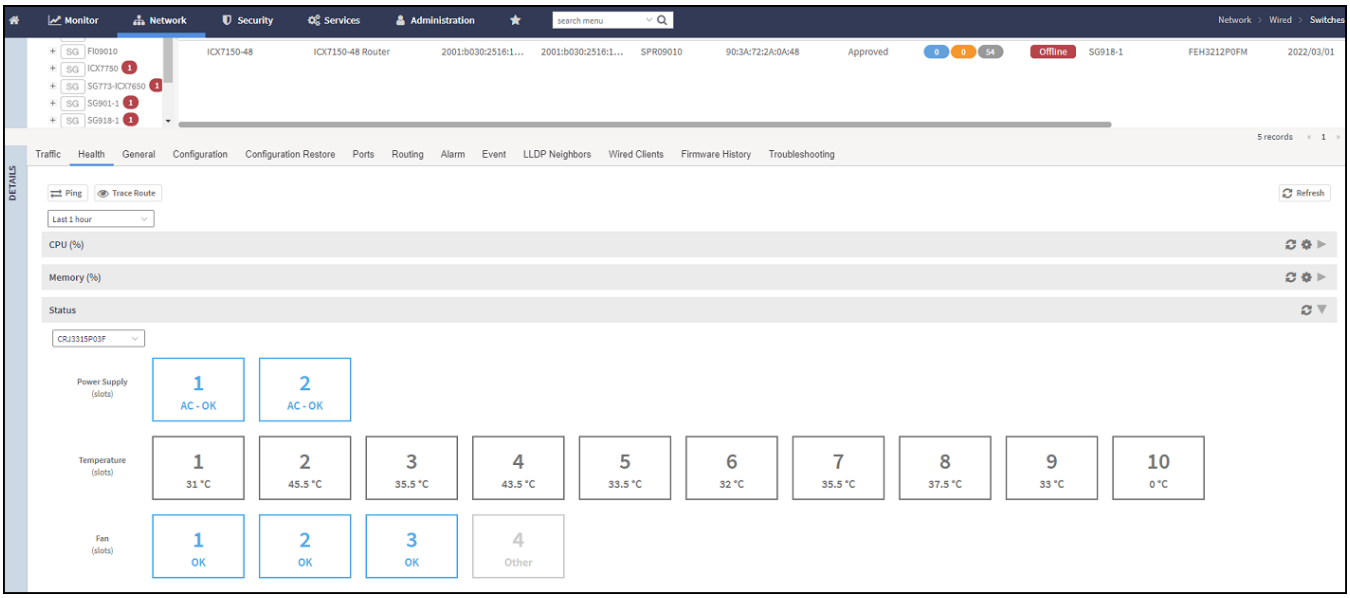


8. In the **Health** tab, from the drop-down menu 

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 233 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

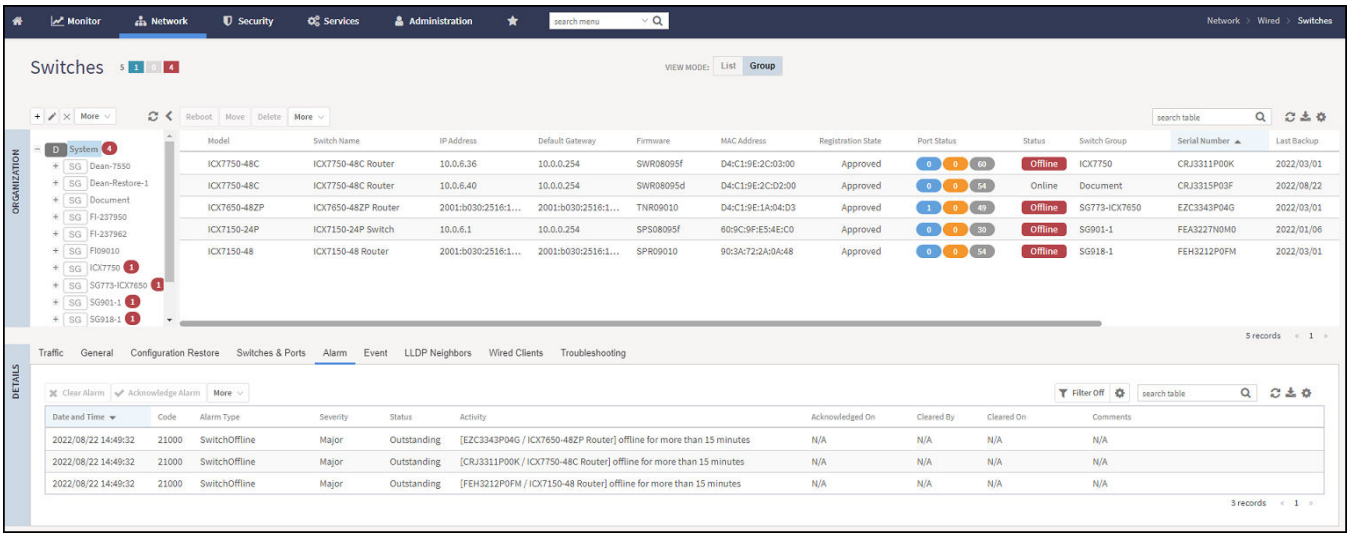
The remaining syslog messages which are categorized by other severity levels are listed in the `switchevent.log` file available in **Diagnostics** > **Application Logs**.

The alarms generate for the switch also reflect in the **Monitor** > **Events and Alarms** > **Events** page.

1. On the menu, click **Network** > **Wired** > **Switches** to display the **Switches** window.

2. In the **Organization** tab, select a **Domain** > **Switch Group** or **Switch Group** and select the **Switch**. In the **Details** tab, click **Alarm** tab.

FIGURE 234 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.

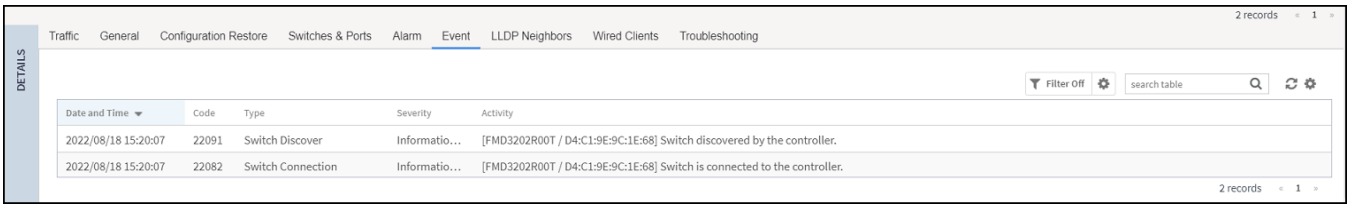
Viewing the Events

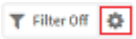
Events are triggered by an occurrence or the detection of certain conditions in the switch. For example, when the temperature of the device reaches warning levels, or when the fan speed changes, an event is triggered. You can find these details in the **Events** tab, accessible for individual switches, stacks, and switch groups.

The alarms generate for the switch also reflect in the **Monitor** > **Events and Alarms** > **Events** page.

1. On the menu, click **Network** > **Wired** > **Switches** to display the **Switches** window.
2. From the system tree, select a **Domain** > **Switch Group** or **Switch Group** and select the **Switch**.
3. In the **Details** pane, click the **Events** tab.

   FIGURE 235 Events Tab



4. The following information is displayed in the **Events** tab.
   a) **Date and Time**: Displays the date and time when the event occurred.
   b) **Code**: Displays the event code (see the Alarm and Event Reference Guide for your controller platform more information).
   c) **Type**: Displays the type of event that occurred (for example, Switch configuration updated).
   d) **Severity**: Displays the severity level assigned to the events such as Critical, Debug, Informational, Warning, Major etc.
   e) **Activity**: Displays additional details about the event.
5. 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.
6. Click  to filter the alarms by their severity, date and time.

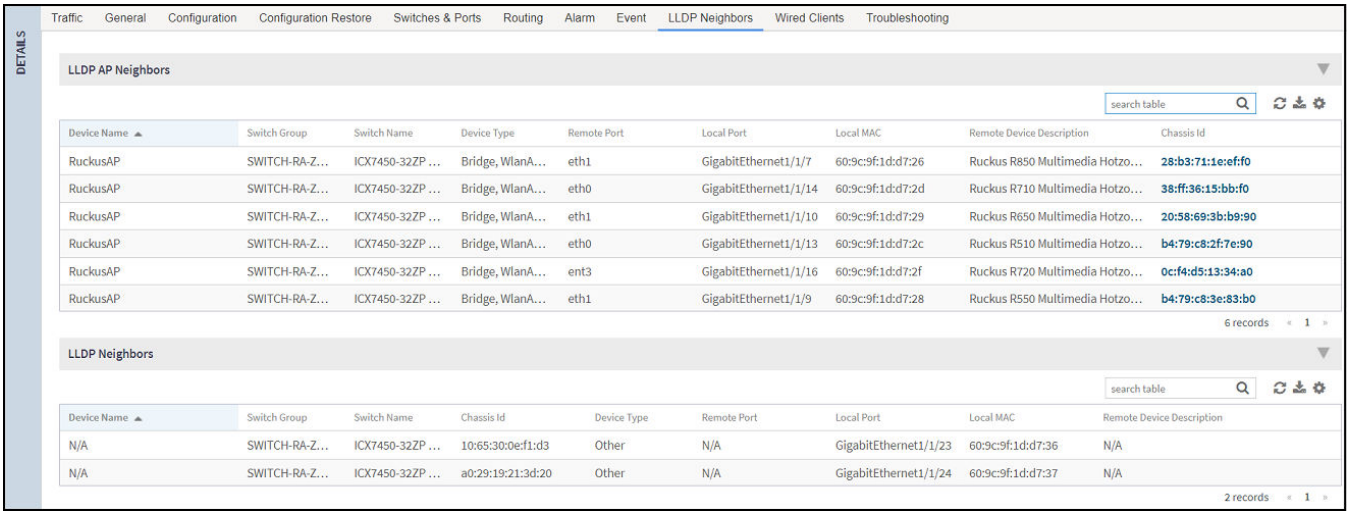
Viewing LLDP Neighbor Information

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. On the menu, click **Network** > **Wired** > **Switches** to display the **Switches** window.

2. In the **Organization** tab, select a **Domain** > **Switch Group** or **Switch Group** and select the **Switch**. In the **Details** tab, click **LLDP Neighbors** tab.

FIGURE 236 LLDP Neighbors Connected to the Switch



The following LLDP Neighbors information for switch is displayed in the **LLDP AP Neighbors** tab and **LLDP Neighbors** tab:

- Device Name: Displays the name of the LLDP neighbor or AP neighbor connected to the switch.
- Switch Group: The name of the group to which the switch belongs.
- Switch Name: The name of the switch or group.
- Device Type: Displays the name of the device type (for example, Router).
- Remote Port: Displays the remote port to which the device is connected.
- Local Port: Displays the local port the device is connected to.
- Local MAC: Displays the local MAC address of the device.
- Remote Device Description: displays the name of the remote device.
- Chassis Id: Display the chassis id information.

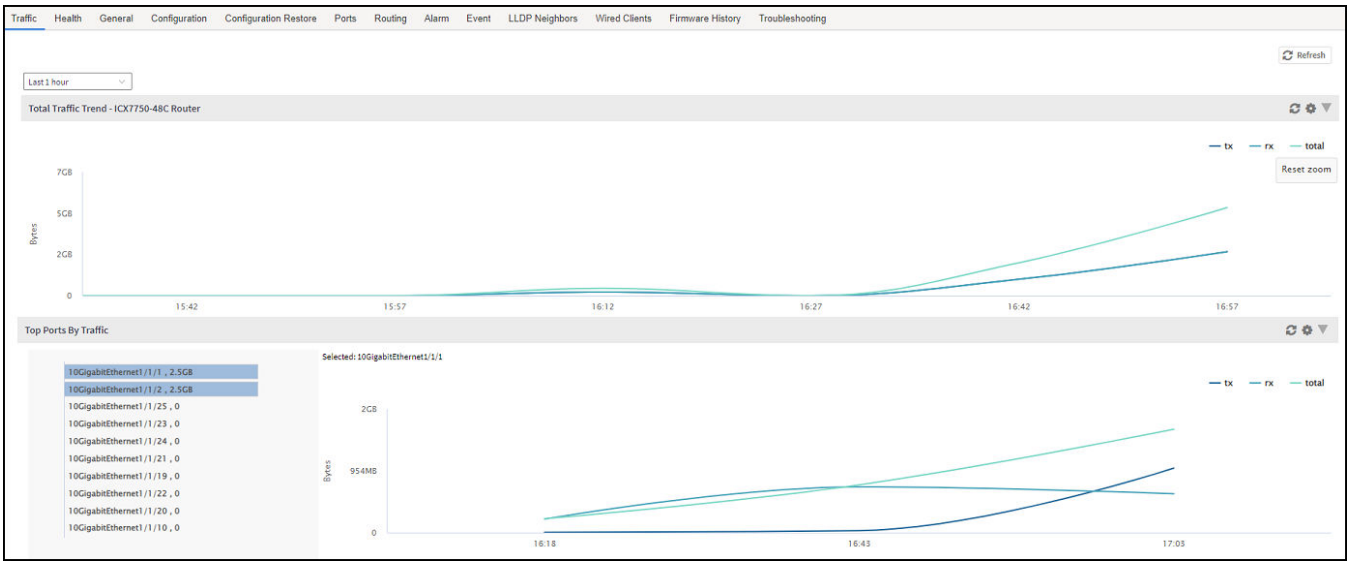
Viewing Traffic Trends in the Switch

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. On the menu, click **Network** > **Wired** > **Switches** to display the **Switches** window.

2. In the **Organization** tab, select a **Domain** > **Switch Group** or **Switch Group** and select the **Switch**. In the **Details** tab, click **Traffic** tab.

FIGURE 237 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.

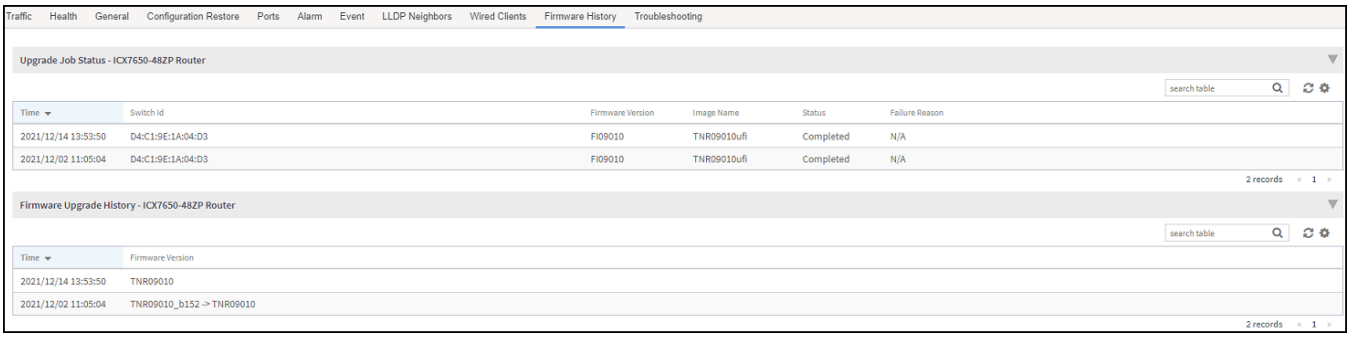
Viewing Firmware History of the Switch

The **Firmware History** allows you to view the detailed status and results of the firmware updates for a switch, as well as view the history of past firmware upgrades on the switch.

You must upgrade the switch firmware as described in Scheduling a Firmware Upgrade for Selected Switches on page 438

1. On the menu, click **Network** > **Wired** > **Switches** to display the **Switches** window.
2. From the system tree, select a **Domain** > **Switch Group** or **Switch Group** and select the **Switch**.
3. In the **Details** pane, click the **Firmware History** tab.

   FIGURE 238 Viewing Firmware History



4. In the **Upgrade Job Status** section, you can verify the upgrade status including the time, switch ID, firmware version, image name, status and any failure reasons (if applicable).
5. In the **Firmware Upgrade History** section, you can see the times of previous upgrades and the firmware versions used.

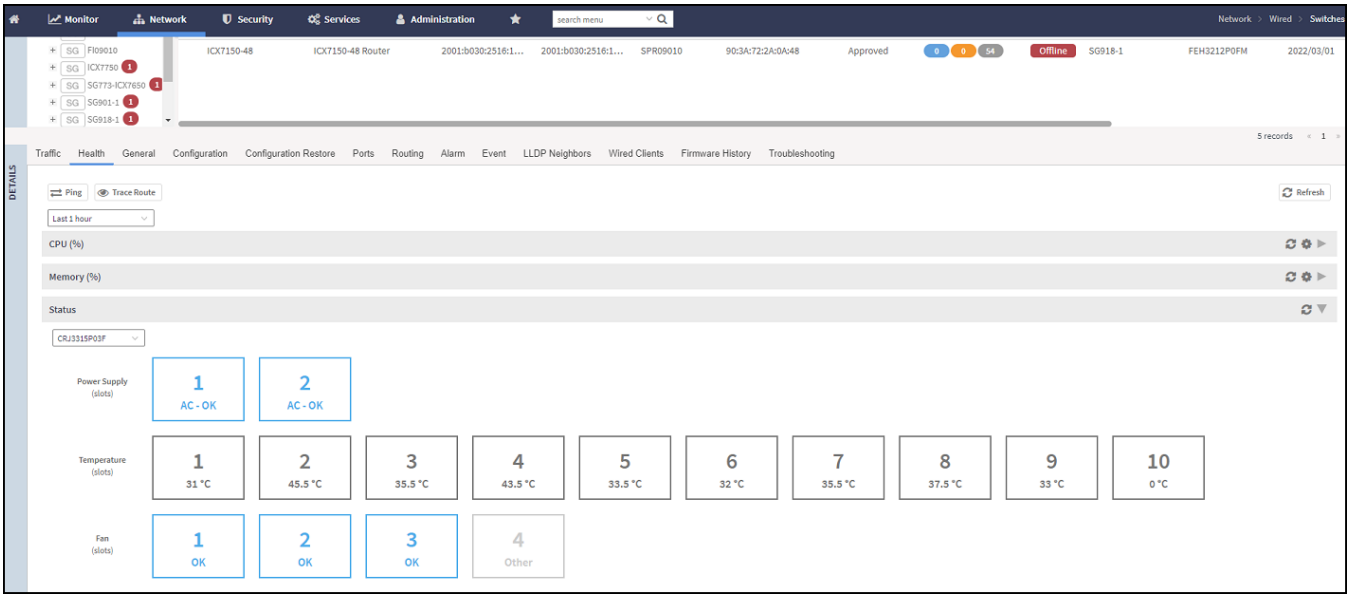
Viewing PoE Utilization and Health Status of the Switch

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. On the menu, click **Network** > **Wired** > **Switches** to display the **Switches** window.
2. In the **Organization** tab, select a **Domain** > **Switch Group** or **Switch Group** and select the **Switch**.

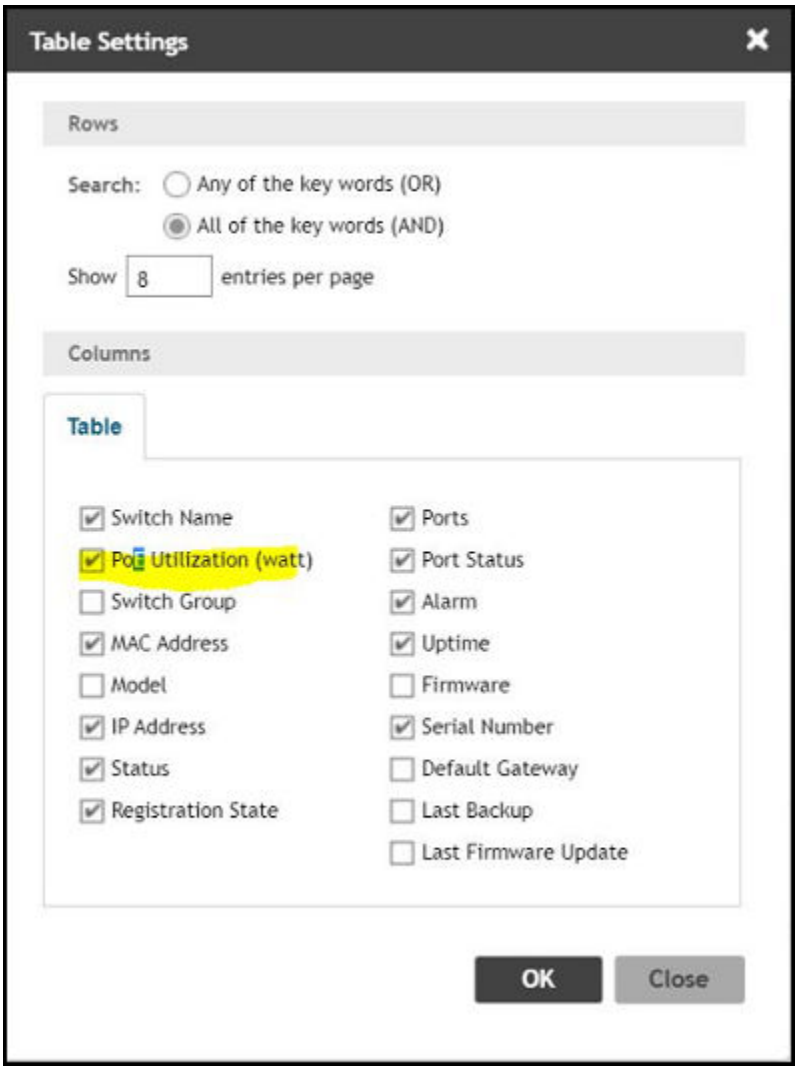
3. In the **Details** tab, click **Health** tab. In the **Status** tab you can view the health status, such as the power supply, temperature, and fan status of the stack switch.

FIGURE 239 Viewing the Health Status of Stack Switch



4. To enable the PoE Utilization, In the **Organization** tab, click icon at the top right to display the **Table Settings** dialog box.

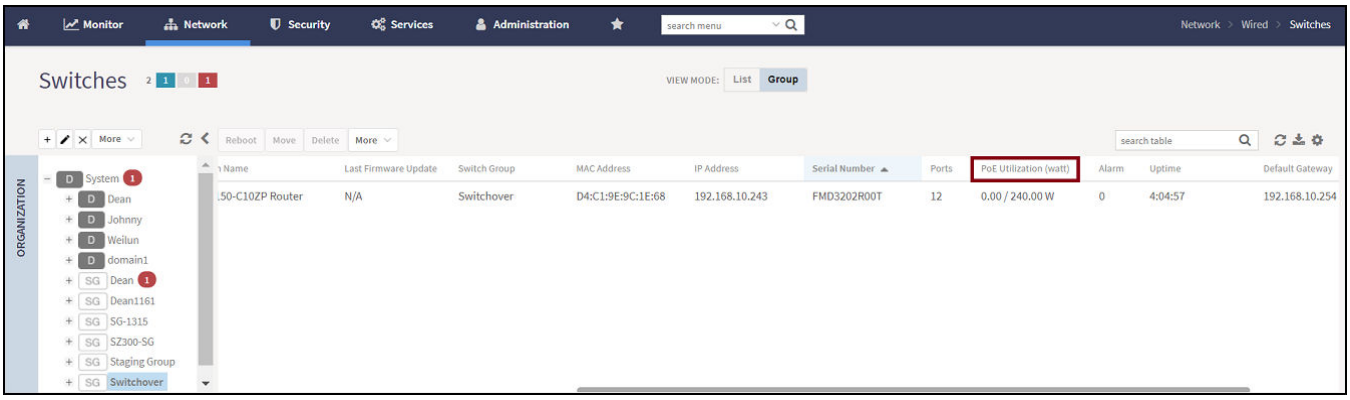
FIGURE 240 Enabling the PoE Utilization



5. Select the **PoE Utilization (watt)** from the table.
6. Click **OK**.

7. In the **Organization** tab, select the **Switch**, to view the **PoE Utilization (watt)** field listed in the table.

   FIGURE 241 Viewing the PoE Utilization Field



Viewing Switches on the Dashboard

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

1. On the menu, click **Monitor** > **Dashboard** > **Wired** to display the **Dashboard** window.
2. In the **Health** tab, click System icon to display the connected switches.

   The **Settings-Health Dashboard** page is displayed.

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

FIGURE 242 Viewing Wired Dashboard - Ball

FIGURE 243 Viewing Wired Dashboard - Topology

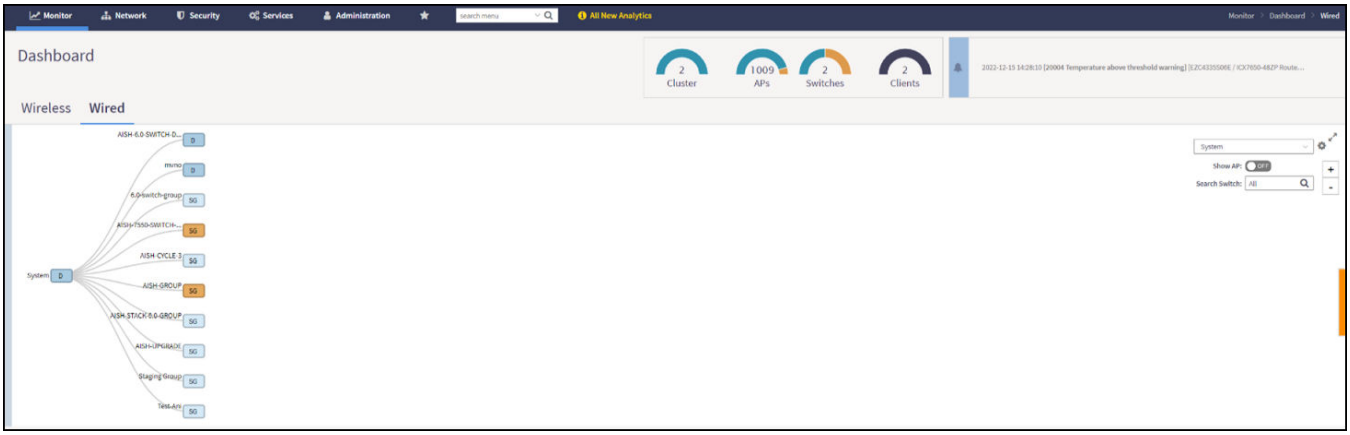


FIGURE 244 Showing Wired Devices Using Topology View Mode

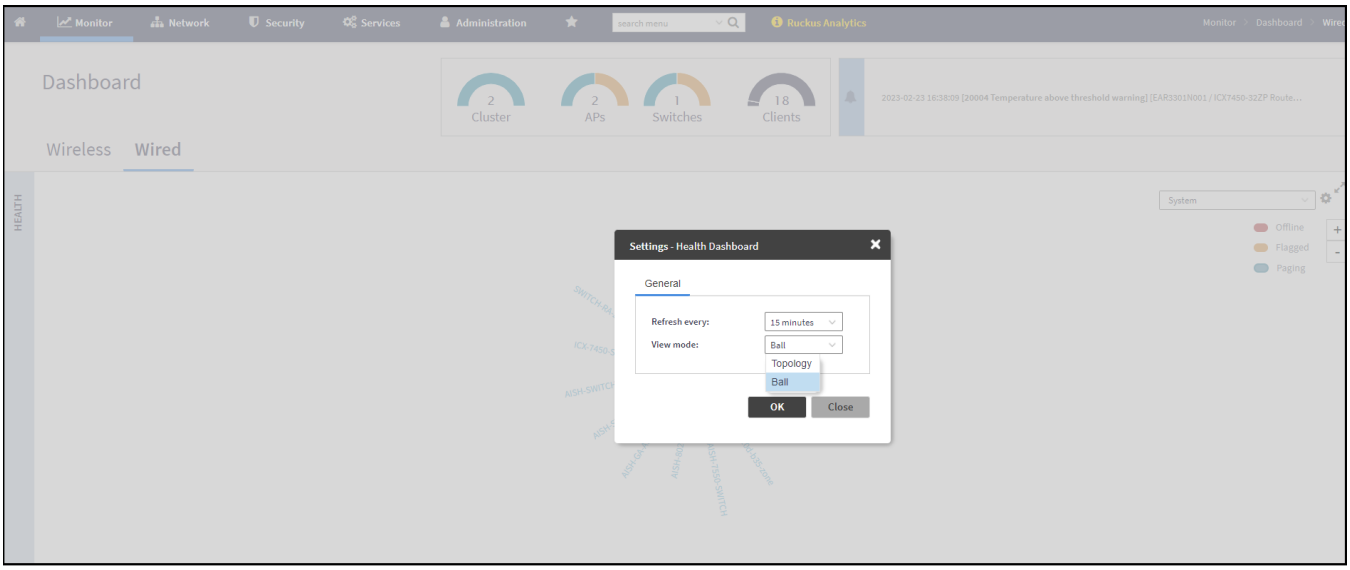
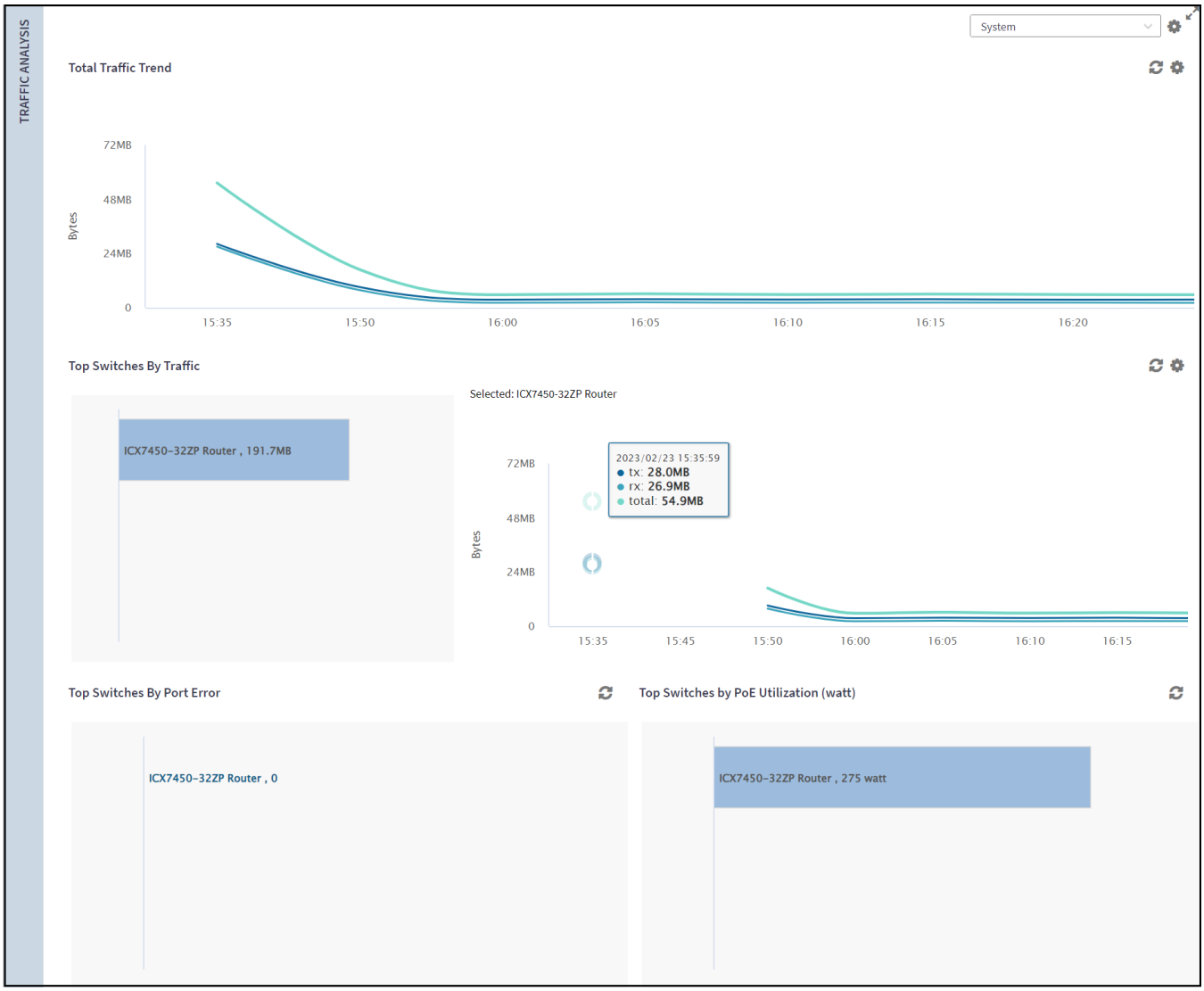


FIGURE 245 Viewing Traffic Analysis



The **Health** tab displays the number of switches that are online, offline, and flagged.

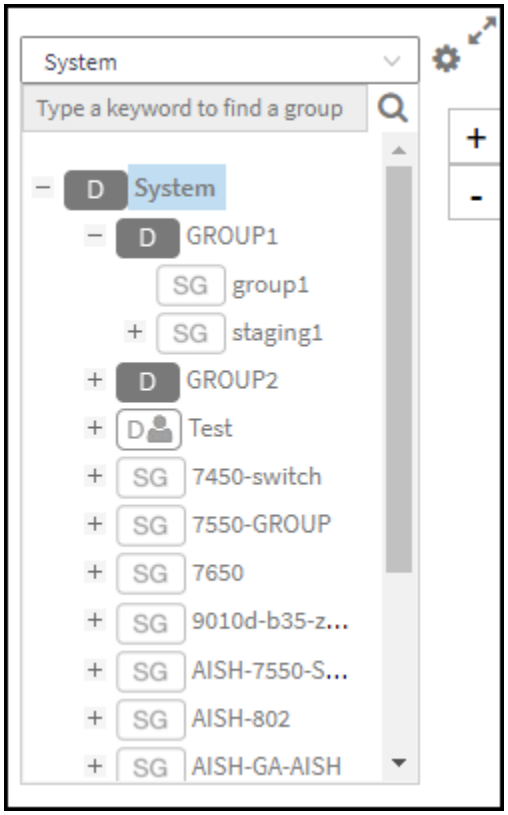
The **Traffic Analysis** tab displays the following information:

- Total Traffic Trend
- Top Switches By Traffic
- Top Switches By Port Error
- Top Switches by PoE Utilization (watt)

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. 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 246 Showing Elements on the Health Dashboard



Improving Switch Configuration Change Management

Starting with the 7.0 release, the controller automatically verifies the switch with a Master backup every hour for any configuration changes. If there is a configuration change from the controller GUI or the switch, the controller triggers a configuration backup for the switch. Subsequently, the controller displays a warning on the **Switches** page, notifying that the latest running configuration backup of the switch differs from the Master backup.

NOTE
In earlier releases, warnings for differing backups were issued after a day, which was inconvenient.

Perform the below steps to view the switch with Master backup for configuration changes.

1. From the main menu, go to **Network** > **Wired** > **Switches**.

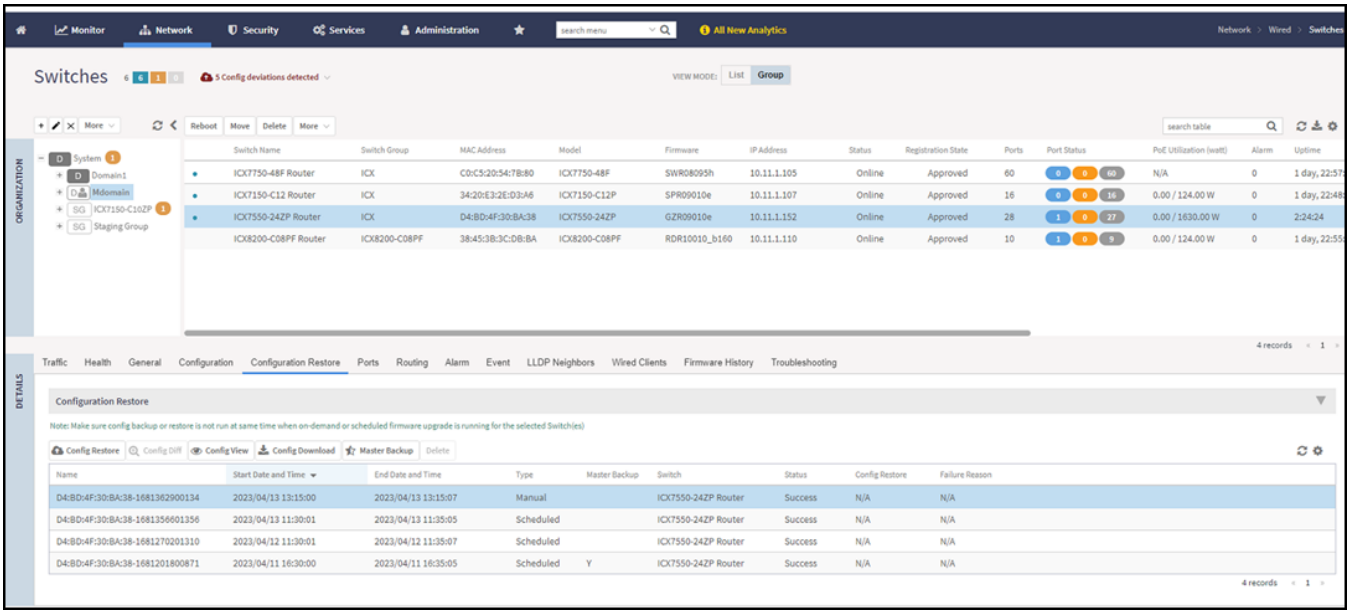
   The **Switches** page is displayed.

2. Select a Switch. Click the **Configuration Restore** tab.

   A list of backup configurations is displayed.

3. Set a specific configuration to be the Master by selecting a specific backup configuration and clicking the **Master Backup** button. A confirmation dialog box appears. Click **Yes**. The page refreshes, displaying a **Y** in the Master Backup column.

FIGURE 247 Viewing the Switch Master Backup Configuration



After a configuration has been selected as the Master Backup, any subsequent switch configuration changes will trigger the controller to automatically initiate a switch configuration backup.

Switch Clients

Switch Clients

The Switch Clients tab presents a summary of both wireless and wired switch clients.

From the dashboard, go to **Monitor** > **Clients** > **Switch Clients.** The **Switch Clients** page is displayed.

To view the switch clients associated with a particular switch group, select a switch group. The details of the switch client are shown on the right pane.

TABLE 63 Details of the 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.

TABLE 63 Details of the Switch Client (continued)

Column Name	Description
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.

350 West Java Dr., Sunnyvale, CA 94089 USA
https://www.commscope.com