CONFIGURATION GUIDE

RUCKUS SmartZone (LT-GD) WLAN Management Guide, 6.1.2

Supporting SmartZone Release 6.1.2

Part Number: 800-73526-001 Rev A
Publication Date: November 2023

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 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 **Open a Case** section.
- Priority 2 (P2)—High. Network or service is impacted, but not down. Business impact may be high. Workaround may be available. Go to the **Open a Case** section.
- Priority 3 (P3)—Medium. Network or service is moderately impacted, but most business remains functional. Go to the **Self-Service Resources** section.
- Priority 4 (P4)—Low. Requests for information, product documentation, or product enhancements. Go to the **Self-Service Resources** section.

Open a Case

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

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

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

Self-Service Resources

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

- Technical Documentation—https://support.ruckuswireless.com/documents
- Community Forums—https://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 TAC with additional data from your troubleshooting analysis if you still require assistance through a support case or RMA. If you still require help, open and manage your case at https://support.ruckuswireless.com/case_management.

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. You create a CommScope account and then register for, and request access for, CommScope University.

Document Conventions

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

TABLE 1 Text Conventions

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

Notes, Cautions, and Safety Warnings

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

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

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

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

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

Command Syntax Conventions

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

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

About This Guide

New in This Document

TABLE 2 Key Features and Enhancements in *SmartZone 6.1.2 Rev A* (*November 2023*)

Feature	Description	Reference
BSS_Priority	**Updated**: The **Priority** feature from the **Wireless Client Isolation** section is renamed as **BSS Priority** and is moved to the **Advanced Options** section for **WLAN Configuration**.	Creating a WLAN Configuration on page 17

Wireless Network

Domains, Zones, WLAN Groups, and WLANs

If your wireless network covers a large physical environment (for example, a multi-floor building or multi-building office) and you want to manage and provide different WLAN services to different areas of your environment, you can virtually split them using the following hierarchy:

- Domains: Geographical grouping for regulatory operation
- Zones: Comprised of multiple WLAN groups
- WLAN Groups: Comprised of multiple WLANs
- WLANs: Provide wireless network service

Viewing Modes

The **View Mode** on the upper-right corner of the page provides two options to view the WLANs available in the system:

- **List**—Displays the list of all WLANs irrespective of the Zone or Group they belong.
- **Group**—Displays the list of WLANs that belong to a specific Zone or Group.

The following WLAN details can be viewed regardless of the mode selected:

- **Name**
- **Alert**
- **SSID**
- **Auth Method**
- **Encryption Method**
- **Clients**
- **Traffic**
- **VLAN**
- **Application Recognition**
- **Tunneled**

Creating a WLAN Domain for an MSP

A Managed Services Provider (MSP) manages and assumes a defined set of responsibility. You can create an MSP managed domain, to manage all their settings within that domain.

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

Complete the following steps to create a WLAN Domain for an MSP:

1. From the **Network** > **Wireless** > **Wireless LANs** , select **System** from the tree hierarchy.
2. Click the **Create** button, the **Create Group** form is displayed.

3. Configure the following details:
   a) Enter a **Name** for the domain.
   b) Enter a **Description** about the domain.
   c) In **Managed by Partner**, select the **Enable** check box.

   By default, the **Type** selected is **Domain** and the **Parent Group** displays the group to which this domain will be tagged.
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.

When you 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 3 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
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 Single 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.

Complete the following steps to move a single WLAN from its current WLAN zone to a different zone:

1. From the main menu, go to **Network** > **Wireless** > **Wireless LANs**, and locate the WLAN zone that you want to move to a different WLAN zone.
2. Click **More** and select **Move**. The **Select Destination Management Domain** dialog box is displayed.
3. Select the destination WLAN zone and click **OK**.

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

   The WLAN is moved to the destination location.

Extracting a WLAN Template

You can extract only the WLAN-related configuration to a WLAN template.

Complete the following steps to extract a WLAN template.

1. From the main menu, go to **Network** > **Wireless** > **Wireless LANs**and locate the zone from where you want to extract the WLAN template.
2. Click **More** and select **Extract WLAN Template**. The **Extract WLAN Template** dialog box is displayed.
3. For **WLAN Template Name**, enter a name for the template.
4. Click **OK**. A message is displayed stating that the WLAN template was extracted successfully.
5. Click **OK**.

   The extracted WLAN template can be viewed at **System** > **Templates** > **WLAN Templates**.

Applying a WLAN Template

You can apply only the WLAN-related configuration to an AP zone using a WLAN template. You can apply the WLAN template to zones where the AP's firmware version is later than the Zone templates firmware version. An unsupported firmware version of the WLAN template is automatically upgraded to its next version before being upgraded to the current version.

Complete the following steps to apply a WLAN template.

1. From the main menu, go to **Network** > **Wireless** > **Wireless LANs** and locate the zone from where you want to extract the WLAN template.
2. Click **More** and select **Apply WLAN Template**, The **Apply WLAN Template** dialog box is displayed.
3. From the **Select a WLAN template** list, select the template.
4. Click **Next**. The **Apply WLAN template to selected zone** dialog box is displayed.
5. Complete the required options:
   - Create all WLANs and WLAN profiles from the template if they do not already exist in the target zones.
   - If the target zones have a WLAN or WLAN profile with the same name as the template, overwrite the current settings with settings from the template.
   - Click **OK**. A confirmation dialog box is displayed.
6. Click **OK**.

Changing the AP's Firmware

Each firmware version has its own set of functionality, security, and performance. Selecting a particular firmware version enable access to resources specific to that firmware.

Complete the following steps to change the AP's firmware.

1. From the main menu, go to **Network** > **Wireless** > **Wireless LANs**and locate the zone from where you want to change the AP firmware.
2. Click **More** and select **Change AP Firmware**.
3. Choose the AP firmware that you want to change.

Configuring Cluster Switchover

Cluster switchover is moving the APs between clusters.

Complete the following steps to choose the APs to switch over a cluster.

1. From the main menu, go to **Network** > **Wireless** > **Access Points**and locate the zone that you want to switch.
2. Click **More** and select **Switch Over Clusters**. The **Switch Over Clusters** dialog box is displayed.
3. For **Switch Over Clusters**, enter the IP address or the FQDN of the new controller.
4. Click **OK**. A message stating the APs are moved to the new cluster is displayed .
5. Click **OK**.

   The AP can be viewed in the new controller under the default zone.

Triggering a Preferred Node

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

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

Complete the following steps to trigger a preferred node.

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

1. From the main menu, go to **Network** > **Wireless** > **Wireless LANs** and locate zone.
2. Click **More** and select **Trigger Preferred Node**. A confirmation dialog box is displayed.
3. Click **OK**.

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-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 17.

     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

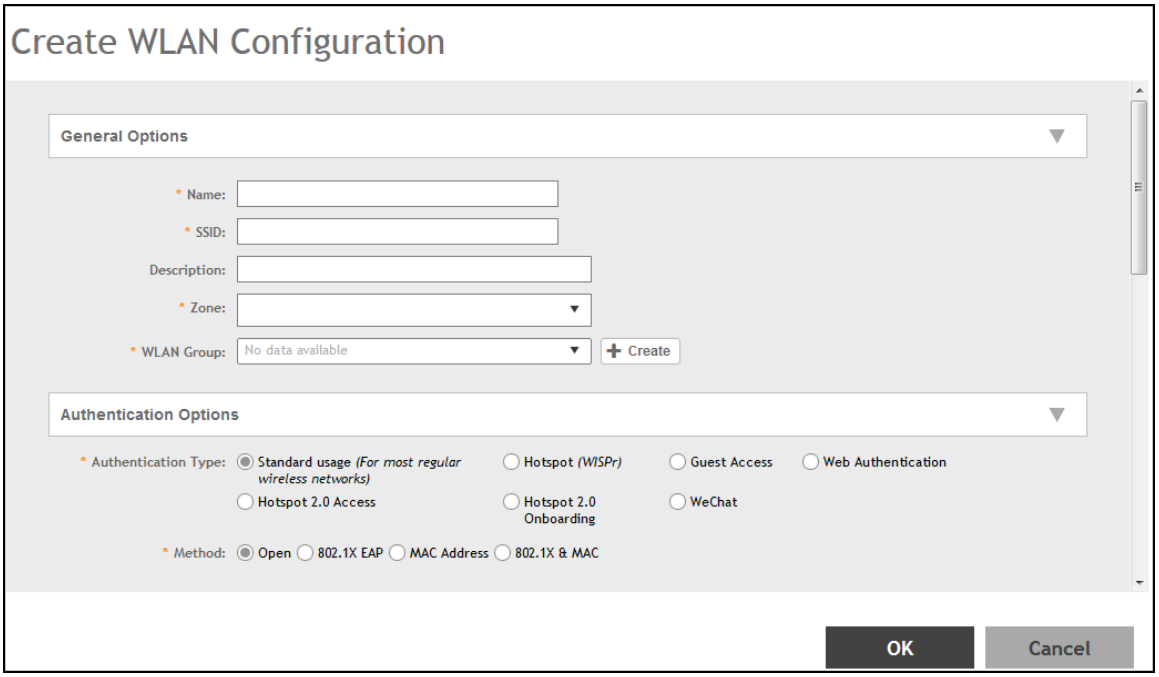
Creating a WLAN Configuration

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 1 Create WLAN Configuration Page



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

TABLE 4 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.

TABLE 4 WLAN Configuration for SZ100 and vSZ-E (continued)

Field	Description	Your Action
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		
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. • **WeChat**—Click this option if you want the WLAN usage through WeChat.

TABLE 4 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 4 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 passess, 802.1x EAP authentication is processed. After the two authentication methods succeed, the user equipment gains access to the WLAN. Authentication is handled by a back-end RADIUS server. When this authentication method is selected, the **MAC Authentication** and **MAC Address Format** fields will be shown within the **Authentication Options** section.
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 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 4 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. Choose the **Algorithm** – **AES**: a. Enter **Passphrase** b. Enter **SAE Passphrase** c. Select or clear **Show** d. In the **802.11w MFP** field, **Capable** is the default selected option • **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. • **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**

TABLE 4 WLAN Configuration for SZ100 and vSZ-E (continued)

Field	Description	Your Action
		• **WEP-64 (40 bits)**—Provides a lower level of encryption, and is less secure, using 40-bit WEP encryption. a. Choose the **WEP Key**. b. Enter **HEX** value. • **WEP-128 (104 bits)**—Provides a higher level of encryption than WEP-64, using a 104-bit key for WEP encryption. However, WEP is inherently less secure than WPA. a. Choose the **WEP Key**. b. Enter **HEX** value. • **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 WPAmixed 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**
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. b. Select the server from the menu. c. Select the **Enable RFC Location Delivery Support.**.

TABLE 4 WLAN Configuration for SZ100 and vSZ-E (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 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.
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.

TABLE 4 WLAN Configuration for SZ100 and vSZ-E (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 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.
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		

TABLE 4 WLAN Configuration for SZ100 and vSZ-E (continued)

Field	Description	Your Action
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 approriate: • **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**.

TABLE 4 WLAN Configuration for SZ100 and vSZ-E (continued)

Field	Description	Your Action
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**
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.

TABLE 4 WLAN Configuration for SZ100 and vSZ-E (continued)

Field	Description	Your Action
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.
Advanced Options		
BSS Priority	Determines high versus low transmit preference of one WLAN compared to another. Traffic for high priority WLANs is always sent before low priority WLANs in the same QoS category (background, best effort, video, voice).	Choose the priority: • **High** • **Low**
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**.

TABLE 4 WLAN Configuration for SZ100 and vSZ-E (continued)

Field	Description	Your Action
Hotspot 2.0 Onboarding	Allows devices to connect to a Wi-Fi network automatically, wherein the service providers engage in roaming partnerships to provide seamless access to Wi-Fi networks. The devices are authenticated using credentials or certificates.	Select the check box to allow Hotspot 2.0 onboaring for the WISPr WLAN.
Hide SSID	Removes the SSID from Beacon frames. By removing the SSID, in most cases, clients will not show this SSID in their scan list unless the device is already configured to connect. This can simplify the network decision for an end user.	Select the check box.
Client Load Balancing	Disables client load balancing on this WLAN if the option is selected.	Select the check box to disable client load balancing on this WLAN.
Proxy ARP	Enables proxy ARP. When proxy ARP is enabled on a WLAN, the AP provides 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.
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.

TABLE 4 WLAN Configuration for SZ100 and vSZ-E (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 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.
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.

TABLE 4 WLAN Configuration for SZ100 and vSZ-E (continued)

Field	Description	Your Action
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 4 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	Allows legacy Wi-Fi 5 clients with outdated drivers to interoperate with a Wi-Fi 6 AP. Disable Wi-Fi 6, if the client drivers on the network are not the latest or are free of bugs. Wi-Fi 6 clients connecting to a WLAN with Wi-Fi 6 disabled on a Wi-Fi 6 AP will not be able to use Wi-Fi 6 features such as the OFDMA and TWT. **NOTE** Wifi 6 feature is supported for the firmware release 5.2.1 and above.	Select the option.
OFDM Only	Disconnects 802.11b devices from the WLAN and all devices are forced to use higher data rates for more efficient airtime usage. This setting only affects the 2.4-GHz radio. OFDM is used by 802.11a, g, n, and ac, but is not supported by 802.11b.	Select the 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

TABLE 4 WLAN Configuration for SZ100 and vSZ-E (continued)

Field	Description	Your Action
6G Mgmt Tx Rate	Sets the transmit rate for management frame types such as beacon and probes.	Select one of the following option: • 6 mbps • 9 mbps • 12 mbps • 18 mbps • 24 mbps
Service Schedule	Controls when the WLAN service is active. The purpose of this setting is to automatically enable or disable a WLAN based on a predetermined schedule. By default, the service is **Always On**. **Always Off** can be 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.
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.

TABLE 4 WLAN Configuration for SZ100 and vSZ-E (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 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.
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", "youtube", "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.

TABLE 4 WLAN Configuration for SZ100 and vSZ-E (continued)

Field	Description	Your Action
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.
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.

TABLE 5 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.

TABLE 5 WLAN Configuration for SZ300 and vSZ-H (continued)

Field	Description	Your Action
Authentication Options		
Authentication Type	Defines the type of authentication flow for the WLAN. **NOTE** Authentication types such as WeChat, Web Authentication, and Guest Access are not supported by APs in IPv6 mode.	Select the required option: • **Standard Usage**—This is a regular WLAN suitable for most wireless networks. • **Hotspot (WISPr)**—Click this option if want to use a hotspot service (use this type for external captive portal workflows) or WISPr. **NOTE** Hotspot (WISPr) applies to WLAN traffic that is tunneled and not tunneled. • **Guest Access**—Click this option if you want guest users to use this WLAN. After you complete creating this WLAN for guest access, you can start generating guest passes. For more information about Hotspot 2.0 online signup, see the Hotspot 2.0 Reference Guide for this release. • **Web Authentication**—Click this option if you want to require all WLAN users to complete a web-based logon to this network every time they attempt to connect. • **Hotspot 2.0 Access**—Click this option if you want a Hotspot 2.0 operator profile that you previously created to use this WLAN. See the Hotspot 2.0 Reference Guide for this release. **NOTE** You can select 8021.X EAP + “WPA3” or “WPA2/WPA3-Mixed” for HS2.0 access wlan to add more security. • **Hotspot 2.0 Onboarding**—Click this option if you want to use this WLAN for Hotspot 2.0 onboarding. See the Hotspot 2.0 Reference Guide for this release for more information. Hotspot 2.0 onboarding allows for Open and 802.1x EAP authentication methods. • **WeChat**—Click this option if you want the WLAN usage through WeChat.

TABLE 5 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 passess, 802.1x EAP authentication is processed. After the two authentication methods succeed, the user equipment gains access to the WLAN. Authentication is handled by a back-end RADIUS server. When this authentication method is selected, the MAC Authentication and MAC Address Format fields will be shown within the Authentication Options section.
Encryption Options		

TABLE 5 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.	Select the option: • **WPA2**—Enhanced WPA encryption using AES encryption algorithm. a. Choose **Algorithm**: – **AES**: 1. Enter **Passphrase**. 2. Select or clear **Show**. 3. Select › the **Enable 802.11 Fast BSS Transition** check box and enter the **Mobility Domain ID**. › the required **802.11w MFP** option. 4. **Dynamic PSK** › **Disable** › **Internal** a. Enter **DPSK Length** b. Choose **DPSK Type** c. Select **DPSK Expiration** › **External**—Enables **Authentication Service** – **AUTO**: 1. Enter **Passphrase**. 2. Select or clear **Show**. • **WPA3**—Enhanced WPA3 encryption using AES encryption algorithm. a. Choose **Algorithm**: – **AES**: 1. Enter **Passphrase**. 2. Select or clear **Show**. 3. In the **802.11w MFP** field, " Required" is the default selected option. – **AES-GCMP-256**: › **NOTE** WPA3-Enterprise cannot be supported by the 802.11ac Wave-1 AP models. • **WPA2/WPA3-Mixed** Encryption - Allows mixed networks of WPA2- and WPA3-compliant devices using AES algorithm. a. 1. Choose **Algorithm**: – **AES**: a. Enter **Passphrase**. b. Enter **SAE Passphrase** c. Select or clear **Show**. d. In the **802.11w MFP** field, " Capable" is the default selected option b. Choose **Algorithm**: – **AES**: 1. Enter **Passphrase**. 2. Enter **SAE Passphrase** 3. Select or clear **Show**.

TABLE 5 WLAN Configuration for SZ300 and vSZ-H (continued)

Field	Description	Your Action
		• **Opportunistic Wireless Encryption 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** • **WEP-64 (40 bits)**—Provides a lower level of encryption, and is less secure, using 40-bit WEP encryption. a. Choose the **WEP Key**. b. Enter **HEX** value. • **WEP-128 (104 bits)**—Provides a higher level of encryption than WEP-64, using a 104-bit key for WEP encryption. However, WEP is inherently less secure than WPA. a. Choose the **WEP Key**. b. Enter **HEX** value. • **None**
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		

TABLE 5 WLAN Configuration for SZ300 and vSZ-H (continued)

Field	Description	Your Action
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 comtroller 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. b. Select the server from the menu. c. Select **Enable RFC Location Delivery Support**.
Accounting Server	Specifies the server used for accounting messages. By enabling Proxy, accounting messages are sent by the controller. In a non-proxy mode, the AP will communicate accounting messages directly.	a. Select the **Use controller as proxy** check box. b. Select the server from the menu.
Hotspot Portal (for WLAN **Authentication Type**: **Hotspot (WisPr)**)		
Hotspot (WISPr) Portal	Defines hotspot behavior such as redirects, session timers, and location information among others.	Select the hotspot portal profile that you want this WLAN to use.
Bypass CNA	Bypasses the Apple CNA feature on iOS and OS X devices that connect to this WLAN.	Select the **Enable** check box.

TABLE 5 WLAN Configuration for SZ300 and vSZ-H (continued)

Field	Description	Your Action
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.
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.

TABLE 5 WLAN Configuration for SZ300 and vSZ-H (continued)

Field	Description	Your Action
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		
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 approriate: • **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.

TABLE 5 WLAN Configuration for SZ300 and vSZ-H (continued)

Field	Description	Your Action
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**
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**

TABLE 5 WLAN Configuration for SZ300 and vSZ-H (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	Enables DPI-based Layer 7 application recognition, and if enabled, an application control policy. Recognition and control are performed on the AP.	Select the option.
Client Virtual ID Extraction	Extracts the Virtual IDs of the users who login into the social media , public email such as wechat, whatsapp, hotmail, and cloud disk, and send these virtual ids to the auditing system.	**NOTE** To enable the Client Virtual ID Extraction, enable Application Recognition Control, and ensure that Sigpack contains regular version.
URL Filtering	Enables URL filtering on the WLAN controller to block or allow access to specific websites or web pages.	Select the option.
Advanced Options		
BSS Priority	Determines high versus low transmit preference of one WLAN compared to another. Traffic for high priority WLANs is always sent before low priority WLANs in the same QoS category (background, best effort, video, voice).	Choose the priority: • **High** • **Low**

TABLE 5 WLAN Configuration for SZ300 and vSZ-H (continued)

Field	Description	Your Action
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 Onboaring for the WISPr WLAN.
Hide SSID	Removes the SSID from beacon frames. By removing the SSID, in most cases, clients will not show this SSID in their scan list unless the device is already configured to connect. This can simplify the network decision for an end user.	Select the check box.
Client Load Balancing	Disables client load balancing on this WLAN if the option is selected.	Select the check box to disable client load balancing on this WLAN.
Proxy ARP	Enables proxy ARP. When proxy ARP is enabled on a WLAN, the AP provides ARP response service for stations. When the AP receives an ARP request for a known host, it replies with an ARP response on behalf of the host. If the AP receives a request for an unknown host, it forwards the request.	Select the check box.
DGAF	Disables AP from forwarding downstream group-addressed frames. This option is available only when proxy ARP is enabled.	Select the option.
ND Proxy	Enables Neighbor Discovery proxy. When ND proxy is enabled on a WLAN, the AP provides Neighbor Advertisement service for stations. When the AP receives a Neighbor solicitation request for a known host, it replies with a Neighbor Advertisement on behalf of the host. If the AP receives a request for an unknown host, it forwards the request. **NOTE** This feature is available only on IPv6 and Dual zone and is enabled by default.	Enable the option.

TABLE 5 WLAN Configuration for SZ300 and vSZ-H (continued)

Field	Description	Your Action
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.
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.

TABLE 5 WLAN Configuration for SZ300 and vSZ-H (continued)

Field	Description	Your Action
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.
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.

TABLE 5 WLAN Configuration for SZ300 and vSZ-H (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 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.
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.

TABLE 5 WLAN Configuration for SZ300 and vSZ-H (continued)

Field	Description	Your Action
Directed MC/BC Threshold	Defines the per-radio-client count at which an AP stops converting group-addressed data traffic to unicast. However, the Directed Threshold logic is only one part of the access points' multicast handling logic, which means there may be other factors that determine whether a frame is transmitted as unicast or multicast. APs support a feature called Directed Multicast (configurable only on AP CLI, enabled by default), which adds additional logic to the multicast flow. If Directed Multicast is disabled, the AP uses the Directed Threshold as the only criteria to determine whether to transmit a multicast packet as unicast. However, when Directed Multicast is enabled, the flow is changed. Directed Multicast is a feature that checks to see if a multicast packet is well-known or not. For well-known multicast packets, for example, Bonjour, uPNP, most IPv6 link- and node-local, and Spectralink, the AP still applies the Directed Threshold logic to determine conversion to unicast. For non well-known types, the AP monitors and maintains a database of client subscriptions using IGMP and MLD. If associated clients are subscribed to the multicast stream, then the AP always converts these packets to unicast, regardless of the Directed Threshold configuration. If there are no clients subscribed to the multicast stream, the AP drops these packets. It is important to be aware of this behavior when validating multicast operation in a deployment.	Enter the client count number. Range: 0 through 128.
Client Tx/Rx Statistics	Stops the controller from monitoring traffic statistics for unauthorized clients.	Select the check box.
User Session Timeout	Indicates the duration after which idle clients will be disconnected. **NOTE** Before getting disconnected the client can be either in an idle state or connected to the WLAN (SSID).	Enter the duration. Range: 120 to 864000 seconds (10 days). Default Value: 172800 seconds (2 days). **NOTE** This default value will remain effected only when the session timeout is not applied from the Radius server. **NOTE** The user session timeout is displayed only for those WLANs in which 802.1X or MAC authentication is enabled.

TABLE 5 WLAN Configuration for SZ300 and vSZ-H (continued)

Field	Description	Your Action
User Session Timeout	Indicates the duration after which the client gets disconnected. **NOTE** Before getting disconnected the client can be either in an idle state or connected to the WLAN.	Enter the duration. Range: 120 to 864000 seconds (10 days). Default Value: 172800 seconds (2 days). **NOTE** This default value will remain effected only when the session timeout is not applied from the Radius server.
WiFi 6	Allows legacy Wi-Fi 5 clients with outdated drivers to interoperate with a Wi-Fi 6 AP. Use this option to disable Wi-Fi 6 if the client drivers on the network are not the latest or are free of bugs. Wi-Fi 6 clients connecting to a WLAN with Wi-Fi 6 disabled on a Wi-Fi 6 AP will not be able to use Wi-Fi 6 features such as the OFDMA and TWT. **NOTE** Wifi 6 feature is supported for the firmware release 5.2.1 and above.	Select the option.
OFDM Only	Disconnects 802.11b devices from the WLAN and all devices are forced to use higher data rates for more efficient airtime usage. This setting only affects the 2.4-GHz radio. OFDM is used by 802.11a, g, n, and ac, but is not supported by 802.11b.	Select the check box.
BSS Min Rate	Forces client devices to be both closer to the AP and to use higher, more efficient rates when you increase the BSS minimum rate above the default (all rates) setting. The BSS minimum rate is the lowest data rate supported on the WLAN. When OFDM-only is enabled, it takes higher priority than BSS minimum rate settings.	Select the option.
Mgmt Tx Rate	Sets the transmit rate for management frame types such as beacon and probes.	Select the value.
6G BSS Min Rate	Forces client devices to both be closer to the AP and to use higher, more efficient rates when you increase the BSS minimum rate above the default (all rates) setting. The BSS minimum rate is the lowest data rate supported on the WLAN. When OFDM-only is enabled, it takes higher priority than BSS minimum rate settings.	Select one of the following option: • 6 mbps • 9 mbps • 12 mbps • 18 mbps • 24 mbps

TABLE 5 WLAN Configuration for SZ300 and vSZ-H (continued)

Field	Description	Your Action
6G Mgmt Tx Rate	Sets the transmit rate for management frame types such as beacon and probes.	Select one of the following option: • 6 mbps • 9 mbps • 12 mbps • 18 mbps • 24 mbps
Service Schedule	Controls when the WLAN service is active. The purpose of this setting is to automatically enable or disable a WLAN based on a predetermined schedule. By default, the service is **Always On**. **Always Off** can be selected in order to create a WLAN and apply it, but prevent it from advertising until ready. The **Specific** setting allows a configurable schedule based on time of day and days of the week. **NOTE** When a service schedule is created, it is saved by the 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 5 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%, .i.e. 3.00Mbps to 4.00Mbps max per second traffic passes. This limit is only for downlink and shall not be affected by BSS Min Rate setting. **NOTE** SSID Rate Limit always take precedence, if, Mutlicast Rate Limit is also configured.	Select the **Uplink** and **Downlink** check boxes and enter the limiting rates in Mbps, respectively. Range: 1 through 100 Mbps. **NOTE** Multicast Rate Limit value cannot exceed SSID Rate Limit values for respective **Uplink** and **Downlink** direction.
DNS Server Profile	Allows the AP to inspect DHCP messages and overwrite the DNS servers with the DNS server configured in this profile. This allows for policy-based DNS application in which unique users/roles should use a different DNS server than others.	Select a profile from the menu. Select **Disable** from the menu if you want to disable the DNS Server profile for the WLAN service. Click  to add a new profile or click  to edit a profile.
DNS Spoofing Profile	When an AP receives a DNS packet, all the fields in the packet are validated. **NOTE** Only A/AAA server DNS query packets are considered. When same domain name is present in both DNS spoofing profile and walled garden table in the WISPr WLAN, then the AP DNS cache is updated with the IP address present in the DNS spoofing profile. If DNS spoofing and URL filtering with safe search is enabled, URLfiltering (safe search) takes precedence for the Google, YouTube, and Bing domain names. If safe search is not enabled, DNS spoofing takes the precedence. If safe search is not enabled and URL filtering is enabled also DNS-Spoof takes the precedence.	Select a profile from the menu. Select **Disable** from the menu if you want to disable the DNS Spoofing profile for the WLAN service. Click  to add a new profile or click  to edit a profile

TABLE 5 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.

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.

802.11r Fast BSS Transition

802.11r Fast BSS Transition is a fast roaming protocol that reduces the number of frame exchanges required for roaming and allows the clients and APs to reuse the master keys obtained during a prior authentication exchange. 802.11r is most helpful for 802.1X networks. Client support is required for 802.11r to work.

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.

802.11w Management Frame Protection

802.11w Management Frame Protection(MFP) provides additional security measures for management frames. Not all client devices support 802.11w.

Check your client devices before enabling 11w. If “Required” is selected in the client device", clients must support 11w in order to connect. If “Capable” is selected, clients with or without 11w should be able to connect. However, note that some clients with poor driver software may have connection problems even if 11w is set to "Capable".

Multiple Basic Service Set Identifier (MBSSID)

Multiple BSSID is by default enabled on 6GHz radio.

Typically an access point uses one beacon for advertising a BSSID. MBSSID reduces this overhead of the AP by integrating multiple beacons into one beacon. MBSSID reduces the overhead.

The rule for Multi BSSID is a user must assign BSSIDs from a sufficiently large set of MAC addresses so that each assigned BSSID is unique and each of them must have the same 48 - n msbs for all 2n BSSID group.

The Multiple BSSID capability enables the advertisement of information for BSSIDs using a single beacon or probe response frame instead of multiple beacon and probe response frame.

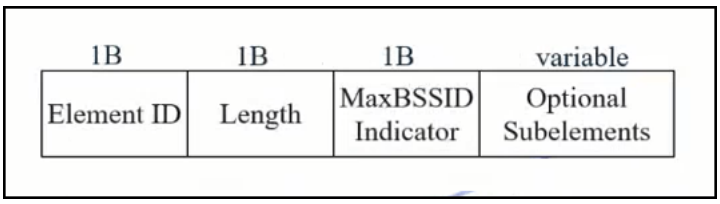
A 32 bit bitmask, the lower 16 bits of which specifies the pdevs for which the feature needs to enabled.

Bit corresponding to 6GHz radio is reserved as MBSSID is mandatory for 6GHz.

A MBSSID set is characterized as follows -

- All members of the set use a common operating class, channel, channel access functions, and antenna connnector.
- MaxBSSID indicator contains n, with 2n maximum number of BSSIDs in the set.
- Members of the set have the same 47-n MSBs in there BSSIDs.

FIGURE 2 Multi BSSID



Multiple BSSID Configuration

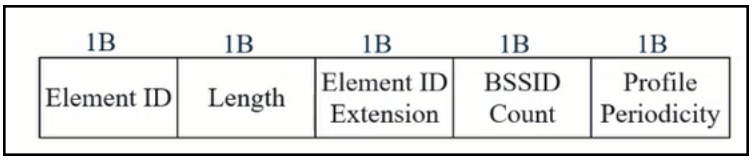
Multiple BSSID configuration element.

- Element ID - 255
- Element ID extension - 55
- BSSID count - Carries the total number of active BSSIDs in the MBSSID set.
- Profile periodicity - Indicates the least number of beacon frames a STA needs to receive in order to discover all the active non transmitted BSSIDs in the set.

Ext Tag: Multiple BSSID Configuration

```
Tag number: Element ID Extension (255)
Ext Tag length: 3
Ext Tag number: Multiple BSSID Configuration (55)
BSSID count: 16
Profile Periodicity: 3
```

FIGURE 3 Multiple BSSID Configuration



Enhanced Multi-BSSID Advertisement (EMA)

Due to the beacon size limitation, RUCKUS supports a maximum of 6 SSIDs per MBSSID beacon in a primary group. Out of which 5 SSIDs are used for user configured WLANs and the first SSID (RKS_TX_VAP) is reserved for TxVAP. This RKS_TX_VAP is created when a user brings up the first WLAN. The RKS_TX_VAP is pulled down, if the user brings down all the remaining WLANs in the 6GHz.

If mesh WLAN is enabled, secondary group contains MBSSID beacon.

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. This feature controls the RSSI threshold setting for Transient Client Management. Because Airtime Decongestion controls the **RSSI threshold** setting for Transient Client Management, when enabled, it disables the RSSI threshold configuration in **Transient Client Management**.

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

Client Load Balancing

Enabling load balancing can improve WLAN performance by helping to spread the wireless client load between nearby access points, so that one AP does not get overloaded while another sits idle.

Load balancing can be controlled from within the controller web interface to balance the number of clients per radio on adjacent APs.

Adjacent APs are determined by the controller at startup by measuring the RSSI during channel scans. After startup, the controller uses subsequent scans to update the list of adjacent APs periodically and when a new AP sends its first scan report. When an AP leaves, the controller immediately updates the list of adjacent APs and refreshes the client limits at each affected AP.

Once the controller is aware of which APs are adjacent to each other, it begins managing the client load by sending the configured client limits to the APs. These limits are soft values that can be exceeded in several scenarios, including:

- When a client signal is so weak that it may not be able to support a link with another AP
- When a client signal is so strong that it really belongs on this AP.

The APs maintain these configured client limits and enforce them once they reach the limits by withholding probe responses and authentication responses on any radio that has reached its limit.

NOTE
Adaptive Client Load Balancing (ACLB) is not supported on AP R730 in SmartZone 5.1.1 release. The R730 AP supports only legacy client load balancing (CLB). The R730 AP is supported only in SZ6.1.0 firmware zone. ACLB is disabled by default if capacity mode is configured on the controller. If station mode is configured, ACLB acts as legacy CLB on the AP.

Client Load Balancing Considerations

Before you enable load balancing, keep the following considerations in mind:

- The load balancing rules apply only to client devices; the AP always responds to another AP that is attempting to set up or maintain a mesh network.
- Load balancing does not disassociate clients already connected.
- Load balancing takes action before a client association request, reducing the chance of client misbehavior.
- Load balancing does not require any time-critical interaction between APs and the controller.
- Provides control of adjacent AP distance with safeguards against abandoning clients.

- Load balancing can be disabled on a per-WLAN basis. For instance, on a voice WLAN, load balancing may not be desired due to voice roaming considerations.
- Background scanning must be enabled on the WLAN for load balancing to work.

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.

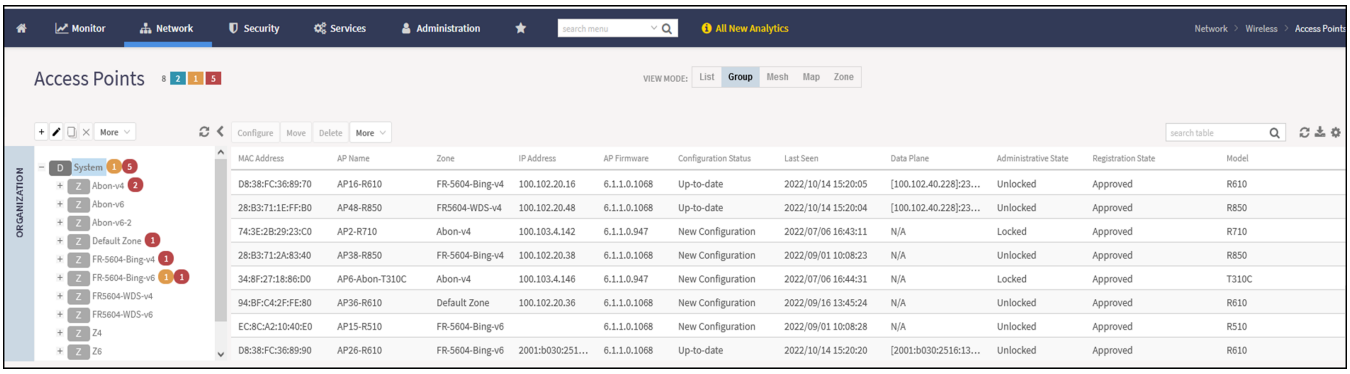
Creating an AP Zone

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

To create an AP zone, complete the following steps.

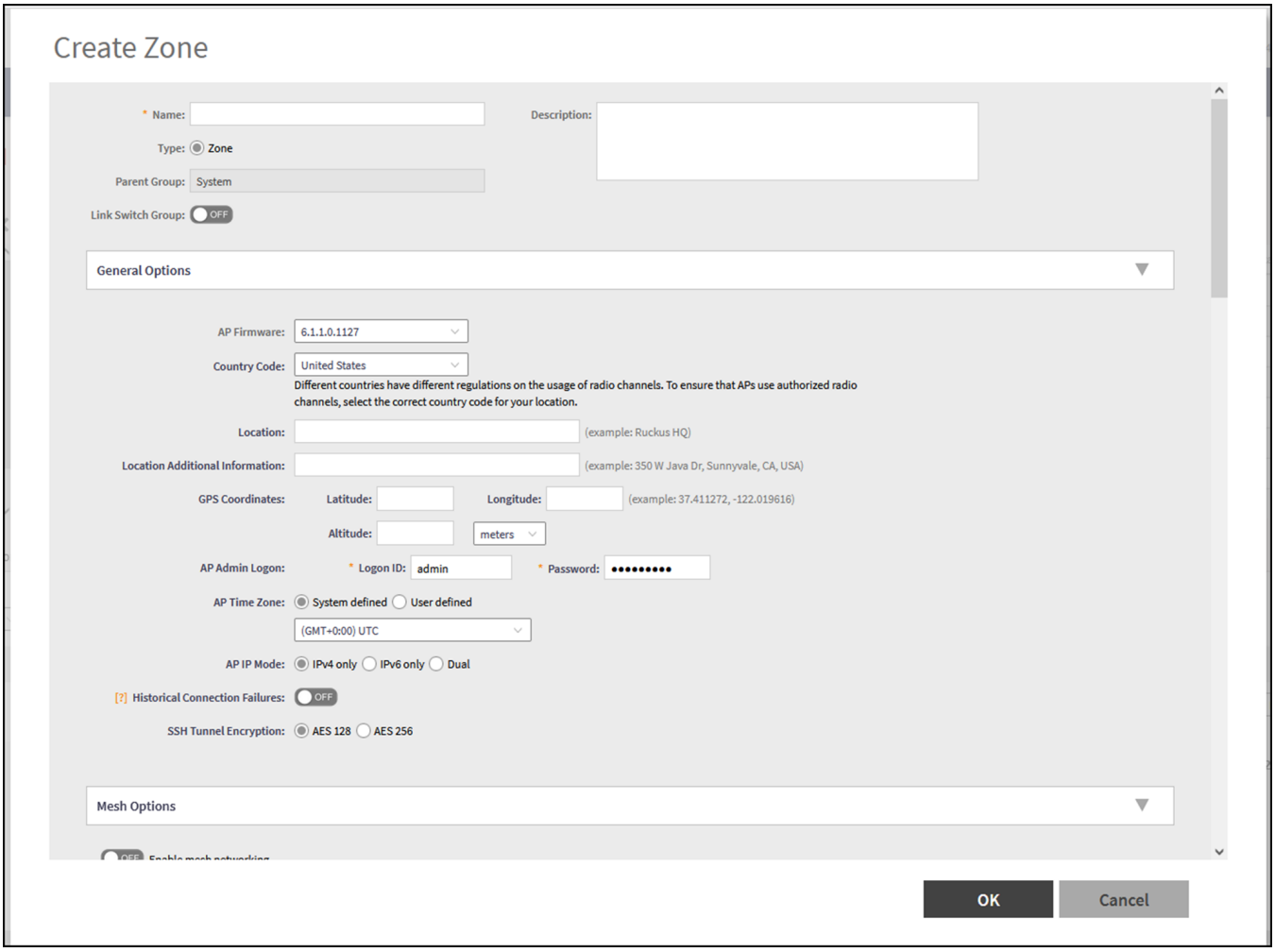
1. On the menu, click **Network** > **Wireless** > **Access Point**.

FIGURE 4 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 5 Create Zone Page



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

TABLE 6 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 6 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.
Configuration > General Options		
AP Firmware	Indicates the firmware to which it applies.	Select the firmware.
Country Code	Indicates the country code. Using the correct country code helps ensure that APs use only authorized radio channels.	Select the country code.
Location	Indicates the generic location.	Enter the location.
Location Additional Information	Indicates detailed location.	Enter additional location information.
GPS Coordinates	Indicates the geographical location.	Enter the following coordinates: • **Longitude** • **Latitude** • **Altitude**
AP Admin Logon	Indicates the administrator logon credentials.	Enter the **Logon ID** and **Password**.
AP Time Zone	Indicates the time zone that applies.	Select a time zone, and enter the details as required.
AP IP Mode	Indicates the IP version that applies.	Select the IP version. IPv6, IPv4, and dual addressing modes are supported.
Historical Connection Failures	Allows the zone APs to report client connection failures so that the administrator can view past connection problems from the Troubleshooting menu. **NOTE** For enterprise profile (vSZ-E) is 5 days, for carrier profile (vSZ-H) is 3 days.	Click the button.
DP Group	Specifies the group for the zone. **NOTE** This option is supported only on vSZ-H.	Select the DP group from the list.
SSH Tunnel Encryption	Specifies the encryption that reduces the load on controller control of SSH traffic.	Select the required option: • **AES 128** • **AES 256**
Cluster Redundancy	Provides cluster redundancy option for the zone. **NOTE** Cluster redundancy is supported only on SZ300 and vSZ-H.	Select the required option: • **Zone Enable** • **Zone Disable**
Configuration > Mesh Options		

TABLE 6 AP Zone Details for SZ300 and vSZ-H platforms (continued)

Field	Description	Your Action
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.
Configuration > **Radio Options**		
Dual-5G Mode	Enables third radio operator in 2.4 GHz, Lower 5 GHz, and Upper 5 GHz. By default, the **Dual-5G Mode** is enabled. In the enabled mode, radio-0 will be on 2.4GHz band, radio-1 will be on 5G Lower band and radio-2 will be on 5G Upper band. • 5G Lower BAND : UNII-1, UNII-2A • 5G Upper BAND : UNII-2C, UNII-3 In the disabled mode, the radio-0 will be on 2.4GHz band, radio-1 will be on 5G band and radio-2 will be on 6G band. This also depends on the country code.	Select or keep the default **Dual-5G Mode** option.
Configuration > **Band/Spectrum Configuration** > **2.4 GHz**		
Channelization	Indicates the channel width.	Set the channel width used during transmission to either 20 or 40 (MHz), or select Auto to set it automatically.
Channel	Indicates the channel to use.	Select one of the options: Auto, 1, 6 or 11.
Auto Cell Sizing	Enables the AP to share information on interference seen by each other and dynamically adjust their radio Tx power and Rx parameters to minimize interference. Enabling this option disables the TX Power Adjustment configuration. **NOTE** Ensure that Background Scan is enabled.	Select the option.

TABLE 6 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 2.4 GHz radio. By default, the TX power is set to Full on the 2.4 GHz radio. **NOTE** If you choose Min, the transmit power is set to 0dBm (1mW) per chain for 11n APs, and 2dBm per chain for 11ac APs. If you choose Max, the transmit power is set to the maximum allowable value according to the AP's capability and the operating country's regulations.	Select the preferred TX power.
Protection Mode	Indicates the mechanism to reduce frame collision.	Choose one of the following options: • None • RTS/CTS • CTS Only
Background Scan	Allows the AP radio to scan other channels in the band for accessing channel health and capacity, detecting rogue devices, optimizing and mainting mesh links and to discover AP neighbors.	Enter the duration in seconds. Range: 1 through 65535.
Auto Channel Selection	Automatically adjusts the channel using the ChannelFly option.	Select the required option. For **ChannelFly**, set the **Channel Change Frequency** and **Full Optimization Period**.
Configuration > **Band/Spectrum Configuration** > **5 GHz**		
Channelization	Indicates the channel width.	Set the channel width used during transmission: Auto, 20, 40, 80 and 160.
Channel	Indicates the channel to use.	Select the required options for the Indoor and Outdoor APs.
Secondary Channel	Indicates the secondary channel to used.	By default, the Indoor and Outdoor option is set to Auto.
Allow DFS Channels	Allows ZoneFlex APs to use DFS channels.	Click to enable the option.
Allow Channel 144	Provides channel 140 and 144 support for 11ac and 11ax APs. Enabling this option supports 20 MHz, 40 MHz, or 80 MHz channel modes. The 160 MHz mode is supported if the AP supports this mode. Disabling this option provides Channel 140 support only to 20 MHz mode. **NOTE** This option is available for selection only if you enable the **DFS Channels** option. **NOTE** This feature is currently supported only in the United States.	Click to enable the option.
Allow Indoor Channels	Allows outdoor APs to use channels regulated as for indoor use only.	Click to enable the option.

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

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

TABLE 6 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 mainting mesh links and to discover AP neighbors.	Enter the duration in seconds. Range: 1 through 65535.
Auto Channel Selection	Automatically adjusts the channel using the ChannelFly option.	Select the required option. For **ChannelFly**, set the **Channel Change Frequency** and **Full Optimization Period**.
Configuration > **Band/Spectrum Configuration** > **Upper 5 GHz**		
Channelization	Indicates the channel width.	Set the channel width used during transmission: Auto, 20, 40, 80 and 160.
Channel	Indicates the channel to use.	Select the required options for the Indoor and Outdoor APs.
Allow DFS Channels	Allows ZoneFlex APs to use DFS channels.	Click to enable the option.
Allow Channel 144	Provides channel 140 and 144 support for 11ac and 11ax APs. Enabling this option supports 20 MHz, 40 MHz, or 80 MHz channel modes. The 160 MHz mode is supported if the AP supports this mode. Disabling this option provides Channel 140 support only to 20 MHz mode. **NOTE** This option is available for selection only if you enable the **DFS Channels** option. **NOTE** This feature is currently supported only in the United States.	Click to enable the option.
Auto Cell Sizing	Enables the AP to share information on interference seen by each other and dynamically adjust their radio Tx power and Rx parameters to minimize interference. Enabling this option disables the TX Power Adjustment configuration. **NOTE** Ensure that Background Scan is enabled.	Select the option.
TX Power Adjustment	Allows to manually configure the transmit power on the Upper 5 GHz radio. By default, the TX power is set to Full on the Upper 5 GHz radio. **NOTE** If you choose Min, the transmit power is set to 0dBm (1mW) per chain for 11n APs, and 2dBm per chain for 11ac APs. If you choose Max, the transmit power is set to the maximum allowable value according to the AP's capability and the operating country's regulations.	Select the preferred TX power.
Background Scan	Allows the AP radio to scan other channels in the band for accessing channel health and capacity, detecting rogue devices, optimizing and mainting mesh links and to discover AP neighbors.	Enter the duration in seconds. Range: 1 through 65535.

TABLE 6 AP Zone Details for SZ300 and vSZ-H platforms (continued)

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

TABLE 6 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. › **Portocol**: select between UDP and TCP protocols. – **Secondary Server Address**: If the primary server goes down, the AP sends syslog messages to the secondary server as backup. › **Port**: Enter the syslog port number on the respective servers. › **Portocol**: Select between UDP and TCP protocols. – **Event Facility**: Select the facility level that will be used by the syslog message. Options include: Keep Original, Local0 (default), Local1, Local2, Local3, Local4, Local5, Local6, and Local7. – **Priority**: Select the lowest priority level for which events will be sent to the syslog server. For example, to only receive syslog messages for events with the warning (and higher) priority, select **Warning**. To receive syslog messages for all events, select **All**. – **Send Logs**: Select the type of messages to be sent to the syslog server. For example, General Logs, Client Logs or All Logs. • AP External Syslog Profile: Select the profile from the drop-down or click Add to create a new profile.
Configuration > AP SNMP Options		
Enable AP SNMP	Indicates if the AP SNMP option is enabled.	Select the check box.
Config Type	Enables custom or AP SNMP Profile Agent.	Select the check box. • Custom: Select this option to create customized SNMPv2 and SNMPv3 profile agents. • AP SNMP Profile Agent: Select this option to create AP SNMPv2 and SNMPv3 profile agents directly.

TABLE 6 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. Enter the **Auth Pass Phrase**. d. Select the **Privacy** option. e. Select the required **Privilege**. If you select **Notification**, select the option **Trap** or **Inform** and enter the **Target IP** and **Target Port**. f. Click **OK**.
Configuration > **Cellular Options**		
LTE Band Lock	Displays the list of LTE bands (4G/3G) and allows you to lock one or more bands from the list. Once a lock is enabled, the connection is established only to the specified bands. **NOTE** The list of bands is only applicable to: • **Domain** • **USA** • **Canada** • **Japan**	Select the check box and choose the band from: • **Primary Sim** • **Secondary Sim**
Configuration > **Advanced Options**		
Restricted AP Access Profile **NOTE** This feature is available from 5.2 release and onwards.	Restricted AP Access blocks access to the AP's standard well know open ports to protect the APs and enhance their security.	Select the Restricted AP Access profile from the drop-down. You can also create a new profile by clicking **+** icon. **NOTE** By default this feature is disabled. **NOTE** You can add maximum five Restricted AP Access profiles for a zone.
Channel Mode	Indicates if location-based service is enabled. If you want to allow indoor APs that belong to this zone to use wireless channels that are Channel Mode regulated as indoor-use only.	Select the **Allow indoor channels** check box.
Smart Monitor	Indicates AP interval check and retry threshold settings.	Select the check box and enter the interval and threshold.
AP Ping Latency Interval	Measures the latency between the controller and AP periodically, and sends this data to SCI.	Enable by moving the button to ON to measure latency.

TABLE 6 AP Zone Details for SZ300 and vSZ-H platforms (continued)

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

TABLE 6 AP Zone Details for SZ300 and vSZ-H platforms (continued)

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

TABLE 7 AP Zone Details for SZ100 and vSZ-E platforms

Field	Description	Your Action
Name	Indicates the name of the zone orAP group.	Enter a name.
Description	Indicates the short description assigned to the zone or AP group.	Enter a brief description
Type	Indicates if you are creating a domain, zone, or an AP group.	Appears by default. You can also choose the option.
Parent Group	Indicates the parent AP group.	Appears by default.
Link Switch Group	Allows to create a link between the switch group and an AP.	You can enable or disable the option. When the link state is enabled, you can modify the name and description of the switch group, the AP zone will change accordingly. When the link is disabled, the AP zone and switch group no longer share same name and description, but the link between them still exists. To delete the link, modify the name of AP zone or switch group. After successful deletion of the link, the **Link AP Zone** option is unavailable.
Configuration > General Options		
AP Firmware	Indicates the firmware to which it applies.	Select the firmware.
Country Code	Indicates the country code. Using the correct country code helps ensure that APs use only authorized radio channels.	Select the country code.
Location	Indicates the generic location.	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 admininstrator 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**
Configuration > Mesh Options		
Enable mesh networking in this zone	Enables managed APs to automatically form a wireless mesh network, in which participant nodes (APs) cooperate to route packets.	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.

TABLE 7 AP Zone Details for SZ100 and vSZ-E platforms (continued)

Field	Description	Your Action
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.
Configuration > **Radio Options**		
Dual-5G Mode	Enables third radio operator in 2.4 GHz, Lower 5 GHz, and Upper 5 GHz. By default, the **Dual-5G Mode** is enabled. In the enabled mode, radio-0 will be on 2.4GHz band, radio-1 will be on 5G Lower band and radio-2 will be on 5G Upper band. • 5G Lower BAND : UNII-1, UNII-2A • 5G Upper BAND : UNII-2C, UNII-3 In the disabled mode, the radio-0 will be on 2.4GHz band, radio-1 will be on 5G band and radio-2 will be on 6G band. This also depends on the country code.	Select or keep the default **Dual-5G Mode** option.
Configuration > **Band/Spectrum Configuration** > **2.4 GHz**		
Channelization	Indicates the channel width.	Set the channel width used during transmission to either 20 or 40 (MHz), or select Auto to set it automatically.
Channel	Indicates the channel to use.	Select one of the options: Auto, 1, 6 or 11.
Auto Cell Sizing	Enables the AP to share information on interference seen by each other and dynamically adjust their radio Tx power and Rx parameters to minimize interference. Enabling this option disables the TX Power Adjustment configuration. **NOTE** Ensure that Background Scan is enabled.	Select the option.
TX Power Adjustment	Allows to manually configure the transmit power on the 2.4 GHz radio. By default, the TX power is set to Full on the 2.4 GHz radio. **NOTE** If you choose Min, the transmit power is set to 0dBm (1mW) per chain for 11n APs, and 2dBm per chain for 11ac APs. If you choose Max, the transmit power is set to the maximum allowable value according to the AP's capability and the operating country's regulations.	Select the preferred TX power.
Protection Mode	Indicates the mechanism to reduce frame collision.	Choose one of the following options: • None • RTS/CTS • CTS Only
Background Scan	Allows the AP radio to scan other channels in the band for accessing channel health and capacity, detecting rogue devices, optimizing and mainting mesh links and to discover AP neighbors.	Enter the duration in seconds. Range: 1 through 65535.

TABLE 7 AP Zone Details for SZ100 and vSZ-E platforms (continued)

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

TABLE 7 AP Zone Details for SZ100 and vSZ-E platforms (continued)

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

TABLE 7 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 Lower 5 GHz radio. By default, the TX power is set to Full on the Lower 5 GHz radio. **NOTE** If you choose Min, the transmit power is set to 0dBm (1mW) per chain for 11n APs, and 2dBm per chain for 11ac APs. If you choose Max, the transmit power is set to the maximum allowable value according to the AP's capability and the operating country's regulations.	Select the preferred TX power.
Background Scan	Allows the AP radio to scan other channels in the band for accessing channel health and capacity, detecting rogue devices, optimizing and mainting mesh links and to discover AP neighbors.	Enter the duration in seconds. Range: 1 through 65535.
Auto Channel Selection	Automatically adjusts the channel using the ChannelFly option.	Select the required option. For **ChannelFly**, set the **Channel Change Frequency** and **Full Optimization Period**.
Configuration > **Band/Spectrum Configuration** > **Upper 5 GHz**		
Channelization	Indicates the channel width.	Set the channel width used during transmission: Auto, 20, 40, 80 and 160.
Channel	Indicates the channel to use.	Select the required options for the Indoor and Outdoor APs.
Allow DFS Channels	Allows ZoneFlex APs to use DFS channels.	Click to enable the option.
Allow Channel 144	Provides channel 140 and 144 support for 11ac and 11ax APs. Enabling this option supports 20 MHz, 40 MHz, or 80 MHz channel modes. The 160 MHz mode is supported if the AP supports this mode. Disabling this option provides Channel 140 support only to 20 MHz mode. **NOTE** This option is available for selection only if you enable the **DFS Channels** option. **NOTE** This feature is currently supported only in the United States.	Click to enable the option.

TABLE 7 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 Upper 5 GHz radio. By default, the TX power is set to Full on the Upper 5 GHz radio. **NOTE** If you choose Min, the transmit power is set to 0dBm (1mW) per chain for 11n APs, and 2dBm per chain for 11ac APs. If you choose Max, the transmit power is set to the maximum allowable value according to the AP's capability and the operating country's regulations.	Select the preferred TX power.
Background Scan	Allows the AP radio to scan other channels in the band for accessing channel health and capacity, detecting rogue devices, optimizing and mainting mesh links and to discover AP neighbors.	Enter the duration in seconds. Range: 1 through 65535.
Auto Channel Selection	Automatically adjusts the channel using the ChannelFly option.	Select the required option. For **ChannelFly**, set the **Channel Change Frequency** and **Full Optimization Period**.
Configuration > AP GRE Tunnel Options		
Ruckus GRE 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 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	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.
Configuration > Syslog Options		

TABLE 7 AP Zone Details for SZ100 and vSZ-E platforms (continued)

Field	Description	Your Action
Enable external syslog server for APs	Enables the AP to send syslog data to the syslog server on the network.	Select the option.
Config Type	Allows to customize or select an external syslog server profile.	Select the option: • Custom: Configure the details for the AP to send syslog messages to syslog server. **NOTE** The IP address format that you enter here will depend on the AP IP mode that you selected earlier in this procedure. If you selected IPv4 Only, enter an IPv4 address. If you selected IPv6 Only, enter an IPv6 address. – **Primary Server Address**: If the primary server goes to sends syslog messages. › **Port**: enter the syslog port number on the respective servers. › **Portocol**: select between UDP and TCP protocols – **Secondary Server Address**: If the primary server goes down, the AP sends syslog messages to the secondary server as backup. › **Port**: enter the syslog port number on the respective servers. › **Portocol**: select between UDP and TCP protocols – **Event Facility**: Select the facility level that will be used by the syslog message. Options include: Keep Original, Local0 (default), Local1, Local2, Local3, Local4, Local5, Local6, and Local7. – **Priority**: Select the lowest priority level for which events will be sent to the syslog server. For example, to only receive syslog messages for events with the warning (and higher) priority, select **Warning**. To receive syslog messages for all events, select **All**. – **Send Logs**: Select the type of messages to be sent to the syslog server. For example, General Logs, Client Logs or All Logs. • AP External Syslog Profile: Select the profile from the drop-down or click Add to create a new profile.
Configuration > 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 7 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.
Configuration > **Cellular Options**		
LTE Band Lock	Displays the list of LTE bands (4G/3G) and allows you to lock one or more bands from the list. Once a lock is enabled, the connection is established only to the specified bands. **NOTE** The list of bands is only applicable to: • **Domain** • **USA** • **Canada** • **Japan**	Select the check box and choose the band from: • **Primary Sim** • **Secondary Sim**
Configuration > **Advanced Options**		
Restricted AP Access Profile **NOTE** This feature is available from 5.2 release and onwards.	Restricted AP Access blocks access to the AP's standard well know open ports to protect the APs and enhance their security.	Select the Restricted AP Access profile from the drop-down. You can also create a new profile by clicking **+** icon. **NOTE** By default this feature is disabled. **NOTE** You can add maximum five Restricted AP Access profiles for a zone.
Channel Mode	Indicates if location-based service is enabled. If you want to allow indoor APs that belong to this zone to use wireless channels that are Channel Mode regulated as indoor-use only.	Select the **Allow indoor channels** check box.
Smart Monitor	Indicates AP interval check and retry threshold settings.	Select the check box and enter the interval and threshold.
AP Ping Latency Interval	Measures the latency between the controller and AP periodically, and sends this data to SCI.	Enable by moving the button to ON to measure latency.

TABLE 7 AP Zone Details for SZ100 and vSZ-E platforms (continued)

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

TABLE 7 AP Zone Details for SZ100 and vSZ-E platforms (continued)

Field	Description	Your Action
Steering Mode	Controls the APs' steering behavior for load balancing and band balancing.	Select the option and use the slider to actively control associated stations to meet the distribution requirements allowing band balancing and load balancing: • Basic (default): During heavy load conditions, this option withholds probe and authentication responses in order to achieve load balance. • Proactive: This is a dynamic form of band balancing where some selected associated clients are rebalanced on the AP or across APs utilizing the 802.11v BTM. The AP sends a BTM message to the client to roam and it is left to the client's discretion to make its roaming decision. • Strict: This is an aggressive form of balancing where some selected associated clients are forced to rebalance utilizing the 802.11v BTM. The AP sends a BTM message to the client to roam. If the client does not roam, the client is forced to disconnect after 10 seconds. Additionally, some selected non-802.11v clients are forcefully disconnected directly to force them to roam. **NOTE** The band change is applicable only for those connected clients that support the 802.11v standard. Enter the percentage of client load on the 2.4 GHz band.
Location Based Service	Indicates that the location-based service is enabled.	• Select the check box and choose the options. • **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**. **NOTE** The Recovery SSID is available when an AP does not get a reply back for unicast arping to its configured gateway.

TABLE 7 AP Zone Details for SZ100 and vSZ-E platforms (continued)

Field	Description	Your Action
My.Ruckus support for Tunnel-WLAN/ VLAN	By default, support for LBO, tunneled-WLAN, and non-default management VLAN is disabled because it adds an ACL which affects the LBO and tunneled-WLAN performance. Enabling this support may have a 10 percent impact on the Wi-Fi performance.	Enable the option for support.

4. Click **OK**.

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

NOTE

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

Auto Cell Sizing

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

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

ChannelFly and Background Scanning

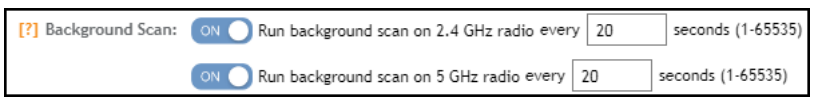
The controller offers the ChannelFly and Background Scanning automatic channel selection methods for spectrum utilization and performance optimization.

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

TABLE 8

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

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

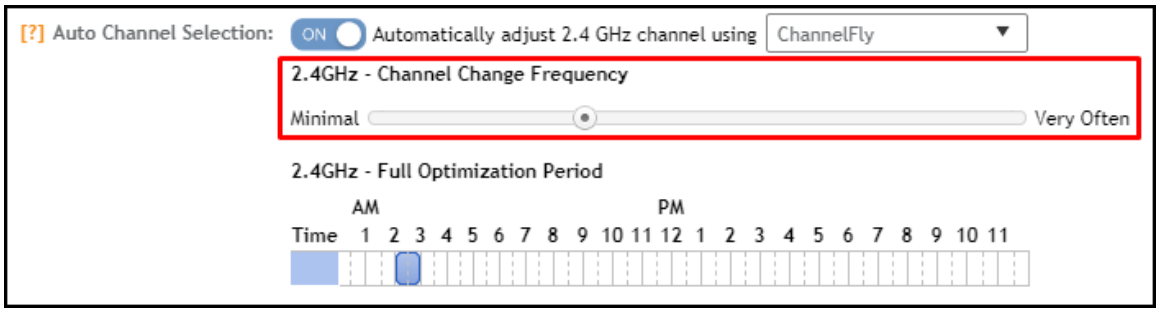


ChannelFly

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

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

The *Channel Change Frequency* (CCF) configuration allows the user to specify the responsive of ChannelFly to interference with consideration for the impact on associated clients. ChannelFly will avoid performing channel changes when a certain number of clients are associated to the AP on a per-radio basis. This threshold is defined by the CCF. **With the default CCF of 33, channel changes may occur only when there are 3 or fewer associated clients**. The CCF also affects the probability that a channel change occurs when a better channel is found. However, a channel change will only occur when the number of associate clients is below the client threshold as defined in Table 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

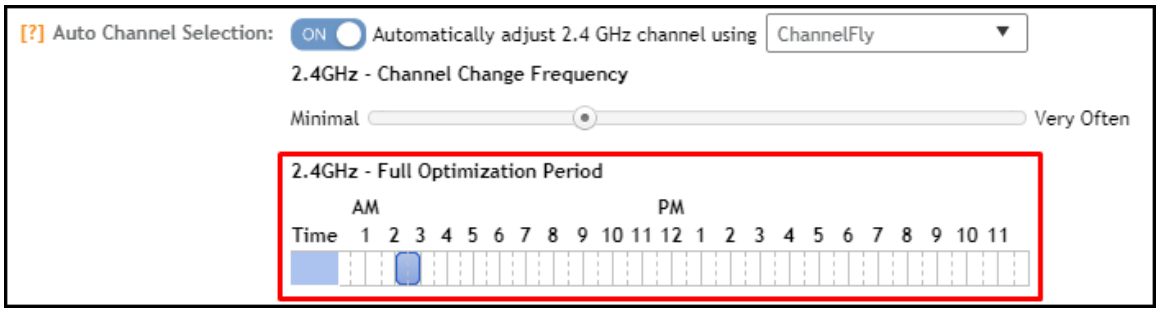
CCF	100	90	80	70	60	50	40	30	20	10	1
Client Threshold	10	9	8	7	6	5	4	3	2	1	0

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.

VLAN Pooling

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

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

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

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

Creating an AP Group

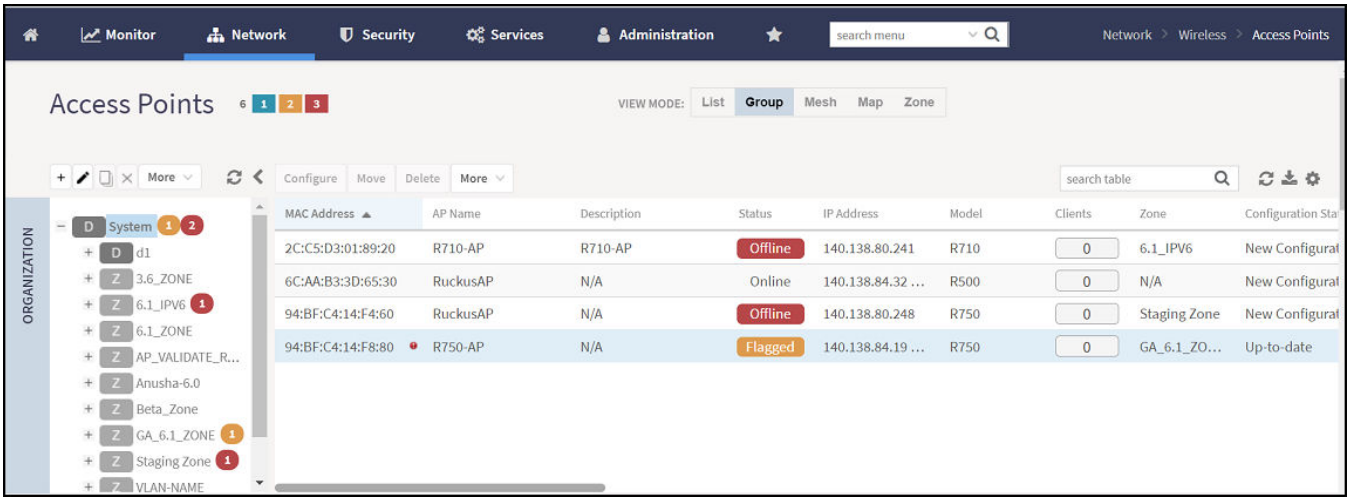
By creating an AP group, you can configure a profile that defines the channels, radio settings, Ethernet ports and other configurable fields for all members of the group or for all APs of a specific model in the group.

Follow these steps to create an AP group.

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

   The **Access Point** page is displayed.

   FIGURE 6 Access Point Page



2. From the System tree hierarchy, select the location (for example: System, Domain, Zone) and click  . The **Create 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 11 AP Group Details

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

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

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

TABLE 11 AP Group Details (continued)

Field	Description	Your Action
Auto Channel Selection	Automatically adjusts the channel using the **ChannelFly** option.	For **ChannelFly**, set the **Channel Change Frequency** and **Full Optimization Period**.
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%, .i.e. 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.
Configuration > Band/Spectrum Configuration > Lower 5 GHz		
Channelization	Indicates the channel width.	Set the channel width used during transmission: Auto, 20, 40, 80 and 160.
Channel	Indicates the channel to use.	Select the required options for the Indoor and Outdoor APs.
Allow DFS Channels	Allows ZoneFlex APs to use DFS channels.	Click to enable the option.
Allow Indoor Channels	Allows outdoor APs to use channels regulated as for indoor use only.	Click to enable the option.
Auto Cell Sizing	Enables the AP to share information on interference seen by each other and dynamically adjust their radio Tx power and Rx parameters to minimize interference. Enabling this option disables the TX Power Adjustment configuration. **NOTE** Ensure that Background Scan is enabled.	Select the option.

TABLE 11 AP Group Details (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 mainting mesh links and to discover AP neighbors.	Enter the duration in seconds. Range: 1 through 65535.
Auto Channel Selection	Automatically adjusts the channel using the **ChannelFly** option.	Select the required option. For **ChannelFly**, set the **Channel Change Frequency** and **Full Optimization Period**.
Configuration > **Band/Spectrum Configuration** > **Upper 5 GHz**		
Channelization	Indicates the channel width.	Set the channel width used during transmission: Auto, 20, 40, 80 and 160.
Channel	Indicates the channel to use.	Select the required options for the Indoor and Outdoor APs.
Allow DFS Channels	Allows ZoneFlex APs to use DFS channels.	Click to enable the option.
Allow Channel 144	Provides channel 140 and 144 support for 11ac and 11ax APs. Enabling this option supports 20 MHz, 40 MHz, or 80 MHz channel modes. The 160 MHz mode is supported if the AP supports this mode. Disabling this option provides Channel 140 support only to 20 MHz mode. **NOTE** This option is available 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 11 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 mainting mesh links and to discover AP neighbors.	Enter the duration in seconds. Range: 1 through 65535.
Auto Channel Selection	Automatically adjusts the channel using the **ChannelFly** option.	Select the required option. For **ChannelFly**, set the **Channel Change Frequency** and **Full Optimization Period** options.
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.
Configuration > AP SNMP Options		
Override zone configuration	Indicates that the AP Group configuration overrides the zone configuration.	Select the check box.
Enable AP SNMP	Indicates if the AP SNMP option is enabled.	Select the check box.
SNMPv2 Agent	Indicates SNMPv2 Agent is applied.	1. Click **Create** and enter **Community**. 2. Select the required **Privilege**. If you select **Notification** enter the **Target IP**. 3. Click **OK**.
SNMPv3 Agent	Indicates SNMPv3 Agent is applied.	1. Click **Create** and enter **User**. 2. Select the required **Authentication**. 3. Enter the **Auth Pass Phrase**. 4. Select the **Privacy** option. 5. Select the required **Privilege**. If you select **Notification** select the option **Trap** or **Inform** and enter the **Target IP** and **Target Port**. 6. Click **OK**.
Configuration > Model Specific Options **NOTE** Select the **Override** check box for that setting, and then configure the setting.		

TABLE 11 AP Group Details (continued)

Field	Description	Your Action
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	Indicates whether the selected AP is operation in the PoE mode. **NOTE** You can set the PoE operating mode from the **AP Configuration** tab on the controller or using the **get power-mode** CLI command. • R550 • R610 • R650 • R710 • R720 • R730 • R750 • R850 • M510 • H550 • T610 • T610S • T750 • T750SE 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 11 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.
Configuration > Cellular Options		
LTE Band Lock	Displays the list of LTE bands (4G/3G) and allows you to lock one or more bands from the list. Once a lock is enabled, the connection will be established only to the specified bands. The LTE band lock function is disabled by default. **NOTE** The list of bands is only applicable to: • **Domain** • **USA** • **Canada** • **Japan**	Select **Override zone configuration** to enable and choose the band from the following: • **Primary Sim** • **Secondary Sim**
Configuration > Advanced Options		
Location Based Service	Enables location-based service for the AP group.	• Select the **Override zone configuration** check box. • Select the **Enable LBS Service** check box. • **Select an LBS Server** from the drop-down.
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.

TABLE 11 AP Group Details (continued)

Field	Description	Your Action
Client Admission Control	Indicates the load thresholds on the AP at which it will stop accepting new clients.	Select the **Override** check box respective to **2.4 GHz Radio** or **5 GHz Radio** and update the following details: • **Enable** **NOTE** Client load balancing and band balancing will be disabled for this AP group. • **Min Client Count** • **Max Radio Load** • **Min Client Throughput**
Rogue Classification Policy	Indicates the parameters used to classify rogue APs. This option is available only if you enable the **Rogue AP Detection**option.	Select the options for rogue classification policy: • Enable the **Override** option and select the rogue classification policy from the list to override for this group. • Enable the **Override** option and enter the **Report RSSI Threshold**. Range: **0** through **100**. • Enable the **Overide** option to override the aggressiveness of protecting the network and choose one of the following: – **Aggressive** – **Auto** – **Conservative** • Enable the **Override** option and enter the **Jamming Threshold** in percentage.
Recovery SSID	Allows you to enable or disable the Recovery(Island) SSID broadcast on the controller.	Enable **Recovery SSID Broadcast**
Direct Multicast	Indicates whether multicast traffic is sent from a wired device, wireless device or from the network.	Select one or more of the following: • **Multicast Traffic from Wired Client** • **Multicast Traffic from Wireless Client** • **Multicast Traffic from Network**
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.

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. Go to **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.

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.
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.

Option	Description
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.

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

7. Click **OK**.

Supported LLDP Attributes

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

LLDP information is sent by devices from each of their interfaces at a fixed interval (default is 30 seconds), in the form of an Ethernet frame. Each LLDP Ethernet frame contains a sequence of type-length-value (TLV) structures starting with Chassis ID, Port ID and Time to Live (TTL) TLV. Table 2 lists the LLDP attributes supported by the controller.

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.

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.

Attribute (TLV)	Description
System Description	Indicates the AP model plus software version
System Capabilities	Indicates the AP's capabilities (Bridge, WLAN AP, Router, Docsis), and which capabilities are enabled
Management Address	Indicates the management IP address of the AP
Port Description	Indicates the description of the port in alphanumeric format

Configuring the Port Settings of a Particular AP Model

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

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

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

   The following restrictions apply:

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

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

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

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 12 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 12 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	Indicates the channel width.	Set the channel width used during transmission to either 20 or 40 (MHz), or select Auto to set it automatically.
Channel	Indicates the channel to use.	Select one of the options: Auto, 1, 6 or 11.
Auto Cell Sizing	Enables the AP to share information on interference seen by each other and dynamically adjust their radio Tx power and Rx parameters to minimize interference. Enabling this option disables the TX Power Adjustment configuration. **NOTE** Ensure that Background Scan is enabled.	Select the option.
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	Allows to manually override the protection mode and select from the options - • None • RTS/CTS • CTS Only	Select the preferred protection mode.

TABLE 12 Access Point Edit Parameters (continued)

Field	Description	Your Action
WLAN Group	Allows to manully configure the WLAN Group. To add a WLAN group, refer to the **Creating a WLAN group** section of the *RUCKUS SmartZone (LT-GA) WLAN Management Guide (SZ300/vSZ-H)*.	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 mainting mesh links and to discover AP neighbors.	Enter the duration in seconds. Range: 1 through 65535.
Auto Channel Selection	Automatically adjusts the channel using the ChannelFly option.	Select the required option. For **ChannelFly**, set the **Channel Change Frequency** and **Full Optimization Period**.
AP Configuration > **Band/Spectrum Configuration** > **5 GHz**		
Channelization	Indicates the channel width.	Set the channel width used during transmission: Auto, 20, 40, 80 and 160.
Channel	Indicates the channel to use.	Select the required options for the Indoor and Outdoor APs.
Secondary Channel	Indicates the secondary channel to used.	By default, the Indoor and Outdoor option is set to Auto.
Allow DFS Channels	Allows ZoneFlex APs to use DFS channels.	Click to enable the option.
Allow Channel 144	Provides channel 140 and 144 support for 11ac and 11ax APs. Enabling this option supports 20 MHz, 40 MHz, or 80 MHz channel modes. The 160 MHz mode is supported if the AP supports this mode. Disabling this option provides Channel 140 support only to 20 MHz mode. **NOTE** This option is available for selection only if you enable the **DFS Channels** option. **NOTE** This feature is currently supported only in the United States.	Click to enable the option.
Allow Indoor Channels	Allows outdoor APs to use channels regulated as for indoor use only.	Click to enable the option.
Auto Cell Sizing	Enables the AP to share information on interference seen by each other and dynamically adjust their radio Tx power and Rx parameters to minimize interference. Enabling this option disables the TX Power Adjustment configuration. **NOTE** Ensure that Background Scan is enabled.	Select the option.

TABLE 12 Access Point Edit Parameters (continued)

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

TABLE 12 Access Point Edit Parameters (continued)

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

TABLE 12 Access Point Edit Parameters (continued)

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

TABLE 12 Access Point Edit Parameters (continued)

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

TABLE 12 Access Point Edit Parameters (continued)

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

TABLE 12 Access Point Edit Parameters (continued)

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

TABLE 12 Access Point Edit Parameters (continued)

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

NOTE

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

Configuring the M510 AP

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

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

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

TABLE 13 Access Point Edit Parameters

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

TABLE 13 Access Point Edit Parameters (continued)

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

TABLE 13 Access Point Edit Parameters (continued)

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

TABLE 13 Access Point Edit Parameters (continued)

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

TABLE 13 Access Point Edit Parameters (continued)

Field	Description	Your Action
PoE Operating Mode	Allows you to operate using PoE mode.	Select the option.
Port Settings	Indicates the port settings.	Select the option and choose the required LAN option.
AP Configuration > Advanced Options		
Mesh Mode	Select the appropriate mesh mode.	• Auto - Mesh mode is assigned automatically. • Root AP - Only runs as a root AP. • Mesh AP - Only runs as a mesh AP. • Disable - Disables the mesh mode.
Uplink Selection	Select the appropriate uplink.	• Smart - Mesh APs automatically select the best uplink. • Manual - Only selected APs can be used for uplink.
Uplink Radio	Select the appropriate uplink radio.	• Auto • 2nd Radio • 3rd Radio **NOTE** The uplink radio works only in R760 and R560 Access Points.
Network Settings	Determines the network settings.	Select the IPv4 settings from the following options: • **Static**: Enter the **IP Address**, **Network Mask**, **Gateway**, **Primary DNS**, and **Secondary DNS**. • **Dynamic** • **Keep the AP's Setting**
Smart Monitor	Indicates the AP interval check and retry threshold settings.	Select the required check boxes.
Syslog Options	Determines if external syslog server settings are applicable.	Select the required check boxes. For the **Enable external syslog server** option, update the following information: • **Server Address** • **Port** • **Facility for Event** • **Priority**
Hotspot 2.0 version Profile	Indicates the hotspot profile that you want to assign to the group.	Select the required option or click **Create** and update the following details: • Enter the **Name**. • Enter the **Description**. • Enter the **Venue Names**. • Select the **Venue Category**. • Select the **Type**. • Enter the **WLAN Metrics**.

TABLE 13 Access Point Edit Parameters (continued)

Field	Description	Your Action
AP Management VLAN	Indicates the AP management VLAN settings.	Select the check box and choose the option. **ATTENTION** For standalone APs, set the AP Ethernet port to trunk before changing the AP management VLAN settings.
Auto Channel Selection	Indicates auto-channel settings.	Select the check box and choose the option.
Client Admission Control	Indicates the load thresholds on the AP at which it will stop accepting new clients.	Select the check boxes and update the following details: • **Min Client Count** • **Max Radio Load** • **Min Client Throughput**
Protection Mode	Indicates the protection mode settings for the AP.	You can override the protection mode settings at 2.4 GHz, and select one of the following options: • **None** • **RTS/CTS (Request to Send/Clear to Send flow control mechanism that allows receiver and the transmitter to alert each other to their state)** • **CTS Only**
Venue Code	Indicates the venue code.	You can choose to override this setting and enter the code in the field provided.
Recovery SSID	Indicates the recovery SSID.	Select the **Enable Recovery SSID Broadcast** option for the AP to broadcast the SSID so it can be visible during discovery.
Direct Multicast	Indicates the direction in which multicast traffic can be sent.	Configure the AP to multicast traffic from wired clients, wireless clients, and from the network.
Swap Configuration		
Add Swap-In AP	Allows swapping of APs.	Select the check box and enter the **Swap-in AP MAC** details.

3. Click **OK**.

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

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

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 14 Zone Template Details

Field	Description	Your Action
General Options		
Zone Name	Indicates a name for the Zone.	Enter a name.
Description	Indicates a short description.	Enter a brief description
AP Firmware	Indicates the firmware to which it applies.	Select the firmware.
Country Code	Indicates the country code to ensure that this zone uses authorized radio channels.	Select the country code.
Location	Indicates generic location.	Enter the location.
Location Additional Information	Indicates detailed location.	Enter additional location information.
GPS Coordinates	Indicates the geographical location.	Enter the following coordinates in meters or floor: • **Longitude** • **Latitude** • **Altitude**
AP Admin Logon	Indicates the admin logon credentials. For the Default Zone, the 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		

TABLE 14 Zone Template Details (continued)

Field	Description	Your Action
Channel Range	Indicates that you want to override the 2.4GHz channel range that has been configured for the zone.	Select **Select Channel Range (2.4G)** check boxes for the channels on which you want the 2.4GHz radios to operate. Channel options include channels 1 to 11. By default, all channels are selected.
DFS Channels	Allows ZoneFlex APs to use DFS channels.	Click to enable the option.
Channel 144	Provides channel 140 and 144 support for 11ac and 11ax APs. Enabling this option supports 20 MHz, 40 MHz, or 80 MHz channel modes. The 80+80 MHz and 160 MHz modes are supported if the AP supports these modes. Disabling this option provides Channel 140 support only to 20 MHz mode. **NOTE** This option is available for selection only if you enable the **DFS Channels** option. **NOTE** This feature is currently supported only in the United States.	Click to enable the option.
Channel Range (5G) Indoor	Indicates for what channels want the 5GHz radios to operate.	Select the check boxes.
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 14 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 14 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 14 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 14 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.

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.

Switching Over Clusters

Switchover helps move individual switches or switches in a switch groups across clusters.

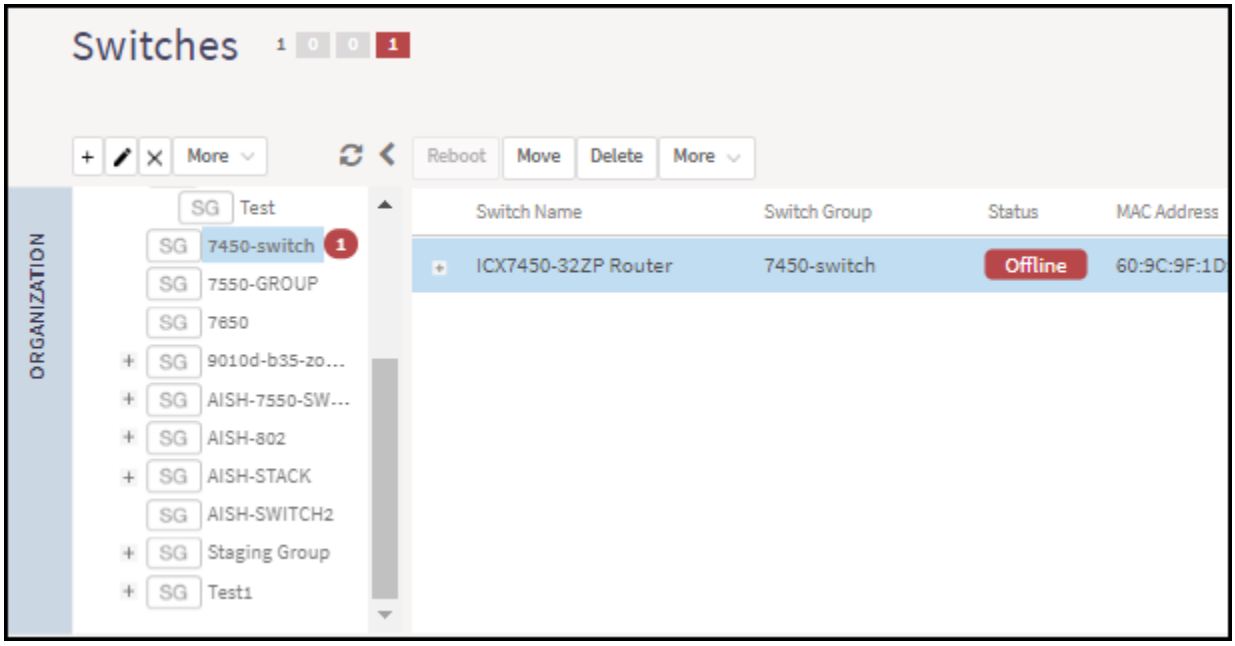
NOTE
Ensure that a switch registation rule is created on the target cluster before switching over to another cluster. For more information, refer to *Creating Switch Registration rules*.

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*.

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. In the **Organization** tab, select a **Domain** > **Switch Group** or **Switch Group** and select the **Switch**.

FIGURE 7 Selecting a Switch



3. In the **Organization** tab, click **More** > **Switch Over Cluster** to display the **Switch Over Cluster** dialog box.
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.

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 8 Load Balancing

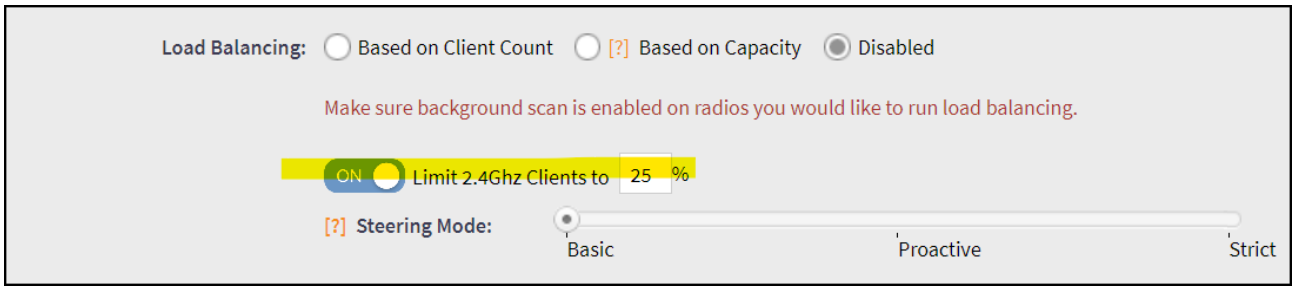
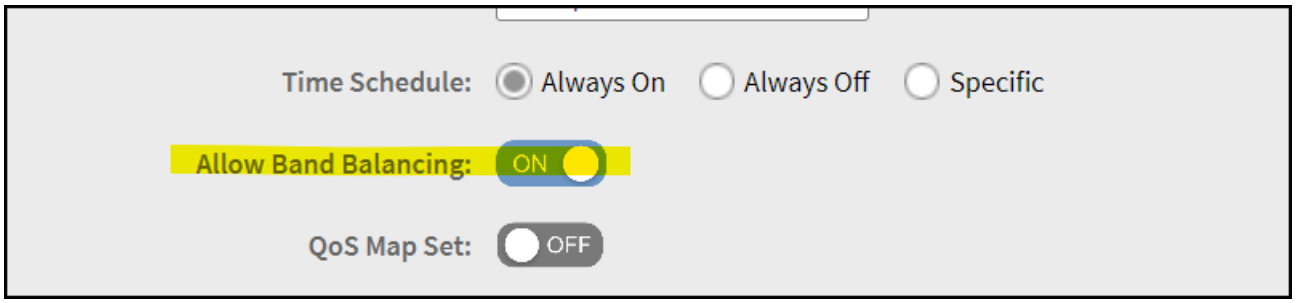


FIGURE 9 Band Balancing



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.

Bypassing Apple CNA

Some Apple iOS and OS X clients include Captive Network Assistant (CNA), which allows clients to connect to an open captive portal WLAN without displaying the login page.

When a client connects to a wireless network, the CNA launches a pre-browser login utility and it sends a request to a success page on the Apple® website. If the success page is returned, the device assumes it has network connectivity and no action is taken. However, this login utility is not a fully functional browser, and does not support HTML, HTML5, PHP, or other embedded video. In some situations, the ability to skip the login page for open WLANs is a benefit. However, for other guest or public access designs, the lack of ability to control the entire web authentication process is not desirable.

The controller provides an option to work around Apple CNA if it is not desirable for your specific deployment. With CNA bypass enabled, captive portal (web-based authentication) login must be performed by opening a browser to any unauthenticated page (HTTP) to get redirected to the login page.

Band or Spectrum Configuration

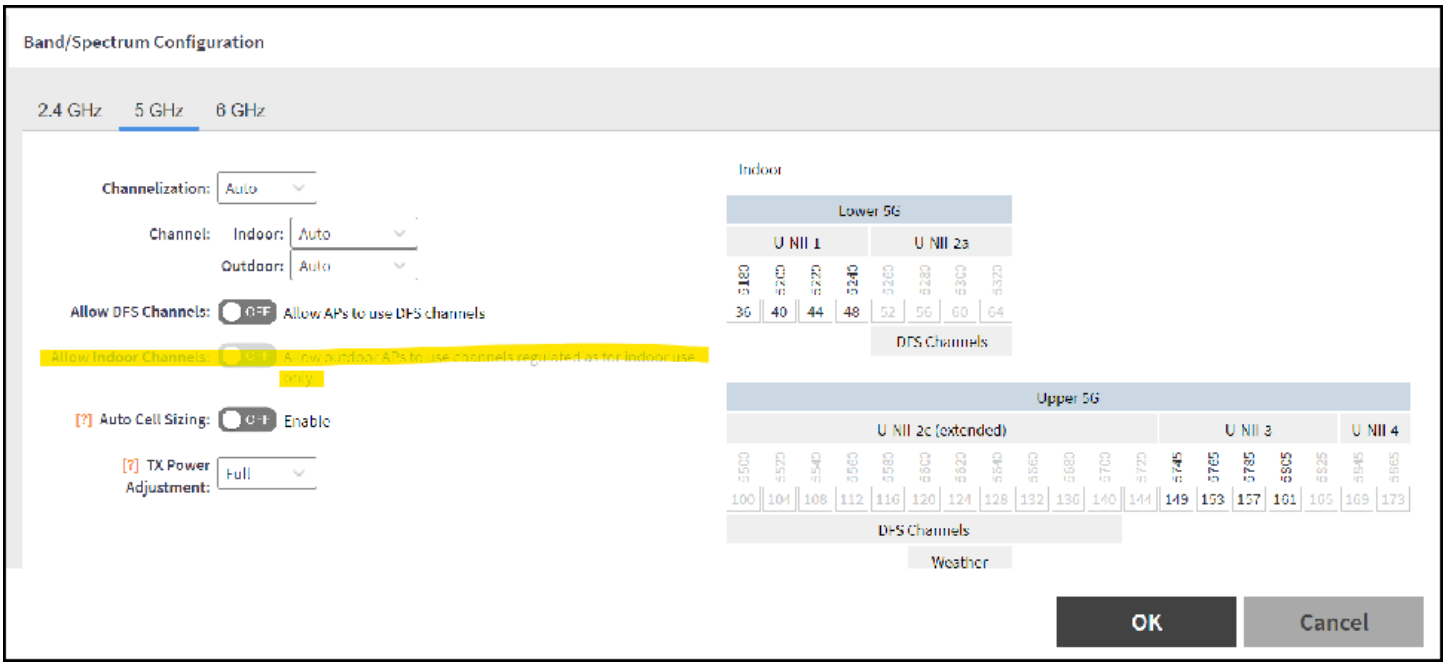
Band or spectrum configuration is a method of statistically picking the most potent channel for an AP.

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

Some countries restrict certain 5-GHz channels to indoor use only. For instance, Germany restricts channels in the 5.15-GHz to 5.25-GHz band to indoor use. When ZoneFlex Outdoor APs and Bridges with 5-GHz radios (ZoneFlex 7762, 7762-S, 7762-T, 7761-CM, and 7731) are set to a country code where these restrictions apply, the AP or Bridge can no longer be set to an indoor-only channel and will no longer select from amongst a channel set that includes these indoor-only channels when SmartSelect or Auto Channel selection is used, unless the administrator configures the AP to allow use of these channels.

For instance, if the AP is installed in a challenging indoor environment (such as a warehouse), the administrator may want to allow the AP to use an indoor-only channel. These channels can be enabled for use through the AP CLI or the controller web interface.

FIGURE 10 Band or Spectrum Configuration



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 15 Portal-based WLANs

WLAN Type	User Credential	Portal on Which WLAN is Hosted
Guest	Guest passes on the controller	AP
Hotspot (WISPr)	RADIUS server; LDAP/Active Directory from SmartZone 3.2 and later	External portal server or internal portal on the controller
WebAuth	RADIUS/LDAP/Active Directory	AP

Guest and WebAuth WLAN portals are hosted on the controller AP with limited customization.

WISPr WLANs are usually hosted on external portal servers providing the flexibility to customize. WISPr WLANs allow for sophisticated customization such as providing a customized login page which could include locale information, advertisements and so on.

WISPr WLANs can also be configured to bypass the authentication portal so that if the MAC address of an end user device (used as a credential) is stored on a RADIUS server, there is no need to redirect the end user to the portal server for authentication.

Portal-Based WLANs Characteristics

Portal-based WLANs have the following characteristics:

WebAuth WLANs have the following characteristics:

- Does not provide an option to modify the portal (WYSIWYG)
- Handles user authentication by the RADIUS server, LDAP, and Active Directory
- Allows redirecting of user web pages

Guest WLANs have the following characteristics:

- Provides an option to modify the portal elements such as the logo, Terms and Conditions, title, and so on
- Handles user authentication by using guest passphrases (or selecting the **Always Accepted**option)
- Allows redirecting of user web pages
- Does not possess a local database, LDAP, Active Directory, or RADIUS server

Hotspot (WISPr) WLANs (Internal Portal) have the following characteristics:

- Internal Portal
  - Provides an option to modify the portal elements such as the logo, Terms and Conditions, title, and so on
  - Handles user authentication by the local database, LDAP, Active Directory, RADIUS server (or selecting the **Always Accepted** option)
  - Allows redirecting user web pages
  - Supports the Walled Garden approach to allow user access to specific areas within the network
- Hotspot (WISPr) WLANs (External Portal) have the following characteristics:
  - Allows customization of the portal pages through external services
  - Supports Northbound Portal Interface for authentication
  - Handles user authentication by the local database, LDAP, Active Directory, RADIUS server (or selecting the **Always Accepted** option)
  - Allows redirecting of user web pages
  - Supports the Walled Garden approach to allow user access to specific areas within the network

Multicast Rate Filter

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

- **FIGURE 11** Multicast Rate Limiting

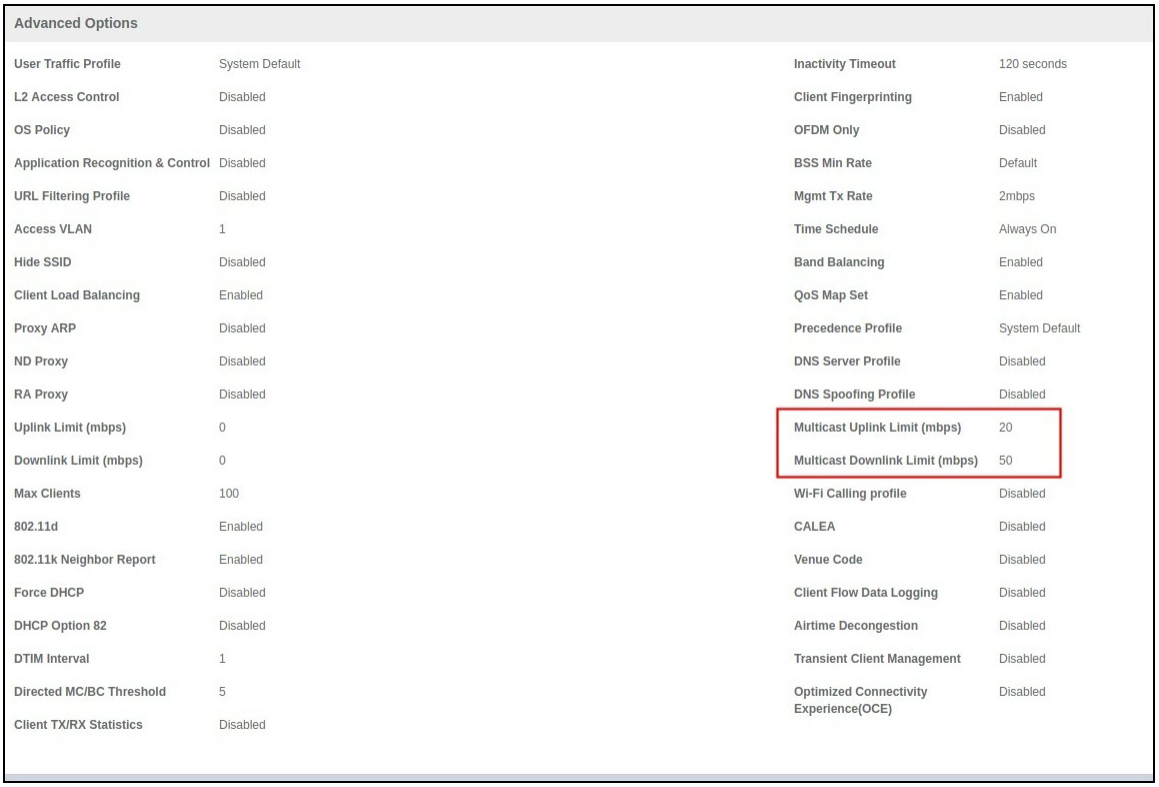
Configuring the Multicast rate limit

- 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 12 Configuring the Multicast Rate Limit



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

FIGURE 13 WLAN Preview

Transient Client Management

Transient Client Management allows only those clients that stay within the coverage region of the AP for a minimum period of time to associate with the AP and use the network service. For example, in a train station or downtown area, there may be passersby who do not intend to connect and utilize the network service. However, their Wi-Fi devices may conduct an active/passive scanning and may be roaming from cellular to Wi-Fi, from one Wi-Fi AP to another Wi-Fi AP, or from Wi-Fi to cellular, which could compromise the experience of users who are connected and using the network service. First-time client association may be delayed.

Transient Client Management uses statistical methods to delay the association of transient clients to an AP. Venue administrators will be able to tune configuration parameters based on typical observed dwell times and RSSI of transient clients. Transient Client Management delivers efficient airtime utilization and minimizes cellular-to-Wi-Fi handoffs and AP-to-AP roaming of transient clients.

Optimized Connectivity Experience

Optimized Connectivity Experience (OCE) delivers a better overall connectivity experience by enabling probe response suppression and by preventing devices with marginal connectivity to join the network.

When OCE is enabled, the affected APs and stations are excluded from Airtime Decongestion and Transient Client Management, resulting in reduction in probe response. Probe response suppression optimizes airtime for data traffic. OCE solves connectivity issues by rejecting any association with clients with poor signals.

VIDEO
Optimized Connectivity Experience. This video provides a brief overview of Optimized Connectivity Experience.
Click to play video in full screen mode.

Fast Initial Link Setup (FILS)

Enable Fast Initial Link Setup (FILS) for 802.1X EAP WLAN and select the realm-based AAA configuration and DHCP server IP address.

Combines the authentication, authorization, and DHCP to reduce EAP frames and skip EAPOL 4-way handshake when station reconnects or roams. It requires AAA to support Higher Layer Protocol (HLP) and EAP-RP. The DHCP server requires the Rapid commit. The following WLAN feature combinations are supported by FILS:

- 802.1x(FILS) + WISPr
- 802.1x(FILS) + MAC Auth
- 802.1x(FILS) + 802.11w
- 802.1x(FILS) + FT

NOTE
FILS provides MAC support. When FILS is enabled, the DHCP Rapid Commit Proxy is also enabled by default. However, it is hidden in the screen.

Create Fast Initial Link Setup (FILS) Realm Profile

Complete the following steps to create Fast Initial Link Setup (FILS) Realm Profile.

1. Go to **Security** > **Authentication** > **FILS Realm Proxy**.

   This displays **Create FILS Realm Profile** screen.
2. In the **Create FILS Realm Profile** screen, enter the following details:
   - Name: Name the profile.
   - Description: Short description for the profile.
   - Realms: Name the Realm and click **Add**.

     The Realm Name is displayed below.
   - Click **Ok**.

   The new profile is displayed in the **FILS Realm Profile** screen.

   NOTE
   The **FILS Realm Profile** can be created from the **Fast Initial Link Setup** by clicking **+** corresponding to the **Realm Profile**.

Configuring Traffic Analysis Display for WLANs

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

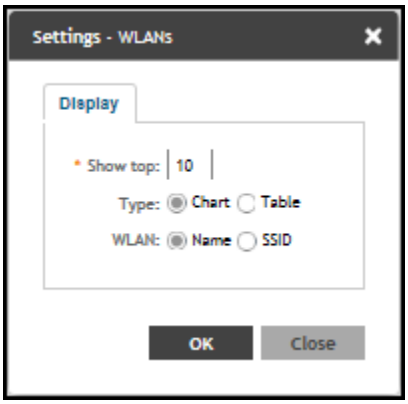
You can view historical and real-time data of the WLANs. Throughput and the number of clients connected to the WLANs are displayed in a bar chart. You must configure the WLAN settings to view its traffic analysis.

Complete the following steps to configure the WLAN settings.

1. From the WLAN area, click settings .

   The WLAN settings form displays.

   FIGURE 14 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**.

Working with Time Schedule Profiles

A **Time Schedule** profile specifies the hours of the day or week during which a WLAN service is enabled or disabled.

For example, a WLAN for student use at a school can be configured to provide wireless access only during school hours. This example involves creating a time schedule profile, and when configuring a WLAN, selecting the schedule profile to enable or disable the WLAN service during those days and hours.

NOTE
Creating a Time Schedule profile will not work properly if the system does not have the correct time. To ensure that the system always maintains the correct time, configure an NTP server and point the system to the IP address of the NTP server.

NOTE
When configuring the WLAN time schedule, all times are based on the time zone setting of your browser. If your browser and the target AP and WLAN are in different time zones, configure the on and off times according to the desired schedule according to your local browser. For example, if you want a WLAN in Los Angeles to turn on at 9 AM and your browser is set to New York time, configure the WLAN time schedule to enable the WLAN at noon.

Creating a Time Schedule Profile

Complete the following steps to create a Time schedule profile.

1. From the main menu, go to **Network** > **Wireless** > **Wireless LANS**, and select a WLAN.
2. Click **Configure**. The **Edit WLAN Configuration** dialog box is displayed.

3. Go to **Advanced Options**.
4. For **Time Schedule**, select **Specific**.

   NOTE
   By default, **Always On** is selected.

5. Click **Create (+)**. The **Create Time Based Access Table** dialog box is displayed.
6. In the **General Options**, enter the schedule name and schedule description.
7. In the **Schedule Table**, create a WLAN schedule profile for the selected wireless LAN.
8. To create the time-based access table for a WLAN, perform the following actions:
   - To enable or disable the WLAN for an entire day, click the day of the week under the **Time** column.
   - To enable or disable the WLAN for specific housr of a specific day, select the squares in the table. A single square represents 30 minutes (two 15-minute blocks).

     Blue-colored cells indicate the hours when the WLAN is enabled. Clear (or white) cells indicate the hours when the WLAN is disabled.
9. Click Ok. The schedule is submitted and the schedule name is displayed.

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 16 WLAN Templates: Contextual Tabs

Tab	Description
General	Displays details of the respective WLAN template.
WLAN	Displays details of the respective WLAN. You can create or configure a WLAN. Refer to *Creating a WLAN Configuration*.
Hotspots and Portals	Displays details of the respective hotspots and portals. Refer to *Working with Hotspots and Portals*.
Access Control	Displays details of the respective access control. Refer to *Configuring Access Control*.
Authentication and Accounting	Displays details of the respective authentication and accounting servers. Refer to *Authentication* and *Accounting* respectively.
Tunnels & Ports	Displays details of the respective tunnels and ports. Refer to *Working with Tunnels and Ports*.
Radius	Displays details of the respective VSA profiles. You can create or configure a VSA profile. Refer to *Creating a Vendor-Specific Attribute Profile*.

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 Firmware**.

6. Choose the **AP IP Mode**.
7. Select **AP SoftGRE Tunnel** to enable all WLANs defined in this template to tunnel traffic to SoftGRE through the AP.
8. Click **OK**.

NOTE
You can select a WLAN and edit, clone or delete its template by selecting the options **Configure**, **Clone** or **Delete** respectively.

Applying a WLAN Template

You can apply the WLAN template to zones where the AP's firmware version is later than the Zone templates firmware version. An unsupported firmware version of the WLAN template is automatically upgraded to its next version before being upgraded to the current version.

To Apply a WLAN template to a zone:

1. Go to **Administration** > **System** > **Templates** > **WLAN Templates**.
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.

How Dynamic VLAN Works

Dynamic VLAN can be used to automatically and dynamically assign wireless clients to different VLANs based on RADIUS attributes.

Dynamic VLAN Requirements:

- A RADIUS server must have already been added to the controller
- WLAN authentication method must be set to 802.1X, MAC address or 802.1X + MAC address

To enable Dynamic VLAN for a WLAN:

1. Go to **Network** > **Wireless** > **Wireless LANs**.
2. Click **Configure** for to the WLAN you want to configure.
3. In **Authentication Server**, select the AAA profile.
4. Expand the **Advanced Settings** section and click the**Enable Dynamic VLAN box** next to Access VLAN.

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

FIGURE 15 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 17 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.

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 129: Bridges Bonjour services from one VLAN to another.
- Bonjour Fencing on page 131: 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.

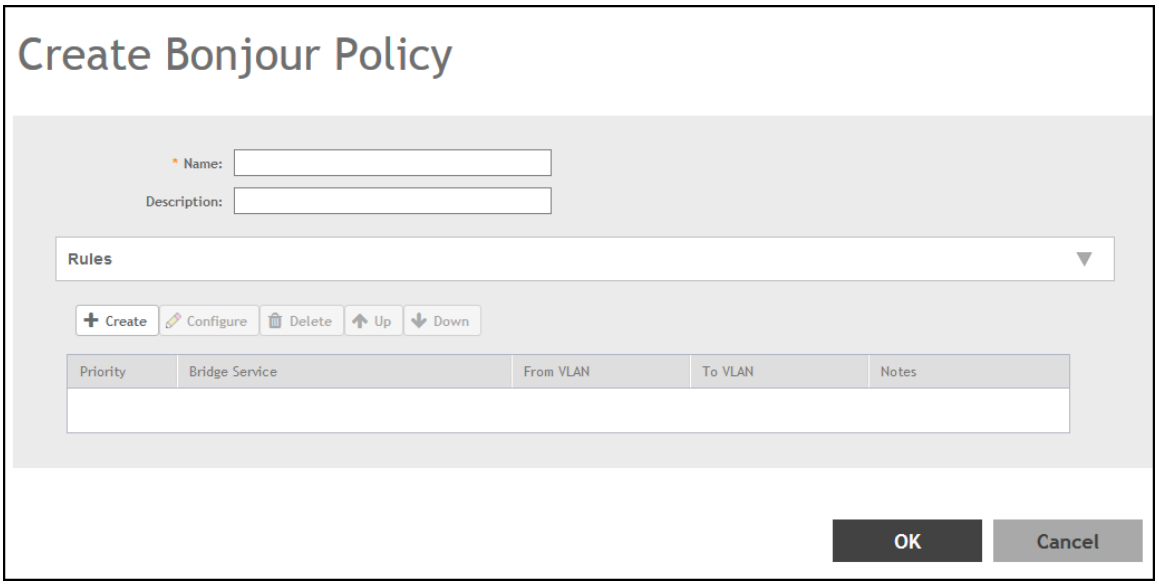
Complete the following steps to create a Bonjour Gateway policy.

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 16 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 131.

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.

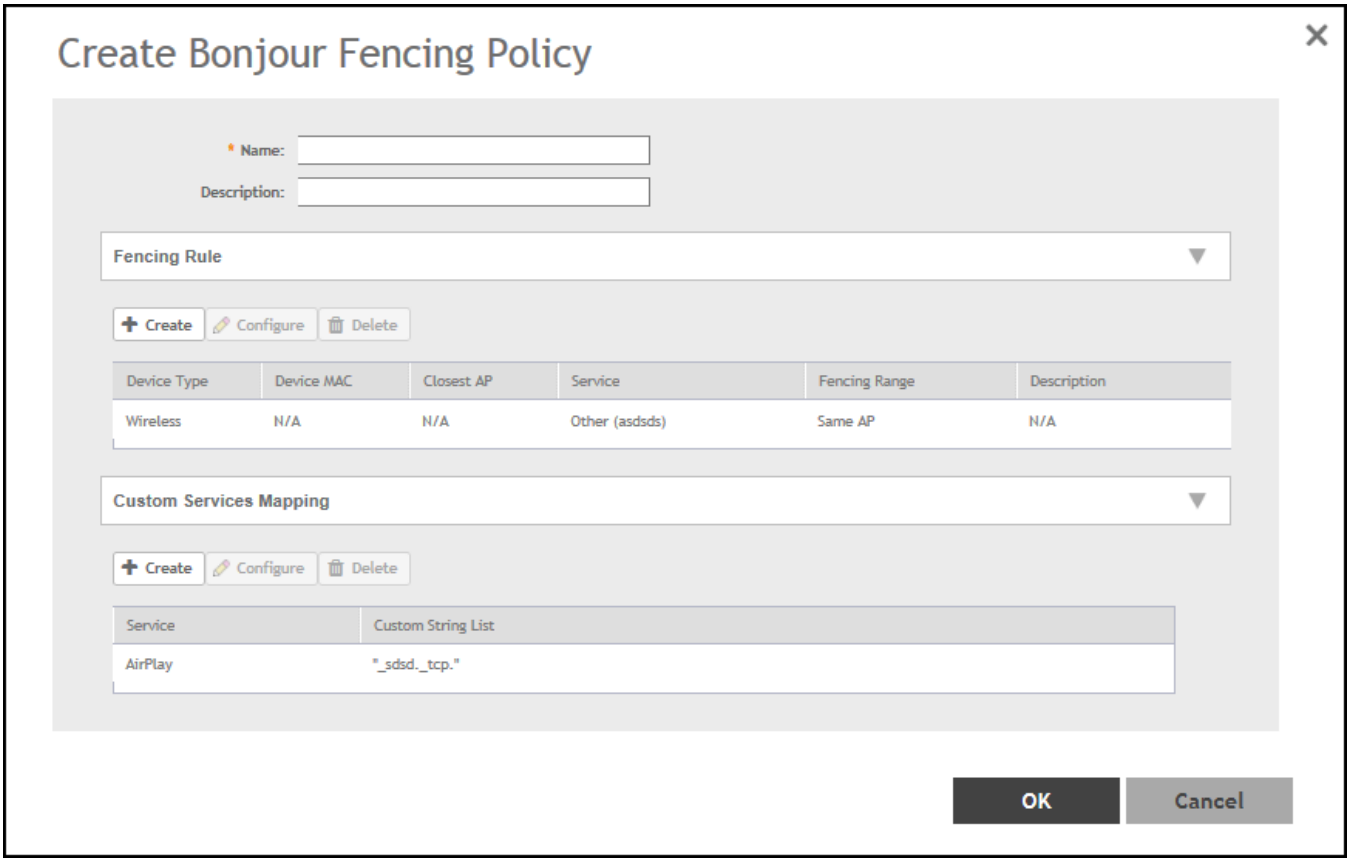
NOTE
Bonjour Fencing for a particular service does not work if another service from the same server, which is not fenced, is enabled simultaneously.

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.

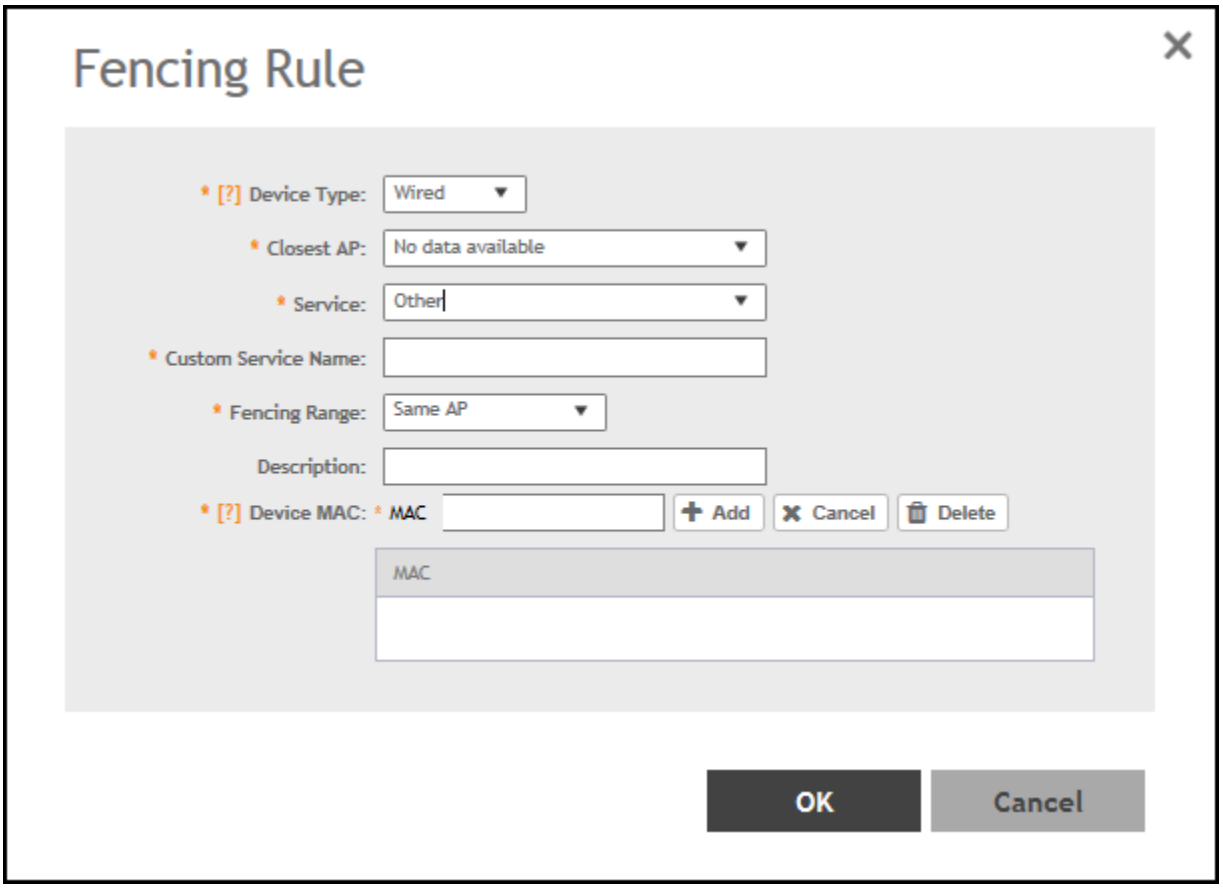
FIGURE 17 Creating a Bonjour Fencing Policy



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 18 Creating a Fencing Rule



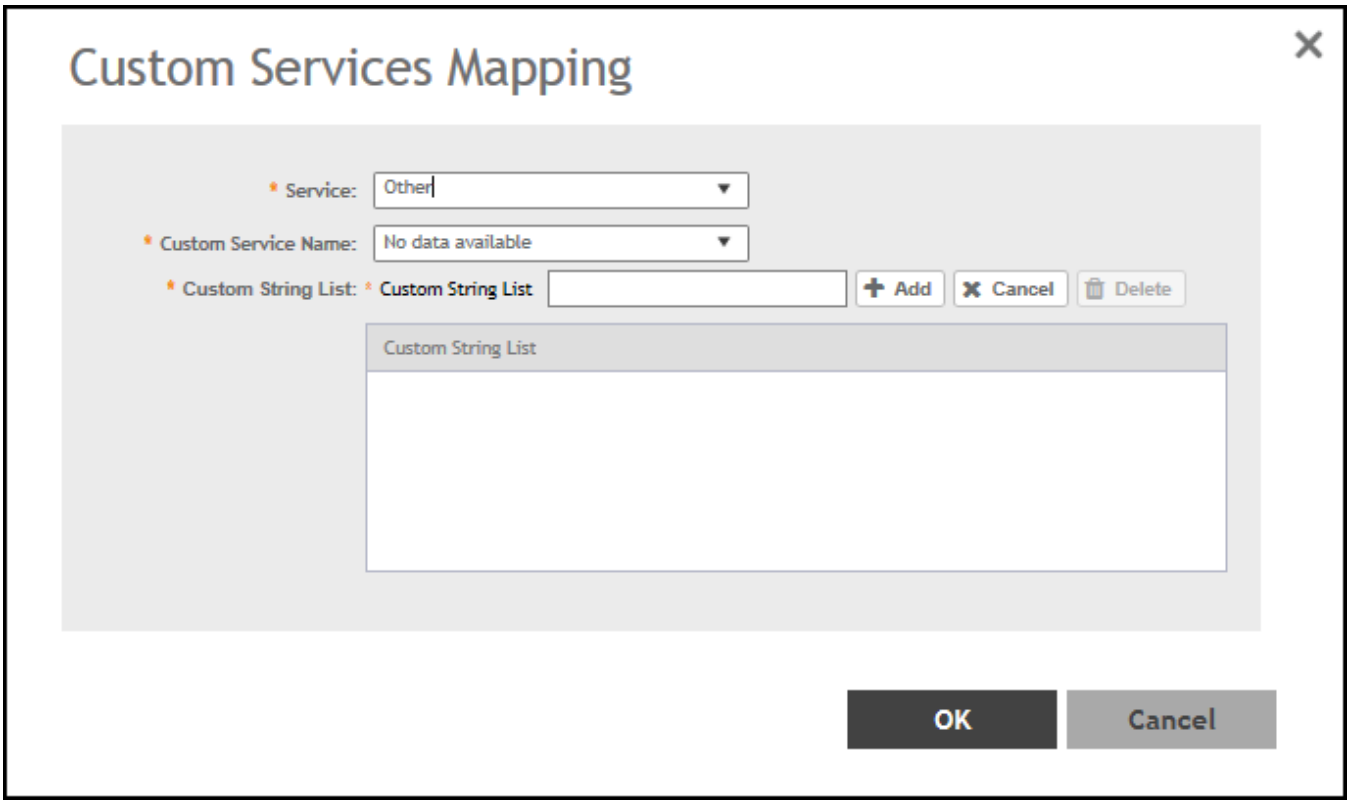
6. Configure the following options:
   - **Device Type**: Select **Wireless** or **Wired** network connection method for the device advertising Bonjour services.
   - **Closest AP**: Select the closest AP to create a physical anchor point for fencing; the closest AP is auto-detected for wireless devices, 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 19 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.

Northbound Data Streaming

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

Configuring Northbound Data Streaming Settings

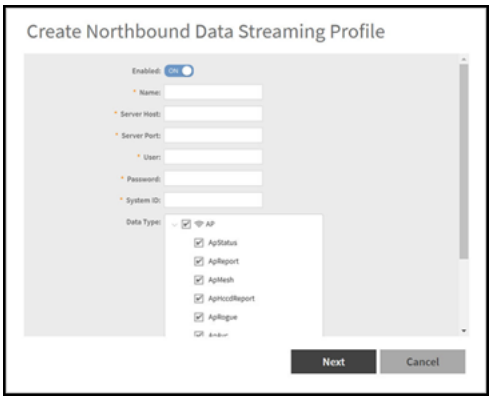
Configuring the Northbound Data Streaming settings in the controller enables data transfer from the controller to the Northbound Data Streaming server using the Message Queuing Telemetry Transport (MQTT) protocol.

NOTE
You can create a maximum of two SCI profiles simultaneously.

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

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

FIGURE 20 Creating a Northbound Data Streaming Profile

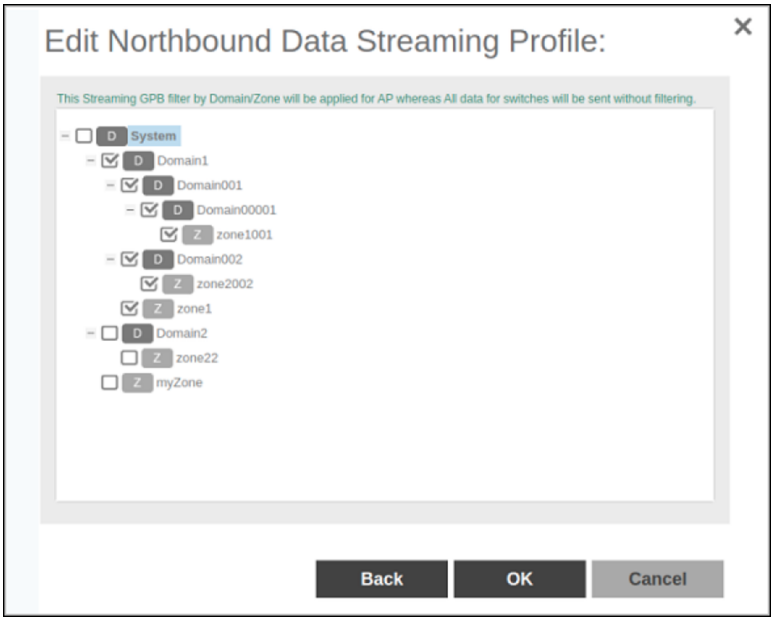


3. Complete the following options:
   - **Enabled**: Set to **ON** to configure the Northbound Data Streaming profile.
   - **Name**: Enter the profile name.
   - **Server Host**: Enter the IP address of the Northbound Data Streaming host server.

     NOTE
     An SCI profile supports only the IPv4 format.

   - **Server Port**: Enter the port number using which the Northbound Data Streaming server and the controller can communicate and transfer data. The ports must be allowed on the firewall.
   - **User**: Enter the name of the user.
   - **Password**: Enter the password for the user.
   - **System ID**: Enter the ID of the Northbound Data Streaming system to access.
   - **Data Type**: Select the required options for the specific data types that must be sent to the Northbound Data Streaming server from the SCI server.
4. Click **Next**.
5. For APs, from the **System** tree, select the required domain or zone to send KPIs or statistics to the Northbound Data Streaming server. For switches, KPIs or the statistics are sent to SCI or Northbound Data Streaming server without filtering.

FIGURE 21 Selecting the Zone or Domain



6. Click **OK**.

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

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

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

Setting the Northbound Portal Password

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

Complete the following steps to configure the northbound portal interface.

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

Dynamic PSK

Dynamic PSKs (DPSKs) are unique PSKs per user or device. You can create or import new DPSKs or view the existing DPSKs on the system.

Generating Dynamic PSKs

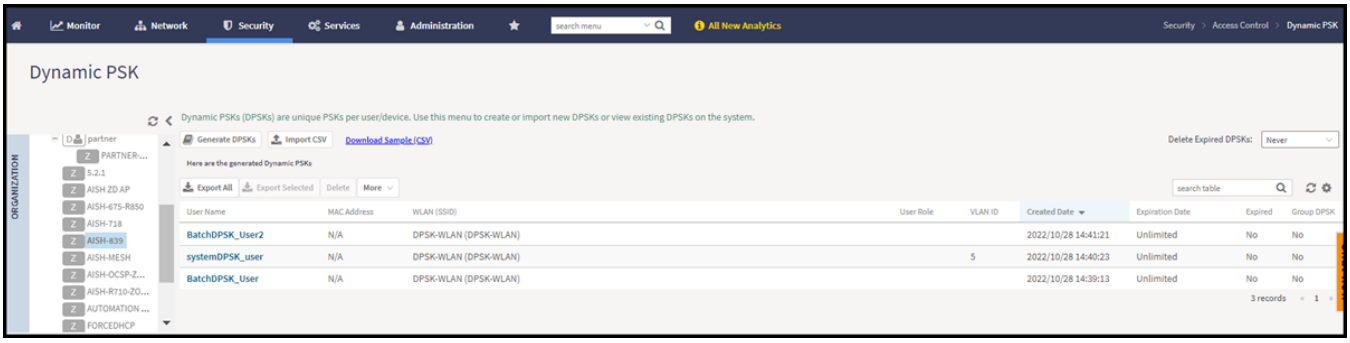
You can generate new dynamic pre-shared keys (PSKs) to secure the Wi-Fi network.

Complete the following steps to generate dynamic PSKs.

1. From the main menu, go to **Security** > **Access Control** > **Dynamic PSK**. The **Dynamic PSK** page is displayed.
2. Click **Generate DPSKs**.

   The **Generate DPSKs** dialog box is displayed.

   FIGURE 22 Dynamic PSK Page



3. Configure the following options:
   - **WLAN**: Select a DPSK-enabled WLAN from the list.
   - **Number of DPSKs**: Enter the number of DPSKs to be created in a zone. A maximum of 500 Unbound or Group DPSKs can be created in one form submission.

     There are three types of DPSKs:

     - Unbound DPSK (DPSK not binding to a specific device yet): Once an unbound DPSK is used by a device, it becomes a bound DPSK and releases one slot from the maximum limit of 500.
     - Group DPSK (DPSK that can be shared between devices): A group DPSK never becomes bound; it always occupies one slot of the 500 limit until deleted by the administrator.
     - Bound DPSK (DPSK bound to a specific device): An administrator can import bound DPSKs using a CSV file by specifying the MAC Address and create bound DPSKs regardless of the 25,000 limitation.

     TABLE 18 Maximum DPSK per zone

Controller version	Max DPSK per zone	Max Unbound DPSK per zone	Max Group DPSK per zone
3.4.x	10000	256	X

TABLE 18 Maximum DPSK per zone (continued)

Controller version	Max DPSK per zone	Max Unbound DPSK per zone	Max Group DPSK per zone
3.5.x	10000	256	64
3.6.x	10000	Share 320 slots for Unbound and Group DPSKs	
5.1	25000	Share 500 slots for Unbound and Group DPSKs	
6.1.0	25000	Share 5,000 slots for Unbound and Group DPSKs	

NOTE
For the SZ300/vSZ-H platform, the maximum number of DPSKs is 25,000 per zone or domain and 50,000 for the system.

- **User Name**: Enter a user name or leave it blank if you want the controller to auto-generate the user name.
- **Passphrase**: Enter a passphrase or leave it blank if you want the controller to auto-generate the passphrase.
- **User Role**: If you have created user roles, select the user role to assign to the device that connects to the controller network using this DPSK. The device will be assigned the same attributes and permissions (VLAN, UTP, time restrictions, and so on) that have been defined for the assigned user role.
- **VLAN ID**: Enter a VLAN ID within the range 1 through 4094.
- **Group DPSK**: Click **Yes** if you want multiple devices to be able to use this DPSK or click **No** if it is to be used by a single device.

4. Click **Generate**.

To delete a DPSK, select the DPSK from the list, and click the **Delete** icon.

Importing Dynamic PSKs

You can import CSV files to create DPSKs to secure the Wi-Fi network.

Follow these steps to import dynamic PSKs (DPSKs):

1. Click **Security** > **Access Control** > **Dynamic PSK**. This displays **Dynamic PSK**screen.
2. Click **Download Sample (CSV)** to download the CSV template for generating DPSKs.

   The following figure shows a sample CSV file.

FIGURE 23 Sample CSV File

A	B	C	D	E	F
User Name	MAC Address	VLAN ID	User Role	Passphrase	Group DPSK
DPSK-User-1	00:11:22:33:44:44				
DPSK-User-2	00:11:22:33:44:55	1		passphrase02	
DPSK-User-3	11:22:33:44:55:66	2	testUserRole	passphrase03	
Group-DPSK-1					Y

3. Modify the CSV file as appropriate and save it. The following fields must be completed in the CSV file:
   - **User Name**: (Mandatory) Enter the user name.
   - **MAC Address**: (Optional) Enterthe MAC address of the device for which to generate a DPSK (bound DPSK). If you leave the **MAC Address** field empty, the controller will generate an unbound DPSK.
   - **VLAN ID**: (Optional) Enter a value to overwrite the WLAN VLAN ID, or leave it empty if you do not want to overwrite the WLAN VLAN ID.
   - **User Role**: (Optional) If you have created user roles, enter the name of the user role that you want to assign to the device that connects to the controller network using this DPSK. The device will be assigned the same attributes and permissions (VLAN, UTP, time restrictions, and so on) that have been defined for the assigned user role.
   - **Passphrase**: (Optional) Enter a passphrase or leave it blank if you want the controller to auto-generate the passphrase.
   - **Group DPSK**: (Optional) Enter **Y** to indicate the entry is a Group DPSK if you want multiple devices to use this DPSK.
4. Click **Import CSV**.

   The **Import CSV** dialog box is displayed.

   NOTE
   Importing a CSV file that contains a MAC address to which an existing DPSK (on the same target WLAN) is already assigned will replace the existing DPSK on the controller database.

5. From the **DPSK Enabled WLAN**, select a WLAN. Only WLANs that support DPSK must be selected.
6. For **Choose File**, click **Browse** to choose the CSV file (or click **Clear** if you want to replace the CSV file).

   You can also specify **Group DPSK** in the CSV file.
7. Click **Upload**.

   The generated DPSKs are displayed on the **Dynamic PSK** page.

   NOTE
   You can import up to 1,000 DPSKs (not over 25K unbound + group DPSKs) at a time.

8. Click **Download CSV** to download a CSV that contains the generated DPSKs.

   The CSV file is displayed in the format shown in the following figure.

FIGURE 24 New CSV Format

User Name	MAC	WLAN (SSID)	Passphrase	VLAN ID	Created Date	Expiration Date
DPSK-User-1	00:11:22:33:44:44	joe-wlan (joe-wlan)	4#4BSXMe		3/17/2016 18:55	Unlimited
DPSK-User-2	00:11:22:33:44:55	joe-wlan (joe-wlan)	rE<r0[]y	1	3/17/2016 18:55	Unlimited
DPSK-User-3	11:22:33:44:55:66	joe-wlan (joe-wlan)	'q=7vqfE	2	3/17/2016 18:55	Unlimited

NOTE
Click **Export All** to export all the dynamic PSKs to a CSV file. You can also export specific dynamic PSKs by selected them and clicking **Export Selected**.

Viewing Generated DPSKs

In addition to downloading the generated DPSK record in CSV format, you can also view the DPSKs that have been generated from the **Generated Dynamic PSKs** tab.

Printing a QR Code

A WLAN-supported DPSK has the **Show QR Code** option in the **Generated Dynamic PSKs** tab to join a Wi-Fi network.

Click **Show QR Code** and the **QR Code** page is displayed. Click **Print** to print the QR code or scan the QR code using a smartphone camera.

FIGURE 25 QR Code Page

Click **Export to CSV** option to export all the generated DPSKs to a CSV file.

Location Services

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

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

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

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

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

   FIGURE 26 Creating a Location-Based Server

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

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

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

   NOTE
   The default port number is 8883.

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

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

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

350 West Java Dr., Sunnyvale, CA 94089 USA
https://www.commscope.com