CONFIGURATION GUIDE

RUCKUS SmartZone (ST-GA) AP Management Guide, 7.0.0

Supporting SmartZone Release 7.0.0

Part Number: 800-73362-001 Rev A
Publication Date: February 2024

Export Restrictions

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

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

Disclaimer

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

Limitation of Liability

IN NO EVENT SHALL COMMSCOPE, COMMSCOPE AFFILIATES, OR THEIR OFFICERS, DIRECTORS, EMPLOYEES, AGENTS, SUPPLIERS, LICENSORS AND THIRD PARTY PARTNERS, BE LIABLE FOR ANY DIRECT, INDIRECT, SPECIAL, PUNITIVE, INCIDENTAL, EXEMPLARY OR CONSEQUENTIAL DAMAGES, OR ANY DAMAGES WHATSOEVER, EVEN IF COMMSCOPE HAS BEEN PREVIOUSLY ADVISED OF THE POSSIBILITY OF SUCH DAMAGES, WHETHER IN AN ACTION UNDER CONTRACT, TORT, OR ANY OTHER THEORY ARISING FROM YOUR ACCESS TO, OR USE OF, THE MATERIALS. Because some jurisdictions do not allow limitations on how long an implied warranty lasts, or the exclusion or limitation of liability for consequential or incidental damages, some of the above limitations may not apply to you.

Trademarks

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

Patent Marking Notice

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

Contents

Contact Information, Resources, and Conventions

Contacting RUCKUS Customer Services and Support

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

New In This Document

TABLE 2 Key Features and Enhancements in *SmartZone 7.0.0 Rev A* (*February 2024*)

Feature	Description	Reference
Hide cellular options	**Removed**: The support for **Cellular Options** is removed.	-
Rehoming managed APs	**New Feature**: Allows the APs to fail back to the source active cluster automatically in an Active-Active cluster deployment.	Rehoming Managed APs on page 63
[R770] :320 Mhz AP Support	**Updated**: Provides 320 MHz channel support for the R770 AP.	Creating an AP Zone on page 141
Limit outdoor AP channelization as 20 MHz in Indonesia.	**New Feature**: Limits the **Channelization** width to 20 MHz for country Indonesia.	• Configuring Access Points on page 69 • Creating an AP Group on page 21 • Creating an AP Zone on page 141
Channelfly as default for all radios and channelization defaults to 40 Mhz for Auto	**Updated**: Channelfly is set as the default mode for all radio frequency and the default value for 5GHz channelization is set to 40 MHz.	• Configuring Access Points on page 69 • Creating an AP Group on page 21 • Creating an AP Zone on page 141
Secure Boot	**New Feature**: The feature allows the implementation of secured boot process.	• Secure Boot on page 94 • Viewing General AP Information on page 93
Energy Efficient Ethernet (EEE)	**New Feature**: Reduce power consumption in APs and switches when there is low data activity or when the network is idle.	Energy Efficient Ethernet (EEE) on page 19
RUCKUS NOR Certificate Safe Storage (RNCSS) Support	**New Feature**: Stores and retrieves the device certificate and key from the NOR flash memory of an AP when the certificate and key is lost or corrupted.	RUCKUS NOR Certificate Safe Storage (RNCSS) Support on page 185
LPI (Low Power Indoor) Mode	**Removed**: The support for LPI mode is removed.	-
M510 AP	**Removed**: The support for M510 AP is removed.	-

AP Ethernet Ports

Creating an Ethernet Port Profile

An Ethernet port profile contains settings that define how an AP will handle VLAN packets when its port is designated as a trunk, access, or general port. By default, three Ethernet port profiles exist: General Port, Access Port, and Trunk Port.

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

1. From the main menu go to **Services** > **Tunnels and Ports**.
2. Select the **Ethernet Port** tab, and then select the zone for which you want to create the profile.
3. Click **Create**.

   The **Create Ethernet Port** page is displayed.

4. Configure the following options:
   - General Options
     - Name: Enter a name for the Ethernet port profile that you are creating.
     - Description: Enter a short description about the profile.
     - Type: The Ethernet port type defines how the AP will manage VLAN frames. You can set Ethernet ports on an AP to one of the following types: Trunk Port, Access Port, or General Port. By selecting the appropriate port type, authentication method, and 802.1X role, you can configure the Ethernet ports to be used for the wired client. If you select a non-user port, there is no restriction on the number of clients supported. If the User Side Port is selected, the maximum number of supported clients is 32 and this number is configurable.
   - Ethernet Port Usage
     - Access Network:
       - Default WAN: Enables default WAN configuration
       - Local Subnet(LAN): Enables DHCP service on ethernet ports. In the **VLAN Options**, select the **VLAN Untag ID** in the ethernet profile which is similar to the DHCP NAT VLAN ID.
       - Tunnel Ethernet Port Profile: Enables tunneling on the ethernet port
     - Anti-spoofing: Prevents attacks on genuine clients from rogue clients that could lead to service disruption, data loss, and so on. This is achieved by matching the MAC address or IP address (IPv4) of the client with the address in the RUCKUS database. If the addresses do not match, the packet is dropped. These checks are also performed on ingress data packets to catch spoofed data packets early.
       - ARP request rate limit: The Address Resolution Protocol (ARP) limits the rate of ARP requests from the connected clients to prevent ARP flooding. Enter the number of packets to be reviewed for ARP attacks per minute. In ARP attacks, a rogue client sends messages to a genuine client to establish connection over the network.
       - DHCP request rate limit: The DHCP request limits the rate of DHCP requests from the connected clients to prevent DHCP flooding. Enter the number of packets to be reviewed for DHCP pool exhaustion, per minute. When rogue clients send a DHCP request with a spoofed address, an IP address from the DHCP pool is assigned to it. If this happens repeatedly, the IP addresses in the DHCP pool are exhausted, and genuine clients may miss out on obtaining the IP addresses.

         NOTE
         When you enable anti-spoofing, an ARP request rate limiter and a DHCP request rate limiter are automatically enabled with default values (in packets per minute) which are applied per client; implying that each client connected to an interface enabled with anti-spoofing is allowed to send a maximum of "X" ARP and DHCP request packets per minute (ppm). The "X" value is configured on the interface to which the client is connected.
     - User Side Port: User Side Port is by default enabled when 802.1x is enabled.
       - Number of clients allowed to be connected: Enter the number of clients that can be connected to the User Side Port. The maximum number of clients that can be connected is 32.
   - Wired Client Isolation
     - Client Isolation: Prevents wired clients from communicating with each other. This option isolates wired client traffic from all hosts on the same VLAN/subnet. By default, this option is disabled. Enable the following options as approriate:
       - Isolate unicast packets: Isolates only unicast packets between a wired client enabled with client isolation and other clients of the AP. By default, this option is enabled.
       - Isolate multicast/broadcast packets: Isolates only multicast/broadcast packets between a wired client enabled with client isolation and other clients of the AP. By default, this option is disabled.
       - Automatic support for VRRP: Isolates packets in Virtual Router Redundancy Protocol (VRRP) deployment. By default, this option is disabled indicating the AP is not in VRRP deployment.

VIDEO

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

Click to play video in full screen mode.

- Authentication Options
  - 802.1X: Select to enable 802.1X authentication.
  - 802.1X Role: Select the authenticator role from the menu.
    - Supplicant: You can customize the user name and password to authenticate as a supplicant role or use the credentials of the AP MAC address.
    - MAC-based Authenticator: Each MAC address host is individually authenticated. Each newly learned MAC address triggers an Extensible Authentication Protocol over LAN (EAPoL) request-identify frame.
    - Port-based Authenticator: Only a single MAC address host must be authenticated for all hosts to be granted access to the network.
  - Enable client visibility regardless of 802.1X authentication: If client visibility is enabled, you can view connected wired client information. Client visibility is enabled by default if the 802.1x authentication method is selected. For the open authentication method, you must enable client visibility based on your requirements.

    NOTE
    You can view statistical information about wired clients without enabling 802.1X authentication.

- Supplicant: Select the authentication type
  - MAC Address: Select this option to use the AP MAC address as the username and password.
  - Custom: Enter customized Username and Password to authenticate.
- VLAN Options
  - VLAN Untag ID: Enter the ID of the native VLAN (typically 1), which is the VLAN into which untagged ingress packets are placed upon arrival. If your network uses a different VLAN as the native VLAN, configure the VLAN Untag ID of the AP Trunk port with the native VLAN used throughout your network. If **Local Subnet** option is selected in **Ethernet Port Usage**, then VLAN ID configured should be the same as one of DHCP NAT VLANs.
  - VLAN Members: Enter the VLAN IDs that you want to use to tag WLAN traffic that will use this profile. You can enter a single VLAN ID or a VLAN ID range (or a combination of both). The valid VLAN ID range is from 1 through 4094. If **Local Subnet** option is selected in **Ethernet Port Usage**, then only DHCP NAT VLANs are allowed on trunk port.
  - Enable Dynamic VLAN: Select this check box if you want the controller to assign VLAN IDs on a per-user basis. Before enabling dynamic VLAN, you must define on the RADIUS server the VLAN IDs that you want to assign to users.

    NOTE
    The Enable Dynamic VLAN option is only available when the Type is set to Access Port and 802.1X authentication is set to MAC-based Authenticator.

NOTE
If you enable client visibility, a maximum of 16 clients can be connected to a port regardless of the 802.1X authentication. The same limitation applies when 802.1X authentication is enabled and client visibility is not enabled.

- Guest VLAN: Select this option if you want to limit the device access to internal network resources only.
- QinQ VLAN: Select the check box and update the ranges:
  - QinQ SVLAN Range: Enter a SVLAN range. The range is 2 through 4095.
  - QinQ CVLAN Range: Enter a CVLAN range. The range is 2 through 4095.

NOTE
For QinQ VLAN to work:
- Port Type: Must be Access Port
- Access Network: Must be Tunnel Ethernet Port traffic
- 802.1x Role: Enabled with Mac Based
- DVLAN: Enabled
- Q in Q (Client Visibility and User Side Port are by default enabled): Enabled

- Authentication and Accounting Services
  - Authentication Server: Select the check box and a controller from the menu to use the controller as a proxy authentication server.
  - Accounting Server: Select the check box and a controller from the menu to use the controller as a proxy accounting server.
  - Enable MAC authentication bypass: Select this check box if you want to use the device MAC address as access credentials (user name and password).
- RADIUS Options
  - NAS ID: Set the NAS ID for the AP to communicate with the RADIUS server. Options include using the AP MAC address or any user-defined address.
  - Delimiter: If the AP MAC address is selected to configure the NAS ID, then you can choose between Dash or Colon as delimiters to separate.
- Firewall Options

NOTE
The User Side Port must be enabled to configure the Firewall Profile, Application Recognition and Control, and URL Filtering Policy.

NOTE
While mapping group attribute values to the user role, avoid special characters or duplicate entries regardless of the order.

  - Firewall Profile: Select the firewall profile for wired ports.
  - Application Recognition and Control: Enable the option for the wired clients.
  - URL Filtering Policy: Enable the option for wired clients.
  - L2 Access Control Policy: Select the Layer 2 policy for wired ports. When the User Side Port is not enabled, a Layer 2 Access Control wired support policy can be mapped directly to the wired port. If the User Side Port is enabled, the Layer 2 Access Control wired support policy can be mapped to the wired port of the firewall profile. Click  to create a new policy. Refer to the **Creating a L2 Access Control Service** section of the *SmartZone Security Guide (SZ300/vSZ-H)* for more information.
- Click **OK**.

NOTE
You can edit, copy, or delete the profile by selecting the options **Configure**, **Clone**, or **Delete**, respectively, from the **Ethernet Port** tab.

VIDEO
Creating Ethernet Port Profiles. Creating an Ethernet port profile (securing secondary wired port), port types explained

Click to play video in full screen mode.

Designating an Ethernet Port Type

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

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

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

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

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

- Segment all ingress traffic on this Access Port to a specific VLAN.
- Redefine the native VLAN on this Trunk Port to match your network configuration.

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

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

Access Ports

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

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

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

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

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

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

TABLE 3 Access Ports with VLANs Configured

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

Trunk Ports

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

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

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

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

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

General Ports

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

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

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

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

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

Energy Efficient Ethernet (EEE)

The Energy Efficient Ethernet (EEE) feature is designed to minimize power usage in APs and switches during periods of low data activity or when the network is idle. It follows the IEEE 802.3az standard for energy efficiency. This helps reduce power consumption, heat dissipation, and noise.

Using the RUCKUS AP CLI, you can enable or disable the EEE feature in one or both the Ethernet ports of an AP.

This EEE feature is disabled by default. To can enable or disable EEE on an AP:

```
rkscli: set eee <ifname> {enable|disable}
```

- `<ifname>`: Ethernet ports, eth0/eth1.
- `enable`: Use this option to enable EEE on the specified interface.
- `disable`: Use this option to disable EEE on the specified interface.

To view the output when EEE is enabled on both the ports of the AP:

```
Please login: admin
password :
Copyright(C) 2024 Ruckus Wireless, Inc. All Rights Reserved.

** Ruckus R760 Multimedia Hotzone Wireless AP: 352202007605

rkscli: get eee

Interface  EEE
-----------------
eth0       Disabled
eth1       Disabled
OK
rkscli:
rkscli: set eee eth1 enable
OK
rkscli:
rkscli: get eee

Interface  EEE
-----------------
eth0       Disabled
eth1       Enabled
OK
rkscli: set eee eth0 enable
OK
rkscli: get eee

Interface  EEE
-----------------
eth0       Enabled
eth1       Enabled
OK
rkscli:
```

By default, the EEE feature is disabled in the RUCKUS ICX Switch regardless of the switch model. Using the RUCKUS ICX Switch CLI, you can enable or disable the EEE feature on the switch either at the global configuration level or at the port level. In Global Configuration mode, you can enable or disable EEE on a RUCKUS ICX switch by entering the **eee** or **no eee** command, respectively.

To view the EEE status for all ports on the ICX switch when EEE is enabled, enter:

```
show eee-statistics
```

Energy Efficient Ethernet (EEE)

This command displays, for each Ethernet port on the ICX switch, the EEE state (enabled or disabled), and whether the port has received low power idle signaling (0 [no] or 1 [yes]).

```
telnet@ICX8200-24ZP Router#show eee-statistics

Port    EEE-State   RxLpIdleReceived   TxLpIdleReceived

1/1/1   Enable          0                 0
1/1/2   Enable          0                 0
1/1/3   Enable          0                 0
1/1/4   Enable          0                 0
1/1/5   Enable          0                 0
1/1/6   Enable          0                 0
1/1/7   Enable          0                 0
1/1/8   Enable          0                 0
1/1/9   Enable          0                 0
1/1/10  Enable          0                 0
1/1/11  Enable          0                 0
1/1/12  Enable          0                 0
1/1/13  Enable          1                 1
1/1/14  Enable          0                 0
1/1/15  Enable          0                 0
1/1/16  Enable          0                 0
1/1/17  Enable          0                 0
1/1/18  Enable          0                 0
1/1/19  Enable          0                 0
1/1/20  Enable          0                 0
1/1/21  Enable          0                 0
1/1/22  Enable          0                 0
1/1/23  Enable          0                 0
1/1/24  Enable          0                 0
telnet@ICX8200-24ZP Router#
```

AP Groups

Creating an AP Group

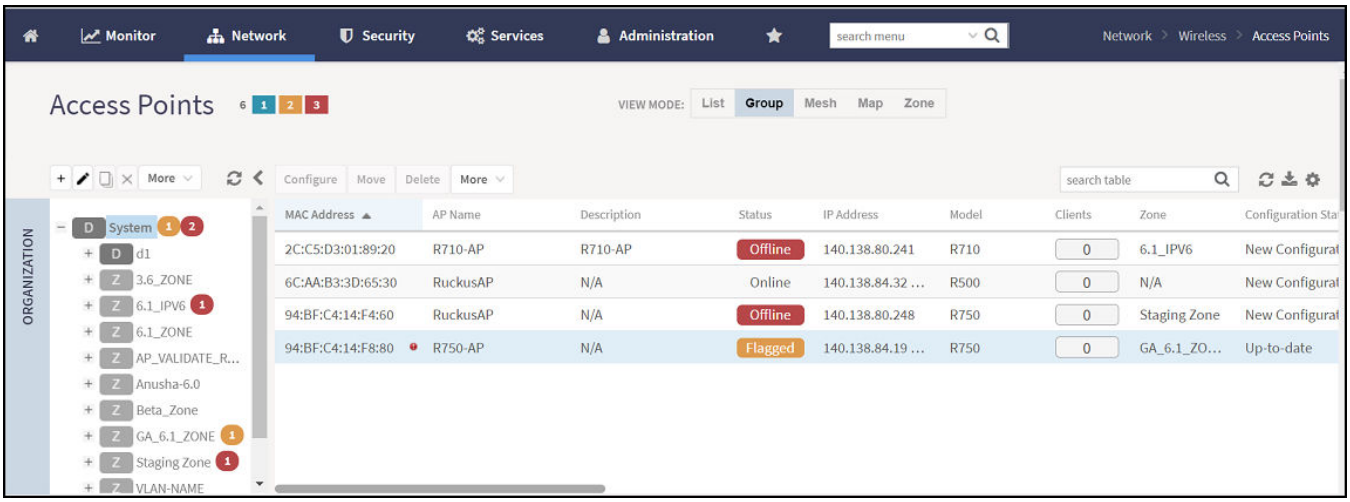
By creating an AP group, you can configure a profile that defines the channels, radio settings, Ethernet ports and other configurable fields for all members of the group or for all APs of a specific model in the group.

To create an AP Group, perform the following:

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

   This displays **Access Points** page.

   FIGURE 1 Access Point Page



2. From the System tree hierarchy, select the zone and click . The **Create AP Group** page is displayed.
3. Enter the details as explained in the following table.

   NOTE

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

4. Click **OK**.

TABLE 4 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

TABLE 4 AP Group Details (continued)

Field	Description	Your Action
Type	Indicates if you are creating a domain, zone or an AP group.	Appears by default. You can also choose the option.
Parent Group	Indicates the parent group that this AP group belongs.	Appears by default.
General Options		
Location	Indicates generic location.	Enter the location.
Location Additional Information	Indicates detailed location.	Enter additional location information.
GPS Coordinates	Indicates the geographical location.	Enter the following coordinates in meters or floor: • **Longitude** • **Latitude** • **Altitude**
Radio Options		
Dual-5G Mode	Enables third radio operator in 2.4 GHz, Lower 5 GHz, and Upper 5 GHz. By default, the **Dual-5G Mode** is enabled. In the enabled mode, radio-0 will be on 2.4GHz band, radio-1 will be on 5G Lower band and radio-2 will be on 5G Upper band. • 5G Lower BAND : UNII-1, UNII-2A • 5G Upper BAND : UNII-2C, UNII-3 In the disabled mode, the radio-0 will be on 2.4GHz band, radio-1 will be on 5G band and radio-2 will be on 6G band. This also depends on the country code.	Select or keep the default **Dual-5G Mode** option.
Band/Spectrum Configuration > 2.4 GHz		
Channelization	Helps manage and allocate radio frequency resources. A lower channel width allows the zone to potentially serve more clients, whereas a higher channel width improves throughput, but potentially serves fewer clients and increases the possibility of interference. The Auto setting defaults to 20 MHz channelization.	Set the channel bandwidth used during transmission to either 20 or 40 (MHz), or select Auto to set it automatically. **NOTE** By default, for the **Country Code** Indonesia, the **Channelization** width is set to 20 MHz only for outdoor APs.
Channel	Indicates the channel to use.	Select one of the options: Auto, 1, 6 or 11.
Auto Cell Sizing	Enables the AP to share information on interference seen by each other and dynamically adjust their radio Tx power and Rx parameters to minimize interference. Enabling this option disables the TX Power Adjustment configuration. **NOTE** Ensure that Background Scan is enabled.	Select the option.

TABLE 4 AP Group Details (continued)

Field	Description	Your Action
TX Power Adjustment	Allows to manually configure the transmit power on the 2.4 GHz radio. By default, the TX power is set to Full on the 2.4 GHz radio. **NOTE** If you choose Min, the transmit power is set to 0dBm (1mW) per chain for 11n APs, and 2dBm per chain for 11ac APs. If you choose Max, the transmit power is set to the maximum allowable value according to the AP's capability and the operating country's regulations.	Select the preferred TX power.
Protection Mode	Indicates the mechanism to reduce frame collision.	Choose one of the following options: • None • RTS/CTS • CTS Only
Background Scan	Allows the AP radio to scan other channels in the band for accessing channel health and capacity, detecting rogue devices, optimizing and maintaining mesh links and to discover AP neighbors.	Enter the duration in seconds. Range: 1 through 65535.
Auto Channel Selection	Automatically adjusts the channel for network self-healing and performance optimization. **ChannelFly** is set as the default option. For the **ChannelFly** option, you may also modify the default settings for the **Channel Change Frequency** and **Full Optimization Period**. The **Channel Change Frequency** slidebar allows you to specify the responsiveness of ChannelFly to interference (with consideration for the impact on associated clients), ranging from Minimal to Very Often. The **Full Optimization Period** timeslot bar allows you to specify one or more periods of time when ChannelFly is allowed to fully optimize the channel plan, ignoring the impact of channel changes on associated clients. Select time periods when the wireless network is servicing the fewest clients.	Select the required option. • **Background Scanning**: Changes the AP channel when there is an interference. • **ChannelFly**: Monitors potential throughput and will change channels to learn each channel's capacity, optimize throughput, and to avoid interference.
Band/Spectrum Configuration > 5 GHz		
Channelization	Helps manage and allocate radio frequency resources. A lower channel width allows the zone to potentially serve more clients, whereas a higher channel width improves throughput, but potentially serves fewer clients and increases the possibility of interference. Prior to SmartZone release 7.0.0, the Auto setting defaulted to 80 MHz channelization. Beginning in SmartZone release 7.0.0, the Auto setting defaults to 40 MHz channelization.	Set the channel bandwidth used during transmission: Auto, 20, 40, 80 and 160. **NOTE** By default, for the **Country Code** Indonesia, the **Channelization** width is set to 20 MHz only for outdoor APs.
Channel	Indicates the channel to use.	Select the required options for the Indoor and Outdoor APs.
Secondary Channel	Indicates the secondary channel to used.	By default, the Indoor and Outdoor option is set to Auto.
Allow DFS Channels	Allows ZoneFlex APs to use DFS channels.	Click to enable the option.

TABLE 4 AP Group Details (continued)

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

TABLE 4 AP Group Details (continued)

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

TABLE 4 AP Group Details (continued)

Field	Description	Your Action
Background Scan	Allows the AP radio to scan other channels in the band for accessing channel health and capacity, detecting rogue devices, optimizing and maintaining mesh links and to discover AP neighbors.	Enter the duration in seconds. Range: 1 through 65535.
Auto Channel Selection	Automatically adjusts the channel for network self-healing and performance optimization. **ChannelFly** is set as the default option. For the **ChannelFly** option, you may also modify the default settings for the **Channel Change Frequency** and **Full Optimization Period**. The **Channel Change Frequency** slidebar allows you to specify the responsiveness of ChannelFly to interference (with consideration for the impact on associated clients), ranging from Minimal to Very Often. The **Full Optimization Period** timeslot bar allows you to specify one or more periods of time when ChannelFly is allowed to fully optimize the channel plan, ignoring the impact of channel changes on associated clients. Select time periods when the wireless network is servicing the fewest clients.	Select the required option. • **Background Scanning**: Changes the AP channel when there is an interference. • **ChannelFly**: Monitors potential throughput and will change channels to learn each channel's capacity, optimize throughput, and to avoid interference.
6G BSS Min Rate	Forces client devices to both be closer to the AP and to use higher, more efficient rates when you increase the BSS minimum rate above the default (all rates) setting. The BSS minimum rate is the lowest data rate supported on the WLAN. When OFDM-only is enabled, it takes higher priority than BSS minimum rate settings.	Select one of the following options: • 6 mbps • 9 mbps • 12 mbps • 18 mbps • 24 mbps
6G Mgmt Tx Rate	Sets the transmit rate for management frame types such as beacon and probes.	Select one of the following options: • 6 mbps • 9 mbps • 12 mbps • 18 mbps • 24 mbps
Multicast Rate Limiting	Multicast rate limit can be configured at WLAN level. The **UplinkDownlink** values are displayed only if the multicast rate limit is enabled. The **Downlink** traffic is limited to 50% of the configured multicast rate limiting. For example, if multicast rate limiting downlink traffic is set to 6Mbps, only 50%, for example: 3.00Mbps to 4.00Mbps traffic passes. This limit is only for downlink and is not affected by BSS Min Rate setting. **NOTE** SSID Rate Limit always takes precedence, if, Mutlicast Rate Limit is also configured.	Select the **Uplink** and **Downlink** check boxes and enter the limiting rates in Mbps, respectively. Range: 1 through 100 Mbps. **NOTE** The Multicast Rate Limit value cannot exceed SSID Rate Limit values for respective **Uplink** and **Downlink** direction.
Band/Spectrum Configuration > **Lower 5 GHz**		

TABLE 4 AP Group Details (continued)

Field	Description	Your Action
Channelization	Helps manage and allocate radio frequency resources. A lower channel width allows the zone to potentially serve more clients, whereas a higher channel width improves throughput, but potentially serves fewer clients and increases the possibility of interference. Prior to SmartZone release 7.0.0, the Auto setting defaulted to 80 MHz channelization. Beginning in SmartZone release 7.0.0, the Auto setting defaults to 40 MHz channelization.	Set the channel bandwidth used during transmission: Auto, 20, 40, 80 and 160. **NOTE** By default, for the **Country Code** Indonesia, the **Channelization** width is set to 20 MHz only for outdoor APs.
Channel	Indicates the channel to use.	Select the required options for the Indoor and Outdoor APs.
Allow DFS Channels	Allows ZoneFlex APs to use DFS channels.	Click to enable the option.
Allow Indoor Channels	Allows outdoor APs to use channels regulated as for indoor use only.	Click to enable the option.
Auto Cell Sizing	Enables the AP to share information on interference seen by each other and dynamically adjust their radio Tx power and Rx parameters to minimize interference. Enabling this option disables the TX Power Adjustment configuration. **NOTE** Ensure that Background Scan is enabled.	Select the option.
TX Power Adjustment	Allows to manually configure the transmit power on the Lower 5 GHz radio. By default, the TX power is set to Full on the Lower 5 GHz radio. **NOTE** If you choose Min, the transmit power is set to 0dBm (1mW) per chain for 11n APs, and 2dBm per chain for 11ac APs. If you choose Max, the transmit power is set to the maximum allowable value according to the AP's capability and the operating country's regulations.	Select the preferred TX power.
Background Scan	Allows the AP radio to scan other channels in the band for accessing channel health and capacity, detecting rogue devices, optimizing and maintaining mesh links and to discover AP neighbors.	Enter the duration in seconds. Range: 1 through 65535.

TABLE 4 AP Group Details (continued)

Field	Description	Your Action
Auto Channel Selection	Automatically adjusts the channel for network self-healing and performance optimization. **ChannelFly** is set as the default option. For the **ChannelFly** option, you may also modify the default settings for the **Channel Change Frequency** and **Full Optimization Period**. The **Channel Change Frequency** slidebar allows you to specify the responsiveness of ChannelFly to interference (with consideration for the impact on associated clients), ranging from Minimal to Very Often. The **Full Optimization Period** timeslot bar allows you to specify one or more periods of time when ChannelFly is allowed to fully optimize the channel plan, ignoring the impact of channel changes on associated clients. Select time periods when the wireless network is servicing the fewest clients.	Select the required option. • **Background Scanning**: Changes the AP channel when there is an interference. • **ChannelFly**: Monitors potential throughput and will change channels to learn each channel's capacity, optimize throughput, and to avoid interference.
Band/Spectrum Configuration > **Upper 5 GHz**		
Channelization	Helps manage and allocate radio frequency resources. A lower channel width allows the zone to potentially serve more clients, whereas a higher channel width improves throughput, but potentially serves fewer clients and increases the possibility of interference. Prior to SmartZone release 7.0.0, the Auto setting defaulted to 80 MHz channelization. Beginning in SmartZone release 7.0.0, the Auto setting defaults to 40 MHz channelization.	Set the channel bandwidth used during transmission: Auto, 20, 40, 80 and 160.
Channel	Indicates the channel to use.	Select the required options for the Indoor and Outdoor APs.
Allow DFS Channels	Allows ZoneFlex APs to use DFS channels.	Click to enable the option.
Allow Channel 144	Provides channel 140 and 144 support for 11ac and 11ax APs. Enabling this option supports 20 MHz, 40 MHz, or 80 MHz channel modes. The 160 MHz mode is supported if the AP supports this mode. Disabling this option provides Channel 140 support only to 20 MHz mode. **NOTE** This option is available only if you enable the **DFS Channels** option. **NOTE** This feature is currently supported only in the United States.	Click to enable the option.
Auto Cell Sizing	Enables the AP to share information on interference seen by each other and dynamically adjust their radio Tx power and Rx parameters to minimize interference. Enabling this option disables the TX Power Adjustment configuration. **NOTE** Ensure that Background Scan is enabled.	Select the option.

TABLE 4 AP Group Details (continued)

Field	Description	Your Action
TX Power Adjustment	Configures the power transmitted on the upper 5ghz, manually on the Upper 5 GHz radio. By default, the Tx power is set to Full on the Upper 5 GHz radio. **NOTE** If you choose Min, the power transmitted power is set to 0dBm (1mW) per chain for 11n APs, and 2dBm per chain for 11ac APs. If you choose Max, the power transmitted power is set to the maximum allowable value according to the AP's capability and the operating country's regulations.	Select the preferred TX power.
Background Scan	Allows the AP radio to scan other channels in the band for accessing channel health and capacity, detecting rogue devices, optimizing and maintaining mesh links and to discover AP neighbors.	Enter the duration in seconds. Range: 1 through 65535.
Auto Channel Selection	Automatically adjusts the channel for network self-healing and performance optimization. **ChannelFly** is set as the default option. For the **ChannelFly** option, you may also modify the default settings for the **Channel Change Frequency** and **Full Optimization Period**. The **Channel Change Frequency** slidebar allows you to specify the responsiveness of ChannelFly to interference (with consideration for the impact on associated clients), ranging from Minimal to Very Often. The **Full Optimization Period** timeslot bar allows you to specify one or more periods of time when ChannelFly is allowed to fully optimize the channel plan, ignoring the impact of channel changes on associated clients. Select time periods when the wireless network is servicing the fewest clients.	Select the required option. • **Background Scanning**: Changes the AP channel when there is an interference. • **ChannelFly**: Monitors potential throughput and will change channels to learn each channel's capacity, optimize throughput, and to avoid interference.
AP GRE Tunnel Options		
Ruckus GRE Forwarding Broadcast	Forwards broadcast traffic from network to tunnel. **NOTE** ARP and DHCP traffic are allowed even if this option disabled.	Click **Override** to enable the Ruckus GRE broadcast forwarding option. Click the **Enable Forwarding Broadcast** option to forward the broadcast traffic.
AP SNMP Options		
Override zone configuration	Indicates that the AP Group configuration overrides the zone configuration.	Select the check box.
Enable AP SNMP	Indicates if the AP SNMP option is enabled.	Select the check box.
SNMPv2 Agent	Indicates SNMPv2 Agent is applied.	1. Click **Create** and enter **Community**. 2. Select the required **Privilege**. If you select **Notification** enter the **Target IP**. 3. Click **OK**.

TABLE 4 AP Group Details (continued)

Field	Description	Your Action
SNMPv3 Agent	Indicates SNMPv3 Agent is applied.	1. Click **Create** and enter **User**. 2. Select the required **Authentication**. 3. Enter the **Auth Pass Phrase**. 4. Select the **Privacy** option. 5. Select the required **Privilege**. If you select **Notification** select the option **Trap** or **Inform** and enter the **Target IP** and **Target Port**. 6. Click **OK**.
Model Specific Options **NOTE** Select the **Override** check box for each setting to change its default configuration.		
AP Model	Indicates AP model for which the configuration is done.	Select the option.
Status LEDs	Disables the status LED on the selected AP model.	Select the option.
LLDP	Enables the Link Layer Discovery Protocol (LLDP) on the selected AP model.	Select the option and enter the following details: • **Advertise Interval**—Enter the duration in seconds. • **Hold Time**—Enter the duration in seconds. • **Enable Management IP TLV**—Select the check box.
External Antenna (2.4 GHz)	Enables the external 2.4 GHz antenna on the selected AP model.	Select the **Enable external antenna** check box, and then set the gain value (between 0 and 90dBi) in the box provided.
External Antenna (5 GHz)	Enables the external 5 GHz antenna on the selected AP model.	Select the **Enable external antenna** check box, and then set the gain value (between 0 and 90dBi) in the box provided.
Port Settings	Indicates the port settings.	Select the option and choose the required LAN option.
PoE out port	Enables PoE out mode.	Select the Enable PoE out ports (specific ZoneFlex AP models only) check box.
PoE Operating Mode	PoE Operating Mode allows manual control of power negotiation between the AP and the power source. Default is Auto, allowing the correct power requirement to be negotiated between the AP and the power source **NOTE** You can set the PoE operating mode from the **AP Configuration** tab on the controller or using the **get power-mode** CLI command. The R730 AP is supported only in SZ6.1.0 firmware zone.	Choose the option. **NOTE** When this option is selected, some AP features are disabled to reduce power consumption, such as the USB port and one of the Ethernet ports.

TABLE 4 AP Group Details (continued)

Field	Description	Your Action
LACP/LAG	Aggregates multiple network interfaces into a single logical or bonded interface. LACP can be enabled only on two-port 11ac wave2 and 11ax APs. A minimum of two ports must be active on AP and switch for LACP/LAG configuration. Enabled on switch ports where the APs Ethernet cables are connected increases the bandwidth between the AP and the switch.	Choose the option: • Keep the AP's settings: Retains the current AP settings. • Disabled: Disables bond configuration. • Enabled: Enables bond configuration. Select the **Bond Port Profile** from the drop-down.
Internal Heater	Enables the heater that is built into the selected AP model	Select the Enable internal heaters (specific AP models only) check box.
USB Port	Disables the USB port. USB ports are enabled by default.	Select the Disable USB port check box.
Advanced Options		
Location Based Service	Enables location-based service for the AP group.	• Select the **Override zone configuration** check box. • Select the **Enable LBS Service** check box. • **Select an LBS Server** from the drop-down.
Hotspot 2.0 Venue Profile	Indicates the hotspot profile that you want to assign to the group.	Select the required option or click **Create** and update the following details: • Enter the **Name**. • Enter the **Description**. • Enter the **Venue Names**. • Select the **Venue Category**. • Select the **Type**. • Enter the **WLAN Metrics**.
AP Management VLAN	Indicates the AP management VLAN settings.	Choose the option. Click **VLAN ID**, and then type the VLAN ID that you want to assign (valid range is from 1 to 4094). To keep the same management VLAN ID that has been configured on the AP, click **Keep AP's settings**. **ATTENTION** For standalone APs, set the AP Ethernet port to trunk before changing the AP Management VLAN settings.
Client Admission Control	Indicates the load thresholds on the AP at which it will stop accepting new clients.	Select the **Override** check box respective to **2.4 GHz Radio** or **5 GHz Radio** and update the following details: • **Enable** **NOTE** Client load balancing and band balancing will be disabled for this AP group. • **Min Client Count** • **Max Radio Load** • **Min Client Throughput**

TABLE 4 AP Group Details (continued)

Field	Description	Your Action
Rogue Classification Policy	Indicates the parameters used to classify rogue APs. This option is available only if you enable the **Rogue AP Detection**option.	Select the options for rogue classification policy: • Enable the **Override** option and select the rogue classification policy from the list to override for this group. • Enable the **Override** option and enter the **Report RSSI Threshold**. Range: **0** through **100**. • Enable the **Override** option to override the aggressiveness of protecting the network and choose one of the following: – **Aggressive** – **Auto** – **Conservative** • Enable the **Override** option and enter the **Jamming Threshold** in percentage.
Recovery SSID	Allows you to enable or disable the Recovery(Island) SSID broadcast on the controller.	Enable **Recovery SSID Broadcast**
Direct Multicast	Indicates whether multicast traffic is sent from a wired device, wireless device or from the network.	Select one or more of the following: • **Multicast Traffic from Wired Client** • **Multicast Traffic from Wireless Client** • **Multicast Traffic from Network**
Venue Code	Indicates the venue code.	You can choose to override this setting and enter the code in the field provided.
BSS Coloring	Indicates the BSS coloring settings.	• Select the **Override zone configuration** check box. • Select the **Enable BSS Coloring** check box.

NOTE

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

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

Working with AP Groups

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

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

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

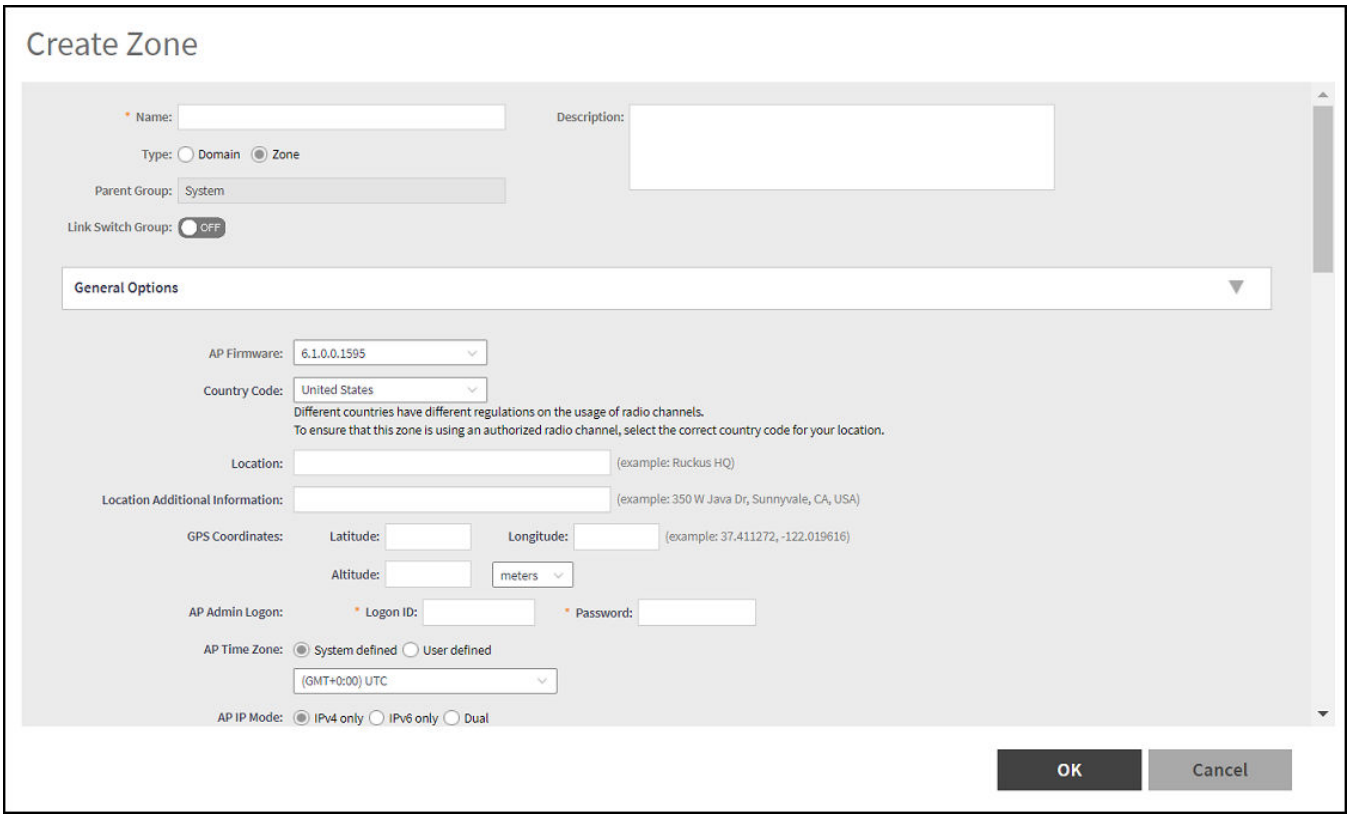
Creating a Monitoring AP Group

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

Perform the following procedure to create a monitoring AP group.

1. From the main menu, click **Monitor** > **Monitoring APs**.
2. Select **System** and click **+** to create a zone.

FIGURE 2 Creating a Zone



3. For **Type**, select **Zone**.
4. Select **General Options** > **AP Admin Logon**, enter the user name and password, and click **OK**.
5. Under **Advanced Options**, enable **Rogue AP Detection**.

6. For **Rogue Classification Policy**, configure the following options:
   a) In the **Report RSSI Threshold** field, enter the threshold (the threshold ranges from 0 through 100).
   b) Enabling the option **Protect the network from malicious rogue access points** has no effect as an AP in monitoring mode is a passive listener.

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

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

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

FIGURE 3 Creating an AP Monitoring Group

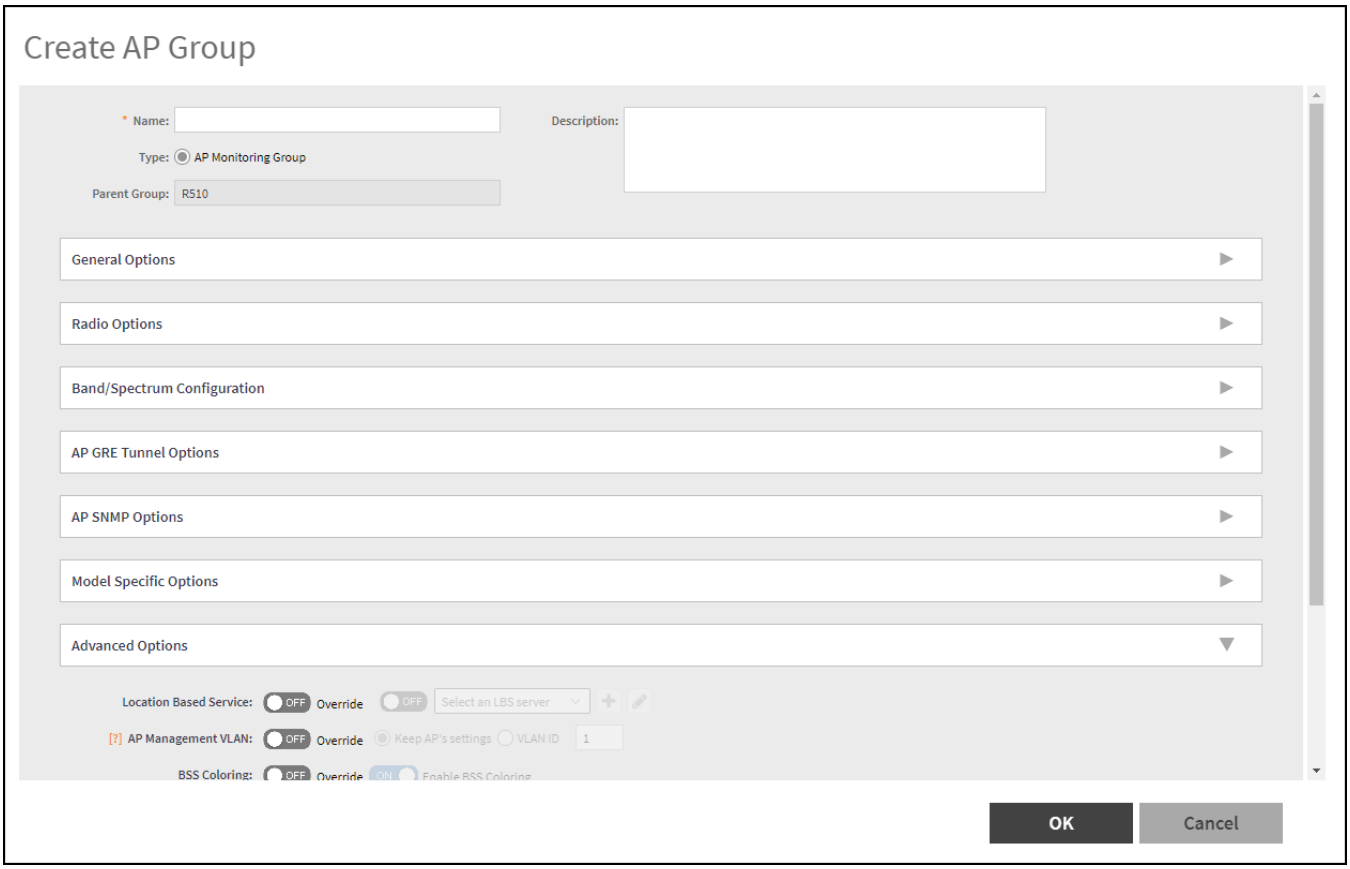
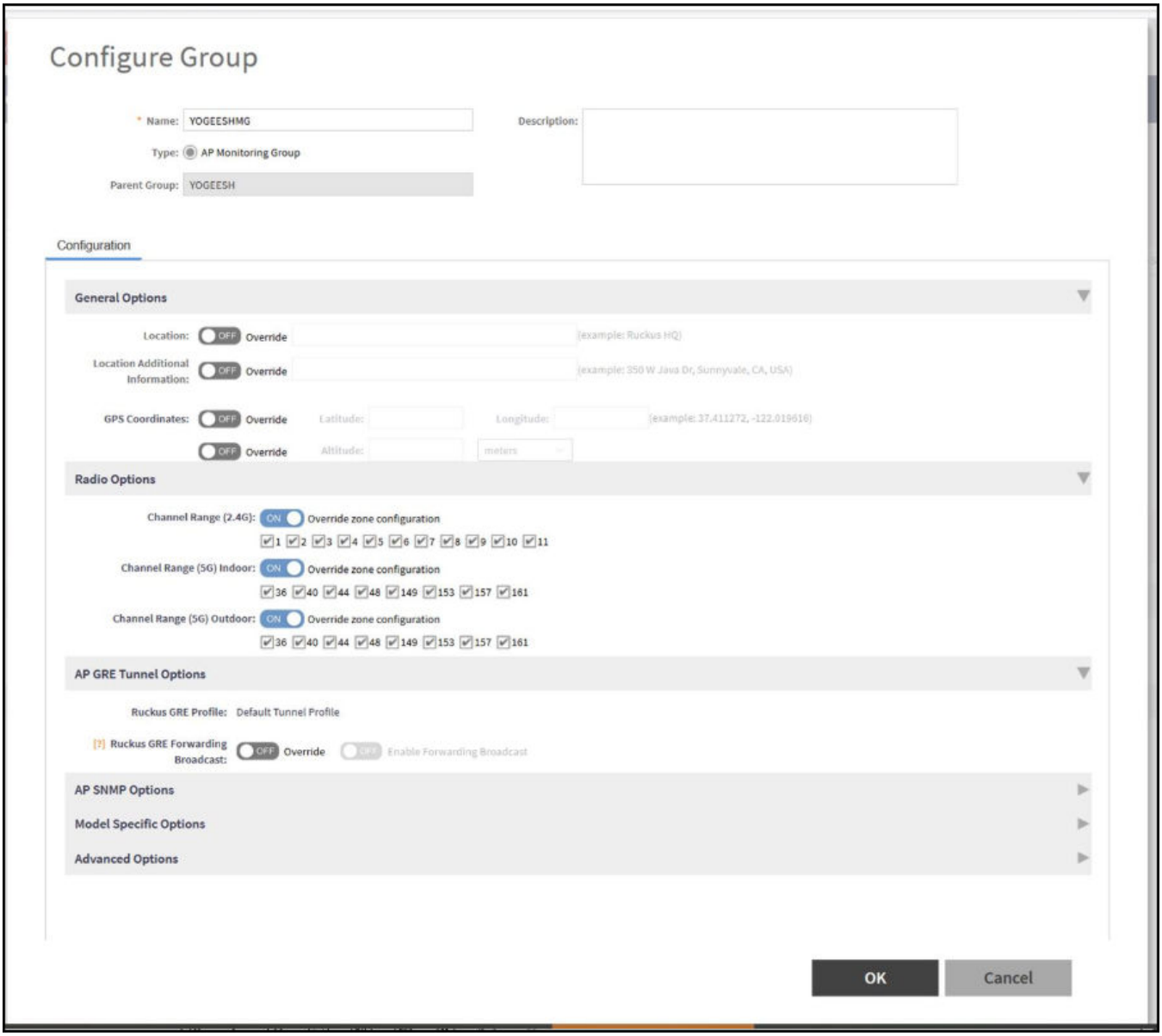


FIGURE 4 Configuring Group



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

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

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

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

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

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

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

    Viewing Associated Events

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

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

AP Health Indicators

Viewing AP Health Indicators

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

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

Performance

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

Connection Failure

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

You can customize the information displayed in the **Performance** section:

1. From the **Access Points** page, select the required domain, zone, AP group, or AP.
2. Scroll down and select the **Health** tab.
3. On the **Performance** bar, select the Setting icon. The **Settings - Performance** pop-up appears. Customize the following:
   - **Show top**: Enter the number of performance failures to be displayed.
   - **Display Channel Change**: Select the required options. For example: **2.4G**, **5G**, and **6G/5G**.
   - **AP**: Choose the unique identifier displayed for each AP. For example: **Name**, **MAC**, **IP**.
4. Click **OK**.

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

AP Provisioning and Swapping

Provisioning and Swapping Access Points

The controller supports the provisioning and swapping of access points.

As an administrator you can:

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

Options for Provisioning and Swapping APs

The controller supports the provisioning and swapping of access points.

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

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

- Network Mask
- Gateway
- Primary DNS
- Secondary DNS
- Serial Number
- IPv6 Address
- IPv6 Gateway
- IPv6 Primary DNS
- IPv6 Secondary DNS

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

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

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

Understanding How Swapping Works

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

TABLE 5 AP swapping stages

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

AP Status

AP Status

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

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

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

  NOTE
  APs that exceed their health threshold and that require your attention are flagged. Refer to the Understanding Cluster and AP Health Icons on page 43 section for more information.

Understanding Cluster and AP Health Icons

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

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

- 1 (Green): Online
- 3 (Orange): Flagged
- 3 (Red): Offline

Online and Offline status are self-explanatory. "Flagged" status is user-defined. You can customize the thresholds at which an AP or cluster enters "flagged" state using the **Settings** (gear) icon in the status bar. For more information, see Customizing Health Status Thresholds on page 43.

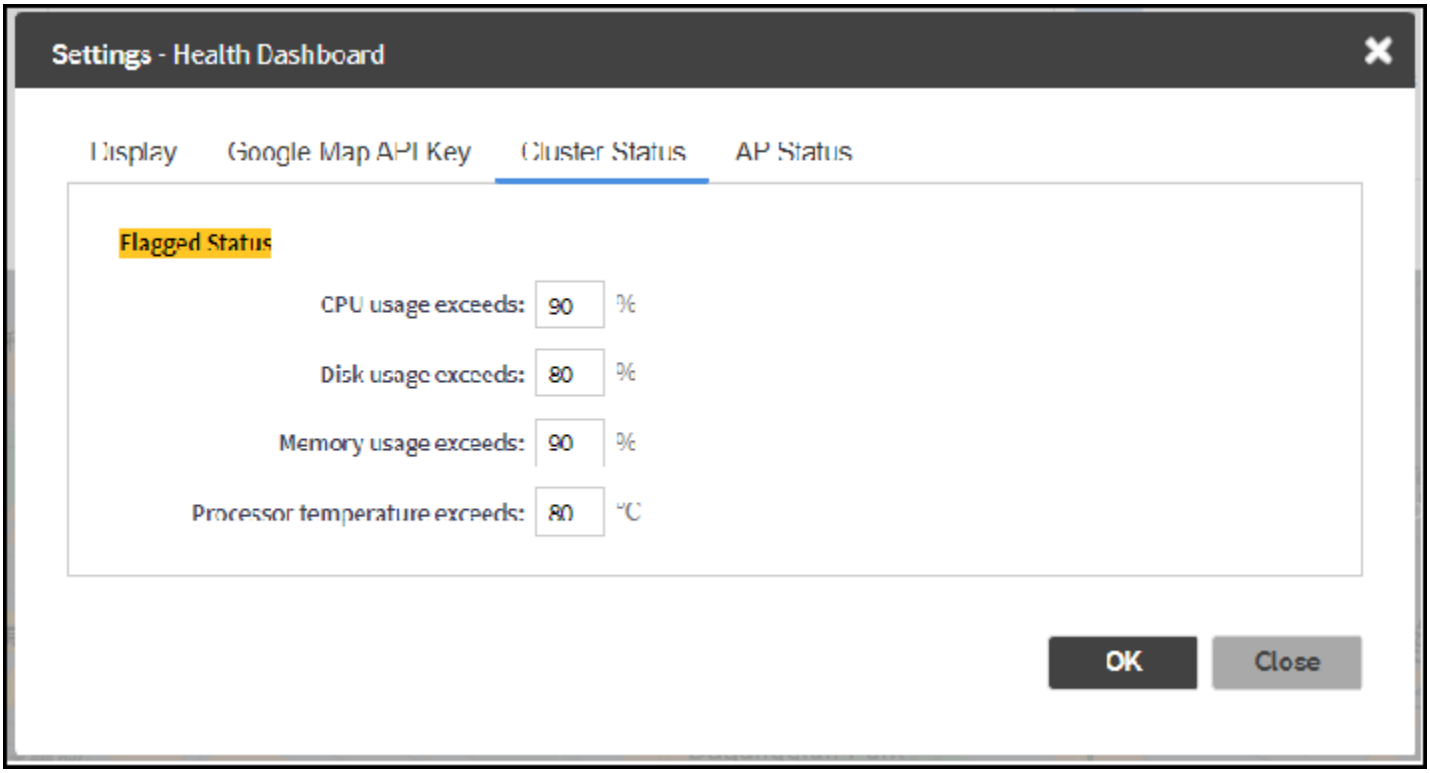
Customizing Health Status Thresholds

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

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

- **Cluster Status**: Configure CPU, hard disk and memory usage percentages above which the cluster will be marked as flagged status.
- **AP Status**: Configure the criteria upon which APs will be flagged. For more information, see the Customizing Health Status Thresholds section.

FIGURE 5 Setting Cluster Health Status Thresholds



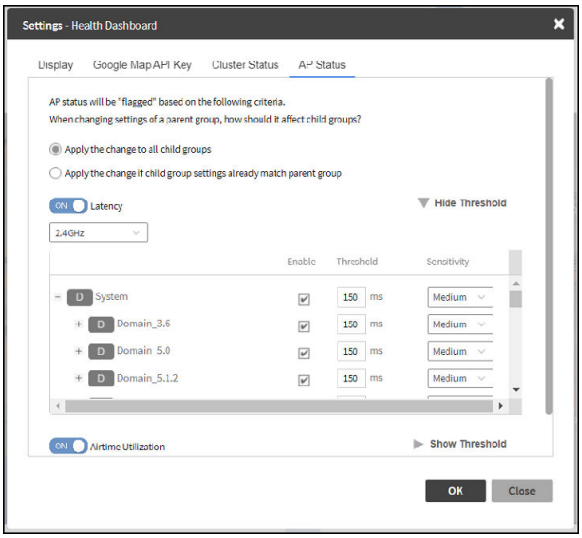
Customizing AP Flagged Status Thresholds

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

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

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

FIGURE 6 Configuring AP Flagged Status Thresholds



SCI Thresholds for each AP

The following are the thresholds from SCI for each AP.

The below thresholds provided is based on per AP model.

TABLE 6 SCI Thresholds

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

Using the Health Dashboard Map

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

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

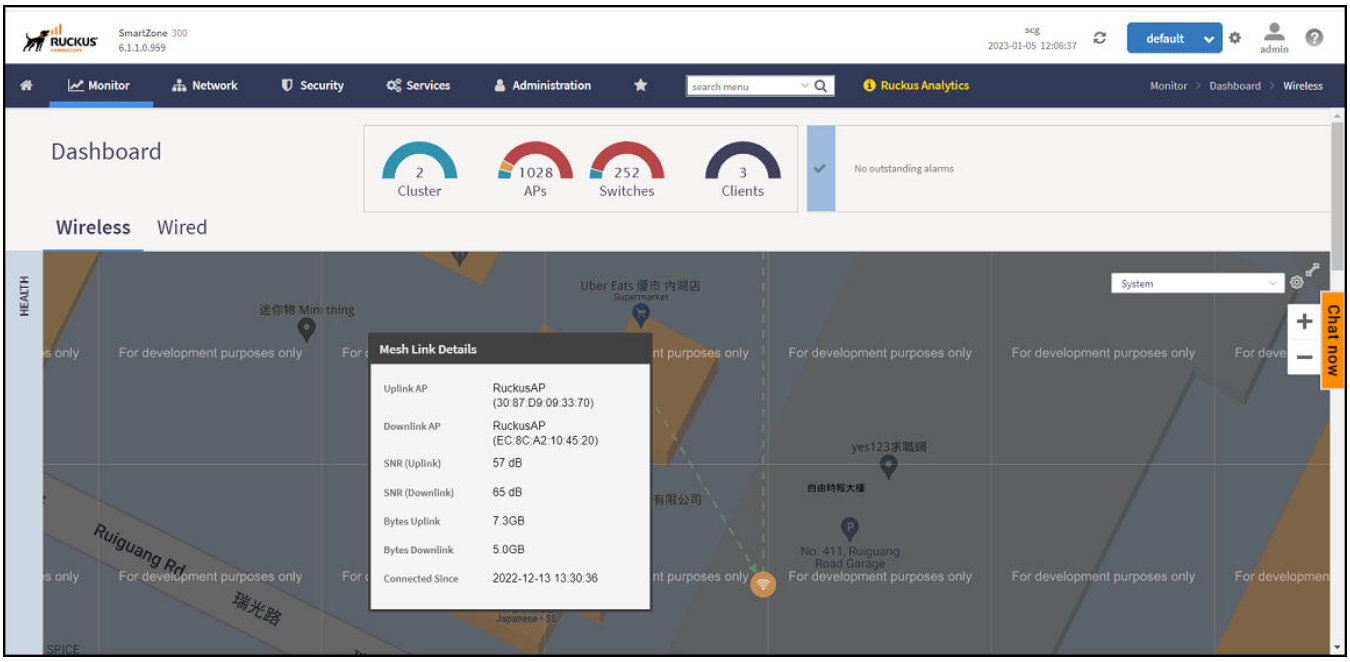
Use the **Settings** icon to configure the information displayed in tooltips when hovering over an AP on the map. You can also change the view mode altogether, from map view to Groups, Control Planes or Data Planes view mode using the settings menu. Additionally, you can also select the check-box to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

- Uplink AP: displays the IP address of the uplink AP to which the wireless client sends data
- Downlink AP: displays the IP address of the downlink AP from which data is sent back to the wireless client
- SNR (Uplink): displays the signal-to-noise ratio in the uplink path

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

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

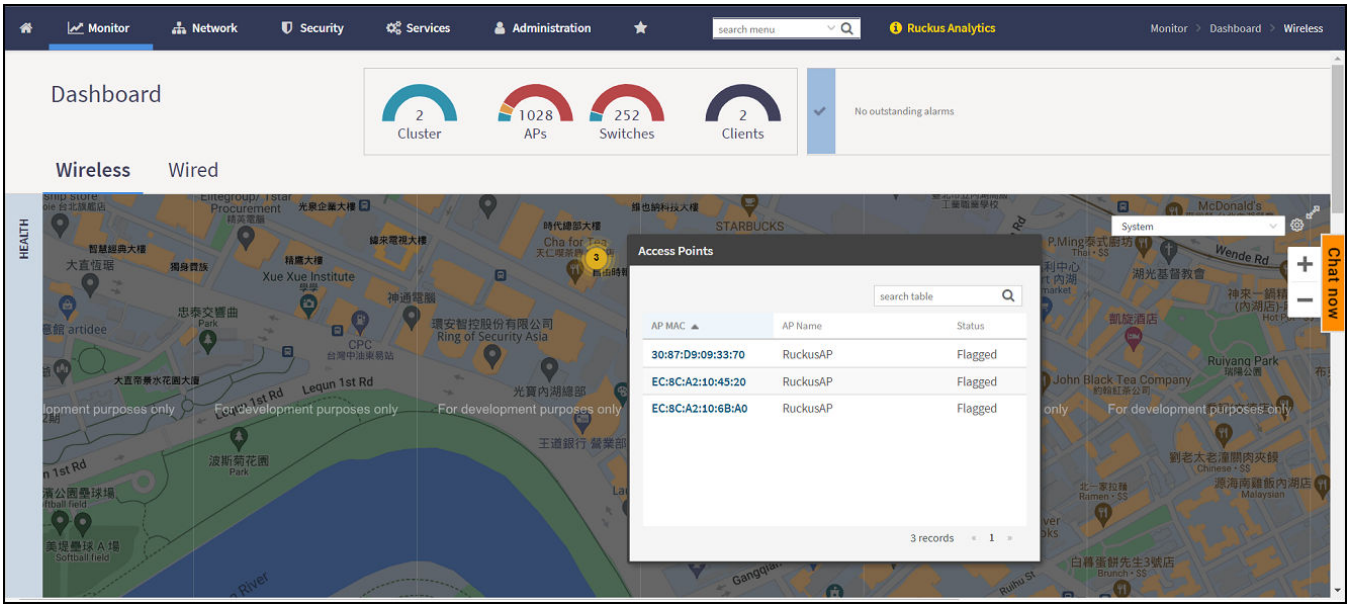
FIGURE 7 Mesh Link Details



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

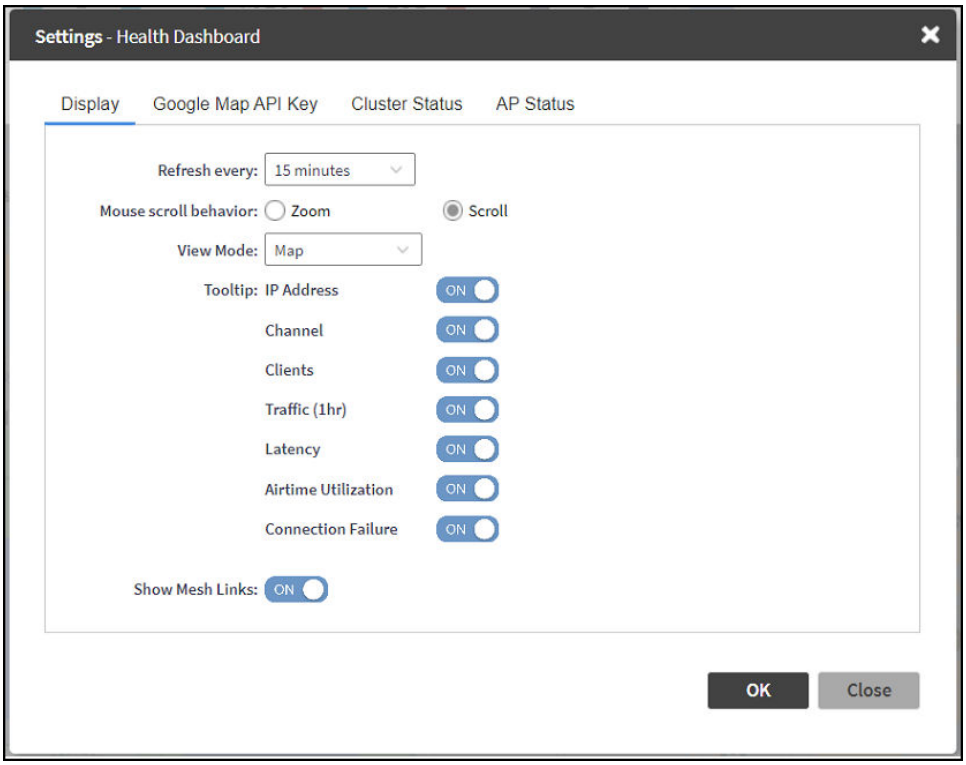
- AP MAC: Displays the MAC address of the AP
- AP Name: Displays the name assigned to the access point
- Status: Displays the status of the AP such as Online or Offline

FIGURE 8 AP Details



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

FIGURE 9 Configuring Map Settings



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

Configuring the Google Map API Key Behavior

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

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

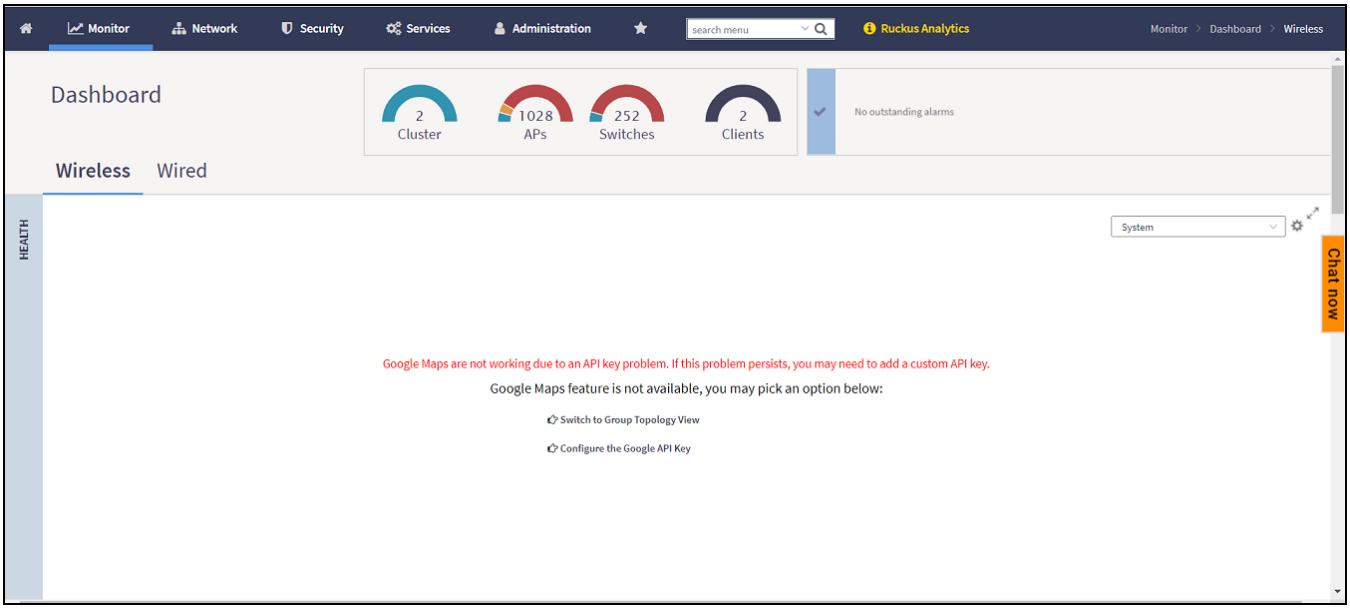
You would also have to generate an API key if you encounter errors such as:

```
MissingKeyMapError
```

or

```
NoApiKeys
```

FIGURE 10 Health dashboard view when API key is not available



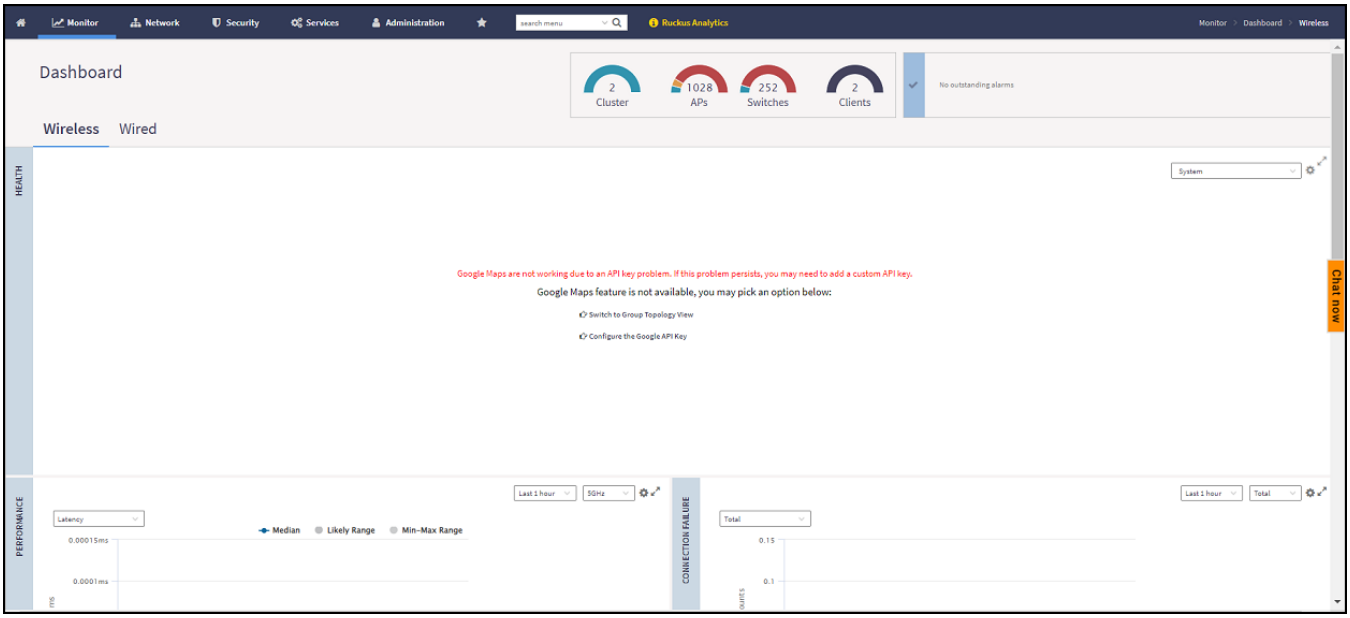
Clicking **Configure the Google API Key** directs you to the **Google Map API Key** tab, where you can manage the Google Map API Key behavior.

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

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

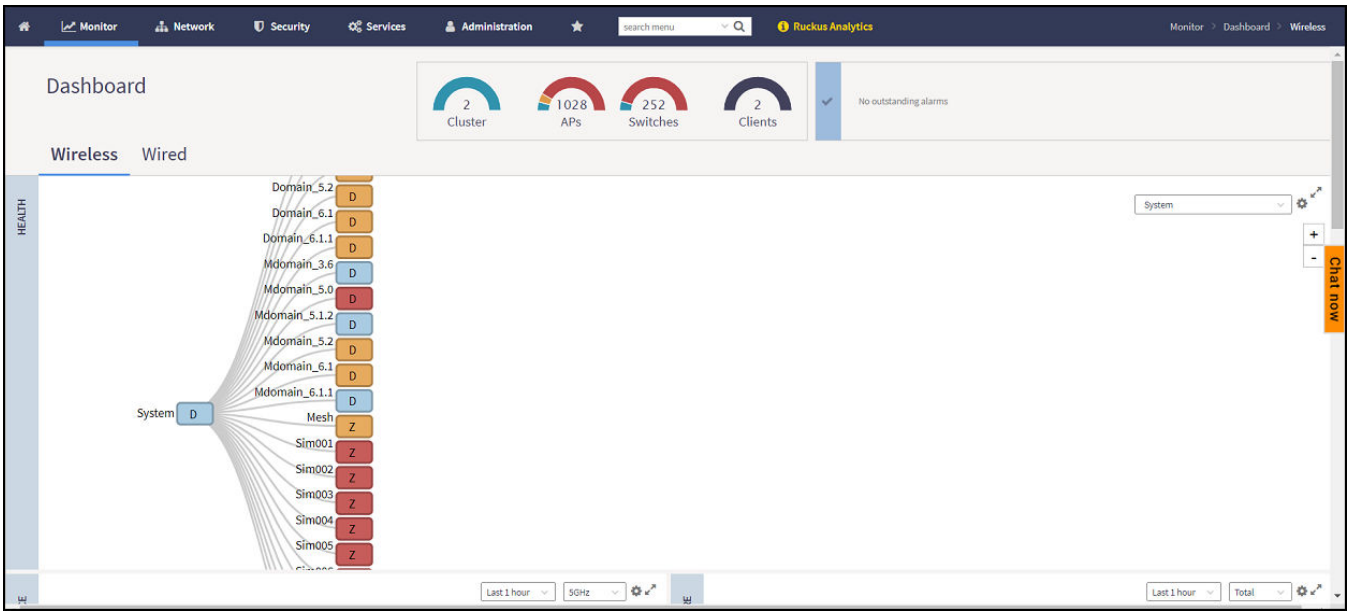
Launching the application displays the **Dashboard** menu, by default.
In **Health**, the map view appears if you are connected to a network. If you are not, then you might see the following screen and would have to view your network deployment as a topology diagram.

FIGURE 11 No Map View



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

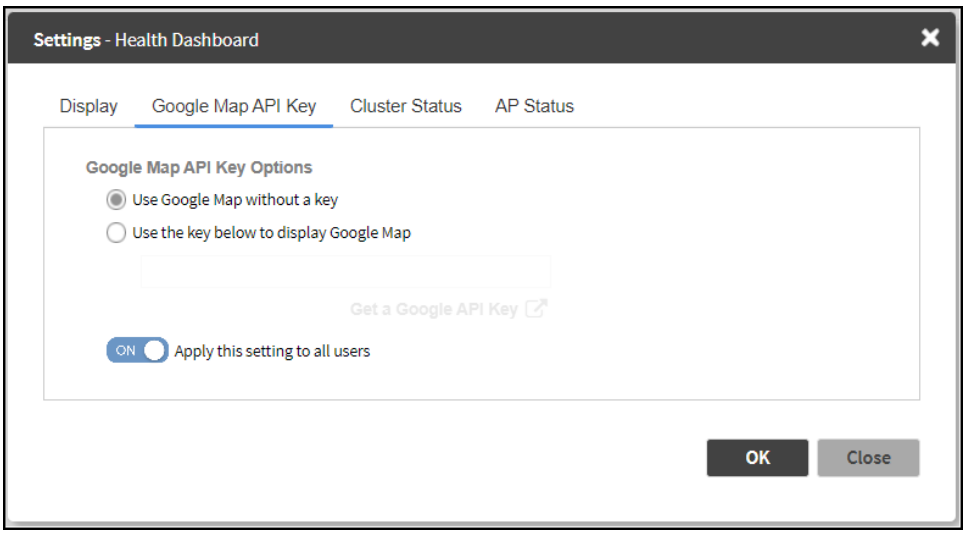
FIGURE 12 Topology View



1. From the map view in **Health**, click the **Settings** icon.

   The **Settings-Map** page appears.

   FIGURE 13 Google Map API Key Options



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

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

   TABLE 7 Google Map API Key Options

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

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

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

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

Viewing AP Performance

Click the Performance tab to analyze the following parameters:

- Latency - Average time delay between an AP and connected clients.
- Airtime Utilization - Percent of airtime utilized, by radio. Following are the statistics that are evaluated:

TABLE 8 Airtime Utilization Statistics

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

Viewing AP Connection Failures

Click the Connection Failure tab to analyze the following parameters

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

You can view the parameters:

- **SZ300 and vSZ-H platforms**: Duration: 1 hour and 24 hours
- **SZ100 and vSZ-E platforms**: Duration: 1 hour, 24 hours, 7 days, and 14 days
- Radio: Total, 2.4 GHz, 5GH

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

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

AP Switchover

Configuring AP Switchover

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

The following task configures APs to swtichover clusters:

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

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

   You have configured AP switchover.

Switch Over Managed APs and External DPs

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

Switch Over APs (per Zone)

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

To switch over APs per zone:

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

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

Switch Over APs (per AP)

To switch over per AP:

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

Switch Over Data Planes (per data plane)

You can switch over external data planes.

To switch over external data planes:

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

AP Traffic Indicators

Viewing AP Traffic Indicators

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

You can view:

- Historical or Real Time traffic
- WLAN traffic

Traffic indicators can be filtered based on the following parameters:

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

To customize Traffic settings:

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

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

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

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

Traffic Analysis

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

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

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

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

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

The parameters are displayed as graphs and bar charts. When you hover over the graph you can view the date and time, median, likely range, min-max range of the parameters. To view specific information on the graph, click and drag the portion. The selected portion would zoom in. To restore to normal view, click the **Reset zoom** button.

Customizing Traffic Analysis

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

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

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

Configuring Traffic Analysis Display for APs

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

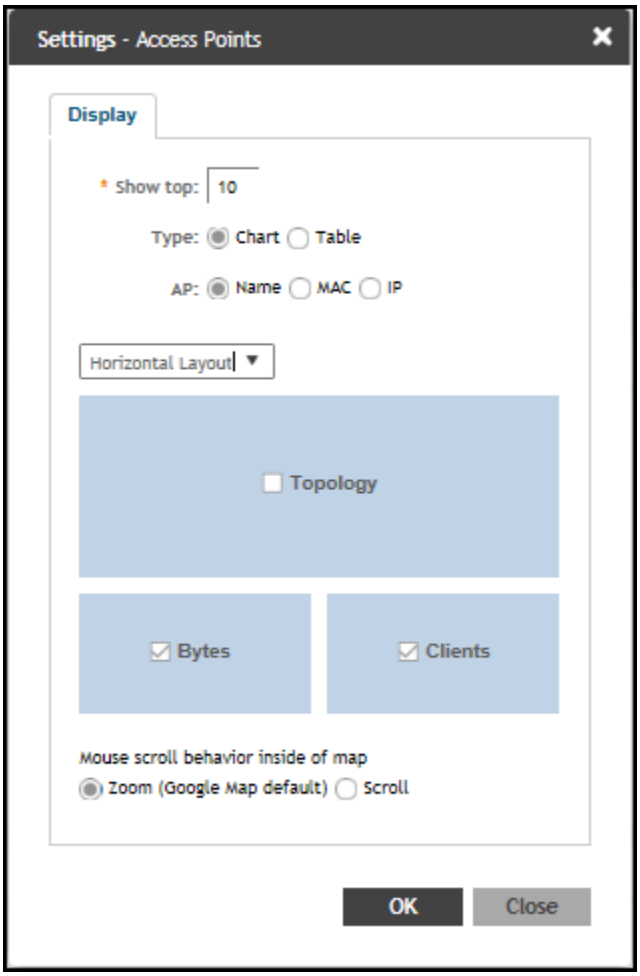
You can view historical and real-time data of the AP. Throughput and the number of clients connected to the AP are displayed in a bar chart. You can view the count of AP model details supported on the system in a pie chart. You must configure the AP settings to view its traffic analysis.

To configure the AP settings:

1. From the Access Points area, click settings .

   The AP setting form displays.

   FIGURE 14 AP Settings Form



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

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

Configuring Traffic Analysis Display for Top Clients

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

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

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

To configure the client settings:

1. From the WLAN area, click settings

   .

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

SmartCell Insight Report on Actual Traffic Rate for APs and Client

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

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

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

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

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

- **Other Rx Time**: How much time did the AP spend receiving broadcast traffic and traffic for other BSSIDs

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

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

The controller will send the following information to SCI at the Client level.

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

AP WLAN Services

Monitoring WLAN Services

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

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

TABLE 9 System, Domain, Zone, and AP Groups Monitoring Tabs for SZ300 and vSZ-H platforms

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

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

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

TABLE 10 System, Zone, and AP Groups Monitoring Tabs for SZ100 and vSZ-E platforms

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

TABLE 10 System, Zone, and AP Groups Monitoring Tabs for SZ100 and vSZ-E platforms (continued)

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

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

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

Triggering a Preferred Node

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

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

Follow these steps to trigger a node:

NOTE
You must enable node affinity before triggering nodes.

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

Rehoming Managed APs and Data Planes

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

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

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

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

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

Rehoming Managed APs

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

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

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

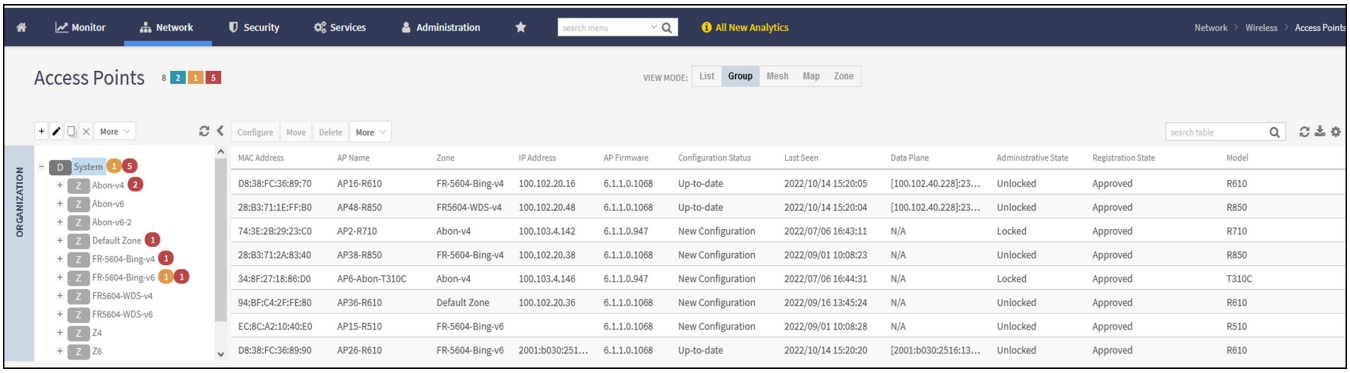
> **NOTE**
> **AP Auto Rehome** is supported only on SZ300 and vSZ platforms.

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

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

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

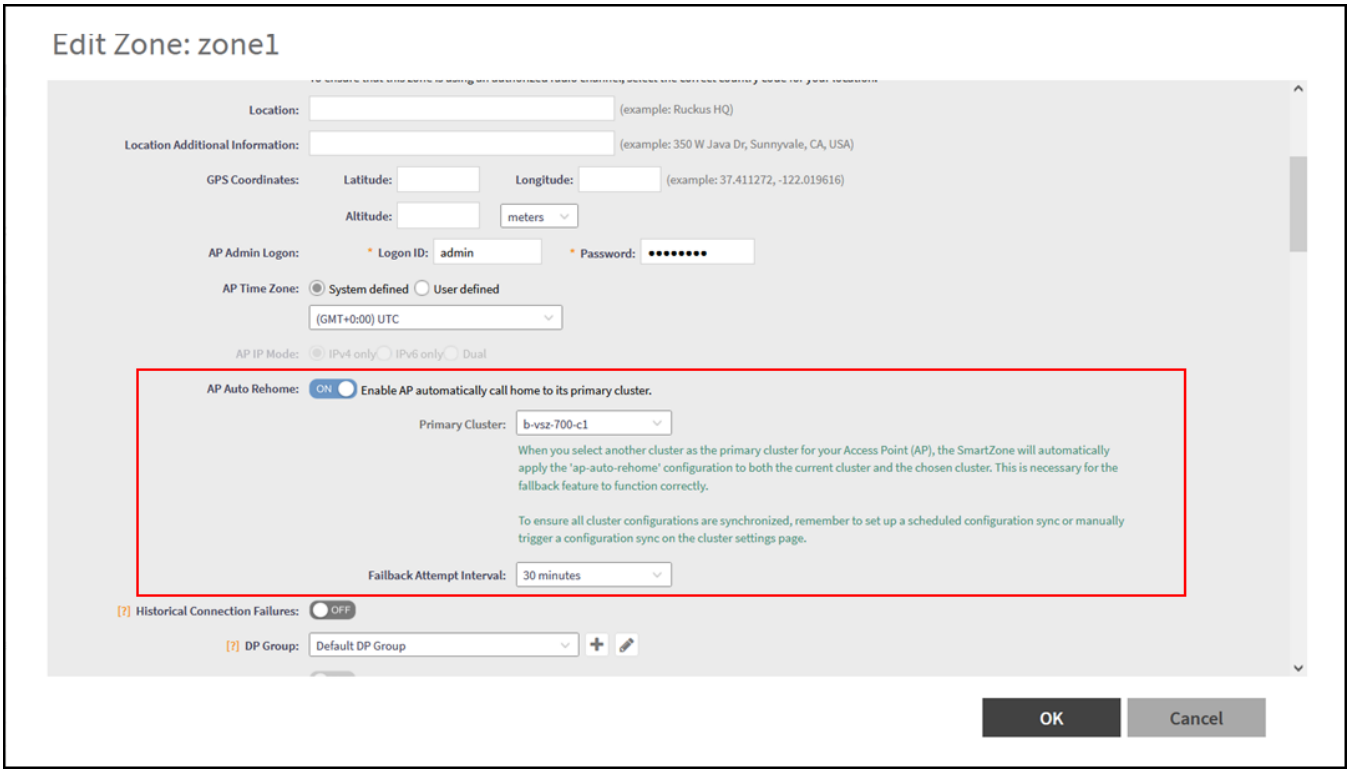
   FIGURE 15 Access Points Page



2. Select the zone that is created in the Active-Active cluster redundancy mode, and click the **Edit** option. To configure a cluster in Active-Active mode, refer to "Enabling Cluster Redundancy" in the *SmartZone Management Guide*.

   The **Edit Zone** page is displayed.

   FIGURE 16 Editing a Zone



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

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

Approving Mesh APs

Viewing Mesh APs

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

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

1. From the main menu, click the **Network** tab.
2. Click **Access Point**, the **Access Point** page appears. On the upper-right corner of the page, select the **Mesh** option from **View** mode.

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

FIGURE 17 Viewing Mesh APs

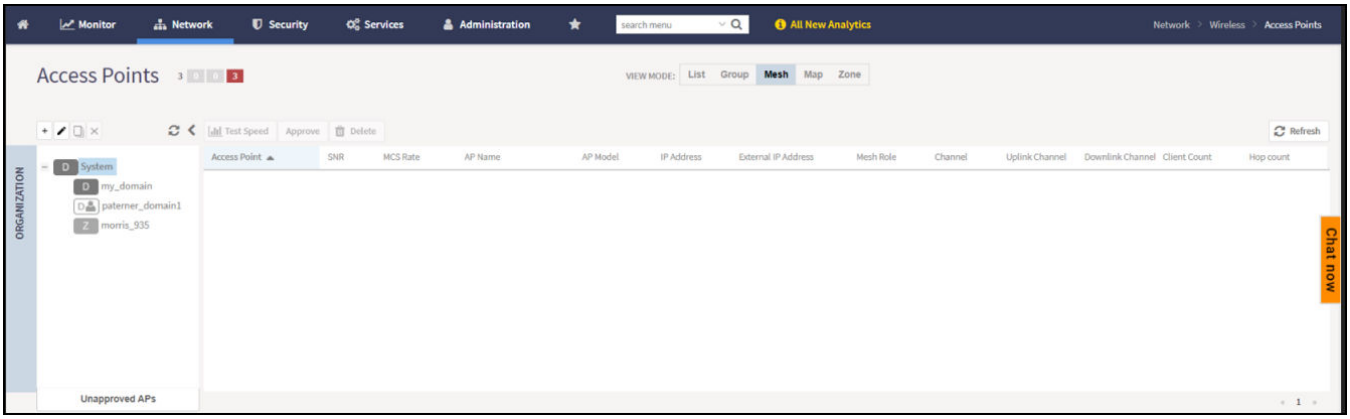


TABLE 11 Access Point Details

Field Name	Description
SNR	Displays the Signal-to-Noise Ratio (SNR), which indicates the signal strength relative to background noise. The SNR value is shown in decibels (dB) and displayed as either the real-time value or the average value over the past 90 seconds.
MCS Rate (Tx) (Rx)	Displays the median of MCS rate Tx/Rx for both client and AP in there respective pages. These values are updated every 180 seconds (Highscale) and 90 seeconds (Essentials).
AP Name	Displays the name assigned to the access point
AP Model	Displays the model name.
IP Address	Displays the IP address assigned to the wireless client
External IP Address	Displays the APs external IP address
Mesh Role	Displays the status of APs
Channel	Displays the wireless channel (and channel width) that the wireless client is using
Traffic (Uplink)	Displays the total uplink traffic (in KB/MB/GB/TB) for this client in this session
Traffic (Downlink)	Displays the total downlink traffic (in KB/MB/GB/TB) for this client in this session
Client Count	Displays the number of client in theAP

TABLE 11 Access Point Details (continued)

Field Name	Description
Hop Count	Displays the number of hop counts

Approving Mesh APs

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

To approve mesh APs:

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

   The mesh APs are listed.
2. To view the list of APs pending for approval, click the **Unapproved APs** below the left pane.
3. From the list, select the AP which is not assigned to a Staging or Default Zone and click **Approve**.

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

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

Configuring APs

Overview of Access Point Configuration

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

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

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

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

Configuring Access Points

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

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

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

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

TABLE 12 Access Point Edit Parameters

Field	Description	Your Action
AP Configuration > **General Options**		

TABLE 12 Access Point Edit Parameters (continued)

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

TABLE 12 Access Point Edit Parameters (continued)

Field	Description	Your Action
TX Power Adjustment	Allows to manually configure the transmit power on the 2.4 GHz radio. By default, the TX power is set to Full on the 2.4 GHz radio. **NOTE** If you choose Min, the transmit power is set to 0dBm (1mW) per chain for 11n APs, and 2dBm per chain for 11ac APs. If you choose Max, the transmit power is set to the maximum allowable value according to the AP's capability and the operating country's regulations.	Select the preferred TX power.
Protection Mode	Allows to manually override the protection mode and select from the options - • None • RTS/CTS • CTS Only	Select the preferred protection mode.
WLAN Group	Allows to manually configure the WLAN Group. To add a WLAN group, refer to 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 maintaining mesh links and to discover AP neighbors.	Enter the duration in seconds. Range: 1 through 65535.
Auto Channel Selection	Automatically adjusts the channel for network self-healing and performance optimization. **ChannelFly** is set as the default option. For the **ChannelFly** option, you may also modify the default settings for the **Channel Change Frequency** and **Full Optimization Period**. The **Channel Change Frequency** slidebar allows you to specify the responsiveness of ChannelFly to interference (with consideration for the impact on associated clients), ranging from Minimal to Very Often. The **Full Optimization Period** timeslot bar allows you to specify one or more periods of time when ChannelFly is allowed to fully optimize the channel plan, ignoring the impact of channel changes on associated clients. Select time periods when the wireless network is servicing the fewest clients.	Select the required option. • **Background Scanning**: Changes the AP channel when there is an interference. • **ChannelFly**: Monitors potential throughput and will change channels to learn each channel's capacity, optimize throughput, and to avoid interference.
AP Configuration > **Band/Spectrum Configuration** > **5 GHz**		
Channelization	Helps manage and allocate radio frequency resources. A lower channel width allows the zone to potentially serve more clients, whereas a higher channel width improves throughput, but potentially serves fewer clients and increases the possibility of interference. Prior to SmartZone release 7.0.0, the Auto setting defaulted to 80 MHz channelization. Beginning in SmartZone release 7.0.0, the Auto setting defaults to 40 MHz channelization.	Set the channel bandwidth used during transmission: Auto, 20, 40, 80 and 160. **NOTE** By default, for the **Country Code** Indonesia, the **Channelization** width is set to 20 MHz only for outdoor APs.

TABLE 12 Access Point Edit Parameters (continued)

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

TABLE 12 Access Point Edit Parameters (continued)

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

TABLE 12 Access Point Edit Parameters (continued)

Field	Description	Your Action
Auto Channel Selection	Automatically adjusts the channel for network self-healing and performance optimization. **ChannelFly** is set as the default option. For the **ChannelFly** option, you may also modify the default settings for the **Channel Change Frequency** and **Full Optimization Period**. The **Channel Change Frequency** slidebar allows you to specify the responsiveness of ChannelFly to interference (with consideration for the impact on associated clients), ranging from Minimal to Very Often. The **Full Optimization Period** timeslot bar allows you to specify one or more periods of time when ChannelFly is allowed to fully optimize the channel plan, ignoring the impact of channel changes on associated clients. Select time periods when the wireless network is servicing the fewest clients.	Select the required option. • **Background Scanning**: Changes the AP channel when there is an interference. • **ChannelFly**: Monitors potential throughput and will change channels to learn each channel's capacity, optimize throughput, and to avoid interference.
AP Configuration > **Band/Spectrum Configuration** > **Lower 5 GHz**		
Channelization	Helps manage and allocate radio frequency resources. A lower channel width allows the zone to potentially serve more clients, whereas a higher channel width improves throughput, but potentially serves fewer clients and increases the possibility of interference. Prior to SmartZone release 7.0.0, the Auto setting defaulted to 80 MHz channelization. Beginning in SmartZone release 7.0.0, the Auto setting defaults to 40 MHz channelization.	Set the channel bandwidth used during transmission: Auto, 20, 40, 80 and 160. **NOTE** By default, for the **Country Code** Indonesia, the **Channelization** width is set to 20 MHz only for outdoor APs.
Channel	Indicates the channel to use.	Select the required options for the Indoor and Outdoor APs.
Allow DFS Channels	Allows ZoneFlex APs to use DFS channels.	Click to enable the option.
Allow Indoor Channels	Allows outdoor APs to use channels regulated as for indoor use only.	Click to enable the option.
Auto Cell Sizing	Enables the AP to share information on interference seen by each other and dynamically adjust their radio Tx power and Rx parameters to minimize interference. Enabling this option disables the TX Power Adjustment configuration. **NOTE** Ensure that Background Scan is enabled.	Select the option.
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 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 maintaining mesh links and to discover AP neighbors.	Enter the duration in seconds. Range: 1 through 65535.
Auto Channel Selection	Automatically adjusts the channel for network self-healing and performance optimization. **ChannelFly** is set as the default option. For the **ChannelFly** option, you may also modify the default settings for the **Channel Change Frequency** and **Full Optimization Period**. The **Channel Change Frequency** slidebar allows you to specify the responsiveness of ChannelFly to interference (with consideration for the impact on associated clients), ranging from Minimal to Very Often. The **Full Optimization Period** timeslot bar allows you to specify one or more periods of time when ChannelFly is allowed to fully optimize the channel plan, ignoring the impact of channel changes on associated clients. Select time periods when the wireless network is servicing the fewest clients.	Select the required option. • **Background Scanning**: Changes the AP channel when there is an interference. • **ChannelFly**: Monitors potential throughput and will change channels to learn each channel's capacity, optimize throughput, and to avoid interference.
AP Configuration > **Band/Spectrum Configuration** > **Upper 5 GHz**		
Channelization	Helps manage and allocate radio frequency resources. A lower channel width allows the zone to potentially serve more clients, whereas a higher channel width improves throughput, but potentially serves fewer clients and increases the possibility of interference. Prior to SmartZone release 7.0.0, the Auto setting defaulted to 80 MHz channelization. Beginning in SmartZone release 7.0.0, the Auto setting defaults to 40 MHz channelization.	Set the channel bandwidth used during transmission: Auto, 20, 40, 80 and 160.
Channel	Indicates the channel to use.	Select the required options for the Indoor and Outdoor APs.
Allow DFS Channels	Allows ZoneFlex APs to use DFS channels.	Click to enable the option.
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 12 Access Point Edit Parameters (continued)

Field	Description	Your Action
Auto Cell Sizing	Enables the AP to share information on interference seen by each other and dynamically adjust their radio Tx power and Rx parameters to minimize interference. Enabling this option disables the TX Power Adjustment configuration. **NOTE** Ensure that Background Scan is enabled.	Select the option.
TX Power Adjustment	Allows to manually configure the transmit power on the Upper 5 GHz radio. By default, the TX power is set to Full on the Upper 5 GHz radio. **NOTE** If you choose Min, the transmit power is set to 0dBm (1mW) per chain for 11n APs, and 2dBm per chain for 11ac APs. If you choose Max, the transmit power is set to the maximum allowable value according to the AP's capability and the operating country's regulations.	Select the preferred TX power.
Background Scan	Allows the AP radio to scan other channels in the band for accessing channel health and capacity, detecting rogue devices, optimizing and maintaining mesh links and to discover AP neighbors.	Enter the duration in seconds. Range: 1 through 65535.
Auto Channel Selection	Automatically adjusts the channel for network self-healing and performance optimization. **ChannelFly** is set as the default option. For the **ChannelFly** option, you may also modify the default settings for the **Channel Change Frequency** and **Full Optimization Period**. The **Channel Change Frequency** slidebar allows you to specify the responsiveness of ChannelFly to interference (with consideration for the impact on associated clients), ranging from Minimal to Very Often. The **Full Optimization Period** timeslot bar allows you to specify one or more periods of time when ChannelFly is allowed to fully optimize the channel plan, ignoring the impact of channel changes on associated clients. Select time periods when the wireless network is servicing the fewest clients.	Select the required option. • **Background Scanning**: Changes the AP channel when there is an interference. • **ChannelFly**: Monitors potential throughput and will change channels to learn each channel's capacity, optimize throughput, and to avoid interference.
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 overrides the AP settings.	Select the check box.
USB Port	Disables the USB port on the selected AP model.	Select the option. USB ports are enabled by default.
Status LEDs	Disable the status LED on the selected AP model.	Select the option.
LLDP	Enables the Link Layer Discovery Protocol (LLDP) on the selected AP model.	Select the option and enter the following details: • **Advertise Interval**—Enter the duration in seconds. • **Hold Time**—Enter the duration in seconds. • **Enable Management IP TLV**—Select the check box.
PoE Operating Mode	Allows you to operate using PoE mode. For optimal LAG performance, a power mode higher than 802.3at is recommended.	Select the option.
LACP/LAG	Aggregates multiple network interfaces into a single logical or bonded interface. LACP can be enabled only on two-port 11ac wave2 and 11ax APs. A minimum of two ports must be active on AP and switch for LACP/LAG configuration. Enabled on switch ports where the APs Ethernet cables are connected increases the bandwidth between the AP and the switch.	Choose the option: • Keep the AP's settings: Retains the current AP settings. • Disabled: Disables bond configuration. • Enabled: Enables bond configuration. Select the **Bond Port Profile** from the drop-down.
Port Settings	Indicates the port settings. This feature is not available if the LACP/LAG feature is selected.	Select the option and choose the required LAN option.
AP Configuration > **Advanced Options**		
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. › **Protocol**: select between UDP and TCP protocols – **Secondary Server Address**: If the primary server goes down, the AP sends syslog messages to the secondary server as backup. › **Port**: enter the syslog port number on the respective servers. › **Protocol**: select between UDP and TCP protocols – **Event Facility**: Select the facility level that will be used by the syslog message. Options include: Keep Original, Local0 (default), Local1, Local2, Local3, Local4, Local5, Local6, and Local7. – **Priority**: Select the lowest priority level for which events will be sent to the syslog server. For example, to only receive syslog messages for events with the warning (and higher) priority, select **Warning**. To receive syslog messages for all events, select **All**. – **Send Logs**: Select the type of messages to be sent to the syslog server. For example, General Logs, Client Logs or All Logs. • AP External Syslog Profile: Select the profile from the drop-down or click Add to create a new profile.

TABLE 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 **Override** option to override the aggressiveness of protecting the network and choose one of the following: – **Aggressive** – **Auto** – **Conservative** • Enable the **Override** option and enter the **Jamming Threshold** in percentage.
Recovery SSID	Allows you to enable or disable the Recovery(Island) SSID broadcast on the controller.	Enable **Recovery SSID Broadcast**
Direct Multicast	Indicates whether multicast traffic is sent from a wired device, wireless device or from the network.	Select one or more of the following: • **Multicast Traffic from Wired Client** • **Multicast Traffic from Wireless Client** • **Multicast Traffic from Network**
Test Speed	Measures the connection performance of the AP. The option must be enabled to run the SpeedFlex traffic test between wireless clients and the AP.	Enable the option.
Swap Configuration		
Add Swap-In AP	Allows to swap APs.	Select the check box and enter the **Swap-in AP MAC** details.

NOTE

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

Band or Spectrum Configuration

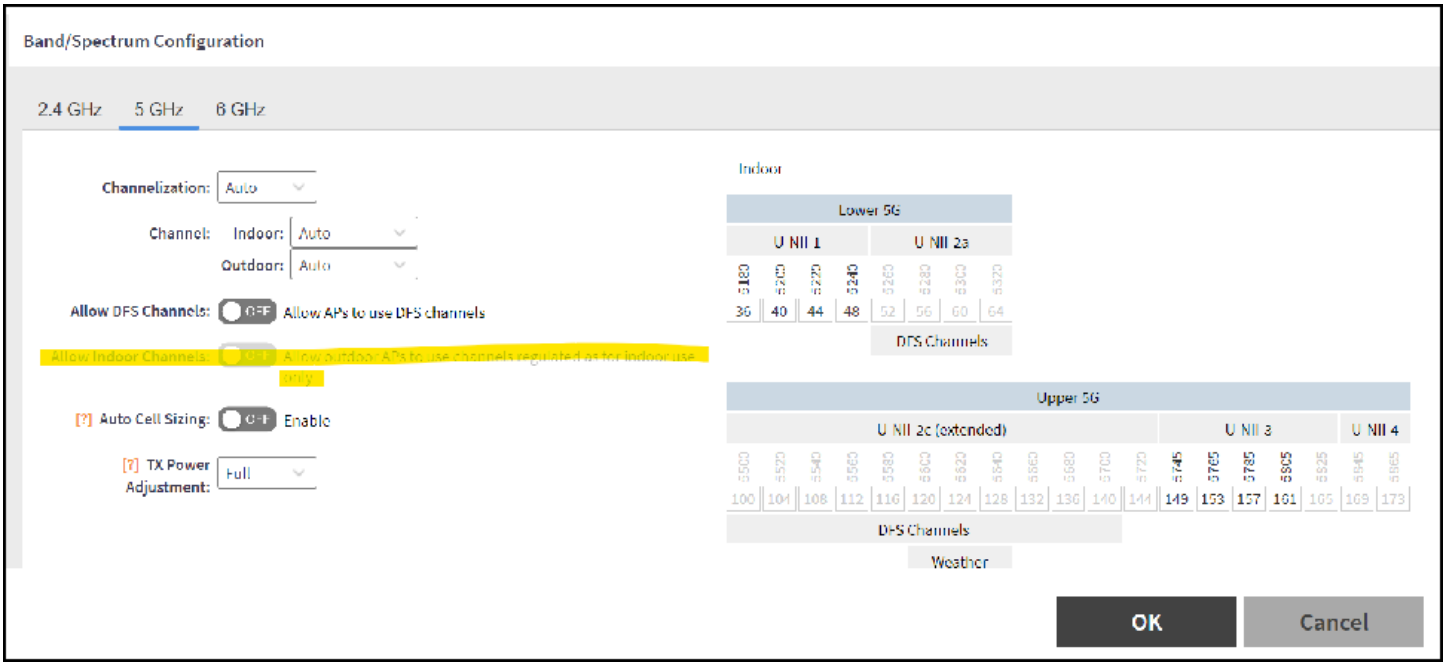
Band or spectrum configuration is a method of statistically picking the most potent channel for an AP.

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 18 Band or Spectrum Configuration



Approving Access Points

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

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

Approving Access Points Manually

To approve an AP manually, perform the following -

1. Go to **Network Wireless Access Points**.
2. On the left hand side, under **System** tree, scroll down and click on the **Staging Zone**.This displays all APs in the queue for approval.
3. Clear the **Automatically approve all join requests** from APs check box.
4. Click **Ok**.

Approving Access Points Automatically

To approve an AP automatically, perform the following -

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

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

Working with AP Registration Rules

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

> **NOTE**
> For SZ300 and vSZ-H platforms, a registration rule is only applied to an AP the first time it joins the controller. If an AP's MAC address already exists on the controller database (whether it is in connected on disconnected state and whether it belongs to the Staging Zone or any other zone), the controller will assign the AP to its last known AP zone.

> **NOTE**
> For SZ100 and vSZ-E platforms, a registration rule is only applied to an AP the first time it joins the controller. If an AP's MAC address already exists on the controller database (whether it is in connected on disconnected state and whether it belongs to the Default Zone or any other zone), the controller will assign the AP to its last known AP zone.

Creating an AP Registration Rule

You must create rules to register an AP.

To create an AP registration rule:

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

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

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

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

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

  You can choose the Rule Type as GPS coordinates, wherein you must provide information about the latitude, longitude and distance to determine if the AP is within the defined area.
- **Provision Tag**: If the access points that are joining the controller have been configured with provision tags, click the Provision Tag option, and then type a tag name in the Provision Tag box. Access points with matching tags will be automatically assigned to the AP zone that you will choose in the next step.

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

6. Click **OK**.

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

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

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

Configuring Registration Rule Priorities

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

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

Follow these steps to configure the registration rule priorities.

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

3. Click **Update Priorities** to save your changes.

Tagging Critical APs

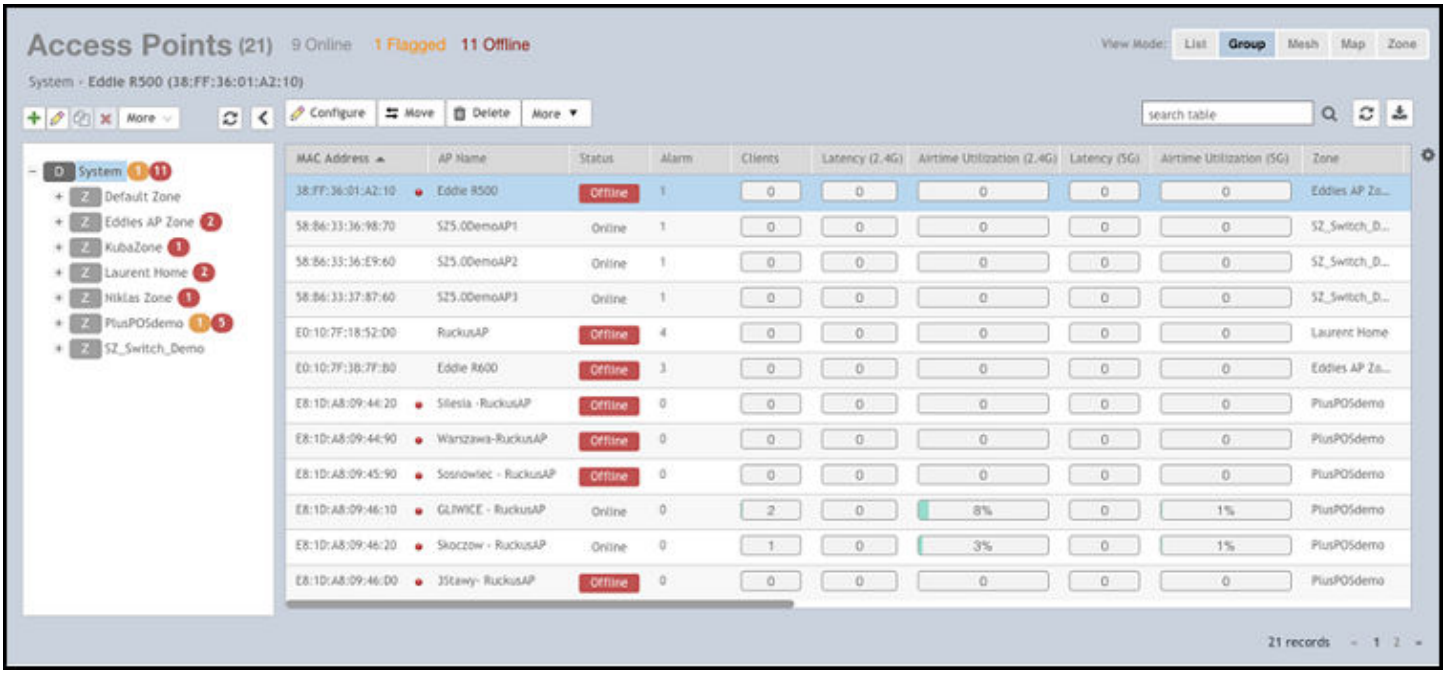
A critical AP is an AP that exceeds the daily traffic threshold (sum of uplink and downlink) data bytes configured on the controller web interface.

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

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

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

FIGURE 19 APs Tagged as Critical



Setting the Country Code

Different countries follow different regulations for radio channel usage.

To ensure that the APs use authorized radio channels:

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

Configuring the Tunnel UDP Port

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

To configuring the tunnel UDP port:

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

Creating an AP MAC OUI Address

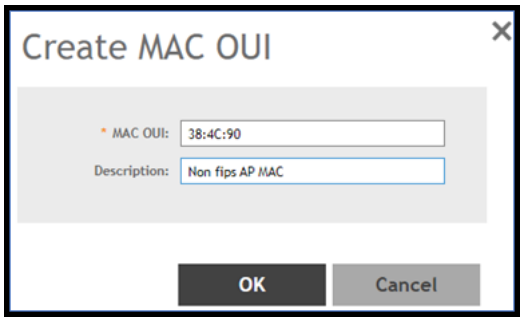
To create the MAC OUI address for an AP, perform the following -

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

FIGURE 20 AP MAC OUI Validation

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

   FIGURE 21 Create MAC OUI

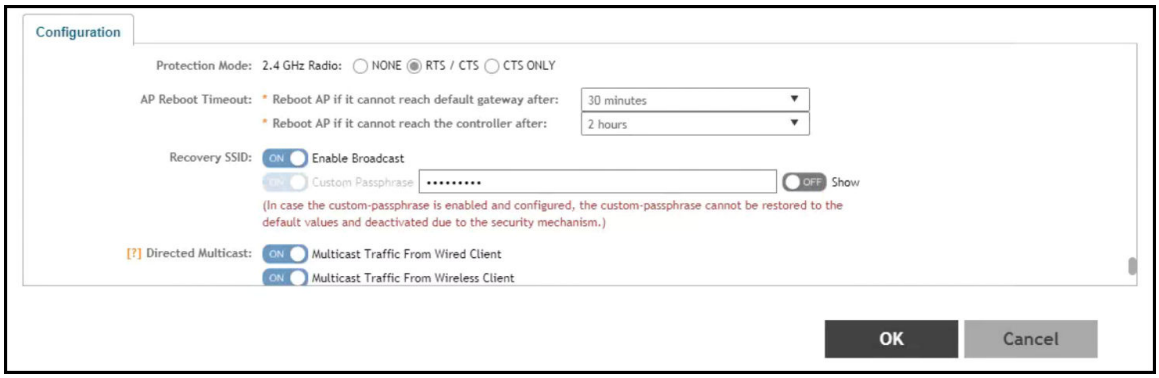


4. Enter the **MAC OUI**.
5. Click **OK**.

AP Admin Password and Recovery SSID

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

Consider the following scenario while generating the configuration:



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

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

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

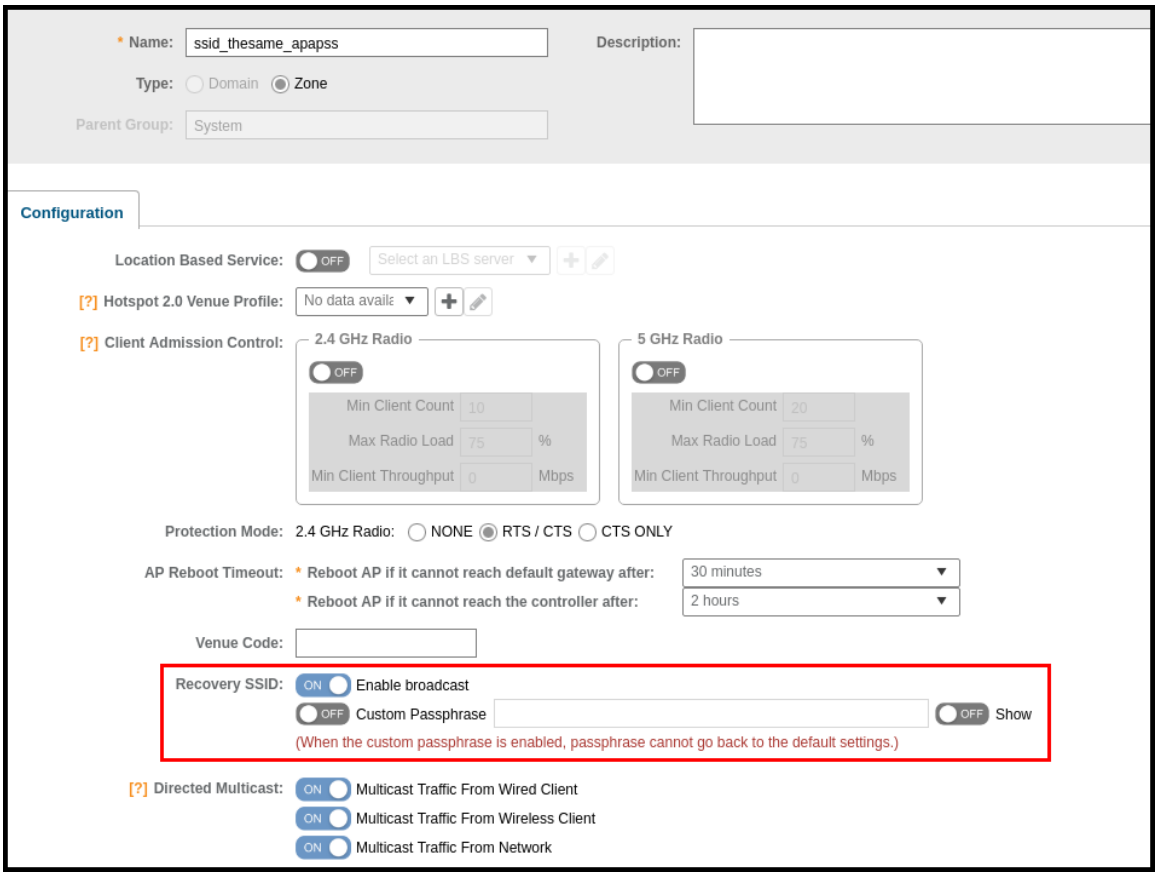
The recovery SSID passphrase(key) will be delivered in GPB configuration as below:

- ccm_zone.proto
- message CcmCommon {
- /** recovery ssid

- */
- optional bool recovery_ssid_enabled = 26
- optional string recovery_ssid_psk_key = 27
- optional int32 server_loss_timeout = 28

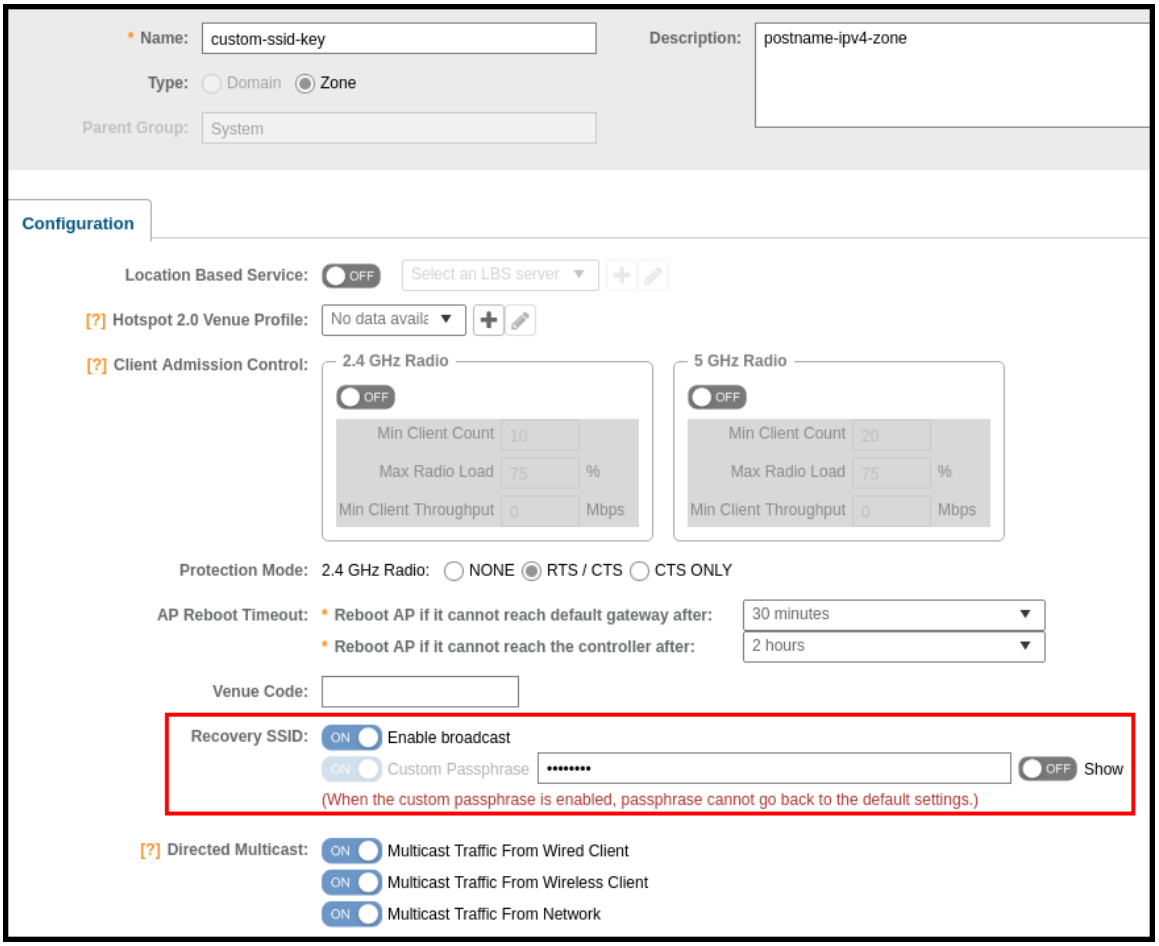
When the Custom passphrase is disabled, the Custom passphrase filed is empty.

FIGURE 22 Custom Passphrase Disabled



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

FIGURE 23 Custom Passphrase Enabled



Power Source in AP Configuration

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

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

The PoE mode as per the industry standards:

TABLE 13 Industry Standard PoE Modes

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

TABLE 14 Non-Standard High Power Solution Summary

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

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

TABLE 15 PoE Mode Settings

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

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

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

POE tables for different 11 AC Access Point

TABLE 16 R710

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

TABLE 17 R610

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

TABLE 18 R720

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

TABLE 18 R720 (continued)

3bt/class5	35W	4/4	4/4	Enabled	Enabled	Enabled	No comments
POE Injector (Model 480125A) 60W	N/A	4/4	4/4	Enabled	Enabled	Enabled	Force to 802.3bt/ class5 from the controller GUI

TABLE 19 T610

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

POE tables for different 11 AX Access Point

TABLE 20 R850

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

TABLE 21 R750

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

TABLE 22 T750

	LLDP Power Ask	**2.4G tx/rx**	**5G tx/rx**	**2.5Gbps eth**	**1Gbps eth**	**USB**	**IOT**	**PSE**	**Comment**
DC	N/A	4/4	4/4	Enabled	Enabled	Enabled	Enabled	Enabled	No comments

TABLE 22 T750 (continued)

AF	N/A	1/4	1/4	Enabled	Disabled	Disabled	Disabled	Disabled	Not supported operation mode
AT w/o USB	25W	4/4	4/4	Enabled	Enabled	Disabled	Enabled	Disabled	No comments
AT with USB	25W	2/4	4/4	Enabled	Disabled	Enabled	Enabled	Disabled	Set AT - mode = 1 via Rkscli
802.3bt/ class5	35W	4/4	4/4	Enabled	Enabled	Enabled	Enabled	Disabled	No comments
803.3bt/ class6	N/A	4/4	4/4	Enabled	Enabled	Enabled	Enabled	Disabled	51W by H/W negotiation
802.3bt/ class7	N/A	4/4	4/4	Enabled	Enabled	Enabled	Enabled	Enabled	62W by H/W negotiation
POE 60W Injector (Model 480125A)	N/A	4/4	4/4	Enabled (1Gbps speed)	Enabled	Enabled	Enabled	Disabled	Force to 802.3bt/ class5
POE 90W Injector	N/A	4/4	4/4	Enabled	Enabled	Enabled	Enabled	Enabled	Force to 802.3bt/ class7

TABLE 23 R650

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

TABLE 24 R550

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

POE tables for different 11AT/ BT5 Access Point

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

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

TABLE 25 R760

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

Monitoring Access Points

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

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

TABLE 26 Access Point Monitoring Tabs

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

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

- **Select ALL** - Selects all the APs in the list.
- **Deselect All**- Clears all selection from the list.
- **Troubleshooting > Client Connection** - Connects to client devices and analyze network connection issues in real-time. See, *Troubleshooting Client Connections*.
- **Troubleshooting > Spectrum Analysis** - Troubleshoots issues remotely, identify sources of interferences within the network and allow administrators access to the RF health of the network environment. See, *Troubleshooting through Spectrum Analysis*.
- **Restart** - Restarts an access point remotely from the web interface.

- **Lock** - Disables all WLAN services on the AP and disconnect all wireless users associated with those WLAN services temporarily.
- **Unlock** - Makes all WLAN services available.
- **Import Batch Provisioning APs** - Import the provisioning file. See, Options for Provisioning and Swapping APs on page 41
- **Import Swapping APs** - Manually trigger the swapping of two APs by clicking the swap action in the row. See, Options for Provisioning and Swapping APs on page 41
- **Export All Batch Provisioning APs** Downloads a CSV file that lists all APs that have been provisioned.. See, Options for Provisioning and Swapping APs on page 41
- **Export All Swapping APs** - Downloads a CSV file that lists all APs that have been swapped. See, Options for Provisioning and Swapping APs on page 41
- **Download Support Log** - Downloads support log.
- **Trigger AP Binary Log** - Triggers binary log for the selected AP.
- **Trigger Preferred Node** - Triggers an AP that belongs to the current zone to connect to the preferred node. See Triggering a Preferred Node on page 62.
- **Download CM Support Log** - Downloads Cable Momdem support log.
- **Restart Cable Modem** - Restarts the cable modem. The AP will disconnect from the network for a short period. The AP will disconnect from the network for a short period.
- **Reset Cable Modem** - Resets the cable modem.
- **Reset Cable Modem to Factory Default** - Resets the cable modem to factory default settings.
- **Untag Critical APs** - Stating APs as non-critical. See, Tagging Critical APs on page 84.
- **Swap** - Swaps current AP to swap-in AP. See, Editing Swap Configuration on page 137
- **Switch Over Clusters** - Moves APs between clusters. See Configuring AP Switchover on page 53.
- **Approve** - Approves AP and completes registering. See, Working with AP Registration Rules on page 82.

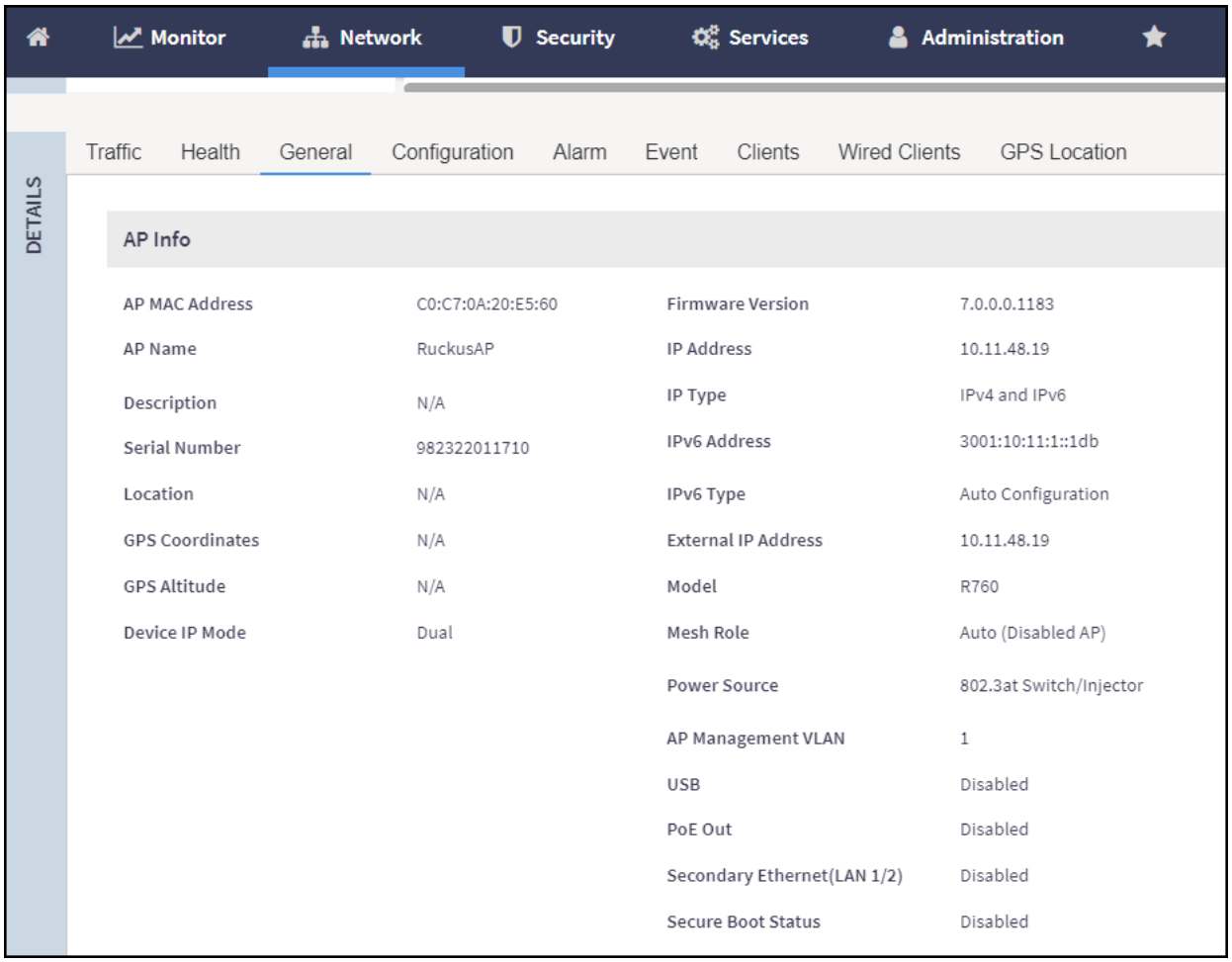
Viewing General AP Information

Complete the following steps to view general AP information.

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

2. In the **General** tab, scroll to the **AP Info** information.

FIGURE 24 General AP Information



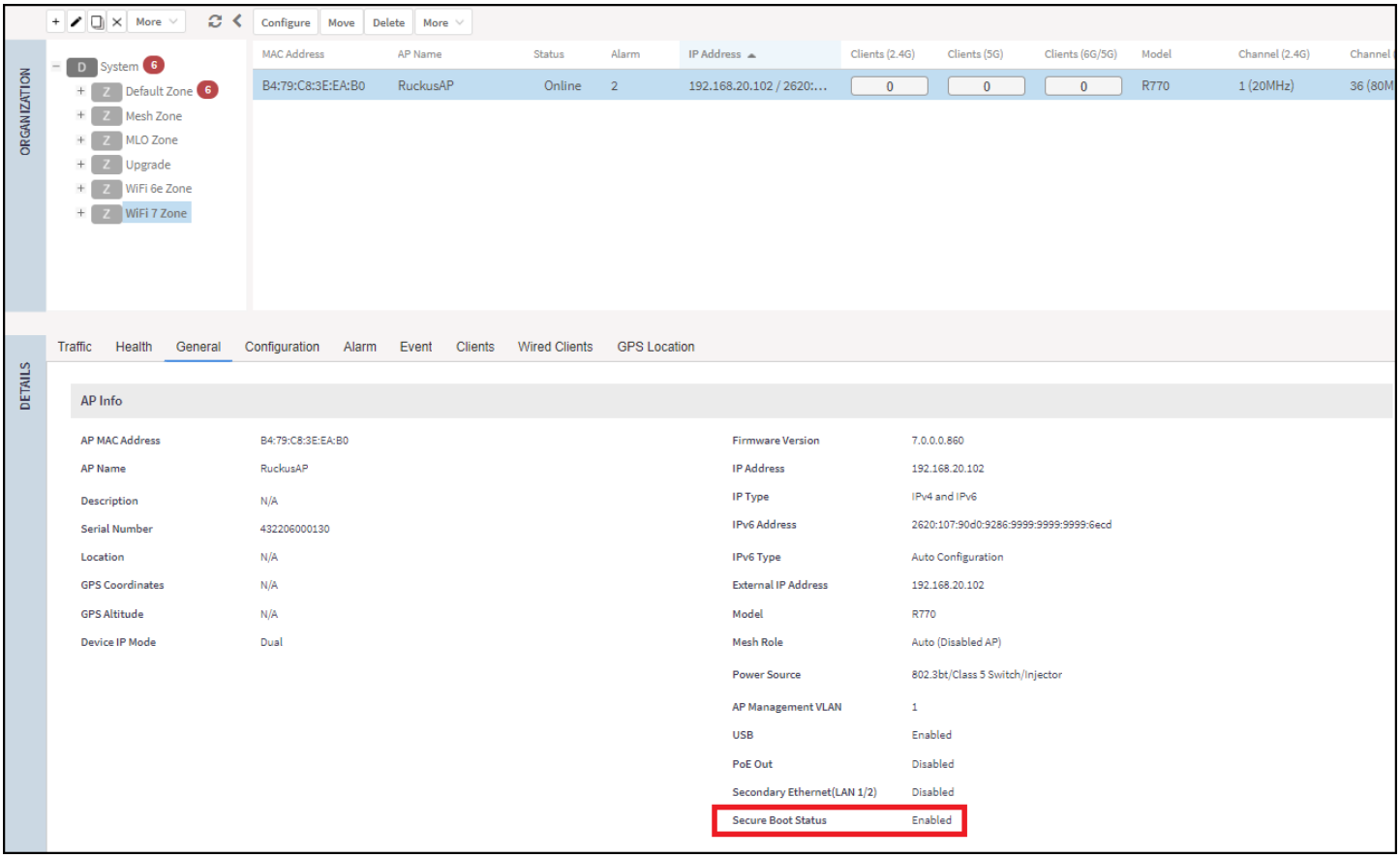
NOTE
For 6.1.1 and later releases, the **Onboard IoT Radio** status is removed.

Secure Boot

Overview

The Secure Boot is a security technology that safeguards against the unauthorized modification of software binaries. The objective of this feature is to implement a secure boot process that includes digital signatures and verification for all bootloader images, up to and including u-boot. This process is designed to prevent unauthorized or corrupted bootloader software from being loaded onto RUCKUS APs during the boot-up sequence.

FIGURE 25 Viewing Secure Boot Status



Requirements

The SmartZone 7.0 and later releases support Secure Boot.

Considerations

NOTE

RUCKUS currently has an Image signing feature, but it's important to note that this feature exclusively signs and verifies the 'rcks_fw.bl7,' which contains the Kernel and Root File System. It does not cover the signing and verification of the bootloader images stored in NOR flash.

Running a Speed Test

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

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

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

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

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

1. From the main menu, go to **Network** > **Wireless**, select **Access Points**.

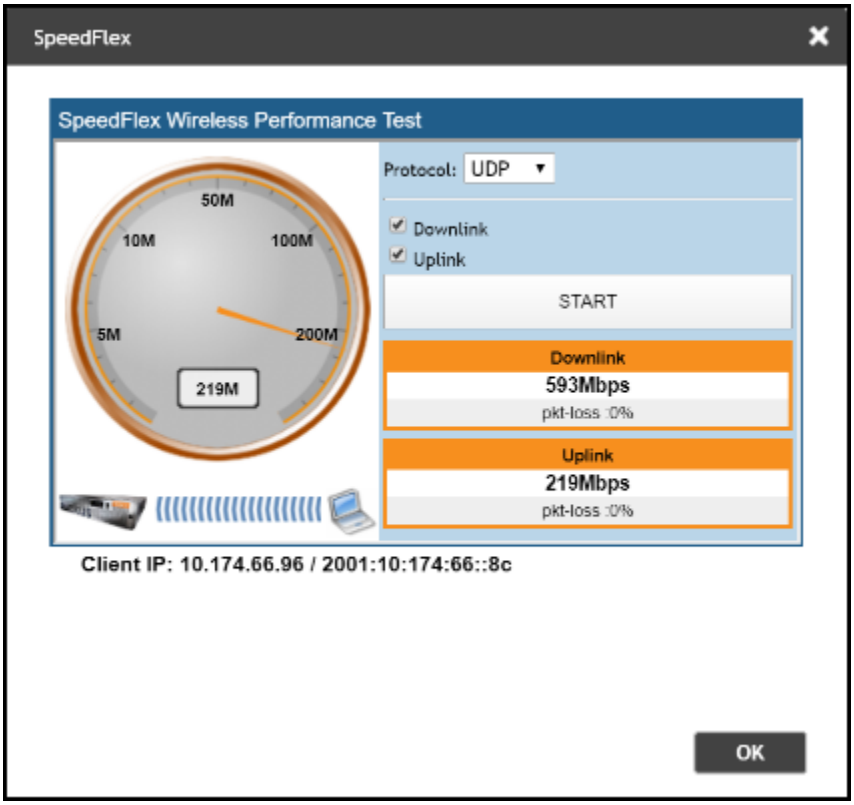
   The **Access Points** page is displayed.
2. Select an AP from the list and then select the **Health** tab.
3. Click **Test Speed**.

   The **SpeedFlex** page is displayed.

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

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

   FIGURE 26 SpeedFlex Test Result



AP Domains

Creating an AP Domain

To create an AP domain:

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

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

NOTE

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

Limiting the Number of APs in a Domain or Zone

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

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

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

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

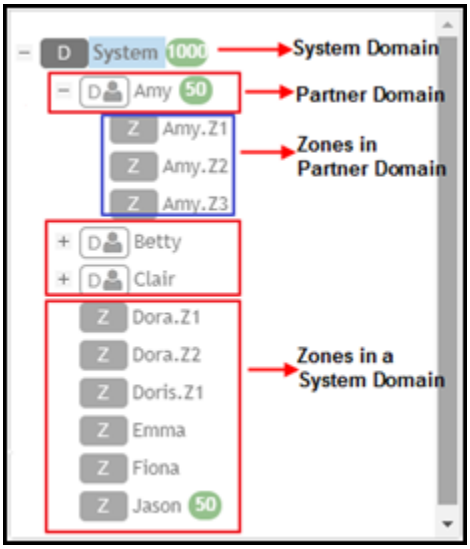
- If the AP number limitation of a Domain or a Zone is increased or reduced.

- If the license capacity is changed.

The following image gives a clarity on:

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

FIGURE 27 System Hierarchy



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

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

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

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

Limiting the AP count for a Zone in a Partner Domain

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

1. Create a super admin account for the partner domain. See the Administrating the Controller chapter.

2. Create a user group and configure the access permissions, resources and administrator account. Refer to the **Creating User Groups** section of the *SmartZone Management Guide (SZ300/vSZ-H)*.

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

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

     ```
     Account Name@Domain
     ```

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

     ```
     User@TestDomain
     ```

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

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

Hierarchy

Hierarchy Overview

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

You can virtually split them using the following hierarchy:

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

Link Layer Discovery Protocol (LLDP)

Link Aggregation Control Protocol (LACP) support for R720 AP

The R720 AP is a four-stream 802.11ac Wave 2 access point. The AP can transmit to multiple Wave 2 clients in parallel, improving the RF efficiency in addition to faster connectivity and reliable network performance.

NOTE
LACP or Bonding feature is configurable using AP RKS CLI mode though the web user interface configuration option is limited to APs R720, R710 and R610.

NOTE
LACP or Bonding feature option enable or disable is a service-affecting feature configuration. This feature can be used during setup or maintenance mode only when there are no active downlink (DL) or uplink (UL) traffic in progress.

NOTE
To support LACP or Link Aggregation Group (LAG) feature on RUCKUS APs, the administrator needs to ensure correct PoE power modes to Bring-Up LAN1 and 2 ports. For example, PoE-at+ for R720, PoE-at for R710, and so on. Refer to the respective AP product guides for details. LACP/LAG UL throughput is limited to around 1 Gbps.

Supported LLDP Attributes

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

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

TABLE 27 LLDP Attributes

Attribute (TLV)	Description
Chassis ID	Indicates the MAC address of the AP's br0 interface
Port ID	Identifies the port from which the LLDP packet was sent
Time to Live	Same as LLDP Hold Time. Indicates the length of time (in seconds) that a receiving device will hold the LLDP information sent by the selected AP model before discarding it. The default value is 120 seconds.
System Name	Indicates the name assigned to the AP. The default name of RUCKUS APs is RuckusAP.
System Description	Indicates the AP model plus software version

TABLE 27 LLDP Attributes (continued)

Attribute (TLV)	Description
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

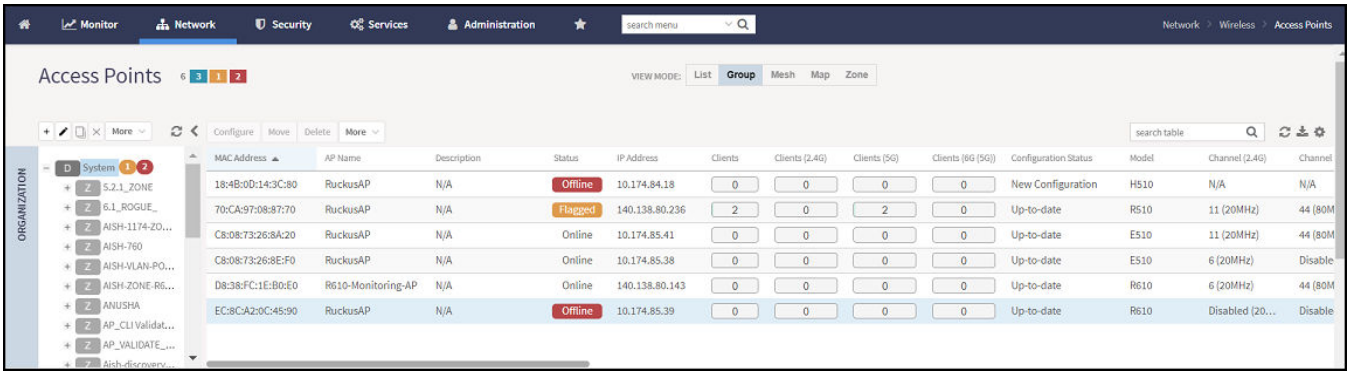
Enabling the LACP Support for a Zone

Perform the following procedure to enable the LACP support for a zone.

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

   The **Access Points** page is displayed.

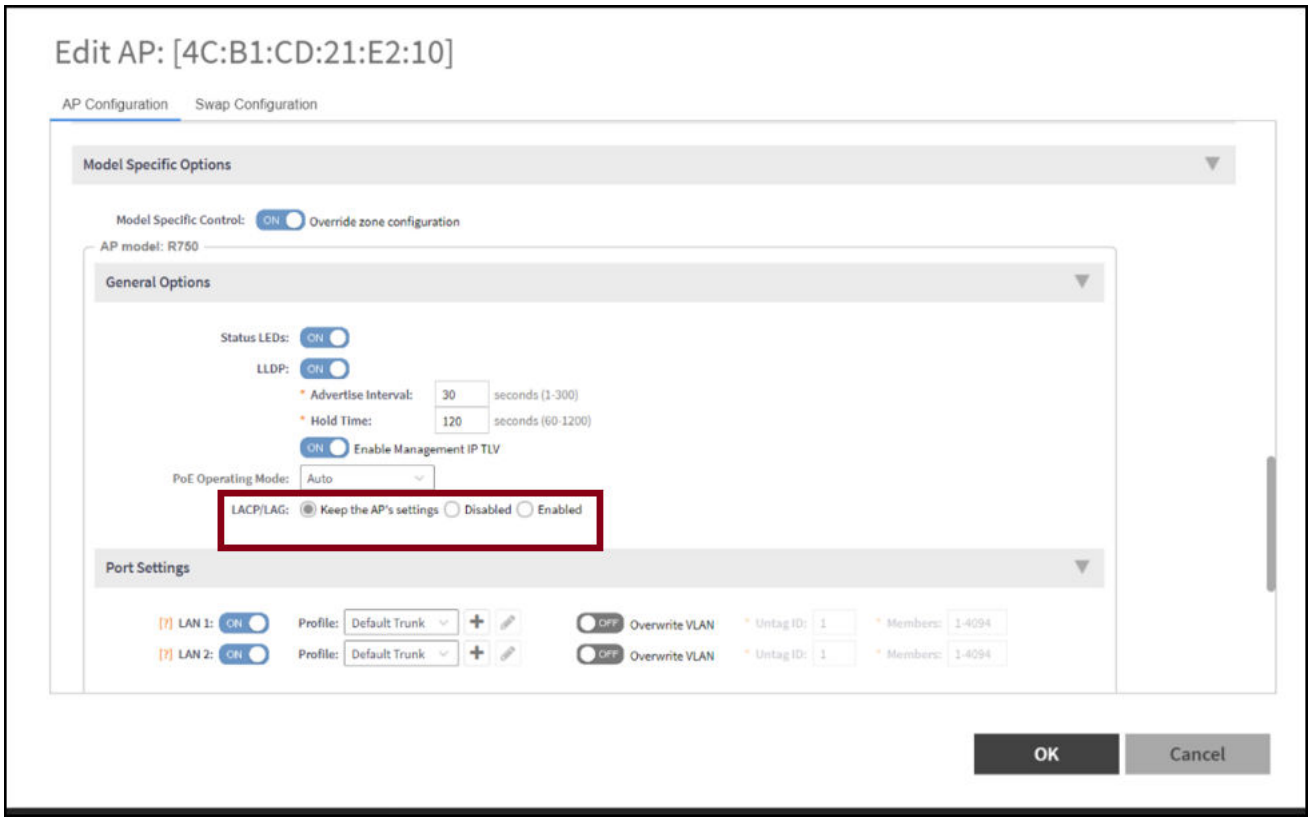
   FIGURE 28 Viewing the Access Points



2. Select a zone and click  .

   The **Configure Group** page is displayed.

   FIGURE 29 Enabling LACP Support for a Zone



3. Enter the zone name.
4. Under **Configuration**, select **R720** from the **Select an AP Model** list.
5. Under **General Options**, enable **LACP**.

   NOTE
   By default, LACP is disabled.

   NOTE
   To support the LACP and LAG feature on RUCKUS APs, ensure that the correct PoE mode is selected to bring up LAN1,2 ports. For example, PoE-at+ for R720, PoE-at for R710. The LACP and LAG UL throughput is limited to around 1Gbps.

6. Click **OK**.

Enabling LACP Support for an AP

Perform the following procedure to enable the LACP support for an AP.

1. From the main menu, go to **Network** > **Wireless**, select **Access Points**. The Access Point page is displayed.
2. Select an AP group from the zone.
3. Select an AP and click .
4. In the **Edit AP** page, enter the AP name.
5. Under **Configuration**, select **R720** from the **Select an AP Model** list.
6. Under **General Options**, enable **LACP**.

   NOTE
   By default, LACP is disabled.

   NOTE
   To support the LACP and LAG feature on RUCKUS APs, ensure that the correct PoE mode is selected to bring up LAN1,2 ports. For example, PoE-at+ for R720, PoE-at for R710. The LACP and LAG UL throughput is limited to around 1Gbps.

7. Click **OK**.

   NOTE
   When you enable or disable LACP, the corresponding status is updated in the **General** tab of the **Access Points** page.

Enabling LACP Support for an AP Group

Perform the following procedure to enable the LACP support for an AP group.

1. From the main menu, go to **Network** > **Wireless**, select **Access Points**.
2. Select an AP group from the zone and click .
3. In the **Configure** page, enter the name of the AP group.
4. Under **Configuration**, select **R720** from the **Select an AP Model** list.
5. Under **General Options**, enable **LACP**.

   NOTE
   By default, LACP is disabled. To enable LACP, both **LACP** and **Override** must be enabled.

   NOTE
   To support the LACP and LAG feature on RUCKUS APs, ensure that the correct PoE mode is selected to bring up LAN1,2 ports. For example, PoE-at+ for R720, PoE-at for R710. The LACP and LAG UL throughput is limited to around 1Gbps.

6. Click **OK**.

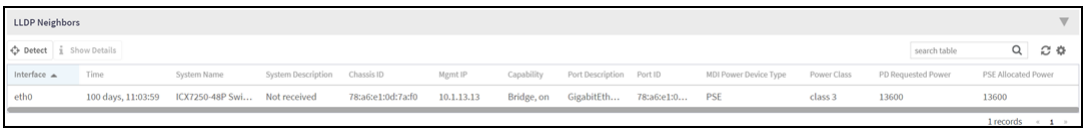
Viewing LLDP Neighbors

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

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

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

   FIGURE 30 Neighbor LLDP APs for a Non-Mesh Zone

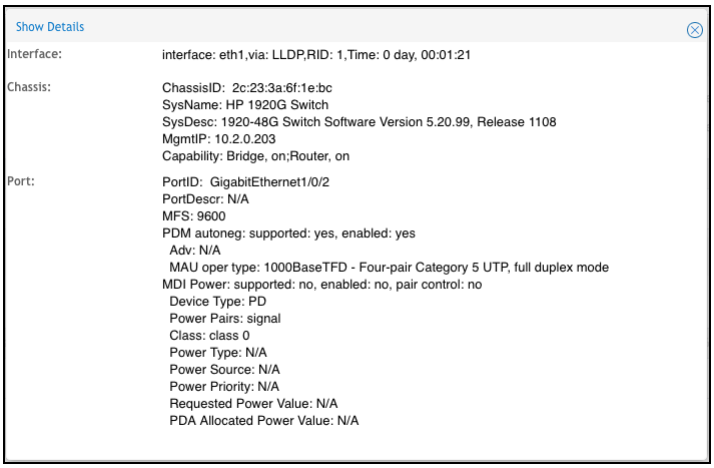


   You can view basic information about the LLDP AP neighbor such as:

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

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

   FIGURE 31 Additional LLDP AP Neighbor Details



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

Model Specific Settings

Configuring Model-Based Settings

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

Complete the following steps to configure model based settings.

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

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

TABLE 28 Configuring the Model Specific Options

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

TABLE 28 Configuring the Model Specific Options (continued)

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

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

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

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

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

TABLE 29 Configuring the Options for LAN Port

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

7. Click **OK**.

Configuring the Port Settings of a Particular AP Model

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

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

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

   The following restrictions apply:

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

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

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

Multiple Tunnel Support

Multi-Tunnel Support for Access Points

In prior RUCKUS solutions, APs could only support a single tunnel to a data plane, as well as a local break out. In this release, we're adding support for RUCKUS APs to provide multiple simultaneous tunnels to different data planes.

For 5.0, the AP will support a single RUCKUS GRE tunnel (with our without encryption) while supporting up to three SoftGRE (without encryption) tunnels, in addition to local breakout option. The tunneling will be based on SSID configurations on the AP.

This feature is designed to help in common MSP (Managed Service Provider) use cases, where each of the MSP's customer will have the possibility to get its own tunnel directly to the data center.

Before configuring multiple tunnels, consider the following configuration prerequisites:

- Ensure that there is a reachable SoftGRE gateway and also verify that there is network connectivity.
- Ensure that the zone is configured with correct SoftGRE gateway information.
- Verify that the SSID to SoftGRE tunnel mapping is correct.
- Verify the SoftGRE tunnel configuration and run time status using the command **get softgre***tunnel-index*. The tunnel index can be 1, 2, or 3.

Configuring Multiple Tunnels for Zone Templates

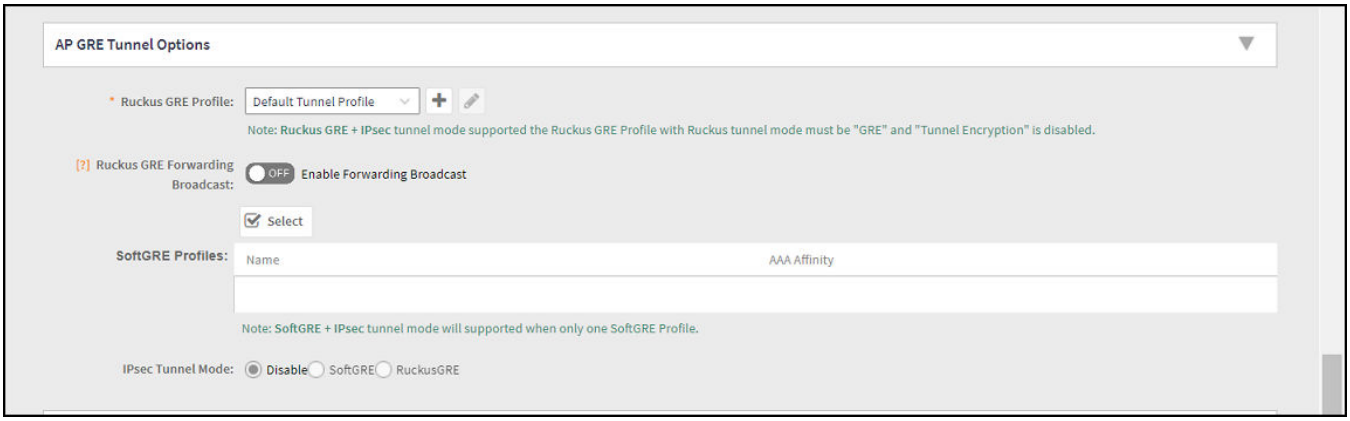
Multiple tunnels can be configured for a zone template.

Perform the following steps to select a tunnel profile for a zone template.

1. From the main menu, go to **Administration** > **System** > **Template** > **Zone Templates**.
2. Click **Create**.

   The **Create Zone Template** form appears.

   FIGURE 32 Configuring a RUCKUS GRE Profile

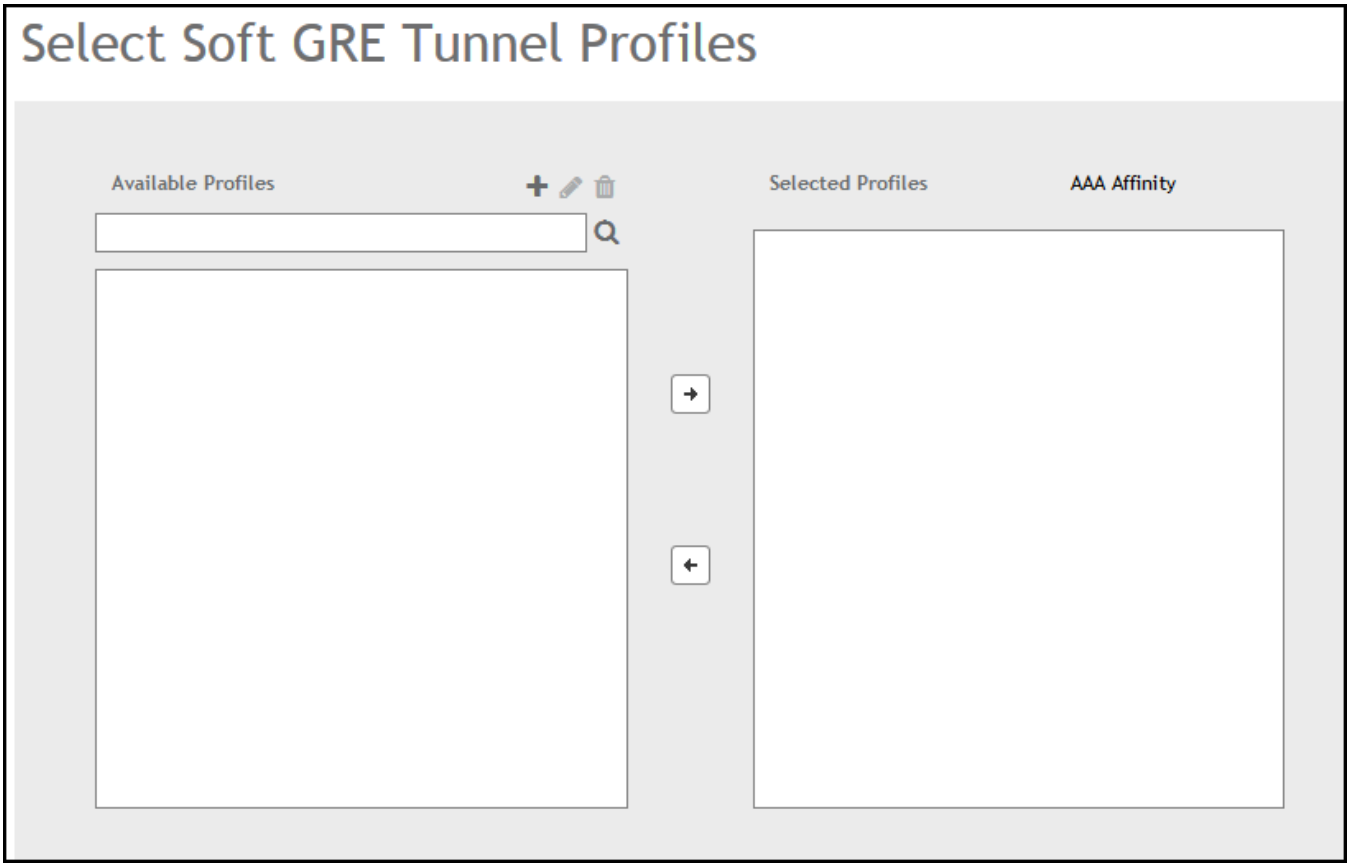


3. Navigate to the **AP GRE Tunnel Options** section.
4. For the **Ruckus GRE Profile** select a profile from the drop-down menu.

   Click the **+** icon to create a new Ruckus GRE profile.
5. Click the **Select** checkbox above the SoftGRE Profiles box.

   A form appears from which you can select the SoftGRE profiles that you want to apply to the zone. The profiles you can select are displayed under **Available Profiles**. Select the profile and click the **->** icon to choose it. The profile is now listed under the **Selected Profiles** area.

   FIGURE 33 SoftGRE Profiles Form



   You can also click the **+** icon to create a new SoftGRE profile.

   If you wish to deselect a profile, select it and click the **<-** icon. The profile will be moved back to the **Available Profiles** area and will not be applied to that zone.
6. Click **OK**.

   Your multiple tunnel configuration for the zone template is saved.

Configuring Multiple Tunnels for Zone

Multiple tunnels can be configured for a zone.

To configure the tunnel types for an AP zone, perform the following steps.

1. From the main menu, go to **Network** > **Wireless**, select **Access Points**, the **Access Point** page is displayed, select the AP from the list.
2. From the System tree, select the location where you want to create the zone. For example, System or Domain. Click **+** icon.

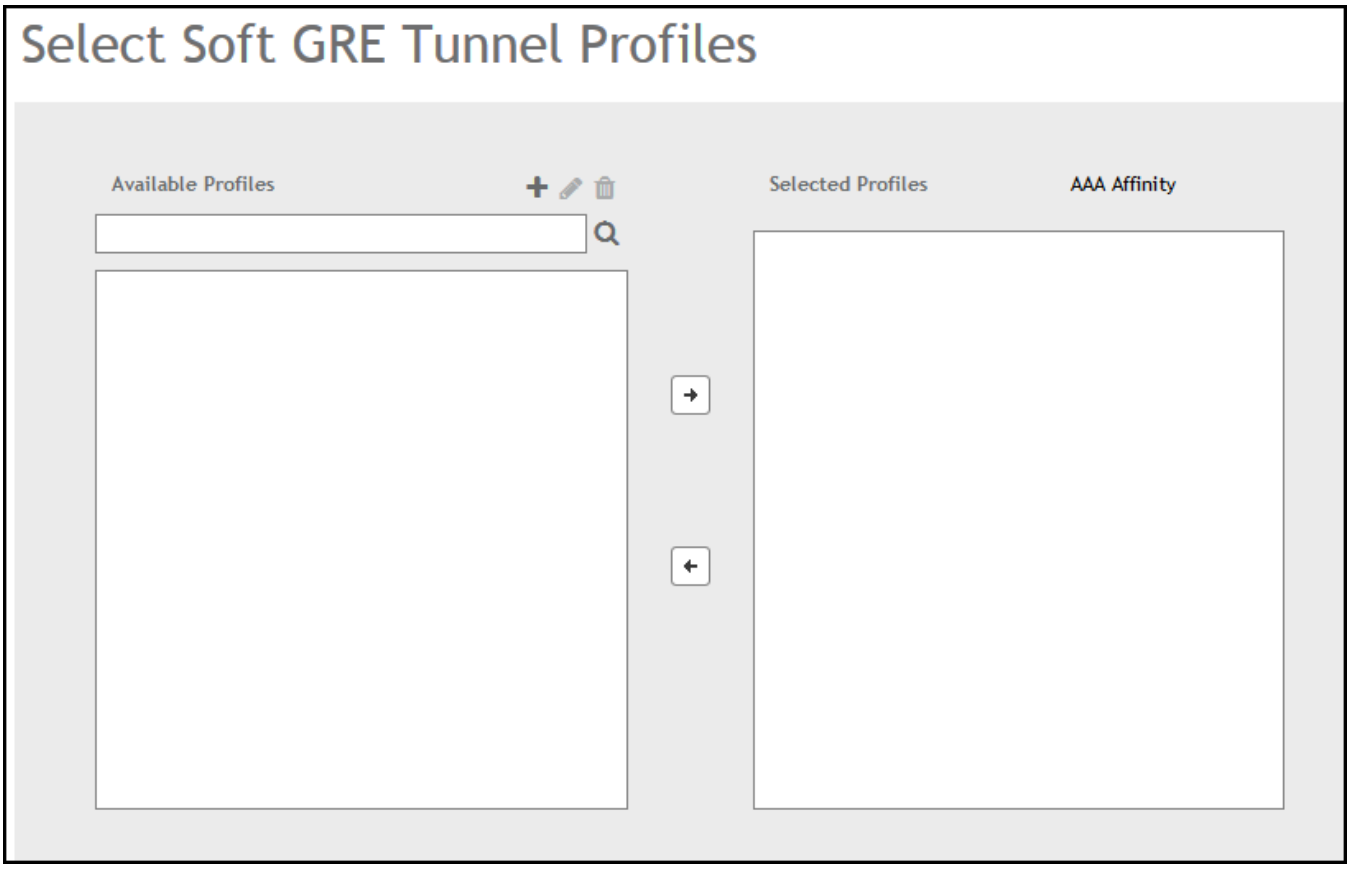
   The **Create Group** page appears.
3. Under **Type**, select **Zone**.
4. Navigate to the **AP GRE Tunnel** section.
5. For the **Ruckus GRE Profile** select a profile from the drop-down menu.

   Click the **+** icon to create a new Ruckus GRE profile.

6. Click the **Select** checkbox above the SoftGRE Profiles box.

   A form appears from which you can select the SoftGRE profiles that you want to apply to the zone. The profiles you can select are displayed under **Available Profiles**. Select the profile and click the **->** icon to choose it. The profile is now listed under the **Selected Profiles** area.

   FIGURE 34 SoftGRE Profiles Form



   You can also click the **+** icon to create a new SoftGRE profile.

   If you wish to deselect a profile, select it and click the **<-** icon. The profile will be moved back to the **Available Profiles** area and will not be applied to that zone.

7. Click **OK**.

   Your multiple tunnel configuration for the zone is saved.

Configuring Multiple Tunnels in WLANs

In WLANs where there is an option to tunnel the traffic, you can choose the tunneling profile the WLAN can use.

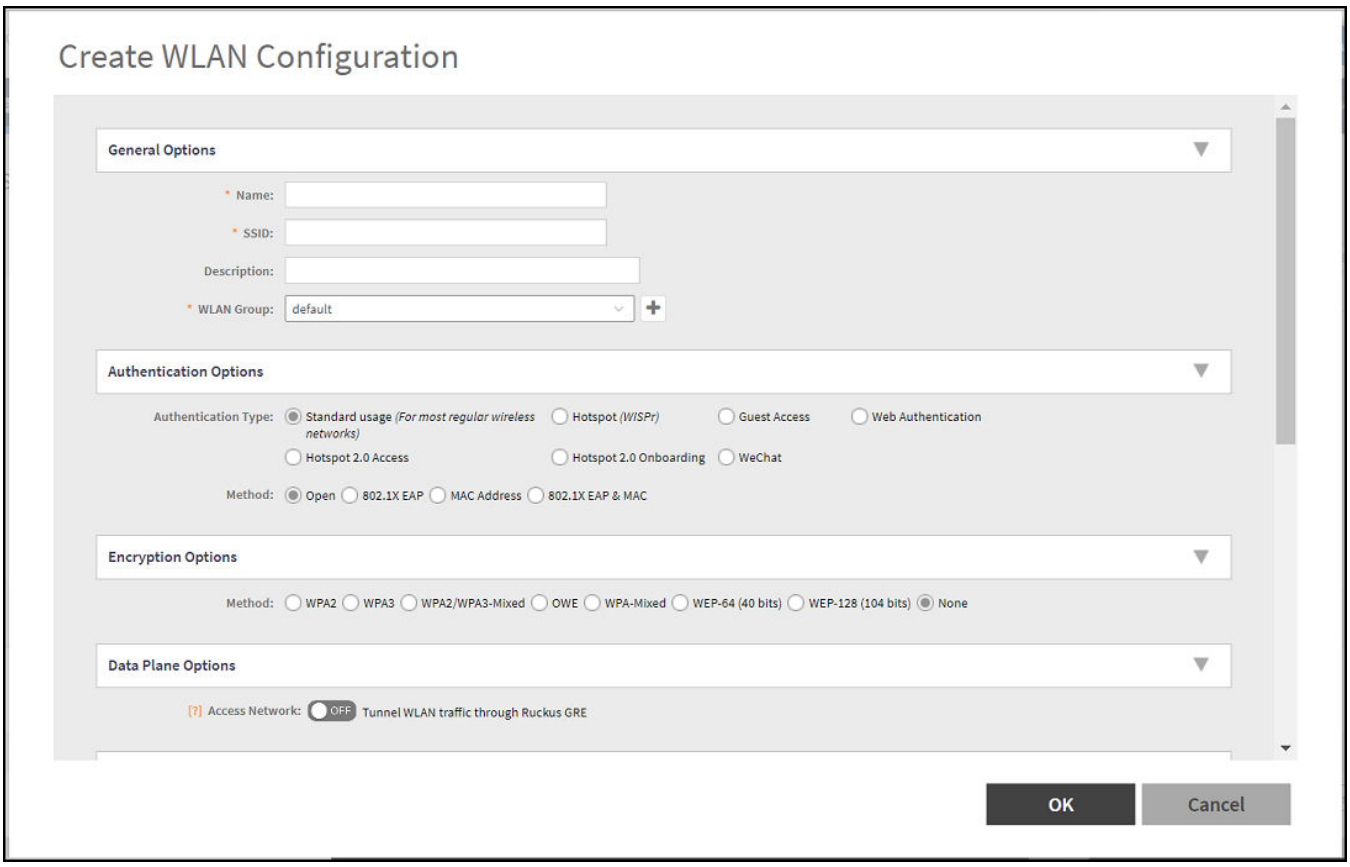
Perform the following steps to enable tunneling in WLANs.

1. Go to **Network** > **Wireless** > **Wireless LANs**, from the **System tree hierarchy**, select the **Zone** where you want to create a WLAN.

2. Click **Create**.

   The **Create WLAN Configuration** page appears.

   FIGURE 35 Tunneling Options while Creating a WLAN Configuration



3. In the section **Data Plane Options** , enable the **Tunnel WLAN traffic through Ruckus GRE** switch.

You have successfully configured the tunneling option to forward traffic in a WLAN.

Neighbor APs

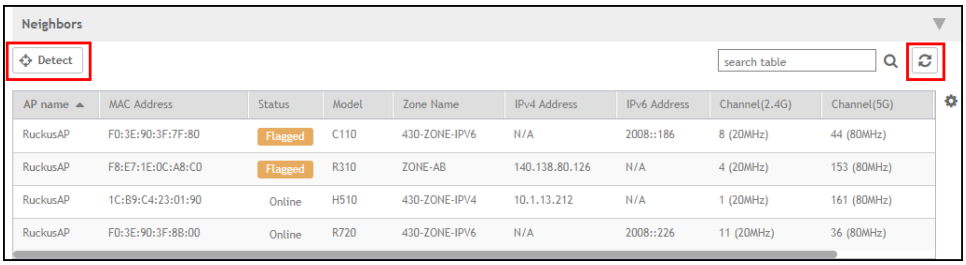
Viewing Neighbor APs in a Non-Mesh Zone

To view neighbor APs in a Non-Mesh zone:

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

   The list of neighboring APs are displayed in the table.

   FIGURE 36 Neighbor APs for a Non-Mesh Zone



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

Packet Capture

Configuring Packet Capture for APs

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

To configure Packet Capture:

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

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

         Wireshark station IP: Enter the IP address.

         MAC Address Filter: Enter the MAC address.

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

         Wireshark station IP: Enter the IP address.

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

         MAC Address Filter: Enter the MAC address.

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

         MAC Address Filter: Enter the MAC address.

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

Support Logs

Application Logs

Application Logs

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

Viewing and Downloading Logs

Complete the following steps to view and download logs.

1. From the main menu, click **Monitor**.
2. Under **Troubleshooting & Diagnostics**, click **Application Logs**.

   The **Application Logs** screen is displayed.
3. Select a control plane from the **Select Control Plane** dropdown list to view and download logs.
4. Select the **Log Type** and click **Download**. You can download the logs using the following options.

TABLE 30 Download Options

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

System Logs

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

The following table lists the controller applications that are running.

TABLE 31 Controller Applications and Log Types for SZ300 and vSZ-H controller platforms

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

TABLE 32 Controller Applications and Log Types for SZ100 and vSZ-E controller platforms

Application	Description
API	The application program interface (API) provides an interface for customers to configure and monitor the system
CaptivePortal	Performs portal redirect for clients and manages the walled garden and blacklist
Cassandra	The controller database server that stores most of the run-time information and statistical data
Configurer	Performs configuration synchronization and cluster operations (for example, join, remove, upgrade, backup, and restore)
Diagnostics	An interface that customers can use to upload RUCKUS scripts for performing troubleshooting or applying software patches

TABLE 32 Controller Applications and Log Types for SZ100 and vSZ-E controller platforms (continued)

Application	Description
ElasticSearch	Scalable real-time search engine used in the controller
MemCached	The controller memory cache that stores client authentication information for fast authentication or roaming
MemProxy	Replicates MemCached entries to other cluster nodes
Mosquitto	A lightweight method used to carry out messaging between LBS and APs
Northbound	Performs UE authentication and handles approval or denial of UEs to APs
RadiusProxy	Sets the RADIUS dispatch rules and synchronizes configuration to each cluster node
SNMP	Provides a framework for the monitoring devices on a network. The SNMP manager is used to control and monitor the activities of network hosts using SNMP.
SubscriberManagement	A process for maintaining local user credentials for WISPr authentication
SubscriberPortal	Internal portal page for WISPr (hotspot)
System	Collects and sends log information from all processes
Web	Runs the controller management web server

Downloading the Support Log from an Access Point

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

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

To download a support log from an AP:

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

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

Debugging an AP Failure

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

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

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

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

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

8. Extract the file to get the himem rb0 logs .gz files.

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

Reports

Rogue Devices

Viewing Rogue Devices

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

If the user has enabled rogue AP detection, a zone is configured for monitoring (refer to Configuring Monitoring APs), click **Report** > **Rogue Devices**. Under **Device Type**, select **Access Point** or **Client**. The **Rogue Devices** page displays all the rogue APs or rogue clients that the controller has detected on the network, including the following information:

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

Marking Rogue Access Points

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

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

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

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

Locating a Rogue Device

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

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

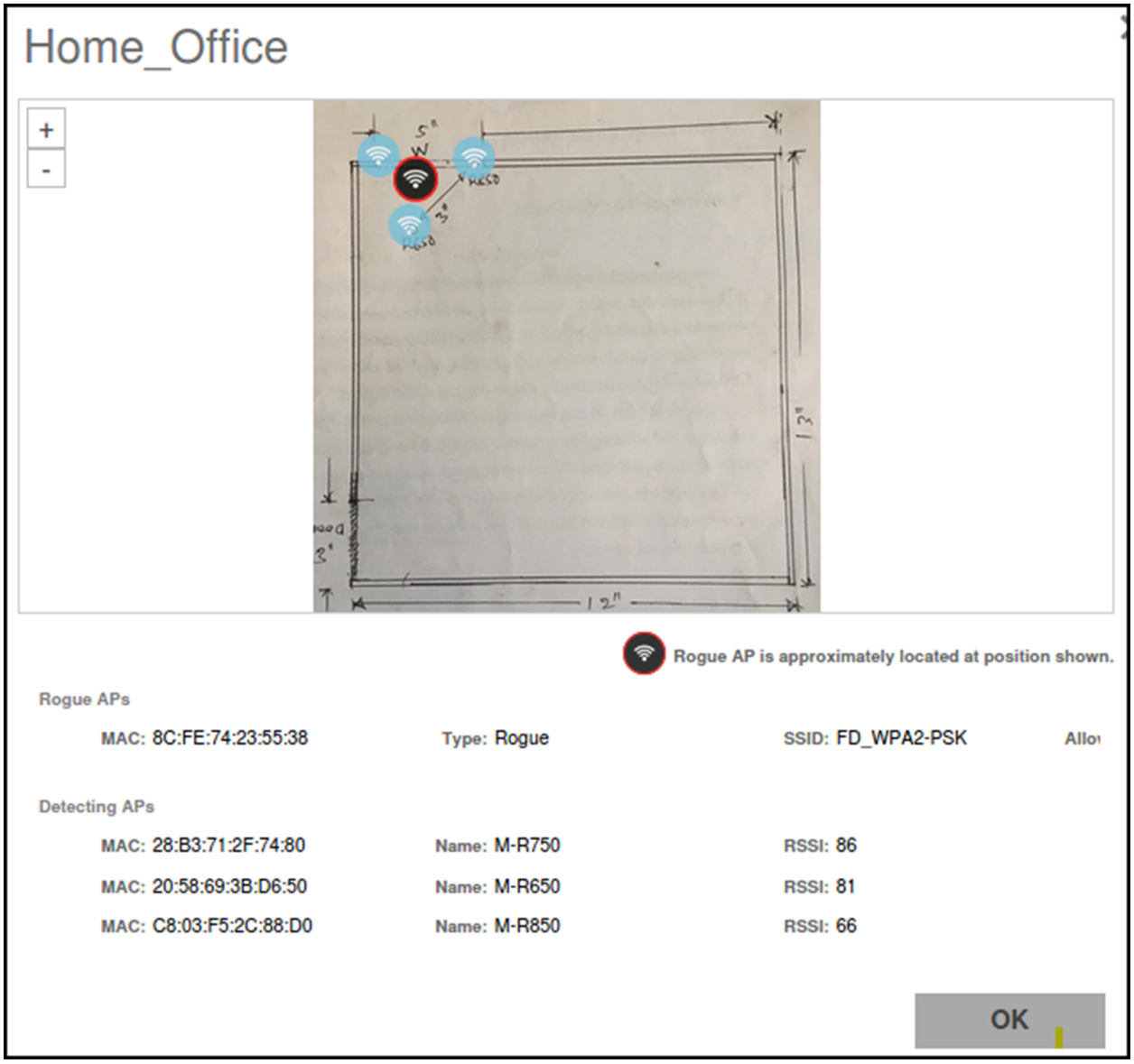
1. From the left pane, select **Report** > **Rogue Devices**.
2. Under **Device Type**, select **Access Point** or **Client**.

3. Click **Locate Rogue**.

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

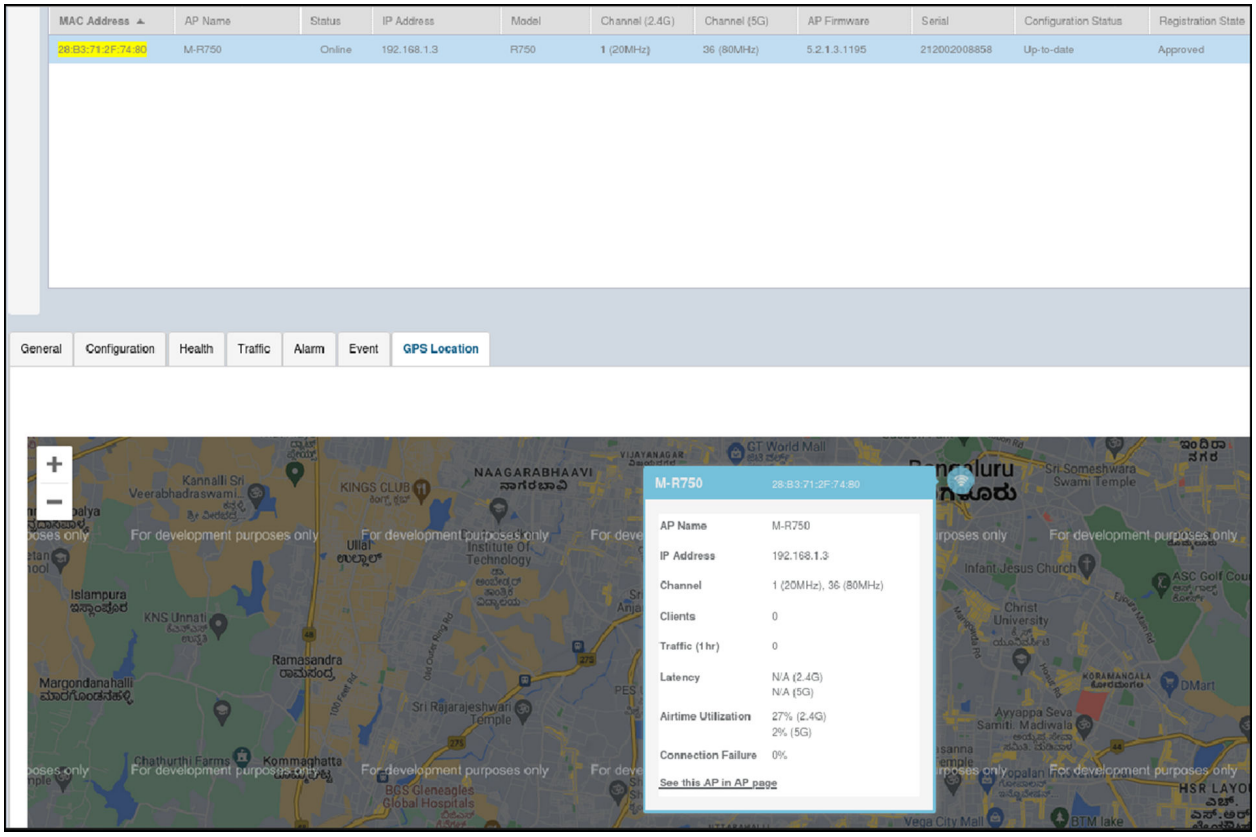
   - **Map**: Displays the monitor APs and rogue AP/UE detected on the floor map that is uploaded.

     FIGURE 37 Map View



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

FIGURE 38 Satellite View



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

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

- Rogue APs: MAC address, type, and SSID
- Detecting APs: MAC address, name, and RSSI

4. Click **OK**.

Historical AP Client Stats

Viewing AP Client Statistics

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

To view AP Client Statistics:

1. From the left pane, select **Monitor**>**Report** > **Historical Client Stats**. The Ruckus AP Client page appears.
2. Update the parameters as explained in Table 33.

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

TABLE 33 AP Client Statistics Report Parameters

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

Table 34 contains historical client statistics report based on the UE session statistics.

TABLE 34 AP Client Statistics Report Attributes

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

RUCKUS AP Tunnel Stats

Viewing Statistics for RUCKUS GRE Tunnels

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

To view the RUCKUS GRE Tunnel Statistics:

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

2. Update the parameters as explained in Table 35.
3. Click:
   - **Load Data**— To view the report in the workspace.
   - **Export CSV**—To open or save the report in CSV file format.

TABLE 35 RUCKUS GRE Report Parameters

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

Table 36 contains the report based on the statistics for RUCKUS GRE. Each entry contains the 15 minutes cumulative data.

TABLE 36 RUCKUS GRE report attributes

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

Viewing Statistics for SoftGRE Tunnels

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

To view the SoftGRE Tunnel statistics:

1. Select **Monitor** > **Report** > **Ruckus AP Tunnel Stats**. The Ruckus GRE tab appears by default.
2. Select **SoftGRE**. Update the parameters as explained in Table 37.
3. Click:
   - **Load Data**— To view the report in the workspace.
   - **Export CSV**—To open or save the report in CSV file format.

TABLE 37 SoftGRE Report Parameters

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

TABLE 37 SoftGRE Report Parameters (continued)

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

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

TABLE 38 SoftGRE Report Attributes

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

Viewing Statistics for SoftGRE IPsec Tunnels

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

To view the SoftGRE IPsec Tunnel Statistics:

1. elect **Monitor** > **Report** > **Ruckus AP Tunnel Stats**. The Ruckus GRE tab appears by default.
2. Select **SoftGRE + IPsec**. Update the parameters as explained in Table 39.
3. Click:
   - **Load Data**— To view the report in the workspace.
   - **Export CSV**—To open or save the report in CSV file format.

TABLE 39 SoftGRE + IPsec Report Parameters

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

Table 40 contains the report based on the statistics for access point IPsec. Each entry contains the 15 minutes cumulative data.

TABLE 40 SoftGRE + IPsecReport Attributes

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

TABLE 40 SoftGRE + IPsecReport Attributes (continued)

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

Core Network Tunnel Stats

Viewing Statistics for the L2oGRE Core Network Tunnel

An L2oGRE forwarding profile defines the gateway and tunnel configuration for the core network of L2oGRE tunnels.

Complete the following steps to view the statistics for the L2oGRE core network tunnel.

1. From the main menu, go to **Monitor** > **Report** > **Core Network Tunnel Stats**. The **L2oGRE** dialog box is displayed.
2. Configure the following options:
   - **Time Period:** Move the slider to set the duration for which you want to view the report.
   - **Data Plane:** Select the data plane.
   - **Gateway IP Address:** Enter the gateway IP address.
   - **MVNO Name:** Select the mobile network operation name (MVNO).
3. Click **Load Data** to view the report in the workspace or **Export CSV** to open or save the report in CSV file format.

Table 41 contains the report attributes based on the statistics for the L2oGRE core network tunnel.

TABLE 41 L2oGRE Core Network Tunnel Attributes

Attribute	Type	Description
Time	Long	Bin ID, which is stamped at 15-minute intervals; for example, 10:00, 10:15, 10:30.
TX Bytes	Long	Indicates the number of bytes sent.
RX Bytes	Long	Indicates the number of bytes received.
TX Packets	Long	Indicates the number of packets sent.
RX Packets	Long	Indicates the number of packets received.
Dropped Packets	Long	Indicates the number of packets dropped.

Viewing Statistics for the GTP Core Network Tunnel

GPRS Tunneling Protocol (GTP) transmits user data packets and signals between the controller and the gateway GPRS support node (GGSN).You can view historical traffic statistics and trends of the GTP core tunnels.

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

Complete the following steps to view the GTP core network tunnel statistics.

1. From the main menu, go to **Monitor** > **Report** > **RUCKUS AP Tunnel Stats**. The **SoftGRE** dialog box is displayed.

2. Select GTP and configure the following options:
   - **Time Period:** Move the slider to set the duration for which you want to view the report.
   - **Zone Name:** Select the zone name.
   - **Gateway IP Address:** Enter the gateway IP address.
   - **AP MAC or IP Address:** Enter the AP MAC address or IP address.
3. Click **Load Data** to view the report in the workspace or **Export CSV** to open or save the report in CSV file format.

The below table lists the attributes based on the statistics for the GTP. Each entry contains the cumulative data for the 15-minute interval.

TABLE 42 GTP Report Attributes

Attribute	Type	Description
Time	Long	Bin ID, which is stamped at 15-minute intervals; for example, 10:00, 10:15, 10:30.
TX Bytes	Long	Indicates the number of bytes sent.
RX Bytes	Long	Indicates the number of bytes received.
TX Packets	Long	Indicates the number of packets sent.
RX Packets	Long	Indicates the number of packets received.
Tx Dropped Packets	Long	Indicates the number of packets dropped while sending.
Rx Dropped Packets	Long	Indicates the number of packets dropped while receiving.
Bad GTPU	Long	Indicates a tunneling mechanism that provides a service for carrying user data packets dropped.
RX TEID Invalid	Long	Indicates the number of invalid packets received by Tunnel End Point Identifiers (TEID).
TX TEID Invalid	Long	Indicates the number of invalid packets sent by the Tunnel End Point Identifiers (TEID).
Echo RX	Long	Indicates the echo message received.
Last Echo RX Time	Long	Indicates the time when the last echo message was received.

Swap Configuration

Editing Swap Configuration

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

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

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

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

You have completed editing the swap configuration.

Viewing Managed APs

Viewing Managed Access Points

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

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

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

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

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

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

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

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

Zones

Working with AP Zones

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

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

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

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

Before creating an AP zone, RUCKUS recommends that you first set the default system time zone on the General Settings page. This will help ensure that each new AP zone will use the correct country. For information on how to set the default system time zone, refer to the **Configuring System Time** section of the *SmartZone 6.1.x (LT-GA) Installation Guide (SZ300/vSZ-H)* Guide.

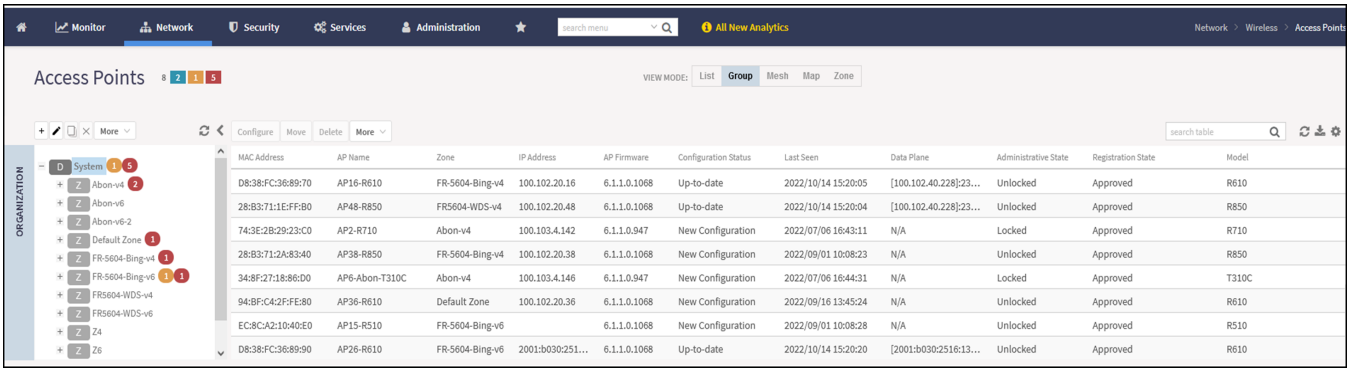
Creating an AP Zone

An AP zone functions as a way of grouping RUCKUS wireless APs and applying settings which includes WLANs to these groups. Each AP zone can have upto six WLAN services.

To create an AP zone, complete the following steps:

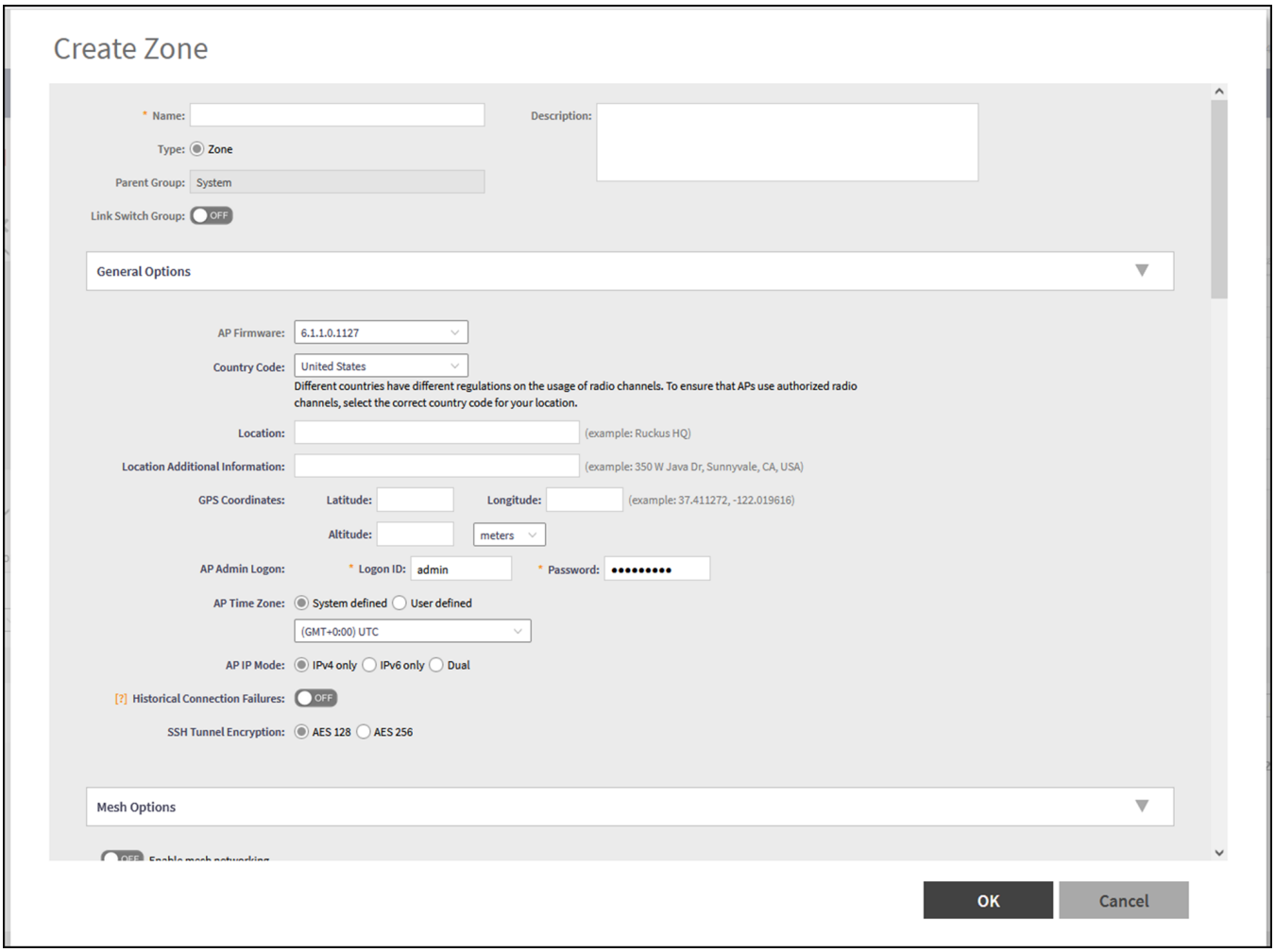
1. On the menu, click **Network** > **Wireless** > **Access Point**.

FIGURE 39 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 40 Create Zone Page



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

TABLE 43 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.
Link Switch Group	Allows to create a link between the switch group and an AP.	You can enable or disable the option. When the link state is enabled, you can modify the name and description of the switch group, the AP zone will change accordingly. When the link is disabled, the AP zone and switch group no longer share same name and description, but the link between them still exists. To delete the link, modify the name of AP zone or switch group. After successful deletion of the link, the **Link AP Zone** option is unavailable.
General Options		
AP Firmware	Indicates the firmware to which it applies.	Select the firmware.
Country Code	Indicates the country code. Using the correct country code helps ensure that APs use only authorized radio channels.	Select the country code.
Location	Indicates the generic location.	Enter the location.
Location Additional Information	Indicates detailed location.	Enter additional location information.
GPS Coordinates	Indicates the geographical location.	Enter the following coordinates: • **Longitude** • **Latitude** • **Altitude**
AP Admin Logon	Indicates the administrator logon credentials.	Enter the **Logon ID** and **Password**.
AP Time Zone	Indicates the time zone that applies.	Select a time zone, and enter the details as required.
AP IP Mode	Indicates the IP version that applies.	Select the IP version. IPv6, IPv4, and dual addressing modes are supported.
Historical Connection Failures	Allows the zone APs to report client connection failures so that the administrator can view past connection problems from the Troubleshooting menu. **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.

TABLE 43 AP Zone Details for SZ300 and vSZ-H platforms (continued)

Field	Description	Your Action
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**
Mesh Options		
NOTE Regardless of Single or Dual band, APs mesh with only there channel of radio which is in range.		
Enable mesh networking in this zone	Enables managed APs to automatically form a wireless mesh network, in which participant nodes (APs) cooperate to route packets.	Click the button.
Zero Touch Mesh	Enables a new AP to join the network using wireless connection.	Click the button.
Mesh Name (ESSID)	Indicates the mesh name.	Enter a name for the mesh network. Alternatively, do nothing to accept the default mesh name that the controller has generated.
Mesh Passphrase	Indicates the passphrase used by the controller to secure the traffic between Mesh APs.	Enter a passphrase that contains at least 12 characters. Alternatively, click **Generate** to generate a random passphrase with 32 characters or more.
Mesh Radio Option	Indicates the channel range configured.	Select the channel option: 2.4 GHz or 5 GHz/6 GHz.
Radio Options		
Dual-5G Mode	Enables third radio operator in 2.4 GHz, Lower 5 GHz, and Upper 5 GHz. By default, the **Dual-5G Mode** is enabled. In the enabled mode, radio-0 will be on 2.4GHz band, radio-1 will be on 5G Lower band and radio-2 will be on 5G Upper band. • 5G Lower BAND : UNII-1, UNII-2A • 5G Upper BAND : UNII-2C, UNII-3 In the disabled mode, the radio-0 will be on 2.4GHz band, radio-1 will be on 5G band and radio-2 will be on 6G band. This also depends on the country code.	Select or keep the default **Dual-5G Mode** option.
Band/Spectrum Configuration > **2.4 GHz**		
Channelization	Helps manage and allocate radio frequency resources. A lower channel width allows the zone to potentially serve more clients, whereas a higher channel width improves throughput, but potentially serves fewer clients and increases the possibility of interference. The Auto setting defaults to 20 MHz channelization.	Set the channel bandwidth used during transmission to either **20** or **40** (MHz), or select **Auto** to set it automatically. **NOTE** By default, for the **Country Code** Indonesia, the **Channelization** width is set to 20 MHz only for outdoor APs.
Channel	Indicates the channel to use.	Select one of the options: **Auto**, **1**, **6** or **11**.

TABLE 43 AP Zone Details for SZ300 and vSZ-H platforms (continued)

Field	Description	Your Action
Auto Cell Sizing	Enables the AP to share information on interference seen by each other and dynamically adjust their radio Tx power and Rx parameters to minimize interference. Enabling this option disables the TX Power Adjustment configuration. **NOTE** Ensure that Background Scan is enabled.	Select the option.
TX Power Adjustment	Allows to manually configure the transmit power on the 2.4 GHz radio. By default, the TX power is set to Full on the 2.4 GHz radio. **NOTE** If you choose Min, the transmit power is set to 0dBm (1mW) per chain for 11n APs, and 2dBm per chain for 11ac APs. If you choose Max, the transmit power is set to the maximum allowable value according to the AP's capability and the operating country's regulations.	Select the preferred TX power.
Protection Mode	Indicates the mechanism to reduce frame collision.	Choose one of the following options: ● None ● RTS/CTS ● CTS Only
Background Scan	Allows the AP radio to scan other channels in the band for accessing channel health and capacity, detecting rogue devices, optimizing and maintaining mesh links and to discover AP neighbors.	Enter the duration in seconds. Range: 1 through 65535.
Auto Channel Selection	Automatically adjusts the channel for network self-healing and performance optimization. **ChannelFly** is set as the default option. For the **ChannelFly** option, you may also modify the default settings for the **Channel Change Frequency** and **Full Optimization Period**. The **Channel Change Frequency** slidebar allows you to specify the responsiveness of ChannelFly to interference (with consideration for the impact on associated clients), ranging from Minimal to Very Often. The **Full Optimization Period** timeslot bar allows you to specify one or more periods of time when ChannelFly is allowed to fully optimize the channel plan, ignoring the impact of channel changes on associated clients. Select time periods when the wireless network is servicing the fewest clients.	Select the required option. ● **Background Scanning**: Changes the AP channel when there is interference. ● **ChannelFly**: Monitors potential throughput and will change channels to learn each channel's capacity, optimize throughput, and to avoid interference.
Band/Spectrum Configuration > **5 GHz**		

TABLE 43 AP Zone Details for SZ300 and vSZ-H platforms (continued)

Field	Description	Your Action
Channelization	Helps manage and allocate radio frequency resources. A lower channel width allows the zone to potentially serve more clients, whereas a higher channel width improves throughput, but potentially serves fewer clients and increases the possibility of interference. Prior to SmartZone release 7.0.0, the Auto setting defaulted to 80 MHz channelization. Beginning in SmartZone release 7.0.0, the Auto setting defaults to 40 MHz channelization.	Set the channel bandwidth used during transmission: Auto, 20, 40, 80 and 160. **NOTE** By default, for the **Country Code** Indonesia, the **Channelization** width is set to 20 MHz only for outdoor APs.
Channel	Indicates the channel to use.	Select the required options for the Indoor and Outdoor APs.
Secondary Channel	Indicates the secondary channel to used.	By default, the Indoor and Outdoor option is set to Auto.
Allow DFS Channels	Allows ZoneFlex APs to use DFS channels.	Click to enable the option.
Allow Channel 144	Provides channel 140 and 144 support for 11ac and 11ax APs. Enabling this option supports 20 MHz, 40 MHz, or 80 MHz channel modes. The 160 MHz mode is supported if the AP supports this mode. Disabling this option provides Channel 140 support only to 20 MHz mode. **NOTE** This option is available for selection only if you enable the **DFS Channels** option. **NOTE** This feature is currently supported only in the United States.	Click to enable the option.
Allow Indoor Channels	Allows outdoor APs to use channels regulated as for indoor use only.	Click to enable the option.
Auto Cell Sizing	Enables the AP to share information on interference seen by each other and dynamically adjust their radio Tx power and Rx parameters to minimize interference. Enabling this option disables the TX Power Adjustment configuration. **NOTE** Ensure that Background Scan is enabled.	Select the option.
TX Power Adjustment	Allows to manually configure the transmit power on the 5 GHz radio. By default, the TX power is set to Full on the 5 GHz radio. **NOTE** If you choose Min, the transmit power is set to 0dBm (1mW) per chain for 11n APs, and 2dBm per chain for 11ac APs. If you choose Max, the transmit power is set to the maximum allowable value according to the AP's capability and the operating country's regulations.	Select the preferred TX power.

TABLE 43 AP Zone Details for SZ300 and vSZ-H platforms (continued)

Field	Description	Your Action
Background Scan	Allows the AP radio to scan other channels in the band for accessing channel health and capacity, detecting rogue devices, optimizing and maintaining mesh links and to discover AP neighbors.	Enter the duration in seconds. Range: 1 through 65535.
Auto Channel Selection	Automatically adjusts the channel for network self-healing and performance optimization. **ChannelFly** is set as the default option. For the **ChannelFly** option, you may also modify the default settings for the **Channel Change Frequency** and **Full Optimization Period**. The **Channel Change Frequency** slidebar allows you to specify the responsiveness of ChannelFly to interference (with consideration for the impact on associated clients), ranging from Minimal to Very Often. The **Full Optimization Period** timeslot bar allows you to specify one or more periods of time when ChannelFly is allowed to fully optimize the channel plan, ignoring the impact of channel changes on associated clients. Select time periods when the wireless network is servicing the fewest clients.	Select the required option. • **Background Scanning**: Changes the AP channel when there is interference. • **ChannelFly**: Monitors potential throughput and will change channels to learn each channel's capacity, optimize throughput, and to avoid interference.
Band/Spectrum Configuration > **6 GHz** **NOTE** This tab is available only if the **Tri-band Dual-5G Mode** option is not enabled.		
Channelization	Helps manage and allocate radio frequency resources. A lower channel width allows the zone to potentially serve more clients, whereas a higher channel width improves throughput, but potentially serves fewer clients and increases the possibility of interference. The Auto setting defaults to 160 MHz channelization.	Set the channel bandwidth used during transmission: **Auto**, **20**, **40**, **80**, **160** and **320**. **NOTE** The 320 MHz-radio frequency is available only for the R770 AP 6 GHz radio frequency.
Channel	Indicates the channel to use. The 320 MHz channelization supporting the R770 AP has two types of channel; the 320 Mhz-1 channel with channel center frequency numbered 31, 95, and 159, and the 320 Mhz-2 channel with channel center frequency numbered 63, 127, and 191.	Select the required channel for the APs. **NOTE** If 320 channelization is selected, then the selected channel may also require a Group selection. • **Auto**: Group selection is not available. • Channels **1** through **29**: **Group 1** is the default selection. **Group 2** cannot be selected. • Channels **33** through **189**: **Group 1** is the default selection, but you may select either **Group 1** or **Group 2**. • Channels **193** through **221**: **Group 2** is the default selection. **Group 1** cannot be selected.

TABLE 43 AP Zone Details for SZ300 and vSZ-H platforms (continued)

Field	Description	Your Action
Auto Cell Sizing	Enables the AP to share information on interference seen by each other and dynamically adjust their radio Tx power and Rx parameters to minimize interference. Enabling this option disables the TX Power Adjustment configuration. **NOTE** Ensure that Background Scan is enabled.	Select the option.
TX Power Adjustment	Allows to manually configure the transmit power on the 6 GHz radio. By default, the TX power is set to Full on the 6 GHz radio. **NOTE** If you choose Min, the transmit power is set to 0dBm (1mW) per chain for 11n APs, and 2dBm per chain for 11ac APs. If you choose Max, the transmit power is set to the maximum allowable value according to the AP's capability and the operating country's regulations.	Select the preferred TX power.
Background Scan	Allows the AP radio to scan other channels in the band for accessing channel health and capacity, detecting rogue devices, optimizing and maintaining mesh links and to discover AP neighbors.	Enter the duration in seconds. Range: 1 through 65535.
Auto Channel Selection	Automatically adjusts the channel for network self-healing and performance optimization. **ChannelFly** is set as the default option. For the **ChannelFly** option, you may also modify the default settings for the **Channel Change Frequency** and **Full Optimization Period**. The **Channel Change Frequency** slidebar allows you to specify the responsiveness of ChannelFly to interference (with consideration for the impact on associated clients), ranging from Minimal to Very Often. The **Full Optimization Period** timeslot bar allows you to specify one or more periods of time when ChannelFly is allowed to fully optimize the channel plan, ignoring the impact of channel changes on associated clients. Select time periods when the wireless network is servicing the fewest clients.	Select the required option. • **Background Scanning**: Changes the AP channel when there is interference. • **ChannelFly**: Monitors potential throughput and will change channels to learn each channel's capacity, optimize throughput, and to avoid interference.
Band/Spectrum Configuration > **Lower 5 GHz**		

TABLE 43 AP Zone Details for SZ300 and vSZ-H platforms (continued)

Field	Description	Your Action
Channelization	Helps manage and allocate radio frequency resources. A lower channel width allows the zone to potentially serve more clients, whereas a higher channel width improves throughput, but potentially serves fewer clients and increases the possibility of interference. Prior to SmartZone release 7.0.0, the Auto setting defaulted to 80 MHz channelization. Beginning in SmartZone release 7.0.0, the Auto setting defaults to 40 MHz channelization.	Set the channel bandwidth used during transmission: Auto, 20, 40, 80 and 160. **NOTE** By default, for the **Country Code** Indonesia, the **Channelization** width is set to 20 MHz only for outdoor APs.
Channel	Indicates the channel to use.	Select the required options for the Indoor and Outdoor APs.
Allow DFS Channels	Allows ZoneFlex APs to use DFS channels.	Click to enable the option.
Allow Indoor Channels	Allows outdoor APs to use channels regulated as for indoor use only.	Click to enable the option.
Auto Cell Sizing	Enables the AP to share information on interference seen by each other and dynamically adjust their radio Tx power and Rx parameters to minimize interference. Enabling this option disables the TX Power Adjustment configuration. **NOTE** Ensure that Background Scan is enabled.	Select the option.
TX Power Adjustment	Allows to manually configure the transmit power on the Lower 5 GHz radio. By default, the TX power is set to Full on the Lower 5 GHz radio. **NOTE** If you choose Min, the transmit power is set to 0dBm (1mW) per chain for 11n APs, and 2dBm per chain for 11ac APs. If you choose Max, the transmit power is set to the maximum allowable value according to the AP's capability and the operating country's regulations.	Select the preferred TX power.
Background Scan	Allows the AP radio to scan other channels in the band for accessing channel health and capacity, detecting rogue devices, optimizing and maintaining mesh links and to discover AP neighbors.	Enter the duration in seconds. Range: 1 through 65535.

TABLE 43 AP Zone Details for SZ300 and vSZ-H platforms (continued)

Field	Description	Your Action
Auto Channel Selection	Automatically adjusts the channel for network self-healing and performance optimization. **ChannelFly** is set as the default option. For the **ChannelFly** option, you may also modify the default settings for the **Channel Change Frequency** and **Full Optimization Period**. The **Channel Change Frequency** slidebar allows you to specify the responsiveness of ChannelFly to interference (with consideration for the impact on associated clients), ranging from Minimal to Very Often. The **Full Optimization Period** timeslot bar allows you to specify one or more periods of time when ChannelFly is allowed to fully optimize the channel plan, ignoring the impact of channel changes on associated clients. Select time periods when the wireless network is servicing the fewest clients.	Select the required option. • **Background Scanning**: Changes the AP channel when there is interference. • **ChannelFly**: Monitors potential throughput and will change channels to learn each channel's capacity, optimize throughput, and to avoid interference.
Band/Spectrum Configuration > **Upper 5 GHz**		
Channelization	Helps manage and allocate radio frequency resources. A lower channel width allows the zone to potentially serve more clients, whereas a higher channel width improves throughput, but potentially serves fewer clients and increases the possibility of interference. Prior to SmartZone release 7.0.0, the Auto setting defaulted to 80 MHz channelization. Beginning in SmartZone release 7.0.0, the Auto setting defaults to 40 MHz channelization.	Set the channel bandwidth used during transmission: Auto, 20, 40, 80 and 160.
Channel	Indicates the channel to use.	Select the required options for the Indoor and Outdoor APs.
Allow DFS Channels	Allows ZoneFlex APs to use DFS channels.	Click to enable the option.
Allow Channel 144	Provides channel 140 and 144 support for 11ac and 11ax APs. Enabling this option supports 20 MHz, 40 MHz, or 80 MHz channel modes. The 160 MHz mode is supported if the AP supports this mode. Disabling this option provides Channel 140 support only to 20 MHz mode. **NOTE** This option is available 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 43 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 Upper 5 GHz radio. By default, the TX power is set to Full on the Upper 5 GHz radio. **NOTE** If you choose Min, the transmit power is set to 0dBm (1mW) per chain for 11n APs, and 2dBm per chain for 11ac APs. If you choose Max, the transmit power is set to the maximum allowable value according to the AP's capability and the operating country's regulations.	Select the preferred TX power.
Background Scan	Allows the AP radio to scan other channels in the band for accessing channel health and capacity, detecting rogue devices, optimizing and maintaining mesh links and to discover AP neighbors.	Enter the duration in seconds. Range: 1 through 65535.
Auto Channel Selection	Automatically adjusts the channel for network self-healing and performance optimization. **ChannelFly** is set as the default option. For the **ChannelFly** option, you may also modify the default settings for the **Channel Change Frequency** and **Full Optimization Period**. The **Channel Change Frequency** slidebar allows you to specify the responsiveness of ChannelFly to interference (with consideration for the impact on associated clients), ranging from Minimal to Very Often. The **Full Optimization Period** timeslot bar allows you to specify one or more periods of time when ChannelFly is allowed to fully optimize the channel plan, ignoring the impact of channel changes on associated clients. Select time periods when the wireless network is servicing the fewest clients.	Select the required option. • **Background Scanning**: Changes the AP channel when there is interference. • **ChannelFly**: Monitors potential throughput and will change channels to learn each channel's capacity, optimize throughput, and to avoid interference.
AP GRE Tunnel Options		
Ruckus GRE Profile	Indicates the GRE tunnel profile.	Choose the GRE tunnel profile from the list.
Ruckus GRE Forwarding Broadcast	Forwards the broadcast traffic from network to tunnel.	Click the option to enable forwarding broadcast.

TABLE 43 AP Zone Details for SZ300 and vSZ-H platforms (continued)

Field	Description	Your Action
Soft GRE Profiles	Indicates the SoftGRE profiles that you want to apply to the zone.	a. Click the **Select** check box, a form is displayed. b. From the **Available Profiles**, select the profile and click the -> icon to choose it. You can also click the + icon to create a new SoftGRE profile. c. Click **OK**.
IPsec Tunnel Mode	Indicated the tunnel mode for the Ruckus GRE and SoftGRE profile.	Select an option: ● Disable ● SoftGRE ● Ruckus GRE
IPsec Tunnel Profile	Indicates the tunnel profile for SoftGRE. **NOTE** Select the same tunnel type for IPsec tunnel profile in WLAN configuration.	Choose the option from the drop-down.
Syslog Options		
Enable external syslog server for APs	Enables the AP to send syslog data to the syslog server on the network.	Select the option.

TABLE 43 AP Zone Details for SZ300 and vSZ-H platforms (continued)

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

TABLE 43 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**.
Advanced Options		
Restricted AP Access Profile **NOTE** This feature is available from 5.2 release and onwards.	Restricted AP Access blocks access to the AP's standard well know open ports to protect the APs and enhance their security.	Select the Restricted AP Access profile from the drop-down. You can also create a new profile by clicking **+** icon. **NOTE** By default this feature is disabled. **NOTE** You can add maximum five Restricted AP Access profiles for a zone.
Channel Mode	Indicates if location-based service is enabled. If you want to allow indoor APs that belong to this zone to use wireless channels that are Channel Mode regulated as indoor-use only.	Select the **Allow indoor channels** check box.
Smart Monitor	Indicates AP interval check and retry threshold settings.	Select the check box and enter the interval and threshold.
AP Ping Latency Interval	Measures the latency between the controller and AP periodically, and sends this data to SCI.	Enable by moving the button to ON to measure latency.
AP Management VLAN	Indicates the AP management VLAN settings.	Choose the option. Click **VLAN ID**, and then type the VLAN ID that you want to assign (valid range is from 1 to 4094). To keep the same management VLAN ID that has been configured on the AP, click Keep AP's settings. **ATTENTION** For standalone APs, set the AP Ethernet port to trunk before changing the AP Management VLAN settings.

TABLE 43 AP Zone Details for SZ300 and vSZ-H platforms (continued)

Field	Description	Your Action
Rogue AP Detection	Indicates rogue AP settings. **NOTE** Rogue detection AP in active-active mode cluster redundancy environment is restricted from storing its own BSSIDs to avoid considering its own APs as rogues attacking.	Enable the option.
Rogue Classification Policy	Indicates the parameters used to classify rogue APs. This option is available only if you enable the **Rogue AP Detection** option.	Select the options for rogue classification policy: ● – **Enable events and alarms for all rogue devices** – **Enable events and alarms for malicious rogues only** ● **Report RSSI Threshold**: Enter the threshold. Range: **0** through **100**. ● **Protect the network from malicious rogue access points**: Enable the option and choose one of the following: – **Aggressive** – **Auto** – **Conservative** ● **Radio Jamming Detection**: Enable the option and enter the **Jamming Threshold** in percentage.
DoS Protection	Indicates settings for blocking a client.	Select the check box and enter the duration in seconds.
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 43 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 44 AP Zone Details for SZ100 and vSZ-E platforms

Field	Description	Your Action
Name	Indicates the name of the zone or AP group.	Enter a name.
Description	Indicates the short description assigned to the zone or AP group.	Enter a brief description
Type	Indicates if you are creating a domain, zone, or an AP group.	Appears by default. You can also choose the option.
Parent Group	Indicates the parent AP group.	Appears by default.
Link Switch Group	Allows to create a link between the switch group and an AP.	You can enable or disable the option. When the link state is enabled, you can modify the name and description of the switch group, the AP zone will change accordingly. When the link is disabled, the AP zone and switch group no longer share same name and description, but the link between them still exists. To delete the link, modify the name of AP zone or switch group. After successful deletion of the link, the **Link AP Zone** option is unavailable.
General Options		
AP Firmware	Indicates the firmware to which it applies.	Select the firmware.
Country Code	Indicates the country code. Using the correct country code helps ensure that APs use only authorized radio channels.	Select the country code.
Location	Indicates the generic location.	Enter the location.
Location Additional Information	Indicates detailed location.	Enter additional location information.
GPS Coordinates	Indicates the geographical location.	Enter the following coordinates: • **Longitude** • **Latitude** • **Altitude**
AP Admin Logon	Indicates the administrator logon credentials.	Enter the **Logon ID** and **Password**.
AP Time Zone	Indicates the time zone that applies.	Select a time zone, and enter the details as required.
AP IP Mode	Indicates the IP version that applies.	Select the IP version. IPv6, IPv4, and dual addressing modes are supported.
Historical Connection Failures	Allows the zone APs to report client connection failures so that the administrator can view past connection problems from the Troubleshooting menu.	Click the button.
SSH Tunnel Encryption	Specifies the encryption that reduces the load on controller control of SSH traffic.	Select the required option: • **AES 128** • **AES 256**
Mesh Options		
Enable mesh networking in this zone	Enables managed APs to automatically form a wireless mesh network, in which participant nodes (APs) cooperate to route packets.	Click the button.
Zero Touch Mesh	Enables a new AP to join the network using wireless connection.	Click the button.
Mesh Name (ESSID)	Indicates the mesh name.	Enter a name for the mesh network. Alternatively, do nothing to accept the default mesh name that the controller has generated.

TABLE 44 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.
Radio Options		
Dual-5G Mode	Enables third radio operator in 2.4 GHz, Lower 5 GHz, and Upper 5 GHz. By default, the **Dual-5G Mode** is enabled. In the enabled mode, radio-0 will be on 2.4GHz band, radio-1 will be on 5G Lower band and radio-2 will be on 5G Upper band. ● 5G Lower BAND : UNII-1, UNII-2A ● 5G Upper BAND : UNII-2C, UNII-3 In the disabled mode, the radio-0 will be on 2.4GHz band, radio-1 will be on 5G band and radio-2 will be on 6G band. This also depends on the country code.	Select or keep the default **Dual-5G Mode** option.
Band/Spectrum Configuration > **2.4 GHz**		
Channelization	Helps manage and allocate radio frequency resources. A lower channel width allows the zone to potentially serve more clients, whereas a higher channel width improves throughput, but potentially serves fewer clients and increases the possibility of interference. The Auto setting defaults to 20 MHz channelization.	Set the channel bandwidth used during transmission to either 20 or 40 (MHz), or select Auto to set it automatically. **NOTE** By default, for the **Country Code** Indonesia, the **Channelization** width is set to 20 MHz only for outdoor APs.
Channel	Indicates the channel to use.	Select one of the options: Auto, 1, 6 or 11.
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

TABLE 44 AP Zone Details for SZ100 and vSZ-E platforms (continued)

Field	Description	Your Action
Background Scan	Allows the AP radio to scan other channels in the band for accessing channel health and capacity, detecting rogue devices, optimizing and maintaining mesh links and to discover AP neighbors.	Enter the duration in seconds. Range: 1 through 65535.
Auto Channel Selection	Automatically adjusts the channel for network self-healing and performance optimization. **ChannelFly** is set as the default option. For the **ChannelFly** option, you may also modify the default settings for the **Channel Change Frequency** and **Full Optimization Period**. The **Channel Change Frequency** slidebar allows you to specify the responsiveness of ChannelFly to interference (with consideration for the impact on associated clients), ranging from Minimal to Very Often. The **Full Optimization Period** timeslot bar allows you to specify one or more periods of time when ChannelFly is allowed to fully optimize the channel plan, ignoring the impact of channel changes on associated clients. Select time periods when the wireless network is servicing the fewest clients.	Select the required option. • **Background Scanning**: Changes the AP channel when there is interference. • **ChannelFly**: Monitors potential throughput and will change channels to learn each channel's capacity, optimize throughput, and to avoid interference.
Band/Spectrum Configuration > **5 GHz**		
Channelization	Helps manage and allocate radio frequency resources. A lower channel width allows the zone to potentially serve more clients, whereas a higher channel width improves throughput, but potentially serves fewer clients and increases the possibility of interference. Prior to SmartZone release 7.0.0, the Auto setting defaulted to 80 MHz channelization. Beginning in SmartZone release 7.0.0, the Auto setting defaults to 40 MHz channelization.	Set the channel bandwidth used during transmission: Auto, 20, 40, 80 and 160. **NOTE** By default, for the **Country Code** Indonesia, the **Channelization** width is set to 20 MHz only for outdoor APs.
Channel	Indicates the channel to use.	Select the required options for the Indoor and Outdoor APs.
Secondary Channel	Indicates the secondary channel to used.	By default, the Indoor and Outdoor option is set to Auto.
Allow DFS Channels	Allows ZoneFlex APs to use DFS channels.	Click to enable the option.
Allow Channel 144	Provides channel 140 and 144 support for 11ac and 11ax APs. Enabling this option supports 20 MHz, 40 MHz, or 80 MHz channel modes. The 160 MHz mode is supported if the AP supports this mode. Disabling this option provides Channel 140 support only to 20 MHz mode. **NOTE** This option is available for selection only if you enable the **DFS Channels** option. **NOTE** This feature is currently supported only in the United States.	Click to enable the option.

TABLE 44 AP Zone Details for SZ100 and vSZ-E platforms (continued)

Field	Description	Your Action
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 maintaining mesh links and to discover AP neighbors.	Enter the duration in seconds. Range: 1 through 65535.
Auto Channel Selection	Automatically adjusts the channel for network self-healing and performance optimization. **ChannelFly** is set as the default option. For the **ChannelFly** option, you may also modify the default settings for the **Channel Change Frequency** and **Full Optimization Period**. The **Channel Change Frequency** slidebar allows you to specify the responsiveness of ChannelFly to interference (with consideration for the impact on associated clients), ranging from Minimal to Very Often. The **Full Optimization Period** timeslot bar allows you to specify one or more periods of time when ChannelFly is allowed to fully optimize the channel plan, ignoring the impact of channel changes on associated clients. Select time periods when the wireless network is servicing the fewest clients.	Select the required option. • **Background Scanning**: Changes the AP channel when there is interference. • **ChannelFly**: Monitors potential throughput and will change channels to learn each channel's capacity, optimize throughput, and to avoid interference.
Band/Spectrum Configuration > **6 GHz** **NOTE** This tab is available only if the Tri-band Dual-5G Mode option is not enabled.		

TABLE 44 AP Zone Details for SZ100 and vSZ-E platforms (continued)

Field	Description	Your Action
Channelization	Helps manage and allocate radio frequency resources. A lower channel width allows the zone to potentially serve more clients, whereas a higher channel width improves throughput, but potentially serves fewer clients and increases the possibility of interference. The Auto setting defaults to 160 MHz channelization.	Set the channel bandwidth used during transmission: **Auto**, **20**, **40**, **80**, **160** and **320**. **NOTE** The 320 MHz-radio frequency is available only for the R770 AP 6 GHz radio frequency.
Channel	Indicates the channel to use. The 320 MHz channelization supporting the R770 AP has two types of channel; the 320 Mhz-1 channel with channel center frequency numbered 31, 95, and 159, and the 320 Mhz-2 channel with channel center frequency numbered 63, 127, and 191.	Select the required channel for the APs. **NOTE** If 320 channelization is selected, then the selected channel may also require a Group selection. ● **Auto**: Group selection is not available. ● Channels **1** through **29**: **Group 1** is the default selection. **Group 2** cannot be selected. ● Channels **33** through **189**: **Group 1** is the default selection, but you may select either **Group 1** or **Group 2**. ● Channels **193** through **221**: **Group 2** is the default selection. **Group 1** cannot be selected.
Auto Cell Sizing	Enables the AP to share information on interference seen by each other and dynamically adjust their radio Tx power and Rx parameters to minimize interference. Enabling this option disables the TX Power Adjustment configuration. **NOTE** Ensure that Background Scan is enabled.	Select the option.
TX Power Adjustment	Allows to manually configure the transmit power on the 6 GHz radio. By default, the TX power is set to Full on the 6 GHz radio. **NOTE** If you choose Min, the transmit power is set to 0dBm (1mW) per chain for 11n APs, and 2dBm per chain for 11ac APs. If you choose Max, the transmit power is set to the maximum allowable value according to the AP's capability and the operating country's regulations.	Select the preferred TX power.
Background Scan	Allows the AP radio to scan other channels in the band for accessing channel health and capacity, detecting rogue devices, optimizing and maintaining mesh links and to discover AP neighbors.	Enter the duration in seconds. Range: 1 through 65535.

TABLE 44 AP Zone Details for SZ100 and vSZ-E platforms (continued)

Field	Description	Your Action
Auto Channel Selection	Automatically adjusts the channel for network self-healing and performance optimization. **ChannelFly** is set as the default option. For the **ChannelFly** option, you may also modify the default settings for the **Channel Change Frequency** and **Full Optimization Period**. The **Channel Change Frequency** slidebar allows you to specify the responsiveness of ChannelFly to interference (with consideration for the impact on associated clients), ranging from Minimal to Very Often. The **Full Optimization Period** timeslot bar allows you to specify one or more periods of time when ChannelFly is allowed to fully optimize the channel plan, ignoring the impact of channel changes on associated clients. Select time periods when the wireless network is servicing the fewest clients.	Select the required option. • **Background Scanning**: Changes the AP channel when there is interference. • **ChannelFly**: Monitors potential throughput and will change channels to learn each channel's capacity, optimize throughput, and to avoid interference.
Band/Spectrum Configuration > **Lower 5 GHz**		
Channelization	Helps manage and allocate radio frequency resources. A lower channel width allows the zone to potentially serve more clients, whereas a higher channel width improves throughput, but potentially serves fewer clients and increases the possibility of interference. Prior to SmartZone release 7.0.0, the Auto setting defaulted to 80 MHz channelization. Beginning in SmartZone release 7.0.0, the Auto setting defaults to 40 MHz channelization.	Set the channel bandwidth used during transmission: Auto, 20, 40, 80 and 160. **NOTE** By default, for the **Country Code** Indonesia, the **Channelization** width is set to 20 MHz only for outdoor APs.
Channel	Indicates the channel to use.	Select the required options for the Indoor and Outdoor APs.
Allow DFS Channels	Allows ZoneFlex APs to use DFS channels.	Click to enable the option.
Allow Indoor Channels	Allows outdoor APs to use channels regulated as for indoor use only.	Click to enable the option.
Auto Cell Sizing	Enables the AP to share information on interference seen by each other and dynamically adjust their radio Tx power and Rx parameters to minimize interference. Enabling this option disables the TX Power Adjustment configuration. **NOTE** Ensure that Background Scan is enabled.	Select the option.

TABLE 44 AP Zone Details for SZ100 and vSZ-E platforms (continued)

Field	Description	Your Action
TX Power Adjustment	Allows to manually configure the transmit power on the Lower 5 GHz radio. By default, the TX power is set to Full on the Lower 5 GHz radio. **NOTE** If you choose Min, the transmit power is set to 0dBm (1mW) per chain for 11n APs, and 2dBm per chain for 11ac APs. If you choose Max, the transmit power is set to the maximum allowable value according to the AP's capability and the operating country's regulations.	Select the preferred TX power.
Background Scan	Allows the AP radio to scan other channels in the band for accessing channel health and capacity, detecting rogue devices, optimizing and maintaining mesh links and to discover AP neighbors.	Enter the duration in seconds. Range: 1 through 65535.
Auto Channel Selection	Automatically adjusts the channel for network self-healing and performance optimization. **ChannelFly** is set as the default option. For the **ChannelFly** option, you may also modify the default settings for the **Channel Change Frequency** and **Full Optimization Period**. The **Channel Change Frequency** slidebar allows you to specify the responsiveness of ChannelFly to interference (with consideration for the impact on associated clients), ranging from Minimal to Very Often. The **Full Optimization Period** timeslot bar allows you to specify one or more periods of time when ChannelFly is allowed to fully optimize the channel plan, ignoring the impact of channel changes on associated clients. Select time periods when the wireless network is servicing the fewest clients.	Select the required option. • **Background Scanning**: Changes the AP channel when there is interference. • **ChannelFly**: Monitors potential throughput and will change channels to learn each channel's capacity, optimize throughput, and to avoid interference.
Band/Spectrum Configuration > **Upper 5 GHz**		
Channelization	Helps manage and allocate radio frequency resources. A lower channel width allows the zone to potentially serve more clients, whereas a higher channel width improves throughput, but potentially serves fewer clients and increases the possibility of interference. Prior to SmartZone release 7.0.0, the Auto setting defaulted to 80 MHz channelization. Beginning in SmartZone release 7.0.0, the Auto setting defaults to 40 MHz channelization.	Set the channel bandwidth used during transmission: Auto, 20, 40, 80 and 160.
Channel	Indicates the channel to use.	Select the required options for the Indoor and Outdoor APs.
Allow DFS Channels	Allows ZoneFlex APs to use DFS channels.	Click to enable the option.

TABLE 44 AP Zone Details for SZ100 and vSZ-E platforms (continued)

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

TABLE 44 AP Zone Details for SZ100 and vSZ-E platforms (continued)

Field	Description	Your Action
Auto Channel Selection	Automatically adjusts the channel for network self-healing and performance optimization. **ChannelFly** is set as the default option. For the **ChannelFly** option, you may also modify the default settings for the **Channel Change Frequency** and **Full Optimization Period**. The **Channel Change Frequency** slidebar allows you to specify the responsiveness of ChannelFly to interference (with consideration for the impact on associated clients), ranging from Minimal to Very Often. The **Full Optimization Period** timeslot bar allows you to specify one or more periods of time when ChannelFly is allowed to fully optimize the channel plan, ignoring the impact of channel changes on associated clients. Select time periods when the wireless network is servicing the fewest clients.	Select the required option. ● **Background Scanning**: Changes the AP channel when there is interference. ● **ChannelFly**: Monitors potential throughput and will change channels to learn each channel's capacity, optimize throughput, and to avoid interference.
AP GRE Tunnel Options		
Ruckus GRE Profile	Indicates the GRE tunnel profile.	Choose the GRE tunnel profile from the list.
Ruckus GRE Forwarding Broadcast	Forwards the broadcast traffic from network to tunnel.	Click the option to enable forwarding broadcast.
Soft GRE Profiles	Indicates the SoftGRE profiles that you want to apply to the zone.	a. Click the **Select** check box, a form is displayed. b. From the **Available Profiles**, select the profile and click the -> icon to choose it. You can also click the + icon to create a new SoftGRE profile. c. Click **OK**.
IPsec Tunnel Mode	Indicates the tunnel mode for the Ruckus GRE and SoftGRE profile.	Select an option: ● Disable ● SoftGRE ● Ruckus GRE
IPsec Tunnel Profile	Indicates the tunnel profile for SoftGRE. **NOTE** Select the same tunnel type for IPsec tunnel profile in WLAN configuration.	Choose the option from the list.
Syslog Options		
Enable external syslog server for APs	Enables the AP to send syslog data to the syslog server on the network.	Select the option.

TABLE 44 AP Zone Details for SZ100 and vSZ-E platforms (continued)

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

TABLE 44 AP Zone Details for SZ100 and vSZ-E platforms (continued)

Field	Description	Your Action
SNMPv3 Agent	Indicates SNMPv3 agent is applied.	If the SNMPv3 agent is enabled, configure the community settings. a. Click **Create** and enter **User**. b. Select the required **Authentication**. c. Enter the **Auth Pass Phrase**. d. Select the **Privacy** option. e. Select the required **Privilege**. If you select **Notification**, select the option **Trap** or **Inform** and enter the **Target IP** and **Target Port**. f. Click **OK**.
DHCP Service for Wi-Fi Clients		
Enable DHCP Service in this zone	Enables the DHCP service for this zone.	Select the check box.
Advanced Options		
Restricted AP Access Profile **NOTE** This feature is available from 5.2 release and onwards.	Restricted AP Access blocks access to the AP's standard well know open ports to protect the APs and enhance their security.	Select the Restricted AP Access profile from the drop-down. You can also create a new profile by clicking **+** icon. **NOTE** By default this feature is disabled. **NOTE** You can add maximum five Restricted AP Access profiles for a zone.
Channel Mode	Indicates if location-based service is enabled. If you want to allow indoor APs that belong to this zone to use wireless channels that are Channel Mode regulated as indoor-use only.	Select the **Allow indoor channels** check box.
Smart Monitor	Indicates AP interval check and retry threshold settings.	Select the check box and enter the interval and threshold.
AP Ping Latency Interval	Measures the latency between the controller and AP periodically, and sends this data to SCI.	Enable by moving the button to ON to measure latency.
AP Management VLAN	Indicates the AP management VLAN settings.	Choose the option. Click **VLAN ID**, and then type the VLAN ID that you want to assign (valid range is from 1 to 4094). To keep the same management VLAN ID that has been configured on the AP, click Keep AP's settings. **ATTENTION** For standalone APs, set the AP Ethernet port to trunk before changing the AP Management VLAN settings.
Rogue AP Detection	Indicates rogue AP settings. **NOTE** Rogue detection AP in active-active mode cluster redundancy environment is restricted from storing its own BSSIDs to avoid considering its own APs as rogues attacking.	Enable the option.

TABLE 44 AP Zone Details for SZ100 and vSZ-E platforms (continued)

Field	Description	Your Action
Rogue Classification Policy	Indicates the parameters used to classify rogue APs. This option is available only if you enable the **Rogue AP Detection** option.	Select the options for rogue classification policy: ● **Enable events and alarms for all rogue devices** ● **Enable events and alarms for malicious rogues only** ● **Report RSSI Threshold** - enter the threshold. Range: **0** through **100**. ● **Protect the network from malicious rogue access points** - Enable the option and choose one of the following: – **Aggressive** – **Auto** – **Conservative** ● **Radio Jamming Detection** - Enable the option and enter the **Jamming Threshold** in percentage.
DoS Protection	Indicates settings for blocking a client.	Select the check box and enter the duration in seconds.
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.
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.

TABLE 44 AP Zone Details for SZ100 and vSZ-E platforms (continued)

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

4. Click **OK**.

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

NOTE

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

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

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

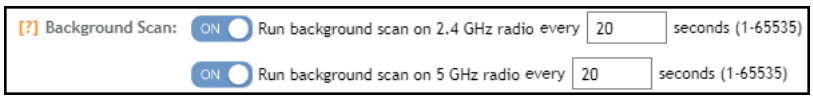
The controller offers the ChannelFly and Background Scanning automatic channel selection methods for spectrum utilization and performance optimization.

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 45

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.

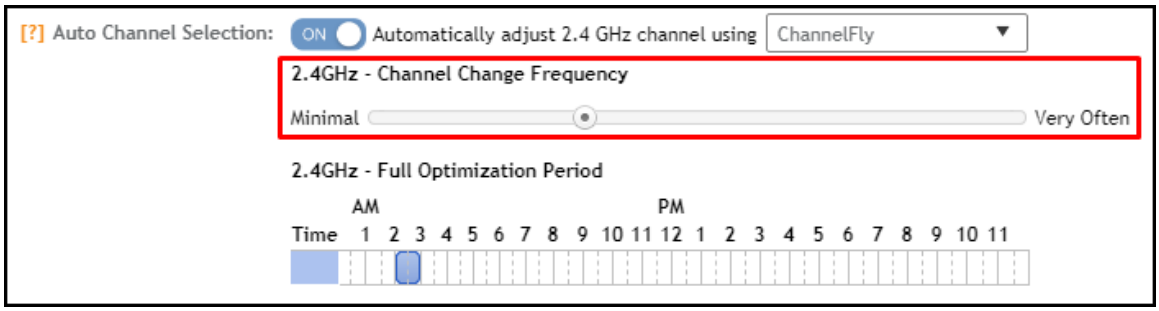


ChannelFly

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 46.



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 46 Client Threshold Table

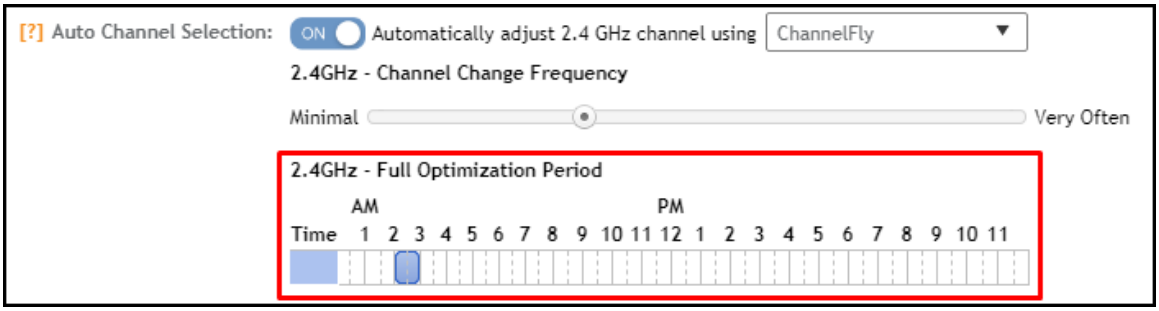
CCF	100	90	80	70	60	50	40	30	20	10	1
Client Threshold	10	9	8	7	6	5	4	3	2	1	0

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 47 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.

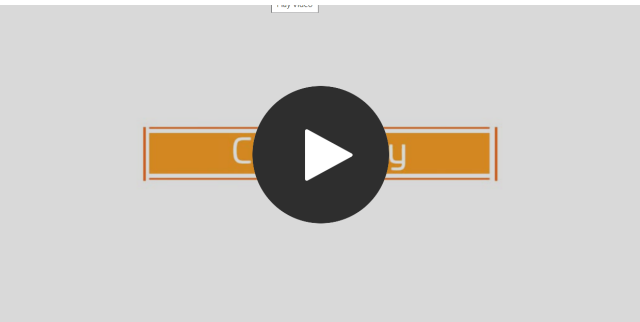
Background Scanning uses Background Scan to collect information on the presence of neighboring APs. Background Scanning focuses on finding a channel with the fewest number of neighbors.

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.

Moving an AP Zone Location

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

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

Creating a New Zone using a Zone Template

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

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

Extracting a Zone Template

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

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

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

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

Applying a Zone Template

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

Follow these steps to apply a zone template:

1. From the Access Points page, locate the zone where you want to apply the zone template.
2. Click **More** and select **Apply Zone Template**, the **Import Zone Template** dialog box appears.
3. From the **Select a Zone template** drop-down, select the template.
4. Click **OK**, a confirmation message appears asking to apply the zone template to the AP zone.
5. Click **Yes**. The zone template was applied successfully.

   You have completed applying zone template to the AP zone.

Configuring Templates

Working with Zone Templates

You can create, configure, and clone zone templates.

To view details about a zone template, go to **Administration** > **System** > **Templates** > **Zone Templates** and click a zone. The respective contextual tabs are displayed at the bottom of the page.

TABLE 48 Zone Templates: Contextual Tabs

Tab	Description
Zone Configuration	Displays details of the respective zone template.
AP Group	Displays details of the respective AP group. You can create or configure an AP group. Refer to *Creating an AP Group*.
WLAN	Displays details of the respective WLAN and WLAN group. You can create or configure a WLAN and a WLAN group. Refer to *Working with WLANs and WLAN Groups*.
Hotspots and Portals	Displays details of the respective hotspots and portals. Refer to *Working with Hotspots and Portals*.
Access Control	Displays details of the respective access control. Refer to *Configuring Access Control*.

TABLE 48 Zone Templates: Contextual Tabs (continued)

Tab	Description
Authentication and Accounting	Displays details of the respective authentication and accounting servers. Refer to *Authentication* and *Accounting* respectively.
Bonjour	Displays details of the respective Bonjour services. Refer to *Bonjour*.
Tunnels & Ports	Displays details of the respective tunnels and ports. Refer to *Working with Tunnels and Ports*.
WIPS	Displays details of the respective WIPS policies. Refer to *Classifying Rogue Policies*.
Radius	Displays details of the respective VSA profiles. You can create or configure a VSA profile. Refer to *Creating a Vendor-Specific Attribute Profile*.

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 49 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**.

TABLE 49 Zone Template Details (continued)

Field	Description	Your Action
AP IP Mode	Indicates the IP version that applies.	Select the option: • **IPv4 only** • **IPv6 only** • **Dual**
Historical Connection Failures	Allows the zone APs to report client connection failures so that the administrator can view past connection problems from the Troubleshooting menu.	Click the button.
DP Zone Affinity Profile	Specifies the DP affinity profile for the zone. **NOTE** This option is supported only on vSZ-H.	Select the zone affinity profile from the list.
SSH Tunnel Encryption	Specifies the encryption that reduces the load on control of SSH traffic.	Select the required option: • **AES 128** • **AES 256**
Cluster Redundancy	Provides cluster redundancy option for the zone. **NOTE** Cluster redundancy is supported only on SZ300 and vSZ-H.	Select the required option: • **Zone Enable** • **Zone Disable**
Radio Options		
Channel Range	Indicates that you want to override the 2.4GHz channel range that has been configured for the zone.	Select **Select Channel Range (2.4G)** check boxes for the channels on which you want the 2.4GHz radios to operate. Channel options include channels 1 to 11. By default, all channels are selected.
DFS Channels	Allows ZoneFlex APs to use DFS channels.	Click to enable the option.
Channel 144	Provides channel 140 and 144 support for 11ac and 11ax APs. Enabling this option supports 20 MHz, 40 MHz, or 80 MHz channel modes. The 80+80 MHz and 160 MHz modes are supported if the AP supports these modes. Disabling this option provides Channel 140 support only to 20 MHz mode. **NOTE** This option is available for selection only if you enable the **DFS Channels** option. **NOTE** This feature is currently supported only in the United States.	Click to enable the option.
Channel Range (5G) Indoor	Indicates for what channels want the 5GHz radios to operate.	Select the check boxes.
Channel Range (5G) Outdoor	Indicates for what channels want the 5GHz radios to operate.	Select the check boxes.

TABLE 49 Zone Template Details (continued)

Field	Description	Your Action
Radio Options b/g/n (2.4 GHz)	Indicates the radio option 2.4 GHz configurations.	Select the following options: • **Channelization**—Set the channel width used during transmission to either **20** or **40** (MHz), or select **Auto** to set it automatic. • **Channel**—Select the channel to use for the b/g/n (2.4GHz) radio, or select **Auto** to set it automatic. • **TX Power Adjustment**—Select the preferred TX power, if you want to manually configure the transmit power on the 2.4GHz radio. By default, TX power is set to **Full/Auto** on the 2.4GHz radio. **NOTE** If you choose Min, the transmit power is set to 0dBm (1mW) per chain for 11n APs, and 2dBm per chain for 11ac APs. If you choose Max, the transmit power is set to the max allowable value according to the AP's capability and the operating country's regulations.
Radio Options a/n/ac (5 GHz)	Indicates the radio option 5 GHz configurations.	Select the following options: • **Channelization**—Set the channel width used during transmission to either **20**, **40**, **80**, **80+80** or select **Auto**. • **Channel**—For Indoor and Outdoor, select the channel to use for the a/n/c (5GHz) radio, or select **Auto**. • **TX Power Adjustment**—Select the preferred TX power, if you want to manually configure the transmit power on the 5GHz radio. By default, TX power is set to **Full/Auto** on the 5GHz radio. **NOTE** If you choose Min, the transmit power is set to 0dBm (1mW) per chain for 11n APs, and 2dBm per chain for 11ac APs. If you choose Max, the transmit power is set to the max allowable value according to the AP's capability and the operating country's regulations.
AP GRE Tunnel Options		
Ruckus GRE Profile	Indicates the GRE tunnel profile.	Choose the GRE tunnel profile from the drop-down.
Ruckus GRE Forwarding Broadcast	Forwards the broadcast traffic from network to tunnel.	Click the option to enable forwarding broadcast.
Soft GRE Profiles	Indicates the SoftGRE profiles that you want to apply to the zone.	a. Click the **Select** checkbox, a form is displayed. b. From the A**vailable Profiles**, select the profile and click the -> icon to choose it. You can also click the + icon to create a new SoftGRE profile. c. Click **OK**.

TABLE 49 Zone Template Details (continued)

Field	Description	Your Action
IPsec Tunnel Mode	Indicated the tunnel mode for the Ruckus GRE and SoftGRE profile.	Select an option: ● Disable ● SoftGRE ● Ruckus GRE
IPsec Tunnel Profile	Indicates the tunnel profile for SoftGRE. **NOTE** Select the same tunnel type for IPsec tunnel profile in WLAN configuration.	Choose the option from the drop-down.
Syslog Options		
Enable external syslog server for Aps	Indicates if an external syslog server is enabled.	Select the check box and update the following details for the AP to send syslog messages to syslog server. If the primary server goes down, the AP send syslog messages to the secondary server as backup: ● **Primary Server Address** ● **Secondary Server Address** ● **Port** for the respective servers ● **Portocol**: select between UDP and TCP protocols ● **Event Facility** ● **Priority** ● **Send Logs**: you can choose to send the General Logs, Client Logs or All Logs
AP SNMP Options		
Enable AP SNMP	Indicates if the AP SNMP option is enabled.	Select the check box.
SNMPv2 Agent	Indicates SNMPv2 Agent is applied.	a. Click **Create** and enter **Community**. b. Select the required **Privilege**: **Read** or **Write**. c. Click **OK**.
SNMPv3 Agent	Indicates SNMPv3 Agent is applied.	a. Click **Create** and enter **User**. b. Select the required **Authentication**: ● **None** ● **SHA** 1. Enter the **Auth Pass Phrase** 2. Select the **Privacy** option. For **DES** and **AES** options, Enter the **Privacy Phrase**. ● **MD5** 1. Enter the **Auth Pass Phrase** 2. Select the **Privacy** option. For **DES** and **AES** options, Enter the **Privacy Phrase**. c. Select the required **Privilege**: **Read** or **Write**. d. Click **OK**.
Advanced Options		
Channel Mode	Indicates if location-based service is enabled.	Select the check box and choose the option.
Auto Channel Selection	Indicates auto-channel settings.	Select the required check boxes and choose the option.
Background Scan	Runs a background scan.	Select the respective check boxes and enter the duration in seconds.

TABLE 49 Zone Template Details (continued)

Field	Description	Your Action
Smart Monitor	Indicates AP interval check and retry threshold settings.	Select the check box and enter the duration and threshold.
AP Ping Latency Interval	Measures the latency between the controller and AP periodically, and send this data to SCI	Enable by moving the radio button to ON to measure latency.
AP Management VLAN	Indicates the AP management VLAN settings.	Choose the option. If you select **VLAN ID**, enter the VLAN ID that you want to assign (valid range is from 1 to 4094). To keep the same management VLAN ID that has been configured on the AP, click **Keep AP's settings**. **ATTENTION** For standalone APs, set the AP ethernet port to trunk before changing the AP Management VLAN settings.
Rogue AP Detection	Indicates rogue AP settings. **NOTE** Rogue detection AP in active-active mode cluster redundancy environment is restricted from storing its own BSSIDs to avoid considering its own APs as 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.

TABLE 49 Zone Template Details (continued)

Field	Description	Your Action
Location Based Service	To disable the LBS service for this AP group, clear the Enable LBS service check box. To use a different LBS server for this AP group, select the Enable LBS service check box, and then select the LBS server that you want to use from the drop-down list.	Select the check box and choose the options.
Client Admission Control	Indicates the load thresholds on the AP at which it will stop accepting new clients. **NOTE** Client admission cannot be enabled when client load balancing or band balancing is enabled.	Select the **Enable** check box 2.4 GHz Radio or 5GHz Radio and update the following details: • **Min Client Count** • **Max Radio Load** • **Min Client Throughput**
AP Reboot Timeout	Indicates AP reboot settings.	Choose the required option for: • **Reboot AP if it cannot reach default gateway after** • **Reboot AP if it cannot reach the controller after**
Recovery SSID	Allows you to enable or disable the Recovery(Island) SSID broadcast on the controller.	Enable **Recovery SSID Broadcast**
Direct Multicast	Indicates whether multicast traffic is sent from a wired device, wireless device or from the network.	Select one or more of the following: • **Multicast Traffic from Wired Client** • **Multicast Traffic from Wireless Client** • **Multicast Traffic from Network**

4. Click **OK**.

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

Exporting Zone Templates

You can export a zone template.

To export a zone template:

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

   NOTE
   For SmartZone 5.2.1 or earlier releases, from the application select, **System** > **Templates** > **Zone Templates**.

2. Select the zone template that you want to export and click **Export Template**.
3. A pop-up appears prompting you to **Open** or **Save** the zone template file with .**bak** extension. Click:
   - **Open**—To view the template file
   - **Save**—Select the destination folder where you want to save the template file and then click **Open** to view it.

Importing Zone Templates

You can import zone templates and upload them to the system.

> **NOTE**
> Configuration references to global services or profiles cannot be imported, manually configure it after importing.

To import a zone template:

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

   > **NOTE**
   > For SmartZone 5.2.1 or earlier releases, from the application select, **System** > **Templates** > **Zone Templates**.

2. Click **Import**, the Import Zone Templates form appears.
3. Click **Browse** and select the template file.
4. Click **Upload**.

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.

Configuring And Monitoring AP Zones

If no tunneled WLANs exist in the zone, you can change the tunnel type from SoftGRE to GRE or GRE + UDP.

MVNO accounts are currently unsupported by SoftGRE tunnels. If you create an MVNO account and assign an AP zone that is using a SoftGRE tunnel, an error message appears.

1. Follow the steps as described in *Creating an AP Zone* in *RUCKUS SmartZone AP Management Guide* to change the tunnel type from SoftGRE.
2. Scroll down to the **AP GRE Tunnel Options** section and select the **Ruckus GRE Profile** or click **Add** to create a new profile.
3. From the Create Ruckus GRE Profile window, select the **Ruckus Tunnel Mode** to change from SoftGRE.

   If you attempt to change the tunnel type when a tunneled WLAN exists within the zone, the following error message appears:

   ```
   Unable to update the configuration of the AP zone. Reason: It is disallowed to change the
   tunnel type, because it
   has tunneled WLAN.
   ```
4. Click **OK**.

   The zone configuration information is displayed.

Moving a Single Access Point to a Different AP Zone

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

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

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

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

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

BSS Coloring

Configuring BSS Coloring for a Zone

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

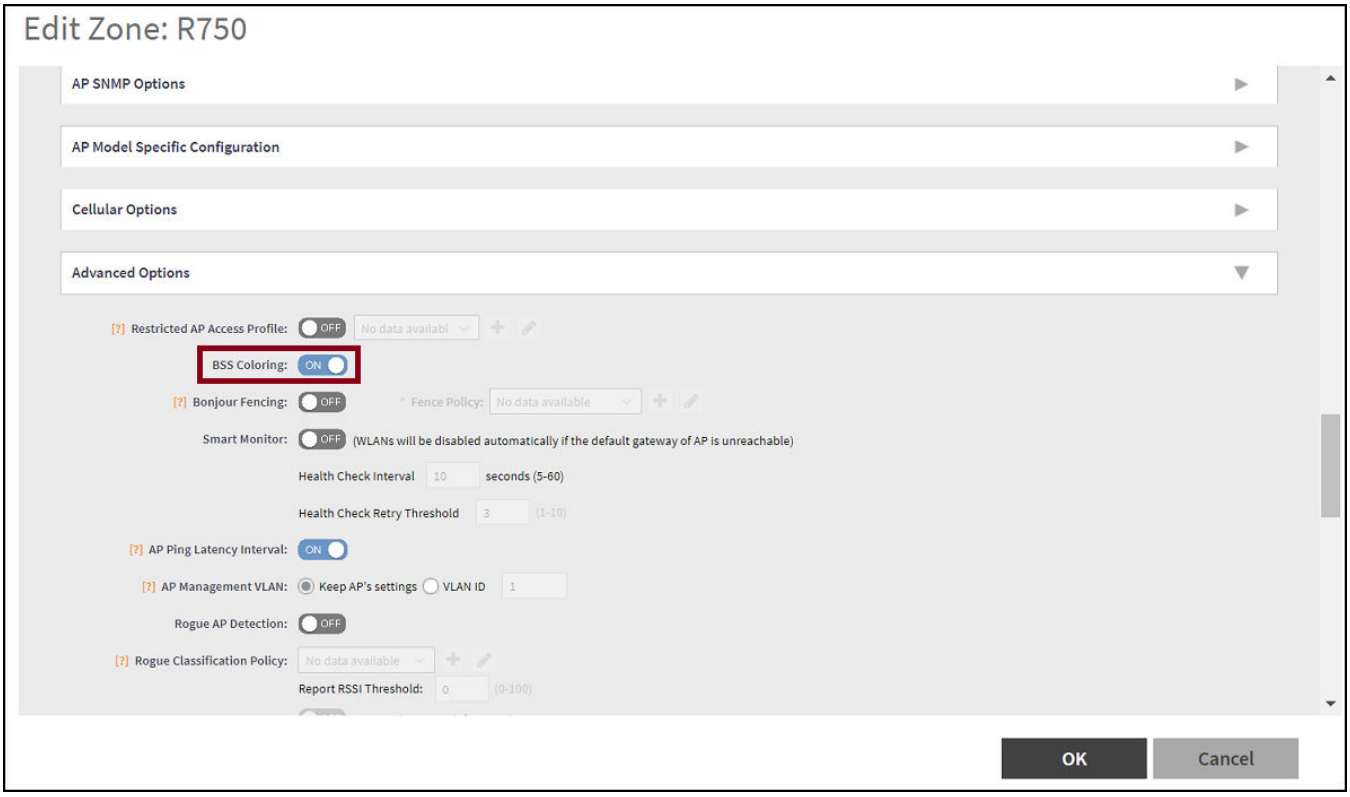
Complete the following steps to configure BSS Coloring for a zone.

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

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

   The **Configure Zone** page is displayed.

   FIGURE 41 Configuring BSS Coloring in Zone Configuration



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

   NOTE
   The BSS color value is automatically selected.

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

Configuring BSS Coloring for an Individual Access Point

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

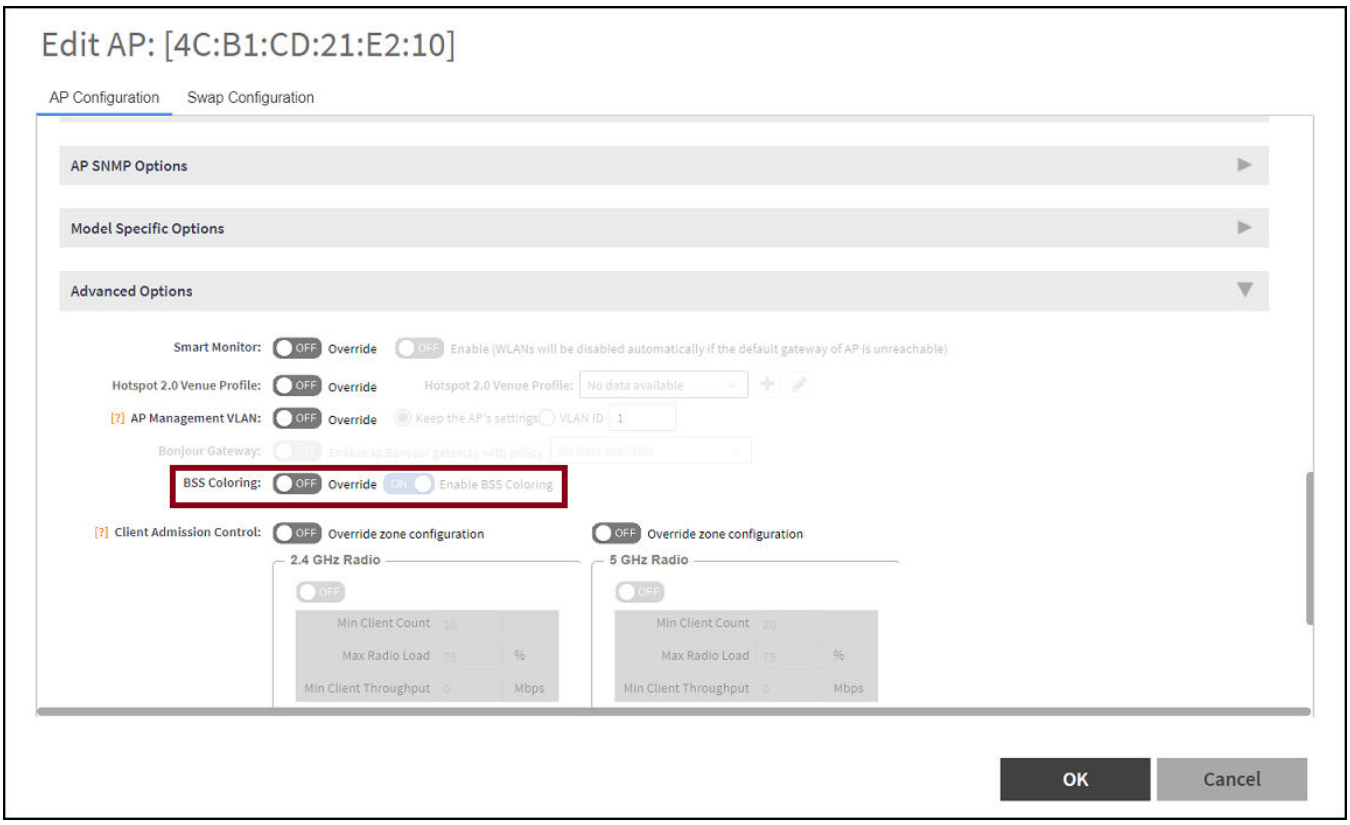
NOTE
BSS Coloring for individual access points is available for 802.11ax APs only.

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

3. Click **Configure**.

   The **AP Configuration** page is displayed.

   FIGURE 42 Configuring BSS Coloring for an Individual Access Point Configuration



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

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

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

Configuring BSS Coloring within an AP Group

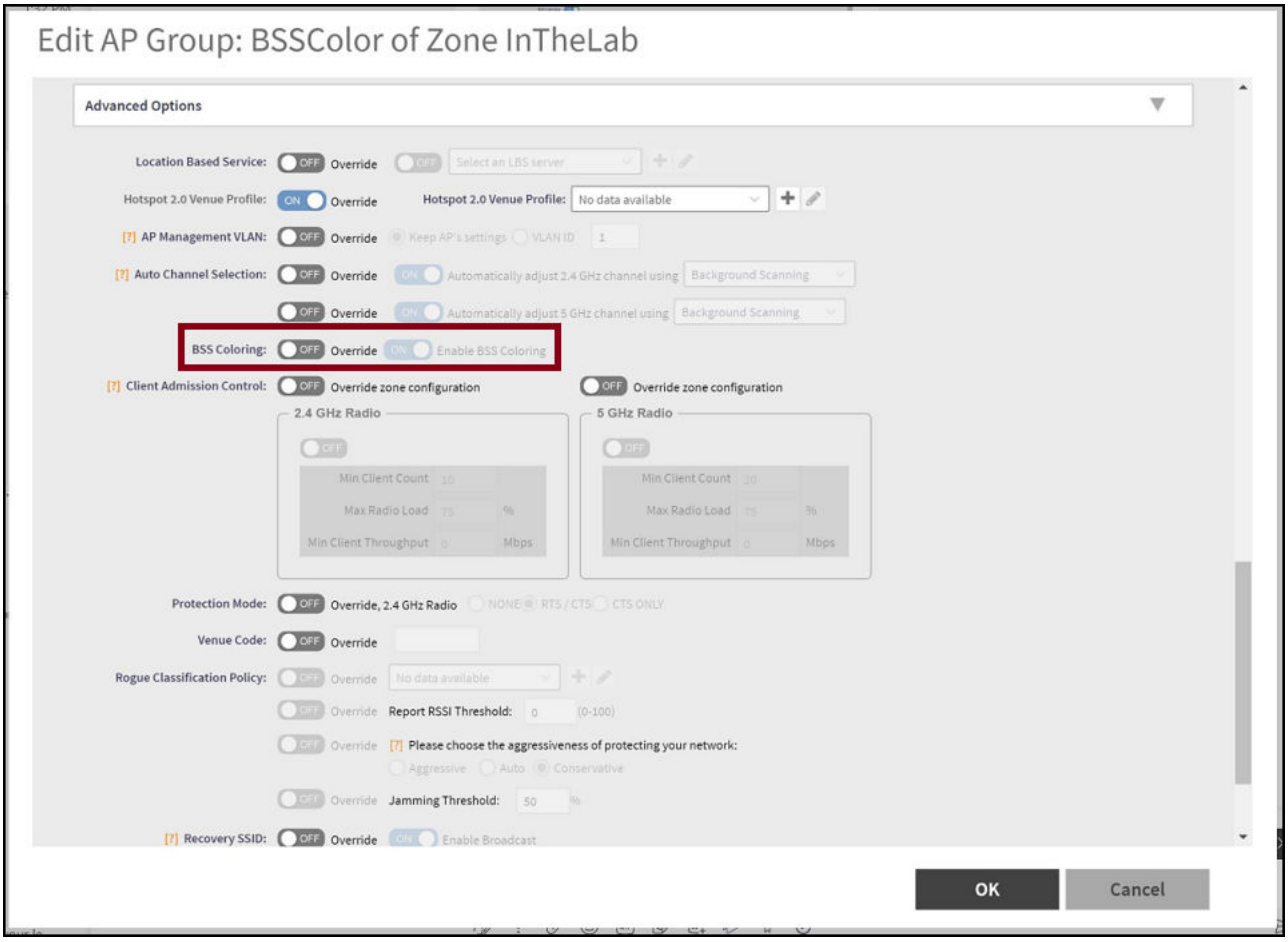
Complete the followings steps to configure the BSS Coloring within an AP group.

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

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

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

   FIGURE 43 Configuring BSS Coloring within an AP Group



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

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

RUCKUS NOR Certificate Safe Storage (RNCSS) Support

RUCKUS NOR Certificate Safe Storage (RNCSS) Support

RUCKUS NOR Certificate Safe Storage (RNCSS) is an application that stores and retrieves the device certificate and key from the NOT OR (NOR) flash memory of an AP, in the event of corruption or loss of the device certificate and key.

RNCSS Overview

The RNCSS procedure is executed in two phases:

- **Backup**: Storing the certificate and key to the NOR flash memory.

  From the unused NOR flash memory of an AP, a new memory region called the Certificate Partition is utilized for the backup.
- **Recovery**: Verification and recovery of certificate and key from the NOR flash memory during bootup.

For a newly manufactured AP in the factory setup phase, the RNCSS feature is effective on the first bootup; an initial backup is performed to install the device certificate and key in the NOR memory along with the AP serial number, MAC address, and the Magic ID (refer to New NOR Memory Region (Certificate Partition) on page 186).

For APs that are already deployed in a network, the RNCSS feature is effective after a firmware image upgrade. On the first reboot, an initial backup is performed to store the device certificate and key in the NOR memory.

After the RNCSS support is initiated on new and deployed APs, the AP checks for the device certificate during every reboot. If it is lost or corrupted, the NOR certificate copy is retrieved and stored in the mount point. Upon backup and recovery of the device certificate and key, the corresponding events are triggered and reported to the controller. Refer to System Events on page 188 for more information on the RNCSS-related events.

> **NOTE**
> In case the NOR certificate copy is lost or corrupted, the NOT AND (NAND) or the Embedded MultiMedia Card (eMMC) certificate copy is backed up to the NOR memory. Conversely, if the NAND or the eMMC certificate copy is lost or corrupted, then the NOR copy is used. The lost or corrupted device certificate and key is retrieved on the next AP reboot. Refer to Certificate and Key Backup and Recovery Mechanism in a Deployed AP on page 187 for more information.

The RNCSS feature provides the following benefits:

- A backup of the certificate and key is always available in the NOR flash memory.
- Reduces the occurences of Return Merchandise Authorization (RMA) for the impacted APs due to critical certificate data loss.
- Eliminates redundant data storage in both the NAND, eMMC, and NOR flash memory.
- The NOR flash memory is more robust and reliable than the NAND or the eMMC flash memory.
- Enhanced security in cases where an AP serial number or a MAC address is modified.

Requirements

The memory utilization of the NOR memory region varies depending on the AP models. Refer to Supported AP Models and NOR Memory Utilization for RNCSS on page 187 for more information.

Considerations

Beginning with SmartZone 7.0.0, the RNCSS feature is introduced. During an upgrade to SmartZone 7.0.0, the RNCSS feature is enabled automatically, and disabled during a downgrade to an earlier version of SmartZone. A copy of the certificate and key is retained in the NOR memory after a downgrade, but they are not used.

Impacted Systems

- Change in the existing AP bootup design.
- Modification in Device Tree Source (DTS) of an AP due to the introduction of the new NOR memory region.

Limitations

The RNCSS logs created during the bootup in the factory setup phase may not be seen in the external syslog server since the logs are sent to the server after an AP is assigned an IP address.

New NOR Memory Region (Certificate Partition)

The new NOR memory region is used to store the device certificate and key.

The new NOR memory region has two sections:

- Header
- Body

The header has the following information:

MagicID (8)	RUCKUS-specific unique ID
Serial No (16)	Serial number of the AP
MAC (6)	MAC address of the AP
Checksum (2)	Checksum of the header
Size (4)	Number of bytes of the body
Version (1)	Version of the header
Reserved (3)	Reserved for future use (for header size, in multiples of 4)

The body has the following information:

Type (2)	Type (cert / key / system.data / 3k_cert / 3k_key)
Length (4)	Length of the data
Value (64 + *)	1- sha256sum of the data 2 - actual data

Certificate and Key Backup and Recovery Mechanism in a Deployed AP

The following section explains the backup and recovery mechanism used in the RUCKUS NOR Certificate Safe Storage (RNCSS) feature.

1. After a firmware image is upgraded on a deployed AP and during the first bootup, the AP stores and validates the certificate and key to the NOR memory region. If the validation fails, the certificate and key is backed up to the NOR memory region. On every reboot, the certificate and key is validated in the NAND or eMMC, and in the NOR copy.
2. If the certificate or key, or both, is corrupted or lost, they are recovered using the following RNCSS recovery procedure:
   a) The RNCSS recovery validates the NOR memory's header by verifying the checksum of the header. If the checksum fails, the data bytes count is verified, else the certificate's NOR memory is dumped.
   b) The AP MAC address and serial number from the NOR memory are compared with the current AP MAC address and serial number, and their values are logged into the syslog server. In case of a mismatch, an event is trigerred to the controller.
   c) In case the certificate and key is corrupted, a backup is taken and their storage locations are logged in to the syslog and the support log.
   d) The type, length, value (TLV) attributes are parsed and their checksum is validated. The parsed files are stored in a temporary location and in case of Trusted Platform Module (TPM) APs `system.data` is stored only in the TPM directory.
   e) Upon successful verification of the certificate and key, they are stored in the mount point. The temporary files are erased and the bootup sequence is continued.
   f) If the verification fails with a header mismatch error, then the NOR memory may be corrupted. If the verification fails with a certificate or key error, then the certificate or key region in the NOR memory may be corrupted.

   For any assistance, contact the RUCKUS Customer Support and be ready to provide your support log.

Supported AP Models and NOR Memory Utilization for RNCSS

RUCKUS NOR Certificate Safe Storage (RNCSS) is supported in the following AP models:

TABLE 50 Supported AP Models for RNCSS

AP Category	AP Models
802.11ax	H350, H550, R350, R550, R560, R650, R750, R760, R850, T750, T750se
802.11ac - Wave 2	C110, E510, H320, H510, R320, R510, T305e, T305i, T310c, T310d, T310n, T310s, T350c, T350d, T350ns, T350se, T811cm
802.11ac - Wave 1	R610, R710, R720, T610, T610s, T710, T710s

NOTE
All the AP models in 802.11ac wave 1 AP category and the C110, R510, and T811cm AP models in the 802.11ac wave 2 AP category have a 4-MB NOR flash memory; rest of the AP models have a 16-MB NOR flash memory.

In APs with a 16-MB NOR flash memory, from the unused 8 MB free space, 2 MB is used for the Certificate Partition to store the certificate and key. In APs with a 4-MB NOR flash memory, approximately 832 KB is used by the RNCSS.

Refer to the following example table to understand how the NOR memory is utilized in a 4-MB and a 16-MB NOR flash memory for the RNCSS procedure.

TABLE 51 Example of Memory Utilization in the NOR Memory

	4 MB NOR	16 MB NOR	AP[1] (4 MB NOR and 16 MB NOR)
Size of Certificate and Key	~3 KB	~3 KB	~3 KB
Size of system.data (zipped) (only for TPM APs)	~600 bytes	~600 bytes	~600 bytes

TABLE 51 Example of Memory Utilization in the NOR Memory (continued)

	4 MB NOR	16 MB NOR	AP[1] (4 MB NOR and 16 MB NOR)
Certificate Memory Region in NOR Flash	~832 KB *(0xD0000 Bytes)*	2 MB	1 MB
Header Size	40 bytes	40 bytes	40 bytes
Body Size	~831.96 KB *(0xCFFD8 Bytes)*	~1.99996 MB *(0x1FFFD8 Bytes)*	~0.99996 MB *(0xFFFD8 Bytes)*

[1] 802.11ac Wave 1 AP Models excluding T350c, T350d, T350ns, T350se, and T811cm

System Events

During the RUCKUS NOR Certificate Safe Storage (RNCSS) procedure, system events are raised and reported to the controller.

Refer to the following table for information on the RNCSS-related system events.

TABLE 52 RNCSS System Events

Event Code	Severity	Description
286	Warning	This event occurs when the RNCSS procedure finds a NAND or an eMMC copy of the device certificate/key that is corrupted or missing and it is recovered using the NOR copy during reboot or when using a manual recovery command.
287	Warning	This event occurs when the RNCSS procedure finds the NOR copy of the device certificate/key is corrupted or missing and it is backed up using the the NAND or the eMMC copy during reboot or when using a manual backup command.
288	Warning	This event occurs when the RNCSS procedure finds the serial number or the MAC address of an AP stored in NOR does not match with the current AP device MAC address or serial number during reboot or when using a manual command.

External Syslog Server

External Syslog Server

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

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

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

Creating an External Syslog Server Profile

The MSPs (Managed Service Provider) can set the external syslog servers one by one. This feature extracts the external syslog server setting as a profile. These profiles will be regulated by the MSP framework. The customers can then select the partner's domain-level profile while setting up a zone or an AP to send the syslog data to the syslog server on the network.

NOTE
This feature is supported only on vSZ-H.

NOTE
A maximum of 16 profiles can be created per partner domain.

To create an external syslog server profile:

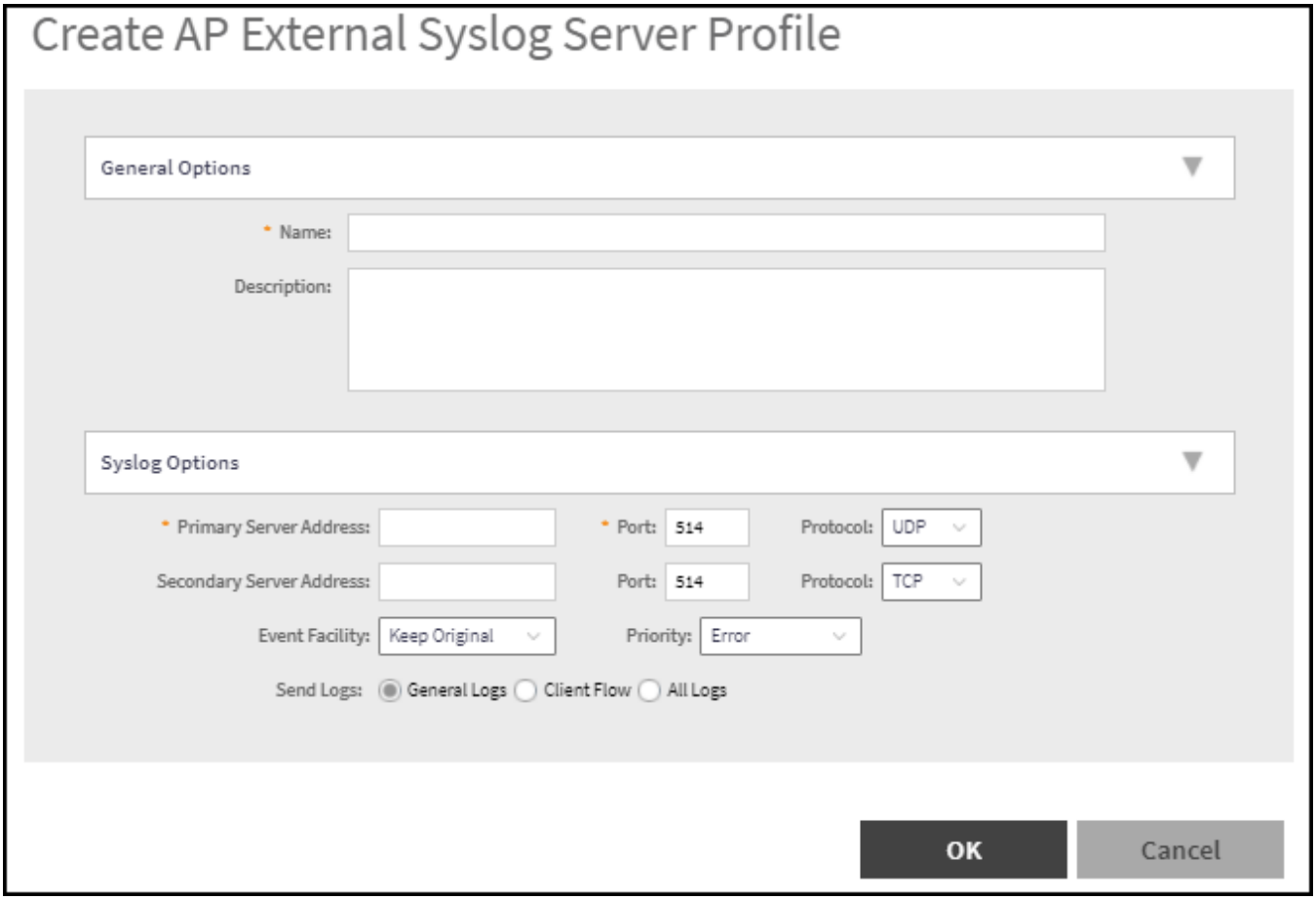
1. Select **Services** > **Others** > **AP External Syslog Server**.

   The **AP External Syslog Server Profile** page is displayed.

2. Click the **Create**.

   The **Create AP External Syslog Server Profile** page is displayed.

   FIGURE 44 Creating AP External Syslog Server Profile



3. Configure the following:
   - Name: Enter a name for the profile you want to create.
   - Description: Enter a short description for the profile.
   - Primary Server Address: Enter the primary server IP address to send the syslog messages.
     - Port: Enter the server port to which the messages must be forwarded.
     - Protocol: Select the protocol.
   - Secondary Server Address: Enter the secondary server IP address to send the syslog messages if the primary server goes down.
     - Port: Enter the server port to which the messages must be forwarded.
     - Protocol: Select the protocol.
   - Event Facility: Select the facility level that will be used by the syslog message. Options include: Keep Original, Local0 (default), Local1, Local2, Local3, Local4, Local5, Local6, and Local7.
   - Priority: Select the lowest priority level for which events will be sent to the syslog server. For example, to only receive syslog messages for events with the warning (and higher) priority, select **Warning**. To receive syslog messages for all events, select **All**.
   - Send logs: Choose to send the General Logs, Client Logs or All Logs
4. Click **OK**.

Support Requirements for the Controller

Support SKU Requirement

To provide the highest quality of service and support to customers, RUCKUS requires customers to have active support for all RUCKUS controllers and AP licenses.

Support SKUs per Controller

For different types of controllers, the support SKUs in the following table are available. You will need one of the support SKUs per controller.

TABLE 53 New SKUs per Controller

Controller Type	Support SKU
vSZ RTU (Virtual controller)	S01-VSCG-1L00, S01-VSCG-3L00, S01-VSCG-5L00, S02-VSCG-1L00, S02-VSCG-3L00, S02-VSCG-5L00, S04-VSCG-1L00, S04-VSCG-3L00, S04-VSCG-5L00, S08-VSCG-1L00, S08-VSCG-3L00, S08-VSCG-5L00, S62-VSCG-1L00, S62-VSCG-3L00, S62-VSCG-5L00
SZ144	S01-S144-1000, S01-S144-3000, S01-S144-5000, S02-S144-1000, S02-S144-3000, S02-S144-5000, S04-S144-1000, S04-S144-3000, S04-S144-5000, S08-S144-1000, S08-S144-3000, S08-S144-5000, S62-S144-1000, S62-S144-3000, S62-S144-5000
SZ104	S01-S104-1000, S01-S104-3000, S01-S104-5000, S02-S104-1000, S02-S104-3000, S02-S104-5000, S04-S104-1000, S04-S104-3000, S04-S104-5000, S08-S104-1000, S08-S104-3000, S08-S104-5000, S62-S104-1000, S62-S104-3000, S62-S104-5000
SZ124	S01-S124-1000, S01-S124-3000, S01-S124-5000, S02-S124-1000, S02-S124-3000, S02-S124-5000, S04-S124-1000, S04-S124-3000, S04-S124-5000, S08-S124-1000, S08-S124-3000, S08-S124-5000, S62-S124-1000, S62-S124-3000, S62-S124-5000
SZ300 (DC Power Supply)	S01-S300-1002, S01-S300-1012, S01-S300-3002, S01-S300-3012, S01-S300-5002, S01-S300-5012, S02-S300-1002, S02-S300-1012, S02-S300-3002, S02-S300-3012, S02-S300-5002, S02-S300-5012, S04-S300-1002, S04-S300-1012

TABLE 54 Renewal SKUs per Controller

Controller Type	Support SKU
vSZ RTU (Virtual controller)	S24-VSCG-1L00, S24-VSCG-3L00, S24-VSCG-5L00, S28-VSCG-1L00, S28-VSCG-3L00, S28-VSCG-5L00, S41-VSCG-1L00, S41-VSCG-3L00, S41-VSCG-5L00, S51-VSCG-1L00, S51-VSCG-3L00, S51-VSCG-5L00, S72-VSCG-1L00, S72-VSCG-3L00, S72-VSCG-5L00
SZ144	S24-S144-1000, S24-S144-3000, S24-S144-5000, S28-S144-1000, S28-S144-3000, S28-S144-5000, S41-S144-1000, S41-S144-3000, S41-S144-5000, S51-S144-1000, S51-S144-3000, S51-S144-5000, S72-S144-1000, S72-S144-3000, S72-S144-5000
SZ104	S24-S104-1000, S24-S104-3000, S24-S104-5000, S28-S104-1000, S28-S104-3000, S28-S104-5000, S41-S104-1000, S41-S104-3000, S41-S104-5000, S51-S104-1000, S51-S104-3000, S51-S104-5000, S72-S104-1000, S72-S104-3000, S72-S104-5000
SZ124	S24-S124-1000, S24-S124-3000, S24-S124-5000, S28-S124-1000, S28-S124-3000, S28-S124-5000, S41-S124-1000, S41-S124-3000, S41-S124-5000, S51-S124-1000, S51-S124-3000, S51-S124-5000, S72-S124-1000, S72-S124-3000, S72-S124-5000
SZ300 (DC Power Supply)	S24-S300-1002, S24-S300-1012, S24-S300-3002, S24-S300-3012, S24-S300-5002, S24-S300-5012, S28-S300-1002, S28-S300-1012, S28-S300-3002, S28-S300-3012, S28-S300-5002, S28-S300-5012, S41-S300-1002, S41-S300-1012, S41-S300-3002, S41-S300-3012, S41-S300-5002, S41-S300-5012, S51-S300-1002, S51-S300-1012, S51-S300-3002, S51-S300-3012, S51-S300-5002, S51-S300-5012, S72-S300-1002, S72-S300

Support SKUs per AP License

For AP licenses, the support SKUs in the following table are available. You will need one of the support SKUs per AP license. You are required to have 100 percent of the AP licenses covered by the support SKUs in order to be entitled to support coverage.

The support requirement ensures that you have full access to the RUCKUS Support team for any assistance or troubleshooting needs. Additionally, it allows you to upgrade your RUCKUS controller to the latest versions as they become available, ensuring you always have access to the newest features and security updates.

TABLE 55 New SKUs per AP License

AP License	Support SKU
L09-0001-SG00	S01-0001-1LSG, S01-0001-3LSG, S01-0001-5LSG, S02-0001-1LSG, S02-0001-3LSG, S02-0001-5LSG, S04-0001-1LSG, S04-0001-3LSG, S04-0001-5LSG, S08-0001-1LSG, S08-0001-3LSG, S08-0001-5LSG, S62-0001-1LSG, S62-0001-3LSG, S62-0001-5LSG

TABLE 56 Renewal SKUs per AP License

AP License	Support SKU
L09-0001-SG00	S24-0001-1LSG, S24-0001-3LSG, S24-0001-5LSG, S28-0001-1LSG, S28-0001-3LSG, S28-0001-5LSG, S41-0001-1LSG, S41-0001-3LSG, S41-0001-5LSG, S51-0001-1LSG, S51-0001-3LSG, S51-0001-5LSG, S72-0001-1LSG, S72-0001-3LSG, S72-0001-5LSG

Managing Licenses

Depending on the number of RUCKUS APs that you need to manage with the controller, you may need to upgrade the controller license as your network expands.

The maximum number of access points that the controller can manage is controlled by the license file that came with the controller. If the number of access points on the network exceeds the limit in the license file, you will need to obtain an additional license file and upload it to the controller.

> **NOTE**
> For information on obtaining additional license files, contact RUCKUS Support Team or an authorized RUCKUS reseller.

The maximum number of APs that a license supports depends on its stock-keeping unit (SKU).

The AP capacity license refers to the number of approved APs, while the Connected AP represents the total number of APs that are currently connected to the controller. AP capacity is based on system resources (CPU/RAM) and not the AP license count.

For example, a single vSZ-H can support:

- 10,000 2-radio APs (1x resources) or
- 5,000 3-radio APs (2x resources) or
- 2,000 ICX switches (5x resources)

Built-in Licenses

Beginning with SmartZone 6.1.0, the SZ144 platform supports 25 permanent AP management licenses that do not require renewal. These permanent licenses are not included in the calculation of the SZ144 support license compliance and are not transferable to any other platforms. SZ144 does not have any default temporary AP license.

Upgrade earlier versions of SZ144 to SZ6.1.0 or later to get the 25 permanent AP licenses. After the upgrade, the number of Switch or RXGW default licenses will be reset to 1. To continue using Switch or RXGW, purchase the required license from RUCKUS.

> **NOTE**
> Purchasing support for the SZ144 appliance will also cover the support for the 25 built in AP licenses.

Viewing Installed Licenses

You can synchronize the license data, import a license file into the controller if it is unable to connect to the RUCKUS SmartLicense system, and release licenses bound to an offline controller by downloading a copy of the licenses.

Perform these steps to check installed licenses.

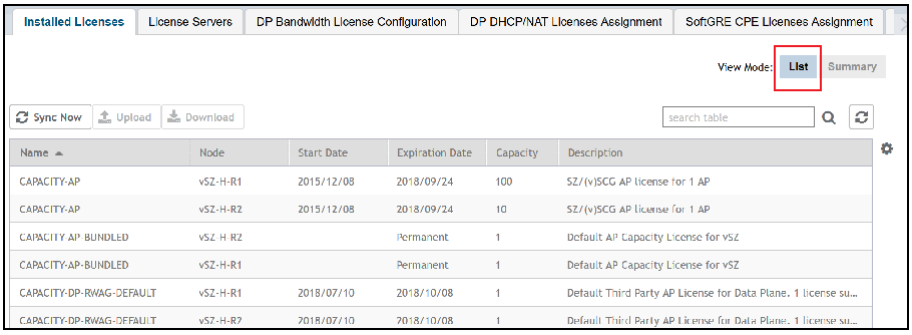
1. Go to **Administration** > **Licenses**.
2. Select the **Installed Licenses** tab.

   The **List** view is displayed as shown in the following example.

3. Select **List** as the View Mode.

   The license **List** view is displayed as shown in the following example.

   FIGURE 45 License List View



In the **List** view, the following information is displayed for licenses that have been uploaded to the controller:

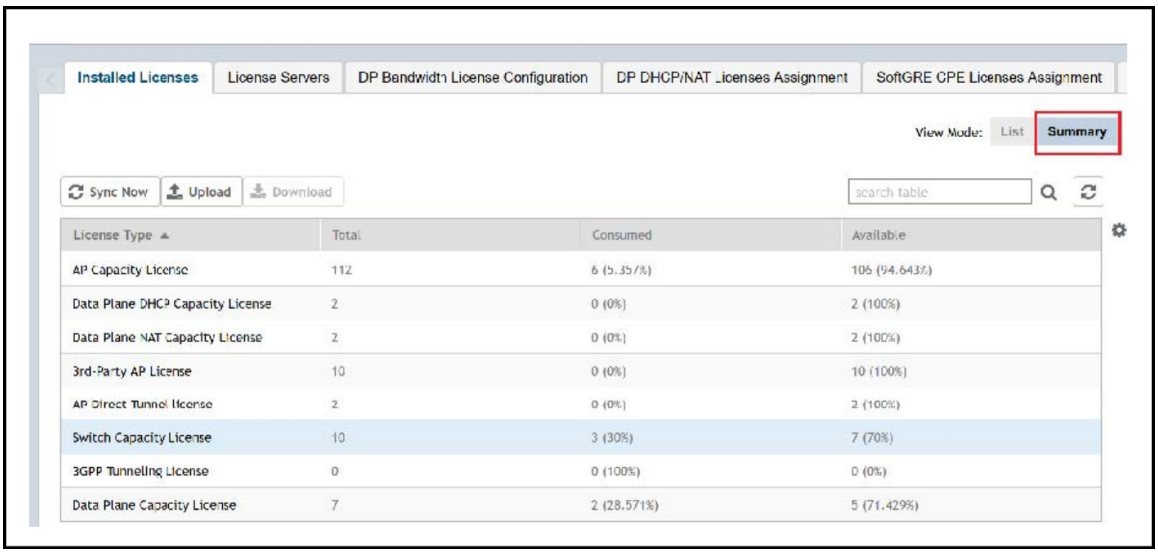
- Name: The name of the node to which the license was uploaded
- Node: The name of the controller node
- Start Date: The date when the license file was activated
- Expiration Date: For time-bound licenses, the date when the license file expires
- Capacity: The number of units or license seats that the license file provides
- Description: The type of license

4. Select **Summary** as the View Mode.

   In the **Summary** view, the information shown in the following example is displayed for the licenses that have been uploaded to the controller.

   - License Type: The type of license uploaded
   - Total: The total licenses (both consumed and available)
   - Consumed: The number of licenses consumed
   - Available: The licenses available

   FIGURE 46 License Summary View



Importing Installed Licenses

If the controller is disconnected from the Internet or is otherwise unable to communicate with the RUCKUS SmartLicense system (due to firewall policies, etc.), you can manually import a license entitlement file into the controller.

NOTE
The option to import a license file manually into the controller is only available if the controller is using the cloud license server.

1. Obtain the license file. You can do this by logging on to your RUCKUS Support account, going to the license management page, and then downloading the license file (the license file is in .bin format).
2. Log on to the controller web interface, and then go to **Administration** > **Administration** > **Licenses**.
3. Select the **Installed Licenses** tab.
4. Select the node for which you are uploading the license file and click **Upload.**

   The **Upload License** page appears where you must provide the following information:

   - Select Controller: Select the node for which you are uploading the license file.
   - Select License File: Click **Browse**, locate the license file (.bin file) that you downloaded from your RUCKUS Support account, and then select it.

The page refreshes, and the information displayed changes to reflect the updated information imported from the SmartLicense platform.

Synchronizing the Controller with the License Server

By default, the controller automatically synchronizes its license data with the selected license server every 24 hours. If you made changes to the controller licenses (for example, you purchased additional licenses) and you want the controller to download the updated license data immediately, you can trigger a manual synchronization.

1. Log in to the controller web interface, and select **Administration** > **Administration** > **Licenses**.
2. Select the **Installed Licenses** tab.
3. Click **Sync Now**.

   When the sync process is complete, the `Sync license with the license server successful` message is displayed. If the previously saved license data is different from the latest license data on the server, the information in the **Installed Licenses** section refreshes to reflect the latest data.

Downloading License Files

If you need to release licenses bound to an offline controller and allow those licenses to be used elsewhere (on a different controller), you can download a copy of the controller licenses. The option to download a copy of the controller licenses is only available if the controller is using the RUCKUS cloud license server.

1. Log on to the controller web interface, and then go to **Administration** > **Administration** > **Licenses**.
2. Select the **Installed Licenses** tab.
3. Click **Download**.

   The **Download License** page appears. In **Select Controller**, select the controller node for which you want to download the license files.

   > **NOTE**
   > You can upload and download license files only if the controller is using the RUCKUS cloud license server.

4. Click **Download**. Your web browser downloads the license files from the controller.
5. When the download is complete, go to the default download folder that you have configured for your web browser, and then verify that the binary copy of the license files (with .bin extension) exists.

Configuring License Bandwidth

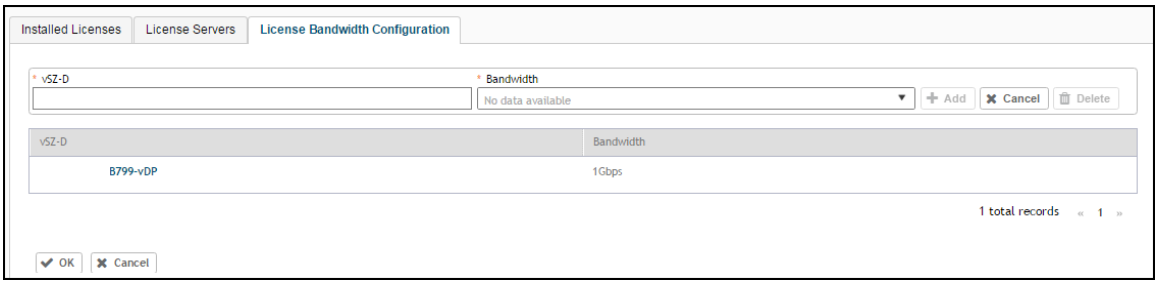
You can assign a license bandwidth for a virtual data plane provided it is already approved. Each virtual data plane can be configured with only one bandwidth license. This feature is applicable only to virtual platforms.

1. Go to **Administration** > **Administration** > **Licenses**.

2. Select the **License Bandwidth Configuration** tab.

   The **License Bandwidth Configuration** page appears.

   FIGURE 47 License Bandwidth Configuration



3. In **vSZ-D**, type the name of the virtual data plane.

   NOTE
   SZ100 and SZ144 controllers are not supported with external DPs (vSZ-D/SZ100-D/SZ144-D).

4. From the **Bandwidth** drop-down menu, select the license bandwidth you want to assign to the virtual data plane. Default is 1Gbps.
5. Click **Add**. The vSZ-D with the assigned license bandwidth is displayed.
6. Click **OK**.

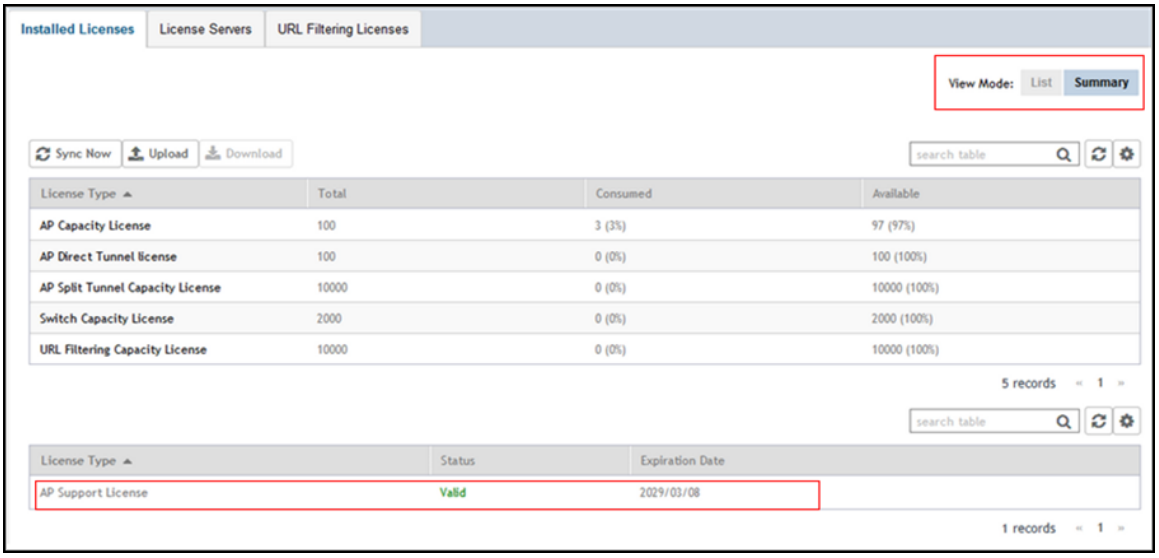
   The message `Submitting form appears`, and the vSZ-D is assigned a bandwidth.

Support AP Licensing for the Controller

In the previous controller releases, users were unable to view the AP support license information untill the controller displayed a warning message during system upgrade.

From the current release, users can view the AP support license information on the controller web user interface by navigating to **Administration**>**Administration**> **Licenses** > **Installed License** retrieved from the license server at any given point of time. To view the AP license status and validity click **View** > **Summary** tab.

FIGURE 48 Installed AP License Summary



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