CONFIGURATION GUIDE

RUCKUS SmartZone (ST-GA) Management Guide, 7.0.0

Supporting SmartZone Release 7.0.0

Part Number: 800-73367-001 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.

New In This Document

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

Feature	Description	Reference
Removal of Legacy UI Menu toggle	**Removed**: The support for this feature is removed.	Setting User Preferences on page 177
RUCKUS AI branding change	**Updated**: Reflects the branding change from RUCKUS Analytics to RUCKUS AI in the SmartZone web interface.	Configuring Cloud Services on page 111
Allowing controller to have separate Auth and Accnt servers.	**Updated**: The feature allows you to configure multiple RADIUS servers with Authentication and Accounting usages, respectively.	Configuring Switch AAA Servers on page 56
Rest API updates	**Updated**: Test environment use case added to determine the rest API support rates for read and write operations.	Rest API on page 171

Authentication

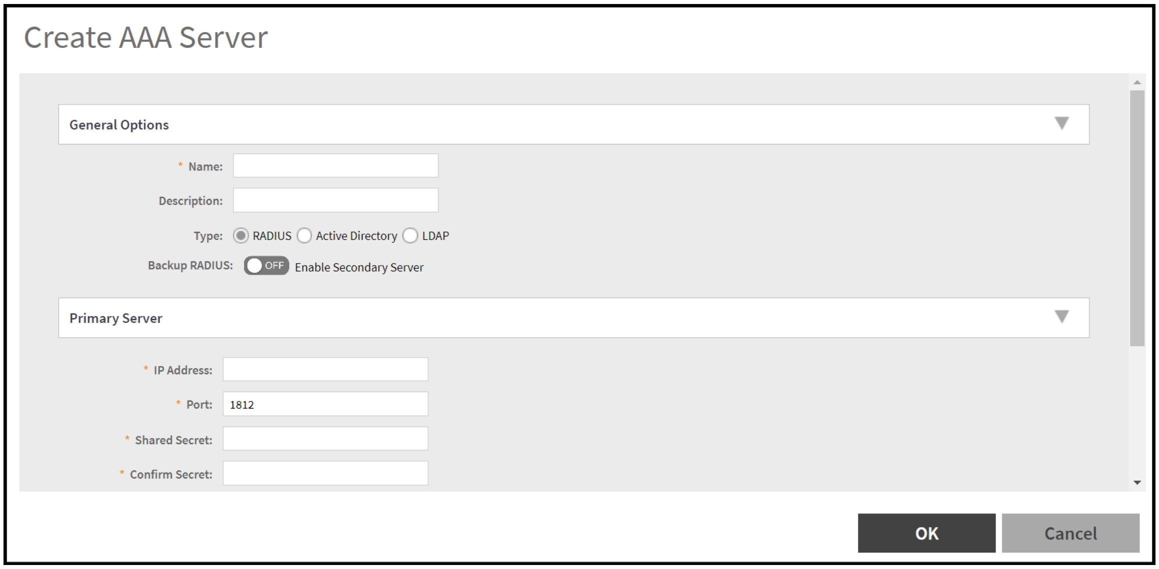
Creating Non-Proxy Authentication AAA Server

A non-proxy AAA server is used when APs connect to the external AAA server directly.

1. Go to **Security** > **Authentication** > **Non-Proxy (AP Authenticator)**.
2. Select a Zone from the system tree and click **Create**.

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

   FIGURE 1 Create AAA Server



Create AAA Server

General Options

* Name:

Description:

Type: ● RADIUS ○ Active Directory ○ LDAP

Backup RADIUS: OFF Enable Secondary Server

Primary Server

* IP Address:

* Port: 1812

* Shared Secret:

* Confirm Secret:

3. Configure the following options:
   - General Options
     - Name: Name the AAA server that you are creating.
     - Description: Short description of the AAA server.
     - Type: Select the type of AAA server that you are creating. Options include **RADIUS**, **Active Directory** and **LDAP**.
     - Backup RADIUS : If secondary RADIUS server exists on the network then only toggle the button to ON to enable the **Secondary Server** option.
   - Primary Server
     - If you select the type as **RADIUS**, configure the following options:
       - IP Address: The IP address of the AAA server. Both IPv4 and IPv6 addressing formats are supported.
       - Port: The port number of the AAA server. The default RADIUS server port number is 1812.
       - Shared Secret: The AAA shared secret.
       - Confirm Secret: Re-enter the shared secret to confirm.

       If you have enabled the secondary server for Backup RADIUS, you must provide similar information as in the primary server.
     - If you select the type as **Active Directory**, configure the following options:
       - IP Address: Enter the IPv4 address of the Active Directory server.
       - Port: Enter the port number of the Active Directory server. The default port number (389) must not be changed unless you have configured the Active Directory server to use a different port.
       - Windows Domain Name: Enter the Windows domain name assigned to the Active Directory server (for example, domain.ruckuswireless.com).
     - If you select the type as **LDAP**, configure the following options:
       - IP Address: Enter the IPv4 address of the LDAP server.
       - Port: Enter the port number of the LDAP server. The default port number is 389.
       - Base Domain Name: Enter the base domain name in LDAP format for all user accounts (for example, dc=ldap,dc=com).
       - Admin Domain Name: Enter the administrator domain name in LDAP format (for example, cn=Admin;dc=*Your Domain*,dc=com).
       - Admin Password: Enter the administrator password for the LDAP server.
       - Confirm Password: Re-enter the administrator password to confirm.
       - Key Attribute: Enter a key attribute to denote users (for example, default: uid)
       - Search Filter: Enter a search filter (for example, objectClass=Person).
4. Under **User Role Mapping**,

   NOTE
   While mapping group attribute value to a user role, avoid special characters, wild-card entries, or duplicate entries regardless of the order. Only the first-matched entry will be mapped to the user role.

   a) **Click** + **Create**. The Create User traffic Profile Mapping dialog box is displayed

   b) In the **Group Attribute Value** field, enter the value to be sent from AAA as part of an Access-Accept.

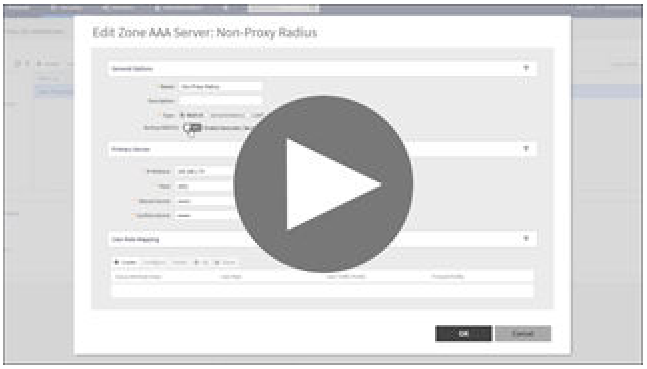
   c) Click **OK**

   d) Select a user role from the **User Role** list or click **+** to create a user role. For more information, refer to *User Roles* in *User Management Guide*.
5. Click **OK**.

   NOTE
   You can also edit, clone and delete an AAA server by selecting the options **Configure**, **Clone**, and **Delete**, respectively, from the **Non-Proxy (AP Authenticator)** tab.

VIDEO

Non-Proxy AAA Configuration. Creating a Proxy or Non-Proxy Authentication service



Edit Zone AAA Server: Non-Proxy Radius

Click to play video in full screen mode.

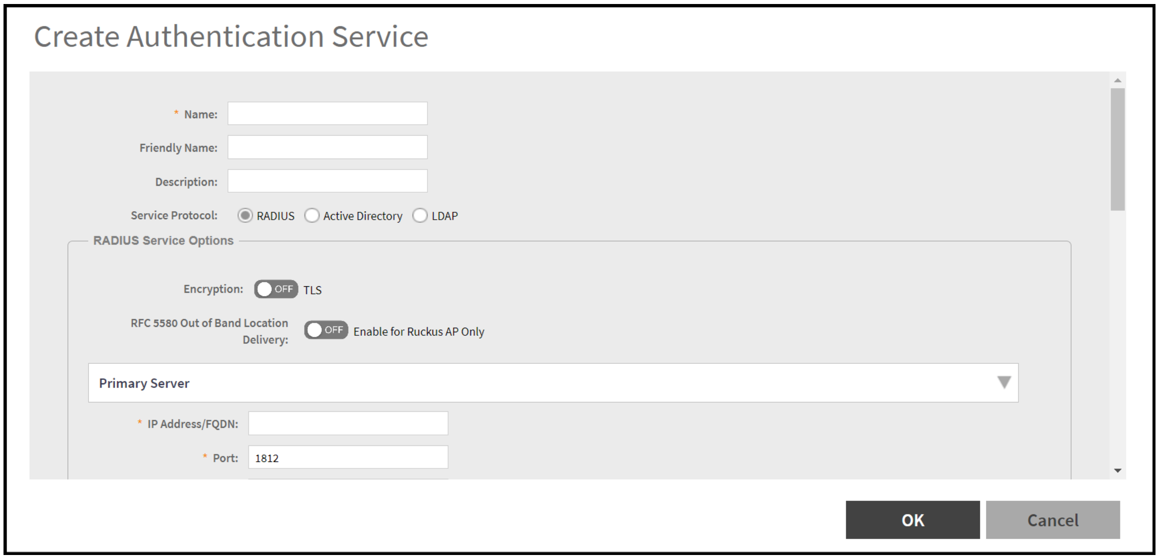
Creating Proxy Authentication AAA Servers

A proxy AAA server is used when APs send authentication or accounting messages to the controller and the controller forwards these messages to an external AAA server.

1. Select **Security** > **Authentication** > **Proxy (SZ Authenticator)**.
2. Select a Zone from the system tree and click **Create**.

   The **Create Authentication Service** is displayed.

   FIGURE 2 Creating an Authentication Service



Create Authentication Service

* Name:

Friendly Name:

Description:

Service Protocol: ● RADIUS ○ Active Directory ○ LDAP

RADIUS Service Options

Encryption: OFF TLS

RFC 5580 Out of Band Location Delivery: OFF Enable for Ruckus AP Only

Primary Server

* IP Address/FQDN:

* Port: 1812

3. Configure the following options:

- Name: Enter a name for the authentication service that you are adding.
- Friendly Name: Enter an alternative name that is easy to remember.
- Description: Enter a description for the authentication service.
- Service Protocol: Select the type of service protocol for the authentication service you are adding. Options are **RADIUS**, **Active Directory**, and **LDAP**.
  - If you select **RADIUS**, refer to RADIUS Service Options on page 17 for more information.
  - If you select **Active Directory**, configure the following options:
    - Global Catalog: Select the **Enable Global Catalog** support if you want the Active Directory server to provide a global list of all objects.
    - Primary Server: For Encryption, select the **Enable TLS Encryption** check box if you want to use the Transport Layer Security (TLS) protocol to secure communication with the server.

      NOTE
      You must also configure the Trusted CA certificates to support TLS encryption.

    - IP Address: Enter the IPv4 address of the Active Directory server.
    - Port: Enter the port number of the Active Directory server. The default port number (389) must not be changed unless you have configured the Active Directory server to use a different port.
    - Windows Domain Name: Enter the Windows domain name assigned to the Active Directory server (for example, domain.ruckuswireless.com).
  - If you select **LDAP**, configure the following options:

    a. Select **Enable TLS Encryption** check box, if you want to use the Transport Layer Security (TLS) protocol to secure communication with the server.

       NOTE
       You must also configure the Trusted CA certificates to support TLS encryption.

    b. IP Address: Enter the IPv4 address of the LDAP server.

    c. Port: Enter the port number of the LDAP server.

    d. Base Domain Name: Enter the base domain name in LDAP format for all user accounts (for example, dc=ldap,dc=com).

    e. Admin Domain Name: Enter the administrator domain name in LDAP format (for example, cn=Admin;dc=*Your Domain*,dc=com).

    f. Admin Password: Enter the administrator password for the LDAP server.

    g. Confirm Password: Re-enter the administrator password to confirm.

    h. Key Attribute: Enter a key attribute to denote users (for example, default: uid).

    i. Search Filter: Enter a search filter (for example, objectClass=Person).
- User Role Mapping:

  NOTE
  While mapping group attribute value to a user role, avoid special characters, wild-card entries, or duplicate entries regardless of the order. Only the firs-matched entry will be mapped to the user role.

  a. Click +Create. The Create User traffic Profile Mapping dialog box is displayed.

  b. In the **Group Attribute Value** field, enter the value to be sent from AAA as part of an Access-Accept.

c. Select a **User Role** from the list or click + to create a new user role. For more information, refer to **User Roles** in the *RUCKUS SmartZone User Management Guide*.

d. Click **OK**.

The mapped user profile is listed.

4. Click **OK**.

NOTE
You can also edit, copy, and delete an AAA server by selecting the options **Configure**, **Clone**, and **Delete**, respectively, from the **Proxy (SZ Authenticator)** tab.

RADIUS Service Options

These are the Radius service options available for the primary and secondary servers.

RFC 5580 Out of Band Location Delivery: If you want out-of-band location delivery (RFC 5580) to apply only to RUCKUS APs, select the **Enable for Ruckus AP Only** check box.

Configure the primary RADIUS server settings as shown in the following table.

TABLE 3 Primary Server Options

Option	Description
IP Address or FQDN	Type the IP address or the Fully Qualified Domain Name (FQDN) of the RADIUS server. IPv4 and IPv6 addressing formats are supported.
Port	Type the port number of the RADIUS server. The default RADIUS server port number is 1812 and the default RADIUS Accounting server port number is 1813.
Shared Secret	Type the RADIUS shared secret.
Confirm Secret	Retype the shared secret to confirm.

If you have a secondary RADIUS server on the network that you want to use as a backup, select the Enable Secondary Server check box, and then configure the settings in the following table.

TABLE 4 Secondary Server Options

Option	Description
Backup RADIUS	Select **Enable Secondary Server**. When a secondary RADIUS server is enabled and the primary RADIUS server becomes unavailable, the secondary Automatic Fallback Disable server takes over the handling of RADIUS requests. When the primary server becomes available again, it takes back control over RADIUS requests from the secondary server. If you want to prevent the primary server from retaking control over RADIUS requests from the secondary server, select the **Automatic Fallback Disable** check box.
IP Address	Type the IP address of the secondary AAA server. IPv4 and IPv6 addressing formats are supported.
Port	Type the port number of the secondary AAA server port number. The default RADIUS server port number is 1812 and the default RADIUS Accounting server port number is 1813.
Shared Secret	Type the AAA shared secret.
Confirm Secret	Retype the shared secret to confirm.

The following options define the health monitoring settings of the primary and secondary RADIUS servers, when the controller is configured as RADIUS proxy for RADIUS Authentication and Accounting messages.

TABLE 5 Health Check Policy

Option	Description
Response Window	Set the time (in seconds) after which, if the AAA server does not respond to a request, the controller will initiate the zombie period (see below). Response Window If the primary AAA server does not respond to RADIUS messages sent after Response Window expires, the controller will forward the retransmitted RADIUS messages to the secondary AAA server. **NOTE** The zombie period is not started immediately after the Response Window expires, but after the configured Response Window plus ¼ of the configured Zombie Period. The default Response Window is 20 seconds
Zombie Period	Set the time (in seconds) after which, if the AAA server does not respond to ANY packets during the zombie period, it will be considered to inactive or unreachable. An AAA server that is marked zombie (inactive or unreachable) will be used to proxy with a low priority. If there are other live AAA servers, the controller will attempt to use these servers first instead of the zombie AAA server. The controller will only proxy requests to a zombie server only when there are no other live servers. Any request that is sent as a proxy to an AAA server will continue to be sent to that AAA server until the home server is marked inactive or unreachable. At that point, the request will fail over to another server, if a live AAA server is available. The default Zombie Period is 40 seconds.
Revive Interval	Set the time (in seconds) after which, if no RADIUS messages are sent as proxy to the AAA server after it has been marked as inactive or unreachable, the controller will mark the AAA server as active again (and assume that it has become reachable again). The default Revive Interval is 120 seconds.
No Response Fail	Click **Yes** to respond with a reject message to the NAS if no response is received from the RADIUS server. Click **No** to skip sending a response.

NOTE
To ensure that the RADIUS fail-over mechanism functions correctly, either accept the default values for the Response Window, Zombie Period, and Revive Interval, or make sure that the value for Response Window is always higher than the value for RADIUS NAS request timeout multiplied by the value for RADIUS NAS max number of retries. For third party APs, you must ensure that the configured Response Window on the controller is higher than the RADIUS NAS request timeout multiplied by the RADIUS value. The maximum number of retries is configured at the 3rd party controller/AP.

Configure the following options.

TABLE 6 Rate Limiting

Options	Description
Maximum Outstanding Requests (MOR)	Set the maximum outstanding requests per server. Type 0 to disable it, or set a value between 10 and 4096.
Threshold (% of MOR)	Set a percentage value of the MOR at which (when reached) the controller will generate an event. Threshold (% of MOR) For example, if the MOR is set to 1000 and the threshold is set to 50%, the controller will generate an event when the number of outstanding requests reaches 500.

TABLE 6 Rate Limiting (continued)

Options	Description
Sanity Timer	Set a timer (in seconds) that will be started whenever a condition that generates an event is reached. This helps prevent conditions that trigger events which occur frequently.

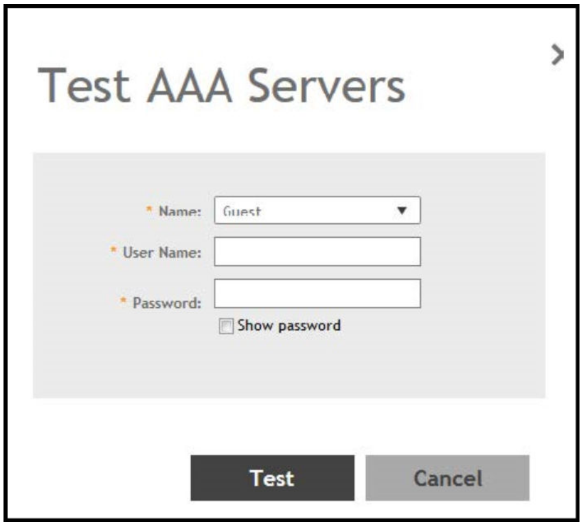
Testing AAA Servers

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

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

   The **Test AAA Server** page appears.

   FIGURE 3 Testing an AAA Server



Test AAA Servers

* Name: Guest

* User Name:

* Password:

□ Show password

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

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

Authentication Support Matrix

It is important to understand the compatibility between AAA servers and different WLANs.

Proxy Mode

In proxy mode, authentication requests are set through the controller.

TABLE 7 Proxy Mode Compatibility

Authentication Source	802.1X	HS 2.0 Secure	Web Auth	Hotspot/WISPr
Local Database	Yes	Yes	No	Yes
IDM-Provisioned Local DB	Yes	Yes	NA	NA
Active Directory	No*	No	Yes	Yes
RADIUS	Yes	Yes	Yes	Yes
LDAP	Yes	No	Yes	Yes

NOTE
To support 802.1X with Active Directory, an external RADIUS server (such as NPS) must be used.

NOTE
IDM Provisioned username (also called local cache credential) is relevant only in secure access after Onboarding.

NOTE
802.1X (MSCHAPv2 via built-in RADIUS using AD-NPS), WebAuth, and WISPr support AD authentication from SmartZone release in 3.2.

NOTE
802.1X, WebAuth, and WISPr support LDAP authentication from SmartZone release in 3.2. For 802.1X authentication, the user password must be in clear text in the LDAP database.

Non-proxy Mode

In the Non-proxy mode, authentication requests are sent directly by AP and not through the controller. The local database is stored on the controller, therefore, authentication sources such as local database and IDM-provisioned local databases are not supported.

TABLE 8 Non-proxy Mode Compatibility

Authentication Source	802.1X	Zero-IT Onboard	HS 2.0 Onboard	HS 2.0 Secure	Web Auth	Hotspot/WISPr
Active Directory	No	No*	No*	No	Yes	No
RADIUS	Yes	No*	No*	No	Yes	Yes*
LDAP	No	No*	No*	No	Yes	No

(*) From the configuration it may seem like non-proxy RADIUS is supported in WISPr, but the call flow goes through the controller.

Profile Configuration

The following table details proxy and non-proxy AAA server configurations against various platforms.

TABLE 9 Profile Configuration

Feature	SZ100	vSZ-E	vSZ-H	Description
Per-Zone ProxyAAA Profiles	NA	NA	NA	Ability to configure a ProxyAAA profile in a specific zone

TABLE 9 Profile Configuration (continued)

Feature	SZ100	vSZ-E	vSZ-H	Description
Global ProxyAAA Profiles	Yes	Yes	Yes	Ability to configure a ProxyAAA profile globally and then use it across zones
Per-Zone NonProxy AAA Profiles	NA	NA	Yes	Ability to configure a Non ProxyAAA profile in a specific zone
Global NonProxy AAA Profiles	Yes	Yes	No	Ability to configure a Non Proxy AAA profile globally and then use it across zones

Dynamic Policy Assignment (Proxy Authentication Types)

The following table details dynamic policy assignments across authentication types.

TABLE 10 Dynamic Policy Assignment (Proxy)

Feature	802.1X	Zero-IT Onboard	HS 2.0 Onboard	HS 2.0 Secure	Web Auth	Hotspot/WISPr	MAC Auth	Description
Dynamic Role Assignment	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Ability to assign a user to a particular local role via a group/role attribute from RADIUS, AD, LDAP. From SmartZone 3.4, Role can contain UTP. Therefore,when you assign a role, you also get the ACL and Rate Limiting policies.
Dynamic VLAN / VLAN Pool	Yes	NA	NA	NA	No	No	Yes	Ability to assign a user to a VLAN through a VLAN attribute from RADIUS, AD, LDAP. From SmartZone release 3.5, you can also assign VLANs and VLAN pools based on the user role.
Dynamic UTP	Yes				Yes	Yes	Yes	Ability to assign a user to a UTP through an attribute from an authentication source.
Dynamic ACL	Yes	Yes	Yes	No	Yes	Yes	Yes	Ability to assign a specific ACL to a user through an attribute from RADIUS, AD, LDAP.

TABLE 10 Dynamic Policy Assignment (Proxy) (continued)

Feature	802.1X	Zero-IT Onboard	HS 2.0 Onboard	HS 2.0 Secure	Web Auth	Hotspot/WISPr	MAC Auth	Description
Dynamic Rate Limit	Yes	Yes	Yes			Yes	Yes	Ability to assign a specific Rate Limit to a user through an attribute from RADIUS, AD, LDAP.

NOTE
In dynamic ACL and Rate limit, since ACL and rate limit are associated with a UTP, assigning a UTP also assigns an ACL or rate limit.

Dynamic Policy Assignment (Non-Proxy Authentication Types)

The following table details dynamic policy assignments across authentication types.

TABLE 11 Dynamic Policy Assignment (Non-Proxy)

Feature	802.1X	HS 2.0 Secure	Web Auth	Description
Dynamic Role Assignment	No			Ability to assign a user to a local role through a group/role attribute from the authentication source.
Dynamic VLAN / VLAN Pool				Ability to assign a user to a VLAN through a VLAN attribute from the authentication source.
Dynamic UTP				Ability to assign a user to a UTP through an attribute from the authentication source. **NOTE** From SmartZone release 3.4, UTP contains ACL and rate limit.
Dynamic ACL				Ability to assign a specific ACL to a user through an attribute from the authentication source. **NOTE** ACLs are a part of a UTP. If you configure a UTP without a rate limit,you effectively only have an ACL.
Dynamic Rate Limit				Ability to assign a specific Rate Limit to a user through an attribute from the authentication source. **NOTE** Rate limiting is also a part of a UTP. If you configure a UTP without ACL, you effectively only have a rate limiting policy.

Other Authentication Features

The following table details authentication support for various authentication features.

TABLE 12 Authentication Features

Feature	Supported	Description
Test AAA - RADIUS	Yes	Ability to test a specific username/password against a configured RADIUS server.
Test AAA - Active Directory	Yes	Ability to test a specific username/password against a configured AD server.
Test AAA - LDAP	Yes	Ability to test a specific username/password against a configured LDAP server. **NOTE** Only Non-Proxy LDAP is supported at the Zone Level.
Test AAA - Return a Role	Yes - supported by RADIUS, AD and LDAP	Ability to return a role assignment when testing a AAA server.
RADIUS CoA - Change Role		Ability to change a user's Role through a Change of Authorization (CoA).
RADIUS CoA - Change VLAN		Ability to change a user's VLAN through a Change of Authorization (CoA).
RADIUS CoA - Change ACL		Ability to change a user's ACL through a Change of Authorization (CoA).
RADIUS CoA - Change Rate Limit		Ability to change a user's rate limit through a Change of Authorization (CoA).
RADIUS CoA - Change Authorization		Ability to authorize or deauthorize a user through a Change of Authorization (CoA). **NOTE** The controller does not provide support for CoA or DM in non-proxy mode.

PAP/CHAP Support

The following table details PAP and CHAP support for various authentication features.

TABLE 13 PAP/CHAP Support

Feature	802.1X	Web Auth	Hotspot/ WISPr	MAC Auth	Notes
Proxy-Mode					
Active Directory	Yes	Yes*	Yes	No	PAP / CHAP is supported for Web Authentication and HotSpot/WISPr. NPS interface (AD) is required for WebAuthenticaiton (CHAP) and 802.1X (MSCHAPv2).
RADIUS	Yes	Yes*	Yes	Yes	
LDAP	Yes	Yes*	Yes	No	PAP / CHAP is supported for Web Authentication and HotSpot/WISPr

TABLE 13 PAP/CHAP Support (continued)

Feature	802.1X	Web Auth	Hotspot/ WISPr	MAC Auth	Notes
LDAP-TLS	Yes	Yes*	Yes	No	This support is available from SmartZone version 3.5.
Active Directory (TLS)	Yes	Yes*	Yes	No	This support is available from SmartZone version 3.5. NPS interface (AD) is required for WebAuthenticaiton (CHAP) and 802.1X (MSCHAPv2).
Non-proxy Mode					
Active Directory	No	Yes*	Yes	No	
RADIUS	Yes	Yes*	Yes	Yes	
LDAP	No	Yes*	Yes	No	

NOTE
(*) This is an AP CLI setting:

```
set aaa auth-method pap|chap
```

It is a global setting for all WebAuth WLANs on the AP. The default is CHAP.

Non-Proxy (Social Login)

To configure social media profile for a user, use client ID and client secret options. Social media login can be activated by turing **On** the Social Media enable button.

Creating Social Media Login Profile

When end-user associated with an OAuth 2.0 WLAN, launches his browser. AP redirects it to the OAuth 2.0 provider login page. The end-user should enter his account and password to authenticate with OAuth 2.0 provider. AP sets the end-user status as authenticated and user is able to use internet.

To configure social media authentication configuration, perform the following:

1. Go to **Security** > **Authentication** > **Non-Proxy (Social Login)**.

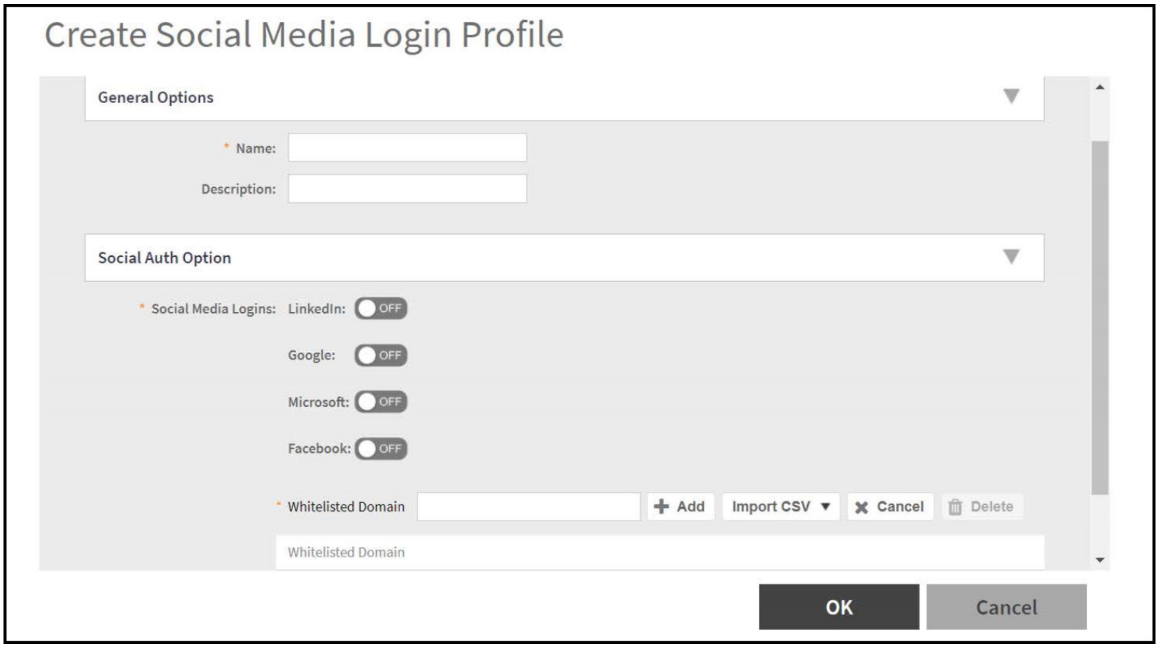
   This displays the zones associated with the Non-Proxy (Social Login).
2. In the **Non-Proxy (Social Login)** screen, select a **Zone** and click **Create**.

   This displays **Create Social Media Login Profile** page.
3. Enter the values in **General Options** and enable the **Social Auth Option** tabs.
4. After you have enabled the **Social Media Logins** it is mandatory to provide the client ID/Secret. If you don't have one, click on the hyperlink provided in **Create Social Media Login Profile** screen to generate a and for particular social media website.

5. Add domains to the **Whitelisted Domain** field by entering the domain name. For example,
   - LinkedIn - *.licdn.com, *.linkedin.com
   - Google - *.geotrust.com, *.gstatic.com
   - Facebook - *.facebook.com, *.fbcdn-profile-a.akamaihd.net, *.fstatic-a.akamaihd.net
   - Microsoft - *.geotrust.com, *.live.com, *.microsoftonline.com, *.auth.gfx.ms, *.msauth.net

   NOTE
   Microsoft based Social media authentication do not support corporate accounts, but personnel email account.

FIGURE 4 Create Social Media Login Profile



Create Social Media Login Profile

General Options

* Name:

Description:

Social Auth Option

* Social Media Logins: LinkedIn: OFF

Google: OFF

Microsoft: OFF

Facebook: OFF

* Whitelisted Domain

Creating Realm Based Authentication Profile

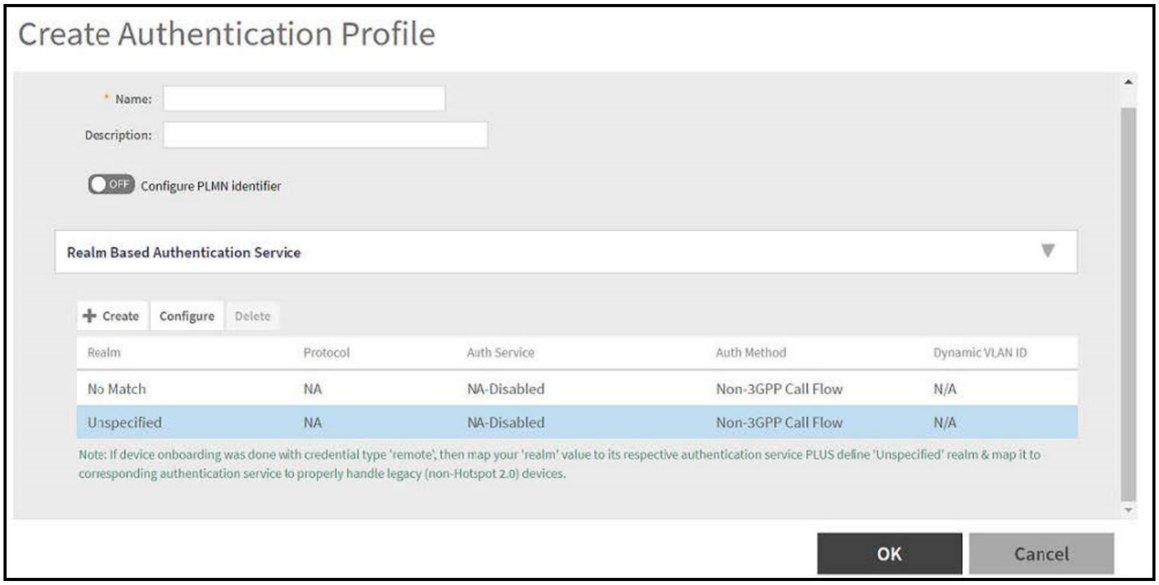
An authentication profile defines the authentication policy when the controller is used as a Radius proxy service for WLANs.

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

2. Click **Create**.

   This displays **Create Authentication Profile** page.

   FIGURE 5 Creating a Realm Based Proxy Authentication Profile



Create Authentication Profile

* Name:

Description:

OFF Configure PLMN identifier

Realm Based Authentication Service

Realm	Protocol	Auth Service	Auth Method	Dynamic VLAN ID
No Match	NA	NA-Disabled	Non-3GPP Call Flow	N/A
Unspecified	NA	NA-Disabled	Non-3GPP Call Flow	N/A

Note: If device onboarding was done with credential type 'remote', then map your 'realm' value to its respective authentication service PLUS define 'Unspecified' realm & map it to corresponding authentication service to properly handle legacy (non-Hotspot 2.0) devices.

3. Configure the following:
   a. Name: Type a name for the authentication service profile that you are creating.
   b. Description: Type a short description of the authentication service profile.
   c. Realm-Based Authentication Service
      - Realm: Type wthere the realm is No Match or Unspecified.
      - Protocol: Displays the type of protocol.
      - Auth Service: Select a default authentication service for the realm.
      - Auth Method: Select an authorization method as 3GPP or Non-3GPP call flow.
      - Dynamic VLAN ID: Type the vlan ID.
   d. Redirect to the URL that the user intends to visit: Allows the guest user to continue to their destination without redirection.
      - Redirect to the following URL: Redirect the user to a specified web page (entered into the text box) prior to forwarding them to their destination. When guest users land on this page, they are shown the expiration time for their guest pass.
4. Click **OK**.

Fast Initial Link Setup (FILS)

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

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

- 802.1x(FILS) + WISPr

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

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

Create Fast Initial Link Setup (FILS) Realm Profile

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

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

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

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

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

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

Accounting

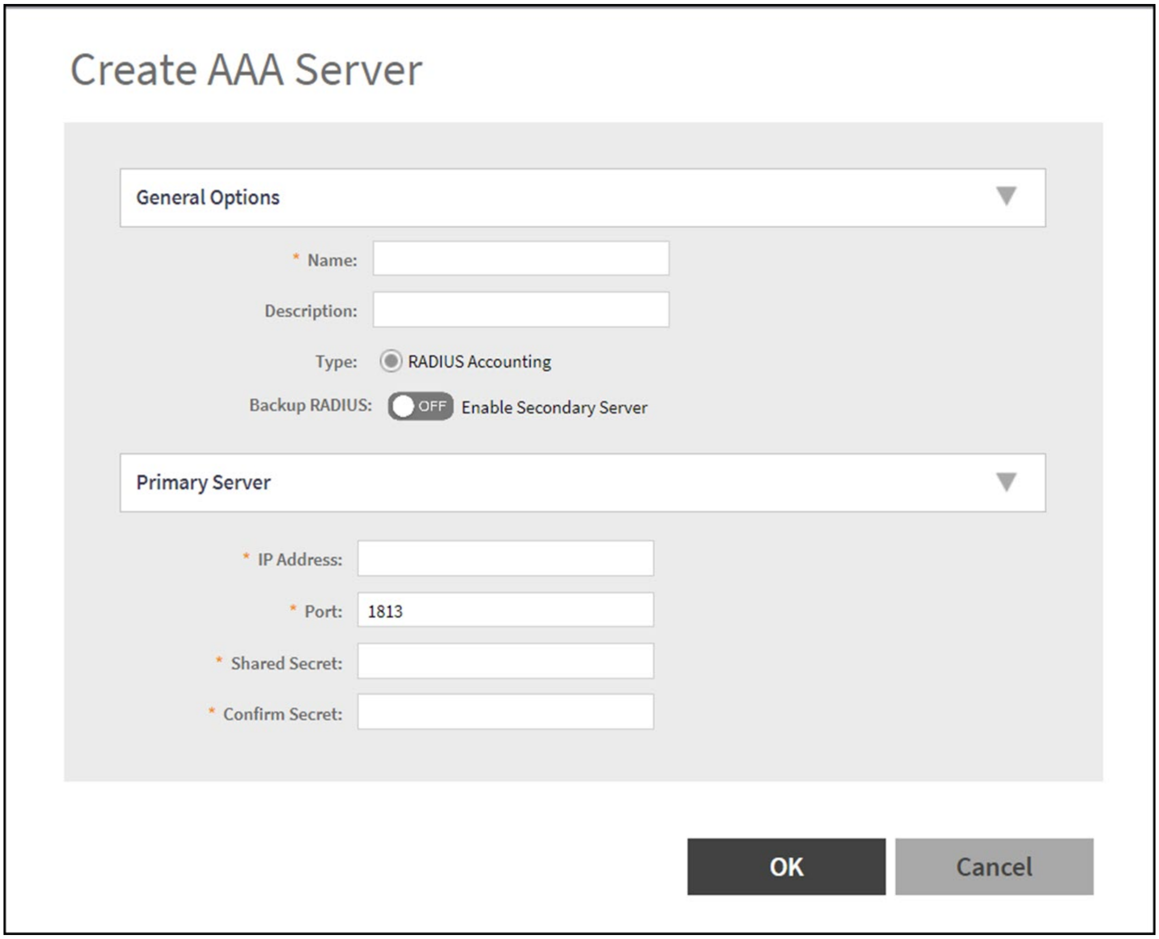
Creating Non-Proxy Accounting AAA Servers

A non proxy AAA server is used when the APs connect to the external AAA server directly.

1. Go to **Security** > **Accounting** > **Non-Proxy**.
2. Select a **Zone** and click **Create**.

   The **Create AAA Server** page appears.

FIGURE 6 Creating an AAA Server



Create AAA Server

General Options

* Name:

Description:

Type: ● RADIUS Accounting

Backup RADIUS: OFF Enable Secondary Server

Primary Server

* IP Address:

* Port: 1813

* Shared Secret:

* Confirm Secret:

3. Configure the following:

   a. General Options

   - Name: Type a name for the AAA server that you are creating.
   - Description: Type a short description of the AAA server.
   - Type: By default, the **RADIUS Accounting** option is selected.

     NOTE
     RFC-5580 is used to convey access-network ownership and location information based on the civic and geospatial location formats in RADIUS protocol.

   - Cluster Redundancy: Click the **Enable Service for Standby Cluster** option to enable cluster redundancy.

     NOTE
     Cluster Redundancy option is available only when this functionality is enabled in cluster configuration.

   - Backup RADIUS (appears if you clicked RADIUS above): Click the **Enable Secondary Server** check box if a secondary RADIUS server exists on the network.

   b. If you selected RADIUS, configure the following options in the Primary and Secondary server sections:

   - IP Address: Type the IP address of the AAA server.
   - Port: Type the port number of the AAA server. The default RADIUS server port number is 1813.
   - Shared Secret: Type the AAA shared secret.
   - Confirm Secret: Retype the shared secret to confirm.

4. Click **OK**.

You have completed creating a Non-proxy Accounting AAA server.

> **NOTE**
> You can also edit, clone and delete an AAA server by selecting the options **Configure**, **Clone** and **Delete** respectively, from the **Non-Proxy** tab.

Creating Proxy Accounting AAA Servers

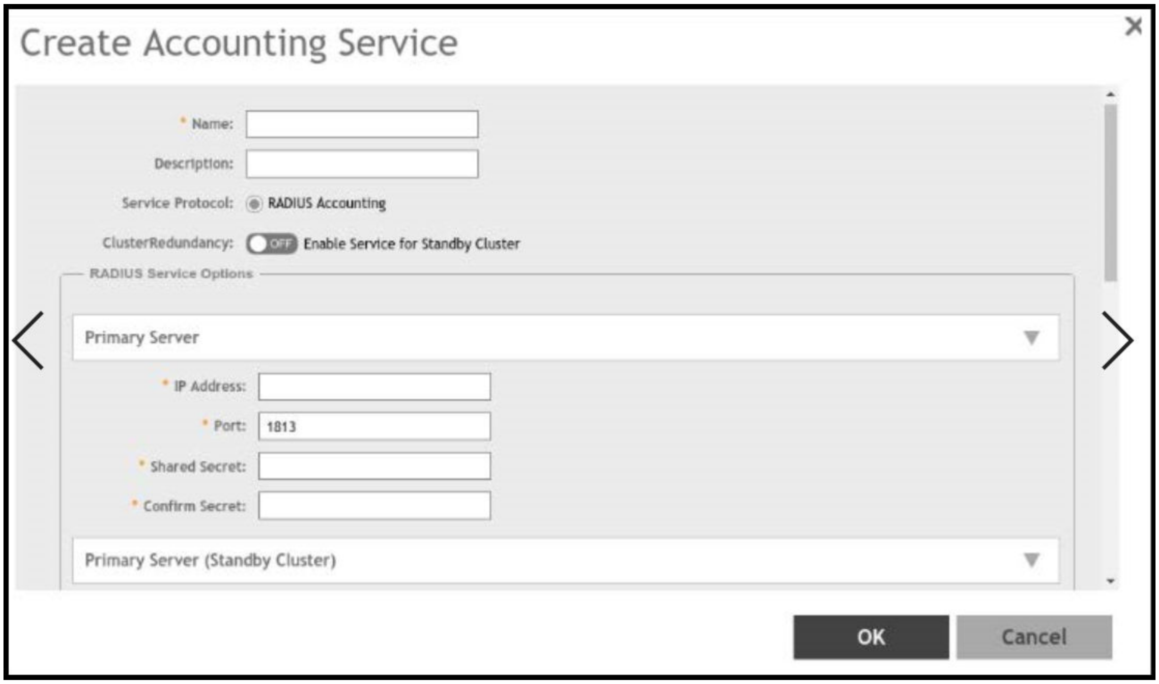
A proxy AAA server is used when APs send authentication/accounting messages to the controller and the controller forwards these messages to an external AAA server.

1. Select **Security** > **Accounting** > **Proxy**.

2. Select a Zone from the system tree and click **Create**.

   The **Create Accounting Service** page appears.

   FIGURE 7 Creating an Accounting Service



Create Accounting Service

* Name:

Description:

Service Protocol: ● RADIUS Accounting

ClusterRedundancy: OFF Enable Service for Standby Cluster

RADIUS Service Options

Primary Server ▼

* IP Address:

* Port: 1813

* Shared Secret:

* Confirm Secret:

Primary Server (Standby Cluster) ▼

3. Configure the following:

   a. Name: Type a name for the authentication service that you are adding.

   b. Description: Type a description for the authentication service.

   c. Service Protocol: By default, the RADIUS Accounting is selected. For more information, see RADIUS Service Options on page 17.

      NOTE
      RFC-5580 is used to convey access-network ownership and location information based on the civic and geospatial location formats in RADIUS protocol.

   d. Cluster Redundancy: Click the **Enable Service for Standby Cluster** option to enable cluster redundancy.

      NOTE
      Cluster Redundancy option is available only when this functionality is enabled in cluster configuration.

4. Click **OK**.

You have completed creating a Proxy Accounting AAA server.

NOTE
You can also edit, clone and delete an AAA server by selecting the options **Configure**, **Clone** and **Delete** respectively, from the **Proxy** tab.

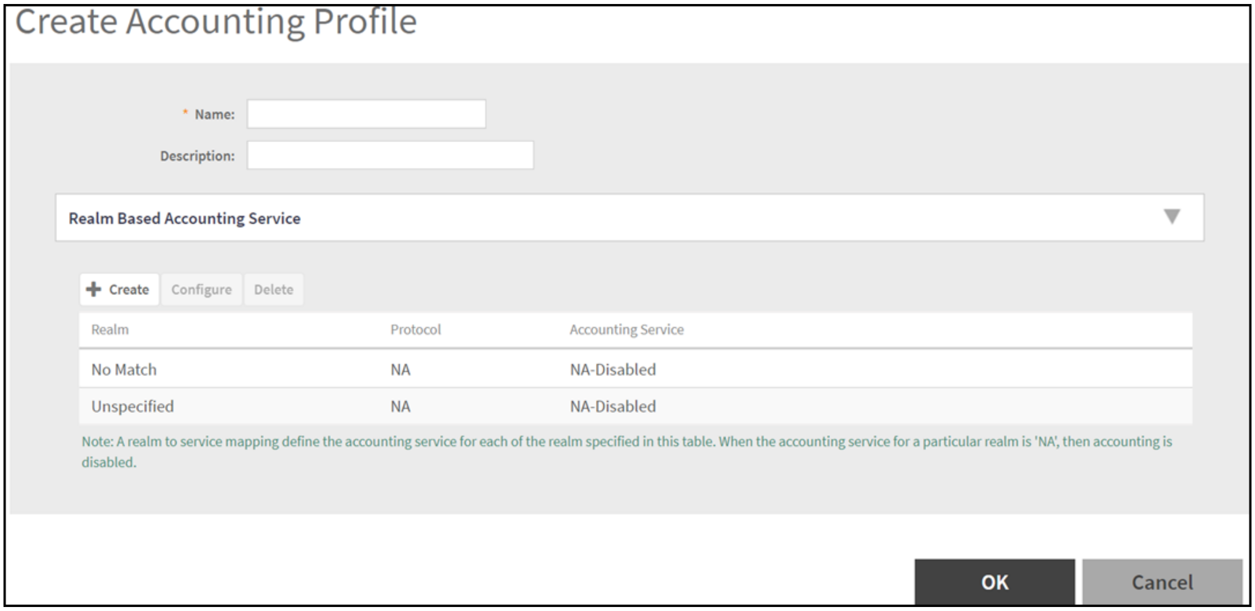
Creating Realm Based Proxy

An accounting profile defines the accounting policy when the controller is used as a RADIUS proxy for WLAN services.

1. Go to **Security** > **Access Control** > **Accounting** > **Realm Based Proxy**.
2. Click **Create**.

   The **Create Accounting Profile** page appears.

   FIGURE 8 Creating an Accounting Profile



Create Accounting Profile

* Name:

Description:

Realm Based Accounting Service

Realm	Protocol	Accounting Service
No Match	NA	NA-Disabled
Unspecified	NA	NA-Disabled

Note: A realm to service mapping define the accounting service for each of the realm specified in this table. When the accounting service for a particular realm is 'NA', then accounting is disabled.

3. Configure the following:
   a. Name: Type a name for the authentication service that you are adding.
   b. Description: Type a description for the authentication service.
   c. Accounting Service per Realm: Specify the accounting service for each of the realms specified in this table. If you set the accounting service for a particular realm to NA-Disabled, then the accounting request is rejected. To create a new service click, **Create** and then configure **Realm** and **Accounting Service**.

      NOTE
      RFC-5580 is used to convey access-network ownership and location information based on the civic and geospatial location formats in RADIUS protocol.

4. Click **OK**.

You have completed creating a Realm-based proxy Accounting AAA server.

NOTE
You can also edit, clone and delete an AAA server by selecting the options **Configure**, **Clone** and **Delete** respectively, from the **Realm Based Proxy** tab.

ECDSA

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

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

The SmartZone provides an option to disable/enable the ECDSA certification on a per-zone basis. The APs in the zone with ECDSA certificate enabled receives an additional controller-signed certificate from the SmartZone. This is called the 3K certificate. The 2K MIC (Manufacturer Installed Certificates) on the APs is still used as the trust anchor for the SmartZone. The 2K MIC and corresponding key (2k length) remains untouched, backward compatibility of the zone only allows 2K certificate/key.

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

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

Cloud Computing Compliance Criteria Catalogue - BSI C5

The C5 catalogue specifies minimum requirements for secure cloud computing.

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

The following are the secure features in AP and SmartZone:

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

Configuring ECDSA and Keys at Zone Level

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

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

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

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

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

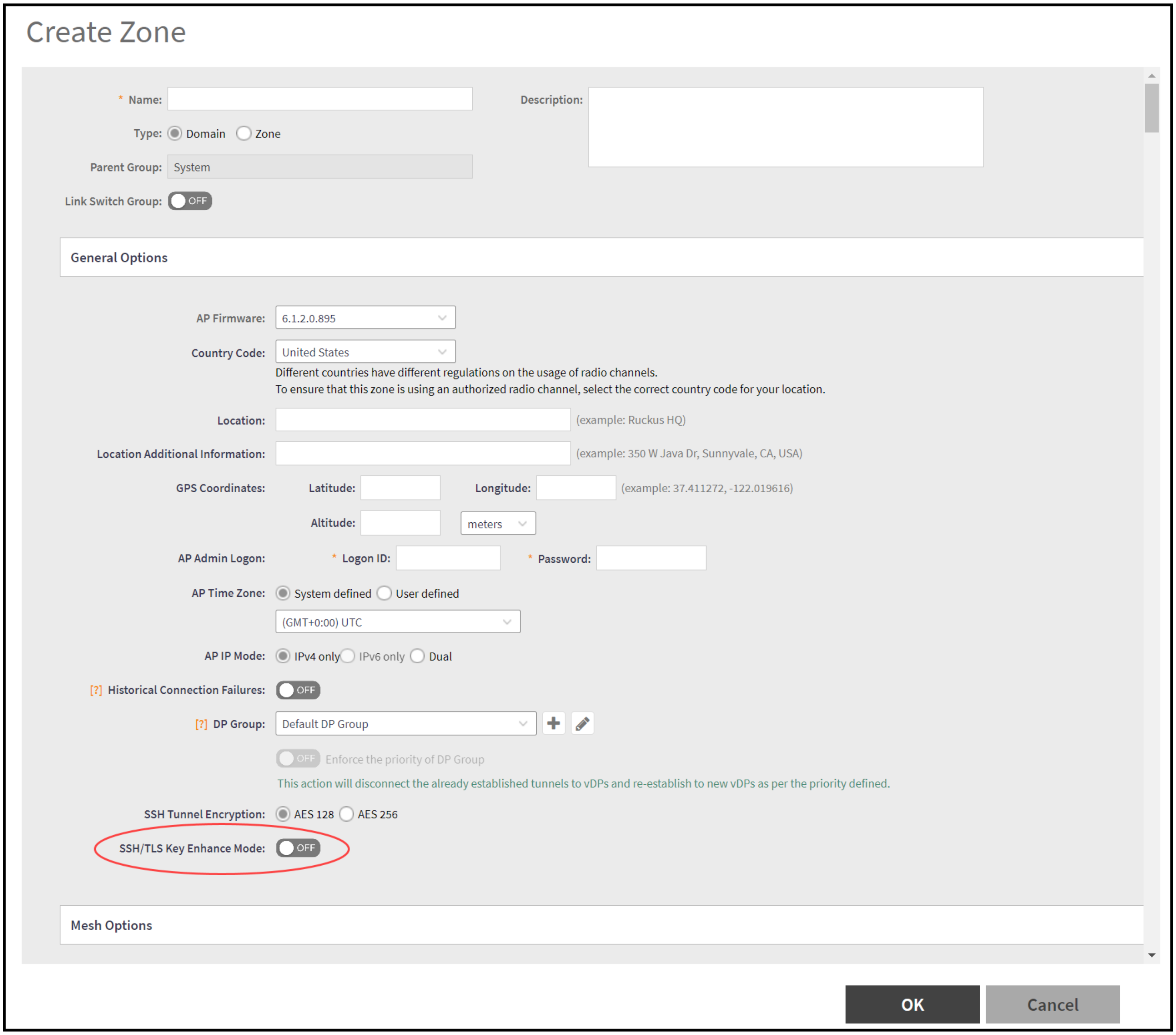
   This displays the **Access Points** page.

2. In the system tree, click **Create Domain/Zone/Group (+)** icon.

   This displays the **Create Zone** page.

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

FIGURE 9 SSH/TLS Key Enhance Mode



Create Zone

* Name:
Description:
Type: ● Domain ○ Zone
Parent Group: System
Link Switch Group: OFF

General Options

AP Firmware: 6.1.2.0.895
Country Code: United States
Different countries have different regulations on the usage of radio channels.
To ensure that this zone is using an authorized radio channel, select the correct country code for your location.
Location: (example: Ruckus HQ)
Location Additional Information: (example: 350 W Java Dr, Sunnyvale, CA, USA)
GPS Coordinates: Latitude: Longitude: (example: 37.411272, -122.019616)
Altitude: meters
AP Admin Logon: * Logon ID: * Password:
AP Time Zone: ● System defined ○ User defined
(GMT+0:00) UTC
AP IP Mode: ● IPv4 only ○ IPv6 only ○ Dual
[?] Historical Connection Failures: OFF
[?] DP Group: Default DP Group
OFF Enforce the priority of DP Group
This action will disconnect the already established tunnels to vDPs and re-establish to new vDPs as per the priority defined.
SSH Tunnel Encryption: ● AES 128 ○ AES 256
SSH/TLS Key Enhance Mode: OFF

Mesh Options

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

Mapping Server ECDSA Certificates

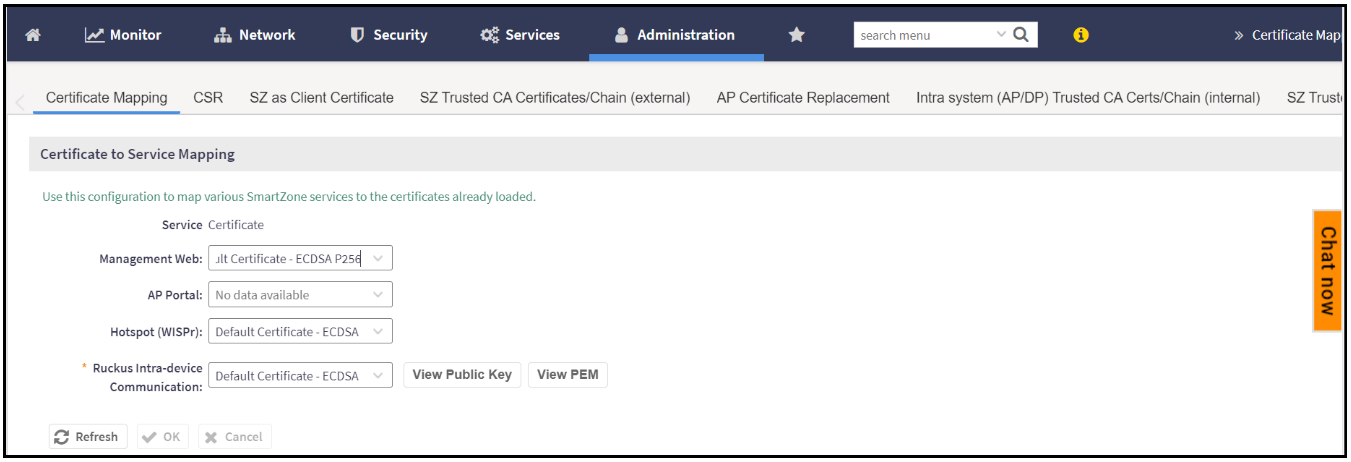
After enabling the **SSH/TLS Key Enhance Mode** at the zone level. You can map the ECDSA certificates to SmartZone (server certificate). This mapping ensures that SmartZone (server) is using 2K/3K RSA or ECDSA certificates during the TLS handshake.

To map the **ECDSA** certificates, perform the following:

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

   This displays **Certificate Mapping** page.

   FIGURE 10 Certificate Mapping



Certificate to Service Mapping

Use this configuration to map various SmartZone services to the certificates already loaded.

Service Certificate

Management Web: ılt Certificate - ECDSA P256

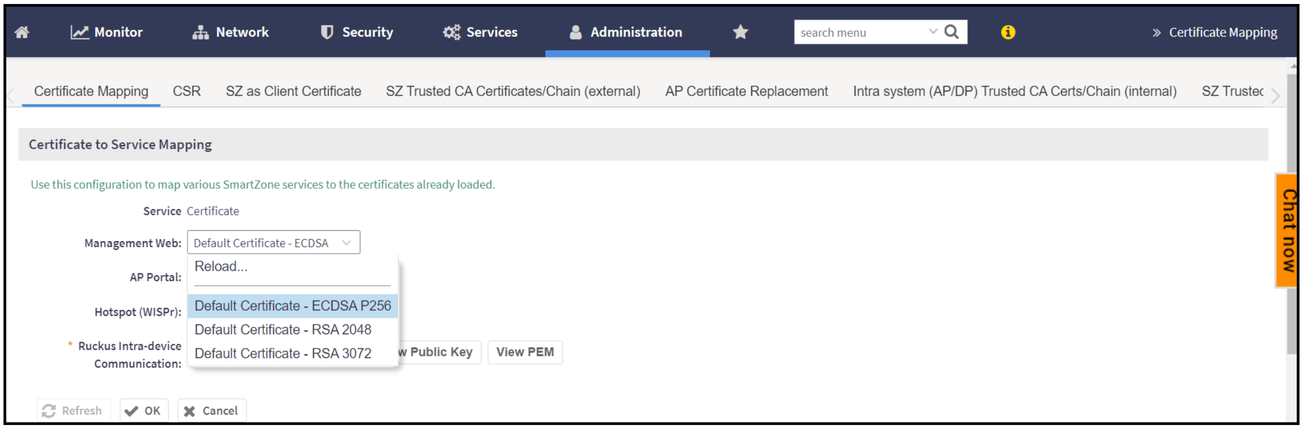
AP Portal: No data available

Hotspot (WISPr): Default Certificate - ECDSA

* Ruckus Intra-device Communication: Default Certificate - ECDSA

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

  FIGURE 11 Management Web



Certificate to Service Mapping

Use this configuration to map various SmartZone services to the certificates already loaded.

Service Certificate

Management Web: Default Certificate - ECDSA

AP Portal:

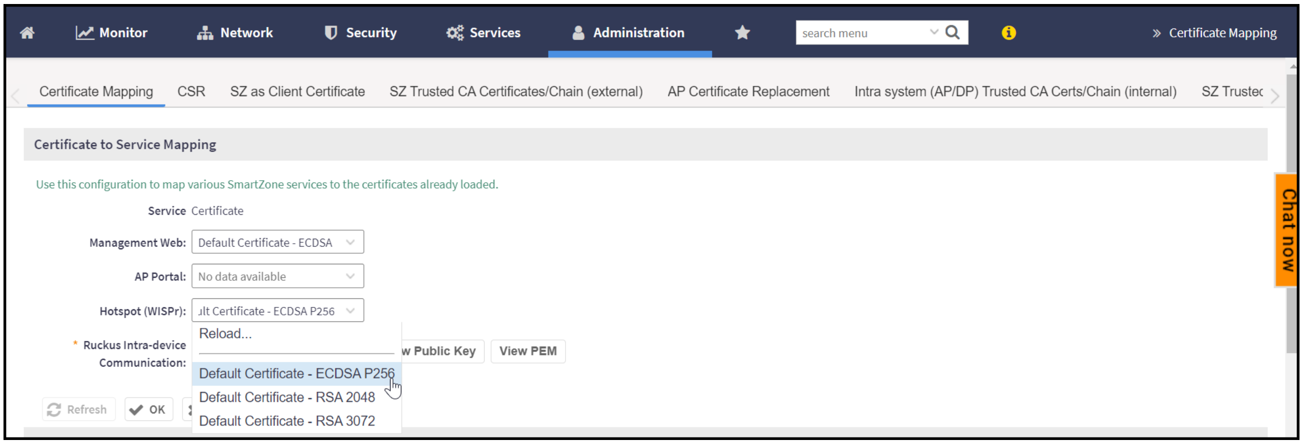
Hotspot (WISPr):

* Ruckus Intra-device Communication:

Default Certificate - ECDSA P256
Default Certificate - RSA 2048
Default Certificate - RSA 3072

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

FIGURE 12 Hotspot (WISPr)


Monitor
Network
Security
Services
Administration
search menu
» Certificate Mapping
Certificate Mapping
CSR
SZ as Client Certificate
SZ Trusted CA Certificates/Chain (external)
AP Certificate Replacement
Intra system (AP/DP) Trusted CA Certs/Chain (internal)
SZ Trustec
Chat now
w Public Key
View PEM
Refresh
OK
Reload...
Default Certificate - ECDSA P256
Default Certificate - RSA 2048
Default Certificate - RSA 3072

Certificate to Service Mapping

Use this configuration to map various SmartZone services to the certificates already loaded.

Service Certificate

Management Web: Default Certificate - ECDSA

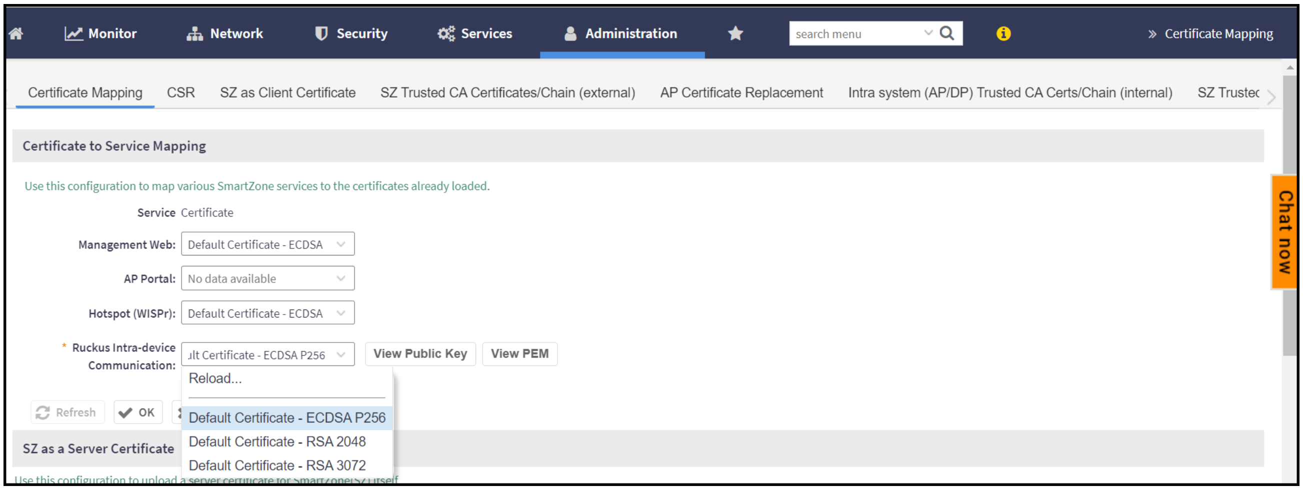
AP Portal: No data available

Hotspot (WISPr): ılt Certificate - ECDSA P256

* Ruckus Intra-device Communication:

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

FIGURE 13 Ruckus Intra-device Communication


Monitor
Network
Security
Services
Administration
search menu
» Certificate Mapping
Certificate Mapping
CSR
SZ as Client Certificate
SZ Trusted CA Certificates/Chain (external)
AP Certificate Replacement
Intra system (AP/DP) Trusted CA Certs/Chain (internal)
SZ Trustec
Chat now
View Public Key
View PEM
Refresh
OK
Reload...
Default Certificate - ECDSA P256
Default Certificate - RSA 2048
Default Certificate - RSA 3072

Certificate to Service Mapping

Use this configuration to map various SmartZone services to the certificates already loaded.

Service Certificate

Management Web: Default Certificate - ECDSA

AP Portal: No data available

Hotspot (WISPr): Default Certificate - ECDSA

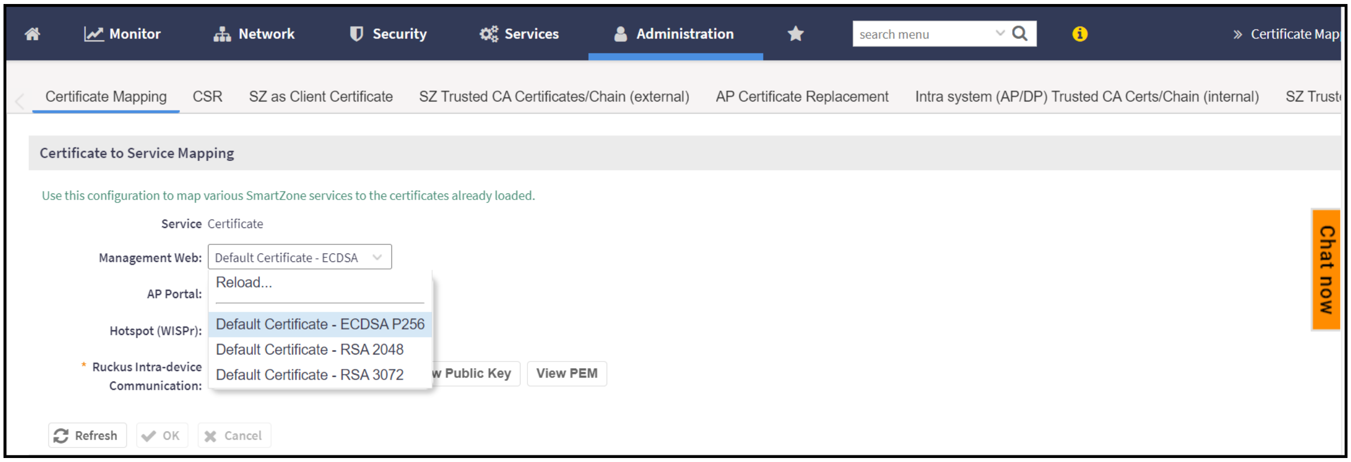
* Ruckus Intra-device Communication: ılt Certificate - ECDSA P256

SZ as a Server Certificate

Use this configuration to upload a server certificate for SmartZone/SZ itself

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

FIGURE 14 ECDSA Certificates


Monitor
Network
Security
Services
Administration
search menu
» Certificate Map
Certificate Mapping
CSR
SZ as Client Certificate
SZ Trusted CA Certificates/Chain (external)
AP Certificate Replacement
Intra system (AP/DP) Trusted CA Certs/Chain (internal)
SZ Trust
Chat now
Reload...
Default Certificate - ECDSA P256
Default Certificate - RSA 2048
Default Certificate - RSA 3072
w Public Key
View PEM
Refresh
OK
Cancel

Certificate to Service Mapping

Use this configuration to map various SmartZone services to the certificates already loaded.

Service Certificate

Management Web: Default Certificate - ECDSA

AP Portal:

Hotspot (WISPr):

* Ruckus Intra-device Communication:

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

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

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

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

1. Click **Security** > **Authentication** > **Proxy (SZ Authenticator)**.

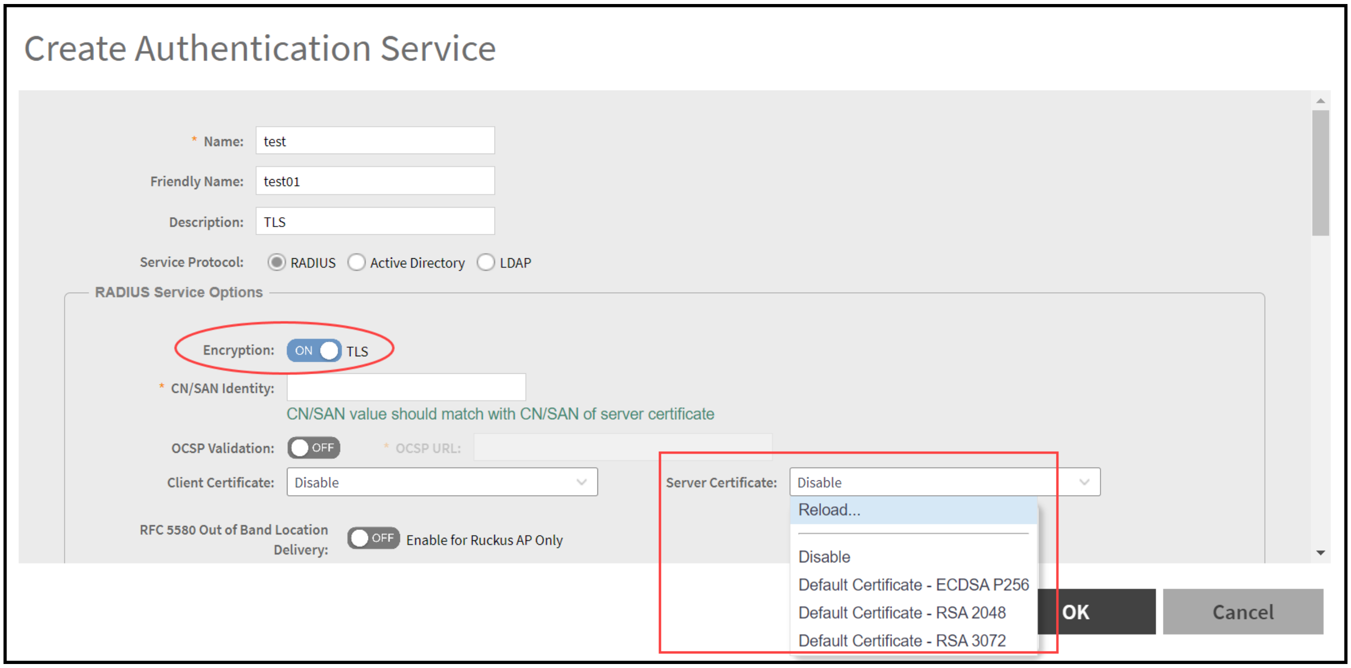
   This displays the **Proxy (SZ Authenticator)** page.
2. In the **Proxy (SZ Authenticator)**, click **Create**.

   This displays **Create Authentication Service** page.

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

   The ECDSA certificates are enabled for RADIUS server.

FIGURE 15 Encryption TLS_Authentication Service



Create Authentication Service

* Name: test

Friendly Name: test01

Description: TLS

Service Protocol: ● RADIUS ○ Active Directory ○ LDAP

RADIUS Service Options

Encryption: ON TLS

* CN/SAN Identity:

CN/SAN value should match with CN/SAN of server certificate

OCSP Validation: OFF

* OCSP URL:

Client Certificate: Disable

Server Certificate: Disable

RFC 5580 Out of Band Location Delivery: OFF Enable for Ruckus AP Only

Reload...
Disable
Default Certificate - ECDSA P256
Default Certificate - RSA 2048
Default Certificate - RSA 3072
OK
Cancel

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

1. Click **Security** > **Accounting** > **Proxy**.

   This displays **Proxy** page.

2. In the **Proxy**, click **Create**.

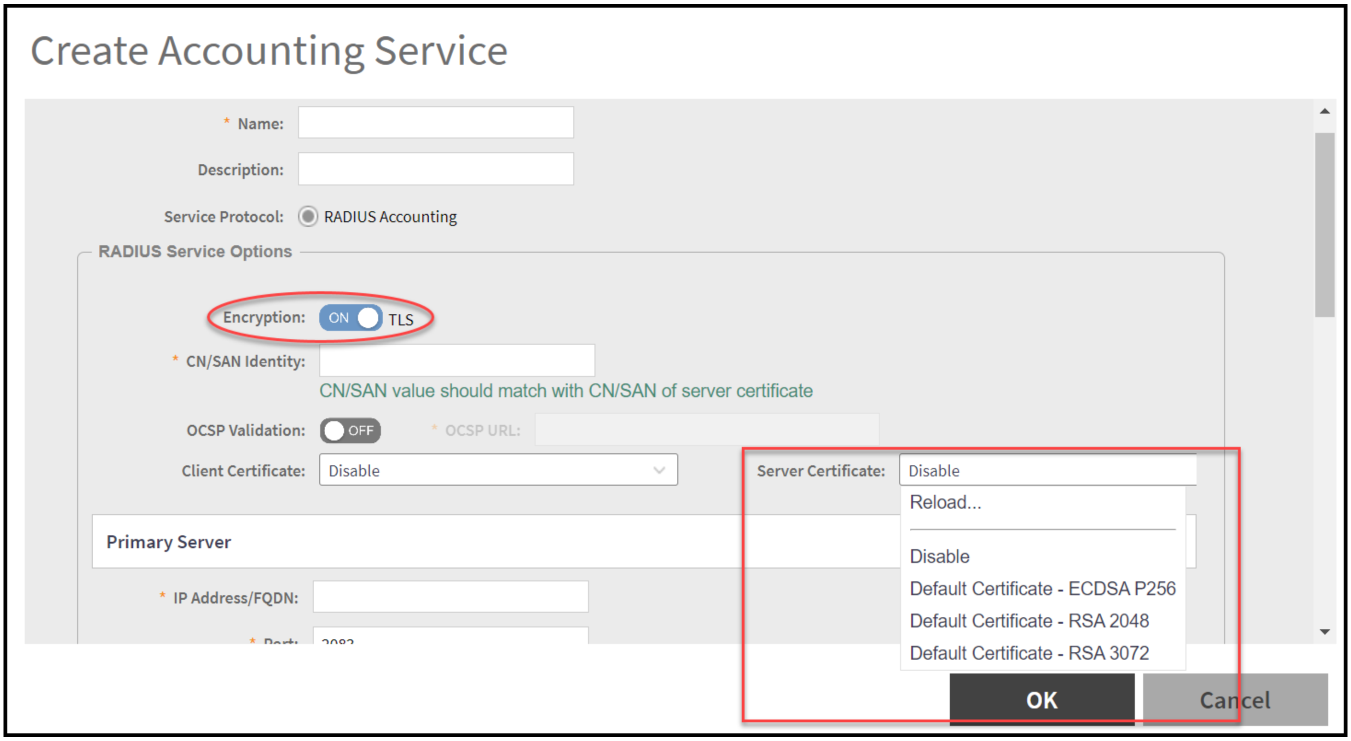
   This displays the **Create Accounting Service** page.

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

   The ECDSA certificates are enabled for RADIUS server.

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

FIGURE 16 Encryption TLS_Accounting Service



Create Accounting Service

* Name:

Description:

Service Protocol: ● RADIUS Accounting

RADIUS Service Options

Encryption: ON TLS

* CN/SAN Identity:

CN/SAN value should match with CN/SAN of server certificate

OCSP Validation: OFF

* OCSP URL:

Client Certificate: Disable

Server Certificate: Disable

Primary Server

* IP Address/FQDN:

* Port: 2083

Reload...
Disable
Default Certificate - ECDSA P256
Default Certificate - RSA 2048
Default Certificate - RSA 3072
OK
Cancel

Administrator and Roles

Managing Administrator and Roles

The controller must be able to manage various administrators and roles that are created within the network to assign tasks and functions, and to authenticate users.

Creating User Groups

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

Perform the following steps to create user groups.

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

   The **Create User Group** is displayed.

4. Configure the following options:
   a. Permission
      1. Name: Type the name of the user group you want to create.
      2. Description: Type a short description for the user group you plan to create.
      3. Permission: Select one of the access permission for the user group from the drop-down menu. You can also grant admin permission to generate guest passes. Select the **Custom** option to manually assign role-based permission in the **Resource** tab page.
      4. Account Security: Select the account security profile that you created to manage the administrator accounts.
      5. Click **Next**.

   b. Resource: From **Select Resources**, choose the resources that you want to assign to this user group. If you have selected **Custom** permission option in the previous step, you can assign the required permission (**Read**, **Modify** or **Full Access**) to these resources. The resources available are SZ, AP, WLAN, User/Device/App, Admin, Guest Pass, MVNO and ICX. Click the → icon and they appear under **Selected Resources** now. Use the ← icon to deselect the resources assigned to the group. To select the right set of resource permission, refer to Resource Group Details.

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

   c. Click **Next**.

   d. Domain: Select the domain from the list of domains to which this user group will be associated. From **Select Domains**, choose the domains you want to assign to this user group. Click the →

      icon and they appear under **Selected Domains** now. Use the ← icon to deselect the domains assigned to the group.

   e. Click **Next**.

   f. Administrator: From **Available Users**, choose the users you want to assign to this user group. Click the →

      icon and they appear under **Selected Users** now. Use the ← icon to deselect the users assigned to the group.

      You can also create Administrator Accounts by clicking the ✚ icon. The **Create Administrator Account** page appears where you can configure the administrator account settings. You can edit the user settings by clicking the ✎ icon and delete the user from the list by clicking 🗑 icon.

   g. Click **Next**.

   h. Review: Verify the configuration of the user group. Click **Back** to make modifications to the configuration settings.

   i. Click **OK** to confirm.

You have created the user groups.

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

Resource Group Details

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

TABLE 14 Resource Group Table

Resource Category	Resources
SZ	System Settings Cluster Settings and Cluster Redundancy Control Planes and Data Planes Firmware and Patches Cluster and Configuration Backups Licensing Cluster Stats and Health System Events and Alarms System Certificates WISPr Northbound Interface SCI Integration
AP	Zones and Zone Templates AP groups AP Settings AP Stats and Health Maps AP Events and Alarms Bonjour Policies Location Services Ethernet Port Profiles Tunneling Profiles and Settings AP Zone Registration
WLAN	WLANs WLAN Groups and Templates AAA Services L2-7 Policies Rate Limiting Application Policies Device OS Policies QoS Controls Hotspots and Portals Hotspot 2.0 Service Schedules VLAN Pools

TABLE 14 Resource Group Table (continued)

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

Creating Administrator Accounts

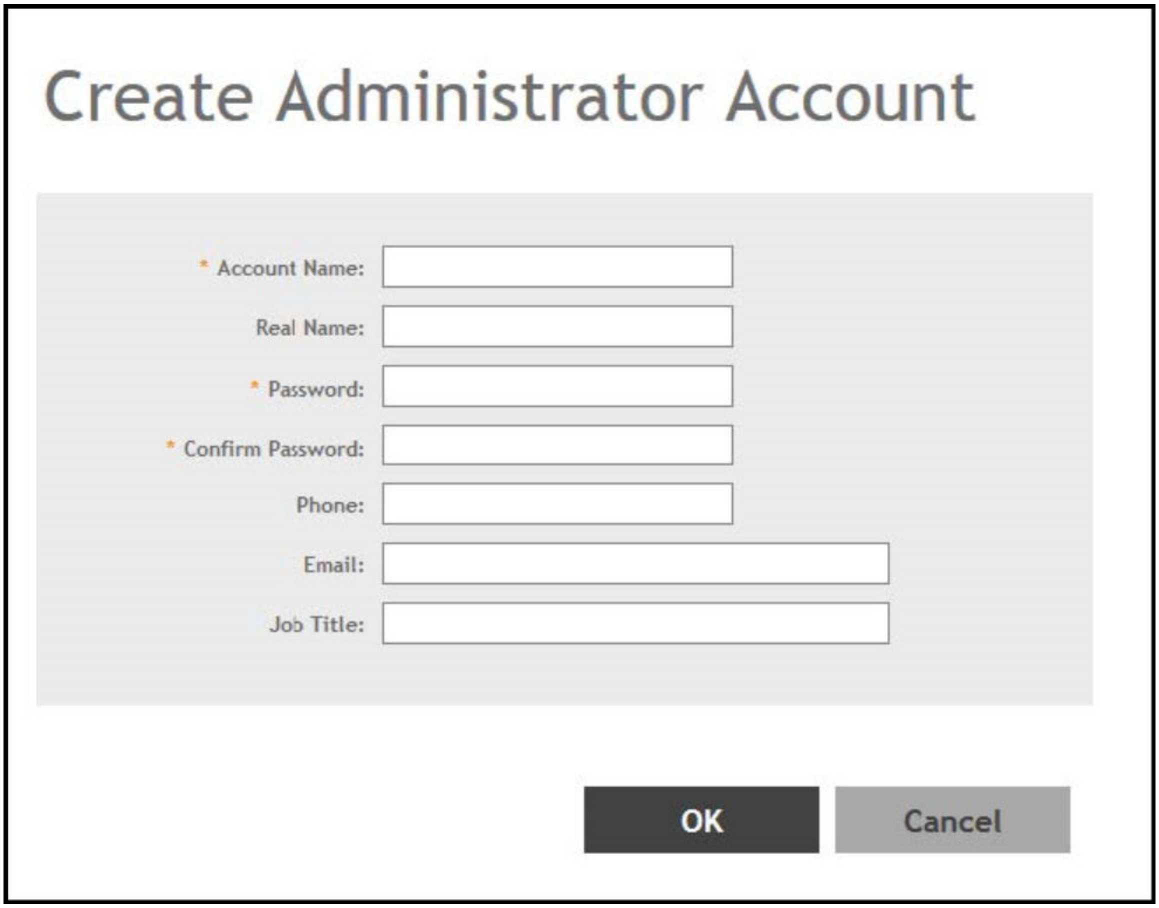
The controller supports the creation of additional administrator accounts. This allows you to share or delegate management and monitoring functions with other members of your organization. You can also modify the status of the administrator account by locking or unlocking it.

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

3. Click **Create**.

   The **Create Administrator Account** page appears.

FIGURE 17 Creating an Administrator Account



Create Administrator Account

* Account Name:	
Real Name:	
* Password:	
* Confirm Password:	
Phone:	
Email:	
Job Title:	

4. Configure the following:

   a. Account Name: Type the name that this administrator will use to log on to the controller.

   b. Real Name: Type the actual name (for example, John Smith) of the administrator.

   c. Password: Type the password that this administrator will use (in conjunction with the Account Name) to log on to the controller.

   d. Confirm Password: Type the same password as above.

   e. Phone: Type the phone number of this administrator.

   f. Email: Type the email address of this administrator.

   g. Job Title: Type the job title or position of this administrator in your organization.

   h. Click **OK**.

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

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

Unlocking an Administrator Account

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

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

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

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

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

Configuring Administrator Accounts

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

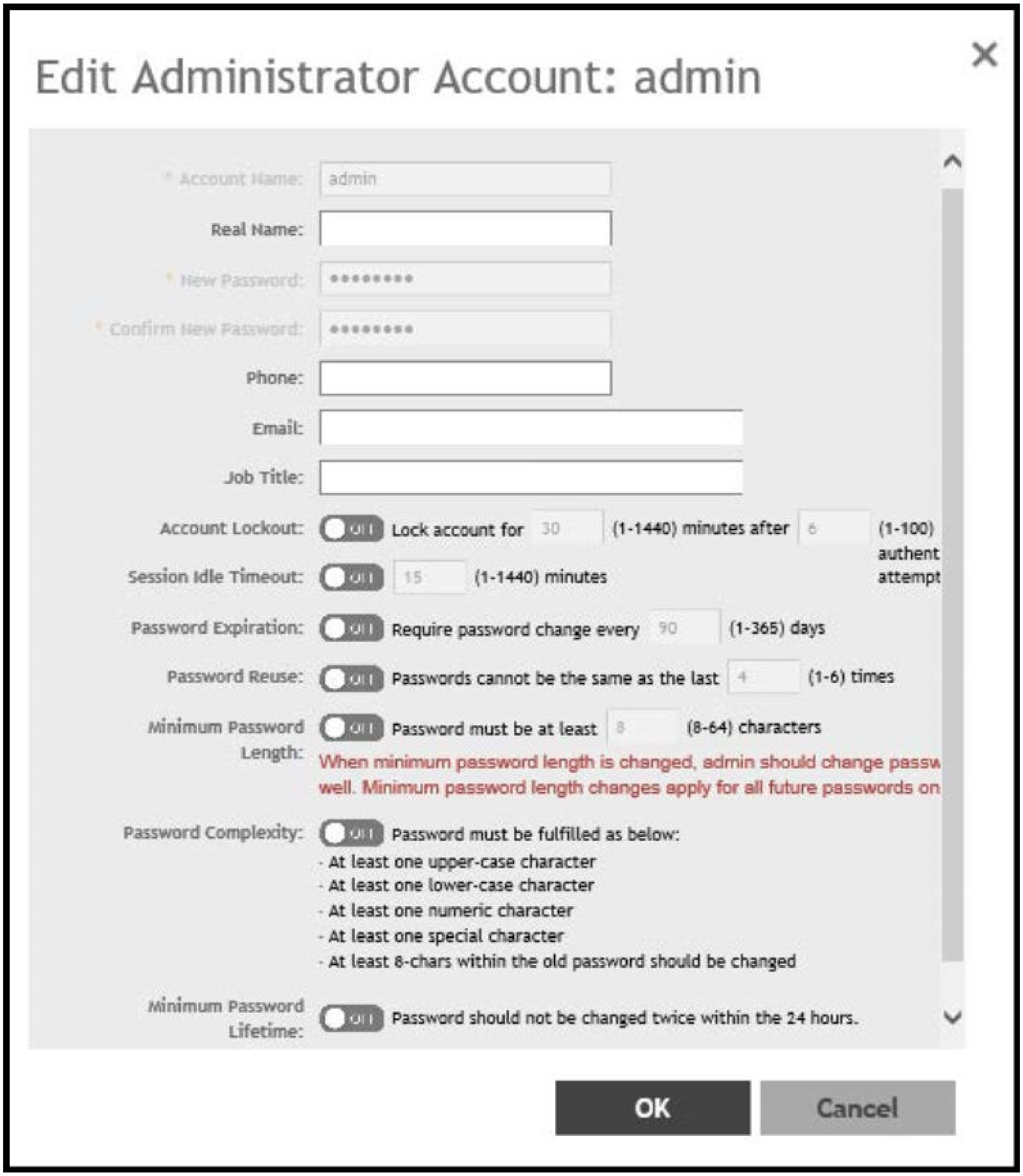
You must log in as a system default *Super Admin* to set the rules.

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

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

   The **Edit Administrator Account** page appears.

FIGURE 18 Configuring an Administrator Account



Edit Administrator Account: admin

* Account Name: admin

Real Name:

* New Password: ••••••••

* Confirm New Password: ••••••••

Phone:

Email:

Job Title:

Account Lockout: Off Lock account for 30 (1-1440) minutes after 6 (1-100) authent attempt

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

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

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

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

When minimum password length is changed, admin should change passw well. Minimum password length changes apply for all future passwords on

Password Complexity: Off Password must be fulfilled as below:

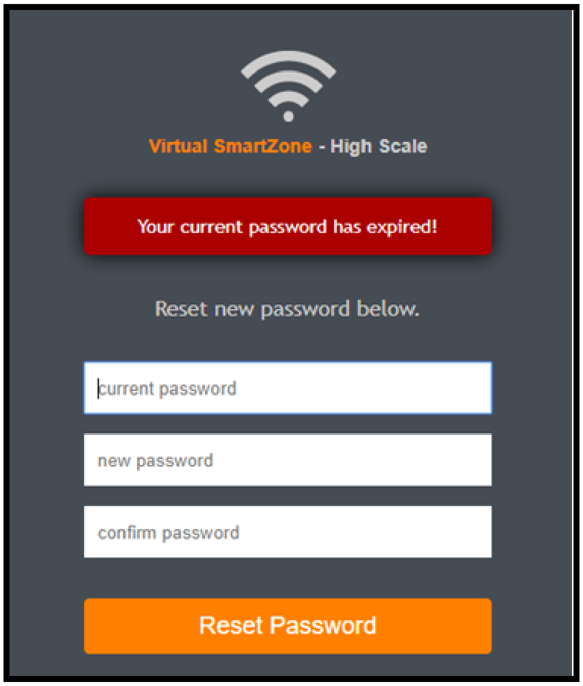
- At least one upper-case character
- At least one lower-case character
- At least one numeric character
- At least one special character
- At least 8-chars within the old password should be changed

Minimum Password Lifetime: Off Password should not be changed twice within the 24 hours.

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

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

     FIGURE 19 Resetting the Old Password

     Virtual SmartZone - High Scale

     Your current password has expired!

     Reset new password below.

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

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

  Select the options you want to apply.

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

5. Click **Ok**.

   The Password Confirmation page is displayed.

6. Enter the password.
7. Click **Ok** to apply the new configuration.

Working with AAA Servers

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

Configuring SmartZone Admin AAA Servers

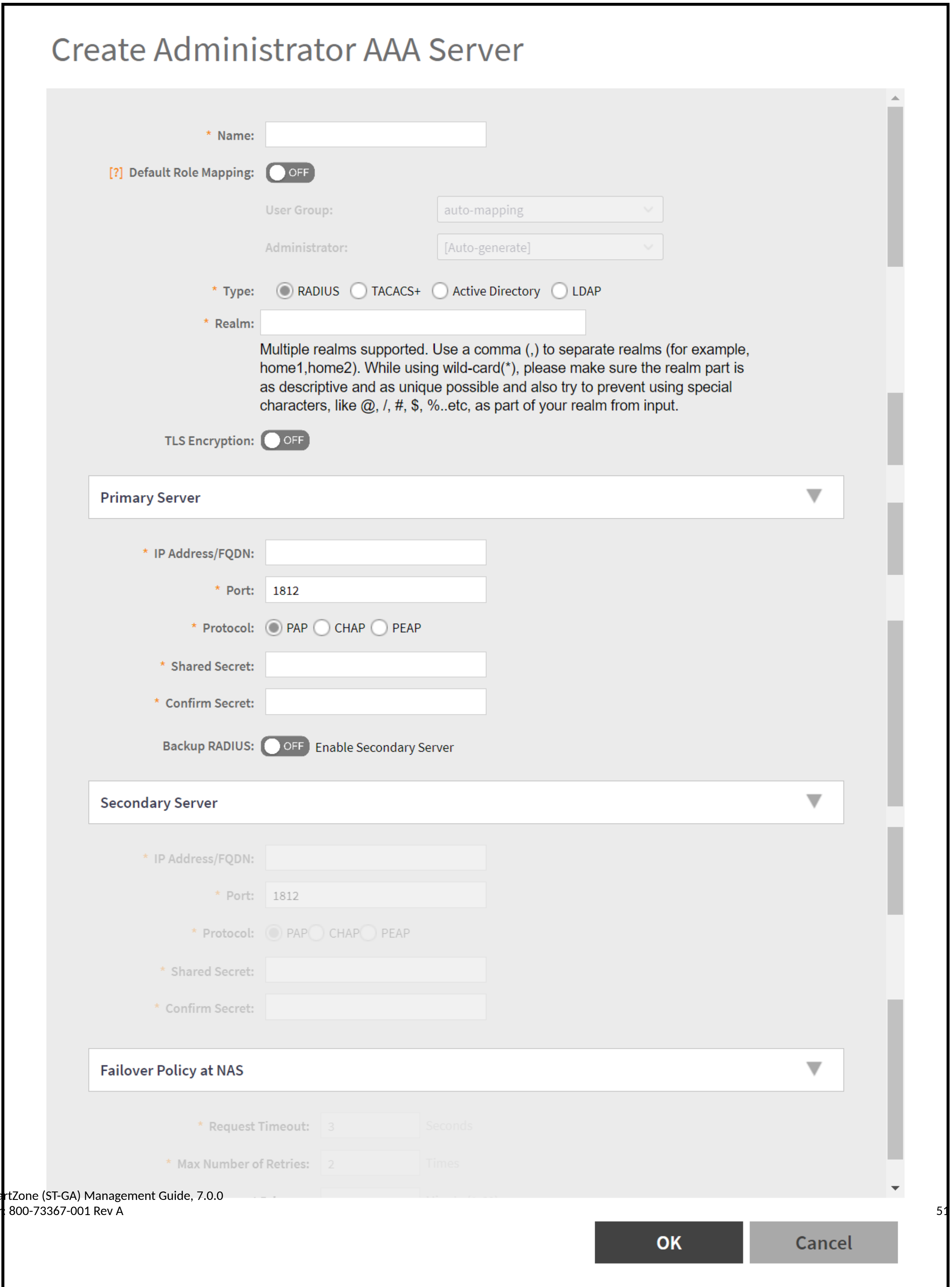
To add and manage AAA servers that the controller can use to authenticate users, complete the following steps.

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

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

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

FIGURE 20 Creating an Administrator AAA Server



Create Administrator AAA Server

* Name:

[?] Default Role Mapping: OFF

User Group: auto-mapping

Administrator: [Auto-generate]

* Type: ● RADIUS ○ TACACS+ ○ Active Directory ○ LDAP

* Realm:

Multiple realms supported. Use a comma (,) to separate realms (for example, home1,home2). While using wild-card(*), please make sure the realm part is as descriptive and as unique possible and also try to prevent using special characters, like @, /, #, $, %..etc, as part of your realm from input.

TLS Encryption: OFF

Primary Server

* IP Address/FQDN:

* Port: 1812

* Protocol: ● PAP ○ CHAP ○ PEAP

* Shared Secret:

* Confirm Secret:

Backup RADIUS: OFF Enable Secondary Server

Secondary Server

* IP Address/FQDN:

* Port: 1812

* Protocol: ● PAP ○ CHAP ○ PEAP

* Shared Secret:

* Confirm Secret:

Failover Policy at NAS

* Request Timeout: 3 Seconds

* Max Number of Retries: 2 Times

3. Enter the AAA server name.
4. For **Type**, select the type of AAA server to authenticate users:
   - **RADIUS**
   - **TACACS+**
   - **Active Directory**
   - **LDAP**
5. For **Realm**, enter the realm or service.

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

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

6. Enable **Default Role Mapping**.

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

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

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

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

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

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

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

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

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

   For **Active Directory**, configure the settings for the **Proxy Agent**.
   - **User Principal Name**: Enter the Windows domain Administrator name
   - **Password**: Enter the administrator password.
   - **Confirm Password**: Re-enter the password to confirm.
8. For **Backup RADIUS**, if a secondary backup server is available on the network, select **Enable Secondary Server**.
9. Under **Secondary Server**, configure the settings of the secondary RADIUS server.
   - **IP Address**: Enter the IP address of the AAA server.
   - **IP Address or FQDN**: Enter the IP address or Fully Qualified Domain Name (FQDN) of the AAA server.

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

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

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

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

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

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

Testing SmartZone Admin AAA Servers

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

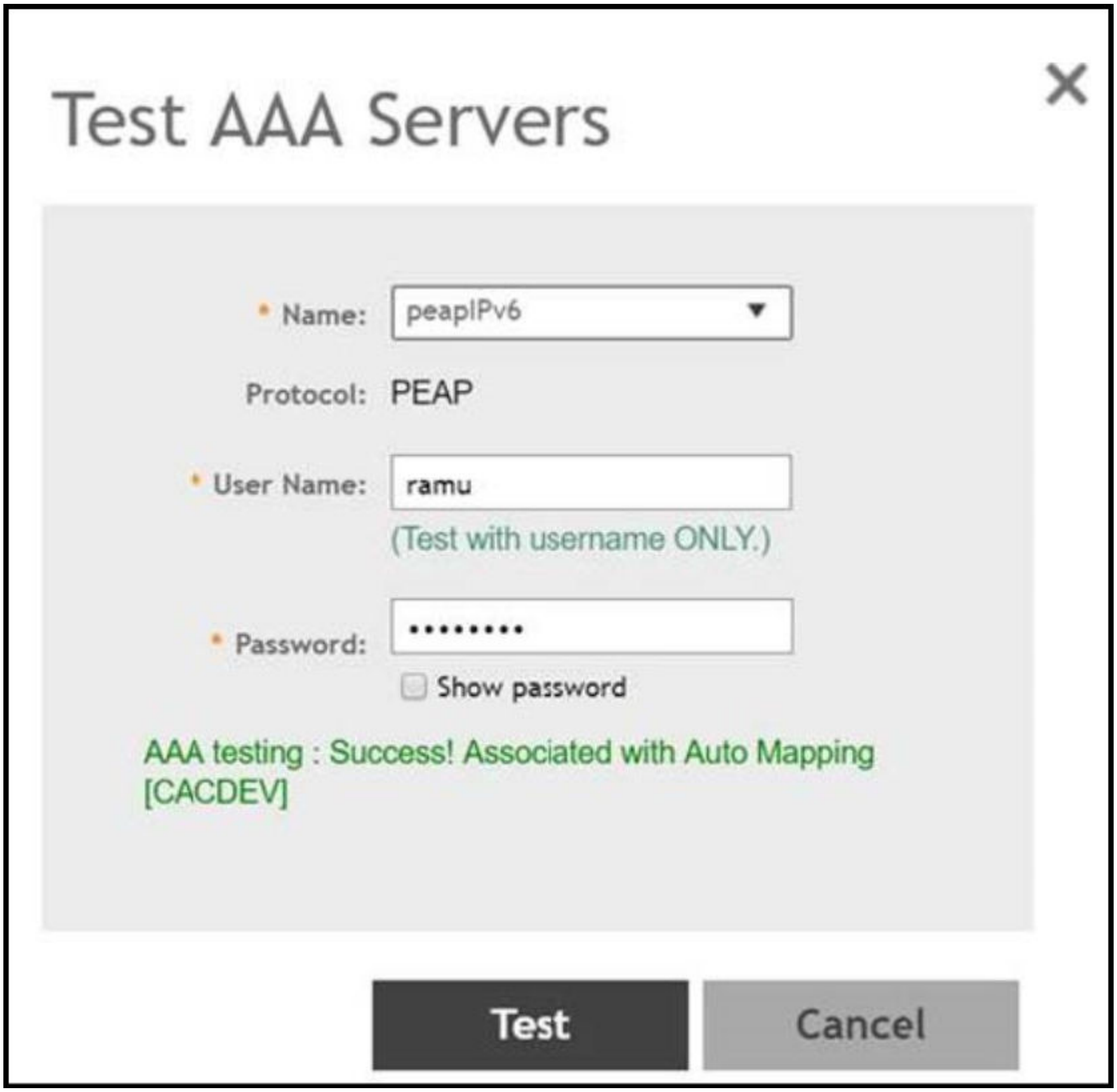
The test queries the AAA server for a known authorized user and return groups associated with the user that can be used for configuring roles within the controller.

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

2. Select the created AAA server and click **Test AAA**.

   An example for testing a RADIUS server is shown in the following figure.

   FIGURE 21 Testing AAA Server: RADIUS



Test AAA Servers

* Name: peapIPv6

Protocol: PEAP

* User Name: ramu

(Test with username ONLY.)

* Password: ••••••••

□ Show password

AAA testing : Success! Associated with Auto Mapping [CACDEV]

   The **Protocol** field is displayed only when the selected AAA server is configured as *Type = RADIUS*

3. **Name**: Is pre-filled based on the selected AAA server.
4. **User Name** : Enter a name that is associated to the group.

   NOTE
   For TACACS+ server, test with username appended with configured service.

5. **Password**: Enter password for the user name you specified.
6. Click **Test**.

If the username is associated with a user group, the following message is displayed: AAA testing: Success! Associated with Auto Mapping. If the username is not associated with any user group, the following message is displayed: "AAA testing: Success! No SZ User or Default role mapping associated".

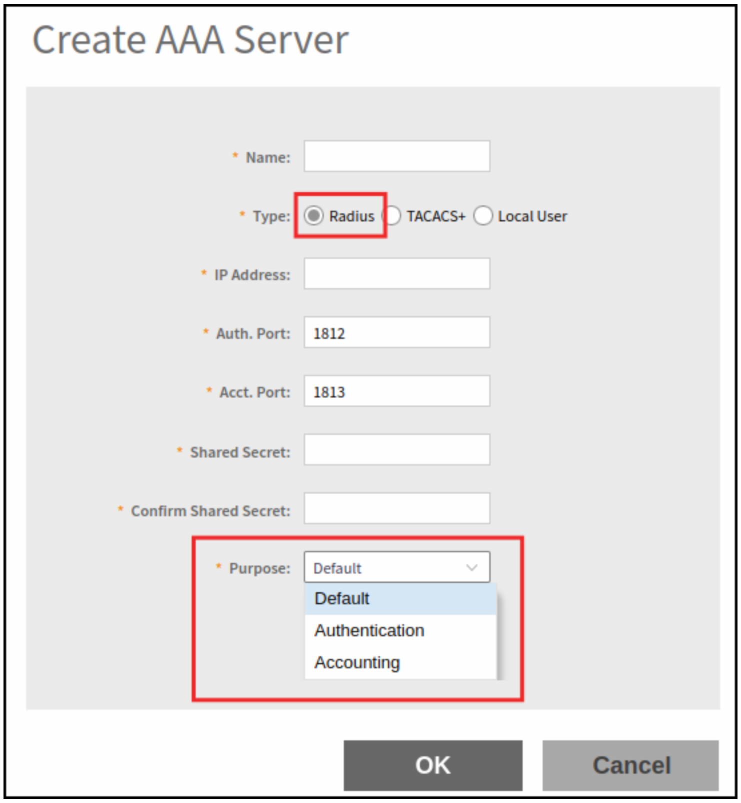
Configuring Switch AAA Servers

To add and manage Authentication, Authorization, and Accounting (AAA) servers that the controller can use for authentication, follow these steps.

1. Select **Network** > **Wired** > **Switches** The **Switches** window is displayed.
2. Select a **Domain** > **Switch Group** and scroll down to view the details.
3. In the **Common Configuration** tab, click the **Configure** icon to display the **Common Configuration** dialog box.
4. Click the **AAA** tab.
5. Expand the **AAA Servers** section.
6. Click the **[+Create]** icon.

   The **Create AAA Server** page is displayed.
7. Enter the AAA server name.
8. For **Type**, select **RADIUS**, **TACACS+** or **Local User** type of AAA server to authenticate user.

   FIGURE 22 Creating a Switch AAA Server with Type as RADIUS



Create AAA Server

* Name:

* Type: ● Radius ○ TACACS+ ○ Local User

* IP Address:

* Auth. Port: 1812

* Acct. Port: 1813

* Shared Secret:

* Confirm Shared Secret:

* Purpose: Default

9. **IP Address**: Enter the IP address of the AAA server.

10. **Auth. Port**: Enter the authentication port that the server is using.

    NOTE
    The default port number is 1812. If you need to enter any other value for the port number, it must be within the range of 0 to 65535.

11. **Acct. Port**: Enter the accounting port that the server is using.

    NOTE
    The default port number is 1813. If you need to enter any other value for the port number, it must be within the range of 0 to 65535.

12. **Shared Secret**: Enter the shared secret.
13. **Confirm Shared Secret**: Re-enter the shared secret to confirm.
14. **Purpose**: When Type=RADIUS, select the purpose for the RADIUS AAA server being created. Values are **Default**, **Authentication** and **Accounting** from the list.

    NOTE
    Starting with 7.0 release, you can set up multiple RADIUS servers with different options such as **Authentication** and **Accounting**. In earlier releases, the controller could only configure a RADIUS server for a switch with the **Default** option.

    NOTE
    The switch supports this setting on FastIron release 08.0.90 and later versions.

    When Type=TACACS+, select the purpose for the TACACS+ AAA server being created. Values are **Default**, **Authentication**, **Authorization**, and **Accounting**. When Type = Local User, select the privilege for the Local User server being created. Values are **Port Config** , **Read Only** and **Read Write**.
15. Click **OK**.

    You can subsequently edit or delete a AAA server by selecting the server from the list in the **AAA Servers** section and selecting **Configure** or **Delete**, respectively.

    NOTE
    The ICX switch fails to delete the TACACS+ and RADIUS AAA servers when pushed from SmartZone or Virtual SmartZone if SNMP query is disabled in the switch or if the switch is pre-configured before joining SmartZone or Virtual SmartZone.

Configuring Switch AAA Server Settings

To configure and manage AAA servers, complete the following steps.

1. Select **Network** > **Wired** > **Switches** > **AAA** .

2. Select **Switch AAA Setting**Select **Switch GroupConfigurationCommon ConfigurationConfigureAAA**, configure the following.

   Login Athentication

   - **SSH Authentication**: Enable the option for secure authentication.
   - **Telnet Authentication**: Enable the option to set Telnet authentication. This option requires SSH authentication to be enabled.
   - **First Pref**: Select the first preferred authentication system.
   - **Second Pref**: Select the second preferred authentication system.
   - **Third Pref**: Select the third preferred authentication system.

   Authorization

   - **Command Authorization**: Enable this option to assign the following authorization services:
     - **Level**: Select the required privilege: **Port Config**, **Read Only**, or **Read Write**.
     - **Server 1**: Select the authorization method for the first server.
     - **Server 2**: Select the authorization method for the second server.
   - **Exec Authorization**: Enable this option to authorize the user to access the privilege mode.
     - **Server 1**: Select the authorization method for the first server.
     - **Server 2**: Select the authorization method for the second server.

   Accounting

   - **Command Accounting**: Enable this option to track the following accounting services:
     - **Level**: Select the required privilege: **Port Config**, **Read Only**, or **Read Write**.
     - **Server 1**: Select the tracking method for the first server.
     - **Server 2**: Select the tracking method for the second server.
   - **Exec Accounting**: Enable this option to track the services in the privilege mode.
     - **Server 1**: Select the tracking method for the first server.
     - **Server 2**: Select the tracking method for the second server.

3. Click **OK**.

AAA Server Authentication

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

1. Enable **Default Role Mapping** to map the external AAA users to a single SZ local admin user.

2. Apply the permissions of AAA users on SZ using the corresponding AAA server attributes.

   Following is an example:

   a. Create three user groups with the following access permissions in SZ:
      - Group1 with SZ super permission
      - Group2 with SZ AP admin permission
      - Group3 with SZ read-only permission

   b. Create three SZ local users corresponding to the user groups as follows:
      - Bind User1 with Group1
      - Bind User2 with Group2
      - Bind User3 with Group3

      NOTE
      Following are the attribute values on AAA servers:
      - RADIUS: **Ruckus-WSG-User=User1** or **User2** or **User3**.
      - TACACS+: **user-name=User1** or **User2** or **User3**.
      - Active Directory and LDAP: **Group cn=Ruckus-WSG-User-User1** or **Ruckus-WSG-User-User2** or **cn=Ruckus-WSG-User-User3**.

   c. Select **Administrator** > **Administrator** > **Admins and Roles** > **AAA** and click **Create** to create an Admin AAA profile.

      Refer to Configuring SmartZone Admin AAA Servers on page 49.

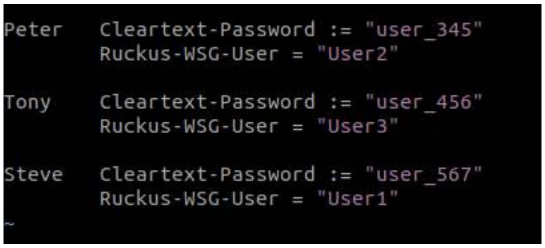
About RADIUS Support

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

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

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

   For example,



```
Peter   Cleartext-Password := "user_345"
        Ruckus-WSG-User = "User2"

Tony    Cleartext-Password := "user_456"
        Ruckus-WSG-User = "User3"

Steve   Cleartext-Password := "user_567"
        Ruckus-WSG-User = "User1"
~
```

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

   NOTE
   Refer to Creating Administrator Accounts on page 44. In this example, RADIUS can use User1, User2, or User3.

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

   NOTE
   Refer to Creating User Groups on page 41.

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

   NOTE
   Refer to Configuring SmartZone Admin AAA Servers on page 49.

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

   NOTE
   The value of super-login depends on the realm configured for the AAA profile. Refer to Creating Administrator Accounts on page 44.

About TACACS+ Support

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

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

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

   For example,

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

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

   NOTE
   Refer to Creating Administrator Accounts on page 44.

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

   NOTE
   Refer to Creating User Groups on page 41.

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

   NOTE
   Refer to Configuring SmartZone Admin AAA Servers on page 49.

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

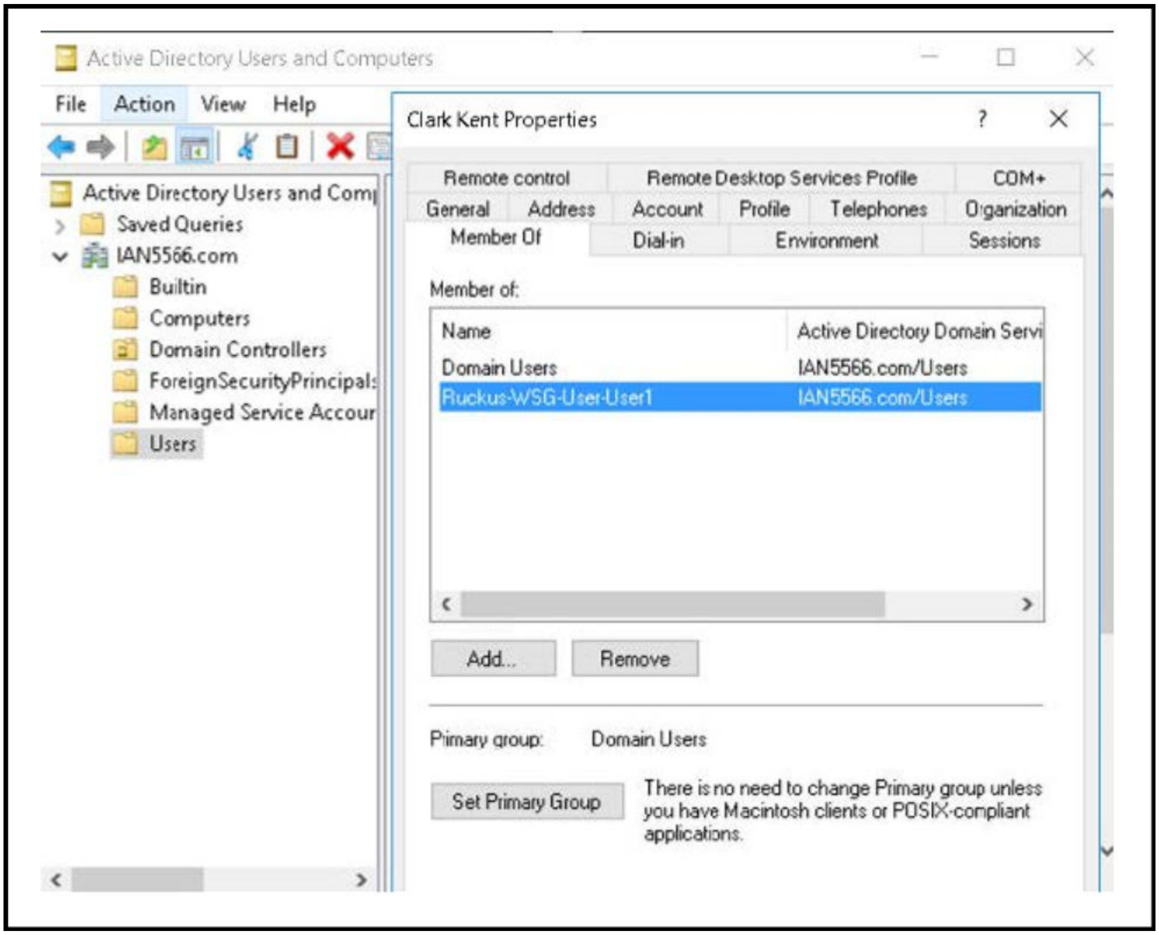
About Active Directory (AD) Support

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

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

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

FIGURE 23 About Active Directory Support



Member of:

Name	Active Directory Domain Servi
Domain Users	IAN5566.com/Users
Ruckus-WSG-User-User1	IAN5566.com/Users

Primary group: Domain Users

There is no need to change Primary group unless you have Macintosh clients or POSIX-compliant applications.

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

   NOTE
   Refer to Creating Administrator Accounts on page 44. In this example, Active Directory can use User1 only.

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

   NOTE
   Refer to Creating User Groups on page 41 .

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

   NOTE
   Refer to Configuring SmartZone Admin AAA Servers on page 49.

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

   NOTE
   The value of super-login depends on the realm configured for the AAA profile. Refer to Creating Administrator Accounts on page 44.

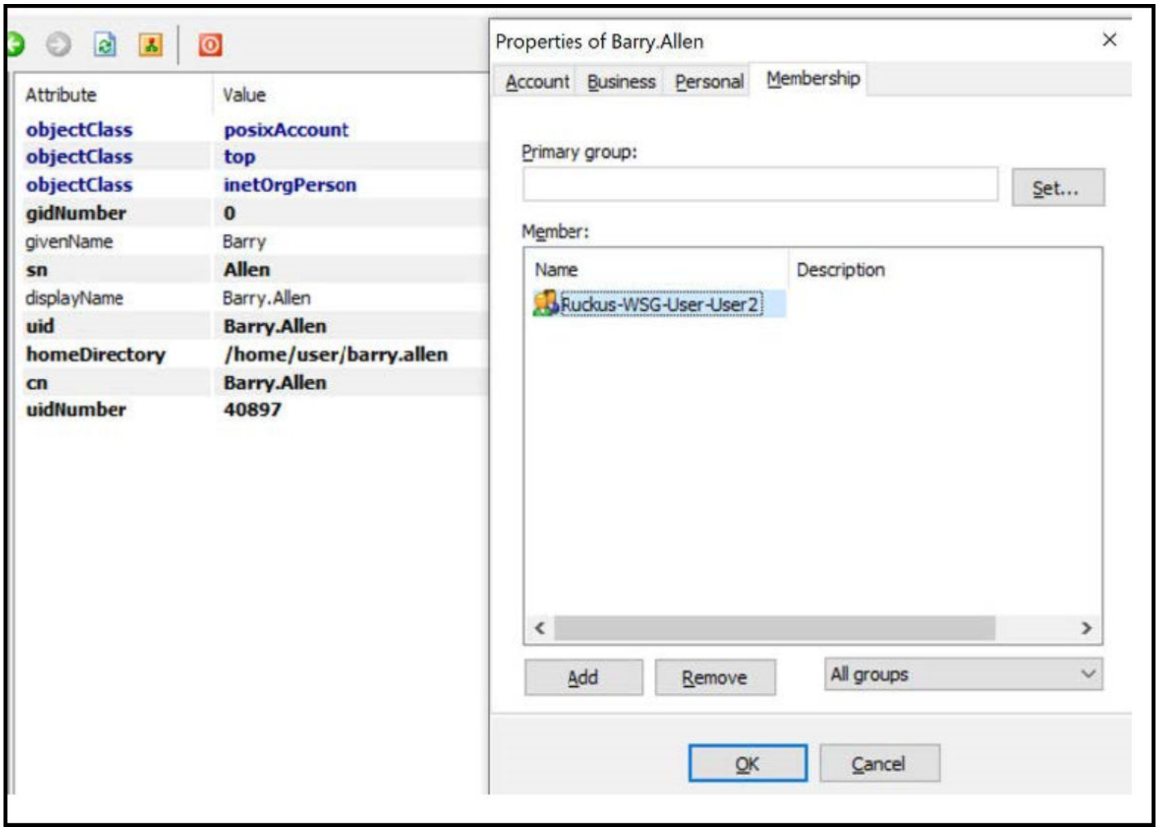
About LDAP Support

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

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

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

FIGURE 24 Supporting LDAP Configuration



Attribute	Value
objectClass	posixAccount
objectClass	top
objectClass	inetOrgPerson
gidNumber	0
givenName	Barry
sn	Allen
displayName	Barry.Allen
uid	Barry.Allen
homeDirectory	/home/user/barry.allen
cn	Barry.Allen
uidNumber	40897

Properties of Barry.Allen

Primary group:

Member:

Name	Description
Ruckus-WSG-User-User2	

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

   NOTE
   Refer to Creating Administrator Accounts on page 44. In this example, LDAP can use User2 only.

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

   NOTE
   Refer to Creating User Groups on page 41.

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

   NOTE
   Refer to Configuring SmartZone Admin AAA Servers on page 49.

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

   NOTE
   The value of super-login depends on the realm configured for the AAA profile. Refer to Creating Administrator Accounts on page 44.

Enabling the Access Control of Management Interface

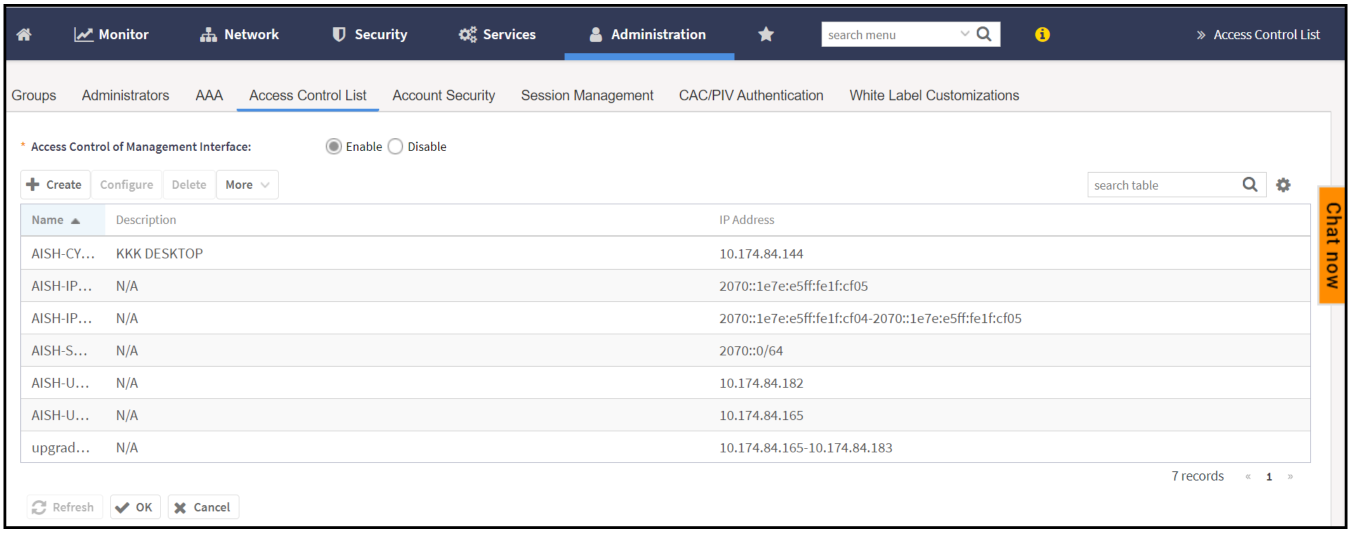
1. click **Administration** > **Admins and Roles** > **Access Control List**.

   This displays the **Access Control of Management Interface** page.

2. Click **Enable**.

   This displays the **Access Control List**.

FIGURE 25 Access Control of Management Interface



* Access Control of Management Interface: ● Enable ○ Disable

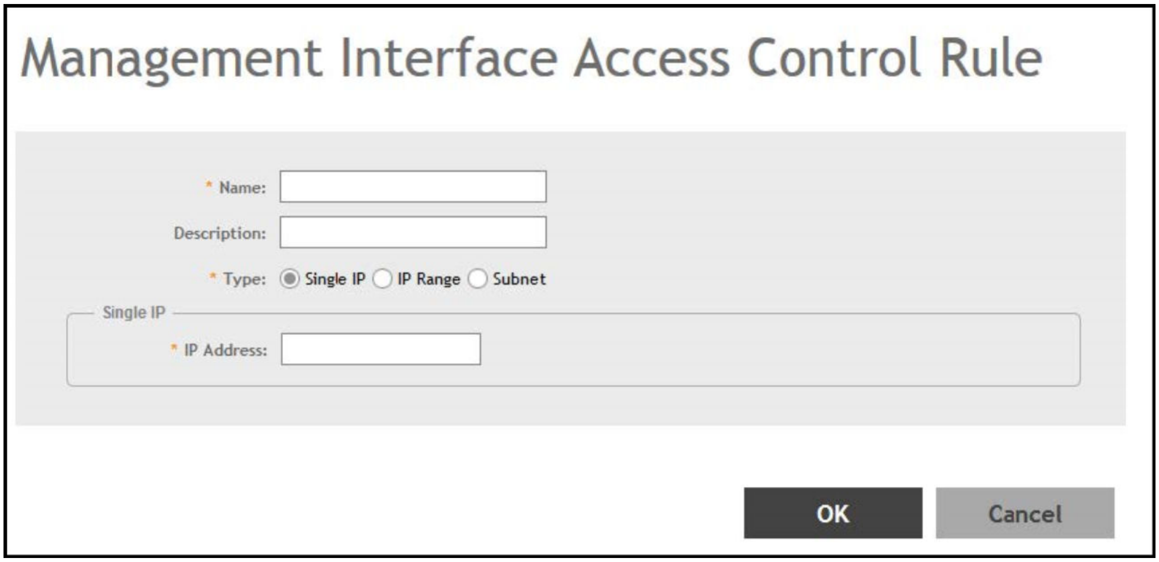
Name ▲	Description	IP Address
AISH-CY...	KKK DESKTOP	10.174.84.144
AISH-IP...	N/A	2070::1e7e:e5ff:fe1f:cf05
AISH-IP...	N/A	2070::1e7e:e5ff:fe1f:cf04-2070::1e7e:e5ff:fe1f:cf05
AISH-S...	N/A	2070::0/64
AISH-U...	N/A	10.174.84.182
AISH-U...	N/A	10.174.84.165
upgrad...	N/A	10.174.84.165-10.174.84.183

7 records « 1 »

3. Click **Create**.

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

   FIGURE 26 Management Interface Access Control Rule



* Type: ● Single IP ○ IP Range ○ Subnet

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

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

Creating Account Security

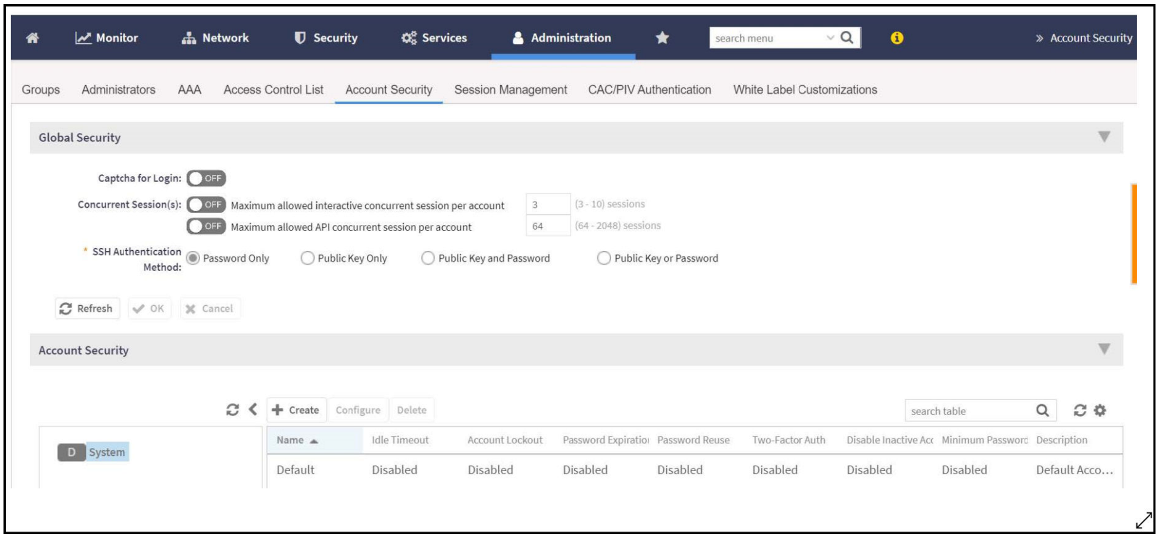
Creating an account security profile enables end-users to control administrative accounts to better manage admin accounts, passwords, login, and DoS prevention.

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

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

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

   FIGURE 27 Account Security page



Global Security

Captcha for Login: OFF

Concurrent Session(s): OFF Maximum allowed interactive concurrent session per account 3 (3 - 10) sessions

OFF Maximum allowed API concurrent session per account 64 (64 - 2048) sessions

* SSH Authentication Method: ● Password Only ○ Public Key Only ○ Public Key and Password ○ Public Key or Password

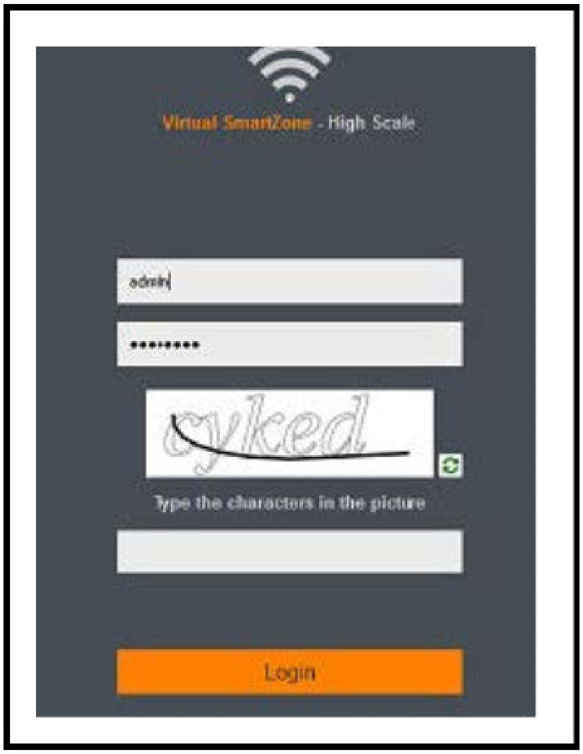
Account Security

Name	Idle Timeout	Account Lockout	Password Expiratio	Password Reuse	Two-Factor Auth	Disable Inactive Acc	Minimum Passwor	Description
Default	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Default Acco…

3. From Global Security, configure the following:

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

   FIGURE 28 Captcha Enabled in the Login Page


Virtual SmartZone - High Scale
admin
••••••••
cyked
Type the characters in the picture
Login

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

   b. Concurrent sessions: Click the required options and enter the number of sessions allowed:

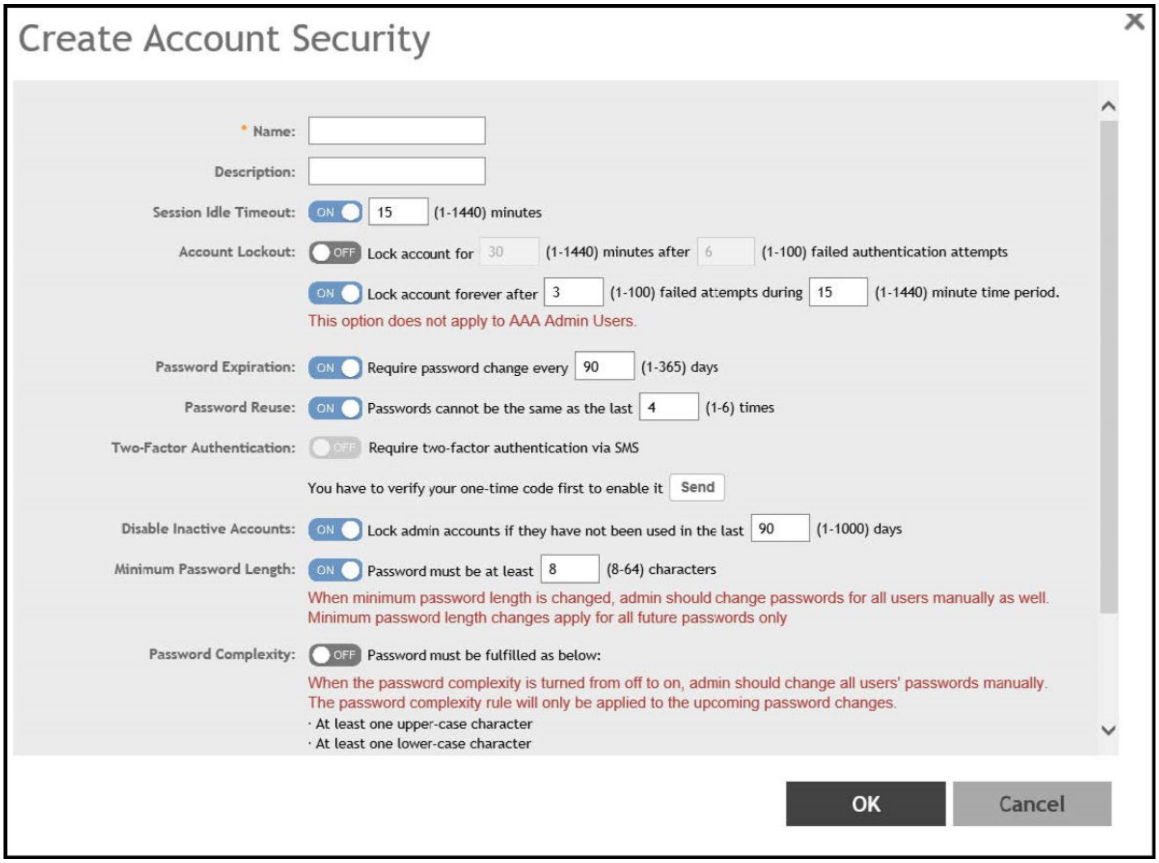
   - **Maximum allowed interactive concurrent session per account**
   - **Maximum allowed API concurrent sessions per account**

   c. Click **OK**.

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

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

   FIGURE 29 Creating Account Security



Create Account Security

* Name:

Description:

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

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

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

This option does not apply to AAA Admin Users.

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

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

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

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

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

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

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

Password Complexity: OFF Password must be fulfilled as below:

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

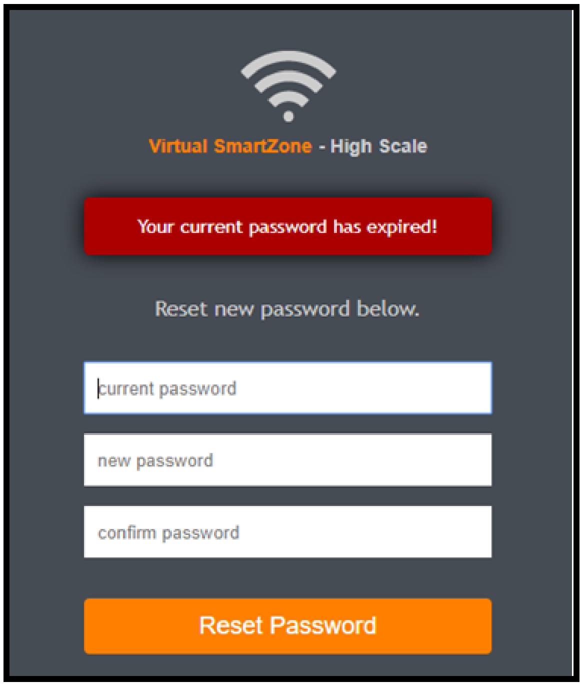
· At least one upper-case character
· At least one lower-case character

5. Configure the following:

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

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

  FIGURE 30 Resetting the Old Password

  Virtual SmartZone - High Scale

  Your current password has expired!

  Reset new password below.

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

- Password Complexity: Ensures that the password applies the following rules:
  - At least one upper-case character
  - At least one lower-case character
  - At least one numeric character
  - At least one special character
  - At least eight characters from the previous password is changed

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

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

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

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

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

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

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

Terminating Administrator Sessions

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

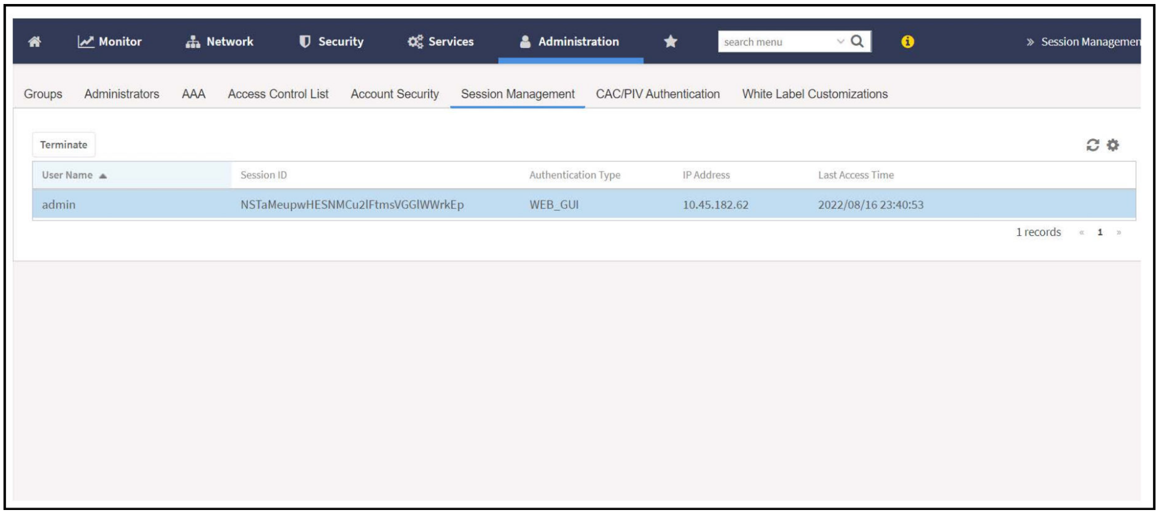
1. From the controller web interface, select **Administration** > **Admin and Roles** > **Session Management**
2. Select the administrator session you want to discontinue and click **Terminate**.

   The **Password Confirmation** page displays.

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

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

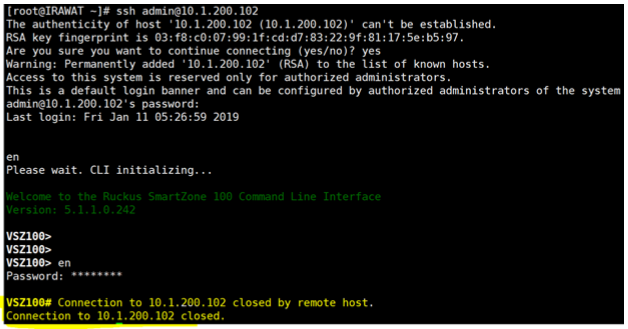
FIGURE 31 Sample Session Termination for Web Interface Session.



User Name ▲	Session ID	Authentication Type	IP Address	Last Access Time
admin	NSTaMeupwHESNMCu2lFtmsVGGlWWrkEp	WEB_GUI	10.45.182.62	2022/08/16 23:40:53

1 records « 1 »

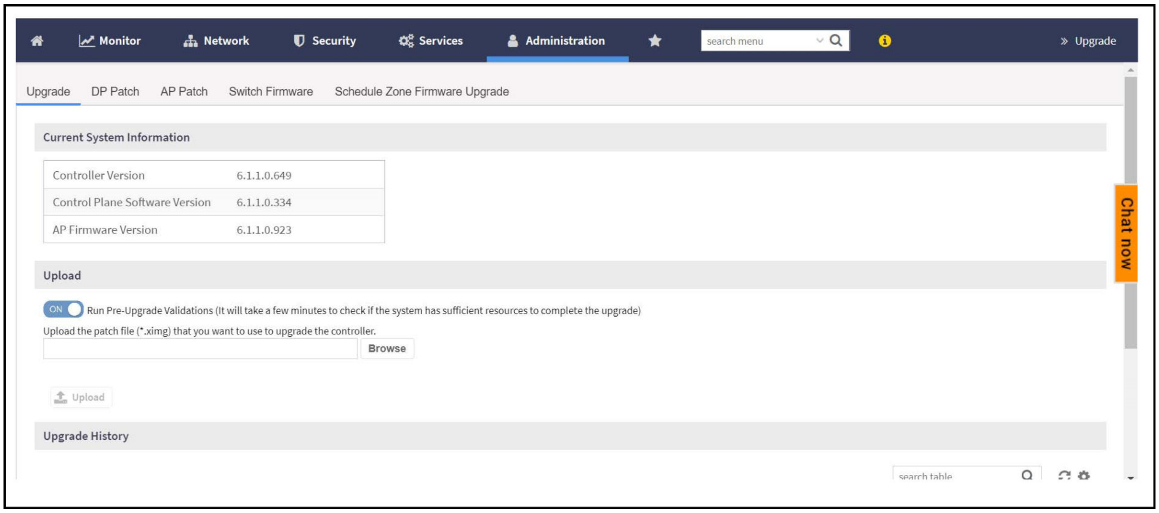
FIGURE 32 Sample Session Termination for CLI Session.



```
[root@IRAWAT ~]# ssh admin@10.1.200.102
The authenticity of host '10.1.200.102 (10.1.200.102)' can't be established.
RSA key fingerprint is 03:f8:c0:07:99:1f:cd:d7:83:22:9f:81:17:5e:b5:97.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.1.200.102' (RSA) to the list of known hosts.
Access to this system is reserved only for authorized administrators.
This is a default login banner and can be configured by authorized administrators of the system
admin@10.1.200.102's password:
Last login: Fri Jan 11 05:26:59 2019


en
Please wait. CLI initializing...

Welcome to the Ruckus SmartZone 100 Command Line Interface
Version: 5.1.1.0.242

VSZ100>
VSZ100>
VSZ100> en
Password: ********

VSZ100# Connection to 10.1.200.102 closed by remote host.
Connection to 10.1.200.102 closed.
```

4. Click the **Admin** icon in the upper right corner and select log off from the drop-down list.

FIGURE 33 Logging out from the UI



Current System Information

Controller Version	6.1.1.0.649
Control Plane Software Version	6.1.1.0.334
AP Firmware Version	6.1.1.0.923

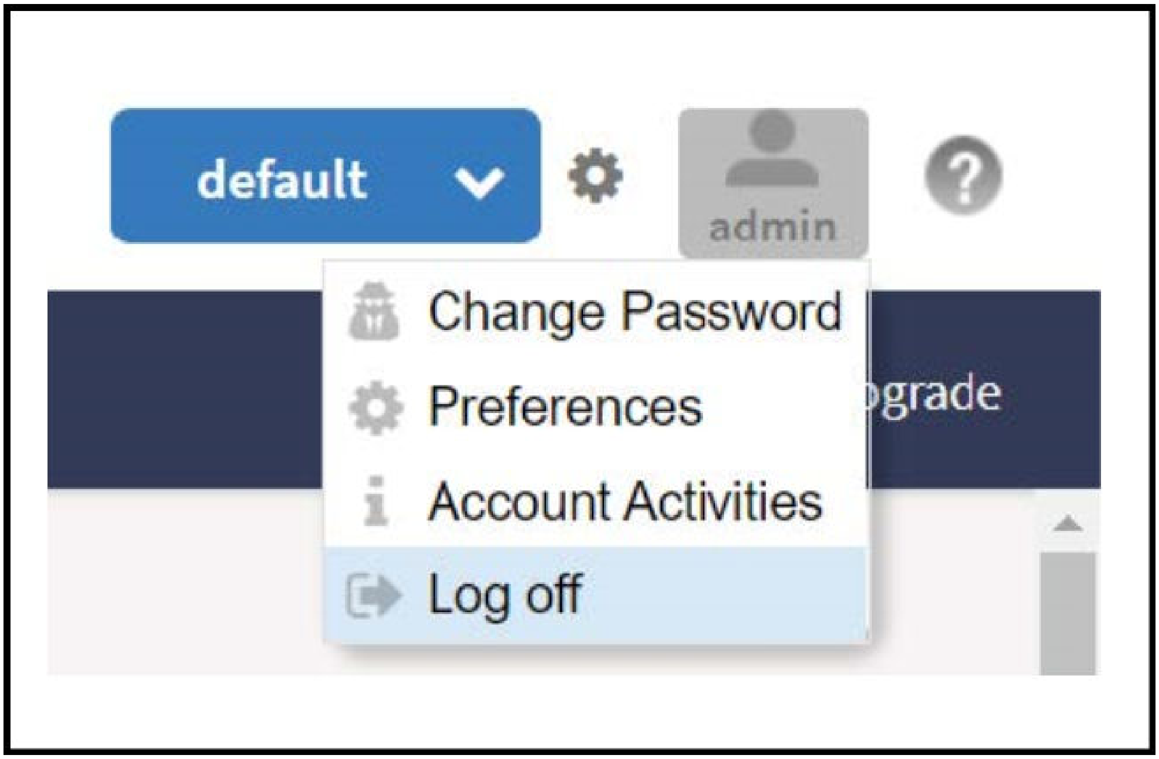
Upload

ON Run Pre-Upgrade Validations (It will take a few minutes to check if the system has sufficient resources to complete the upgrade)

Upload the patch file (*.ximg) that you want to use to upgrade the controller.

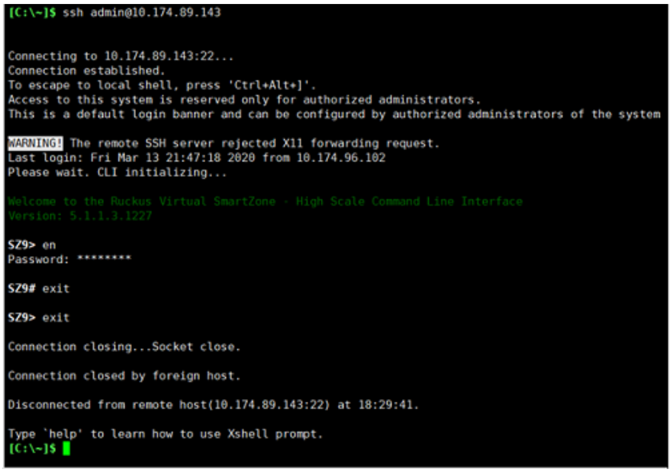
Upgrade History

FIGURE 34 Logging out from the UI Default



5. You can also logout by typing "exit" command in the SSH session.

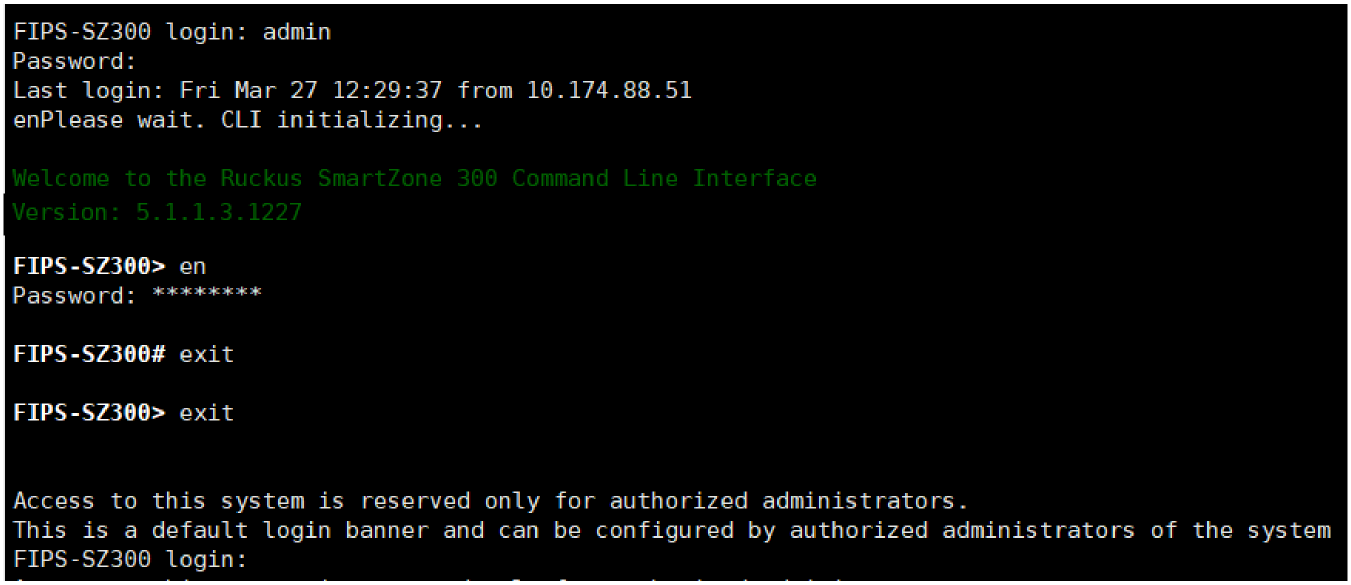
FIGURE 35 Logging out from the SSH session



```
[C:\~]$ ssh admin@10.174.89.143


Connecting to 10.174.89.143:22...
Connection established.
To escape to local shell, press 'Ctrl+Alt+]'.
Access to this system is reserved only for authorized administrators.
This is a default login banner and can be configured by authorized administrators of the system

WARNING! The remote SSH server rejected X11 forwarding request.
Last login: Fri Mar 13 21:47:18 2020 from 10.174.96.102
Please wait. CLI initializing...

Welcome to the Ruckus Virtual SmartZone - High Scale Command Line Interface
Version: 5.1.1.3.1227

SZ9> en
Password: ********

SZ9# exit

SZ9> exit

Connection closing...Socket close.

Connection closed by foreign host.

Disconnected from remote host(10.174.89.143:22) at 18:29:41.

Type `help' to learn how to use Xshell prompt.
[C:\~]$
```

6. You can also logout by typing " exit" command at the console prompt.

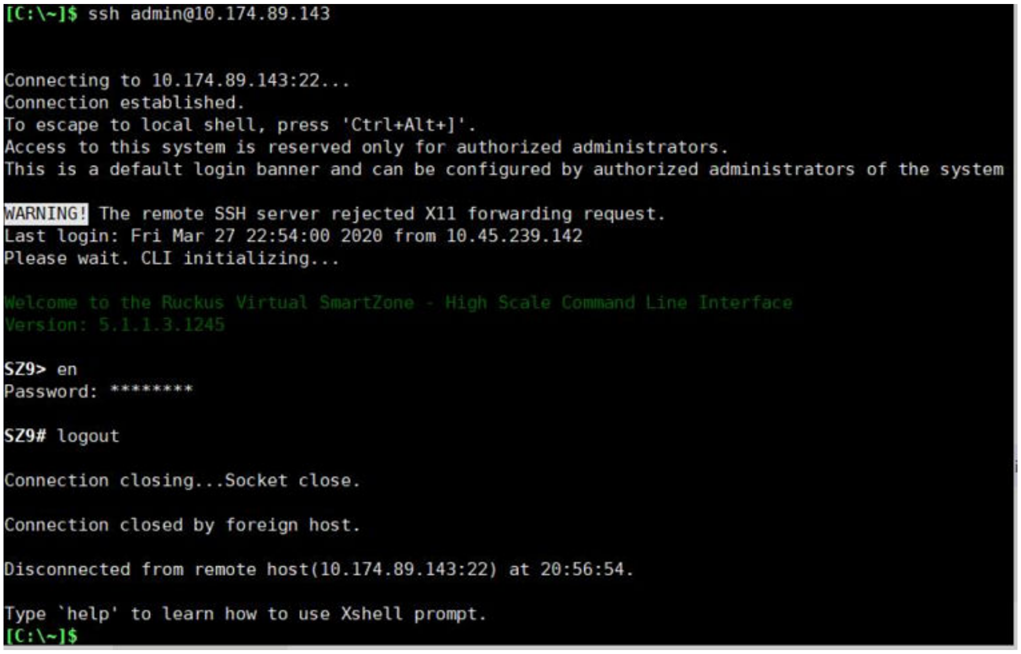
FIGURE 36 Logging out using the console prompt



```
FIPS-SZ300 login: admin
Password:
Last login: Fri Mar 27 12:29:37 from 10.174.88.51
enPlease wait. CLI initializing...

Welcome to the Ruckus SmartZone 300 Command Line Interface
Version: 5.1.1.3.1227

FIPS-SZ300> en
Password: ********

FIPS-SZ300# exit

FIPS-SZ300> exit


Access to this system is reserved only for authorized administrators.
This is a default login banner and can be configured by authorized administrators of the system
FIPS-SZ300 login:
```

7. You can also logout by typing "logout" at the CLI prompt

FIGURE 37 Logging out using CLI prompt



```
[C:\~]$ ssh admin@10.174.89.143


Connecting to 10.174.89.143:22...
Connection established.
To escape to local shell, press 'Ctrl+Alt+]'.
Access to this system is reserved only for authorized administrators.
This is a default login banner and can be configured by authorized administrators of the system

WARNING! The remote SSH server rejected X11 forwarding request.
Last login: Fri Mar 27 22:54:00 2020 from 10.45.239.142
Please wait. CLI initializing...

Welcome to the Ruckus Virtual SmartZone - High Scale Command Line Interface
Version: 5.1.1.3.1245

SZ9> en
Password: ********

SZ9# logout

Connection closing...Socket close.

Connection closed by foreign host.

Disconnected from remote host(10.174.89.143:22) at 20:56:54.

Type `help' to learn how to use Xshell prompt.
[C:\~]$
```

White Label Customization

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

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

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

1. From the **Dashboard**, Click the **Administration** tab.
2. From **Administration,** select **Admins and Roles**.
3. Click the **White Label Customizations** tab.

4. Set the **Enable Customization** button to ON.

   NOTE

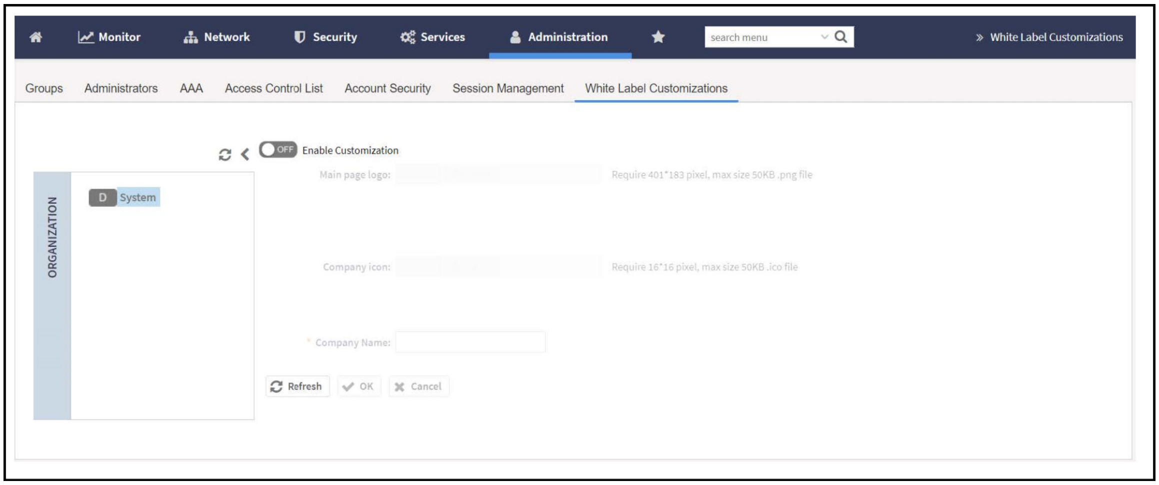
   The partner domain user can view only their own domain to configure logo, icon and name of the company.

   a) **Main page logo**: Click **Browse** to select the company logo.

   b) **Company icon**: Click **Browse** to select the company icon.

   c) **Company Name**: Enter the name of the company.

FIGURE 38 Enabling White Label Customization



OFF Enable Customization

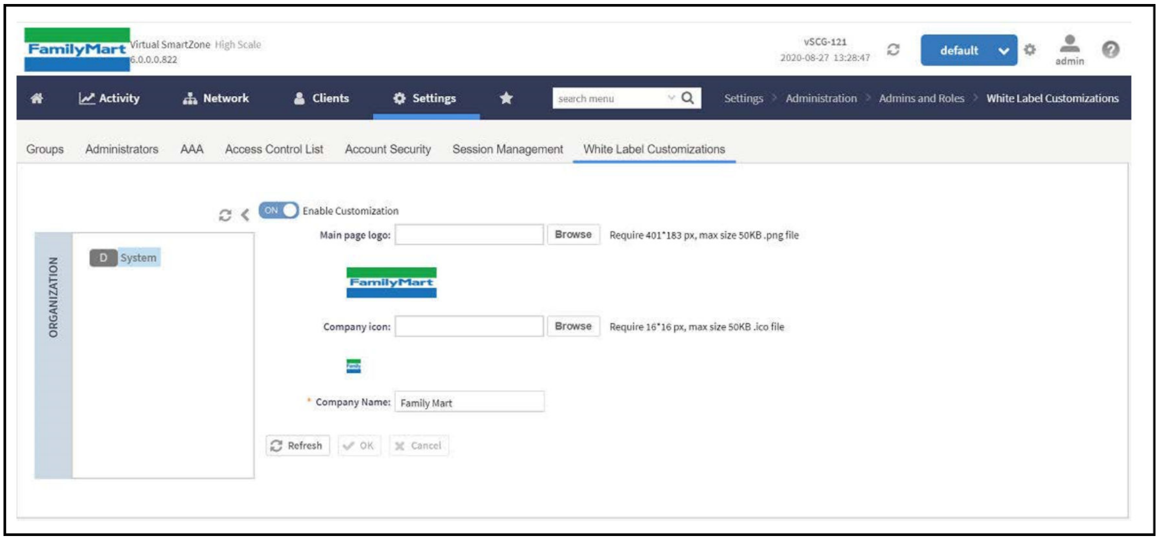
Main page logo: Require 401*183 pixel, max size 50KB .png file

Company icon: Require 16*16 pixel, max size 50KB .ico file

* Company Name:

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

FIGURE 39 New Logo Replaces Initial Logo



ON Enable Customization

Main page logo: Browse Require 401*183 px, max size 50KB .png file

Company icon: Browse Require 16*16 px, max size 50KB .ico file

* Company Name: Family Mart

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

Vendor-Specific Attribute (VSA) Profile

The SmartZone UI provides the VSA profile, where the user can define VSAs to be included in authentication and accounting messages. The AP receives the configuration from the Change and Configuration Management (CCM) and appends the VSAs to each user equipment (UE) authentication and accounting request and forwards the requests to the AAA server.

For HotSpot WISPr, the UE authentication is handled by the northbound Interface (NBI) where Real Application Clusters (RAC) appends the VSAs to the authentication messages and the AP appends the VSAs to the accounting messages.

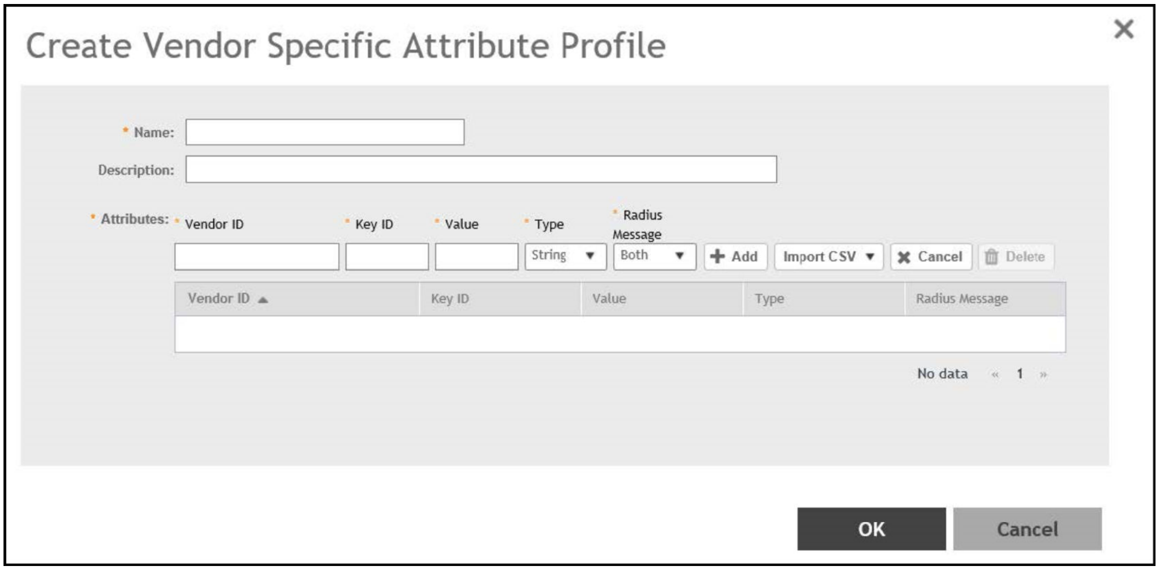
Creating a Vendor-Specific Attribute Profile

Perform the following procedure to add the VSAs in the RADIUS authentication and accounting messages.

1. Select **Services** > **Others** > **Vendor Specific Attribute**.
2. From the **Vendor Specific Attributes Profile** page, select the zone for which you want to create a VSA profile. and click **Create**.

   The **Create Vendor Specific Attribute Profile** page is displayed.

   FIGURE 40 Creating a Vendor-Specific Attribute Profile



3. Enter the profile name and description.

4. Under **Attributes**, define the VSA profile by completing the following steps:

   a) In the **Vendor ID** field, enter an integer from 1 through 65536.

      NOTE
      Do not configure the vendor IDs 25053 (Ruckus) and 14122 (WISPr) because they are reserved for internal use only. If you try to configure these vendor IDs, the system throws an error message.

   b) In the **Key ID** field, enter an integer from 0 through 255.

   c) In the **Value** field, enter an integer or string depending on the **Type** selected.

      NOTE
      The integer range is from 0 through 2147483647. The maximum length of a string is 247 characters.

   d) In the **Type** list, select from the following options:

      - **Integer**
      - **String**

   e) In the **Radius Message** list, select from the following options:

      - **Accounting**: The attributes defined in the VSA profile are included in the accounting messages.
      - **Authentication**: The attributes defined in the VSA profile are included in the authentication messages.
      - **Both**: The attributes defined in the VSA profile are included in both the accounting and authentication messages.

5. Click **Add** to add the VSA profile or click **Import CSV** to upload a CSV file containing multiple VSA profiles.

   NOTE
   To download a CSV template, click the **Import CSV** arrow and select **Download a CSV Sample**.

   The VSA profiles are added to the **Attributes** table. Check the VSA information in the **Attributes** table for any modifications.

   NOTE
   You can edit the VSAs by clicking the **Vendor ID** in the **Attributes** table.

   NOTE
   A maximum of 32 VSAs can be added to a VSA profile. A maximum of 4 VSA profiles can be configured for a zone.

6. Click **OK** to update the VSA profile to the database.

   NOTE
   To edit a VSA profile, select a VSA profile and click **Configure** in the **Vendor Specific Attribute Profile** page.

   NOTE
   To associate a VSA profile to a WLAN, refer to Associating a VSA Profile to a WLAN Configuration on page 77.

   NOTE
   You can also configure a VSA profile in the zone and WLAN templates. For more information, refer to *Working with Zone Templates* and *Working with WLAN Templates* respectively .

Associating a VSA Profile to a WLAN Configuration

Perform the following procedure to associate a VSA profile to a WLAN configuration.

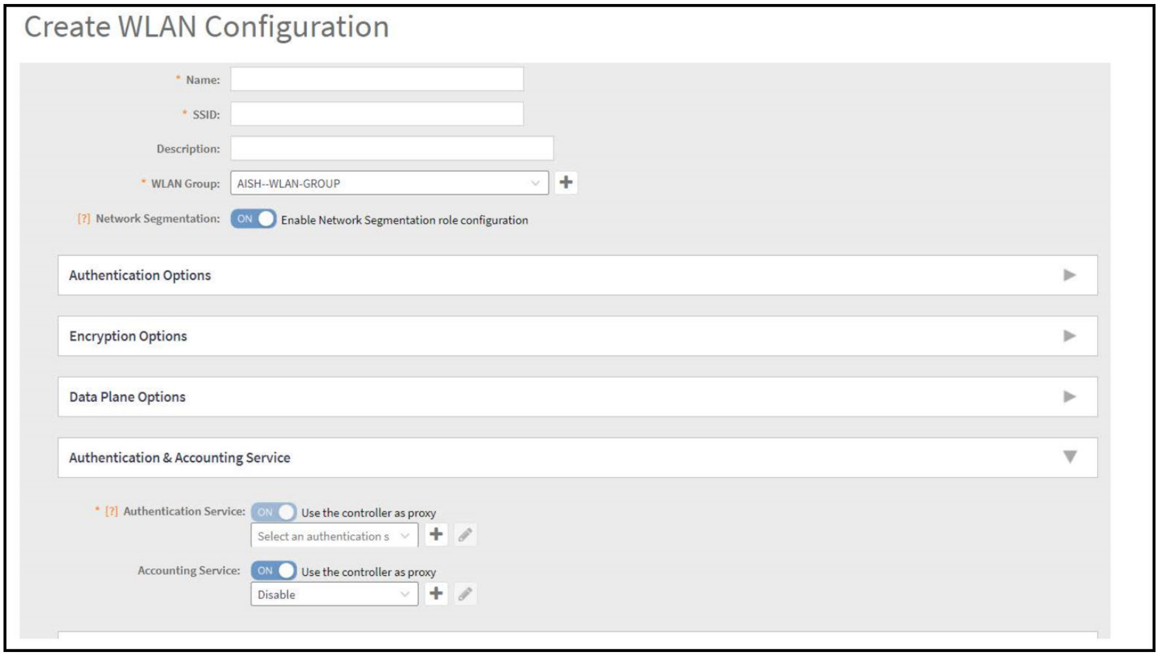
1. On the main menu, click **Network** > **Wireless LANs**.

   The **Wireless LANs** page is displayed.

2. Select the zone where the VSA profiles are created and click **Create**.

   The **Create WLAN Configuration** page is displayed.

   FIGURE 41 Creating a WLAN Configuration



Create WLAN Configuration

* Name:

* SSID:

Description:

* WLAN Group: AISH--WLAN-GROUP

[?] Network Segmentation: ON Enable Network Segmentation role configuration

Authentication Options ▶

Encryption Options ▶

Data Plane Options ▶

Authentication & Accounting Service ▼

* [?] Authentication Service: ON Use the controller as proxy
Select an authentication s

Accounting Service: ON Use the controller as proxy
Disable

3. Under **General Options**, enter the WLAN name and SSID.
4. Under **Authentication and Accounting Service**, complete the following steps:select the authentication service profile.
   a) Under **Authentication Service**, click **Use the controller as proxy** and select the authentication service profile.
   b) Under **Accounting Service**, click **Use the controller as proxy** and select the accounting service profile.
5. Under **Radius Options**, click **Vendor Specific Attribute Profile** and select a VSA profile.

   NOTE
   By default, **Vendor Specific Attribute Profile** is disabled.

   NOTE
   Click ✎ to configure the VSA profile.

6. Under **Advanced Options**, in **Access VLAN**, enter the VLAN ID.

   NOTE
   Enter an integer from 2 through 4094 for **VLAN ID**.

7. Click **OK**.

   NOTE

   The WLAN configuration is shown in the **Access Points** page for the zone where VSA profiles are created.

Global Filters Overview

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

Configuring Global Filters

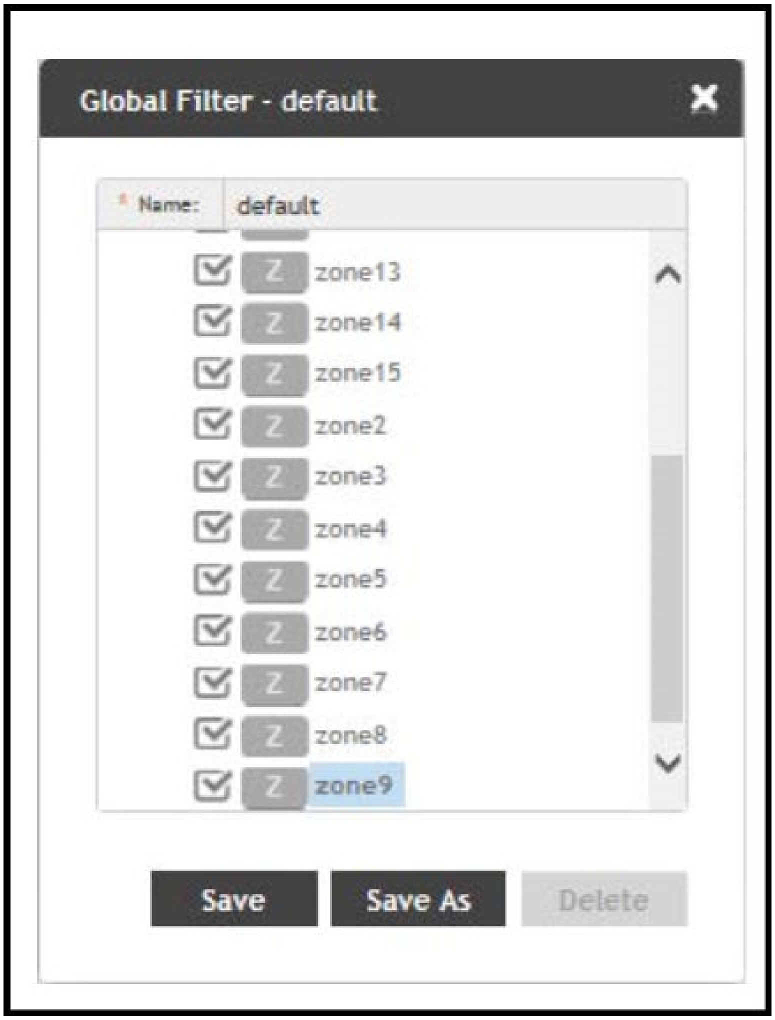
The Global filter setting allows you to set your preferred system filter.

To set the global filter follow the below steps.

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

   The below figure appears.

FIGURE 42 Global Filter Form



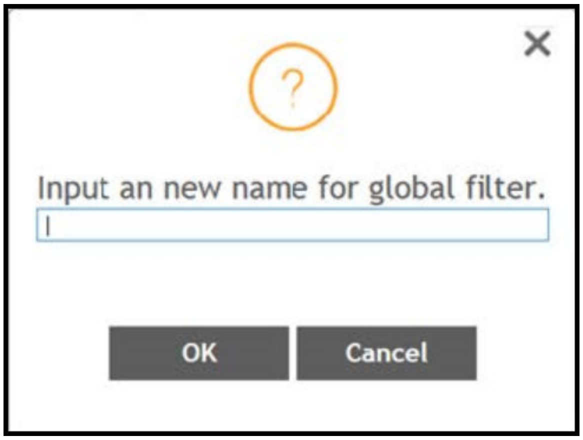
Global Filter - default

* Name: default

☑ Z zone13
☑ Z zone14
☑ Z zone15
☑ Z zone2
☑ Z zone3
☑ Z zone4
☑ Z zone5
☑ Z zone6
☑ Z zone7
☑ Z zone8
☑ Z zone9

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

FIGURE 43 New Name Form



Input an new name for global filter.

NOTE

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

Backup and Restore

Cluster

Administrating the Cluster

SmartZone Cluster Mode

SmartZone system state has two cluster modes.

The two cluster modes are -

- Crash mode
- Suspend mode

Crash mode

The system cluster enters this mode when system meets unexpected error during fresh install or reboot flow. The system runs into ir-recoverable error and should be set to reset-factory settings.

System enters into *Crash mode* in any one of the below conditions:

1. System reboot with environment inconsistency.
   a. Model
   b. Port group (SZ 100)
   c. Firmware Version
2. Fresh install fail.
3. Join cluster fail.

Suspend mode

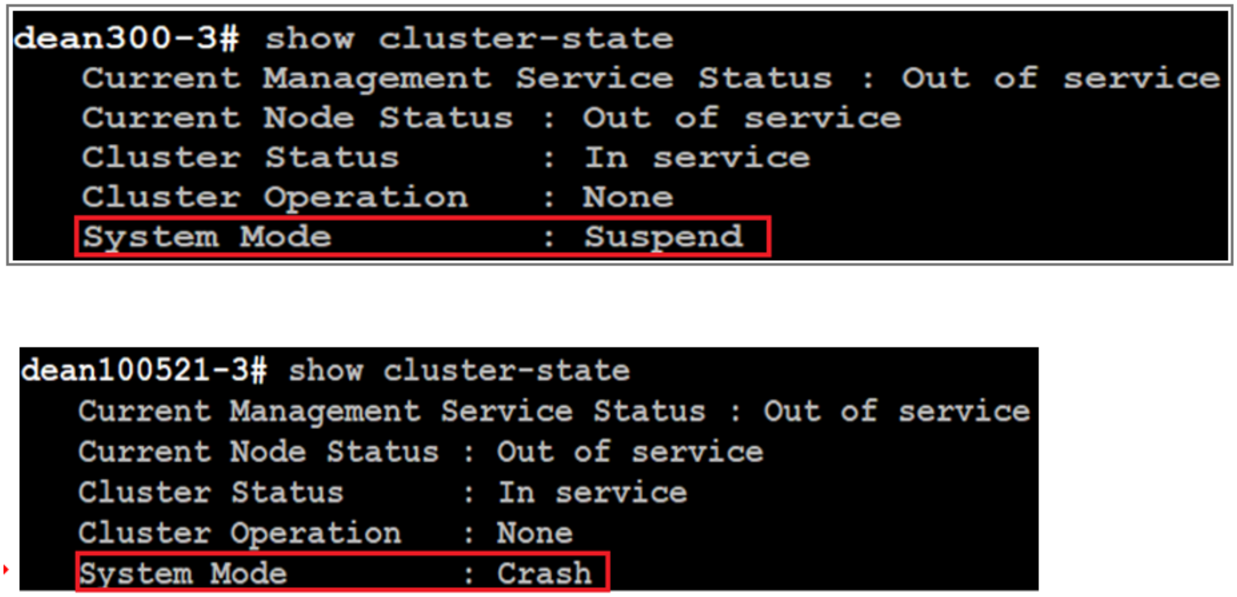
The system enters this mode if there is an environment error during reboot flow. The configurer sets up suspend flag and stops all applications. The system can be recoved by rebooting as it is a temporary fail.

System enters into *Suspend mode* in any one of the below conditions:

1. Platform applications cannot be launched successfully.
2. Failed on membership authentication in cluster .

To check status of the cluster state, use **show cluster-state** command.

FIGURE 44 Crash and Suspended modes

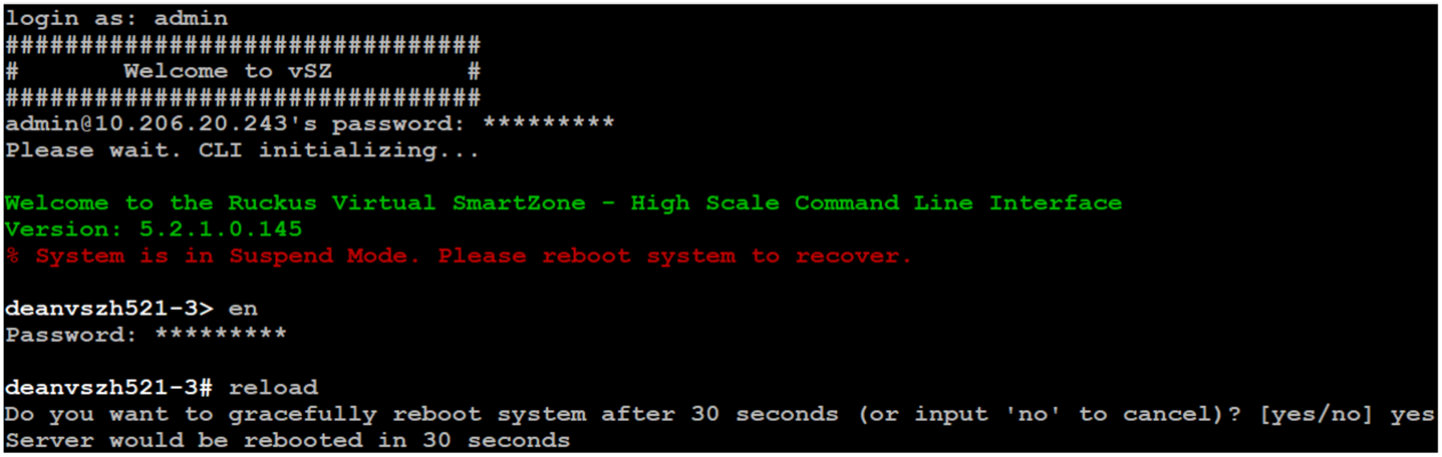


```
dean300-3# show cluster-state
   Current Management Service Status : Out of service
   Current Node Status : Out of service
   Cluster Status          : In service
   Cluster Operation       : None
   System Mode             : Suspend
```

```
dean100521-3# show cluster-state
   Current Management Service Status : Out of service
   Current Node Status : Out of service
   Cluster Status       : In service
   Cluster Operation    : None
   System Mode          : Crash
```

To recover system in case of *Suspend mode*, use **reload** command. System automatically detects suspend flag and clears before launching applications.

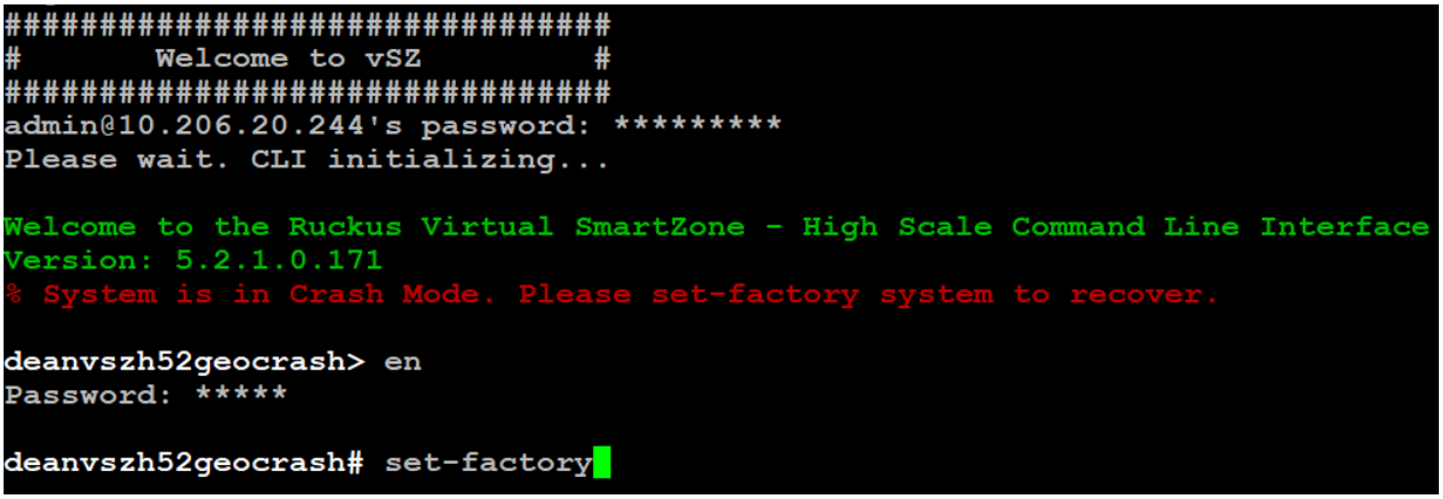
FIGURE 45 reload



```
login as: admin
################################
#       Welcome to vSZ         #
################################
admin@10.206.20.243's password: *********
Please wait. CLI initializing...

Welcome to the Ruckus Virtual SmartZone - High Scale Command Line Interface
Version: 5.2.1.0.145
% System is in Suspend Mode. Please reboot system to recover.

deanvszh521-3> en
Password: *********

deanvszh521-3# reload
Do you want to gracefully reboot system after 30 seconds (or input 'no' to cancel)? [yes/no] yes
Server would be rebooted in 30 seconds
```

To reset system to factory settings in case of *Crash mode*, use **set-factory** command.

FIGURE 46 set-factory



```
################################
#       Welcome to vSZ         #
################################
admin@10.206.20.244's password: *********
Please wait. CLI initializing...

Welcome to the Ruckus Virtual SmartZone - High Scale Command Line Interface
Version: 5.2.1.0.171
% System is in Crash Mode. Please set-factory system to recover.

deanvszh52geocrash> en
Password: *****

deanvszh52geocrash# set-factory
```

Disaster Recovery

Creating cluster backup and restoring cluster configurations periodically helps manage disaster recovery.

Backing up Cluster Configuration

RUCKUS strongly recommends that you back up the controller database periodically. This will help ensure that you can restore the system configuration settings easily if the database becomes corrupted for any reason.

The following are backed up in the system configuration backup file:

TABLE 15 Contents of a cluster configuration backup file

Configuration Data	Administration Data	Report Data	Identity Data
AP zones	Cluster backup	Saved reports	Created profiles
Third-party AP zones	System configuration backups	Historical client statistics	Generated guest passes
Services and profiles	Upgrade settings and history	Network tunnel statistics	
Packages	Uploaded system diagnostic scripts		
System settings	Installed licenses		
Management domains			
Administrator accounts			
MVNO accounts			

A system configuration backup does not include control plane settings, data plane settings, and user-defined interface settings.

1. Go to **Administration** > **Administration** > **Backup and Restore**.
2. Select the **Configuration** tab.
3. In System Configuration Backup History, click **Backup**.

   The following confirmation message appears: `Are you sure you want to back up the controller's configuration?`

4. Click **Yes**.

   A progress bar appears as the controller creates a backup of the its database. When the backup process is complete, the progress bar disappears, and the backup file appears under the **System Configuration Backup History** section.

   > **NOTE**
   > The system will limit the configuration backup to 5 scheduled and 50 Manual backup files.

Scheduling a Configuration Backup

You also have the option to configure the controller to backup its configuration automatically based on a schedule you specify.

1. Go to **Administration** > **Administration** > **Backup and Restore**.
2. Select the **Configuration** tab.
3. In Schedule Backup, you can configure the controller to backup its configuration automatically based on a schedule you specify.
   a. In Schedule Backup, click **Enable**.
   b. In Interval, set the schedule when the controller will automatically create a backup of its configuration. Options include: Daily, Weekly and Monthly.
   c. Hour: Select the hour of the day when the controller must generate the backup.
   d. Minute: Select the minute of the hour.
   e. Click **OK**.

Exporting the Configuration Backup to an FTP Server Automatically

In addition to backing up the configuration file manually, you can configure the controller to export the configuration file to an FTP server automatically whenever you click **Backup**.

Follow these steps to back up the configuration file to an FTP server automatically.

1. Go to **Administration** > **Administration** > **Backup and Restore**.
2. Select the **Configuration** tab.
3. In Auto Export Backup, you can configure the controller to export the configuration file to an FTP server automatically whenever you back up the configuration file.
   a. In Auto Export Backup, click **Enable**. In the **Name prefix** field, type the prefix name of the backup file. The maximum length of the prefix name must not be more than 32 characters.
   b. FTP Server: Select the FTP server to which you want to export the backup file.
   c. Click **Test**. The controller attempts to establish connection to the FTP server using the user name and password that you supplied. If the connection attempt is successful, a success message is displayed. If the connection attempt is unsuccessful, verify that the FTP server details (including the user name and password) are correct, and then click **Test** again.
   d. Click **OK**.
4. After you verify the controller is able to connect to the FTP server successfully, click **OK** to save the FTP server settings.

Downloading a Copy of the Configuration Backup

After you create a configuration backup, you have the option to download the backup file from the **System Configuration Backups History** section.

1. Go to **Administration** > **Administration** > **Backup and Restore**.
2. Select the **Configuration** tab.

3. Locate the entry for the backup file that you want to download. If multiple backup files appear on the list, use the date when you created the backup to find the backup entry that you want.
4. Click **Download**.

   Your web browser downloads the backup file to its default download folder. NOTE: When your web browser completes downloading the backup file, you may see a notification at the bottom of the page.
5. Check the default download folder for your web browser and look for a file that resembles the following naming convention: **[Name prefix]_Configuration_[datetime]_[Version].bak**

   The controller will combine the prefix name with the date and time stamp to generate the filename for automatic backup. For example, RUCKUS_Configuration_20200902071625GMT_6.0.0.0.817.bak.

Restoring a System Configuration Backup

In the event of a failure or emergency where you may need to go back to the previous version of a cluster, you will have to restore your system configuration backup and restart the cluster.

1. Go to **Administration** > **Administration** > **Backup and Restore**.
2. Select the **Configuration** tab.
3. Once you locate the backup file, click **Restore** that is in the same row as the backup file. A confirmation message appears.

   > **NOTE**
   > Take note of the backup version that you are using. At the end of this procedure, you will use the backup version to verify that the restore process was completed successfully.

4. Click **Yes**. The following message appears: `System is restoring. Please wait...` When the restore process is complete, the controller logs you off the web interface automatically.
5. Log on to the controller web interface.

   Check the web interface pages and verify that the setting and data contained in the backup file have been restored successfully to the controller.

Creating a Cluster Backup

Backing up the cluster (includes OS, configuration, database and firmware) periodically enables you to restore it in the event of an emergency. RUCKUS also recommends that you back up the cluster before you upgrade the controller software.

1. Go to **Administration** > **Administration** > **Backup and Restore**.
2. Select the **Cluster** tab.
3. In Cluster Backup and Restore, click **Backup Entire Cluster** to backup both nodes in a cluster.

   The following confirmation message is displayed: `Are you sure you want to back up the cluster?`
4. Click **Yes**.

   The following message is displayed: `The cluster is in maintenance mode. Please wait a few minutes.`

   When the cluster backup process is complete, a new entry is displayed in the **Cluster Backups History** section with a **Created On** value that is approximate to the time when you started the cluster backup process.

Restoring a Cluster Backup

You must be able to restore a cluster to its previous version in the case of a failure.

1. Go to **Monitor** > **Troubleshooting&Diagnostics** > **Application Logs**.
2. Select the **Cluster** tab.
3. In Cluster Backup History, select the cluster and click **Restore**.

   The following confirmation message appears:

   ```
   Are you sure you want to restore the cluster?
   ```
4. Click **Yes**.

   The cluster restore process may take several minutes to complete. When the restore process is complete, the controller logs you off the web interface automatically.

   > **ATTENTION**
   > Do not refresh the controller web interface while the restore process is in progress. Wait for the restore process to complete successfully.

5. Log on to the controller web interface.

   If the web interface displays the message `Cluster is out of service. Please try again in a few minutes` appears after you log on to the controller web interface, wait for about three minutes. The dashboard will appear shortly. The message appears because the controller is still initializing its processes.
6. Go to **Administration** > **Upgrade**, and then check the **Current System Information** section and verify that all nodes in the cluster have been restored to the previous version and are all in service.
7. Go to **Diagnostics** > **Application Logs**, and then under **Application Logs & Status** check the **Health Status** column and verify that all of the controller processes are online.

Replacing a Controller Node

Replacing a Controller Node in Single Node Cluster

This section describes how to replace a controller node in single node cluster. Original configuration backup and a new node are required.

Step 1: Wipe-out Upgrade Controller Node

If the Controller node does not match with the existing cluster version, prepare a new Controller and wipe-out upgrade to the same version of the running cluster. See Performing a Wipe-out Upgrade for Controller Node on page 90.

Step 2: Join New Controller Node

Set up the node as a new controller. For step by step instructions, see the *Getting Started Guide*.

Step 3: Configuration Restore

With original configuration backup follow the steps to restore the configuration in cluster:

1. Prepare the new controller to which you will restore the cluster backup.
   a. Either obtain a new controller or factory reset an existing controller.
   b. Log on to the controller as a system administrator.
   c. Run the setup command to configure the controller's network settings.
   d. Complete the controller setup process from the **CLI**.
2. After you complete the controller setup, log on to the controller web interface as a system administrator.
3. Go to **Administration** > **Administration**>**Backup and Restore**.

   NOTE
   For SmartZone 5.2.1 or earlier releases, select **Administration** > **Backup and Restore**.

4. Select the **Configuration** tab.
5. Click **Upload**. After the configuration file is uploaded successfully, it appears in the Configuration section.
6. Restore the configuration backup to the node either using the web interface or the **CLI**.
   - To use the web interface:
     a. Go to **Administration** > **Backup and Restore** page.
     b. In the **Configuration** tab, locate the configuration backup file that you want to restore.
     c. Click **Restore**.
     d. Follow the prompts (if any) to complete the restore process.
   - To use the **CLI**:
     a. Log on to the **CLI** of the node as a system administrator.
     b. Run the **restore config** command.

Replacing a Controller Node in Multi-Node Cluster

This section describes how to replace a controller node in a multi-node cluster. Removing a node and joining a new node is the standard process to replace a node.

Step 1: Wipe-out Upgrade Controller Node

If the Controller node does not match with the existing cluster version, prepare a new Controller and wipe-out upgrade to the same version of the running cluster. See Performing a Wipe-out Upgrade for Controller Node on page 90.

Step 2: Remove RMA Controller Node

Choose a controller that will remain in the cluster and follow the steps:

1. Log on to the web interface of the chosen controller using administrator credentials.
2. Go to **Network** > **Data and Control Plane**>**Cluster** and locate the node that you want to replace in the cluster planes.

   NOTE
   For SmartZone 5.2.1 or earlier releases, select **System** > **Cluster**.

3. Click **Delete** to remove the node from the cluster.

Step 3: Join the New Controller Node

To join the new controller into the running cluster:

1. Prepare a proper version of the controller by wipe-out upgrade. See Performing a Wipe-out Upgrade for Controller Node on page 90.
2. Set up the node as a new controller, and then join the existing cluster. For step by step instructions, refer to the *Getting Started Guide*.

Performing a Wipe-out Upgrade for Controller Node

If the firmware version on this controller (shown in the Cluster Information page) does not match the firmware version for new cluster setup or join an existing, a message appears and prompts you to upgrade the controller's firmware. Click **Upgrade**, and then follow the prompts to perform the upgrade.

> **NOTE**
> Refer Cautions & Limitations of Administrating a Cluster on page 230 for more information.

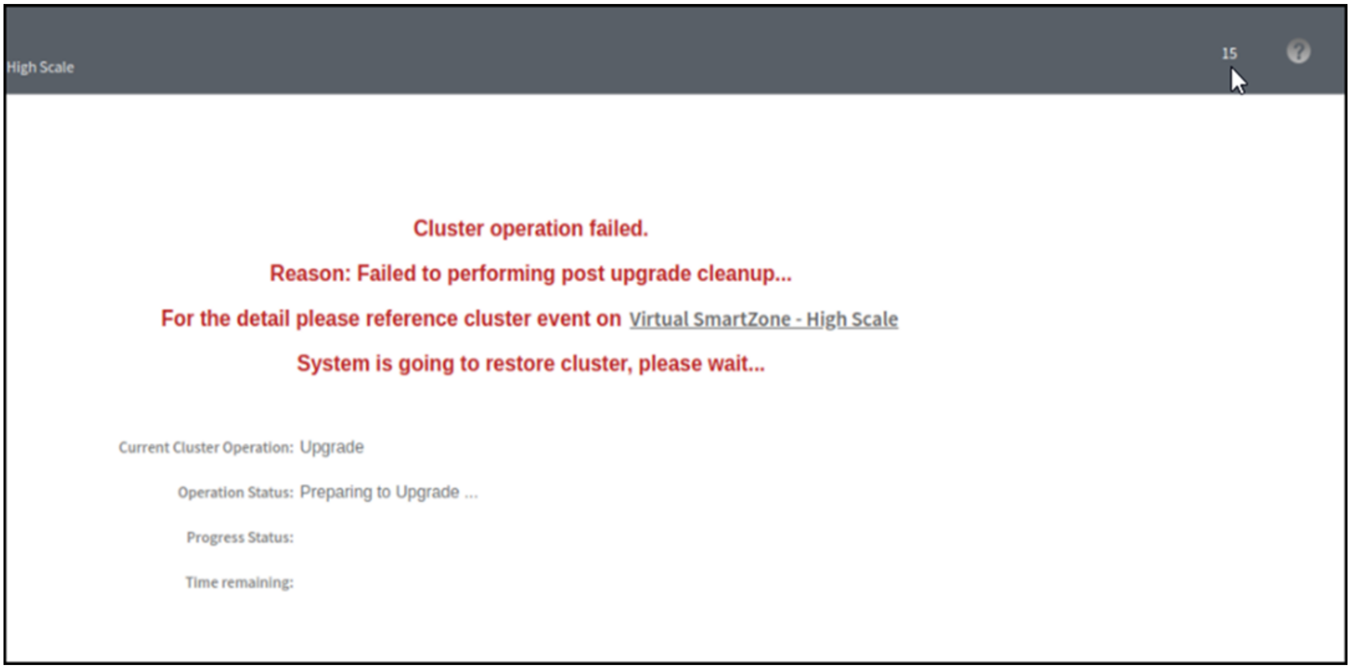
- For controller running firmware version 5.1 or later can do wipe-out upgrade successfully to greater than 5.1.
- For controller running firmware version earlier than 5.1, apply a KSP patch to make wipe-out upgrade successful Contact Ruckus support to receive a KSP patch to apply the patch from CLI.

Restoring a Cluster Automatically on Upgrade Failure

When cluster upgrade fails in the middle, the system will automatically restore the cluster with the backup file prepared in the beginning of the upgrade process and goes back to previous version of the image. The user does not need to manually restore the cluster.

When the cluster fails to upgrade and a restore action is triggered, the system performs the following process:

Starting a restore process



Cluster operation failed.

Reason: Failed to performing post upgrade cleanup...

For the detail please reference cluster event on Virtual SmartZone - High Scale

System is going to restore cluster, please wait...

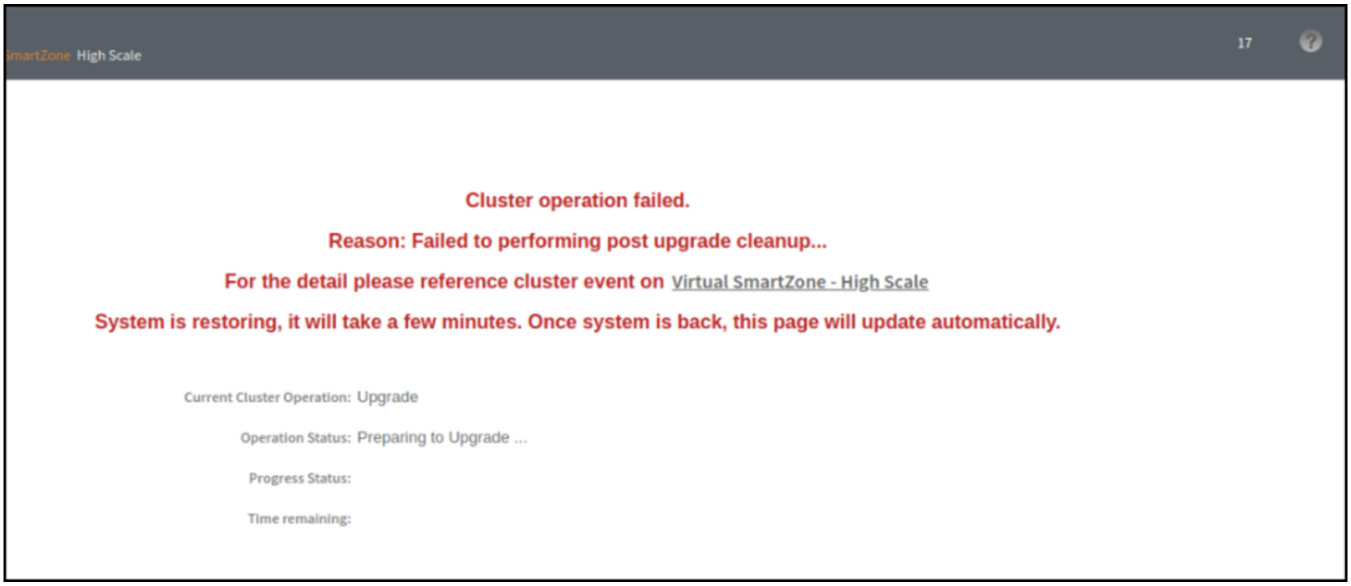
Current Cluster Operation: Upgrade

Operation Status: Preparing to Upgrade ...

Progress Status:

Time remaining:

Restoring cluster



Cluster operation failed.

Reason: Failed to performing post upgrade cleanup...

For the detail please reference cluster event on Virtual SmartZone - High Scale

System is restoring, it will take a few minutes. Once system is back, this page will update automatically.

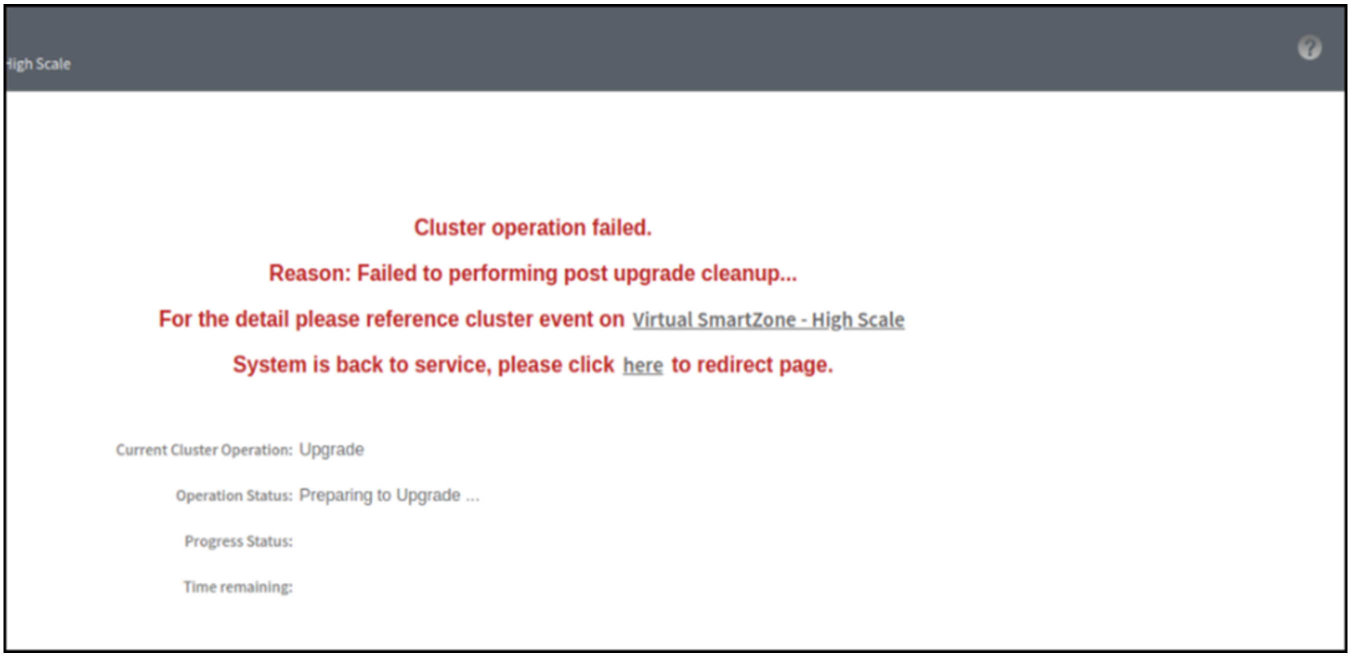
Current Cluster Operation: Upgrade

Operation Status: Preparing to Upgrade ...

Progress Status:

Time remaining:

Cluster back to service



Cluster operation failed.

Reason: Failed to performing post upgrade cleanup...

For the detail please reference cluster event on Virtual SmartZone - High Scale

System is back to service, please click here to redirect page.

Current Cluster Operation: Upgrade

Operation Status: Preparing to Upgrade ...

Progress Status:

Time remaining:

Configuration

Backed Up Configuration Information

The following list show which configuration information will be backing up.

- AP zones
- AP zone global configuration
- Zone templates
- WLAN templates
- AP registration rules
- Access point information
- General system settings
- Web certificate
- SNMP agent
- Alarm to SNMP agent
- Cluster planes
- Management interface ACL
- Domain information
- User credentials and information
- Mobile Virtual Network Operators (MVNO) information

Backing Up and Restoring Configuration

Configuration backup creates a backup of all existing configuration information on the controller. In additional to backing up a different set of information, configuration backup is different from cluster backup in a few ways:

- The configuration backup file is smaller, compared to the cluster backup file.
- The controller can be configured to back up its configuration to an external FTP server automatically.
- Configuration backup does not back up any statistical files or general system configuration.

Backing Up Configuration

There are two methods you can use to back up the controller configuration:

- Backing Up Configuration from the CLI on page 92
- Backing Up Configuration from the Web Interface on page 93

Backing Up Configuration from the CLI

There are two methods you can use to back up the controller configuration either using the web interface or CLI (Command Line Interface).

Follow these steps to back up the controller configuration from the **CLI**.

1. Log on to the controller **CLI** as a system administrator.

2. Run the **enable** command to enable privileged mode on the **CLI**.

   ```
   ruckus> enable
   Password: ********
   ruckus#
   ```

3. Run the **backup config** command to start backing up and transferring the node configuration to an FTP server.

   ```
   ruckus# backup config <ftp-username> <ftp-password> <ftp-server-address> <ftp-server-port>
   Do you want to backup configuration (yes/no)? yes
   Backup Configuration process starts
   Backup Configuration process has been scheduled to run. You can check backup version using 'show
   backup-config'
   ```

4. Run the **show backup-config** command to verify that the backup file has been created.

Backing Up Configuration from the Web Interface

1. For information on how to back up the controller configuration to an external FTP server automatically, see Backing up Cluster Configuration on page 85.
2. In **Auto Export Backup**, click **Enable**.
3. In FTP Server, select the FTP server to which you want to export the backup file.
4. Click **Test**. The controller attempts to establish connection to the FTP server using the user name and password that you supplied. If the connection attempt is successful, the following message appears: `FTP server connection established successfully.`

   If the connection attempt is unsuccessful, verify that the FTP server details (including the user name and password) are correct, and then click **Test** again.
5. After you verify the controller is able to connect to the FTP server successfully, click **OK** to save the FTP server settings.

Backing Up and Restoring the Controller's Network Configuration from an FTP Server

In addition to backing up and restoring the controller's network configuration from its own database, the controller supports backup and restore of its network configuration from an FTP server using the CLI.

This section describes the requirements for backing up and restoring the controller's network configuration from an FTP server, the information that is included in the backup file, and how to perform the backup and restore process.

To back up and restore the controller's network configuration from an FTP server, the controller must have already been set up and in service. In case of a multi-node cluster, all the nodes in the cluster must be in service.

The following table lists the network configuration that is backed up from the control and data planes when you perform a backup procedure to an FTP server.

TABLE 16 Information that is backed up to the FTP server

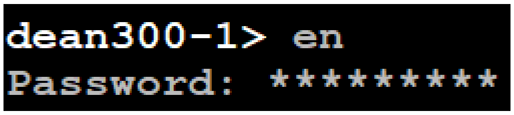
Control Plane	Data Plane
• Control interface • Cluster interface • Management interface • Static routes • User-defined interfaces	• Primary interface • Static routes • Internal subnet prefix

Backing Up to an FTP Server

Follow these steps to back up the controller network configuration to an FTP server.

1. Log on to the controller from the controller's command line interface (CLI). For more information, see the corresponding *Command Line Interface Reference Guide* for your controller platform.
2. At the prompt, enter **en** to enable privileged mode.

   FIGURE 47 Enable privileged mode

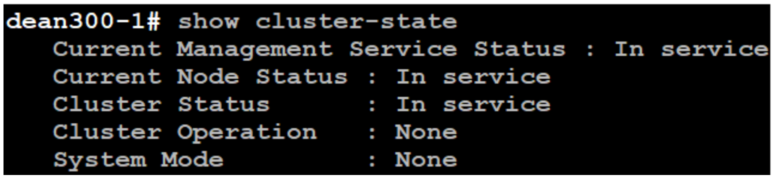


```
dean300-1> en
Password: *********
```

3. Enter - to display the statuses of the node and the cluster.

   Before continuing to the next step, verify that both the node and the cluster are in service.

   FIGURE 48 Verify that both the node and the cluster are in service

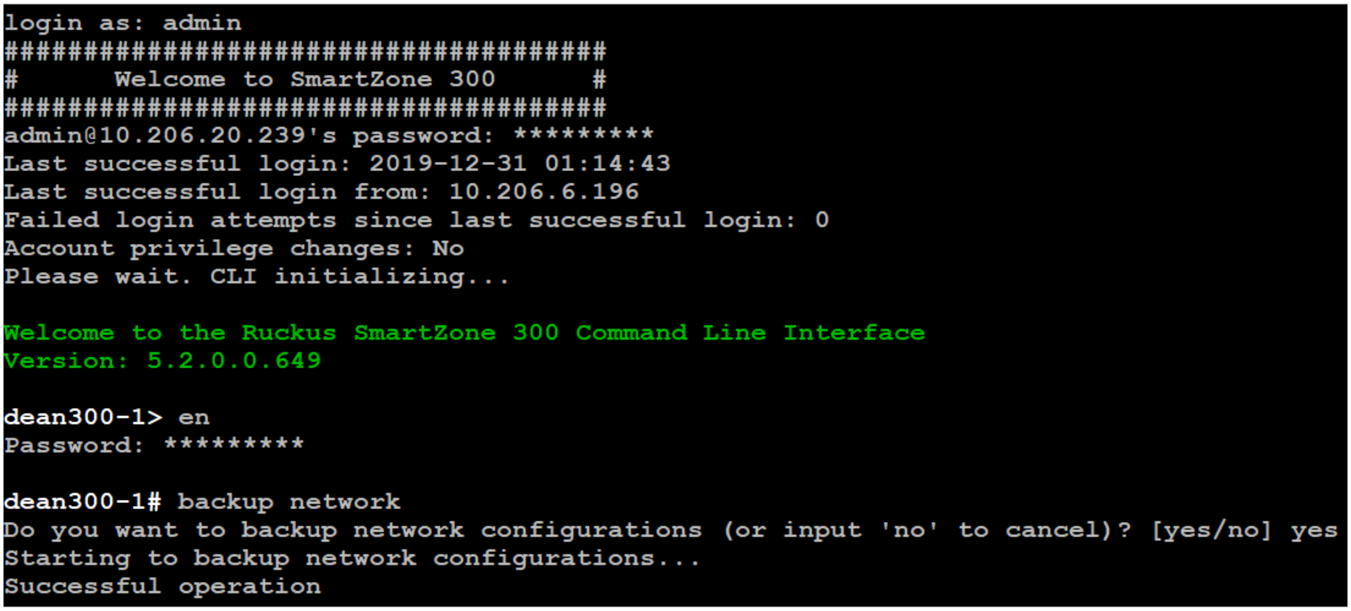


```
dean300-1# show cluster-state
   Current Management Service Status : In service
   Current Node Status : In service
   Cluster Status       : In service
   Cluster Operation    : None
   System Mode          : None
```

4. Enter backup network to back up the controller network configuration, including the control plane and data plane information.

   The controller creates a backup of its network configuration on its database.

   FIGURE 49 Run backup network

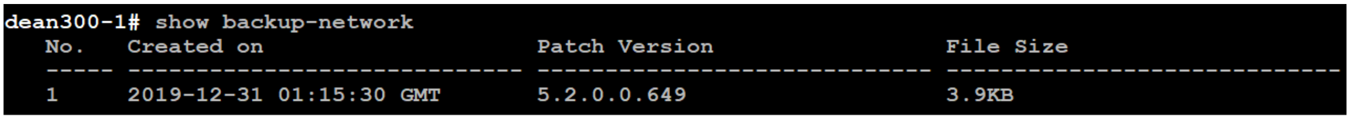


```
login as: admin
#######################################
#      Welcome to SmartZone 300      #
#######################################
admin@10.206.20.239's password: *********
Last successful login: 2019-12-31 01:14:43
Last successful login from: 10.206.6.196
Failed login attempts since last successful login: 0
Account privilege changes: No
Please wait. CLI initializing...

Welcome to the Ruckus SmartZone 300 Command Line Interface
Version: 5.2.0.0.649

dean300-1> en
Password: *********

dean300-1# backup network
Do you want to backup network configurations (or input 'no' to cancel)? [yes/no] yes
Starting to backup network configurations...
Successful operation
```

5. Enter show backup-network to view a list of backup files that have been created.

   Verify that the **Created On** column displays an entry that has a time stamp that is approximate to the time you started the backup.

   FIGURE 50 Enter the show backup-network command

   ```
   dean300-1# show backup-network
      No.   Created on                     Patch Version                  File Size
      ----- ------------------------------ ------------------------------ ------------------------------
      1     2019-12-31 01:15:30 GMT        5.2.0.0.649                    3.9KB
   ```

6. Enter **copy backup-network *{ftp-url}***, where *{ftp-url}* (remove the braces) is the URL or IP address of the FTP server to which you want to back up the cluster configuration.

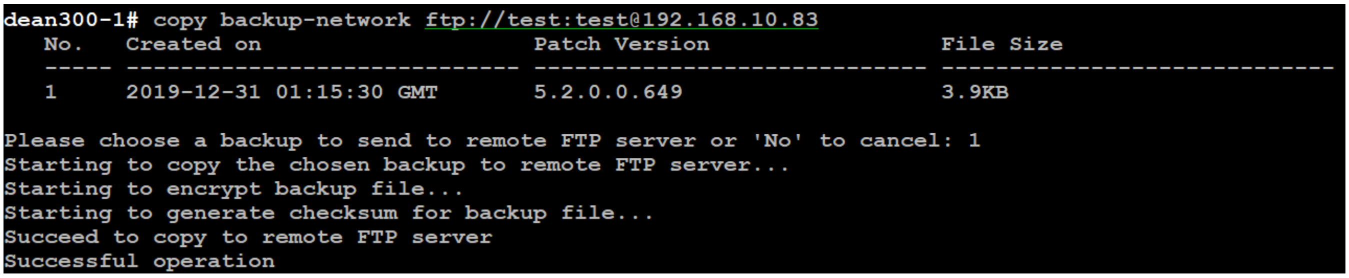
   The **CLI** prompts you to choose the number that corresponds to the backup file that you want to export to the FTP server.

7. Enter the number of the backup file that you want to export to the FTP server.

   The controller encrypts the backup file, and then exports it to the FTP server. When the export process is complete, the following message appears on the **CLI**:

   ```
   Succeed to copy to remote FTP server
   Successful operation  indicates that you have exported the backup file to the FTP server
   successfully
   ```

   FIGURE 51 `Succeed to copy to remote FTP server`

   ```
   dean300-1# copy backup-network ftp://test:test@192.168.10.83
      No.   Created on                     Patch Version                  File Size
      ----- ------------------------------ ------------------------------ ------------------------------
      1     2019-12-31 01:15:30 GMT        5.2.0.0.649                    3.9KB

   Please choose a backup to send to remote FTP server or 'No' to cancel: 1
   Starting to copy the chosen backup to remote FTP server...
   Starting to encrypt backup file...
   Starting to generate checksum for backup file...
   Succeed to copy to remote FTP server
   Successful operation
   ```

8. Using an FTP client, log on to the FTP server, and then verify that the backup file exists.

   The file format of the backup file is `network_<YYYYMMDDHHmmss>_<controller-version>.bak`.

   For example, if you created the backup file on October 24th 2013 at 02:40:22 and the controller version is 2.5.0.0.402, you should see a file named `network_20131024024022_2.5.0.0.402.bak` on the FTP server.

Restoring from an FTP Server

Before you continue, take note of the following limitations with restoring a backup file of the controller network configuration from an FTP server:

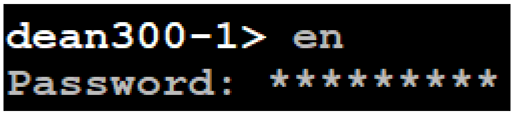
- Only release 2.1 and later support restoring from an FTP server.
- In this current release, restoring the entire cluster from an FTP server is unsupported. The restore process must be performed on one node at a time.
- Restoring from an FTP server can only be performed using the **CLI**.

CAUTION
Restoring a backup file to the controller requires restarting all of the controller services.

Follow these steps to restore a backup file of the controller's network configuration that you previously uploaded to an FTP back to the controller.

1. Log on to the controller from the **CLI**. For more information, see the corresponding *Command Line Interface Reference Guide* for your controller platform.
2. At the prompt, enter **en** to enable privileged mode.

   FIGURE 52 Enable privileged mode

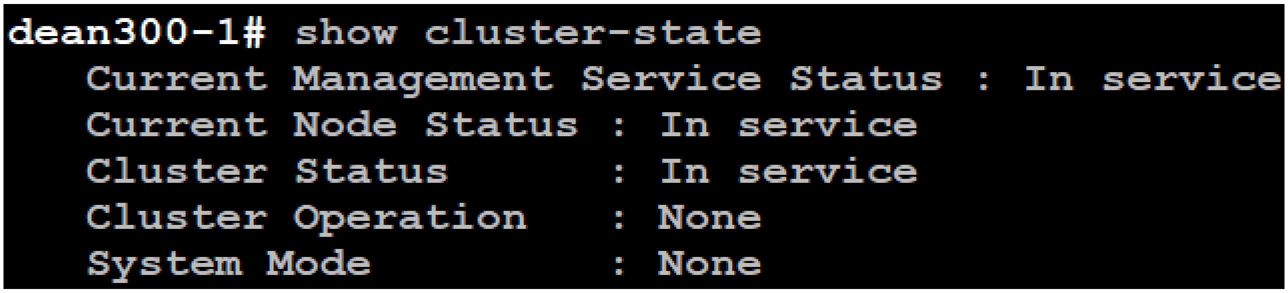
   

   ```
   dean300-1> en
   Password: *********
   ```

3. Enter show cluster-state to display the statuses of the node and the cluster.

   Before continuing to the next step, verify that both the node and the cluster are in service.

   FIGURE 53 Verify that both the node and the cluster are in service

   ```
   dean300-1# show cluster-state
      Current Management Service Status : In service
      Current Node Status       : In service
      Cluster Status            : In service
      Cluster Operation         : None
      System Mode               : None
   ```

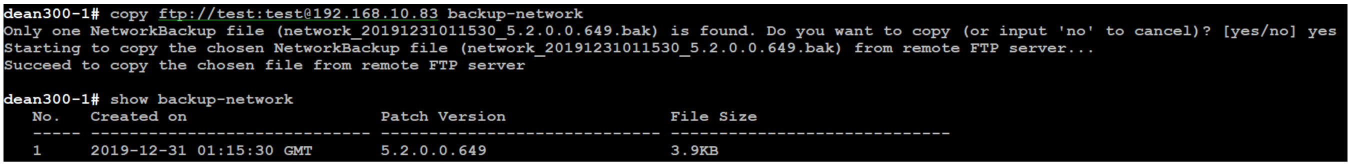
4. Enter the following command to log on to the FTP server and check for available backup files that can be copied to the controller:

   copy <ftp-url> backup-network
5. If multiple backup files exist on the FTP server, the **CLI** prompts you to select the number that corresponds to the file that you want to copy back to the controller.

   If a single backup file exists, the **CLI** prompts you to confirm that you want to copy the existing backup file to the controller.

   When the controller finishes copying the selected backup file from the FTP server back to the controller, the following message appears: `Succeed to copy the chosen file from the remote FTP server`
6. Enter **show backup-network** to verify that the backup file was copied back to the controller successfully.

   FIGURE 54 Verify that the backup file was copied to the controller successfully

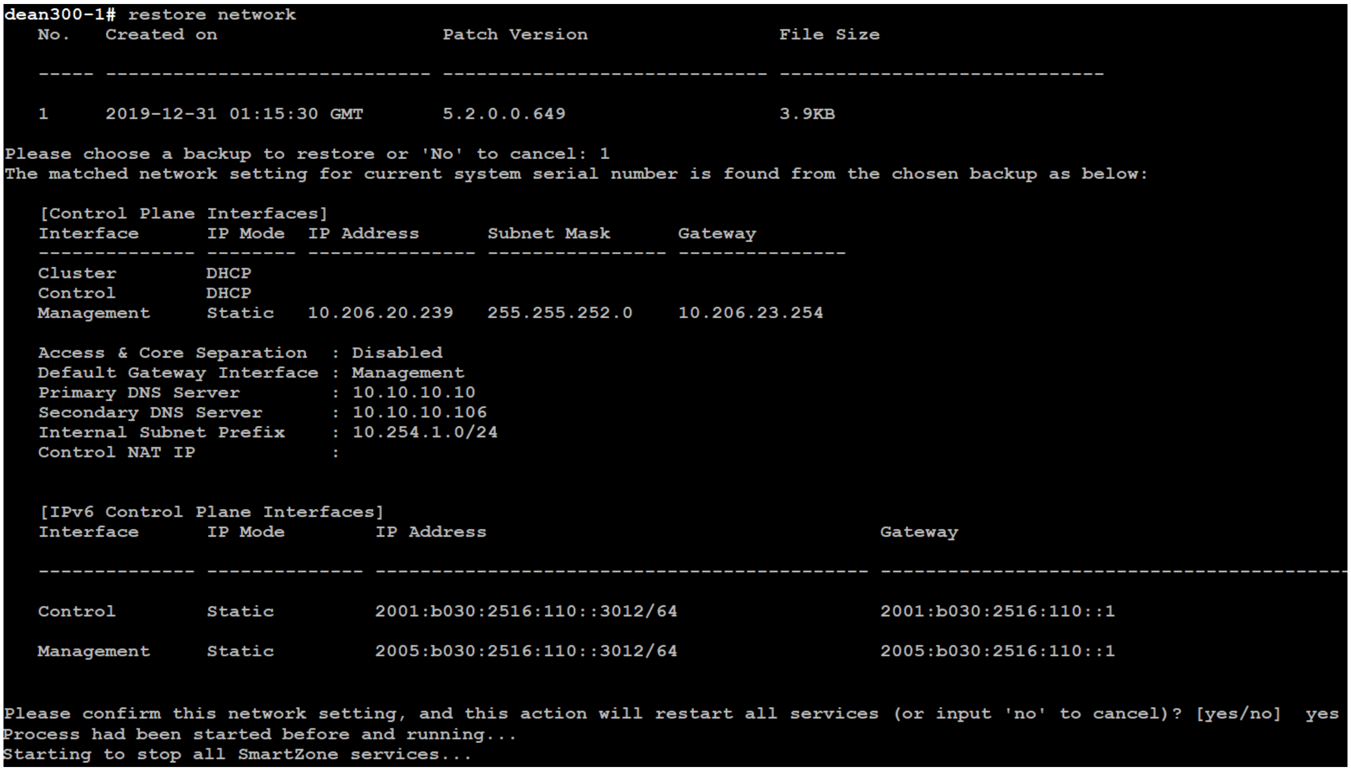
   ```
   dean300-1# copy ftp://test:test@192.168.10.83 backup-network
   Only one NetworkBackup file (network_20191231011530_5.2.0.0.649.bak) is found. Do you want to copy (or input 'no' to cancel)? [yes/no] yes
   Starting to copy the chosen NetworkBackup file (network_20191231011530_5.2.0.0.649.bak) from remote FTP server...
   Succeed to copy the chosen file from remote FTP server

   dean300-1# show backup-network
      No.   Created on                    Patch Version                 File Size
      ----- ----------------------------- ----------------------------- -----------------------------
      1     2019-12-31 01:15:30 GMT       5.2.0.0.649                   3.9KB
   ```

7. Run restore network to start restoring the contents of the backup file to the current controller.

   The **CLI** displays a list of backup files, and then prompts you to select the backup file that you want to restore to the controller.

8. Enter the number that corresponds to the backup file that you want to restore.

FIGURE 55 Enter the number that corresponds to the backup file that you want to restore



```
dean300-1# restore network
   No.   Created on                    Patch Version                 File Size

   ----- ----------------------------- ----------------------------- -----------------------------

   1     2019-12-31 01:15:30 GMT       5.2.0.0.649                   3.9KB

Please choose a backup to restore or 'No' to cancel: 1
The matched network setting for current system serial number is found from the chosen backup as below:

   [Control Plane Interfaces]
   Interface      IP Mode  IP Address      Subnet Mask      Gateway
   -------------- -------- --------------- ---------------- ---------------
   Cluster        DHCP
   Control        DHCP
   Management     Static   10.206.20.239   255.255.252.0    10.206.23.254

   Access & Core Separation  : Disabled
   Default Gateway Interface : Management
   Primary DNS Server        : 10.10.10.10
   Secondary DNS Server      : 10.10.10.106
   Internal Subnet Prefix    : 10.254.1.0/24
   Control NAT IP            :


   [IPv6 Control Plane Interfaces]
   Interface      IP Mode        IP Address                                   Gateway

   -------------- -------------- -------------------------------------------- -----------------------------------------

   Control        Static         2001:b030:2516:110::3012/64                  2001:b030:2516:110::1

   Management     Static         2005:b030:2516:110::3012/64                  2005:b030:2516:110::1


Please confirm this network setting, and this action will restart all services (or input 'no' to cancel)? [yes/no]  yes
Process had been started before and running...
Starting to stop all SmartZone services...
```

The **CLI** displays the network configuration that the selected backup file contains.

If the serial number of the current controller matches the serial number contained in one of the backup files, the **CLI** automatically selects the backup file to restore and displays the network configuration that it contains.

9. Type **yes** to confirm that you want to restore the selected backup file. The controller starts the restore process and performs the following steps:

   a) Stop all services.

   b) Back up the current network configuration.

      This will enable the controller to roll back to the current configuration, in case there is an issue with the restore process.

   c) Clean up the current network configuration.

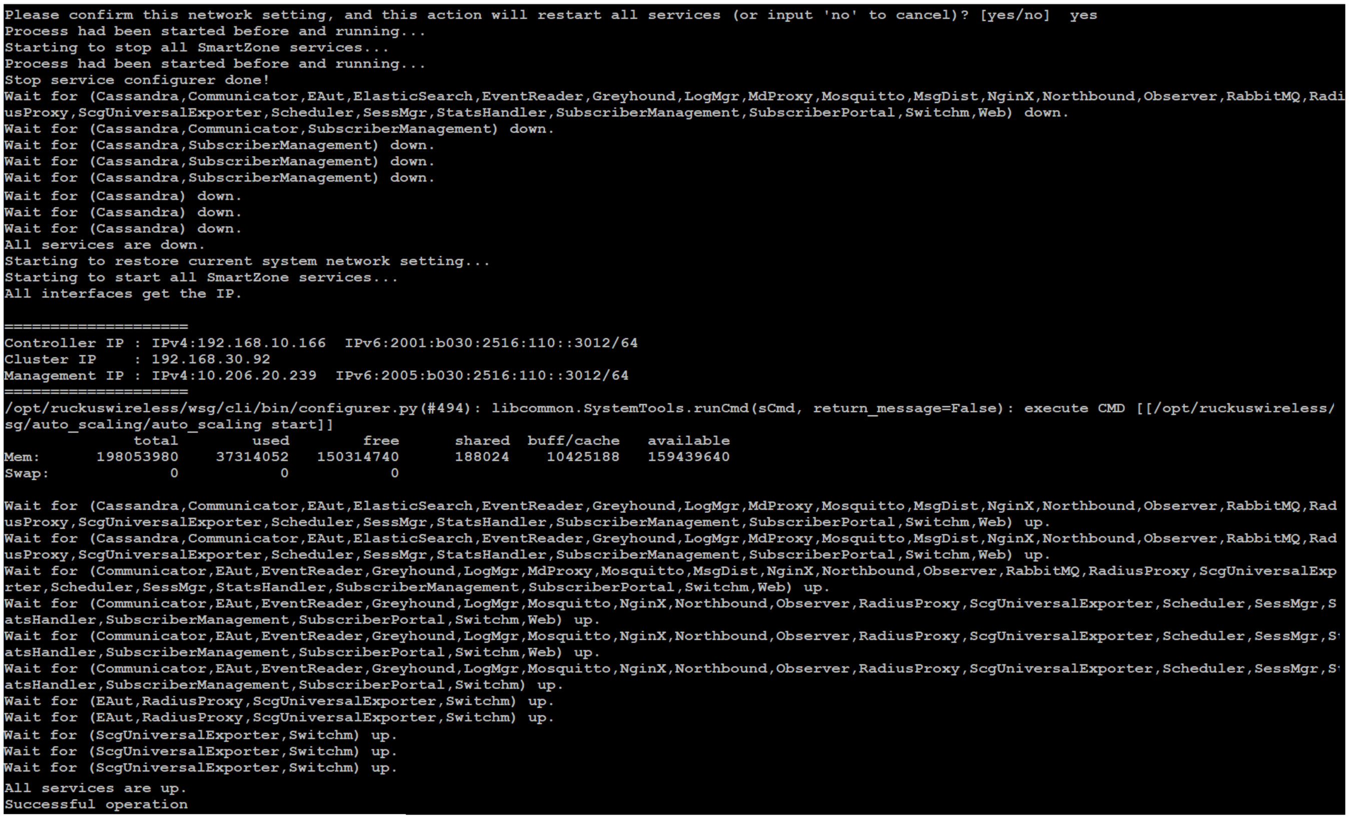
   The controller deletes its previous network configuration, including static routes, name server, user defined interfaces, etc.

10. Restore the network configuration contained in the selected backup file.

11. Restart all services.

    When the restore process is complete, the following message appears on the CLI: `All services are up!`

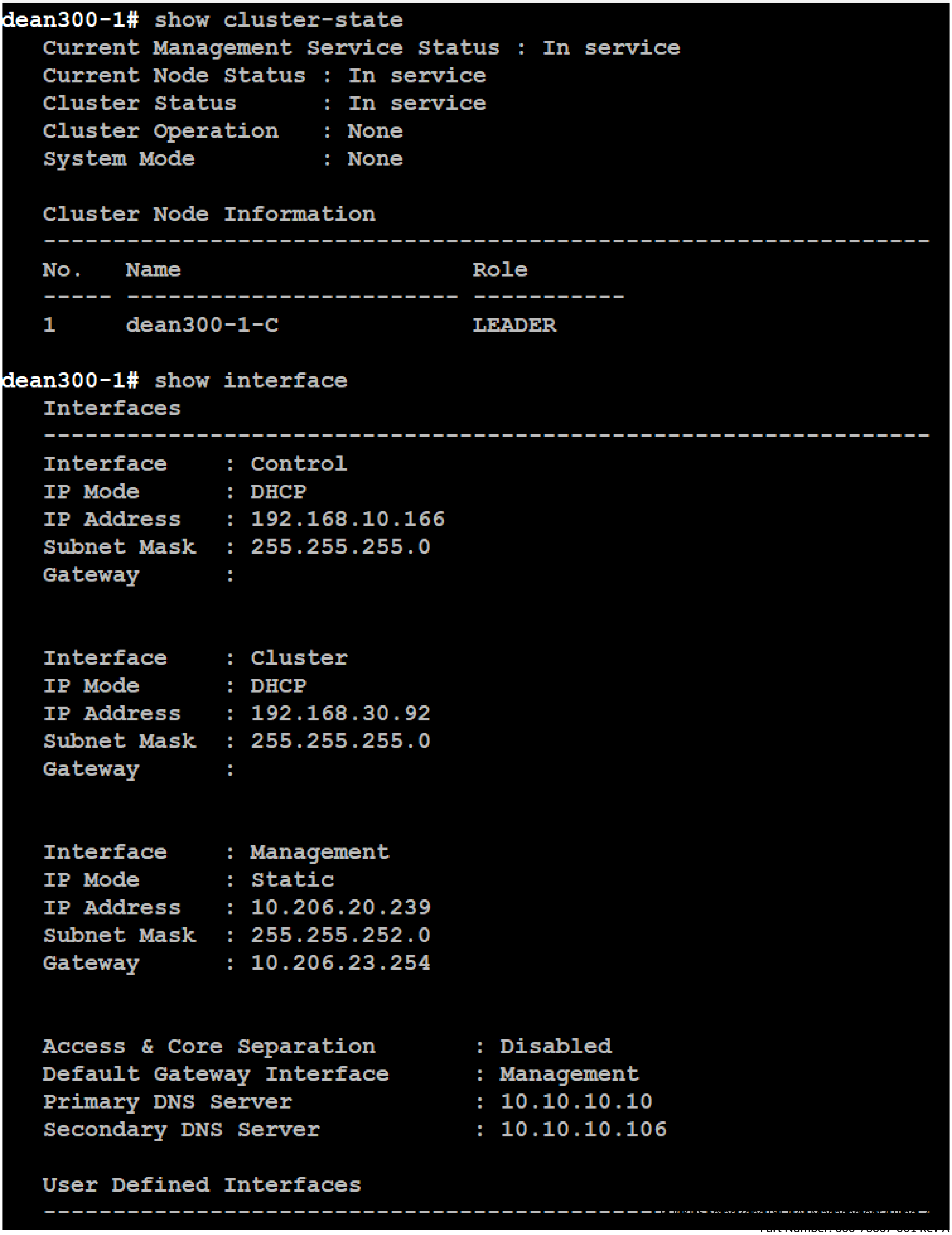
FIGURE 56 The controller performs several steps to restore the backup file



```
Please confirm this network setting, and this action will restart all services (or input 'no' to cancel)? [yes/no]  yes
Process had been started before and running...
Starting to stop all SmartZone services...
Process had been started before and running...
Stop service configurer done!
Wait for (Cassandra,Communicator,EAut,ElasticSearch,EventReader,Greyhound,LogMgr,MdProxy,Mosquitto,MsgDist,NginX,Northbound,Observer,RabbitMQ,Radi
usProxy,ScgUniversalExporter,Scheduler,SessMgr,StatsHandler,SubscriberManagement,SubscriberPortal,Switchm,Web) down.
Wait for (Cassandra,Communicator,SubscriberManagement) down.
Wait for (Cassandra,SubscriberManagement) down.
Wait for (Cassandra,SubscriberManagement) down.
Wait for (Cassandra,SubscriberManagement) down.
Wait for (Cassandra) down.
Wait for (Cassandra) down.
Wait for (Cassandra) down.
All services are down.
Starting to restore current system network setting...
Starting to start all SmartZone services...
All interfaces get the IP.

====================
Controller IP : IPv4:192.168.10.166  IPv6:2001:b030:2516:110::3012/64
Cluster IP    : 192.168.30.92
Management IP : IPv4:10.206.20.239  IPv6:2005:b030:2516:110::3012/64
====================
/opt/ruckuswireless/wsg/cli/bin/configurer.py(#494): libcommon.SystemTools.runCmd(sCmd, return_message=False): execute CMD [[/opt/ruckuswireless/
sg/auto_scaling/auto_scaling start]]
              total        used        free      shared  buff/cache   available
Mem:      198053980    37314052   150314740      188024    10425188   159439640
Swap:             0           0           0

Wait for (Cassandra,Communicator,EAut,ElasticSearch,EventReader,Greyhound,LogMgr,MdProxy,Mosquitto,MsgDist,NginX,Northbound,Observer,RabbitMQ,Rad
usProxy,ScgUniversalExporter,Scheduler,SessMgr,StatsHandler,SubscriberManagement,SubscriberPortal,Switchm,Web) up.
Wait for (Cassandra,Communicator,EAut,ElasticSearch,EventReader,Greyhound,LogMgr,MdProxy,Mosquitto,MsgDist,NginX,Northbound,Observer,RabbitMQ,Rad
usProxy,ScgUniversalExporter,Scheduler,SessMgr,StatsHandler,SubscriberManagement,SubscriberPortal,Switchm,Web) up.
Wait for (Communicator,EAut,EventReader,Greyhound,LogMgr,MdProxy,Mosquitto,MsgDist,NginX,Northbound,Observer,RabbitMQ,RadiusProxy,ScgUniversalExp
rter,Scheduler,SessMgr,StatsHandler,SubscriberManagement,SubscriberPortal,Switchm,Web) up.
Wait for (Communicator,EAut,EventReader,Greyhound,LogMgr,Mosquitto,NginX,Northbound,Observer,RadiusProxy,ScgUniversalExporter,Scheduler,SessMgr,S
atsHandler,SubscriberManagement,SubscriberPortal,Switchm,Web) up.
Wait for (Communicator,EAut,EventReader,Greyhound,LogMgr,Mosquitto,NginX,Northbound,Observer,RadiusProxy,ScgUniversalExporter,Scheduler,SessMgr,S
atsHandler,SubscriberManagement,SubscriberPortal,Switchm,Web) up.
Wait for (Communicator,EAut,EventReader,Greyhound,LogMgr,Mosquitto,NginX,Northbound,Observer,RadiusProxy,ScgUniversalExporter,Scheduler,SessMgr,S
atsHandler,SubscriberManagement,SubscriberPortal,Switchm) up.
Wait for (EAut,RadiusProxy,ScgUniversalExporter,Switchm) up.
Wait for (EAut,RadiusProxy,ScgUniversalExporter,Switchm) up.
Wait for (ScgUniversalExporter,Switchm) up.
Wait for (ScgUniversalExporter,Switchm) up.
Wait for (ScgUniversalExporter,Switchm) up.
All services are up.
Successful operation
```

12. Do the following to verify that the restore process was completed successfully:
    a) Run show cluster-state to verify that the node and the cluster are back in service.
    b) Run show interface to verify that all of the network configuration settings have been restored.

FIGURE 57 Verify that the node and cluster are back in service and that the network configuration has been restored successfully



```
dean300-1# show cluster-state
   Current Management Service Status : In service
   Current Node Status : In service
   Cluster Status      : In service
   Cluster Operation   : None
   System Mode         : None

   Cluster Node Information
   -----------------------------------------------------------------
   No.   Name                     Role
   ----- ------------------------ -----------
   1     dean300-1-C              LEADER

dean300-1# show interface
   Interfaces
   -----------------------------------------------------------------
   Interface     : Control
   IP Mode       : DHCP
   IP Address    : 192.168.10.166
   Subnet Mask   : 255.255.255.0
   Gateway       :


   Interface     : Cluster
   IP Mode       : DHCP
   IP Address    : 192.168.30.92
   Subnet Mask   : 255.255.255.0
   Gateway       :


   Interface     : Management
   IP Mode       : Static
   IP Address    : 10.206.20.239
   Subnet Mask   : 255.255.252.0
   Gateway       : 10.206.23.254


   Access & Core Separation        : Disabled
   Default Gateway Interface       : Management
   Primary DNS Server              : 10.10.10.10
   Secondary DNS Server            : 10.10.10.106

   User Defined Interfaces
   -----------------------------------------------------------------
```

You have completed importing and applying the network configuration backup from the FTP server to the controller.

Support Information

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

To access these guides, select **Adminstraion** > **Help** and select the required guide.

WPA3 R3 Support

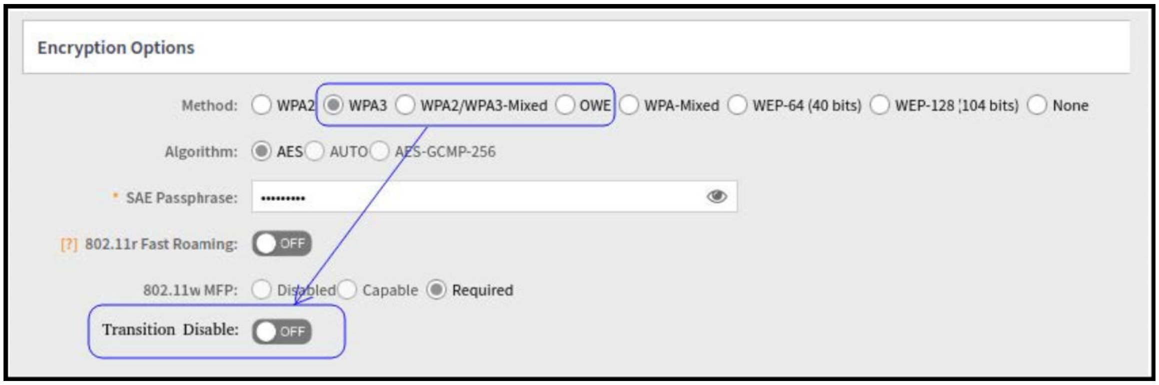
<u>SAE Hash to Element (H2E)</u>

Instead of generating password with ECC/FFC groups by looping, H2E provides a way for direct hashing to obtain the ECC/FFC password element.

An AP that supports H2E sets the SAE H2E bit in Extended RSN Capabilities field in Beacon and Probe Response.

<u>Transition Disable Indication</u>

Tansition Disable Indication



Encryption Options

Method: ○ WPA2 ● WPA3 ○ WPA2/WPA3-Mixed ○ OWE ○ WPA-Mixed ○ WEP-64 (40 bits) ○ WEP-128 (104 bits) ○ None

Algorithm: ● AES ○ AUTO ○ AES-GCMP-256

* SAE Passphrase: •••••••••

[?] 802.11r Fast Roaming: OFF

802.11w MFP: ○ Disabled ○ Capable ● Required

Transition Disable: OFF

- Transition on/off option is provided in the Encryption Options.
- Beacon Protection

  Beacon Protection can only be enabled when PMF is enabled. When Beacon Protection is enabled, the bit 84 in Extended Capability IE should be set to 1. AP should protect Beacon via adding MMIE in all Beacon frames. The BIGTK (Beacon Integrity Group Temporal Key) and BIPN (BIGTK Packet Number) is used for this purpose.

  BIGTK should be renewed whenever there are GTK (Group Temporal Key) updates.
- Operating Channel Validation (OCV)

  AP and STA need to include OCI (Operating Channel Information) as below if it indicates it is OCV Capable.

  - Set bit 14 (OCVC) in RSN capability in RSNE.
  - Add OCI KDE (00-0F-AC-13) in EAPOL M2/M3 and group key update M1/M2 frames. If OCI KDE is incorrect, AP should silently discard the frame.

Troubleshooting Client Connections

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

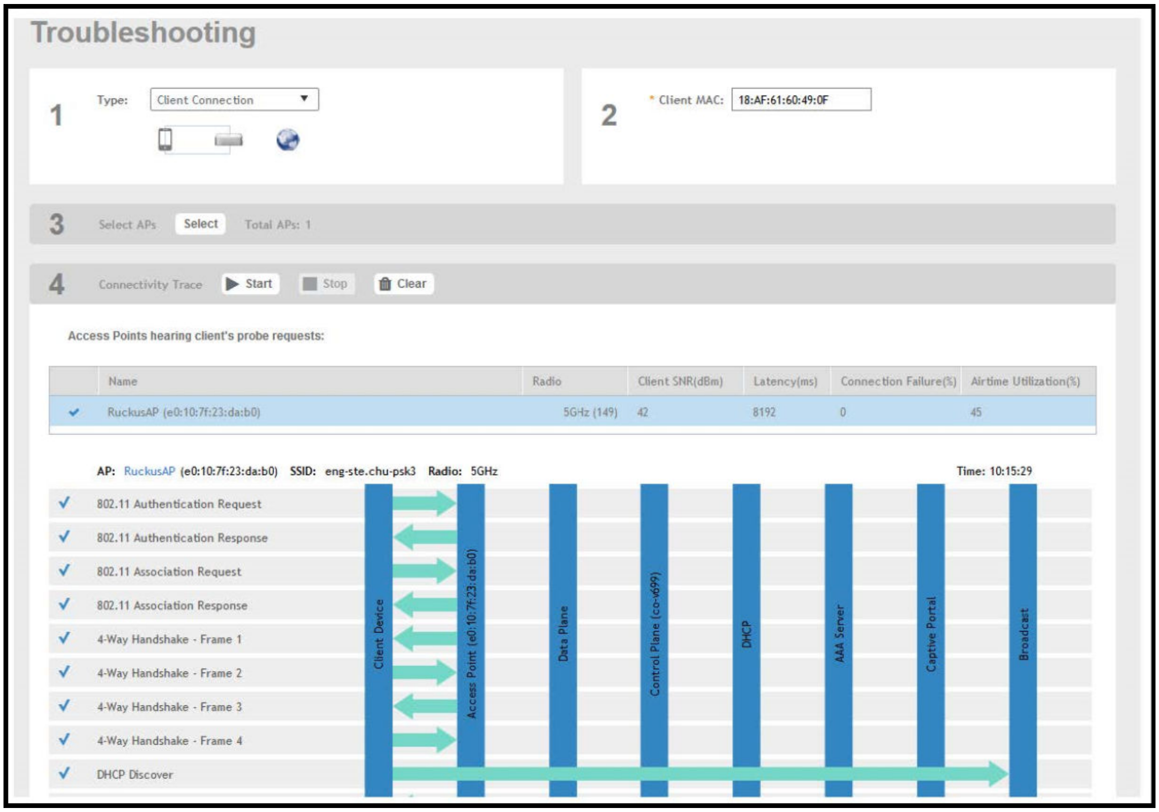
The network administrator types the MAC address of the client device and starts services to identify the connectivity issue. The APs assigned to the client device relay data frames from the device to the controller. The administrator can analyze these frames to determine which stage of the connection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

Perform the following steps to troubleshoot client connections.

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

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

   FIGURE 58 Troubleshooting - Client Connections



Type: Client Connection ▼

* Client MAC: 18:AF:61:60:49:0F

Total APs: 1

Access Points hearing client's probe requests:

	Name	Radio	Client SNR(dBm)	Latency(ms)	Connection Failure(%)	Airtime Utilization(%)
✓	RuckusAP (e0:10:7f:23:da:b0)	5GHz (149)	42	8192	0	45

AP: RuckusAP (e0:10:7f:23:da:b0) SSID: eng-ste.chu-psk3 Radio: 5GHz Time: 10:15:29

✓ 802.11 Authentication Request
✓ 802.11 Authentication Response
✓ 802.11 Association Request
✓ 802.11 Association Response
✓ 4-Way Handshake - Frame 1
✓ 4-Way Handshake - Frame 2
✓ 4-Way Handshake - Frame 3
✓ 4-Way Handshake - Frame 4
✓ DHCP Discover

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

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

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

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

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

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

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

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

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

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

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

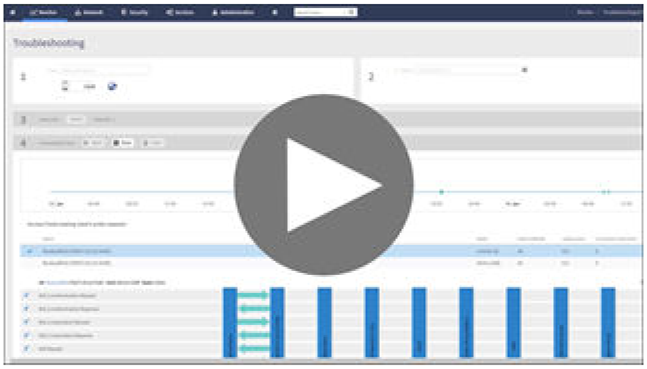
   NOTE
   The following authentication types are supported:

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

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

VIDEO

Client Connection Troubleshooting Demo. Overview of how to use the Client Connection tool.



Click to play video in full screen mode.

Support Bundle

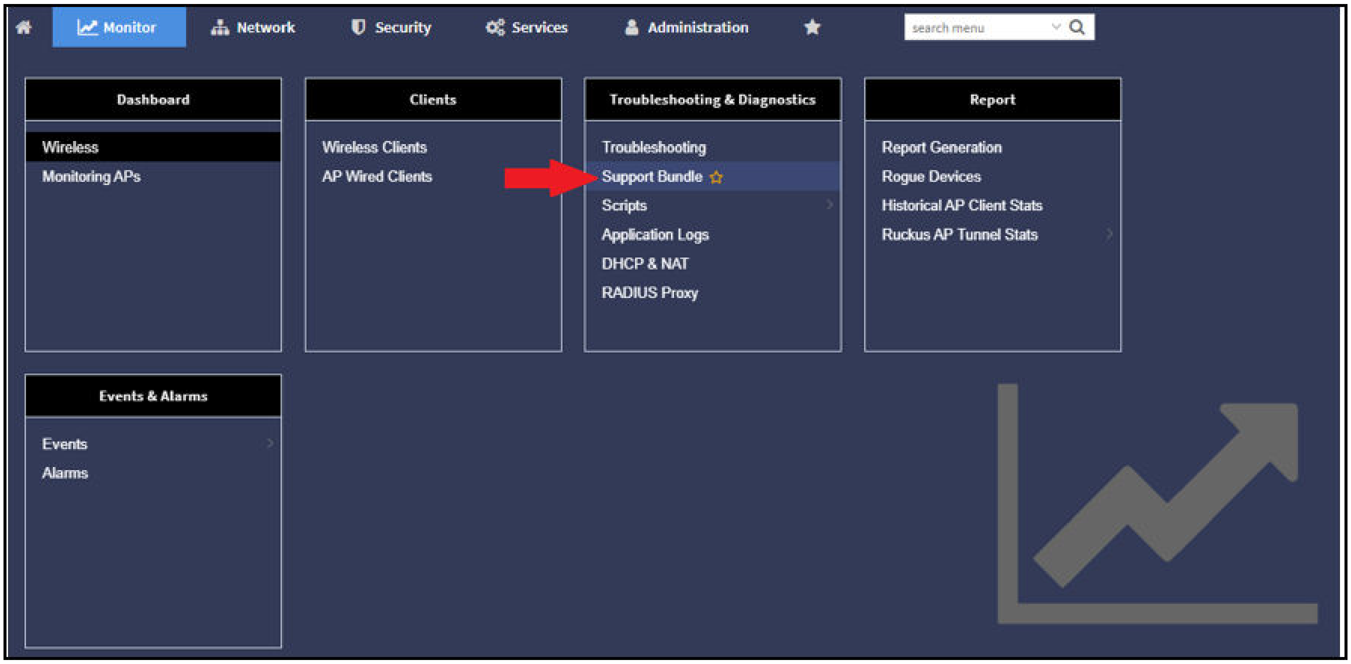
Support Bundle allows you to gather the bundle log files from the controller and APs.

Complete the following steps to enable Support Bundle.

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

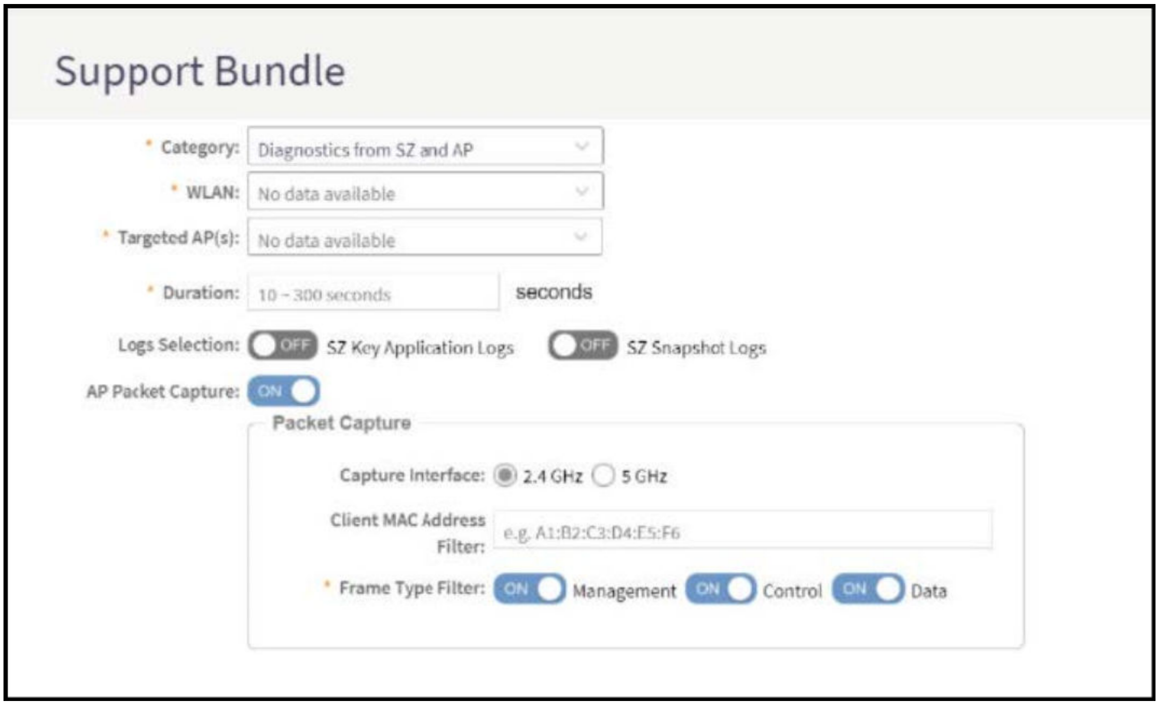
   The **Support Bundle** dialog box is displayed.

   FIGURE 59 Accessing the Support Bundle

2. Configure the following options:

FIGURE 60 Support Bundle Dialog Box



Support Bundle

* Category: Diagnostics from SZ and AP

* WLAN: No data available

* Targeted AP(s): No data available

* Duration: 10 - 300 seconds seconds

Logs Selection: OFF SZ Key Application Logs OFF SZ Snapshot Logs

AP Packet Capture: ON

Packet Capture

Capture Interface: ● 2.4 GHz ○ 5 GHz

Client MAC Address Filter: e.g. A1:B2:C3:D4:E5:F6

* Frame Type Filter: ON Management ON Control ON Data

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

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

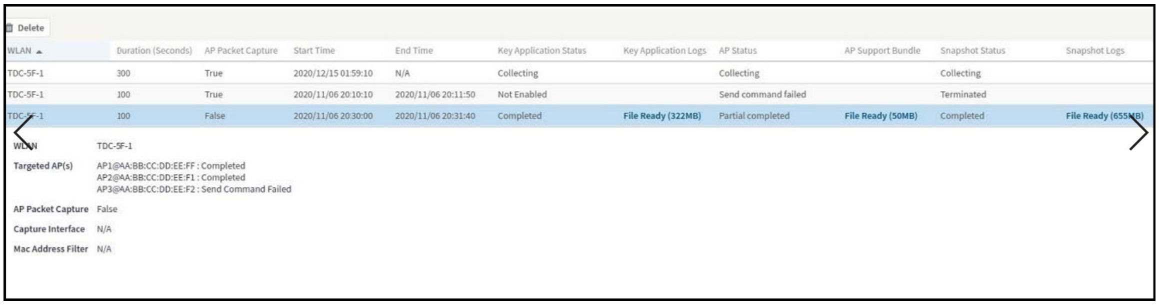
  - The disconnected APs cannot be selected by the user.
  - When the support bundle process is running, user cannot change the **Application Log**.

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

3. Click **OK**.

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

FIGURE 61 Support Bundle Download Options



WLAN ▲	Duration (Seconds)	AP Packet Capture	Start Time	End Time	Key Application Status	Key Application Logs	AP Status	AP Support Bundle	Snapshot Status	Snapshot Logs
TDC-5F-1	300	True	2020/12/15 01:59:10	N/A	Collecting		Collecting		Collecting	
TDC-5F-1	100	True	2020/11/06 20:10:10	2020/11/06 20:11:50	Not Enabled		Send command failed		Terminated	
TDC-5F-1	100	False	2020/11/06 20:30:00	2020/11/06 20:31:40	Completed	File Ready (322MB)	Partial completed	File Ready (50MB)	Completed	File Ready (655MB)

WLAN	TDC-5F-1
Targeted AP(s)	AP1@AA:BB:CC:DD:EE:FF : Completed AP2@AA:BB:CC:DD:EE:F1 : Completed AP3@AA:BB:CC:DD:EE:F2 : Send Command Failed
AP Packet Capture	False
Capture Interface	N/A
Mac Address Filter	N/A

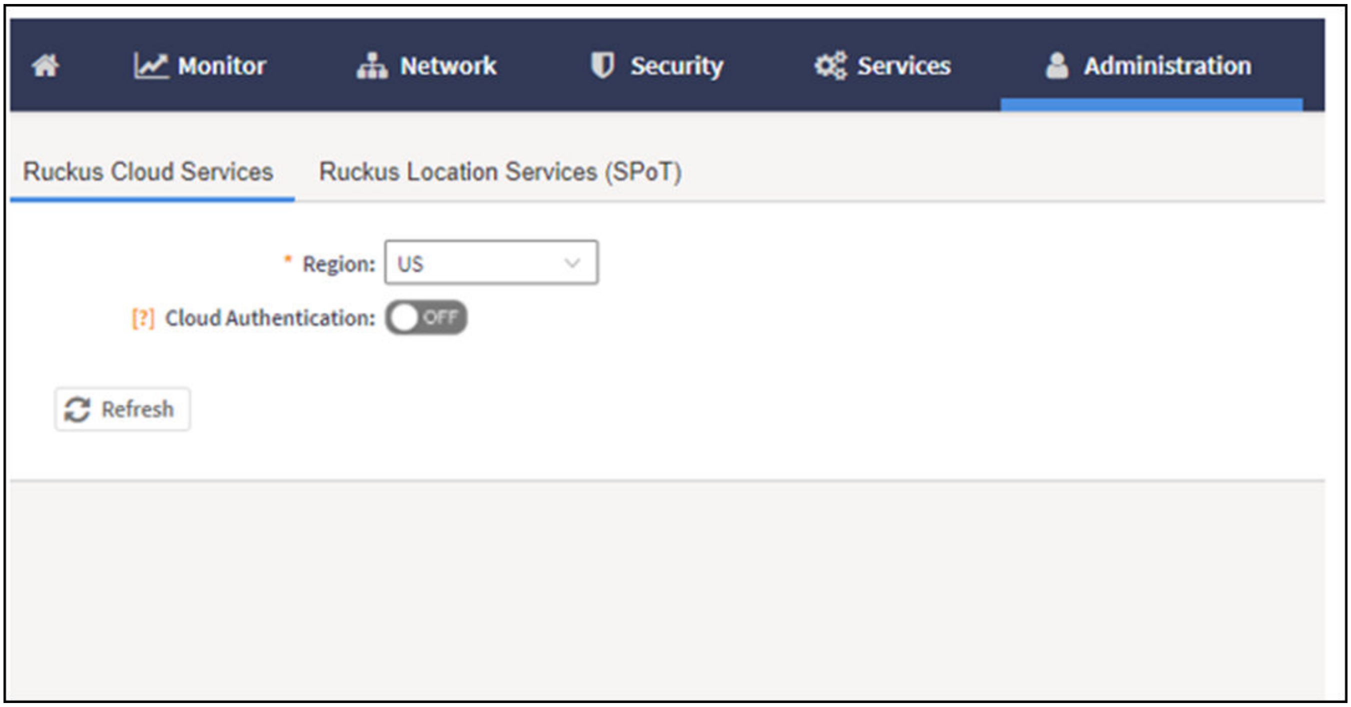
Configuring Cloud Services

Complete the following steps to enable cloud analytics on SmartZone.

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

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

   FIGURE 62 Configuring Cloud Services

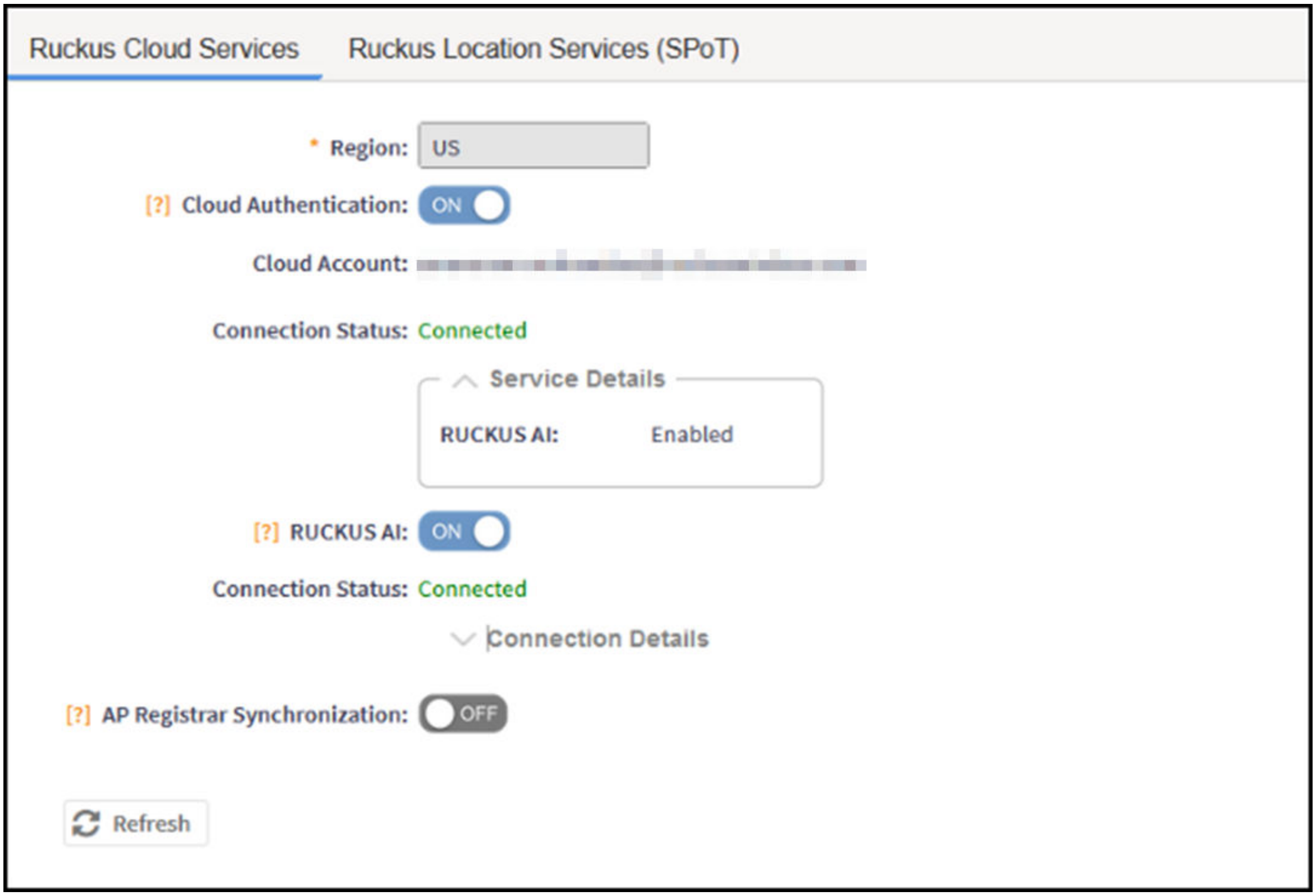
   

   * Region: US

   [?] Cloud Authentication: OFF

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

FIGURE 63 The Log in Page



* Region: US

[?] Cloud Authentication: ON

Cloud Account: [redacted]

Connection Status: Connected

RUCKUS AI: Enabled

[?] RUCKUS AI: ON

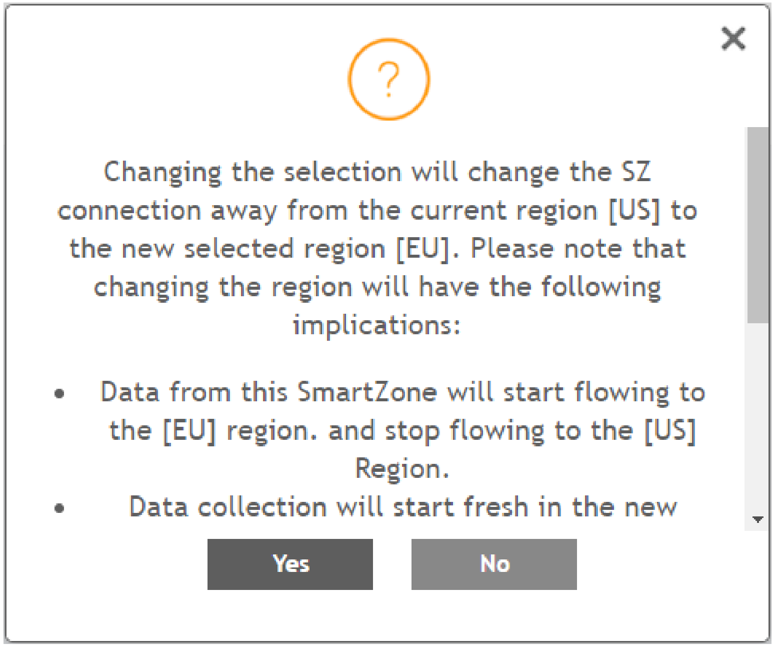
Connection Status: Connected

[?] AP Registrar Synchronization: OFF

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

A confirmation dialog box is displayed.

FIGURE 64 Confirming the Region Change



Changing the selection will change the SZ connection away from the current region [US] to the new selected region [EU]. Please note that changing the region will have the following implications:

- Data from this SmartZone will start flowing to the [EU] region. and stop flowing to the [US] Region.
- Data collection will start fresh in the new

3. Click **Yes** to confirm.

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

4. Select **Cloud SZ Services**.

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

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

5. Select **RUCKUS AI**.

   The connection status for RUCKUS Cloud AI is displayed.

6. Select **AP Registrar Synchronization**.

FIGURE 65 Selecting Export All Batch Provisioning APs

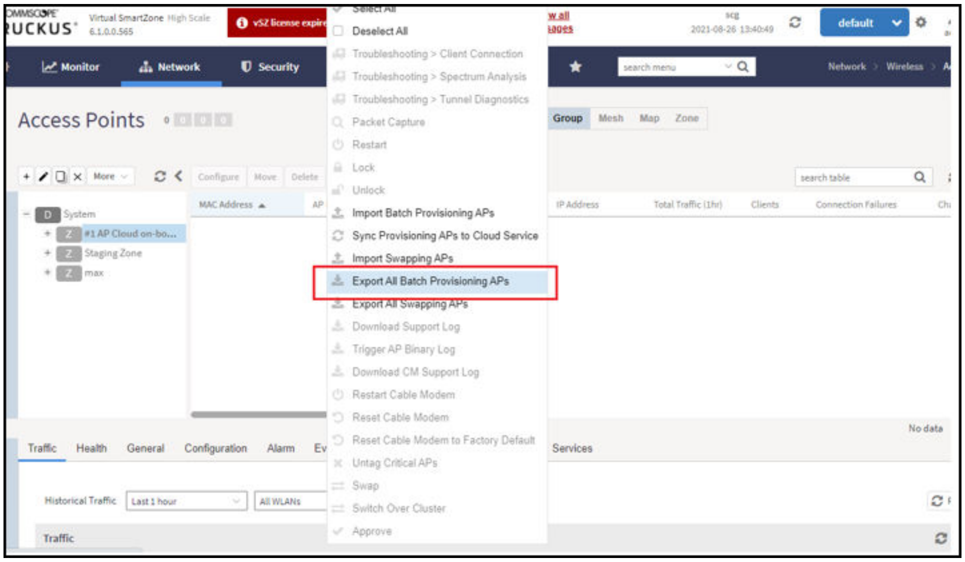
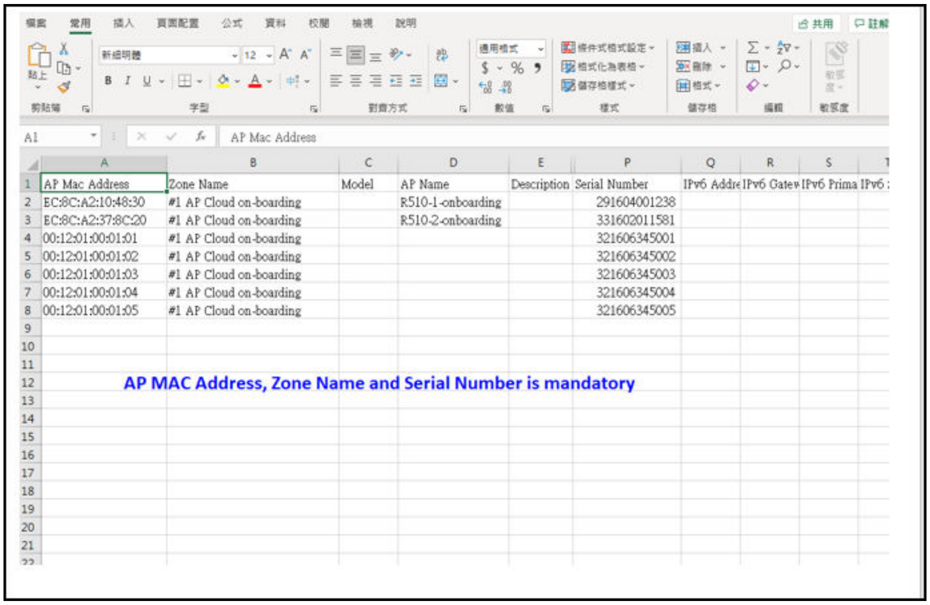


FIGURE 66 Exporting the CSV File



AP Mac Address	Zone Name	Model	AP Name	Description	Serial Number	IPv6 Addre	IPv6 Gatev	IPv6 Prima	IPv6 :
EC:8C:A2:10:48:30	#1 AP Cloud on-boarding		R510-1-onboarding		291604001238				
EC:8C:A2:37:8C:20	#1 AP Cloud on-boarding		R510-2-onboarding		331602011581				
00:12:01:00:01:01	#1 AP Cloud on-boarding				321606345001				
00:12:01:00:01:02	#1 AP Cloud on-boarding				321606345002				
00:12:01:00:01:03	#1 AP Cloud on-boarding				321606345003				
00:12:01:00:01:04	#1 AP Cloud on-boarding				321606345004				
00:12:01:00:01:05	#1 AP Cloud on-boarding				321606345005				

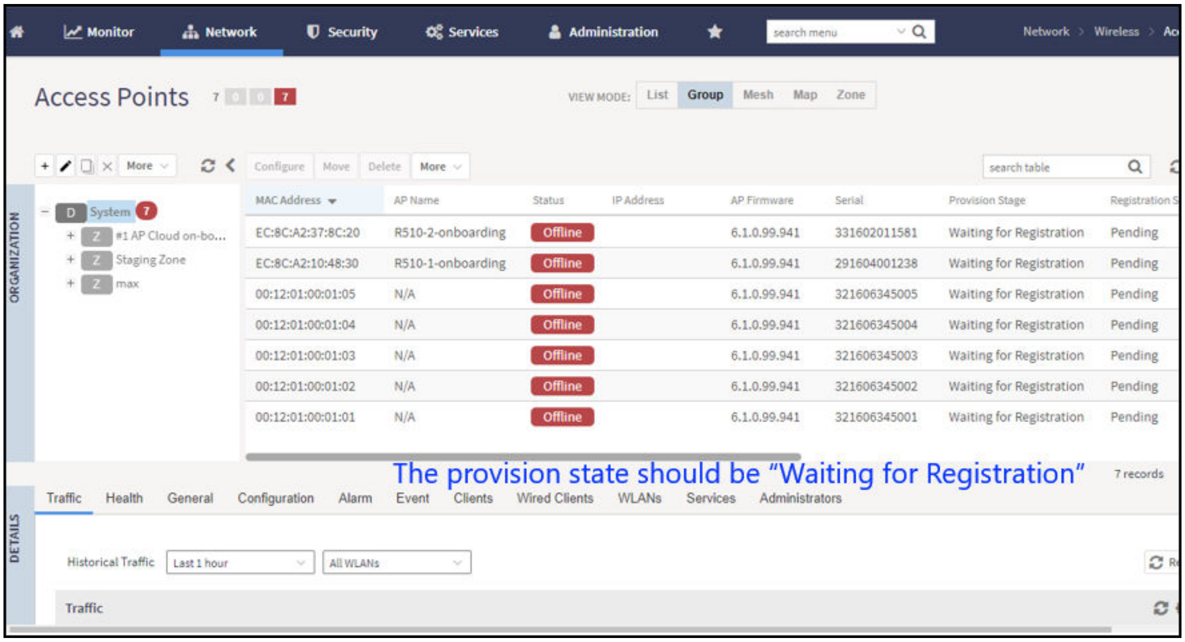
AP MAC Address, Zone Name and Serial Number is mandatory

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

8. Import the provisioning AP list to an AP Zone.

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

FIGURE 67 Importing CSV File

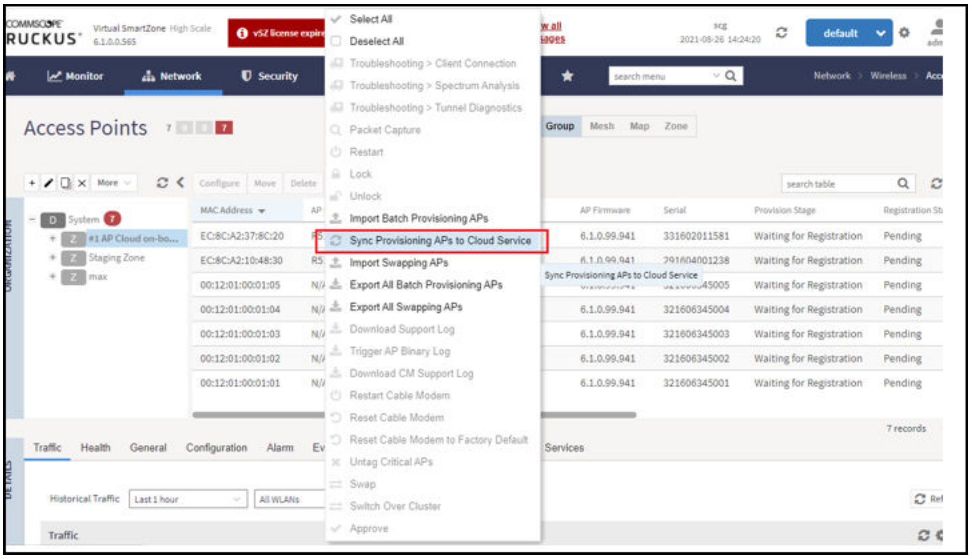

Monitor
Network
Security
Services
Administration
search menu
Network > Wireless > Ac
Access Points 7 0 0 7
VIEW MODE: List Group Mesh Map Zone
More
Configure Move Delete More
search table
ORGANIZATION
System 7
#1 AP Cloud on-bo...
Staging Zone
max
7 records
DETAILS
Traffic Health General Configuration Alarm Event Clients Wired Clients WLANs Services Administrators
Historical Traffic Last 1 hour All WLANs
Traffic

MAC Address	AP Name	Status	IP Address	AP Firmware	Serial	Provision Stage	Registration S
EC:8C:A2:37:8C:20	R510-2-onboarding	Offline		6.1.0.99.941	331602011581	Waiting for Registration	Pending
EC:8C:A2:10:48:30	R510-1-onboarding	Offline		6.1.0.99.941	291604001238	Waiting for Registration	Pending
00:12:01:00:01:05	N/A	Offline		6.1.0.99.941	321606345005	Waiting for Registration	Pending
00:12:01:00:01:04	N/A	Offline		6.1.0.99.941	321606345004	Waiting for Registration	Pending
00:12:01:00:01:03	N/A	Offline		6.1.0.99.941	321606345003	Waiting for Registration	Pending
00:12:01:00:01:02	N/A	Offline		6.1.0.99.941	321606345002	Waiting for Registration	Pending
00:12:01:00:01:01	N/A	Offline		6.1.0.99.941	321606345001	Waiting for Registration	Pending

The provision state should be "Waiting for Registration"

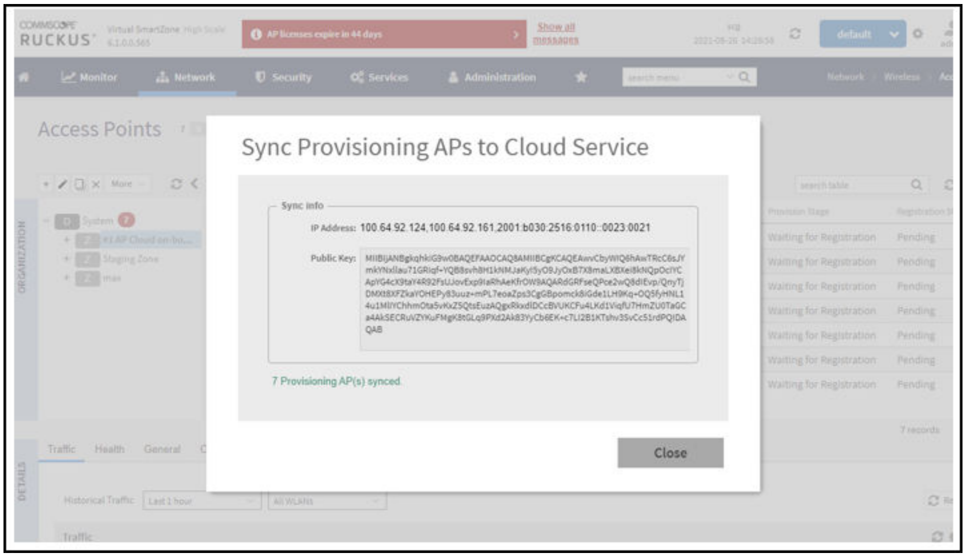
9. Click **More**, and select **Sync Provisioning APs to Cloud Service** from the list.

FIGURE 68 Selecting Sync Provisioning APs to Cloud Service


COMMSCOPE RUCKUS
Virtual SmartZone High Scale 6.1.0.0.565
vSZ license expire
scg 2021-08-26 14:24:20
default
Monitor
Network
Security
Access Points 7
Select All
Deselect All
Troubleshooting > Client Connection
Troubleshooting > Spectrum Analysis
Troubleshooting > Tunnel Diagnostics
Packet Capture
Restart
Lock
Unlock
Import Batch Provisioning APs
Sync Provisioning APs to Cloud Service
Import Swapping APs
Export All Batch Provisioning APs
Export All Swapping APs
Download Support Log
Trigger AP Binary Log
Download CM Support Log
Restart Cable Modem
Reset Cable Modem
Reset Cable Modem to Factory Default
Untag Critical APs
Swap
Switch Over Cluster
Approve
Sync Provisioning APs to Cloud Service
Group Mesh Map Zone
search table
7 records
Traffic Health General Configuration Alarm Ev Services
Historical Traffic Last 1 hour All WLANs
Traffic

10. Ensure synchronization is successful.

FIGURE 69 Ensuring Synchronization Success



Sync Provisioning APs to Cloud Service

Sync info

IP Address: 100.64.92.124,100.64.92.161,2001:b030:2516:0110::0023:0021

Public Key: MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAwvCbyWIQ6hAwTRcC6sJY mkYNxIlau71GRIqf+YQB8svh8H1kNMJaKyI5yO9JyOxB7X8maLXBXeI8kNQpOcIYC ApYG4cX9taY4R92FsUJovExp9IaRhAeKfrOW9AQARdGRFseQPce2wQ8dIEvp/QnyTj DMXt8XFZkaYOHEPy83uuz+mPL7eoaZps3CgGBpomck8iGde1LH9Kq+OQ5fyHNL1 4u1MIlYChhmOta5vKxZ5QtsEuzAQgxRkxdIDCcBVUKCFu4LKd1ViqfU7HmZU0TaGC a4AkSECRuVZYKuFMgK8tGLq9PXd2Ak83YyCb6EK+c7LI2B1KTshv3SvCc51rdPQIDA QAB

7 Provisioning AP(s) synced.

Working with Data and Control Plane

Viewing the System Cluster Overview

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

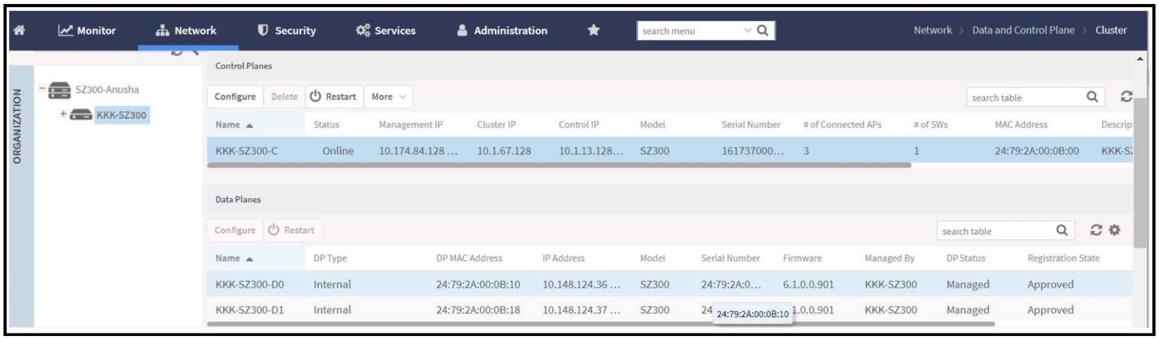
NOTE

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

To view the cluster settings:

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

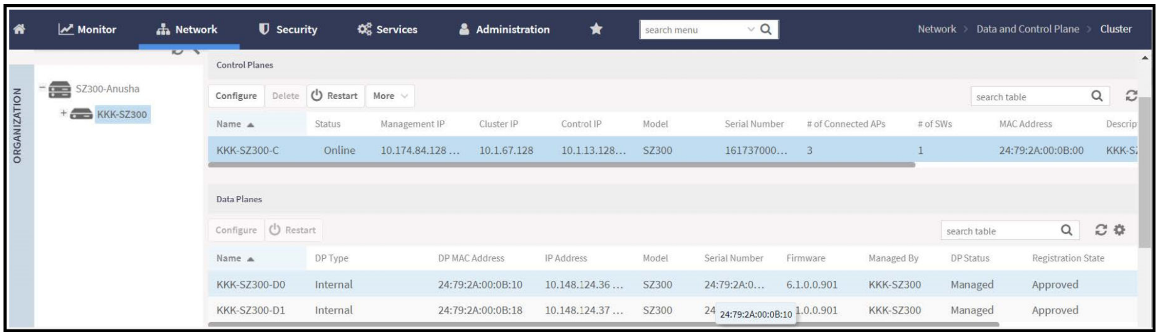
FIGURE 70 System Cluster Overview - SZ300



Name	Status	Management IP	Cluster IP	Control IP	Model	Serial Number	# of Connected APs	# of SWs	MAC Address	Descrip
KKK-SZ300-C	Online	10.174.84.128 ...	10.1.67.128	10.1.13.128...	SZ300	161737000...	3	1	24:79:2A:00:0B:00	KKK-S:

Name	DP Type	DP MAC Address	IP Address	Model	Serial Number	Firmware	Managed By	DP Status	Registration State
KKK-SZ300-D0	Internal	24:79:2A:00:0B:10	10.148.124.36 ...	SZ300	24:79:2A:0...	6.1.0.0.901	KKK-SZ300	Managed	Approved
KKK-SZ300-D1	Internal	24:79:2A:00:0B:18	10.148.124.37 ...	SZ300	24	1.0.0.901	KKK-SZ300	Managed	Approved

FIGURE 71 System Cluster Overview - vSZ-H



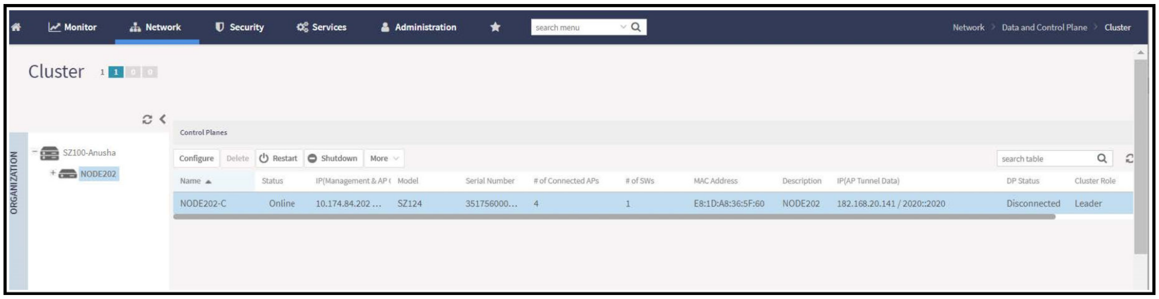
Control Planes

Name ▲	Status	Management IP	Cluster IP	Control IP	Model	Serial Number	# of Connected APs	# of SWs	MAC Address	Descrip
KKK-SZ300-C	Online	10.174.84.128 ...	10.1.67.128	10.1.13.128...	SZ300	161737000...	3	1	24:79:2A:00:0B:00	KKK-S.

Data Planes

Name ▲	DP Type	DP MAC Address	IP Address	Model	Serial Number	Firmware	Managed By	DP Status	Registration State
KKK-SZ300-D0	Internal	24:79:2A:00:0B:10	10.148.124.36 ...	SZ300	24:79:2A:0...	6.1.0.0.901	KKK-SZ300	Managed	Approved
KKK-SZ300-D1	Internal	24:79:2A:00:0B:18	10.148.124.37 ...	SZ300	24 24:79:2A:00:0B:10	1.0.0.901	KKK-SZ300	Managed	Approved

FIGURE 72 System Cluster Overview - SZ100



Control Planes

Name ▲	Status	IP(Management & AP (	Model	Serial Number	# of Connected APs	# of SWs	MAC Address	Description	IP(AP Tunnel Data)	DP Status	Cluster Role
NODE202-C	Online	10.174.84.202 ...	SZ124	351756000...	4	1	E8:1D:A8:36:5F:60	NODE202	182.168.20.141 / 2020::2020	Disconnected	Leader

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

Control Planes and Data Planes

Control planes and data planes are used to control traffic.

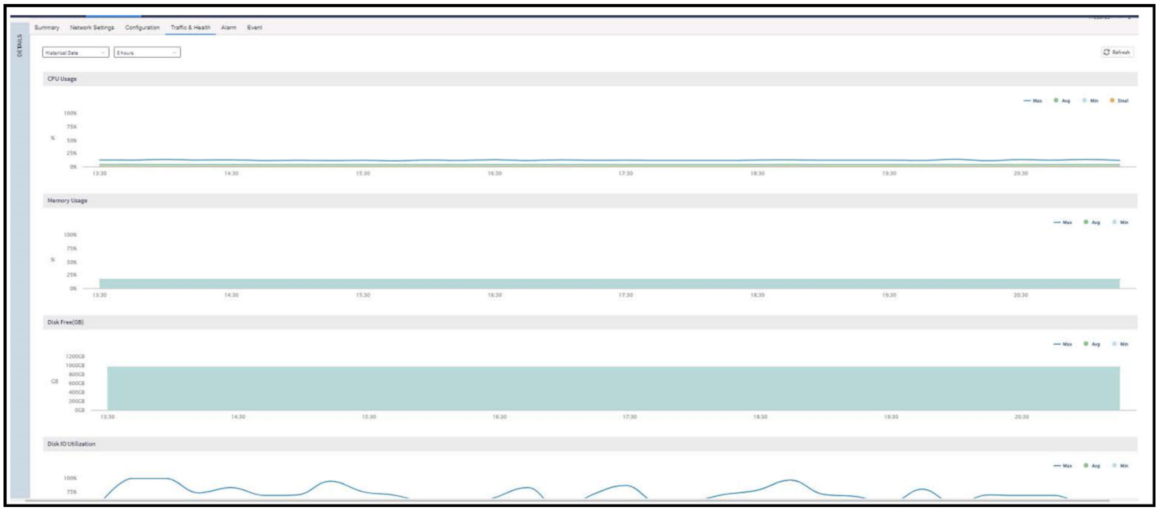
The control plane manages and exchanges routing table information. The control plane packets are processed by the router to update the routing table information. The data plane forwards the traffic along the path according to the logic of the control plane.

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

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

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

FIGURE 73 Viewing the Cluster Traffic



Interface and Routing

To configure a cluster node, you must define interface and routing information.

Interface

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

> **NOTE**
> The user defined interface (UDI) is available in Virtual SmartZone (High-Scale and Essentials) from release 5.1.1.

Static Routing

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

Displaying the Chassis View of Cluster Nodes

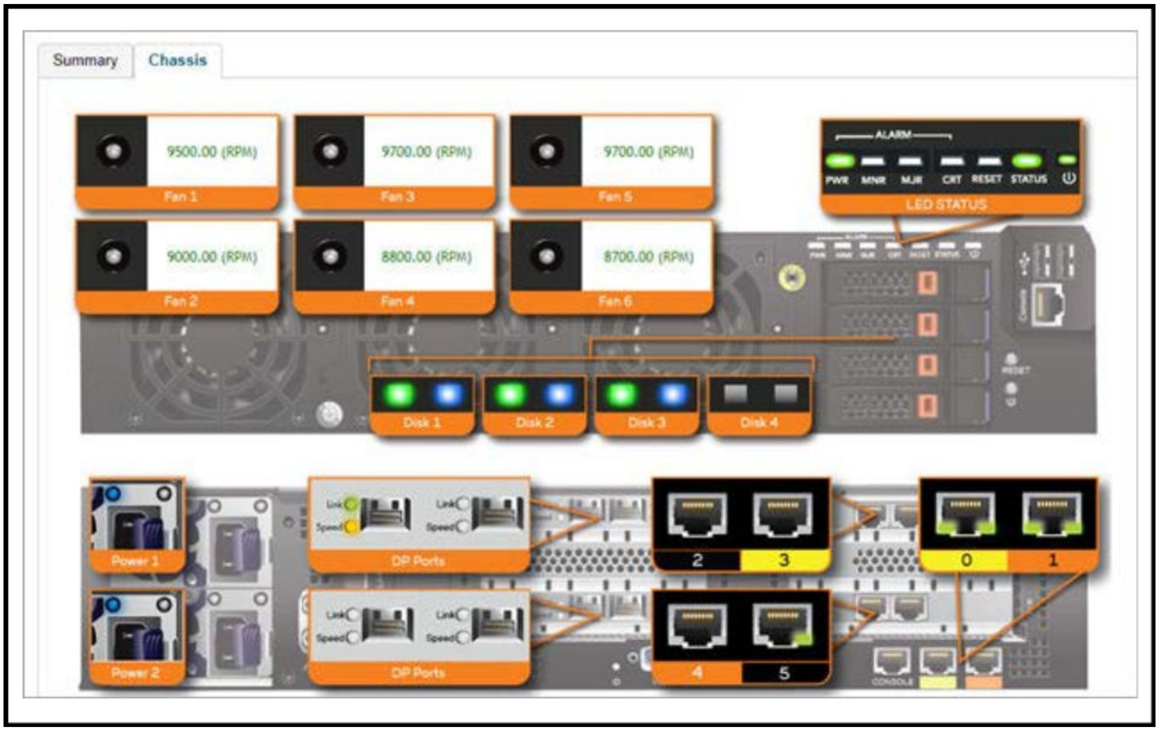
The chassis view provides a graphical representation of the control panel (on the front panel of the controller), including the LEDs.

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

To view the chassis of the cluster node:

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

FIGURE 74 Cluster Node Chassis



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

Cluster Redundancy

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

Active-Standby mode

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

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

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

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

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

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

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

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

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

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

TABLE 17 Standby Cluster Default Mode When Cluster Redundancy Is Enabled

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

Active-Active Mode

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

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

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

Precondition

- **Active-Standby mode**

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

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

- **Active-Active mode**

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

  - All the cluster nodes must be in service.
  - The system version of both clusters must be the same.
  - The model (vSZ-H or SZ300) must be the same.
  - The network interface number must be equal.
  - The IP mode must be the same.
  - Both cluster must apply the same KSPs on all nodes.
  - "Schedule Configuration Sync" can be enabled only in one cluster.

Configuration

- **Active-Standby mode**

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

- **Active-Active mode**

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

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

Cluster Status

- **Active-Standby mode**

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

- **Active-Active mode**

  All clusters work as a normal cluster

Configuration Backup

- **Active-Standby mode**

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

- **Active-Active mode**

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

Deployment Models

- **Active-Standby mode**

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

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

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

- **Active-Active mode**

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

License Management

- **Active-Standby mode**

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

  - Permanent AP licenses

- Default Temporary AP licenses
- Default Temporary AP License Period

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

- **Active-Active mode**

  Licenses in each active cluster are independent.

How Cluster Redundancy Works

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

- Active-Standby mode

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

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

     {

     "Server List":["IP_A1", "IP_A2, "IP_A3", "IP_A4"],

     "Failover List":["IP_B1", "IP_B2, "IP_B3", "IP_B4"]

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

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

- Active-Active mode

  Configurations can be made using the UI.

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

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

     a. Cluster B

     b. Cluster C

     c. Cluster D

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

{

"Server List":["IP_A1", "IP_A2, "IP_A3", "IP_A4"],

"Failover List":["IP_B4", "IP_B2", "IP_B3", "IP_B1"], ["IP_C1", "IP_C4", "IP_C2", "IP_C3"], ["IP_D2", "IP_D1", "IP_D4", "IP_D3"]

}

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

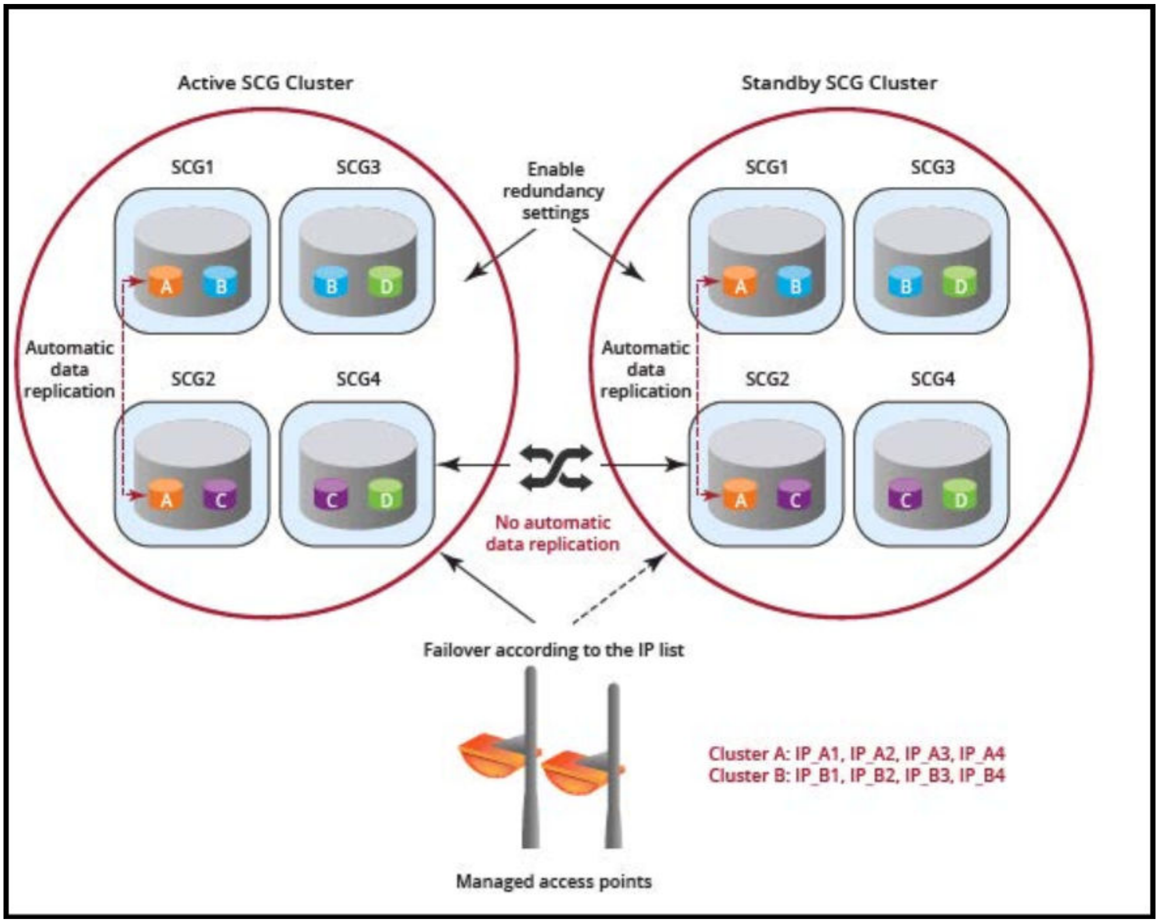
Enabling Cluster Redundancy

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

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

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

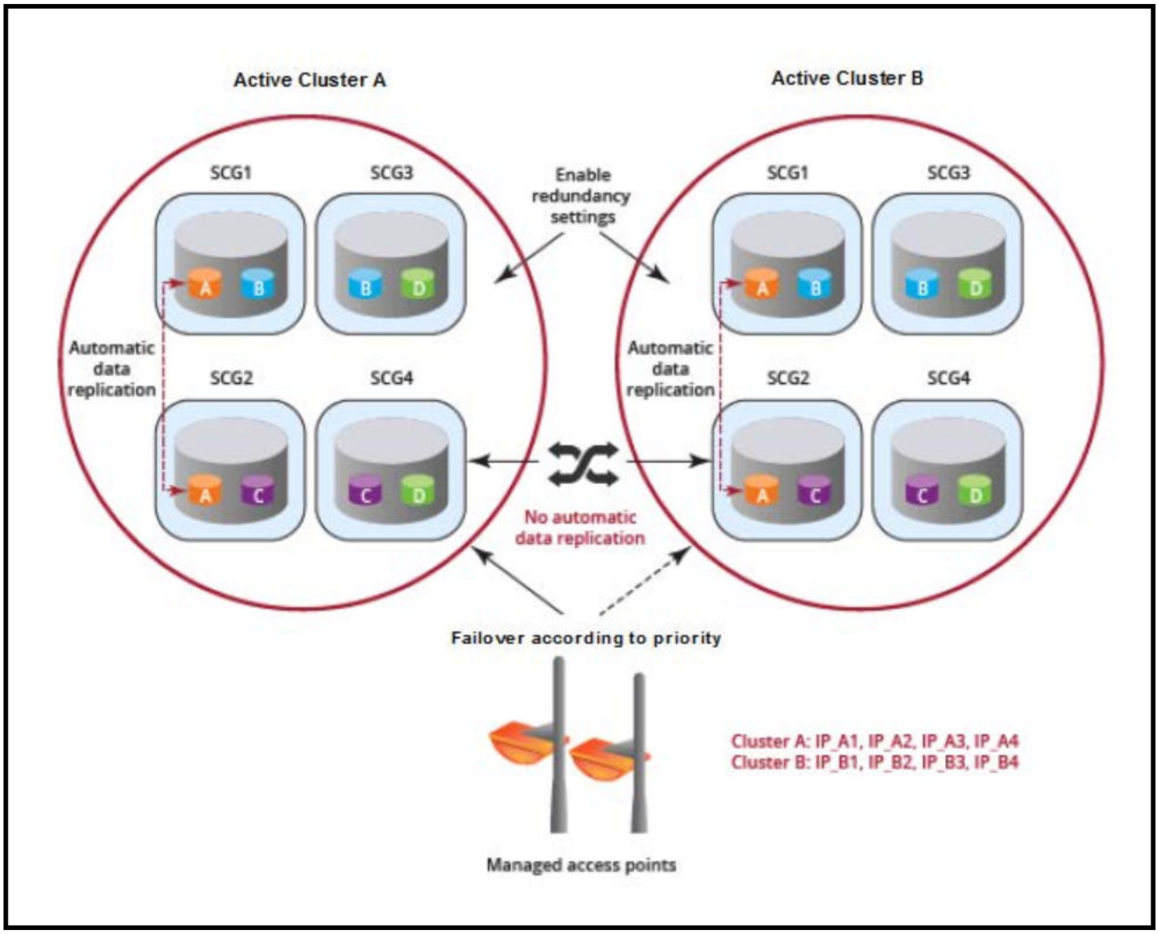
FIGURE 75 Cluster Redundancy for Active-Standby Mode


Active SCG Cluster
Standby SCG Cluster
SCG1
SCG3
SCG2
SCG4
A
B
C
D
Enable redundancy settings
Automatic data replication
No automatic data replication
Failover according to the IP list
Cluster A: IP_A1, IP_A2, IP_A3, IP_A4
Cluster B: IP_B1, IP_B2, IP_B3, IP_B4
Managed access points

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

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

FIGURE 76 Cluster Redundancy for Active-Active Mode


Active Cluster A
Active Cluster B
SCG1
SCG3
SCG2
SCG4
A
B
C
D
Enable redundancy settings
Automatic data replication
No automatic data replication
Failover according to priority
Cluster A: IP_A1, IP_A2, IP_A3, IP_A4
Cluster B: IP_B1, IP_B2, IP_B3, IP_B4
Managed access points

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

Complete the following steps to enable cluster redundancy.

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

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

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

a. **Timing to serve Active cluster**: Determines when the standard cluster turns to backup mode and manages external devices (APs, DPs, and ICX switches).

   - **Active out-of-service**: Only when active cluster is out-of-service (default setting).
   - **Always**: Always on service.

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

b. Enter the admin **Password** of the standby cluster.

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

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

d. For **Time**, select the duration in HH:MM format from the list to periodically sync the configurations.

e. Click **OK**. A confirmation dialog box is displayed.

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

  NOTE
  Switches do not support Active-Active mode failover.

a. For **Password**, enter the admin password of the active cluster.

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

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

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

c. For **Interval**, select the interval to sync and restore the configuration to the target active clusters. If you select **Monthly** or **Weekly**, select the respective day.

d. For **Hour** and **Minutes**, select the hour and minutes to periodically sync the configurations.

e. Click **OK**. A confirmation dialog box is displayed.

6. Click **OK**.

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

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

Viewing Cluster Configuration

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

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

Complete the following steps to view the cluster configuration.

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

   The **Cluster** page is displayed.

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

TABLE 18 Cluster Details

Field	Description	Active Cluster	Standby Cluster
Cluster Configuration			
IP Support	Displays the IP support version.	Yes	Yes
Cluster Redundancy			
Status	Displays the cluster redundancy status.	Yes	Yes
Cluster Redundant Role	States whether the cluster is an active or a standby cluster.	Yes	Yes
Mode	States whether the cluster is in monitor mode or backup mode. ● Monitor mode: Standby cluster serves the active cluster only when the active cluster is out-of-service. ● Backup mode: Standby cluster is always ready to accept external devices from the active cluster. Click **Alter monitoring status** to turn on or turn off the monitoring status of the active cluster. To remove the active cluster, select it from the list and click **Delete**.	No	Yes
Active Cluster	Displays the cluster name and control IP addresses of the cluster.	Yes	Yes
Standby Cluster	Displays the cluster name, management IP addresses, and control IP addresses of the cluster.	Yes	No
Serve Active Cluster Timing	Indicates when the standard cluster turns to backup mode and manages external devices (APs, DPs, and ICX switches). ● Only when active cluster is out-of-service (default setting) ● Always on service	No	Yes
Schedule Configuration Sync	● Status: Displays sync status. ● System Time Zone: Displays the system time zone set. ● Time: Displays the sync time followed every day. ● Last Trigger Time: Displays the date and time the clusters synced last. Applies to both scheduled sync or manually sync. ● Next Trigger Time: Displays the date and time of the next scheduled sync. ● Sync Now: Triggers manual configuration sync operation.	Yes	No
State	Displays the system configuration sync state.	Yes	No
Progress Status	Displays the progressive status of the system configuration sync.	Yes	No

Disabling Cluster Redundancy - Active-Standby from the Active Cluster

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

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

   The **Cluster** page appears.
2. Select the cluster, scroll down and click the **Configuration** tab.
3. On the right side of the **Configuration** area, click **Configure**.

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

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

Disabling Cluster Redundancy - Active-Standby from the Standby Cluster

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

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

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

   The **Cluster** page appears.
2. Select the cluster, scroll down and click the **Configuration** tab.
3. From the**Active Cluster** list, select the cluster and click **Delete**.

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

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

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

   The **Cluster** page appears.
2. Select the cluster, scroll down and click the **Configuration** tab.
3. On the right side of the **Configuration** area, click **Configure**.

   The **Edit Cluster** page appears.
4. In the Cluster Redundancy area, click the **Enable Cluster Redundancy** option, if this option is enabled and the button appears blue in color.

   In **Type**, choose **Active-Active**.
5. From the Target Active Cluster list, select the cluster and click **Delete**.

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

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

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

   The **Cluster** page appears.
2. Select the cluster, scroll down and click the **Configuration** tab.
3. On the right side of the **Configuration** area, click **Configure**.

   The **Edit Cluster** page appears.
4. In the Cluster Redundancy area, click the **Enable Cluster Redundancy** option to switch off the option.
5. Click **OK**.

Configuring the Control Plane

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

To configure a control plane:

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

> **NOTE**
> You must configure the **Control** interface, **IPv4 Cluster** interface, and**Management** interface to be on three different subnets. Failure to do so may result in loss of access to the web interface or failure of system functions and services.

TABLE 19 Configuring Control Plane

Field	Description	Your Action
Physical Interfaces		
IPv4-Control Interface	Indicates the management and IP control settings.	Select the **IP Mode**: • **Static** (*recommended*)—To manually assign an IP address to this interface manually. – Enter the **IP Address**. – Enter **Subnet Mask**. – Enter the **Gateway** router address. – Enter **Control NAT IP** address. • **DHCP**—To automatically obtain an IP address from a DHCP server on the network. – Enter **Control NAT IP**.

TABLE 19 Configuring Control Plane (continued)

Field	Description	Your Action
IPv4-Cluster Interface	Indicates the IPv4 cluster interface settings	Select the **IP Mode**: ● **Static** (*recommended*)—To manually assign an IP address to this interface manually. – Enter the **IP Address**. – Enter **Subnet Mask**. – Enter the **Gateway** router address. ● **DHCP**—To automatically obtain an IP address from a DHCP server on the network.
IPv4-Management Interface	Indicates the IPv4 management interface settings	Select the **IP Mode**: ● **Static** (*recommended*)—To manually assign an IP address to this interface manually. – Enter the **IP Address**. – Enter **Subnet Mask**. – Enter the **Gateway** router address. ● **DHCP**—To automatically obtain an IP address from a DHCP server on the network.
IPv6-Control Interface	Indicates the IPv6 control interface settings	Select the **IP Mode**: ● **Static** (*recommended*)—To manually assign an IP address to this interface manually. – Enter the IPv6 **IP Address** (global only) with a prefix length (for example, 1234::5678:0:C12/123) is required. Link-local addresses are unsupported. – Enter the IPv6 **Gateway** address (global or link-local) without a prefix length. For example, 1234::5678:0:C12 (global address without a prefix length) and fe80::5678:0:C12 (link-local address without a prefix length). ● **Auto**—To automatically obtain an IP address from Router Advertisements (RAs) or from a DHCPv6 server on the network.
IPv6-Management Interface	Indicates the IPv6 management interface settings	Select the **IP Mode**: ● **Static** (*recommended*)—To manually assign an IP address to this interface manually. – Enter the IPv6 **IP Address** (global only) with a prefix length (for example, 1234::5678:0:C12/123) is required. Link-local addresses are unsupported. – Enter the IPv6 **Gateway** address (global or link-local) without a prefix length. For example, 1234::5678:0:C12 (global address without a prefix length) and fe80::5678:0:C12 (link-local address without a prefix length). ● **Auto**—To automatically obtain an IP address from Router Advertisements (RAs) or from a DHCPv6 server on the network.

TABLE 19 Configuring Control Plane (continued)

Field	Description	Your Action
Access & Core Separation	Indicates that the management interface (core side) to be the system default gateway and the control interface (access side) to be used only for access traffic.	Select the **Enable** check box.
IPv4 Default Gateway & DNS	Indicates the IPv4 gateway that you want to use - Control, Cluster, and Management. **NOTE** When **Access & Core Separation** is enabled, the **Default Gateway** field is hidden. **NOTE** The default gateway is NOT set to Control Interface. To properly route AP/UE traffic back through Control Interface, please make sure to enable Access & Core Separation or add static routes in Control Plane Network Settings on Web GUI.	a. **Default Gateway**—Choose the Interface for which you want to assign the default gateway setting. b. **Primary DNS Server**—Enter the server details. c. **Secondary DNS Server**—Enter the server details.
IPv6 Default Gateway & DNS	Indicates the IPv6 gateway that you want to use - Control, Cluster, and Management. **NOTE** When **Access & Core Separation** is enabled, the **Default Gateway** field is hidden. **NOTE** The default gateway is NOT set to Control Interface. To properly route AP/UE traffic back through Control Interface, please make sure to enable Access & Core Separation or add static routes in Control Plane Network Settings on Web GUI.	a. **Default Gateway**—Choose the Interface for which you want to assign the default gateway setting. b. **Primary DNS Server**—Enter the server details. c. **Secondary DNS Server**—Enter the server details.
User Defined Interfaces **NOTE** The control plane and the UDI must be on different subnets. If the control plane and UDI are on the same subnet, and assigned the same IP address, APs will be unable to communicate with the control plane. If the control plane and UDI are on the same subnet and assigned different IP addresses, hotspot clients will not be redirected to the logon URL for user authentication.		
Name	Indicates the name of the interface.	Enter a name.
Physical Interfaces	Indicates the physical interface.	Select **Control Interface**.
Service	Indicates the service.	Select **Hotspot**, the hotspot must uses the control interface as its physical interface.
IP Address	Indicates the IP address that you want to assign to this interface.	Enter the IP address.
Subnet Mask	Indicates the subnet mask for the IP address.	Enter the subnet mask.
Gateway	Indicates the IP address of the gateway router.	Enter the gateway IP address.
VLAN	Indicates the VLAN ID that you want to assign to this interface.	Enter the VLAN ID.
Add	Adds the interface settings.	Click **Add**.

TABLE 19 Configuring Control Plane (continued)

Field	Description	Your Action
Static Routes		
Network Address	Indicates the destination IP address of this route.	Enter the IP address.
Subnet Mask	Indicates a subnet mask for the IP address.	Enter the subnet mask.
Gateway	Indicates the IP address of the gateway router.	Enter the IP address of the gateway router.
Interface	Indicates the physical interface to use for this route.	Select the interface.
Metric	Represents the number of routers between the network and the destination.	Enter the number of routers.
Add	Adds the static route settings.	Click **Add**.

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

Rebalancing APs

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

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

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

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

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

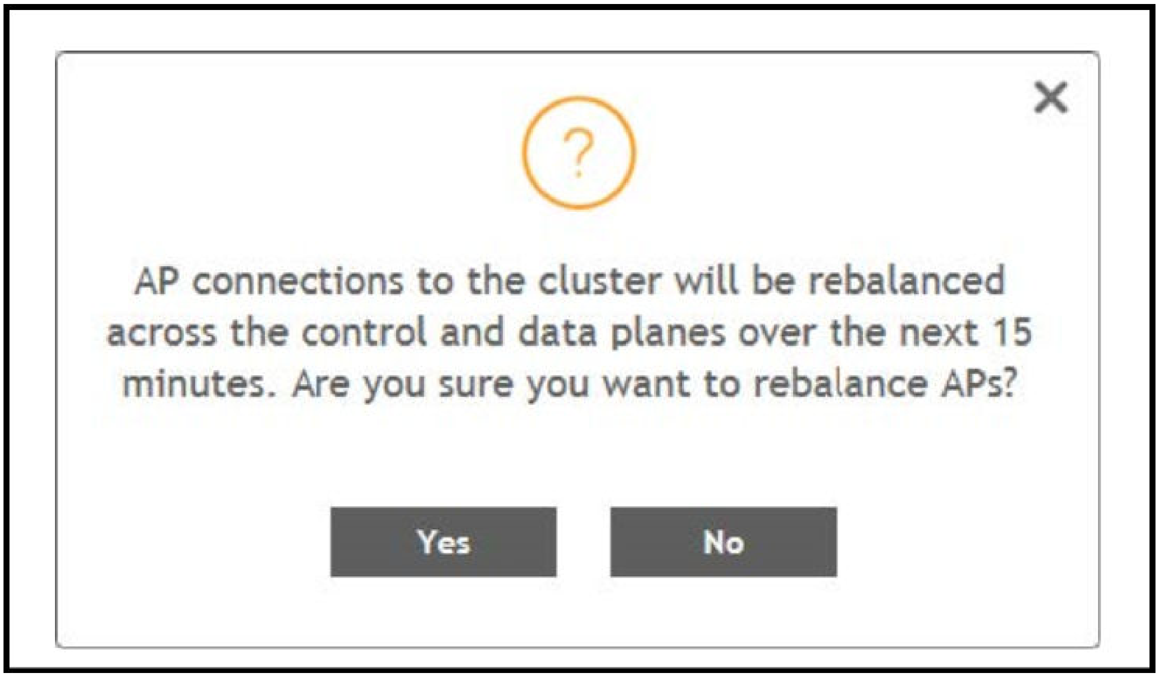
   - **Event 770: Generate ApConfig for plane load rebalance succeeded.**
   - **Event 771: Generate ApConfig for plane load rebalance failed.**

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

To rebalance APs across the nodes:

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

FIGURE 77 AP Rebalancing Form



AP connections to the cluster will be rebalanced across the control and data planes over the next 15 minutes. Are you sure you want to rebalance APs?

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

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

Configuring the Data Plane

By default, the controller sends traffic from its data plane from a single interface.

NOTE
This feature is managed only by vSZ-E and vSZ-H controllers.

If your organization's network requires separation of the access and core traffic, configure access and core separation on the controller.

To configure a data plane:

1. Go to **Network** > **Data and Control Plane** > **Cluster**.
2. Select the data plane from the list and click **Configure**.The Edit Data Plane Network Settings form appears.
3. Configure the settings as explained in Table 20.
4. Click **OK**.

TABLE 20 Configuring Data Plane

Field	Description	Your Action
Network		
Interface Mode	Indicates the traffic direction.	Choose the option: ● **Single Interface** (default)—For the controller to send traffic from its data plane from a single interface. ● **Access and Core Interface**—For the controller to send traffic to the access and core networks separately. NOTE To separate the access and core networks – Use static routes, if the data plane is required to connect to IP addresses in the core network (for example, for DHCP relay or L2oGRE termination) and the destination IP addresses are not part of the core subnet. ● **Keep original configuration**—For the controller to keep the original manual Data Plane setup.
Network > **Primary (Access) Interface**		
IP Mode	Indicates the mode of assigning the IP address to this interface.	Select the option: ● **Static** (*recommended*)—To manually assign an IP address to this interface manually. – Enter the **IP Address**. – Enter **Subnet Mask** for the IP address. – Enter the **Gateway** router address. – Enter the **Primary DNS Server** IP address. – Enter the **Secondary DNS Server** IP address. – Enter **VLAN** ID to tag traffic. – Choose the **Data NAT IP/Port Configured** option. – Enter **Data NAT IP** address. – Enter **Data NAT Port** address. ● **DHCP**—To automatically obtain an IP address from a DHCP server on the network. – Enter **VLAN** ID to tag traffic. – Choose the **Data NAT IP/Port Configured** option.
Network > **IPv6 Primary (Access) Interface**		
IP Mode	Indicates the mode of assigning the IP address to this interface.	Select the option: ● **Static** (*recommended*)—To manually assign an IP address to this interface manually. – Enter the **IP Address**. – Enter the **Gateway** router address. – Enter the **Primary DNS Server** IP address. – Enter the **Secondary DNS Server** IP address. ● **Auto**—To automatically obtain an IP address from a DHCP server on the network.
Network > **Secondary (Core) Interface** (applicable for **Interface Mode**: **Access and Core Interfaces**)		
IP Address	Indicates the IP address of the core network interface.	Enter the IP address. NOTE The secondary/core interface IP address must be configured manually; DHCP is unsupported.
Subnet Mask	Indicates the IP address of the subnet mask.	Enter the subnet mask.

TABLE 20 Configuring Data Plane (continued)

Field	Description	Your Action
VLAN	Indicates that the traffic is tagged with a VLAN ID.	Enter the VLAN ID. **NOTE** If VLANS are configured on both the access and core networks, the VLAN ID that you enter here must be different from the one that you entered for the primary/access interface. **NOTE** You cannot configure the IP address and VLAN settings for a virtual Data Plane from the Primary (Access) and Secondary (Core) Interface sections. Only vSZ-H supports virtual Data Plane.
Disconnect AP when core link down	Indicates that the AP is disconnected secondary core link is down.	Select the check box.
Static Routes		
Network Address	Indicates the destination IP address of this route.	Enter the IP address.
Subnet Mask	Indicates a subnet mask for the IP address.	Enter the subnet mask.
Gateway	Indicates the IP address of the gateway router.	Enter the IP address of the gateway router.
Add	Adds the static route settings.	Click **Add**.
CALEA Relay		
Mark this Data Plane as CALEA Relay (This feature is supported only for vSZ-E and vSZ-H controllers)	Indicates that the data plane uses CALEA relay.	Select the check box.
DHCP Profile		
DHCP Profile	Indicates the data plane DHCP service profile.	Choose the DHCP service profile from the drop-down.
NAT Profile		
NAT Profile	Indicates the data plane NAT service profile.	Choose the NAT service profile from the drop-down.
Syslog		
Enable DHCP syslog	Enables syslog to record the DHCP logs.	Select the check box.
Enable NAT syslog	Enables syslog to record the NAT logs.	Select the check box.
Syslog Server IP	Indicates the IP address of the remote syslog server.	Enter the IP address of the remote syslog server.
Syslog Server Port	Indicates the port number of the remote syslog server.	Enter the Port number of the remote syslog server.

NOTE
You can restart a data plane. To do so, select the data plane from the list and click **Restart**.

NOTE
You can approve or delete a data plane. To do so, select the data plane from the list and click **Approve** or **Delete** respectively. You can also download debug logs or switch over clusters. To do so, select the data plane from the list, click **More** and select **Download** or **Switch Over Clusters** respectively.

NOTE
All configuration changes applicable to vSZ-H are also applicable to SZ100-D.

Monitoring Cluster Settings

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

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

Clearing or Acknowledging Alarms

You can clear or acknowledge an alarm.

To clear an alarm:

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

To acknowledge an alarm:

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

Filtering Events

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

To apply filters:

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

   The Apply Filters form appears.

2. Complete the following criteria.
   - **Severity**: Select a severity level to filter the list of events.

- **Cateogry**: Select a category from the list.
- **Date and Time**: Select the events by their **Start** and **End** dates.

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

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

Creating a DP Group

The vSZ-D version in the same DP group must be the same for consistent AP/DP functioning.

NOTE
Creating a DP group affinity profile is supported only for vSZ-E and vSZ-H platforms.

Complete the following steps to create a DP group.

1. Select **Network** > **Data and Control Plane** > **DP group**.
2. Click **Create**.

   The **Create DP group** form is displayed.
3. Enter a **Name** and **Description** for the DP group.
4. Click **Add**.

   The **Add DP** page is displayed.
5. Select Data Plane from the list and click **OK**.

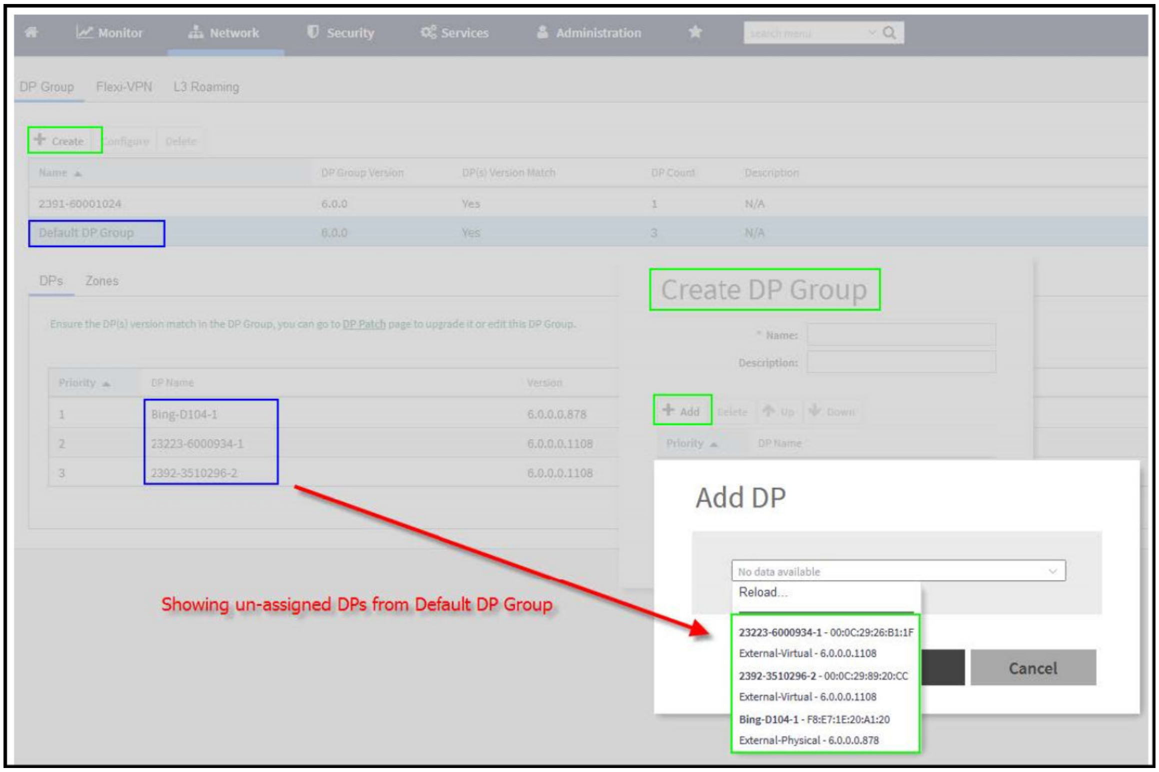
   NOTE
   - While SZ is upgrading from an older version to a newer version, the system validates whether any DP is assigned a duplicate. If a duplicate is encountered, the following warning message is displayed:

     ```
     There is an over-assigned DP in the DP Zone Affinity profiles. Please go to the
     DP Zone Affinity page to edit and make sure only one DP profile is assigned at
     the same time.
     ```
     Once the over-assigned DPs are removed, SZ can upgrade the system.
   - After the configuration that included the over-assigned profiles has been restored, the following message notifies you to correct the configuration:

     ```
     The overlapping DP Group has been detected. There is the over-assigned DP in DP
     Group. Please go to DP Group page to edit and make sure the DP only one DP Group
     assigned at the same time.
     ```

   .

FIGURE 78 Creating a DP Group



Name	DP Group Version	DP(s) Version Match	DP Count	Description
2391-60001024	6.0.0	Yes	1	N/A
Default DP Group	6.0.0	Yes	3	N/A

Ensure the DP(s) version match in the DP Group, you can go to DP Patch page to upgrade it or edit this DP Group.

Priority	DP Name	Version
1	Bing-D104-1	6.0.0.0.878
2	23223-6000934-1	6.0.0.0.1108
3	2392-3510296-2	6.0.0.0.1108

* Name:

Description:

No data available

23223-6000934-1 - 00:0C:29:26:B1:1F
External-Virtual - 6.0.0.0.1108
2392-3510296-2 - 00:0C:29:89:20:CC
External-Virtual - 6.0.0.0.1108
Bing-D104-1 - F8:E7:1E:20:A1:20
External-Physical - 6.0.0.0.878

.

6. Click **OK**.

   NOTE
   You can edit or delete a DP group. To do so, select the DP Group from the list and click **Configure** or **Delete** respectively.

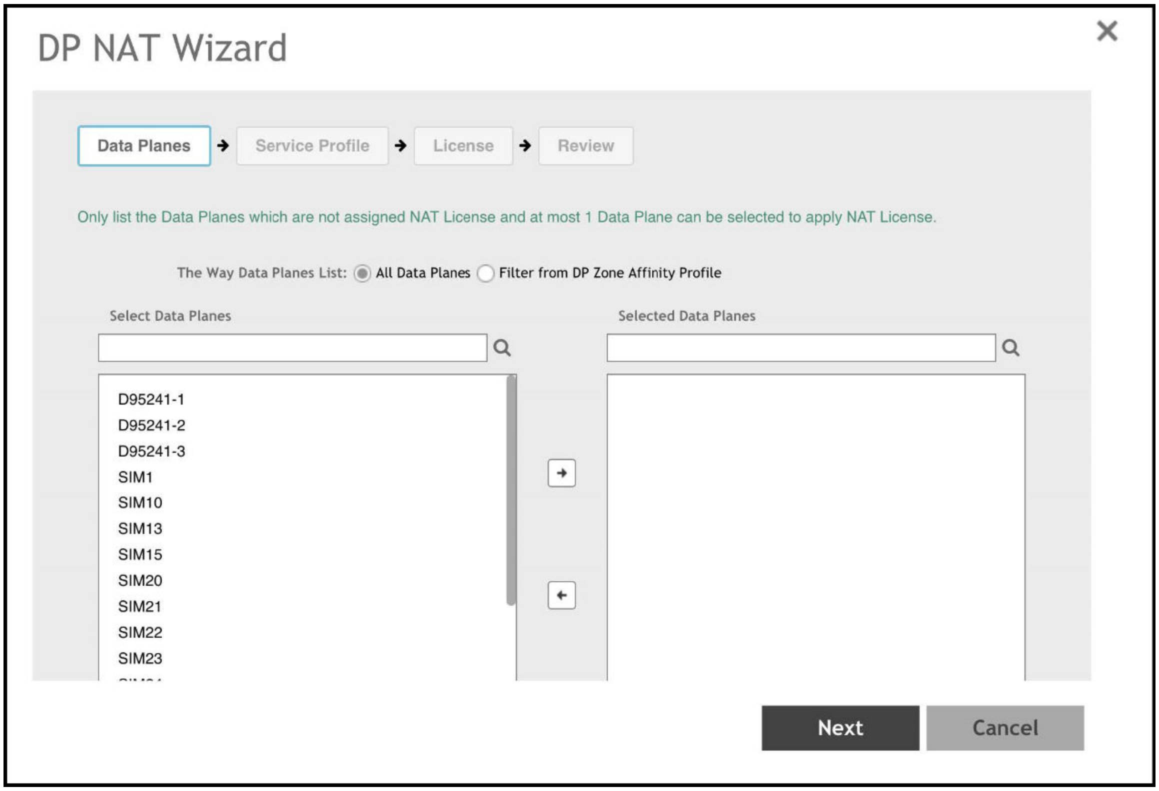
Verifying DP Version Match

From the list, the **DP(s) Version Match** column indicates **Yes** if all the DPs have the same version in the DP Group and **No** if the DPs have different versions in the DP group. You can click the **DP(s)** tab to verify the version of the DP.

DP NAT License Assignment

1. Select the data plane.
2. Option 1 let the user select filter to apply.
3. The "Select Data Planes" is listing DP(s) filtering by option 1.
4. In "Select Data Planes" area, only list DP(s) which has not assigned NAT license.

FIGURE 79 DP NAT WIZARD



DP NAT Wizard

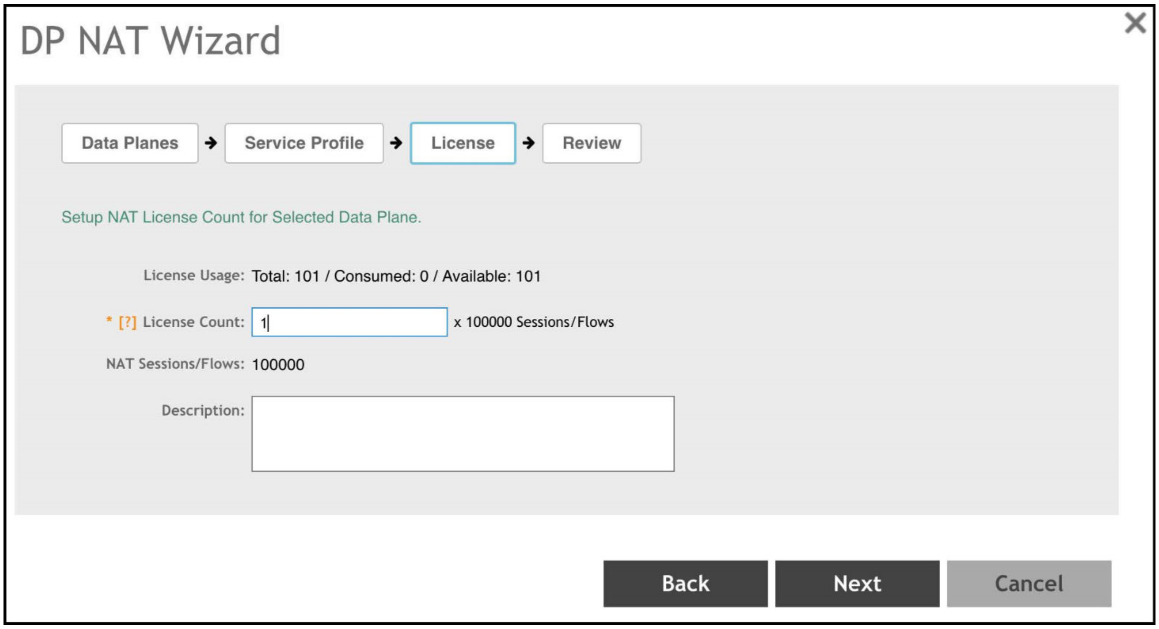
Only list the Data Planes which are not assigned NAT License and at most 1 Data Plane can be selected to apply NAT License.

The Way Data Planes List: ● All Data Planes ○ Filter from DP Zone Affinity Profile

1. Select the NAT service profile.
2. In NAT service profile option, only list the profile which has not assigned to DP.
3. The existed service profile on DP will be replaced after the wizard completed.

Allocate the sufficient license for DP NAT.

FIGURE 80 DP NAT WIZARD License



DP NAT Wizard

Setup NAT License Count for Selected Data Plane.

License Usage: Total: 101 / Consumed: 0 / Available: 101

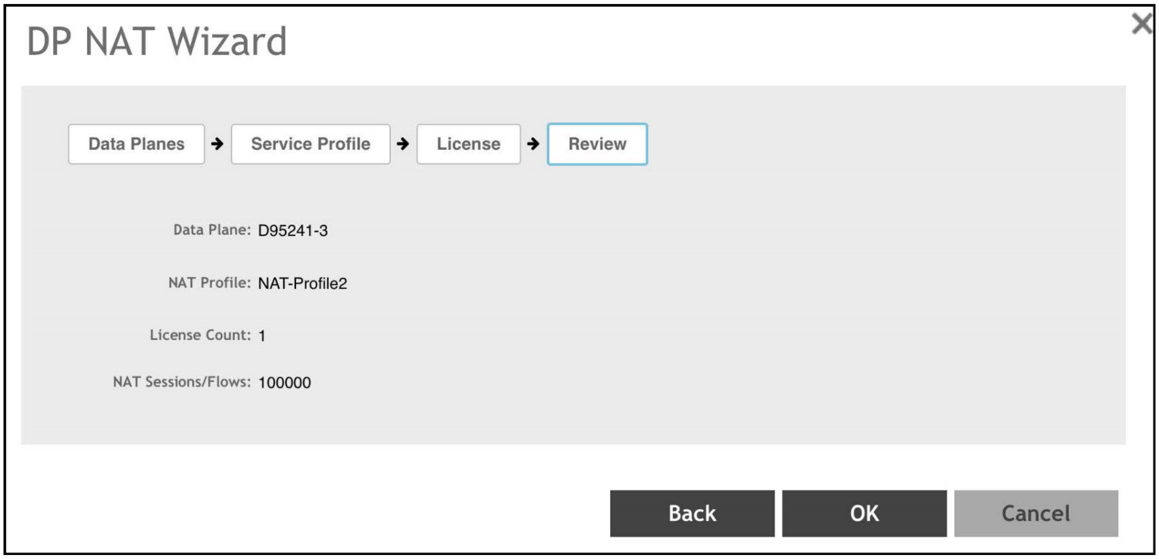
* [?] License Count: 1 x 100000 Sessions/Flows

NAT Sessions/Flows: 100000

Description:

Review all DP NAT configuration before applying.

FIGURE 81 DP NAT WIZARD Review



DP NAT Wizard

Data Plane: D95241-3

NAT Profile: NAT-Profile2

License Count: 1

NAT Sessions/Flows: 100000

Enabling Flexi VPN

You can enable Flexi-VPN and limit the network resources that a UE can access. Flexi-VPN allows an administrator to customize the network topology, and is thereby able to control the network resources accessible to the end-user. This feature is only supported on vSZ-E and vSZ-H, and is enabled by purchasing the Flexi-VPN license.

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

   The **Flexi-VPN** status page is displayed.
2. Select **Flexi-VPN**.

   NOTE
   The Flexi-VPN option is available only if the Access-VLAN ID is configured in manual mode, and when VLAN Pooling, Dynamic VLAN and Core Network VLAN options, and Tunnel NAT are disabled.

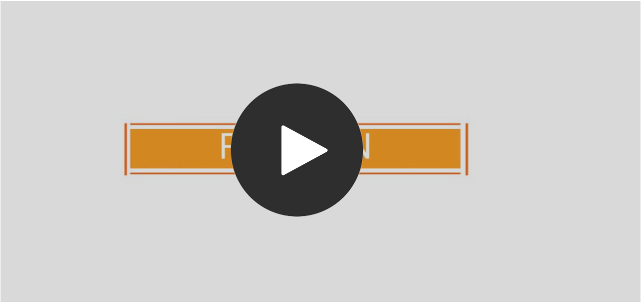
   NOTE
   Flexi-VPN is activated when a Flexi-VPN profile is assigned to a WLAN.

   NOTE
   A maximum of 1024 WLAN IDs can be applied to a Flexi-VPN profile.
   Flexi-VPN supports IPv4 addressing formats and Ruckus GRE tunnel protocol. It does not support IPv6 addressing formats.

The following record table indicates that the Flexi-VPN profile is successfully applied to the WLAN:

- WLAN: displays the name of the WLAN
- Zone: displays the name of the zone.
- Zone Affinity Profile: displays the name of the source data plane from which tunneled traffic starts
- Flexi-VPN Profile: displays the name of the destination data plane to where the tunneled traffic terminates

VIDEO
Flexi-VPN Overview. This video provides a brief overview of Flexi-VPN.



Click to play video in full screen mode.

Enabling L3 Roaming Criteria for DP

Using the layer 3 roaming feature, clients can roam across APs in the network (from one data plane to another data plane). This is typically required when the number of clients in the network increases and clients have to roam from a network that they were connected to, to another WLAN network with similar access settings. This feature enables seamless roaming and ensures session continuity between the client and the network.

NOTE
L3 roaming is only supported on vSZ-H and vSZ-E.

You can configure the roaming criteria for a DP so that it uses one of these two options - UE subnet or WLAN VLAN to access another DP to connect to, within a network. Before this, you must ensure that the L3 roaming feature is enabled in the DP.

1. From the main menu, go to **Network** > **Data and Control Plane** > **L3 Roaming**.

   The **L3 Roaming** page is displayed.
2. Select **L3 Roaming**.
3. Click **Configure** to edit the L3 roaming settings.

   The **Edit L3 Roaming** page is displayed.
4. From **Activate**, you can enable the feature for the DP by selecting Enable or Disable from the drop-down menu.
5. From the **Roaming Criteria** list, select one of the following options to define the data format to establish connection between DPs: UE Subnet or WLAN VLAN.
6. Click **OK**.

You have successfully enabled L3 roaming, and also set the roaming criteria based on which DPs would connect within the network.

> **NOTE**
> If there are more than 40 DPs been approved, the controller limits you to use L3 Roaming.

> **NOTE**
> A fresh controller software installation or upgrade from a version that does not support L3 roaming resets the L3 roaming configuration and it remains disabled. You must enable L3 roaming on a DP again.

Powering Cluster Back

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

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

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

Events and Alarms

Events

Event

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

Viewing Events

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

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

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

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

FIGURE 82 Search Events with OR Option

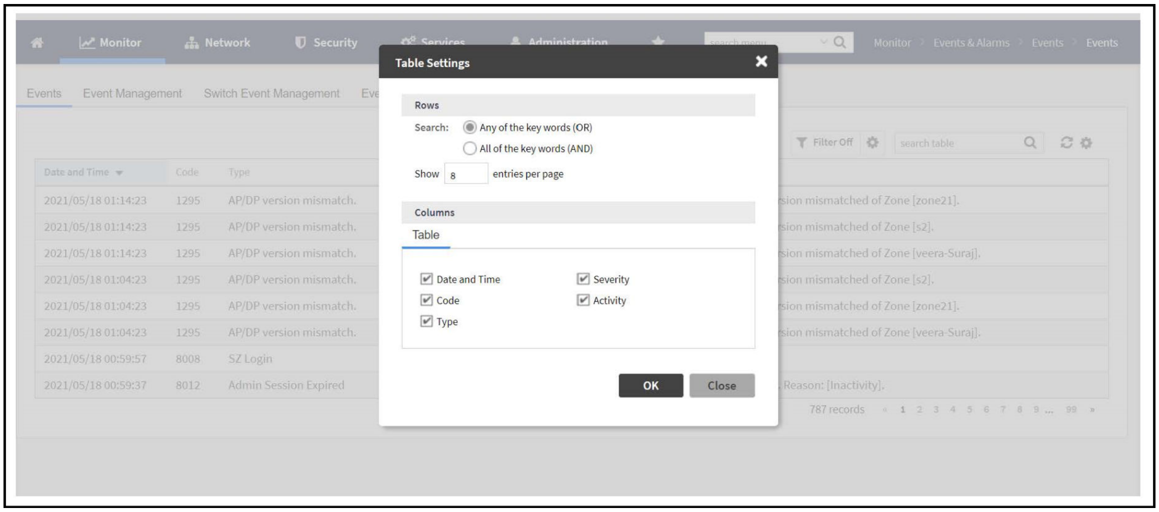


Table Settings

Rows

Search: ● Any of the key words (OR)
○ All of the key words (AND)

Show 8 entries per page

Columns

Table

☑ Date and Time ☑ Severity
☑ Code ☑ Activity
☑ Type

FIGURE 83 Search Events with AND Option

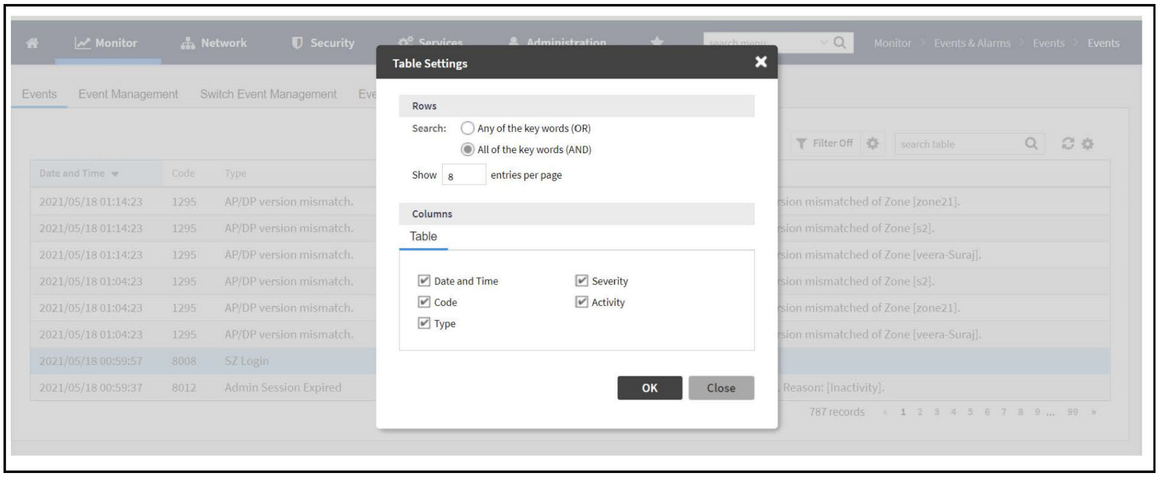


Table Settings

Rows

Search: ○ Any of the key words (OR)
● All of the key words (AND)

Show 8 entries per page

Columns

Table

☑ Date and Time ☑ Severity
☑ Code ☑ Activity
☑ Type

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

Switch Event Management

Sending SNMP Traps and Email Notifications for Switch Events

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

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

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

To configure switch event management:

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

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

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

  System Domain: Displays global setting for Switch event.

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

  Partner Domain: Displays notification setting for the partner domain.

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

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

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

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

Event Management

Sending SNMP Traps and Email Notifications for Events

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

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

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

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

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

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

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

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

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

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

Following information related to the event are displayed:

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

Event Threshold

Configuring Event Threshold

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

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

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

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

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

Switch Custom Events

Creating Custom Events for ICX Switches

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

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

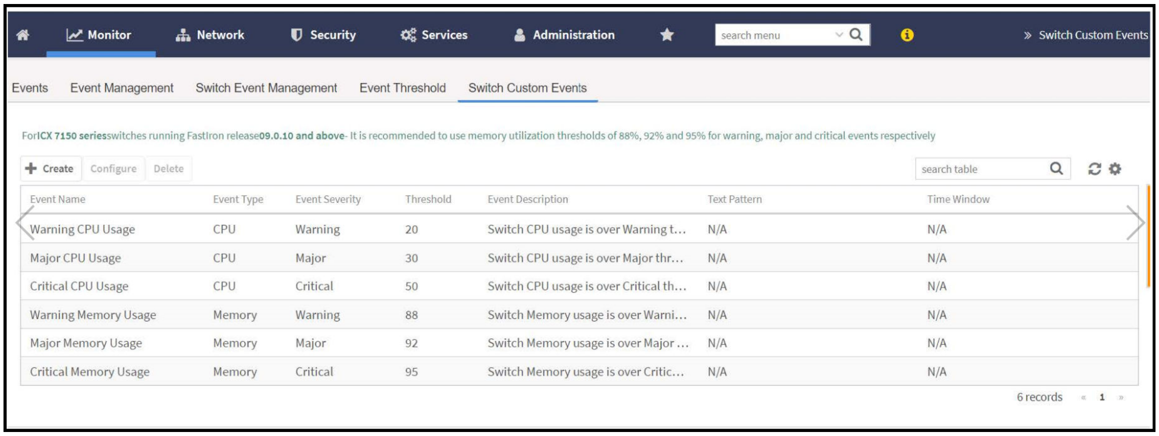
To create a customer event, perform the following steps.

NOTE
DB Persistence must be enabled to generate custom events.

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

   This displays **Switch Custom Events** page.

FIGURE 84 Types of custom events available



ForICX 7150 seriesswitches running FastIron release09.0.10 and above- It is recommended to use memory utilization thresholds of 88%, 92% and 95% for warning, major and critical events respectively

Event Name	Event Type	Event Severity	Threshold	Event Description	Text Pattern	Time Window
Warning CPU Usage	CPU	Warning	20	Switch CPU usage is over Warning t...	N/A	N/A
Major CPU Usage	CPU	Major	30	Switch CPU usage is over Major thr...	N/A	N/A
Critical CPU Usage	CPU	Critical	50	Switch CPU usage is over Critical th...	N/A	N/A
Warning Memory Usage	Memory	Warning	88	Switch Memory usage is over Warni...	N/A	N/A
Major Memory Usage	Memory	Major	92	Switch Memory usage is over Major ...	N/A	N/A
Critical Memory Usage	Memory	Critical	95	Switch Memory usage is over Critic...	N/A	N/A

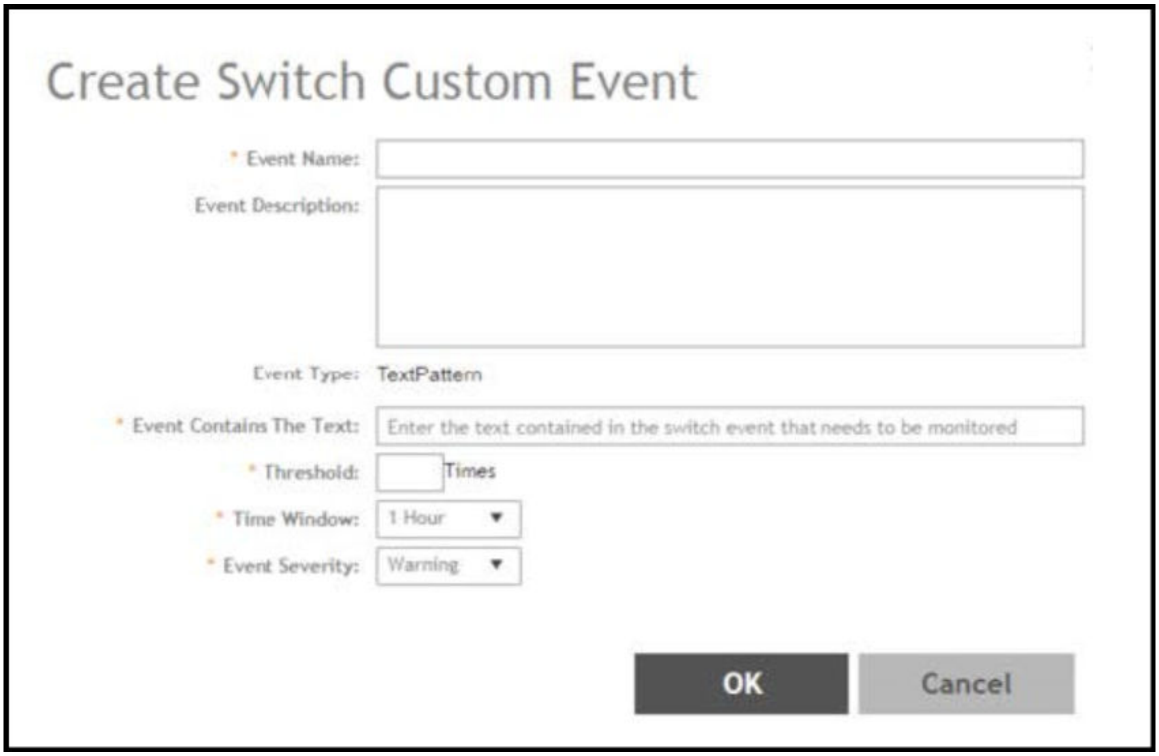
6 records « 1 »

2. Click **Create**.

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

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

   FIGURE 85 Creating custom events for switches - TextPattern type

   Create Switch Custom Event

   * Event Name:

   Event Description:

   Event Type: TextPattern

   * Event Contains The Text: Enter the text contained in the switch event that needs to be monitored

   * Threshold: Times

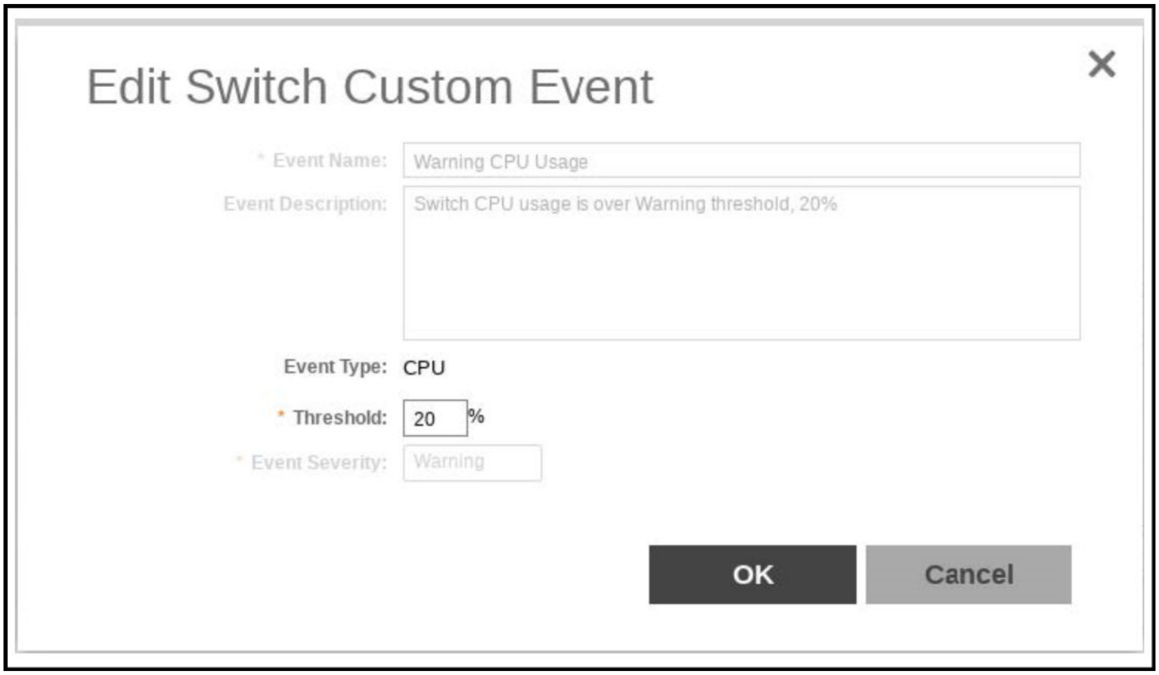
   * Time Window: 1 Hour

   * Event Severity: Warning

   Configure the following:

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

FIGURE 86 Editing custom events for switches - CPU/Memory type



Edit Switch Custom Event

* Event Name: Warning CPU Usage

Event Description: Switch CPU usage is over Warning threshold, 20%

Event Type: CPU

* Threshold: 20 %

* Event Severity: Warning

Configure the following:

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

3. Click **OK**.

Alarms

Configuring Alarms

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

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

- Date and Time: Displays the date and time when the alarm was triggered.
- Code: Displays the alarm code (see the Alarm and Reference Guide for your controller platform for more information).
- Alarm Type: Displays the type of alarm event that occurred (for example, AP reset to factory settings).
- Severity: Displays the severity level assigned to the events such as Critical, Major, Minor and Warning.
- Status: Indicates whether the alarm has already been cleared or still outstanding.

- Activity: Displays additional details about the alarm, including (if available) the specific access point, control plane, or data plane that triggered the alarm.
- Acknowledged On: Displays the date and time when the administrator acknowledge the alarm.
- Cleared By: Displays information about who cleared the alarm.
- Cleared On: Displays the date and time when the alarm was cleared.
- Comments: Displays administrator notes recorded during alarm management.

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

Clearing Alarms

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

To clear an alarm:

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

Acknowledging Alarms

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

To acknowledge an alarm:

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

   This message appears:

   ```
   Are you sure you want to acknowledge the selected alarms?
   ```
   .
2. Select **Yes**.

Applying Filters

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

1. Click the ⚙ icon.

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

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

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

   c. Date and Time: Select the alarms by their start and end dates.

2. Click **OK**.

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

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

File Transfer Protocol

Configuring File Transfer Protocol Server Settings

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

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

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

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

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

Replacing Hardware Components

This section describes replacement of hardware components (including hard disk drives, power supply units, and system fans) on the controller.

Installing or Replacing Hard Disk Drives

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

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

Ordering a Replacement Hard Disk

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

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

Removing the Front Bezel

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

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

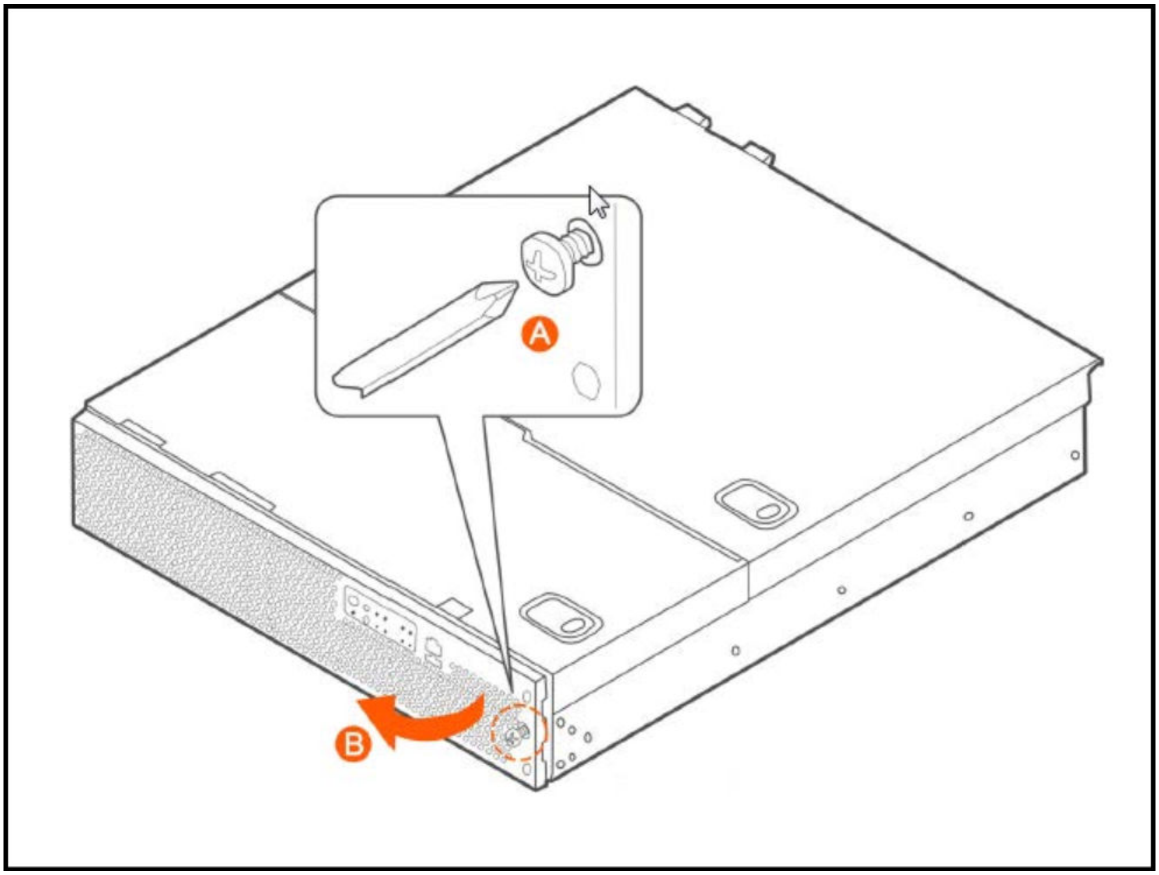
You need to remove the front bezel for tasks such as:

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

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

1. Loosen the captive bezel retention screw on the right side of the bezel (see A in Figure 87).
2. Rotate the bezel to the left to free it from the pins on the front panel (see B in Figure 87), and then remove it.

FIGURE 87 Removing the front bezel



Removing an HDD Carrier from the Chassis

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

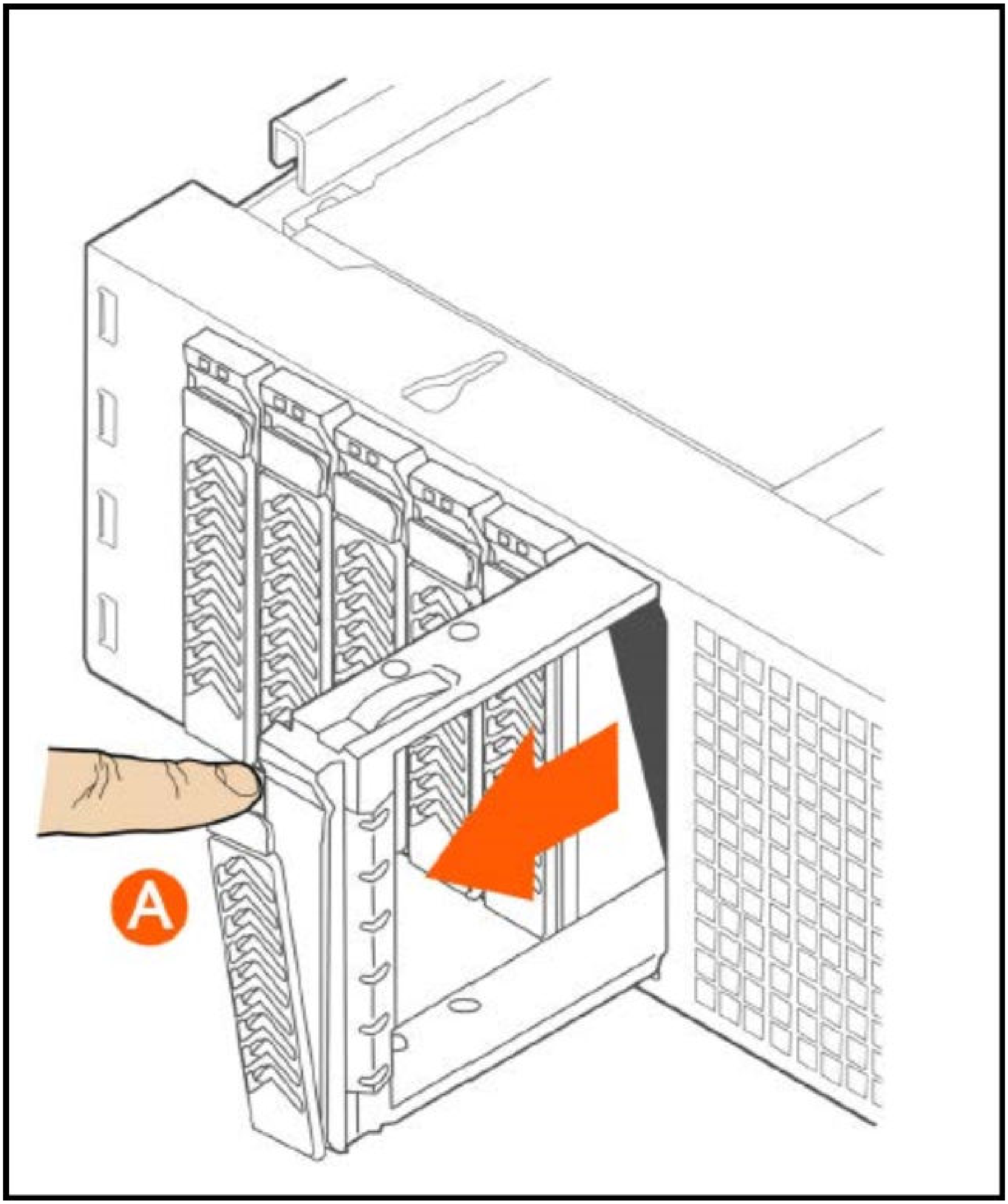
1. Remove the front bezel (see Removing the Front Bezel on page 157).
2. Select the drive bay where you want to install or replace the drive.

   Drive bay 0 must be used first, then drive bay 1 and so on. The drive bay numbers are printed on the front panel below the drive bays.
3. Remove the drive carrier by pressing the green button to open the lever.

   (See A in Figure 88).

4. Pull the drive carrier out of the chassis.

FIGURE 88 Removing the drive carrier

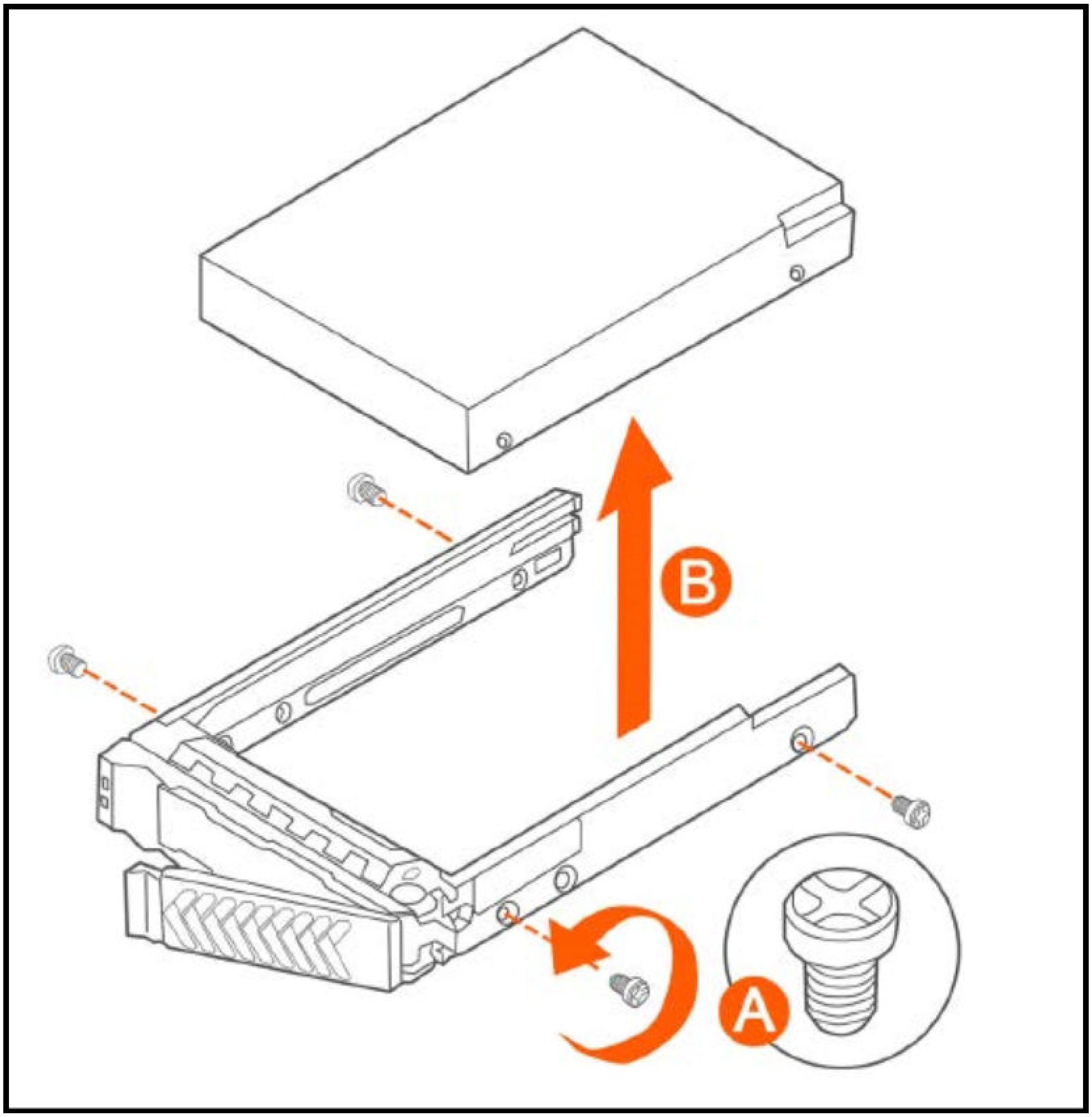


Installing a Hard Drive in a Carrier

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

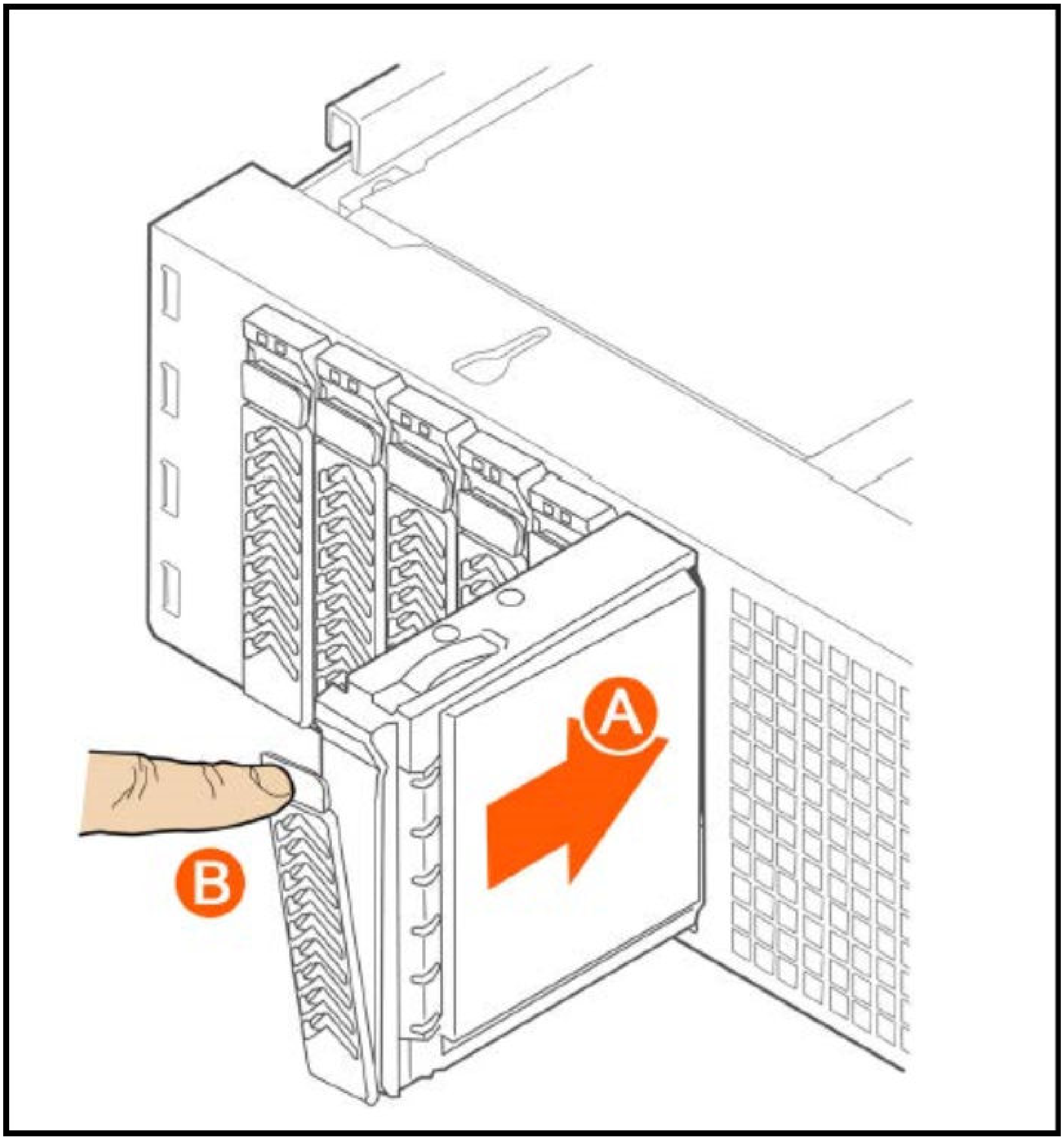
1. If a drive is already installed (that is, if you are replacing the drive), remove it by unfastening the four screws that attach the drive to the drive carrier (see A in Figure 89). Set the screws aside for use with the new drive.
2. Lift the drive out of the carrier (see B in Figure 89).

FIGURE 89 Removing the hard drive



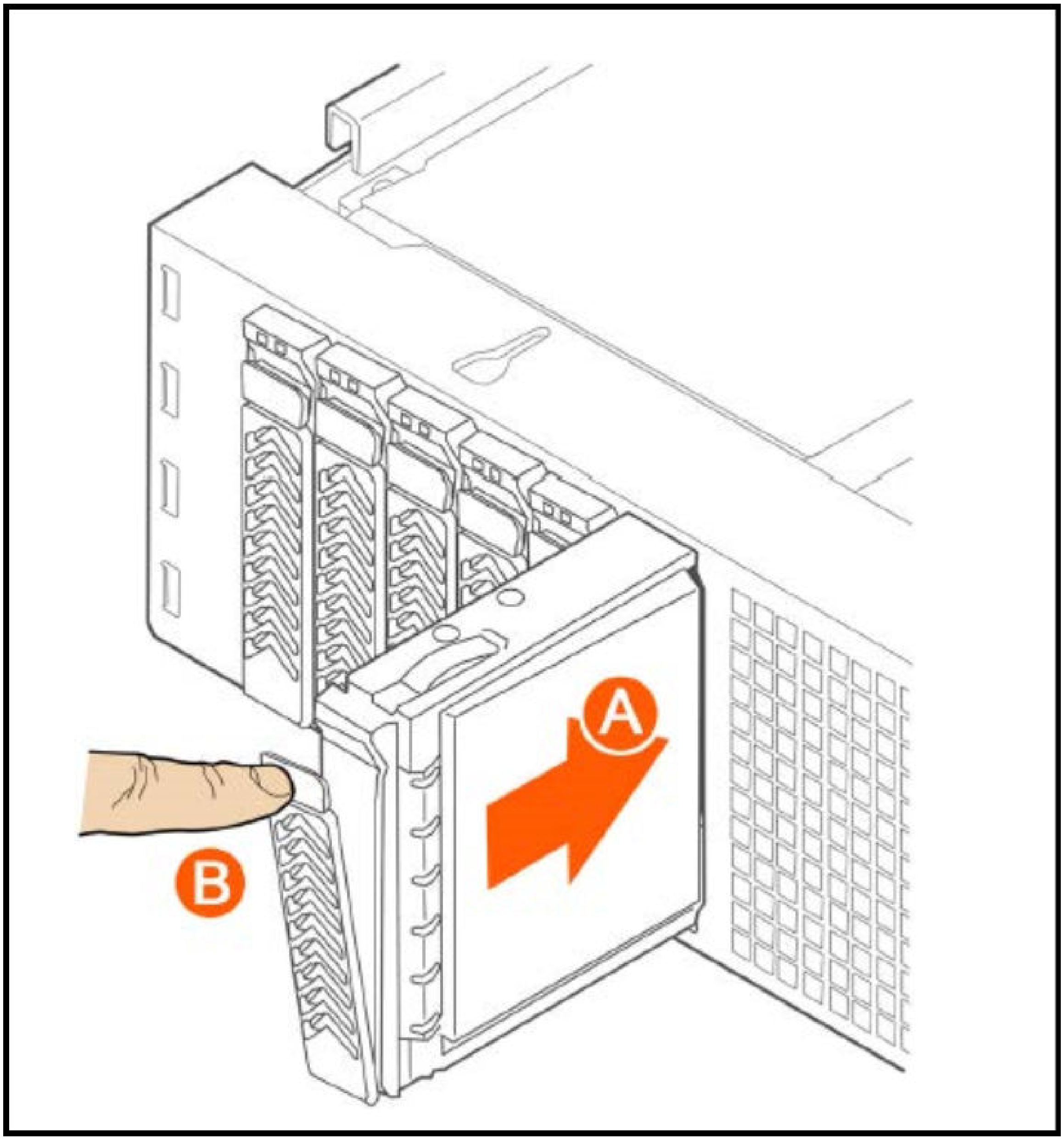
3. Install the new drive in the drive carrier (see A in Figure 90), and then secure the drive with the four screws that come with the carrier (see B).

FIGURE 90 Installing the hard drive



4. With the drive carrier locking lever fully open, push the hard drive carrier into the drive bay in the chassis until it stops (see A in Figure 91).

FIGURE 91 Inserting the carrier back into the chassis



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

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

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

Reinstalling the Front Bezel

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

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

Replacing PSUs

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

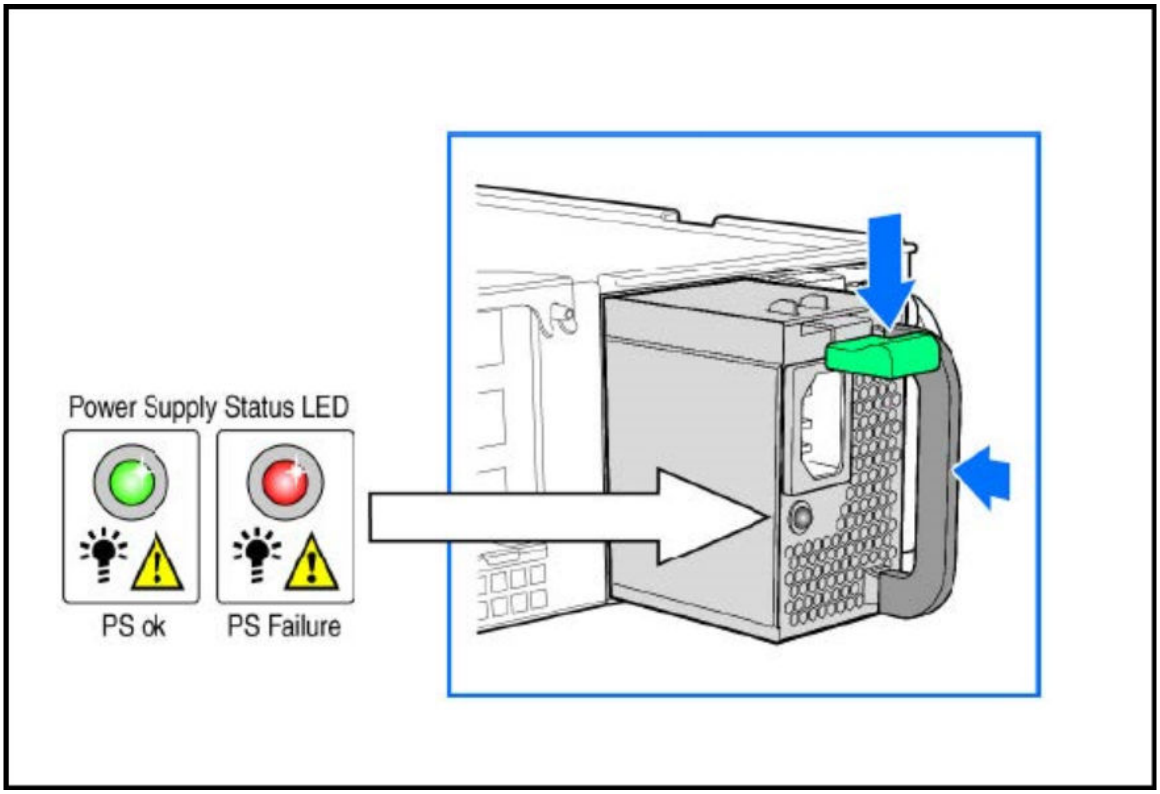
Follow these steps to remove and replace a PSU.

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

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

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

FIGURE 92 Replacing a PSU



Replacing System Fans

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

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

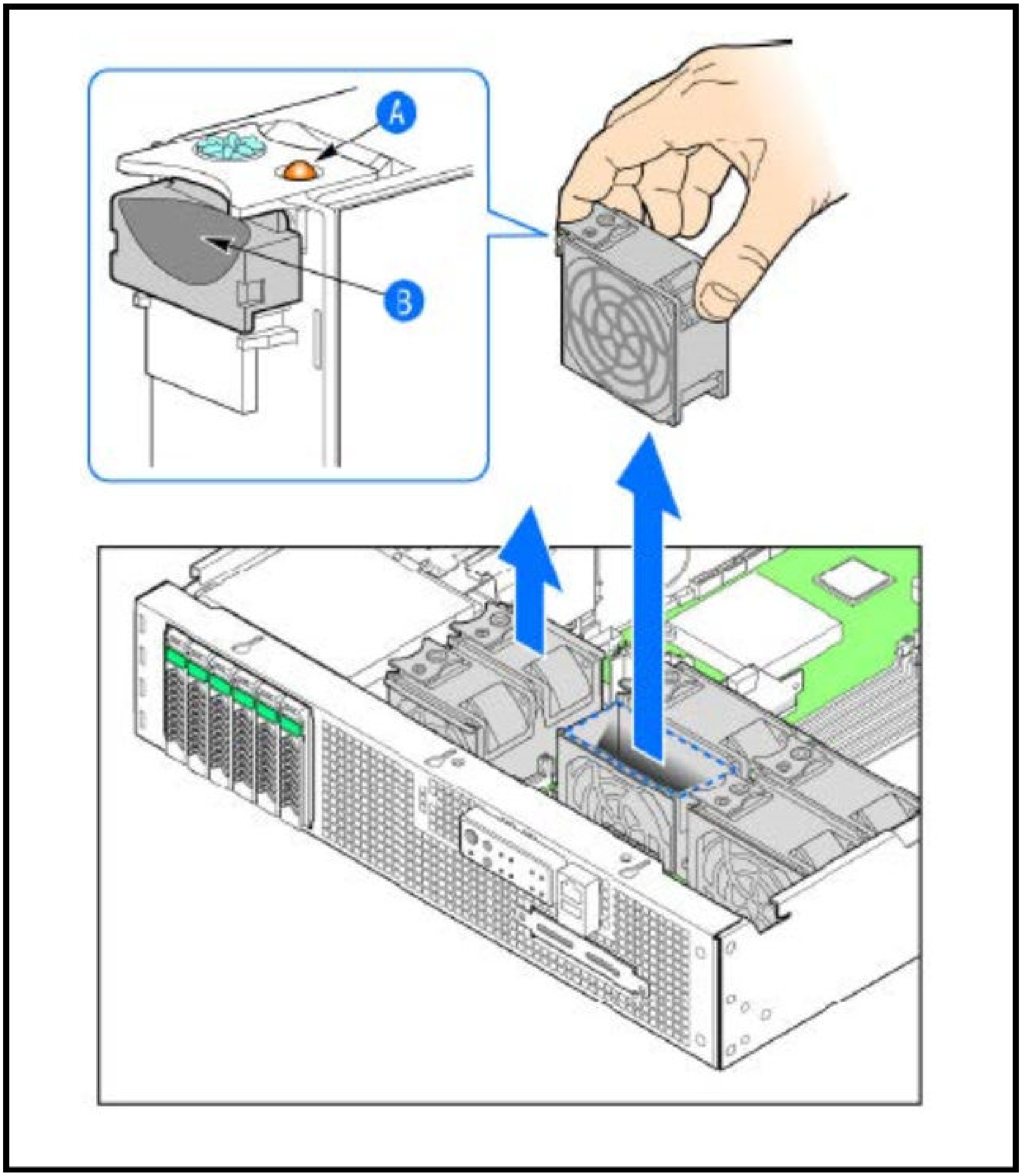
Electrostatic discharge (ESD) can damage internal components such as printed circuit boards and other parts. RUCKUS recommends that you only perform this procedure with adequate ESD protection. At a minimum, wear an anti-static wrist strap attached to the ESD ground strap attachment on the front panel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

Follow these steps to replace a system fan.

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

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

FIGURE 93 Replacing a system fan



MVNO

Managing Mobile Virtual Network Operator (MVNO) Accounts

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

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

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

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

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

3. Configure the following:
    a. The Mobile Virtual Network Operator Summary
        1. 'Domain Name: Type a domain name to which this account will be assigned
        2. Description: Type a brief description about this domain name.
    b. AP Zones of Mobile Virtual Network Operator: Displays the AP zones that are allocated to this MVNO account
        1. Click **Add AP Zone**. The **Add AP Zone** page appears.
        2. AP Zone: Select the AP zone you want to add to the MVNO account from the drop-down menu.
        3. Click **OK**.

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

    c. WLAN Services: Configure the WLAN services to which the MVNO account that you are creating will have management privileges.
        1. Click **Add WLAN**. The **Add WLAN** page appears.
        2. SSID: Select the WLAN to which the MVNO account will have management privileges.

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

        3. Click **OK**.
    d. Super Administrator: Configure and define the logon details and management capabilities that will be assigned to the account.
        1. Account Name: Type the name that this MVNO will use to log on to the controller.
        2. Real Name: Type the actual name (for example, John Smith) of the MVNO.
        3. Password: Type the password that this MVNO will use (in conjunction with the Account Name) to log on to the controller.
        4. Confirm Password: Type the same password as above. f) In Phone, type the phone number of this MVNO.
        5. Phone: Type the phone number of the administrator.
        6. Email: Type the email address of this MVNO.
        7. Job Title: Type the job title or position of this MVNO in his organization.
    e. RADIUS Server for Administrator Authorization and Authentication: See Configuring SmartZone Admin AAA Servers on page 49 for more information.
4. Click **OK**.

You have created an MVNO account.

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

Administrator Activities

Monitoring Administrator Activities

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

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

   The following information is displayed:

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

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

Support Information

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

To access these guides, select **Adminstraion** > **Help** and select the required guide.

Rest API

The following table shows the Rest API support rates for read and write operations.

TABLE 21 SmartZone Rest API Support Rate

Release Summary	Rate (requests)	Description
SZ API Read Support Rate	170 / min	Includes POST and GET calls to query or list objects in SmartZone.
SZ API Write Support Rate	135 / min	Includes POST, PUT, and PATCH calls to create or edit objects in SmartZone.

NOTE
The above test results must be used as a guidance and customers are advised to test the API in their own environment to determine its suitability for specific use case.

Refer to the following table for the test bed and test conditions used in this specific use case scenario.

TABLE 22 Test Bed and Test Conditions

vSZ-H Parameter	Value
Software Version	6.1.1.0.959 and later
vCPUs	24
Memory	48 GB
SSD Storage	600 GB
Number of Nodes	2 (1 NIC)
Number of Domains	1,000 partner domains + 1,000 regular domains
Number of Zones	10,000
Number of APs	10,000
Number of WLANs	10,000 of each type (Open, PSK, 802.1X, WISPr, WISPr+Mac)
Number of User Equipments (clients)	100,000

NOTE
It is important to note that the above test conditions were specific to the testing environment, and different conditions may result in different rest API support rates. RUCKUS cannot guarantee a specific support rate for every possible condition.

Navigating the Dashboard

Setting Up the Controller for the First Time

The controller must first be set up on the network.

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

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

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

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

Logging in to the Web Interface

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

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

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

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

   The following web browsers are supported:

   - Google Chrome
   - Safari
   - Mozilla Firefox

- Internet Explorer
- Microsoft Edge

2. In the address bar, enter the IP address that you assigned to the Management (Web) interface, and append a colon (:) and 8443 (the management port number of the controller) to the end of the address.

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

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

   The controller web interface logon page is displayed.

3. Log in to the controller web interface using the following credentials:
   - **User Name**: admin
   - **Password**: *Password you set in the Setup Wizard*

4. Click **Log On**.

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

Controller Web Interface Features

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

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

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

FIGURE 94 Controller Web Interface Components

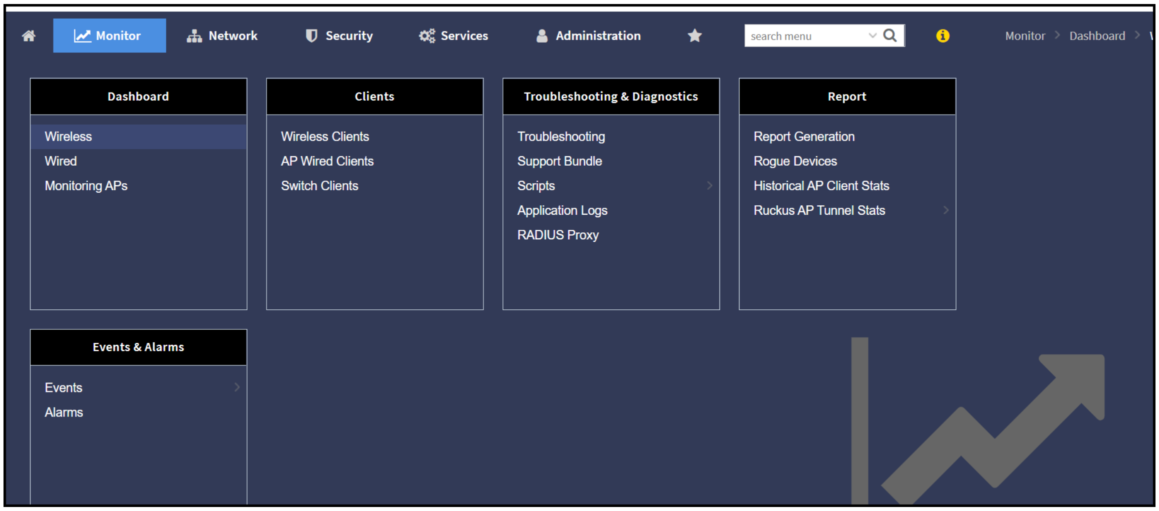
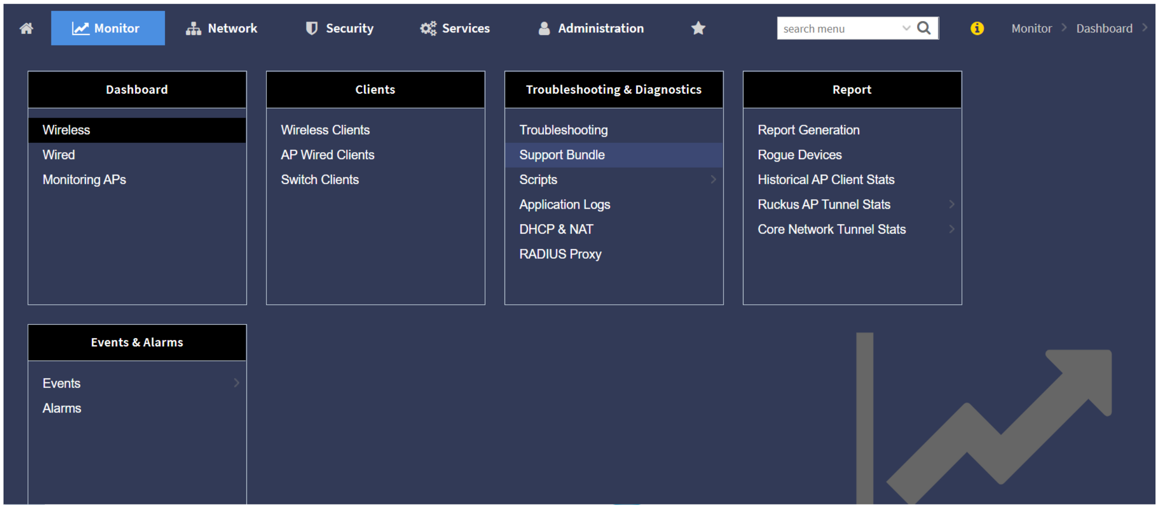


FIGURE 95 Controller Web Interface Components



The following table describes the controller web interface components.

TABLE 23 Controller Web Interface Components

Component	Description	Action
Main Menu	Lists the menus for administrative tasks.	Select the required menu and submenu.
Tab Page	Displays the options specific to the selected menu.	Select the required tab page.
Content Area	Displays tables, forms, and information specific to the selected menu and tab page.	View the tables, forms, and information specific to the selected menu, submenu, and tab page. Double-click an object or profile in a table, for example, a WLAN, to edit the settings.

TABLE 23 Controller Web Interface Components (continued)

Component	Description	Action
Header Bar	Displays information specific to the controller web interface.	Select the required option (from left to right): • Warning: Lists the critical issues to be resolved. • System Date and Time: Displays the current system date and time. • Refresh: Refreshes the web page. • Global filter: Allows you to set the preferred system filter. • My Account link: Allows you to: – Change password – Set session preference – View account activities such as login information and privilege changes – Log off • Online Help: Allows access to web help.

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

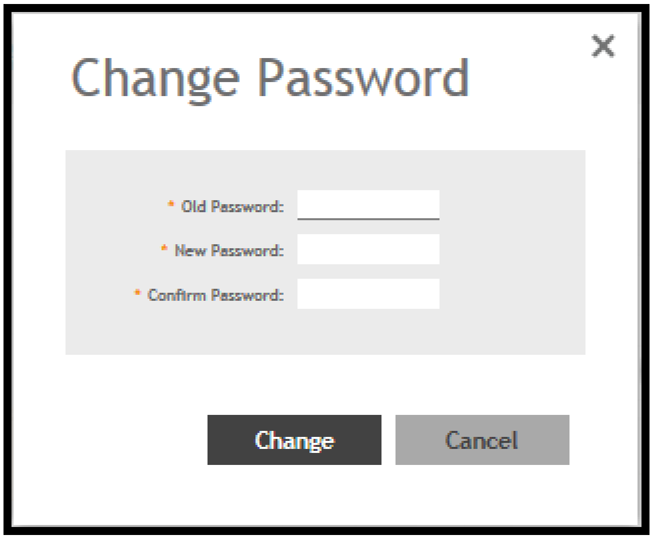
Changing the Administrator Password

Follow these steps to change the administrator password.

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

   The following window is displayed.

   FIGURE 96 Change Password Form



2. Enter:

   - **Old Password**—Your current password.

- **New Password**—Your new password.
- **Confirm Password**—Your new password.

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

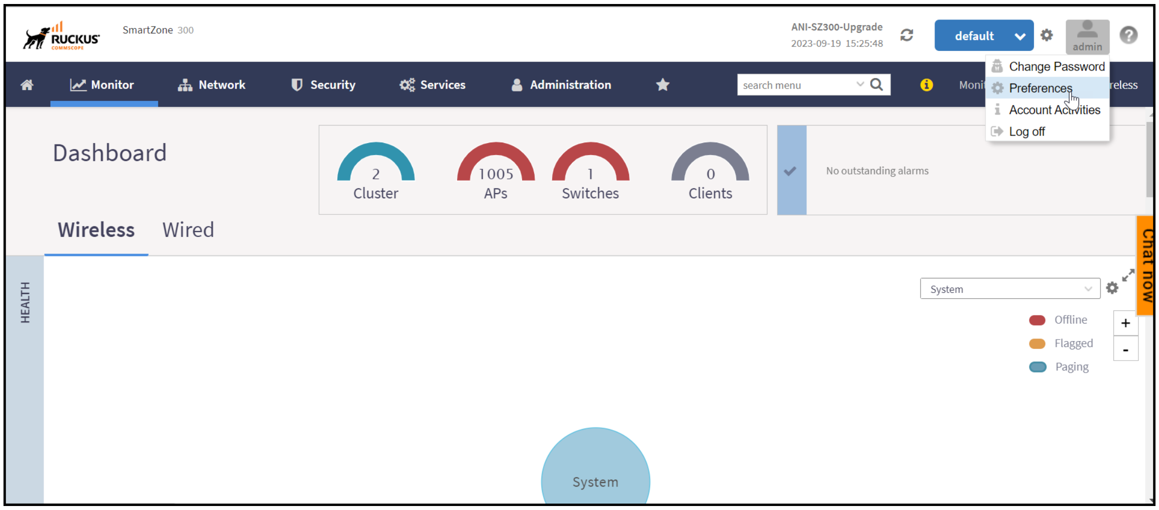
Setting User Preferences

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

1. In the controller web interface, click on the **user profile** and click **Preferences**.

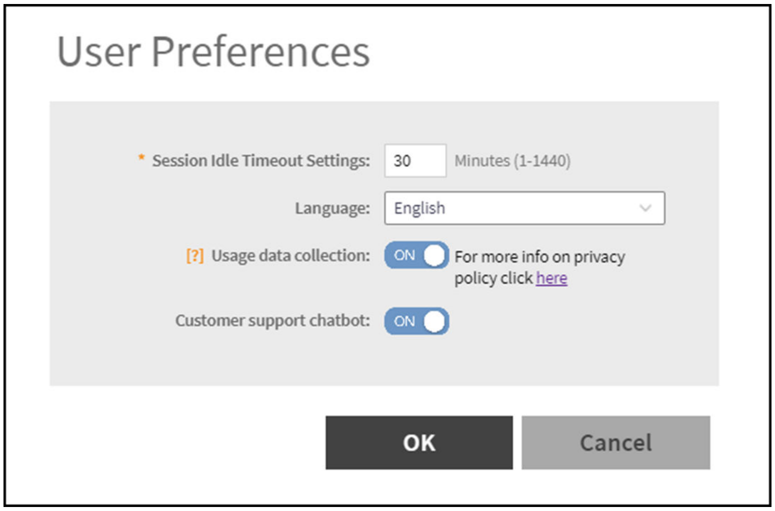
   This displays **User Preferences** page.

   FIGURE 97 User Profile Menu - Preferences



2. In the **User Preferences** page, enter the following details.
   - **Session Idle Timeout Setting** - Enter the duration in **minutes** for the web interface session to refresh.
   - **Language** - Select the language of your choice from the drop-down list to view the web interface content. The following languages are supported in the application -
     - Spanish
     - Brazilian Portuguese
     - French
     - German
     - Italian
     - Russian
     - Simplified Chinese
     - Traditional Chinese
     - Korean
     - Japanese
   - **Usage Data Collection** - By default this button is **Off**, enable this button to collect data for analytics. For more information on data collection, click on the link corresponding to the field.
   - **Customer Support Chat Bot** - By default this button is **On**, this button enables the chat support feature, which is available in the main screen.

FIGURE 98 User Preferences



User Preferences

* Session Idle Timeout Settings: 30 Minutes (1-1440)

Language: English

[?] Usage data collection: ON For more info on privacy policy click here

Customer support chatbot: ON

Logging Off the Controller

You can log off the controller by using either the web interface or the Command Line Interface (CLI).

Logging off Using the Web Interface

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

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

2. Click **Yes**.

   You have completed logging off the web interface

Logging off Using CLI

1. To schedule a shutdown at the CLI prompt, enter the command **shutdown** and specify the delay in seconds before controller shuts down.
2. To shutdown the controller immediately, enter the command **shutdown now**.

Configuring Global Filters

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

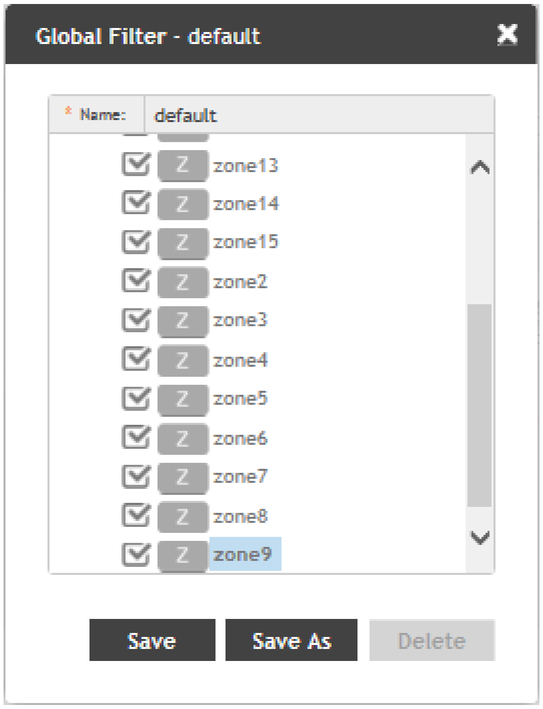
Global filters allow the administrator to define a system scope or system context that applies to all pages of the system as they navigate to different menus. For example, if your system includes 5 zones, but you want to view Zone1 and Zone2 only, you can create and apply such a filter. As you navigate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

To set the global filter:

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

   The below figure appears.

   FIGURE 99 Global Filter Form

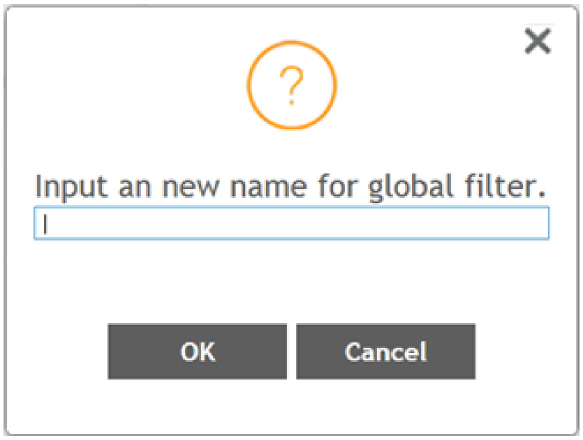
   

   * Name: default

   ☑ Z zone13
   ☑ Z zone14
   ☑ Z zone15
   ☑ Z zone2
   ☑ Z zone3
   ☑ Z zone4
   ☑ Z zone5
   ☑ Z zone6
   ☑ Z zone7
   ☑ Z zone8
   ☑ Z zone9

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

FIGURE 100 New Name Form



Input an new name for global filter.

NOTE

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

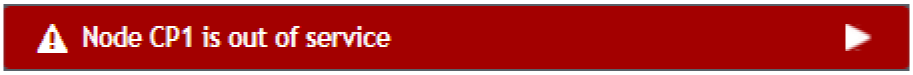
Warnings and Notifications

This section explains about warnings and notifications.

Warnings

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

FIGURE 101 Sample Warning Message



Node CP1 is out of service

A list of warning messages that appear are as follows:

- Default 90-day support expiring soon
- System support expiring soon
- System support has expired
- Default 90-day AP license expiring soon
- Default AP license has expired
- Default 90-day RTU license expiring soon
- RTU has expired
- AP Certificate Expiration
- Node Out of Service
- Cluster Out of Service
- VM Resource Mismatch

- Suggested AP Limit Exceeded
- AP/DP version mismatch
- HDD Health Degradation

Setting Global Notifications

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

- Clearing the alarm
- Acknowledging the Alarm

For more information, refer to the “Managing Alarms and Events” chapter.

Alarm severity are of three types:

- Minor
- Major
- Critical

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

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

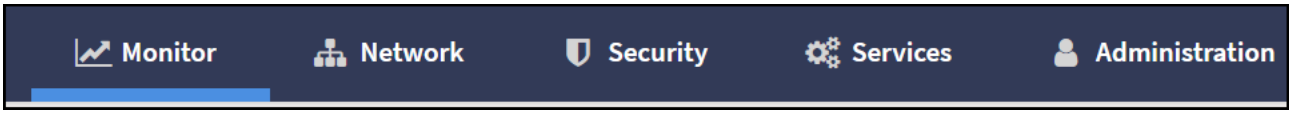
   NOTE
   RUCKUS AI is configured on the SmartZone (controller) platform. When the user connects to RUCKUS AI through the controller, a status tag is displayed in the controller header and the browser re-directs the user to RUCKUS AI page. Currently, this feature is dependent on RUCKUS AI.

Controller User Interface (UI)

Prior to release 6.0.0, the controller menu had vertical layout that resulted in some menu items not being visible on the screen. So, to make navigation easier, a new menu was introduced in release 6.0.0 release. The new menu has features such as **Category**, **Favorite**, **Search** and **Breadcrumbs**.

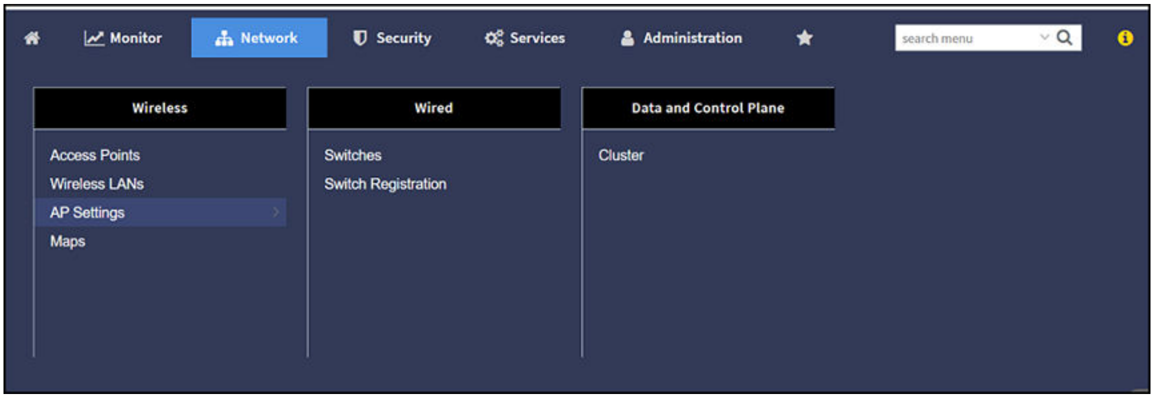
- **Category** - The menu items are organized into distinct categories or groups making it easier to find and access specific functionalities. The various categories are **Monitor**, **Network**, **Security**, **Services** and **Administration**.

  FIGURE 102 Displaying Categories on the Menu Bar

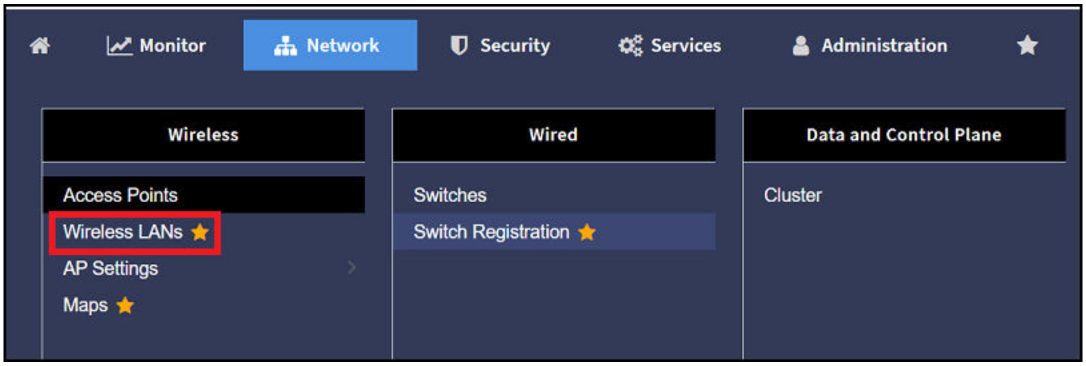
  For example, the menu items under the category **Network** are displayed as per the screenshot below.

FIGURE 103 Displaying Menu Items in the Network Category



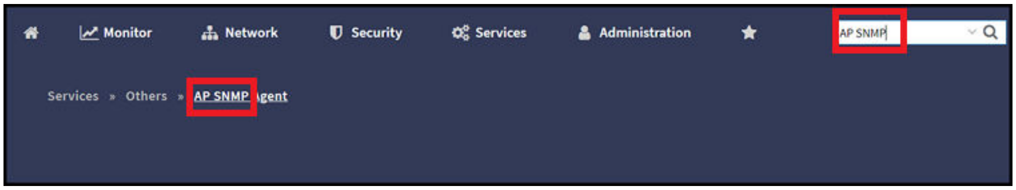
- Favorite - The **Star** icon allows you to mark certain menu items as their favorites or frequently accessed options. This feature saves time by providing quick access to the functions you use most often. The star icon acts like a toggle allowing you to add or remove menu item from your favorite list.

FIGURE 104 Marking Favorites



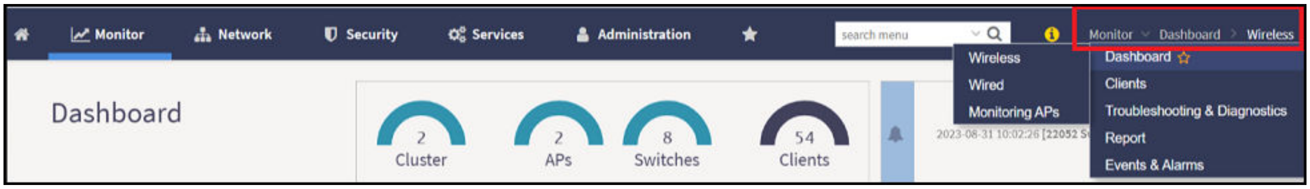
- Search - The **Search** menu increases the usability by allowing you to input keywords specific terms to find relevant information. When you use a search option, it queries the system and returns results that match your input, making it easier to locate specific content or data. It helps you in quickly find what you are looking for.

FIGURE 105 Using the Search Field

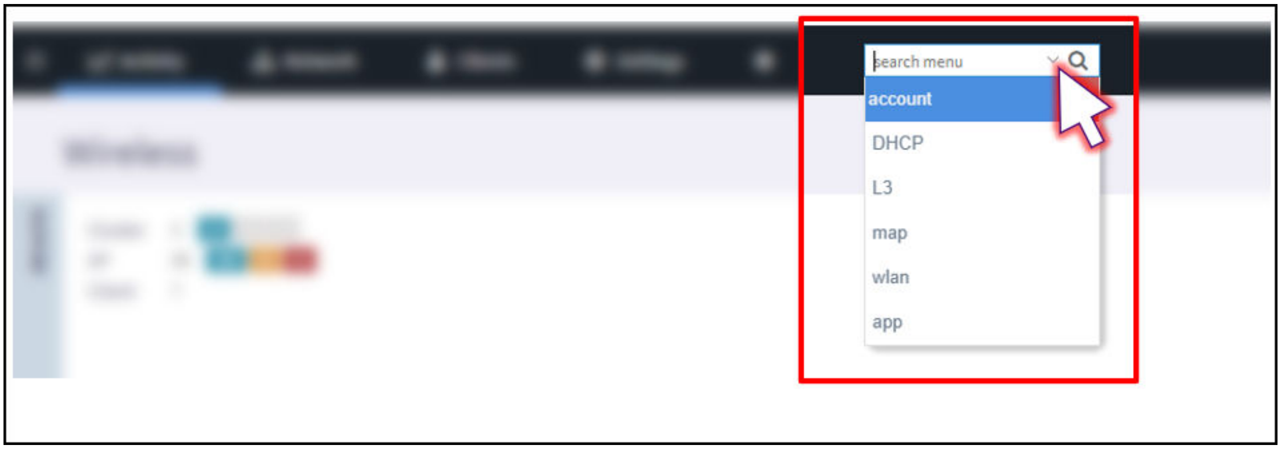


- Breadcrumb - The **Breadcrumb** is a navigation aid that shows your current location within the menu hierarchy. This allows you to see where you are and easily navigate back to previous levels.

FIGURE 106 Displaying Breadcrumb

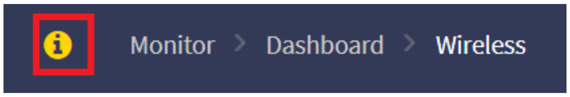


- Search History - The **Search History** typically refers to a record of the searches you've conducted. It can include the keywords or phrases you entered when searching for information.
- **FIGURE 107** Search History



- **i** icon - Starting with the 7.0 release, clicking the **i** icon displays the RUCKUS AI Free Trial offer page, allowing you to avail of this offer. In earlier releases, the RUCKUS Analytics Free Trial offer page was displayed.

FIGURE 108 Viewing **i** icon



Configuring Node Affinity

Node affinity enables administrators to manually configure the controller nodes to which APs will connect.

To do this, set the order of preferred nodes on the node affinity page. Node affinity is implemented at the AP zone level, which means that all APs that belong to a zone will have the same node affinity settings.

If you want APs that belong to the same zone to connect to the same node whenever possible, you can configure set the preferred node for a particular zone.

> **NOTE**
> An affinity profile defines the order of the nodes to which APs that belong to the same zone will connect.

> **NOTE**
> Node affinity profile works only if it is restored in the same cluster. If the configuration must be restored to a different cluster, disable node affinity and remove the node affinity profiles containing nodes that are not available in the new cluster.

> **NOTE**
> Node affinity is not supported on the vSZ-H and vSZ-D platforms.

Enabling Node Affinity

To enable and configure node affinity:

1. Go to **Adminstration** > **System**. The **Node Affinity** page is displayed.
2. Select **Enable Node Affinity**.
3. To:
   - Create an new profile:
     a. Click **Create**, the Create Node Affinity Profile form is displayed.
     b. Enter a **Name** and **Description**.
     c. In the **Node Order** list, select the node and click **Up** or **Down** to position the node in the required order.
     d. Click **OK**.
   - Edit the default profile:
     a. Select the profile from the list and click **Configure**. The Edit Node Affinity Profile form is displayed.
     b. Edit the **Name** and **Description**.
     c. In the **Node Order** list, select the node and click **Up** or **Down** to position the node in the required order.
     d. Click **OK**.

     > **NOTE**
     > When you enable node affinity, disable cluster redundancy.
4. To set the number of times an AP will attempt to connect to the preferred node, enter the **# of Node Retry for Preferred Node**.

The default value is 3 and the accepted range is 1 to 10. If the AP is unable to connect to the preferred node, it will attempt to connect to the node that is next in the order of node priority.

5. In the **Zone Assignment** section, set the node affinity profile that you want each zone to use. Select the Zone from the list and click **Assign Profile**. The Assign Node Affinity Profile to Selected Zones form appears.
6. Select the **Node Affinity Profile** from the drop-down and click **OK**.
7. Click **OK**.

Disabling Node Affinity

Follow these steps to disable node affinity:

1. Go to **Adminstration** > **System**. The **Node Affinity** page is displayed.
2. Clear the **Enable Node Affinity**.
3. Click **OK**. You have disabled node affinity.

Syslog

Configuring the Remote Syslog Server

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

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

Follow these steps to configure the remote syslog server:

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

TABLE 24 Syslog Server Configuration Settings

Field	Description	Your Action
Primary Syslog Server Address	Indicates the syslog server on the network.	a. Enter the server address. b. Enter the **Port number**. c. Choose the **Protocol type**. d. Click **Ping Syslog Server**. If the syslog server is reachable, a flashing green circle and the message **Success** appears after the button.
SecondarySyslog ServerAddress	Indicates the backup syslog server on the network, if any, in case the primary syslog server is unavailable.	a. Enter the server address. b. Enter the **Port number**. c. Choose the **Protocol type**. d. Click **Ping Syslog Server**. If the syslog server is reachable, a flashing green circle and the message **Success** appears after the button.
Application Logs Facility	Indicates the facility for application logs.	a. Select the option from the drop-down. Range: 0 through 7. b. Select one of the following **Filter Severity**: 1. **Emerg** 2. **Alert** 3. **Crit** 4. **Error** 5. **Warning** 6. **Notice** 7. **Info** 8. **Debug**: Default option

TABLE 24 Syslog Server Configuration Settings (continued)

Field	Description	Your Action
Administrator Activity Logs Facility	Indicates the facility for administrator logs.	a. Select the option from the drop-down. Range: 0 through 7. b. Select one of the following **Filter Severity**: 1. **Emerg** 2. **Alert** 3. **Crit** 4. **Error** 5. **Warning** 6. **Notice** 7. **Info** 8. **Debug**: Default option
Other Logs Filter Severity	Indicates the facility for comprehensive logs.	Select one of the following **Filter Severity**: a. **Emerg** b. **Alert** c. **Crit** d. **Error** e. **Warning** f. **Notice** g. **Info** h. **Debug**: Default option
Event Facility	Indicates the facility for event logs.	Select the option from the drop-down. Range: 0 through 7.
Event Filter	Indicates the type of event that must be sent to the syslog server.	Choose the required option: • **All events** — Send all controller events to the syslog server. • **Alleventsexceptclientassociation/disassociationevents** — Send all controller events (except client association and disassociation events) to the syslog server. • **All events above a severity** — Send all controller events that are above the event severity to the syslog server.
Event Filter Severity applies to **Event Filter** > **All events above a severity**	Indicates the lowest severity level. Events above this severity level will be sent to the syslog server.	Select the option from the drop-down. a. **Critical** b. **Major** c. **Minor** d. **Warning** e. **Informational** f. **Debug**: Default option
Priority	Indicates the event severity to syslog priority mapping in the controller.	Choose the **Syslog Priority** among **Error**, **Warning**, **Info** and **Debug**, for the following event severities: • **Critical** • **Major** • **Minor** • **Warning** • **Informational** • **Debug**

Reports

Report Generation

Creating Reports

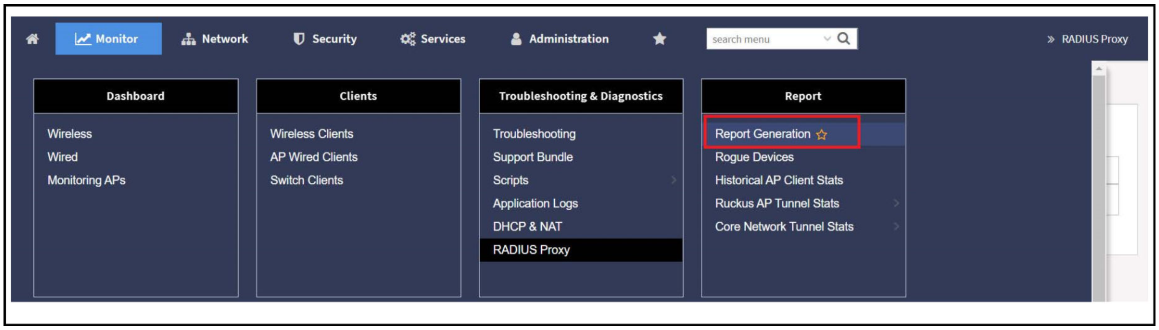
You can create reports to obtain a historical view of the maximum and minimum number of clients connected to the system, the number of clients connected at different time intervals, and the traffic statistics for the switches.

Complete the following steps to create a new report.

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

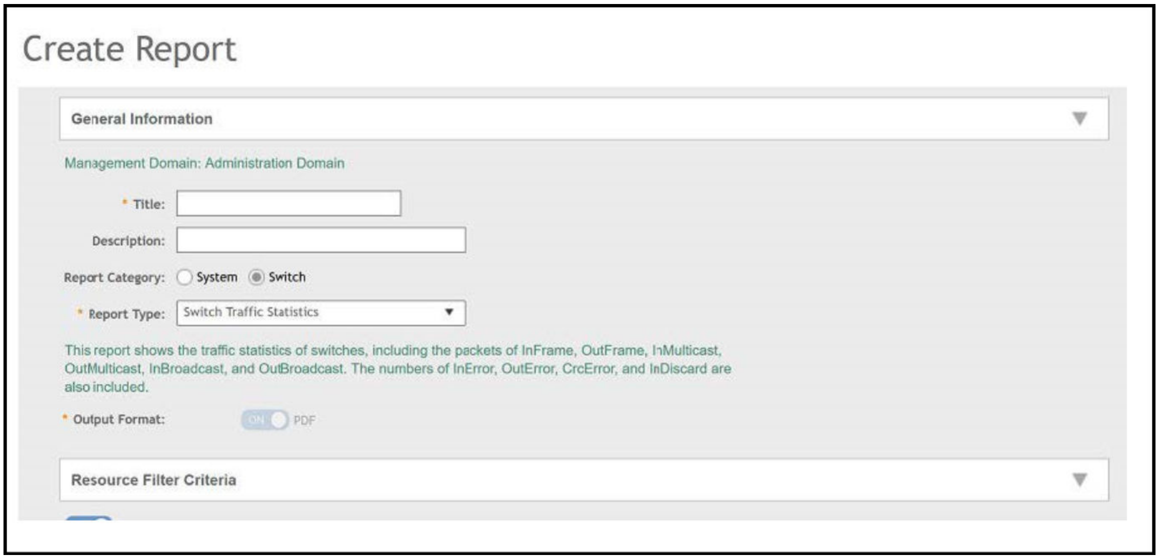
   The **Report Generation** page is displayed.

   FIGURE 109 Report Generation Screen



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

FIGURE 110 Create Report Dialog Box



Create Report

General Information

Management Domain: Administration Domain

* Title:

Description:

Report Category: ○ System ● Switch

* Report Type: Switch Traffic Statistics

This report shows the traffic statistics of switches, including the packets of InFrame, OutFrame, InMulticast, OutMulticast, InBroadcast, and OutBroadcast. The numbers of InError, OutError, CrcError, and InDiscard are also included.

* Output Format: ON PDF

Resource Filter Criteria

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

TABLE 25 Report Parameters

Field	Description	Your Action
General Information		
Title	Indicates the report name.	Enter a title for the report.
Description	Describes the report type.	Enter a short description.
Report Category	Provides an option to generate reports for system or switch devices in the network.	Select **System** or **Switch** as appropriate.
Report Type	Specifies the report type.	Select the required report type.
Output Format	Specifies the report output format.	Select the required report output format.
Resource Filter Criteria		
Device	Indicates the level of resource filtering for which you want to generate the report; for example, Management Domains, AP Zone or Access Point (if you select the System option), and Switch.	Enter the device or switch name or select the device or switch from the list and select the option.
SSID	Indicates the SSID for which you want to generate the report.	Select the check box and select the SSID for which you want the report. You can select **All SSIDs** to generate reports for all the SSIDs available. This option is convenient because you do not have to update the resource filter criteria periodically.
Radio	Indicates the frequency for which you want to generate the report.	Select the check box and select the required frequency: • **2.4G** • **5G** • **6GHz/5GHz**
Time Filter		
Time Interval	Defines the time interval at which to generate the report.	Select the required time interval.

TABLE 25 Report Parameters (continued)

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

4. Click **OK**.

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

Generating Reports

Complete the following steps to generate a report.

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

   The **Report Generation** page is displayed.

2. Select the required report from the list, and click **Generate**. The **Report Generated** form is displayed.

3. Click **OK**. The report is generated and listed in the **Report Results** pane.

4. From the **Result Links** column, select the required format, and click **Open** to view the report.

Short Message Service

Configuring the Short Message Service (SMS) Gateway Server

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

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

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

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

Simple Mail Transfer Protocol

Configuring Simple Mail Transfer Protocol (SMTP) Server Settings

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

Follow these steps to configure the SMTP server settings.

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

   Check with your ISP or mail administrator for the correct encryption settings that you need to set.
10. Click **Test**, to verify if the SMTP server settings are correct. The test completed successfully form appears, click **OK**.
11. Click **OK**.

Simple Network Management Protocol

Enabling Global SNMP Notifications

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

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

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

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

Configuring SNMP v2 Agent

To configure SNMP v2 Agent settings:

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

TABLE 26 SNMP v2 Agent Settings

Field	Description	Your Action
Name	Indicates the AP SNMP profile name.	Enter a name.
Description	Provides a brief explanation of the profile.	Enter a brief explanation.
Community	Indicates that applications which send SNMP Get-Requests to the controller (to retrieve information) will need to send this string along with the request before they will be allowed access.	Enter a name.
Privilege	Indicates the privileges granted to this community.	Select the required privileges: • **Read-Only**—Privilege only to read. • **Read-Write**—Privilege only to read and write. • **Notification**—Privilege to: - **Trap**—Choose this option to send SNMP trap notification. - **Inform**—Choose this option to send SNMP notification. a. Enter the **Target IP** address. b. Enter the **Target Port** number. c. Click **Add**.

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

3. Click **OK**.

Configuring SNMP v3 Agent

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

TABLE 27 SNMPv3 Agent Settings

Field	Description	Your Action
Name	Indicates the AP SNMP profile name.	Enter a name.
Description	Provides a brief explanation of the profile.	Enter a brief explanation.
User	Indicates that applications which send SNMP Get-Requests to the controller (to retrieve information) will need to send this string along with the request before they will be allowed access.	Enter a name.
Authentication	Indicates the authentication method.	Choose the required option: ● **SHA**—Secure Hash Algorithm, message hash function with 160-bit output. a. Enter the **Auth Pass Phrase**. b. Choose the **Privacy** option. - **None**: Use no privacy method. - **DES**: Data Encryption Standard, data block cipher. - **AES**: Advanced Encryption Standard, data block cipher. c. Enter a **Privacy Phrase**, 8 through 32 characters. ● **MD5**—Message-Digest algorithm 5, message hash function with 128-bit output. a. Enter the **Auth Pass Phrase**. b. Choose the **Privacy** option. - **None**: Use no privacy method. - **DES**: Data Encryption Standard, data block cipher. - **AES**: Advanced Encryption Standard, data block cipher. c. Enter a **Privacy Phrase**, 8 through 32 characters.

TABLE 27 SNMPv3 Agent Settings (continued)

Field	Description	Your Action
Privilege	Indicates the privileges granted to this community.	Select the required privileges: • **Read-Only**—Privilege only to read. • **Read-Write**—Privilege only to read and write. • **Notification**—Privilege to: – **Trap**—Choose this option to send SNMP trap notification. – **Inform**—Choose this option to send SNMP notification. a. Enter the **Target IP** address. b. Enter the **Target Port** number. c. Click **Add**.

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

3. Click **OK**.

Creating a RUCKUS GRE Profile

Generic Routing Encapsulation (GRE) provides a way to encapsulate arbitrary packets (payload packet) inside of a transport protocol, and transmit them from one tunnel endpoint to another. You can configure the RUCKUS GRE tunnel profile of the controller to manage AP traffic.

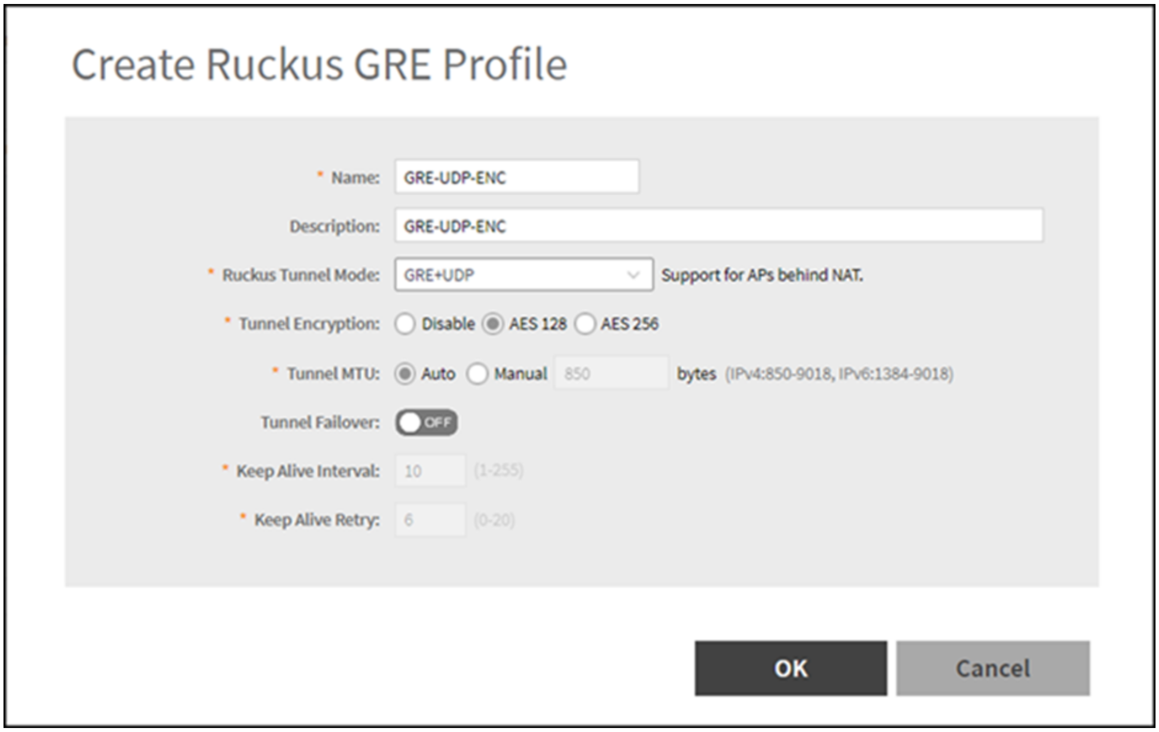
To create a GRE profile follow the below steps.

> **NOTE**
> You can also edit, clone and delete the profile by selecting the options **Configure**, **Clone** and **Delete** respectively, from the **Ruckus GRE** tab.

1. From the main menu go to **Services** > **Tunnels & Ports**.
2. Select the **Ruckus GRE** tab, and select the system to create the profile.
3. Click **Create**.

   The **Create Ruckus GRE Profile** page is displayed.

   FIGURE 111 Creating a Ruckus GRE Profile



Create Ruckus GRE Profile

* Name: GRE-UDP-ENC

Description: GRE-UDP-ENC

* Ruckus Tunnel Mode: GRE+UDP Support for APs behind NAT.

* Tunnel Encryption: ○ Disable ● AES 128 ○ AES 256

* Tunnel MTU: ● Auto ○ Manual 850 bytes (IPv4:850-9018, IPv6:1384-9018)

Tunnel Failover: OFF

* Keep Alive Interval: 10 (1-255)

* Keep Alive Retry: 6 (0-20)

4. Type a name for the profile in the **Name** box.
5. Type a description for the profile in the **Description** box.
6. Select a protocol to use for tunneling WLAN traffic back to the data plane by choosing one of the following after clicking the drop-down arrow in the **Ruckus Tunnel Mode** box:
   - **GRE + UDP**—Select this option to allow APs behind a NAT server to tunnel WLAN traffic back to the data plane.
   - **GRE**—Select this option to tunnel regular WLAN traffic only.

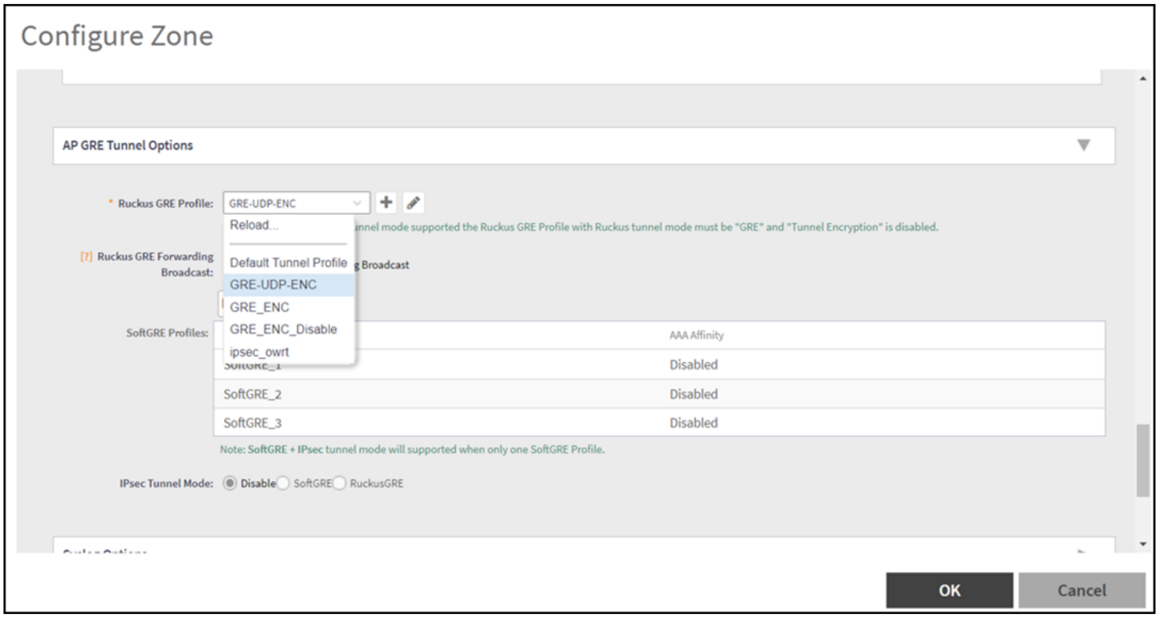
7. To allow managed APs to decrypt 802.11 packets, and then use an AES encrypted tunnel to send them to the data plane. Select one of the **Tunnel Encryption** options:
   - Click the **Disable** radio button to allow only the management traffic to be encrypted; data traffic is unencrypted. This is the default option.
   - Click the **AES 128** radio button to use an AES 128-byte encryption tunnel.
   - Click the **AES 256** radio button to use an AES 256-byte encryption tunnel.

   MTU is the size of the largest protocol data unit that can be passed on the controller network.
8. Set the maximum transmission unit (MTU) for the tunnel using one of the **Tunnel MTU** options:
   - Click the **Auto** radio button. This is the default option.
   - Click the **Manual** radio button and enter the maximum number of bytes. For IPv4 traffic the range is from 850-1500 bytes, for IPv6 traffic the range is from 1384 to 1500 bytes.
9. Set the Tunnel failover option to either OFF or On. By default it is in OFF mode.
10. Enter the **Keep Alive Interval** value. By default the interval value is 10 and the range is between 1-255.
11. Enter the **Keep Alive Retry** value. By default the retry value is 06 and the range is between 0-20.
12. Click **OK**.

Using the created GRE profile in an AP Zone and WLAN

13. From the main menu go to **Network** > **Wireless** > **Access Points** > **Zone** profile to use the created GRE profile.
14. Select the GRE profile from the drop down list. Enable or disable the RUCKUS GRE forwarding broadcast. By default the option is turned OFF. Select the SoftGRE profiles and IPSec Tunnel Mode.

FIGURE 112 Applying the Ruckus GRE Profile



Configure Zone

AP GRE Tunnel Options

* Ruckus GRE Profile: GRE-UDP-ENC

Reload...

Default Tunnel Profile

GRE-UDP-ENC

GRE_ENC

GRE_ENC_Disable

ipsec_owrt

unnel mode supported the Ruckus GRE Profile with Ruckus tunnel mode must be "GRE" and "Tunnel Encryption" is disabled.

[?] Ruckus GRE Forwarding Broadcast: g Broadcast

SoftGRE Profiles:

	AAA Affinity
SoftGRE_1	Disabled
SoftGRE_2	Disabled
SoftGRE_3	Disabled

Note: SoftGRE + IPsec tunnel mode will supported when only one SoftGRE Profile.

IPsec Tunnel Mode: ● Disable ○ SoftGRE ○ RuckusGRE

15. From the main menu go to **Network** > **Wireless LANs** > **WLAN** profile to use the created GRE profile.
16. Another option is navigate to the Zone level configuration and find **AP GRE Tunnel**.
17. Click + to create a new profile.

18. Go to the required WLAN to use the GRE profile.

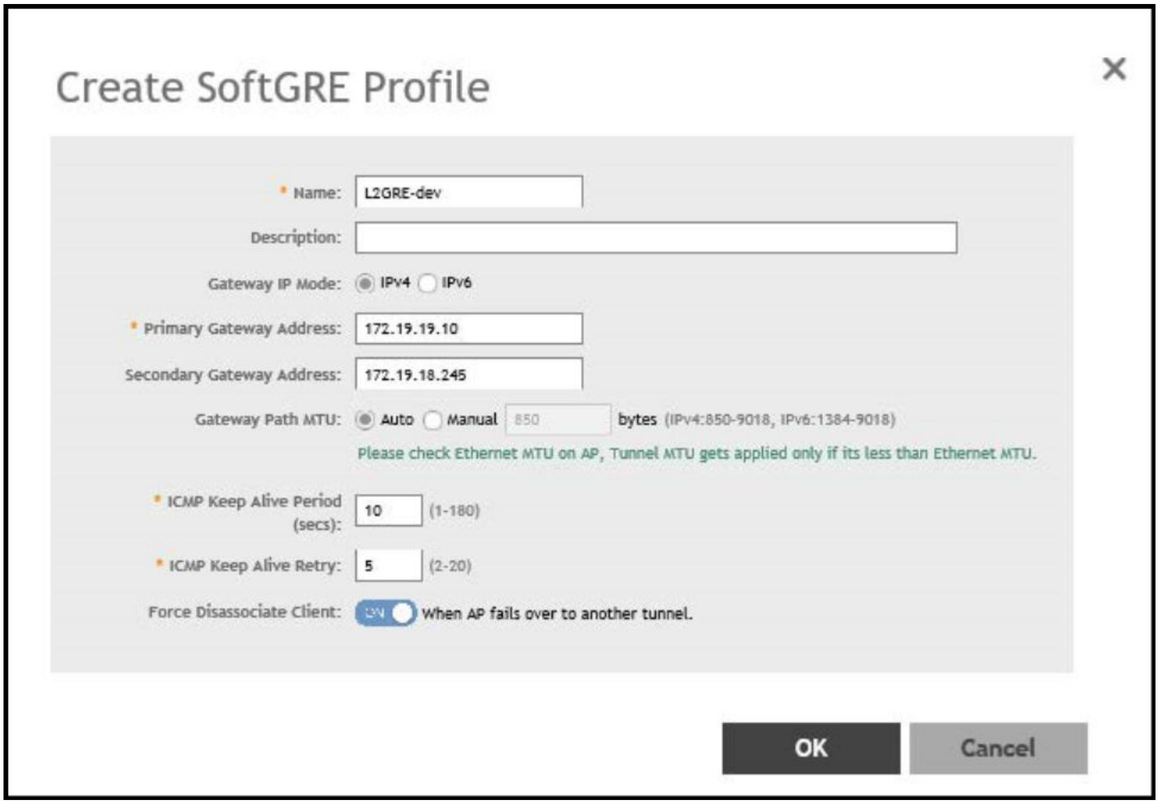
Creating a Soft GRE Profile

You can configure the Soft GRE tunnel profile of the controller to manage AP traffic.

1. From the main menu go to **Services** > **Tunnels and Ports**.
2. Select **SoftGRE** and click **Create**.

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

   FIGURE 113 Creating a SoftGRE Profile



Create SoftGRE Profile

* Name: L2GRE-dev

Description:

Gateway IP Mode: ● IPv4 ○ IPv6

* Primary Gateway Address: 172.19.19.10

Secondary Gateway Address: 172.19.18.245

Gateway Path MTU: ● Auto ○ Manual 850 bytes (IPv4:850-9018, IPv6:1384-9018)

Please check Ethernet MTU on AP, Tunnel MTU gets applied only if its less than Ethernet MTU.

* ICMP Keep Alive Period (secs): 10 (1-180)

* ICMP Keep Alive Retry: 5 (2-20)

Force Disassociate Client: ON When AP fails over to another tunnel.

3. Enter profile name and description.
4. Under **Gateway IP Mode**, select **IPv4** or **IPv6** addressing.
5. In the **Primary Gateway Address** field, enter the IP address or fully-qualified domain name (FQDN) of the primary gateway server.
6. In the **Secondary Gateway Address** field, enter the IP address or fully-qualified domain name (FQDN) of the secondary gateway server.

   NOTE
   If the controller is unable to reach the primary gateway server, the controller automatically attempts to reach the secondary gateway address at the IP address specified by you.

7. For **Gateway Path MTU**, set the maximum transmission unit (MTU) for the gateway path.

   Select one of the following options:

   - **Auto**: This is the default option.
   - **Manual**: The transmission range is from 850 through 1500 bytes.

8. In the **ICMP Keep Alive Period** field, enter the time interval in seconds.

   NOTE
   Time interval is the time taken by the APs to send a keep alive message to an active third party WLAN gateway. The range is from 1 through 180 seconds. The default value is 10 seconds.

9. In the **ICMP Keep Alive Retry** field, enter the number of keep alive attempts.

   NOTE
   Keep alive attempts are the number of attempts that the APs wait for a response from the active third party WLAN gateway before failing over to the standby WLAN gateway. The range is from 2 through 10 attempts. The default value is 5 attempts.

10. Under **Force Disassociate Client**, enable **Disassociate client when AP fails over to another tunnel** if you want to disassociate the client when AP fails over to another tunnel.

    NOTE
    You must select this option if you have enabled **AAA Affinity** while configuring the zone.

11. Click **OK.**

You have created the Soft GRE profile.

NOTE
You can also edit, clone, and delete the profile by selecting the options **Configure**, **Clone**, and **Delete** respectively from the **Soft GRE** tab.

Troubleshooting through Spectrum Analysis

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

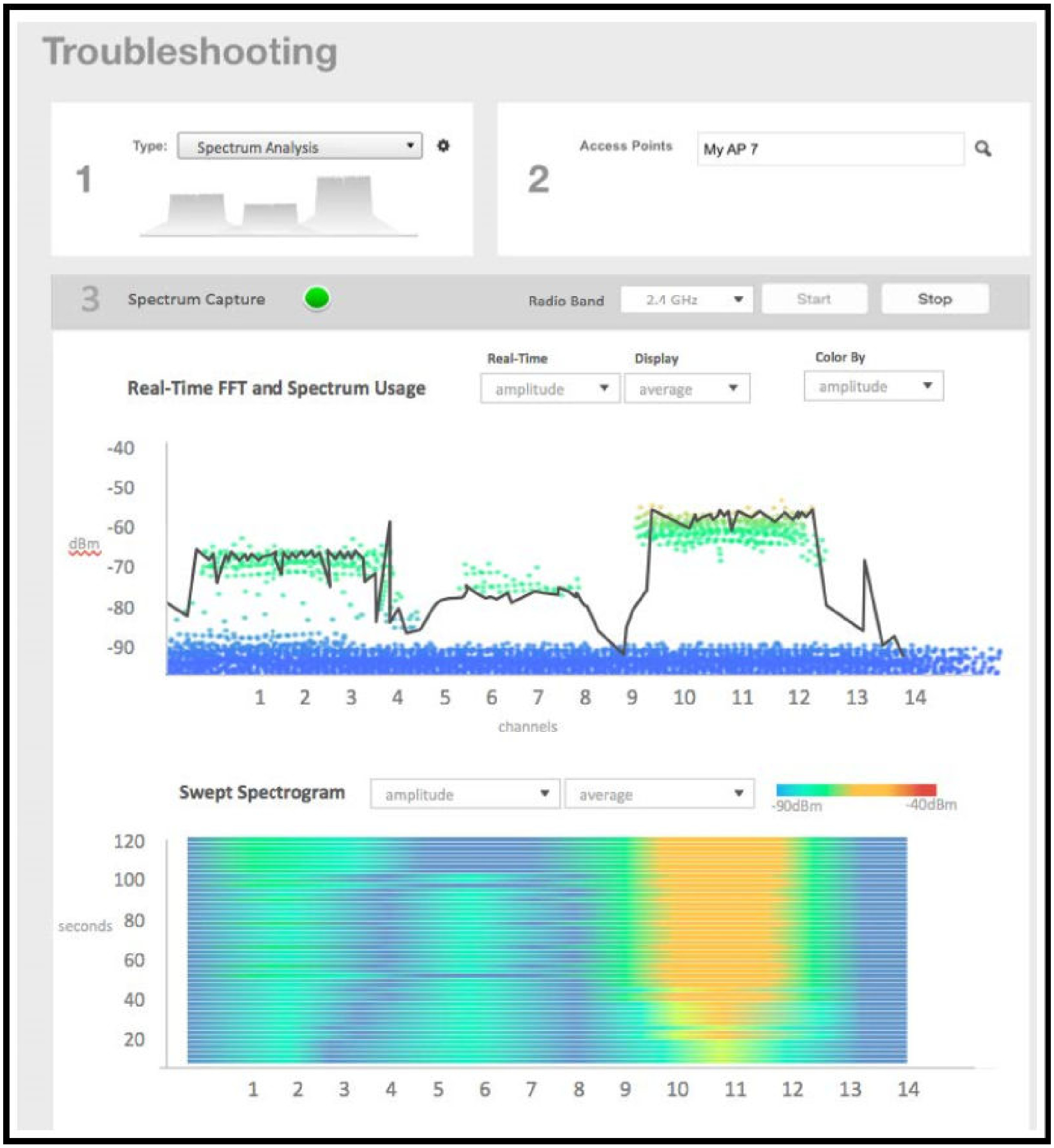
In addition, spectrum analysis provides the flexibility to troubleshoot issues remotely, identify sources of interferences within the network and allow administrators access to the RF health of the network environment.

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

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

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

FIGURE 114 Troubleshooting - Spectrum Analysis



Troubleshooting

1 Type: Spectrum Analysis

2 Access Points: My AP 7

3 Spectrum Capture ● Radio Band: 2.4 GHz

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

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

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

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

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

5. After you select the parameters that you want to use to view the graphs, click **Start**.

6. Click **Stop** to terminate viewing spectrum analysis trends.

Troubleshooting and Diagnostics

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 28 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 29 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 30 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 30 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

DHCP & NAT

Viewing DHCP and NAT Information

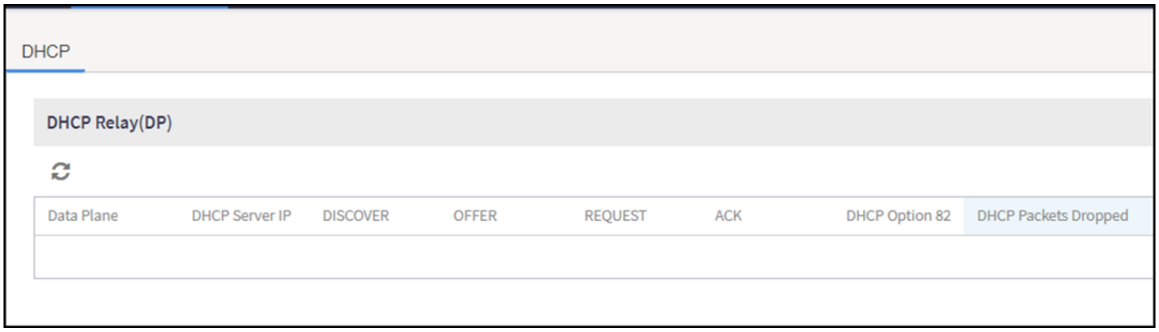
DHCP or NAT functionality on controller managed APs and DPs (data planes) allows customers to reduce costs and complexity by removing the need for DHCP server or NAT router to provide IP addresses to clients. For data traffic aggregation and services delivery, choose the appropriate user profile for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

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

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

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

FIGURE 115 DHCP Relay

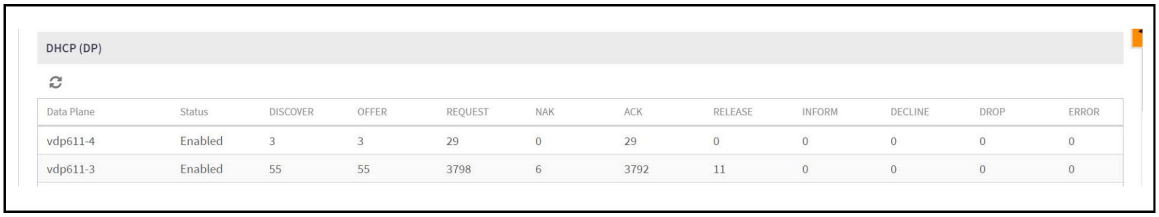


Data Plane	DHCP Server IP	DISCOVER	OFFER	REQUEST	ACK	DHCP Option 82	DHCP Packets Dropped

The following options are seen on virtual controllers.

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

FIGURE 116 DHCP DP

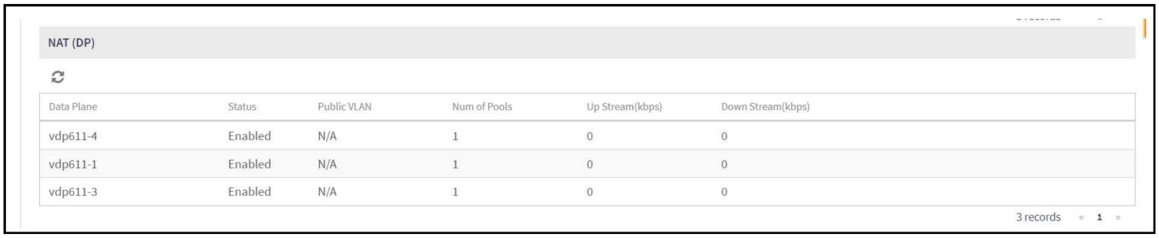


DHCP (DP)

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

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

FIGURE 117 NAT DP



NAT (DP)

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

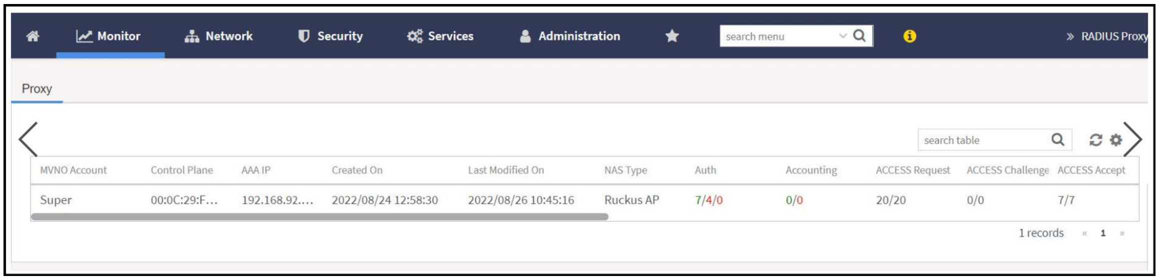
Radius Proxy

Viewing RADIUS Proxy Settings

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

Go to **Monitor** > **Troubleshooting and Diagnostics** > **RADIUS Proxy**. The **Proxy** page appears displaying the RADIUS settings.

FIGURE 118 Diagnostics - RADIUS Proxy



MVNO Account	Control Plane	AAA IP	Created On	Last Modified On	NAS Type	Auth	Accounting	ACCESS Request	ACCESS Challenge	ACCESS Accept
Super	00:0C:29:F...	192.168.92....	2022/08/24 12:58:30	2022/08/26 10:45:16	Ruckus AP	7/4/0	0/0	20/20	0/0	7/7

Upgrade

Upgrading the Controller

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

⚠ CAUTION

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

⚠ CAUTION

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

⚠ CAUTION

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

If you are managing a vSZ-H controller, you can also perform system configuration backup, restore, and upgrade from the controller command line interface.

Performing the Upgrade

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

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

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

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

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

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

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

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

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

   The controller uploads the file to its database, and then performs file verification. After the file is verified, the **Patch for Pending Upgrade** section is populated with information about the upgrade file. If data migration was unsuccessful, the following error is displayed: `Exception occurred during the validation of data migration. Please apply the system configuration backup and contact system administrator.`

7. Click **Backup & Upgrade** to perform the upgrade. The backup operation is done before the system upgrade flow starts. The backup file will be used to restore cluster automatically while the upgrade process fails. Refer to Creating a Cluster Backup on page 87 for more information.

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

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

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

Uploading an AP Patch File

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

1. Go to **Administration** > **Administration** > **Upgrade**.
2. Select the **AP Patch** tab.
3. In Patch File Upload, click **Browse** to select the patch file (with extension .patch).
4. Click **Open**.
5. Click **Upload**. The upload status bar is displayed, and after the patch file is uploaded, the section is populated with the patch filename, size, firmware version, and supporting AP models.
6. Click **Apply Patch**. The apply patch status bar is displayed.

   After the patch file is updated, you will be prompted to log out.

   When you login again, the **AP Patch History** section displays information about the patch file such as start time, AP firmware and model.

You have successfully updated the AP models and AP firmware with the patch file, without having to upgrade the controller software.

Verifying the Upgrade

You can verify that the controller upgrade was completed successfully.

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

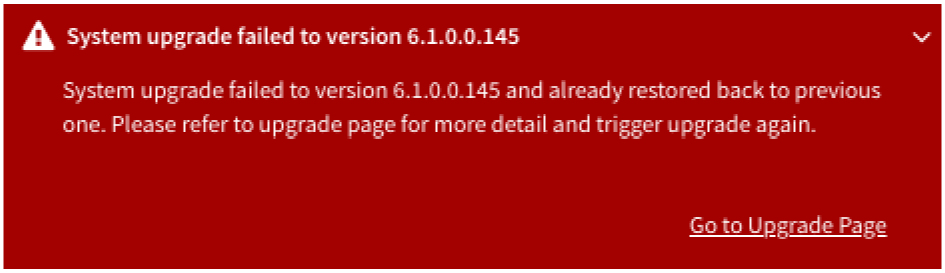
2. In the **Current System Information** section, check the value for *Controller Version*. If the firmware version is newer than the firmware version that controller was using before you started the upgrade process, then the upgrade process was completed successfully.

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

Verifying Upgrade Failure and Restoring Cluster

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

FIGURE 119 Global Warning Message



System upgrade failed to version 6.1.0.0.145

System upgrade failed to version 6.1.0.0.145 and already restored back to previous one. Please refer to upgrade page for more detail and trigger upgrade again.

Go to Upgrade Page

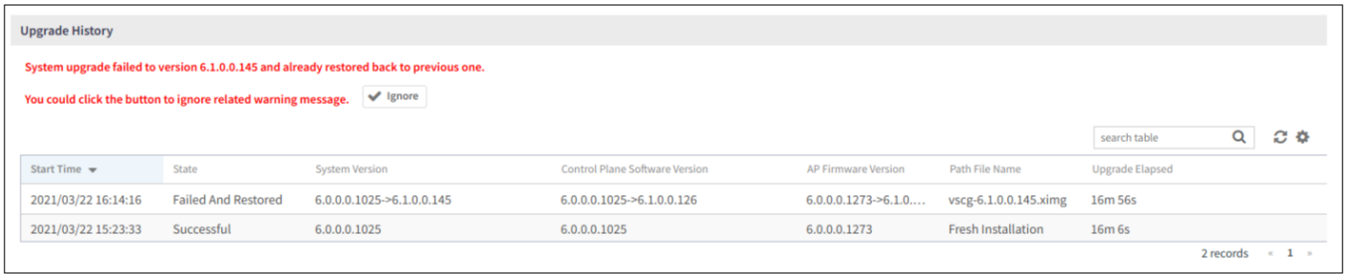
NOTE
Click the **Go to Upgrade Page** link to initiate the **Backup & Upgrade** process again.

For more information on system restore:

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

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

    FIGURE 120 Upgrade History Table

    Upgrade History

    System upgrade failed to version 6.1.0.0.145 and already restored back to previous one.

    You could click the button to ignore related warning message. ✓ Ignore

Start Time ▾	State	System Version	Control Plane Software Version	AP Firmware Version	Path File Name	Upgrade Elapsed
2021/03/22 16:14:16	Failed And Restored	6.0.0.0.1025->6.1.0.0.145	6.0.0.0.1025->6.1.0.0.126	6.0.0.0.1273->6.1.0....	vscg-6.1.0.0.145.ximg	16m 56s
2021/03/22 15:23:33	Successful	6.0.0.0.1025	6.0.0.0.1025	6.0.0.0.1273	Fresh Installation	16m 6s

    2 records « 1 »

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

Rolling Back to a Previous Software Version

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

Here are two:

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

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

- Always back up the controller before attempting a software upgrade. If you are managing a multi-node cluster, back up the entire cluster, and then verify that the backup process completes successfully. See Creating a Cluster Backup on page 87 for the local backup instructions. If you have a local backup and you want to roll back the controller to a previous software version, follow the same procedure described in Creating a Cluster Backup on page 87.
- If you have an FTP server, back up the entire cluster and upload the backup files from all the nodes in a cluster to a remote FTP server. See Backing Up to an FTP Server on page 94 for remote backup instructions and Restoring from an FTP Server on page 95 for remote restore instructions.

Upgrading the Data Plane

You can view and upgrade the virtual data plane version using patch files. This feature is applicable only for virtual platforms.

Upgrading vSZ-D

vSZ support APs starting version 3.4. You must first upgrade vSZ before upgrading vSZ-D, because only a new vSZ can handle an old vSZ-D. There is no order in upgrading the AP zone or vSZ-D. During the vSZ upgrade, all tunnels stay up except the main tunnel which moves to the vSZ. Once the upgrade procedure is completed, allow ten minutes for the vSZ-D to settle.

Upgrade to R5.0 does not support data migration (statistics, events, administrator logs). Only the existing system and the network configuration is preserved. For more information, contact Ruckus support.

Upgrading SZ100-D

SZ100-D is shipped with 3.6.1 release version and you must upgrade it to 5.1 release version. As vSZ manages SZ100-D, ensure that vSZ has the same or later version than SZ100-D. Otherwise, upgrade vSZ before upgrading SZ100-D. SmartZone release 5.1.1 supports SZ100-D. For more information, refer to the *Ruckus SmartZone100-D Quick Setup Guide*.

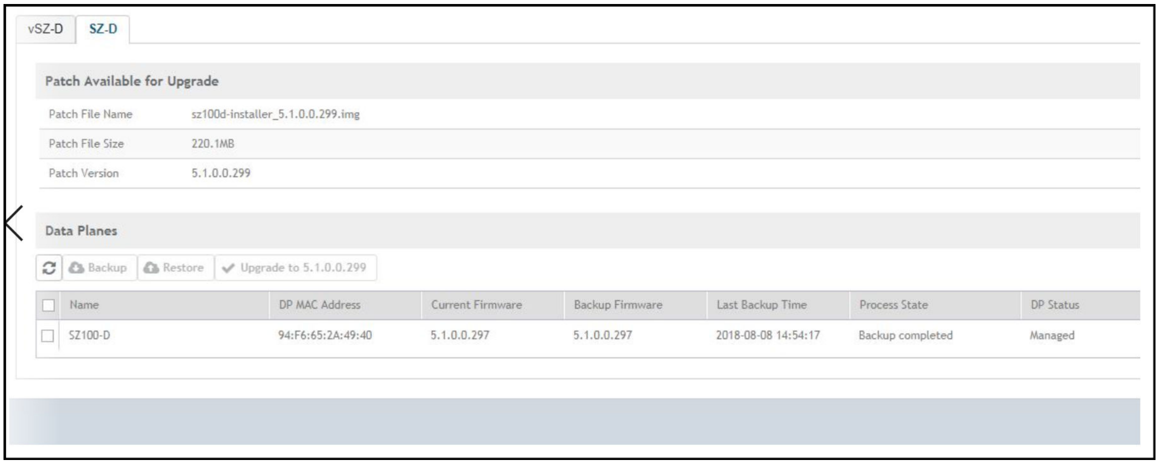
To Upgrade the Data Plane:

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

2. Select the **DP Patch** tab.

   The **DP Patch** page appears.

   FIGURE 121 DP Patch - Data Plane Upgrade

   Patch Available for Upgrade

Patch File Name	sz100d-installer_5.1.0.0.299.img
Patch File Size	220.1MB
Patch Version	5.1.0.0.299

   Data Planes

□	Name	DP MAC Address	Current Firmware	Backup Firmware	Last Backup Time	Process State	DP Status
□	SZ100-D	94:F6:65:2A:49:40	5.1.0.0.297	5.1.0.0.297	2018-08-08 14:54:17	Backup completed	Managed

3. In **Patch File Upload**, click **Browse** to select the patch file (.ximg file).
4. Click **Upload**. The patch files is uploaded.

   The controller automatically identifies the Type of DP (vSZ-D or SZ-D) and switches to the specific Tab page. Uploads the file to its database, and then performs file verification. After the file is verified, the **Patch for Pending Upgrade** section is populated with information about the upgrade file.
   The following details are displayed:

   - Patch File Name: Displays the name of the patch file.
   - Patch File Size: Displays the size of the patch file.
   - Patch Version: Displays the version of the patch file.
5. In **Data Planes**, identify the data plane you want to upgrade, and then choose a patch file version from **Select upgrade version**.
6. Click **Apply** to apply the patch file version to the virtual data plane.

   The following information about the virtual data plane is displayed after the patch file upgrade is completed.

   - Name: Displays the name of the virtual data plane.
   - DP MAC Address: Displays the MAC IP address of the data plane.
   - Current Firmware: Displays the current version of the data plane that has been upgraded.
   - Backup Firmware: Displays the backup version of the data plane.
   - Last Backup Time: Displays the date and time of last backup.
   - Process State: Displays the completion state of the patch file upgrade for the virtual data plane.
   - DP Status: Displays the DP status.

You have successfully upgraded the virtual data plane.

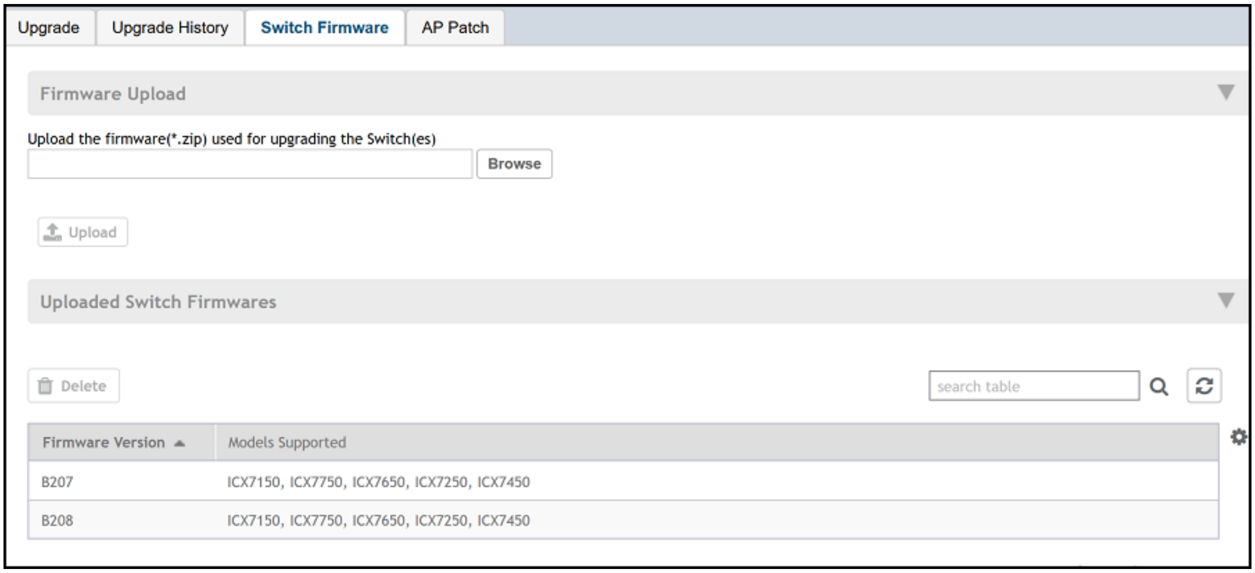
NOTE
To have a copy of the data plane firmware or move back to the older version, you can select the data plane from the list and click **Backup** or **Restore** respectively.

Uploading the Switch Firmware to the Controller

You can upload the latest available firmware to a switch from the controller, thereby upgrading the firmware version of the switch.

1. Select **Administration** > **Administration** > **Upgrade**.
2. Select the **Switch Firmware** tab.

FIGURE 122 Upgrading the Switch Firmware



Upload the firmware(*.zip) used for upgrading the Switch(es)

Firmware Version ▲	Models Supported
B207	ICX7150, ICX7750, ICX7650, ICX7250, ICX7450
B208	ICX7150, ICX7750, ICX7650, ICX7250, ICX7450

3. In Firmware Upload click **Browse** to select the firmware file for upgrading the switch.
4. Click **Open**.
5. Click **Upload**. The upload status bar is displayed, and after the firmware file is uploaded, the **Uploaded Switch Firmwares** section is populated with the firmware version and switch models it supports.

You have successfully uploaded the switch firmware to the controller.

Scheduling a Firmware Upgrade for Selected Switches

You can upgrade or downgrade the firmware version of a switch or multiple switches that you are monitoring. You can upgrade the firmware on demand or schedule a firmware update for a list of selected switches.

Prerequisites

- Upload a valid FastIron firmware version (newer than version 8.0.80) to the controller.
- Sync the controller with the NTP server. On the controller user interface, navigate to **Administration** > **System** > **Time** then click **Sync Server**.

Scheduling Firmware Upgrade

1. From the main menu, click **Network** > **Wired** > **Switches**.

   The **Switches** page is displayed.

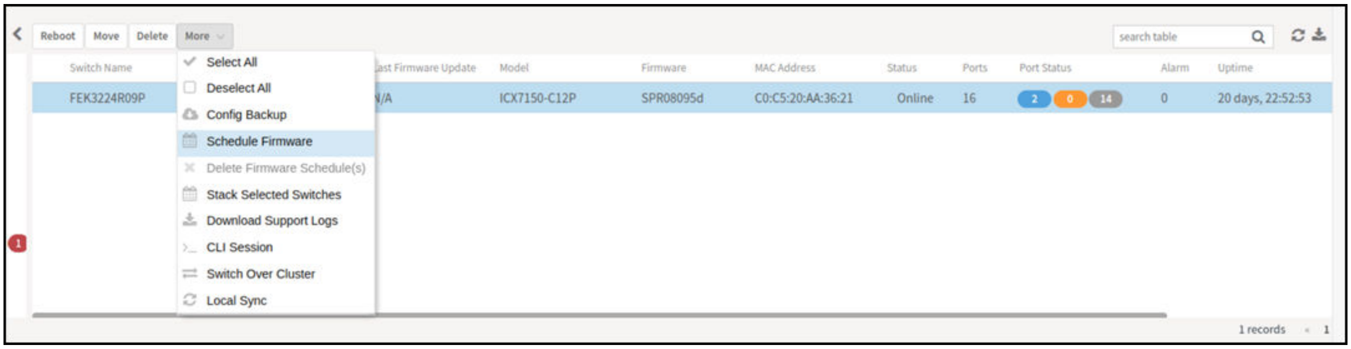
2. Select a **Domain** > **Switch Group** or specific **Switch Group** and select the **Switch** that you want to upgrade.

   NOTE

   To upgrade the firmware for multiple switches simultaneously, hold down the **Ctrl** key as you select the desired switches.

3. Click **More** > **Schedule Firmware**.

FIGURE 123 Selecting Schedule Firmware

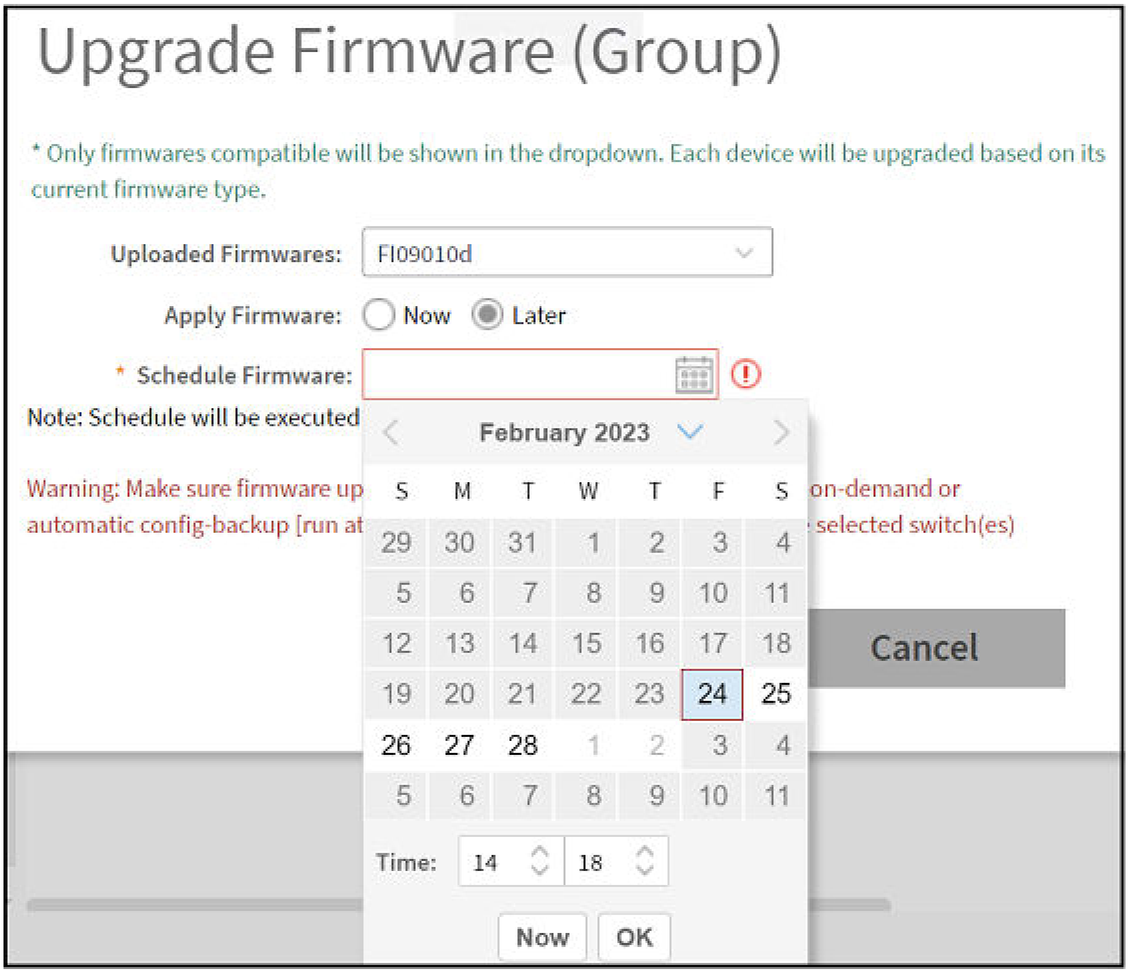


Switch Name	ast Firmware Update	Model	Firmware	MAC Address	Status	Ports	Port Status	Alarm	Uptime
FEK3224R09P	/A	ICX7150-C12P	SPR08095d	C0:C5:20:AA:36:21	Online	16	2 0 14	0	20 days, 22:52:53

1 records

The **Upgrade Firmware** dialog box is displayed.

FIGURE 124 Scheduling Firmware Upgrade



Upgrade Firmware (Group)

* Only firmwares compatible will be shown in the dropdown. Each device will be upgraded based on its current firmware type.

Uploaded Firmwares: FI09010d

Apply Firmware: ○ Now ● Later

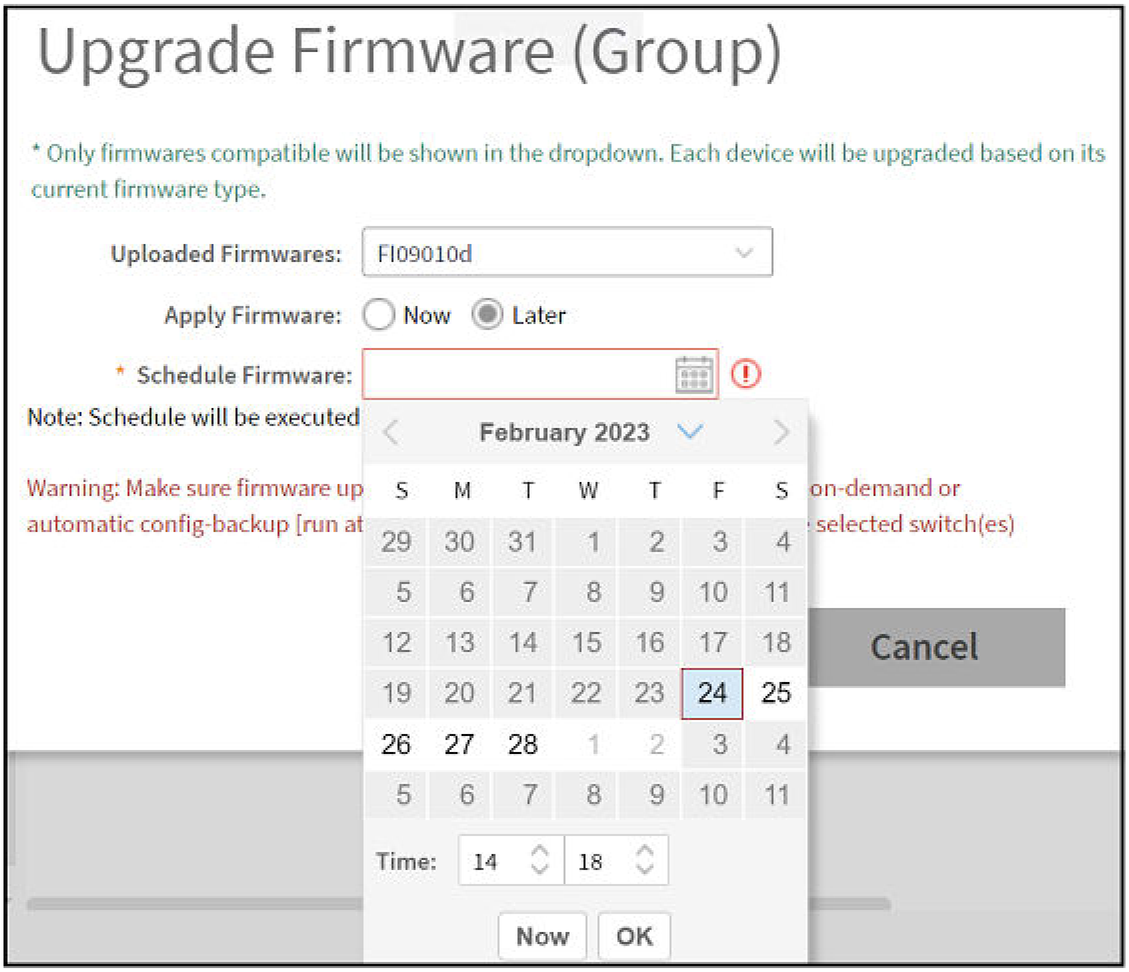
* Schedule Firmware:

Note: Schedule will be executed

Warning: Make sure firmware up on-demand or automatic config-backup [run at selected switch(es)

4. Complete the following fields:
   - **Uploaded Firmwares**: Select the firmware version that you want the switch to be upgraded to.
   - **Firmware Type**: Select type of firmware you want to upload to the switch. Options include **Switch** and **Router** images.
   - **Apply Firmware**: Set when you want to apply the new firmware version to the switch. You can select **Now** or **Later** to schedule your upgrade. If you select **Later**, then you must select the date and time from the **Schedule Firmware** field.

FIGURE 125 Scheduling Firmware Upgrade



Upgrade Firmware (Group)

* Only firmwares compatible will be shown in the dropdown. Each device will be upgraded based on its current firmware type.

Uploaded Firmwares: FI09010d

Apply Firmware: ○ Now ● Later

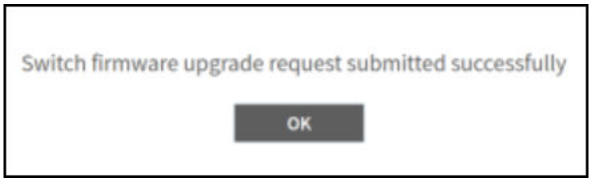
* Schedule Firmware:

Note: Schedule will be executed

Warning: Make sure firmware up on-demand or automatic config-backup [run at selected switch(es)

The switch upgrade request success message is displayed.

FIGURE 126 Switch Upgrade Request Success



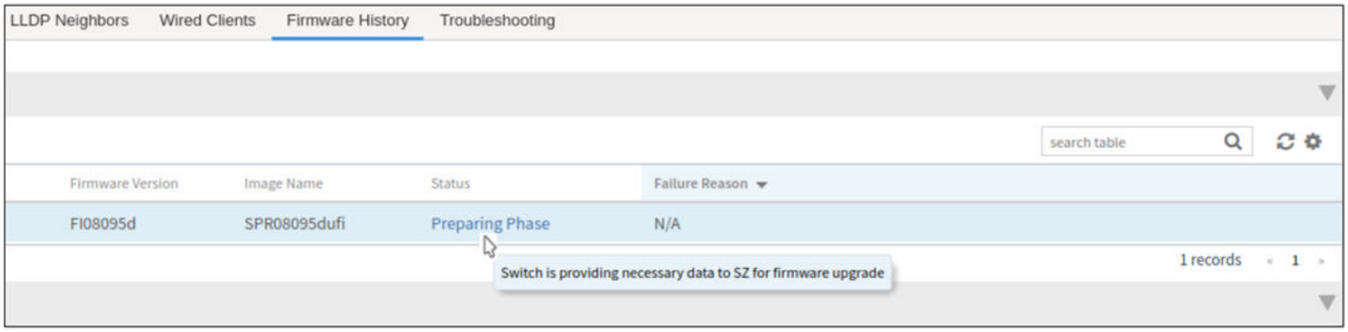
Switch firmware upgrade request submitted successfully

5. Click **OK**.

6. To monitor the firmware upgrade progress, select the target switch and click the **Firmware History** tab. Hover your cursor over any message in the **Status** field for a tooltip providing additional information regarding that stage of the upgrade process.

   The images of six stages of completion along with their tooltips are shown below.

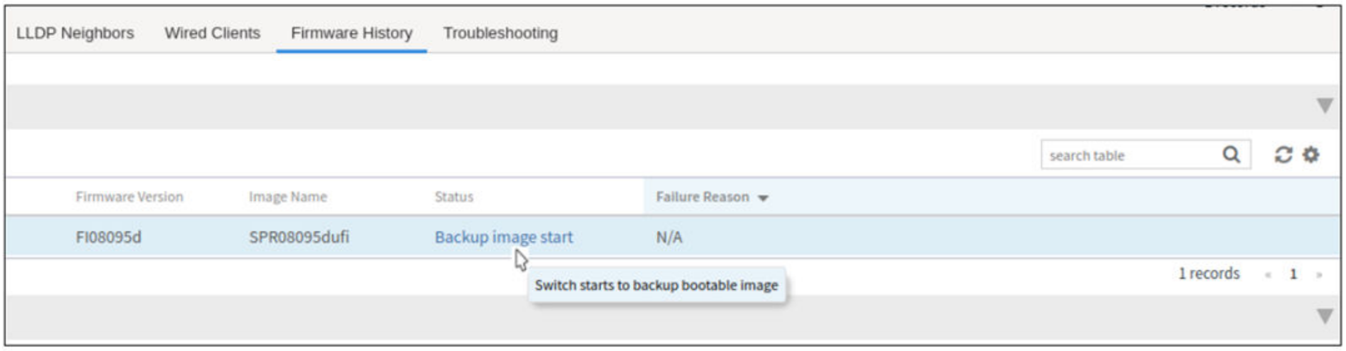
   FIGURE 127 Preparing Phase with Tooltip



Firmware Version	Image Name	Status	Failure Reason
FI08095d	SPR08095dufi	Preparing Phase	N/A

Switch is providing necessary data to SZ for firmware upgrade

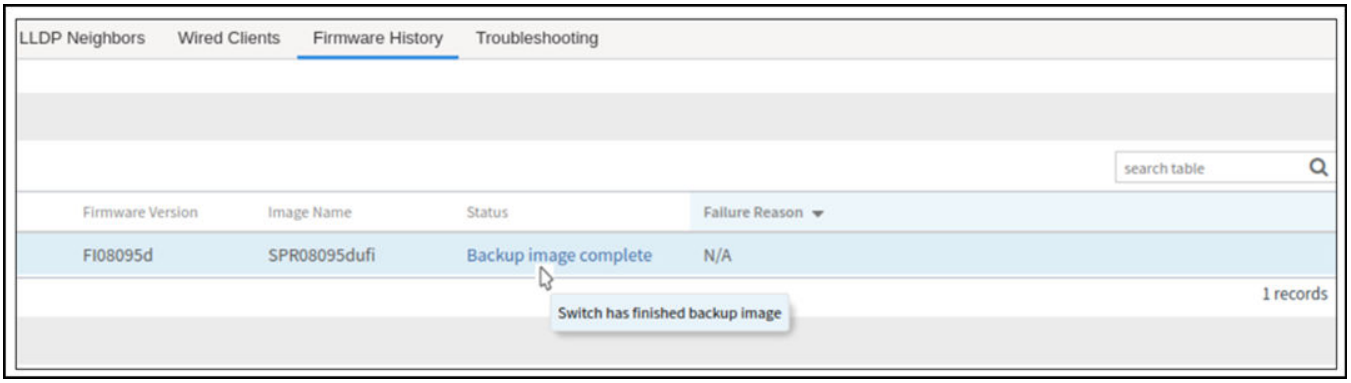
   FIGURE 128 Backup Image Start with Tooltip



Firmware Version	Image Name	Status	Failure Reason
FI08095d	SPR08095dufi	Backup image start	N/A

Switch starts to backup bootable image

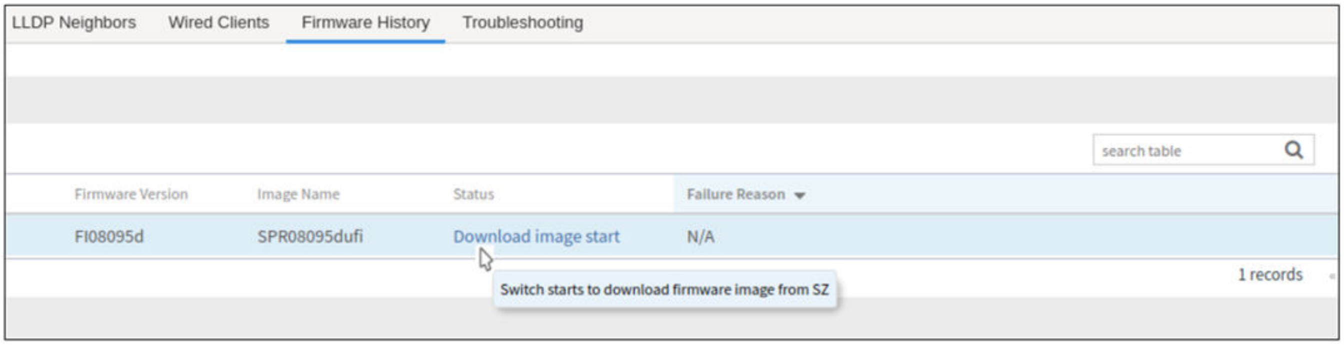
   FIGURE 129 Backup Image Complete with Tooltip



Firmware Version	Image Name	Status	Failure Reason
FI08095d	SPR08095dufi	Backup image complete	N/A

Switch has finished backup image

   FIGURE 130 Download Image Start with Tooltip

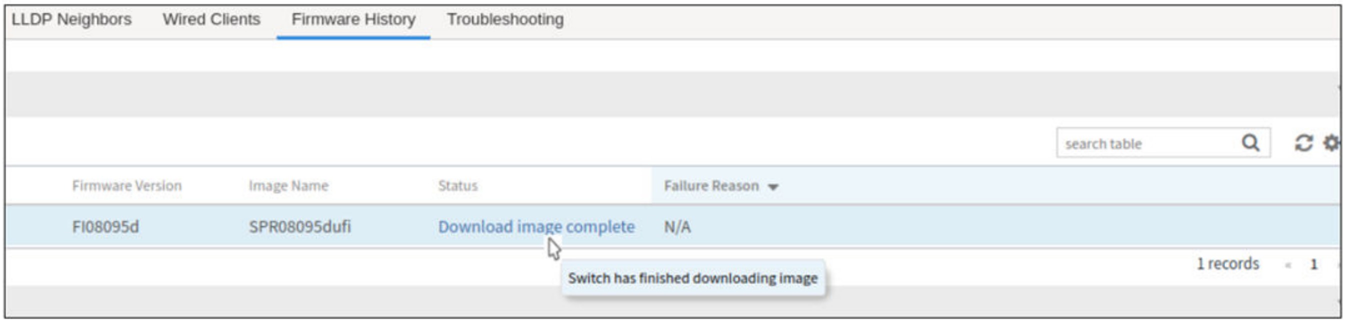


Firmware Version	Image Name	Status	Failure Reason
FI08095d	SPR08095dufi	Download image start	N/A

Switch starts to download firmware image from SZ

1 records

FIGURE 131 Download Image Complete with Tooltip

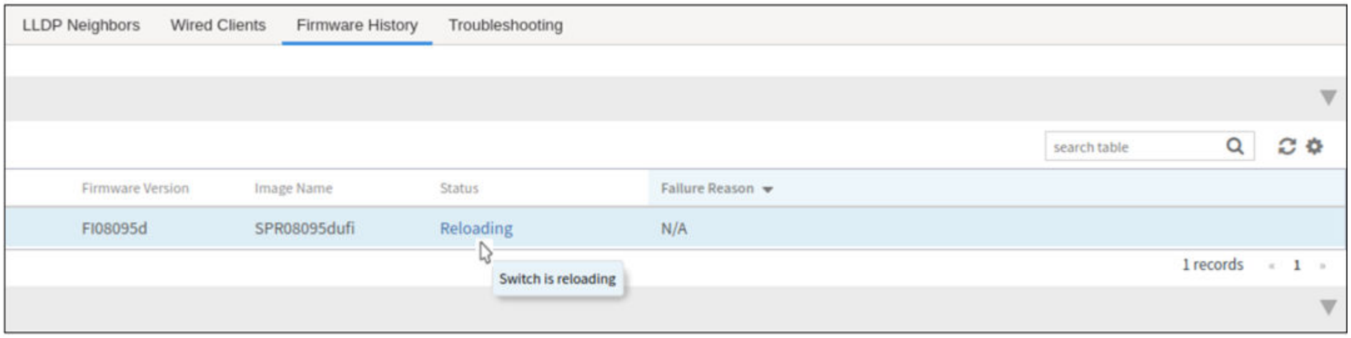


Firmware Version	Image Name	Status	Failure Reason
FI08095d	SPR08095dufi	Download image complete	N/A

Switch has finished downloading image

1 records « 1

FIGURE 132 Reloading phase with tooltip



Firmware Version	Image Name	Status	Failure Reason
FI08095d	SPR08095dufi	Reloading	N/A

Switch is reloading

1 records « 1 »

Delete the Scheduled Firmware Update

If the switch firmware upgrade has not yet been executed, then you can cancel the scheduled upgrade as follows:

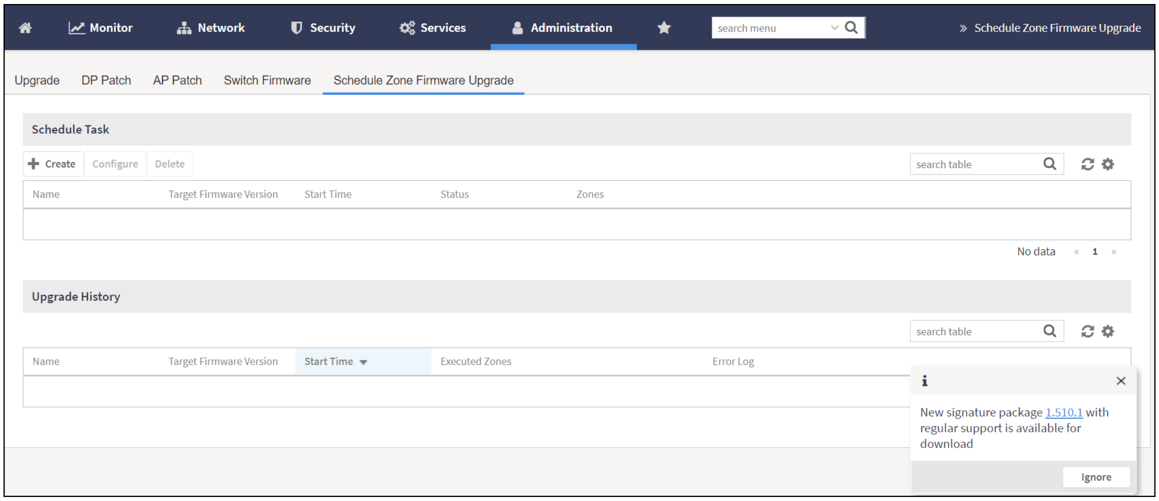
1. In the **Organization** tab, select a **Domain** > **Switch Group** or specific **Switch Group** and select the **Switch**.
2. Click **More** > **Delete Firmware Schedule(s)** to display a **Confirmation Message** dialog box.
3. Click **Yes** to display a **Delete Successful** message dialog box.
4. Click **OK**.

Schedule Zone Firmware Upgrade

The controller allows the administrator to set up a scheduled date and time to upgrade/downgrade single or multiple zone firmware. After a zone firmware upgrade/downgrade task is executed, the administrator can see the zone firmware change history.

1. On the menu, click **Administration** > **Administration** > **Upgrade** > **Schedule Zone Firmware Upgrade** to display the **Schedule Zone Firmware Upgrade** tab.

   FIGURE 133 Schedule Zone Firmware Upgrade



Name	Target Firmware Version	Start Time	Status	Zones

No data « 1 »

Name	Target Firmware Version	Start Time ▼	Executed Zones	Error Log

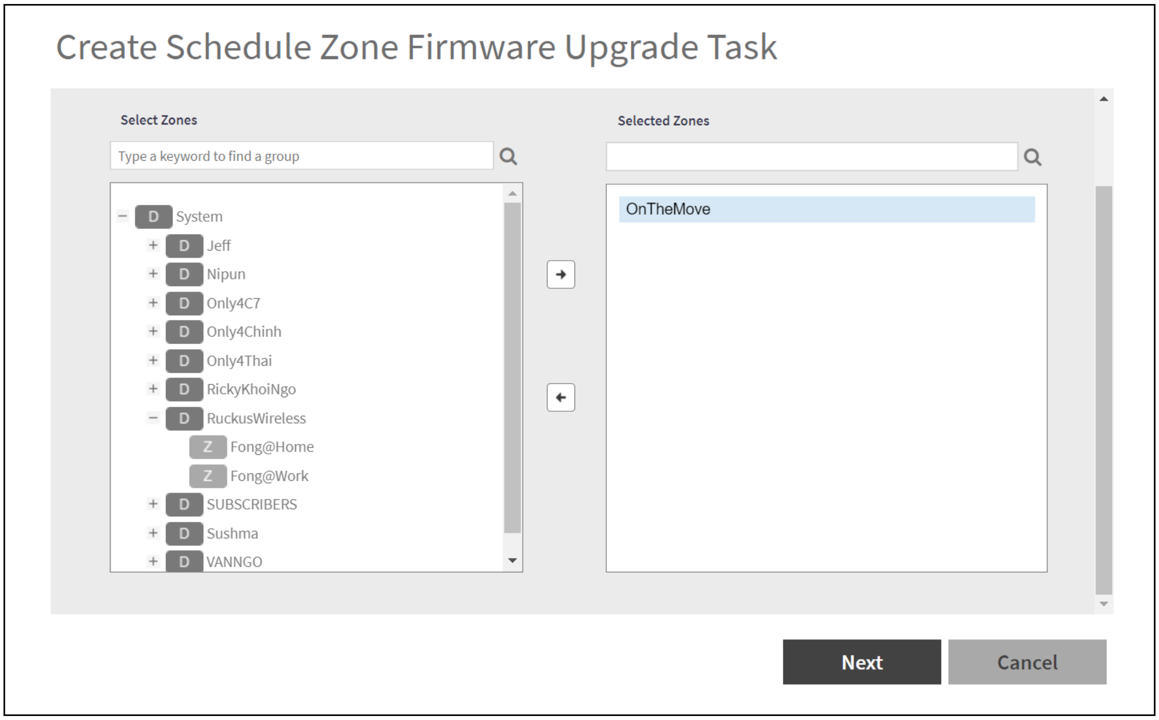
New signature package 1.510.1 with regular support is available for download

2. Click the + Create tab to display the **Create Schedule Zone Firmware Upgrade Task** dialog box.

3. Select a **Zone** or select many **Zones** by pressing the **Ctrl** key and selecting the **Zones** that you want to add to the **Selected Zones** field.

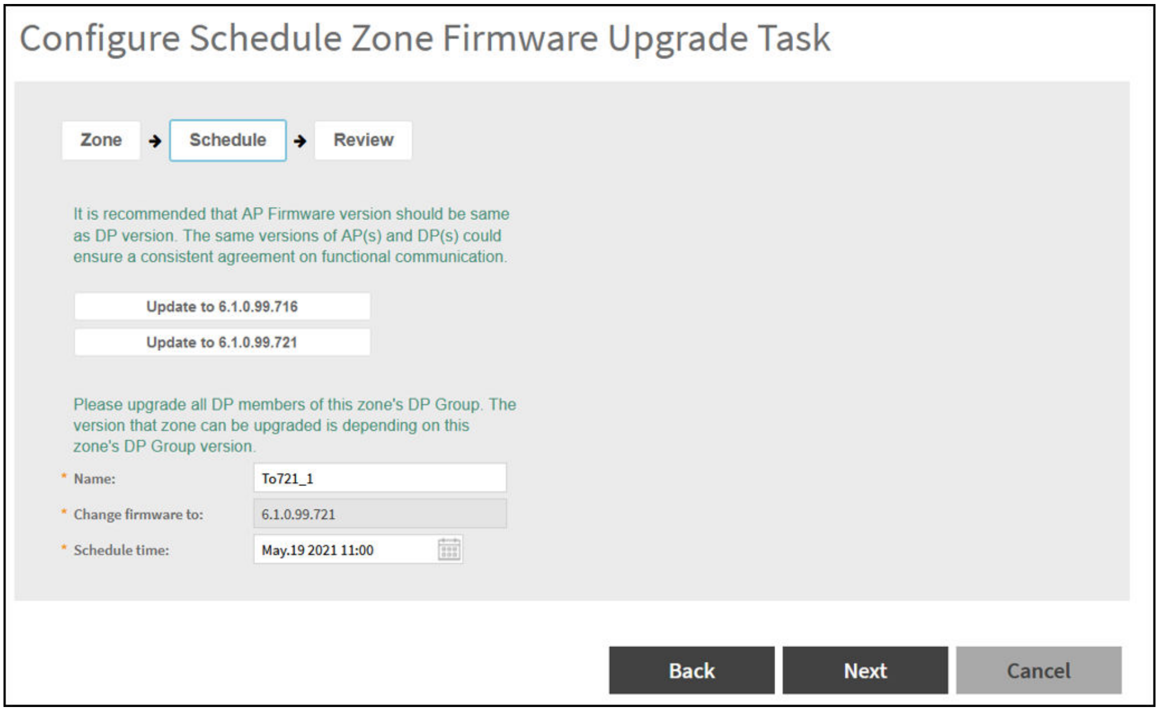
4. Click the → icon to move the selected zones to the **Selected Zones** tab. Click the ← icon to send any selected zones from **Selected Zones** back to the **Select Zones**.

FIGURE 134 Schedule the Zone Firmware Upgrade Task



5. Click **Next** to display the **Schedule** dialog box.

FIGURE 135 Create Schedule Zone Firmware Upgrade Task



It is recommended that AP Firmware version should be same as DP version. The same versions of AP(s) and DP(s) could ensure a consistent agreement on functional communication.

Please upgrade all DP members of this zone's DP Group. The version that zone can be upgraded is depending on this zone's DP Group version.

* Name: To721_1
* Change firmware to: 6.1.0.99.721
* Schedule time: May.19 2021 11:00

6. Complete the following fields:
   - **Name**: Enter the name for this task.
   - **Change Firmware to**: Select the firmware from the list that is available at the beginning of the **Schedule** dialog box.
   - **Scheduled time**: Select the date and time for the scheduled upgrade to execute.
7. Click **Next** to display the **Review** dialog box.
8. Review the task and click **OK**.

Scheduling a Firmware Upgrade for Switch Group

You can upgrade a switch group on a Level 1 group that has no default firmware setting. The forced upgrade allows the device to remain in the same firmware type (Layer 2 still Layer 2, Layer 3 still Layer 3) with only a change to the version type.

NOTE
If the switch group has a default firmware selected the **Firmware Upgrade** option is unavailable.

NOTE
Beginning with FastIron release 10.0.0, a switch ("Layer 2") image will no longer be provided for ICX devices. Only the router ("Layer 3") image will be available. On Upgradeto FastIron 10.0.00, the configuration of any ICX devices operating with the switch image will automatically be translated to the equivalent router image configuration.The target upgrade to 10.0.0 supports only router code.
The following features are deprecated as a result of this change:

- The IP default gateway
- The management VLAN
- Global configuration of the IP address (Going forward, the IP address must be configured at the interface level for each port.)

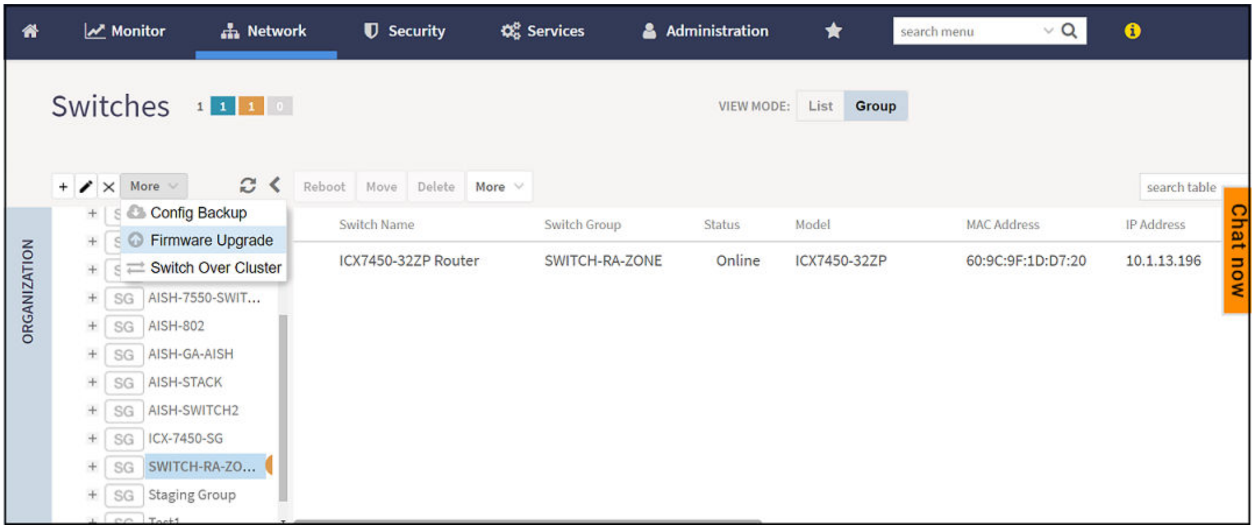
Refer to the RUCKUS FastIron Software Upgrade Guide for additional details.

Complete the following steps to perform a firmware upgrade on the switch group.

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

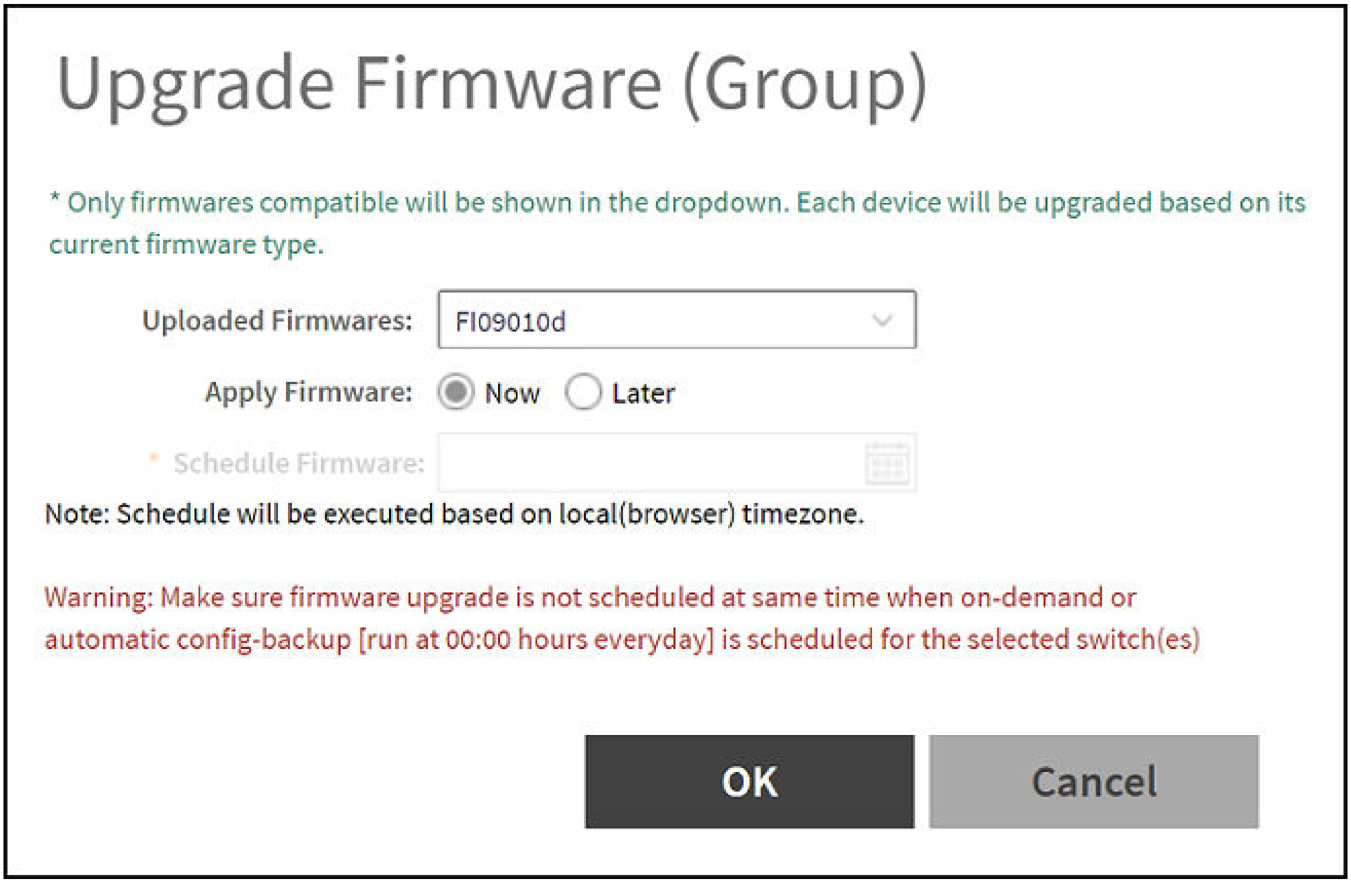
3. Click **More** > **Firmware Upgrade** to display the **Upgrade Firmware (Group)** dialog box.

FIGURE 136 Selecting Firmware Upgrade for a Switch Group



Switch Name	Switch Group	Status	Model	MAC Address	IP Address
ICX7450-32ZP Router	SWITCH-RA-ZONE	Online	ICX7450-32ZP	60:9C:9F:1D:D7:20	10.1.13.196

FIGURE 137 Scheduling the Upgrade for a Switch Group



Upgrade Firmware (Group)

* Only firmwares compatible will be shown in the dropdown. Each device will be upgraded based on its current firmware type.

Uploaded Firmwares: FI09010d

Apply Firmware: ● Now ○ Later

* Schedule Firmware:

Note: Schedule will be executed based on local(browser) timezone.

Warning: Make sure firmware upgrade is not scheduled at same time when on-demand or automatic config-backup [run at 00:00 hours everyday] is scheduled for the selected switch(es)

4. Complete the following fields:
   - **Uploaded Firmwares**: Select firmware from the list.
   - **Apply Firmware**: Select Now or Later to set the new firmware version to the switch group.
   - **Schedule Firmware**: If you select Later for **Apply Firmware**, you must select the date to schedule the upload.
5. Click **OK**.

Cautions & Limitations of Administrating a Cluster

Wipeout Upgrade

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

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

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

Cluster Upgrade

For issues during software upgrade, you can only perform the software rollback from the CLI using the restore command. If you have a two nodes controller cluster, run the restore command on one of the nodes to restore them to the previous software before attempting to upgrade them again. The restore command will trigger restore action on all nodes of the cluster if all nodes could be connected to each other. Confirm if each node could be restored back to the previous version. If any node does not roll back to previous version, execute the restore command again on the failure node. Refer Rolling Back to a Previous Software Version on page 218.

ZD Migration

ZoneDirector to SmartZone Migration

SmartZone controllers are better equipped to handle large WiFi deployments such as within campuses and when customers are vastly distributed; therefore, RUCKUS recommends that you migrate existing ZoneDirector deployments to SmartZone controller deployments. You can migrate ZoneDirector AP configuration information to SmartZone controllers from the controller itself, using a migration tool.

The AP models must be supported by the controller.

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

TABLE 31 Migration Support Matrix

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

> ⚠ **CAUTION**
> **Do not power off the AP during the migration process.**

1. Go to **Administration** > **Administration** > **ZD Migration**.

   The **ZoneDirector Migration** page appears.

2. Configure the following:

   a. ZoneDirector IP Address: Type the IP address of the ZD that you want to migrate.

   b. Admin Credentials: Enter the username and password details to access/login to ZD.

   c. Click **Connect**. Lists of APs connected to the ZD deployment are displayed.

   d. Click **Select AP** to choose the AP information that you want to migrate from ZD.

   e. Click **Migrate** to migrate the AP. The controller imports the ZD configuration and applies it to the selected AP.

   The **ZoneDirector Migration Status** section displays the status of the migration. When completed successfully, a success message is displayed. If migration fails, a failure message is displayed and you can attempt the migration process again.

   > **NOTE**
   > To migrate ZoneDirector Mesh APs to SmartZone, upgrade ZoneDirector to its supported version. For information on the supported versions, refer to the release notes.

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