

# RUCKUS FIPS and Common Criteria Configuration Guide for SmartZone and AP, 5.2.1.3

**Supporting SmartZone Release 5.2.1.3 on SZ300, SZ144, vSZ and vSZ-D**

© 2023 CommScope, Inc. All rights reserved.

No part of this content may be reproduced in any form or by any means or used to make any derivative work (such as translation, transformation, or adaptation) without written permission from CommScope, Inc. and/or its affiliates ("CommScope"). CommScope reserves the right to revise or change this content from time to time without obligation on the part of CommScope to provide notification of such revision or change.

## Export Restrictions

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

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

## Disclaimer

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

## Limitation of Liability

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

## Trademarks

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

## Patent Marking Notice

For applicable patents, see [www.cs-pat.com](http://www.cs-pat.com).

# Contents

---

<b>Contact Information, Resources, and Conventions.....</b>	<b>9</b>
Contacting RUCKUS Customer Services and Support.....	9
What Support Do I Need?.....	9
Open a Case.....	9
Self-Service Resources.....	10
Document Feedback.....	10
RUCKUS Product Documentation Resources.....	10
Online Training Resources.....	10
Document Conventions.....	11
Notes, Cautions, and Safety Warnings.....	11
Command Syntax Conventions.....	11
<b>About This Guide.....</b>	<b>13</b>
What's New in This Document.....	13
<b>Federal Information Processing Standards.....</b>	<b>15</b>
FIPS Mode Overview.....	15
Crypto Officer Roles and Responsibilities.....	15
Zeroization Process.....	16
Quarantine State.....	16
<b>vSZ Installation with FIPS Image.....</b>	<b>17</b>
System Requirements .....	17
vSZ Installation Prerequisites for FIPS.....	17
Creating and Registering the Virtual Machine.....	17
<b>Hardware Configuration with FIPS Image .....</b>	<b>23</b>
<b>Controller Configuration with FIPS Image .....</b>	<b>25</b>
Using FIPS-Related CLI Commands.....	25
Viewing and Downloading FIPS Logs.....	28
Uploading Certificates to SmartZone OS.....	30
Enabling Other Secured Communication Services.....	33
RadSec (RADIUS over TLS).....	35
Configuring RadSec.....	36
Mapping the Authentication Profile for the WLAN.....	49
Viewing the WLAN Configurations List.....	51
Upgrading the Software.....	52
Upgrading (v)SZ Software.....	52
Working with Application Signature Package.....	54
Upgrading the AP Software.....	57
Upgrading the vSZ-D Software.....	60
<b>vSZ-D FIPS Installation with FIPS Image.....</b>	<b>65</b>
System Requirements.....	65
vSZ-D FIPS Installation Prerequisites for FIPS.....	65
Creating and Registering the Virtual Machine (vSZ-D).....	65
Joining vSZ-D to the vSZ Controller.....	71
Using FIPS CLI Commands (vSZ-D).....	75

Downloading vSZ-D FIPS Logs.....	78
<b>AP Configuration in FIPS Mode.....</b>	<b>79</b>
AP Models that Support FIPS Mode.....	79
Joining AP to (v)SZ Controller.....	80
Management Channel between AP/vSZ-D and Controller.....	81
Configuring Regular Mesh.....	82
Creating an AP Zone.....	82
FIPS AP Behavior.....	85
Crypto Officer Roles and Responsibilities for AP.....	86
Quarantine State for AP.....	86
AP Features Not Supported in FIPS Mode.....	86
Recovery SSID Not Supported.....	87
FTP, TFTP, and Web Not Supported.....	88
HTTP and Telnet Management Access Not Supported.....	88
Web Interface Access Through HTTPS Not Supported.....	89
SNMPv1 and SNMPv2c Not Supported.....	90
WLAN Interface Up or Down from AP CLI Not Supported.....	91
Creating a WLAN WPA3 WLAN2/WPA3 Mixed Profile.....	91
Recovery SSID.....	95
SSH Public Key Authentication.....	98
SSH Public Key Authentication.....	98
<b>Configuring SSH Authentication Method.....</b>	<b>99</b>
Connecting to SZ using each of the methods from Linux Client.....	106
<b>X.509 Certificates.....</b>	<b>115</b>
Generating Certificate Signing Request (CSR).....	115
Configuring X.509 Server Certificates on the Controller.....	116
Validating Certificates.....	120
Uploading X.509 Certificates on AP.....	122
Uploading X.509 Certificates on vSZ-D.....	124
<b>Management Certificate Check.....</b>	<b>129</b>
System Behaviour.....	129
Viewing the Default Certificate using Controller Web Interface.....	129
Modifying and Re-generating the Default Certificate using CLI.....	132
<b>Password Management.....</b>	<b>135</b>
<b>Configuring the WLAN Scheduler.....</b>	<b>137</b>
Setting the WLAN Scheduler from the CLI.....	138
<b>Terminating Sessions.....</b>	<b>141</b>
Terminating Sessions for Non-Admin Users.....	142
Terminating Administrator Sessions.....	143
<b>Locking an Administrator Account .....</b>	<b>147</b>
Locking Non-Administrator Accounts.....	148
<b>Setting Up the Login Banner.....</b>	<b>151</b>
<b>Deployment Models.....</b>	<b>155</b>
<b>Configuring RUCKUS GRE and IPSec in WLAN-Concept.....</b>	<b>157</b>
Creating an IPSec Profile.....	157



Creating a RUCKUS GRE Profile.....	159
Creating an AP Zone.....	160
Creating AP GRE Tunnel Profile.....	167
Creating WLAN Configuration.....	168
Mapping RUCKUS GRE and IPsec Profile to WLAN.....	168
<b>System IPsec.....</b>	<b>169</b>
Configuring System IPsec using Preshared Key.....	170
Configuring System IPsec using Certificates.....	173
Configuring IKE and ESP Rekeying Separately.....	176
Configuring System IPsec OCSP Settings.....	179
<b>Configuring System Time.....</b>	<b>185</b>
<b>Adminstrating the Controller.....</b>	<b>189</b>
Adminstrating the Controller using CLI Console.....	189
Adminstrating the Controller Remotely.....	190
<b>Configuring FIPS Disable Mode.....</b>	<b>193</b>
Configuring the FIPS Disable Mode.....	193
FIPS Disable Mode Matrix.....	196
Upgrade Matrix in FIPS Disable Mode.....	197
Features in FIPS Disable Mode.....	197
<b>Wireless Intrusion Detection and Prevention System.....</b>	<b>199</b>
Allowed Device Profile.....	199
Configuring Allowed Device Profile.....	200
Monitoring Access Points (APs).....	203
Integrated Mode.....	203
Overlay Mode.....	203
Hybrid Mode.....	203
Creating a Monitoring Access Point (AP).....	203
Rogue Devices.....	206
Classifying a Rogue Policy.....	206
Viewing Rogue Devices.....	209
Filtering Rogue Devices.....	210
Marking Rogue Access Points.....	210
Locating a Rogue Device.....	210
Audit/Event Alert.....	215
System level Audit/Event Alert.....	216
Zone Level Audit/Event Alert.....	216
Reports.....	217
Access Points or AP Reports.....	217
Client Report.....	219
External Syslog Server.....	221
Configuring External Syslog Server.....	222
Signature Based Detection Rule.....	223
Creating a Signature-Based Detection Profile.....	224
AP MAC OUI Address.....	228
Creating an AP MAC OUI Address.....	228
Different Rule types and Classification.....	228
Active Probing.....	229
Ad Hoc.....	229

AllowListed AP.....	229
AllowListed Client.....	229
Auth Flood.....	230
Client MAC Spoofing.....	230
Connected Unauthorized SSID.....	230
CTS Abuse.....	230
Deauth Flood.....	231
Disassoc Flood.....	231
EAP Flood.....	231
Excessive Power.....	231
Failed Attempts WLAN.....	232
ICS Connection.....	232
Long SSID.....	232
Low RSSI.....	232
MAC OUI.....	233
MAC Spoofing.....	233
Max Clients.....	233
Mesh Network.....	233
Non-Allowlisted AP.....	234
Non-Allowlisted Client.....	234
Null SSID.....	234
Packet Flood.....	234
RTS Abuse.....	235
Same Network.....	235
Signature Based.....	235
SSID.....	235
SSID Spoofing.....	236
Unauthorized Ap Broadcast Authorized SSID.....	236
Unauthorized Auth Scheme.....	236
Unauthorized Encryption Scheme.....	236
Unauthorized SSID.....	237
Unencrypted Traffic.....	237
Weak/Outdated Protocol.....	237
Weak/Unsupported/Disallowed Encryption Scheme.....	237
Windows Hosted Network.....	238
<b>Tamper-Evident Seals.....</b>	<b>239</b>
General Information about Tamper-Evident Seals.....	239
Tamper-Evident Seals on SmartZone144 Devices.....	239
Tamper-Evident Seals on SmartZone 300 Devices.....	243
Tamper-Evident Seals on T610 AP Devices.....	245
Tamper-Evident Seals on R610 AP Devices.....	245
Tamper-Evident Seals on R720 AP Devices.....	246
<b>Trusted Channels Through TSF.....</b>	<b>249</b>
Trusted Communication Channels.....	249
Enabling Trusted Channel Using IEEE 802.11-2012 (WPA2) Standards .....	249
Enabling Trusted Channel Using IEEE 802.1X and IPsec.....	250
<b>FIPS-Compliant Products.....</b>	<b>251</b>
AP Controller Matrix.....	251
FIPS-Compliant Product SKUs and Descriptions.....	251

<b>Connecting the Switches to Controller.....</b>	<b>253</b>
Configuring the Switches to Connect to Controller.....	253
Configuring the Controller to Access the Switch.....	257
Viewing Switch from the Controller.....	258
Deleting Switch from the Controller.....	259
<b>Two-Factor Authentication .....</b>	<b>261</b>
<b>Creating Switch Groups.....</b>	<b>263</b>
<b>Creating User Groups (FIPS).....</b>	<b>265</b>
<b>Importing New Certificates.....</b>	<b>267</b>
<b>Configuring SZ Admin AAA Servers.....</b>	<b>269</b>
<b>Enabling Common Access Card or Personal Identity Verification Authentication.....</b>	<b>273</b>
<b>Events.....</b>	<b>275</b>
Fails to establish TLS tunnel between SZ and External AAA Server.....	275
SZ Login fail.....	275
SZ Login .....	276
SZ Logout .....	276
Unsync NTP time.....	276
SZ Failure of Certificate.....	276
NodeRebooted.....	277
NodeShutdown.....	277
Auditable Events in AP and DP for Common Criteria.....	277
<b>Audit Records.....</b>	<b>281</b>
Viewing the Events and Alarms.....	281
Downloading the Logs from the Controller.....	282
Viewing the Audit Records.....	283



# Contact Information, Resources, and Conventions

---

- [Contacting RUCKUS Customer Services and Support](#)..... 9
- [Document Feedback](#)..... 10
- [RUCKUS Product Documentation Resources](#)..... 10
- [Online Training Resources](#)..... 10
- [Document Conventions](#)..... 11
- [Command Syntax Conventions](#)..... 11

## 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](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](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](mailto:#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	<code>device(config)# interface ethernet 1/1/6</code>
<b>bold</b>	User interface (UI) components such as screen or page names, keyboard keys, software buttons, and field names	On the <b>Start</b> menu, click <b>All Programs</b> .
<i>italics</i>	Publication titles	Refer to the <i>RUCKUS Small Cell Release Notes</i> 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
<b>bold text</b>	Identifies command names, keywords, and command options.
<i>italic text</i>	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, <i>member[member...]</i> .
\	Indicates a "soft" line break in command examples. If a backslash separates two lines of a command input, enter the entire command at the prompt without the backslash.





# About This Guide

- [What's New in This Document.....](#) 13

## What's New in This Document

**TABLE 2** Summary of Enhancements in FIPS Release 5.2.1.3

Feature	Description	Location
Removed all instances of SZ100	Replaced all instances of SZ100, SmartZone 100 to SZ144.	Complete document
Allowed Device Profile	Allowed device profile contains list of MAC addresses of APs and EUDs that are part of the profile and considered as authorized devices.	<a href="#">Allowed Device Profile</a> on page 199
Monitoring Access Points(AP)	Monitoring AP is deployed in 3 modes. <ul style="list-style-type: none"> <li>• Integrated Mode</li> <li>• Overlay Mode</li> <li>• Hybrid Mode</li> </ul>	<a href="#">Monitoring Access Points (APs)</a> on page 203
Rogue Devices	Rogue APs and clients are unauthorized devices that may pose potential threats to a wireless network. Their activities can significantly impact the performance of a wireless network, or even cause serious security issues.	<a href="#">Rogue Devices</a> on page 206
Audit/Event Alert	After the successful detection of rogue devices, alerts are generated and reported to SmartZone controller. These alerts can be viewed by an Administrator.	<a href="#">Audit/Event Alert</a> on page 215
Reports	Reports display a list of rogue devices that were detected in a specific zone containing one or more monitor APs.	<a href="#">Reports</a> on page 217
External System Log	System logging is a method network devices use standard message format to communicate with a logging server.	<a href="#">External Syslog Server</a> on page 221
Signature Based Rules	Signature-based (SB) rules are global configuration. User can create signature-based rules once and use them in a zone or multiple zones.	<a href="#">Signature Based Detection Rule</a> on page 223
AP MAC OUI Address	User must enable the AP MAC OUI validation with specific Organizationally Unique Identifier (OUI) to allow an AP to connect to SmartZone.	<a href="#">AP MAC OUI Address</a> on page 228
Different Rule Types and Classifications	Rogue Classification Policy is configured to Detect and Report the rogues devices in the network.	<a href="#">Different Rule types and Classification</a> on page 228
Administrating the Controller Remotely	Updated the SSHv2 support task steps.	<a href="#">Administrating the Controller Remotely</a> on page 190

## About This Guide

### What's New in This Document

**TABLE 2** Summary of Enhancements in FIPS Release 5.2.1.3 (continued)

Feature	Description	Location
Viewing the Audit Records	Added six new auditable event tables. <ul style="list-style-type: none"><li>• Action taken due to potential security violations.</li><li>• Presence of allowedlisted device.</li><li>• Location of AP or EUD.</li><li>• Detection of rogue AP or EUD.</li><li>• Detection of unauthorized SSID.</li><li>• Sensor wireless transmission capabilities.</li></ul>	<a href="#">Viewing the Audit Records on page 283</a>

# Federal Information Processing Standards

- [FIPS Mode Overview](#)..... 15
- [Crypto Officer Roles and Responsibilities](#)..... 15
- [Zeroization Process](#)..... 16
- [Quarantine State](#)..... 16

## FIPS Mode Overview

A device in Federal Information Processing Standards (FIPS) mode is compliant with the standards established by the United States government, Common Criteria, and the National Institute of Standards and Technology (NIST).

The FIPS Publication 140-2 is a technical standard and worldwide de-facto standard for the implementation of cryptographic modules. The FIPS Publication 140-2 contains security standards developed by the United States government and the National Institute of Standards and Technology (NIST) for use by all non-military government agencies and by government contractors. Due to their importance within the security industry, these standards form a baseline for many security requirements.

Common Criteria (CC) is an international set of guidelines and specifications developed for evaluating information security products, specifically to ensure they meet and agreed-upon security standard for government deployments through Common Criteria Security Target, NIAP Protection Profiles .

You can configure the device to run in FIPS mode to ensure that the device is operating according to the standards stated in FIPS Publication 140-2. .

A device is FIPS 140-2-compliant when the following requirements have been considered:

- Enabling FIPS mode physically brings the devices, FIPS and CC compliance mode wherein only the FIPS and CC compliance cryptographic algorithms and processes are allowed. No additional configuration other than enabling FIPS mode is needed to limit the cryptographic algorithms and processes available to be CC/FIPS compliant.
- Tamper-evident security seals labels are applied to the device according to the instructions included in [Tamper-Evident Seals](#) on page 239. The accessory kit must be purchased separately.
- The device software is placed in FIPS mode with the FIPS security policy applied and CC Security Target applied.

### NOTE

1. Not all software releases support FIPS. Refer to the Release notes for the software you are running to see if it supports FIPS.
2. To determine if the device and current software version are FIPS-certified, refer to <http://csrc.nist.gov/groups/STM/cmvp/validation.html>.
3. For the SmartZone feature configuration, refer to the 5.2.1 Administration Guide, <https://support.ruckuswireless.com/admin/documents/3325-smartzone-5-2-1-ga-administrator-guide-sz300-vs-z-h>.

## Crypto Officer Roles and Responsibilities

The administrator (admin) is treated as a Crypto Officer (CO) and is the default user created during the Controller installation. The admin role is the only user role available on the vSZ-D and the access point (AP). The CO can perform the following FIPS-related activities:

- Zeroization
- Mode change
- Downloading FIPS logs for analysis

- Performing on-demand self-tests
- Restoring the system when it has moved to the quarantine state

Unlike Controller, the vSZ-D and the AP have a single admin login which is the CO role.

Regardless of the component, no administrative action can be performed prior to authentication as an administrator user.

## Zeroization Process

The zeroization process deletes and overwrites all system configuration, network configuration, private and public keys, certificates, passwords, pass phrases, and data. The zeroization process resets the vSZ to factory settings.

For controller, zeroization is achieved by changing the FIPS mode from enable to disable or from disable to enable. A mandatory message is displayed after the **fips enable** command or the **fips disable** command is entered to warn you about the effects of executing the command. You must enter **yes** to confirm or **no** to cancel the command.

## Quarantine State

When a power-on self-test (POST) fails, the system moves to the quarantine state. In the quarantine state, only the CO (admin) can log in to the command line interface (CLI) through console access, and recover the system, and limited CLI commands are available for system recovery.

In the quarantine state, all communication towards external nodes is disabled, and network interfaces are down. The output for the **fips status** command displays the current FIPS mode and the quarantine status, as shown in the following figures.

FIGURE 1 Quarantine Status (vSZ)

```
SZ300-1> en
Password: *****

SZ300-1#
SZ300-1# fips status
FIPS compliance is Enable
In quarantine state
SZ300-1#
```

FIGURE 2 Quarantine Status (vSZ-D)

```
vDP-FIPS# fips status
FIPS compliance is Enable
In quarantine state
vDP-FIPS#
```

To recover from the quarantine state, the CO (admin) must log in to the console and use the **fips disable** command, and enter **yes** to confirm. This cleans up the system and recovers the CLI capabilities. The CO (admin) can use the **setup** command to reconfigure the system.

# vSZ Installation with FIPS Image

- System Requirements ..... 17
- vSZ Installation Prerequisites for FIPS..... 17
- Creating and Registering the Virtual Machine..... 17

## System Requirements

The virtual platform (vSZ) installation can be performed on the following.

- RUCKUS virtual SmartZone (includes vSZ-E and vSZ-H)
  - ESXi 6.5
  - Running on the hardware platform: (Intel(R) Xeon(R) CPU E5-2620 v4 @ 2.10GHz with AES-NI).

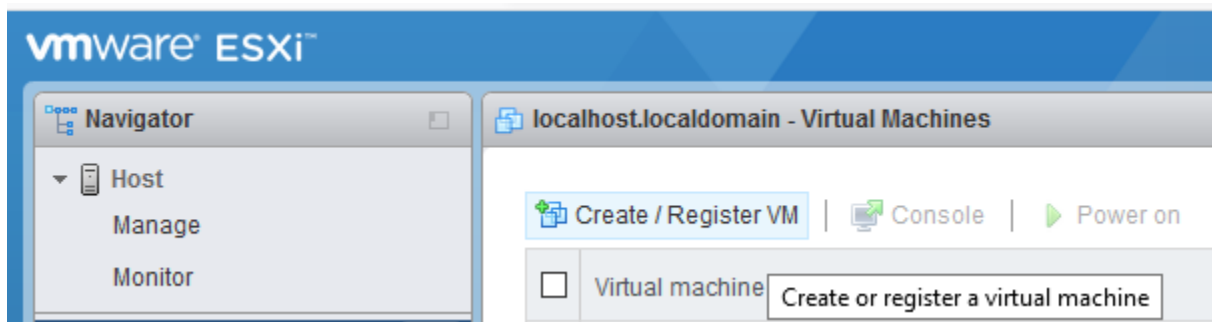
## vSZ Installation Prerequisites for FIPS

To comply with FIPS, you must have a new installation of Controller 5.1.1.3, and a corresponding AP. The system validates the image before it is loaded. The installation fails to work on a system upgraded to Controller 5.1.1.3.

## Creating and Registering the Virtual Machine

1. Install and deploy the .ova file on VMware ESXi using the **Create/Register VM** option, as shown in the following figure.

**FIGURE 3** Create and register VM

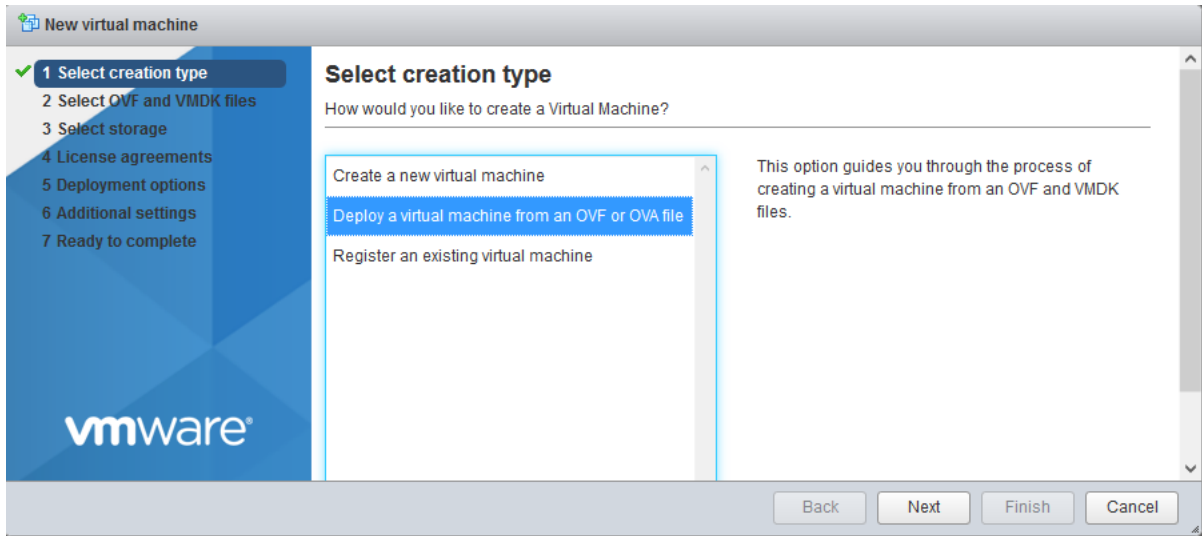


## vSZ Installation with FIPS Image

### Creating and Registering the Virtual Machine

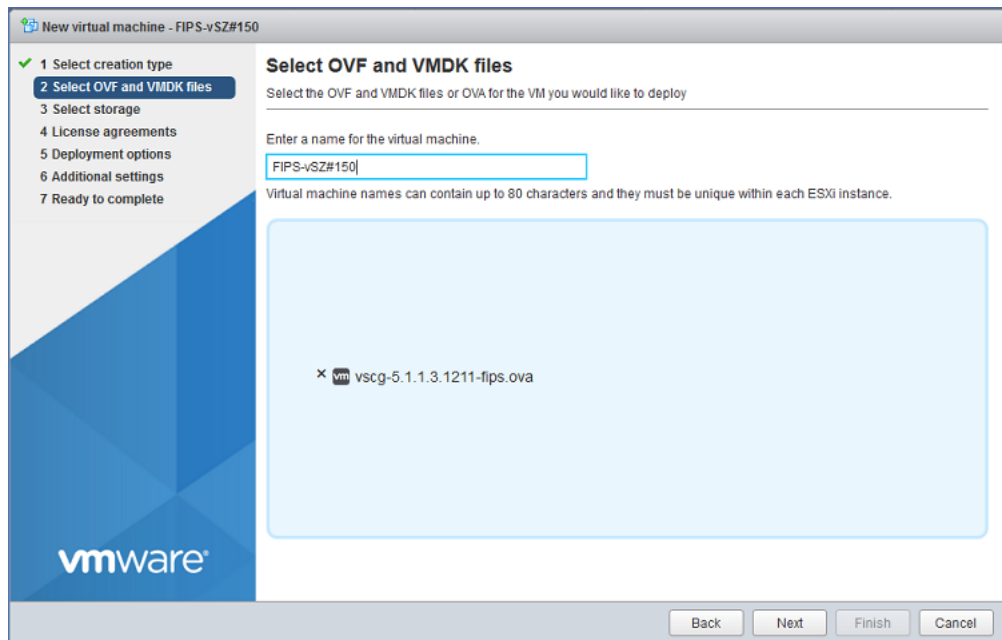
2. Select **Deploy a virtual machine from an OVF or OVA file**.

**FIGURE 4** Selecting the Creation Type



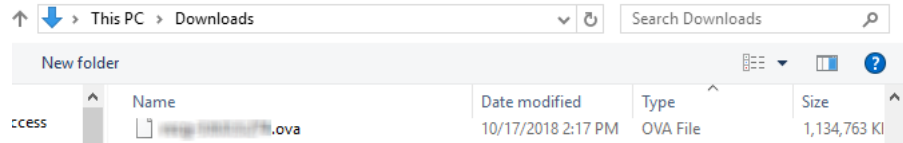
3. Click **Next** to select the OVF and VMDK files.
4. Enter the name of the VM and click the name of the OVF and VMDK file, as shown in the following figure.

**FIGURE 5** Selecting OVF and VMDK Files

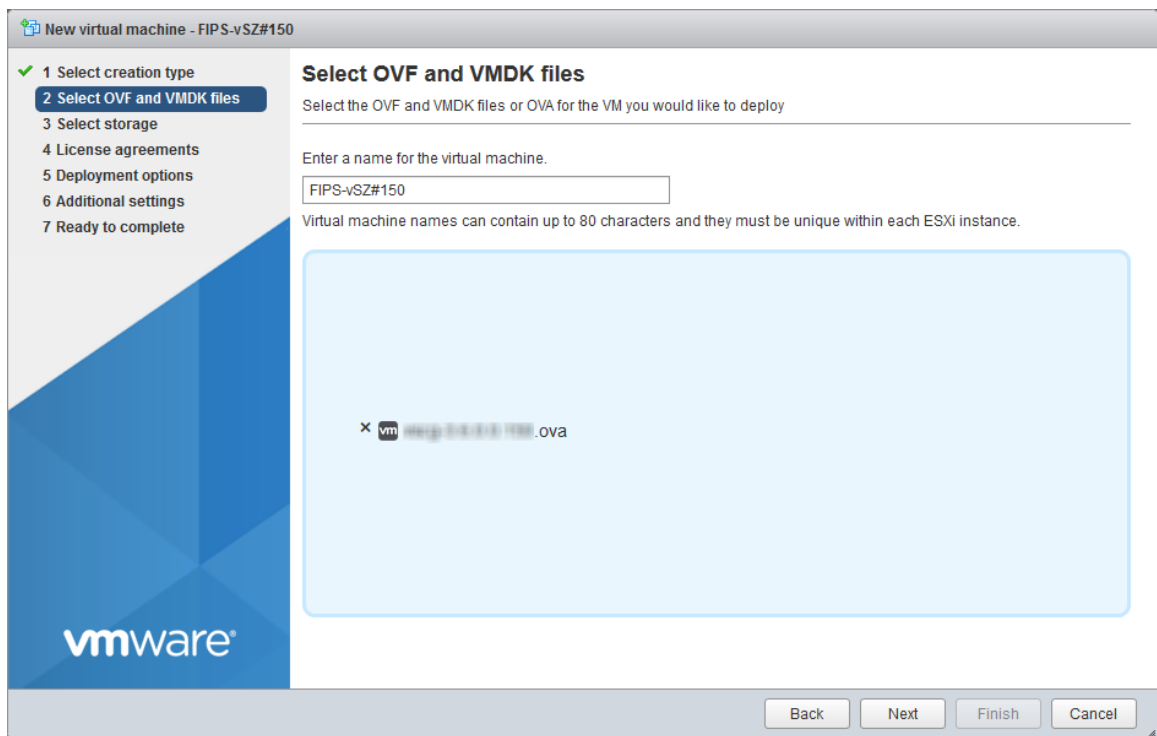


5. Select the .ova file from the browse window. The selected file is displayed in **Select OVF and VMDK files** screen

**FIGURE 6** Selecting the .ova File



**FIGURE 7** Selected .ova File

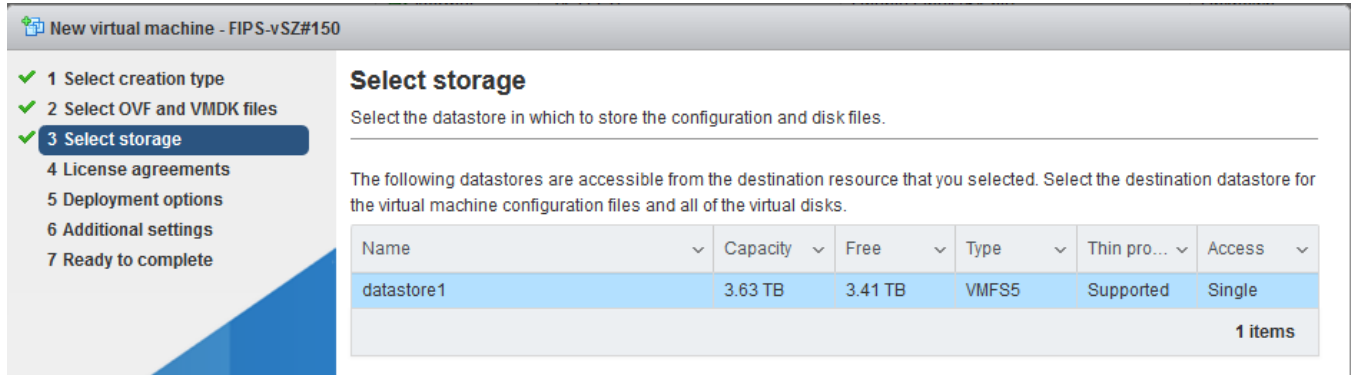


6. Click **Next** to **Select storage**.

**vSZ Installation with FIPS Image**  
Creating and Registering the Virtual Machine

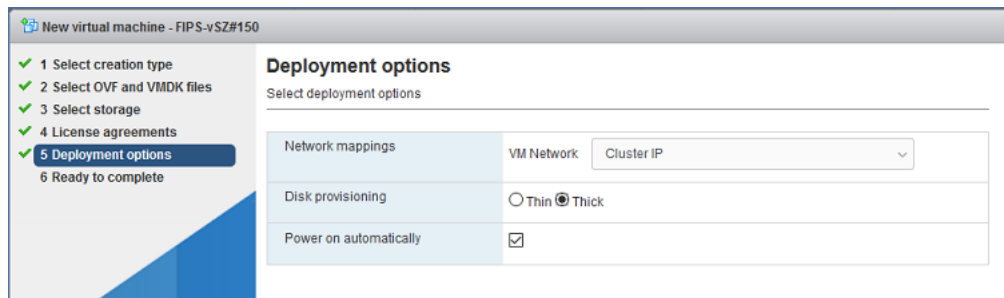
7. Select the required datastore.

**FIGURE 8** Selecting the Datastore



8. Click **Next** to select deployment options.

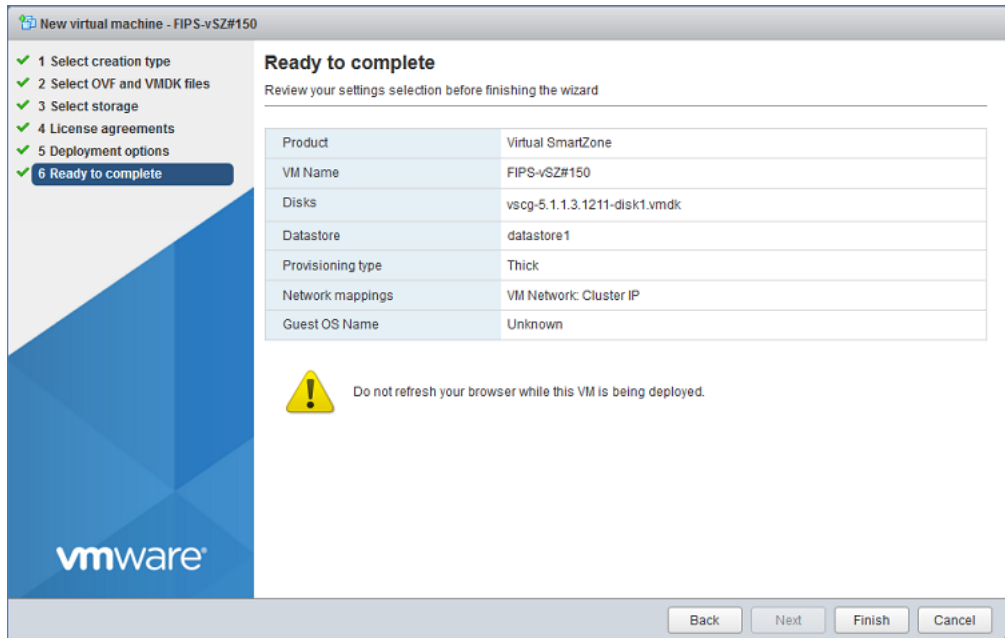
**FIGURE 9** Selecting Deployment Options





- Click **Next** to review your settings.

**FIGURE 10** Ready to complete installation



- Click **Finish** to complete the creation and registration of the virtual machine. The installation process shows the progress and displays the successfully completed tasks.

**FIGURE 11** Successful installation

Task	Target	Initiator	Result
Import VApp	Resources	root	Completed successfully
Power On VM	FIPS-vSZ#150	root	Completed successfully
Upload disk - vscg-5.1.1.3.1211-disk1.vmdk (1 of 1)	FIPS-vSZ#150	root	Completed successfully



# Hardware Configuration with FIPS Image

---

The hardware installation is performed on the following platforms..

- Smart Zone144
- Smart Zone300

**NOTE**

The installation for the hardware platforms is carried out at RUCKUS facility.



# Controller Configuration with FIPS Image

- Using FIPS-Related CLI Commands..... 25
- Viewing and Downloading FIPS Logs..... 28
- Uploading Certificates to SmartZone OS..... 30
- Enabling Other Secured Communication Services..... 33
- RadSec (RADIUS over TLS)..... 35
- Upgrading the Software..... 52

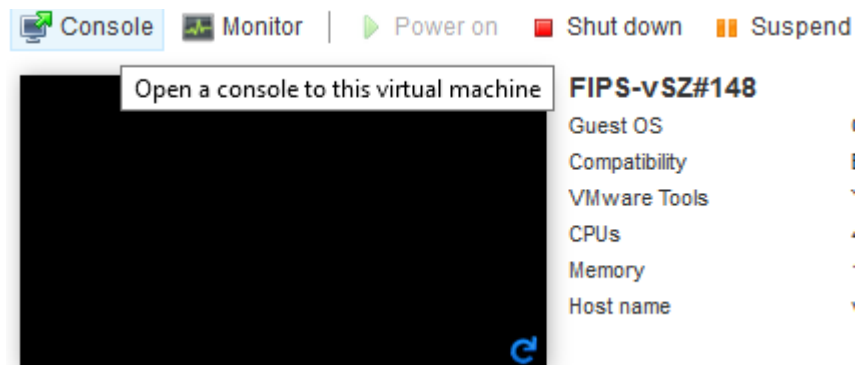
The controller configuration commands are applicable for installation of FIPS across all the controller platforms (SZ144, SZ300 and vSZ).

## Using FIPS-Related CLI Commands

These commands are applicable for installation of FIPS across all the platforms.

1. Once the VM has been deployed, click **Power On** to start the vSZ.
2. Open a console window to log in to the vSZ CLI.

**FIGURE 12** vSZ CLI Console



## Controller Configuration with FIPS Image

### Using FIPS-Related CLI Commands

3. At the login prompt, log in using "admin" as the username and password. At the > prompt, enter the **enable (en)** command and the admin password to change to Privileged EXEC mode.

From this step onwards, the installation process is the same for virtual platforms and hardware.

Use NETBOOT to load the FIPS image in the SZ144 controller hardware.

Use NETBOOT/USB boot to load the FIPS image in the SZ300 controller hardware.

**FIGURE 13** Logging In to Privileged EXEC Mode (vSZ-E)

```
#####
#      Welcome to vSZ      #
#####
admin@10.1.200.13's password:
Last login: Fri Nov 23 13:56:14 2018 from 105.0.0.254
Please wait. CLI initializing...

Welcome to the Ruckus Virtual SmartZone - Essentials Command Line Interface
Version: 3.6.0.3.200

N13> en
Password: *****

N13# █
```

**FIGURE 14** Logging In to Privileged EXEC Mode(SZ300)

```
Connection established.
To escape to local shell, press 'Ctrl+Alt+J'.
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 Dec 7 05:27:33 2018 from 10.137.24.32
Please wait. CLI initializing...

Welcome to the Ruckus SmartZone 300 Command Line Interface
Version: 3.6.0.3.200

FIPS-12> en
Password: *****

FIPS-12# █
```

FIGURE 15 Logging In to Privileged EXEC Mode (SZ144)

```
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 Dec 7 05:27:33 2018 from 10.137.24.32
Please wait. CLI initializing...

Welcome to the Ruckus SmartZone 100 Command Line Interface
Version: 3.4.4.3.200

FIPS-12> en
Password: *****

FIPS-12# █
```

- At the command prompt, enter **fips ?** to display the list of available FIPS commands.

FIGURE 16 List of FIPS Commands

```
vSZ-142# fips
  disable      Disable system FIPS compliance
  enable       Enable system FIPS compliance
  showlog      Show Bootup Selftest Log
  status       Status of system FIPS compliance

vSZ-142# fips _
```

- Enter **fips status** to verify whether FIPS mode is enabled or disabled.

FIGURE 17 Using the fips status Command

```
vSZ-142# fips status
FIPS compliance is Enable
```

**NOTE**

When FIPS mode is enabled or disabled, vSZ is initiated with set-factory to clean up the configuration.

- Enter **fips disable** to disable FIPS mode, and enter **yes** to confirm.

FIGURE 18 Using the fips disable Command

```
vSZ-142# fips disable
Zeroization will be initiated using set factory and the FIPS mode will be set to
Disable (or input 'no' to cancel)? [yes/no] _
```

7. Enter **fips enable** to enable FIPS mode, and enter **yes** to confirm.

FIGURE 19 Using the fips enable Command

```
SmartZone-142# fips enable
Zeroization will be initiated using set factory and the FIPS mode will be set to
Enable (or input 'no' to cancel)? [yes/no] _
```

8. Enter **fips showlog** to display the results of an on-demand test of FIPS crypto modules.

FIGURE 20 Using the fips showlog Command

```
Node1# fips showlog
=====OpenSSL selftest=====
DRBG: PASSED
X931: PASSED
SHA1: PASSED
SHA2: PASSED
HMAC: PASSED
CMAC: PASSED
AES : PASSED
AES-CCM : PASSED
AES-GCM : PASSED
AES-XTS : PASSED
DES : PASSED
RSA : PASSED
ECDSA : PASSED
DSA : PASSED
DH : PASSED
ECDH : PASSED
ECP384 : PASSED
Node1# █
```

**NOTE**

For more information on installation refer *SmartZone Getting Started Guide* and *SmartZone Quick Setup Guide* on support portal.

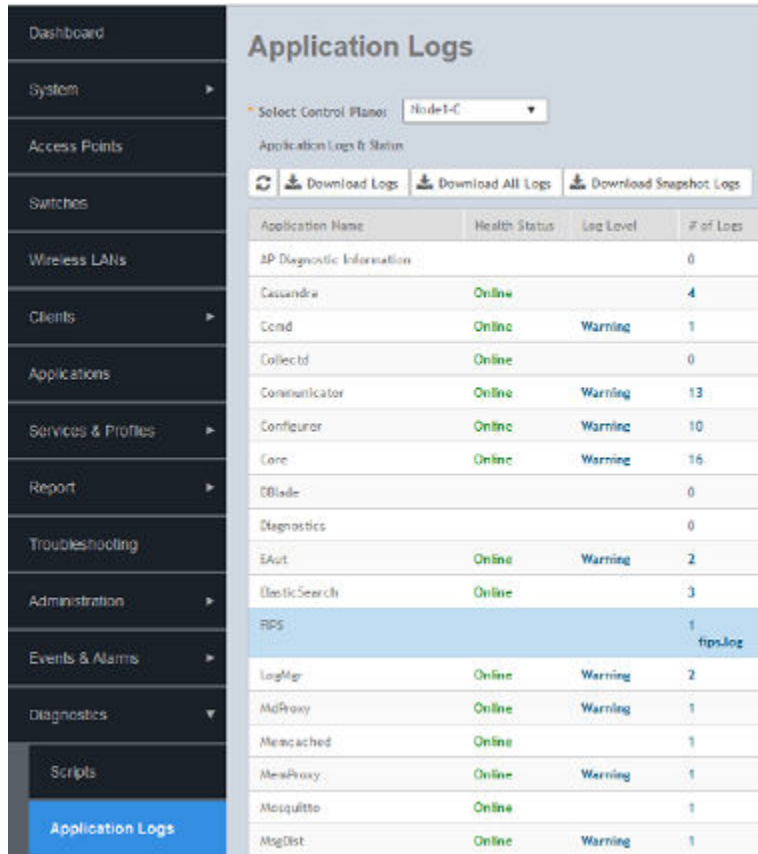
## Viewing and Downloading FIPS Logs

Only the CO (admin) can view and download FIPS logs from the web interface.



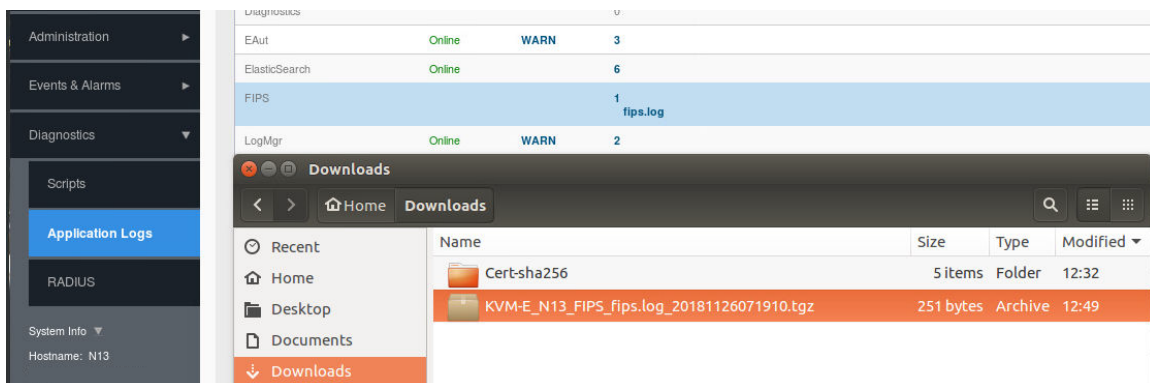
In the web interface, navigate to **Diagnostics > Application Logs > FIPS** to download the logs to the local machine.

**FIGURE 21** Using the Web Interface to Download FIPS Logs



The downloaded log file is compressed as a .zip file.

**FIGURE 22** Downloaded FIPS Logs



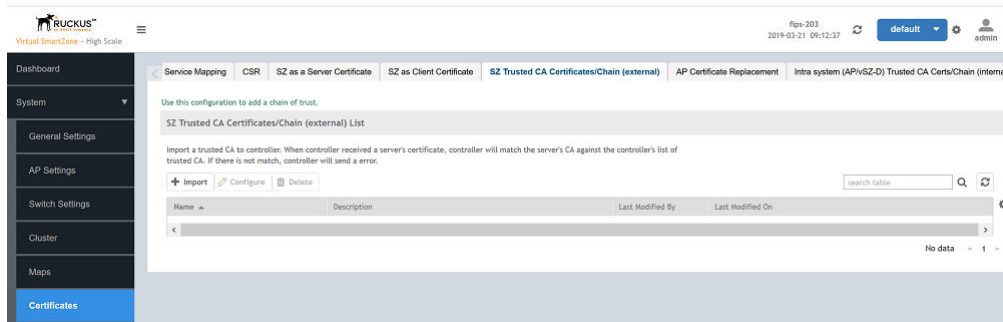
# Uploading Certificates to SmartZone OS

For Active Directory (AD), Lightweight Directory Access Protocol (LDAP), and RADIUS over TLS (RadSec), the root CA is imported to the local machine so that the certificate from the server can be validated against the trusted CA.

Perform the following steps to import the certificate.

1. In the web interface, navigate to **System > Certificates > SZ Trusted CA Certificates/Chain (external)**.

**FIGURE 23** Selecting the Import Option



2. Click the **Import** option.

3. Enter the name in the **Name** field, and click the **Browse** button to the right of the **Root CA Certificate** field to navigate to the appropriate file.

FIGURE 24 Name and Description of the Certificate

## Import CA Certs (Chain)

The screenshot shows a web form titled "Import CA Certs (Chain)". It contains the following fields and controls:

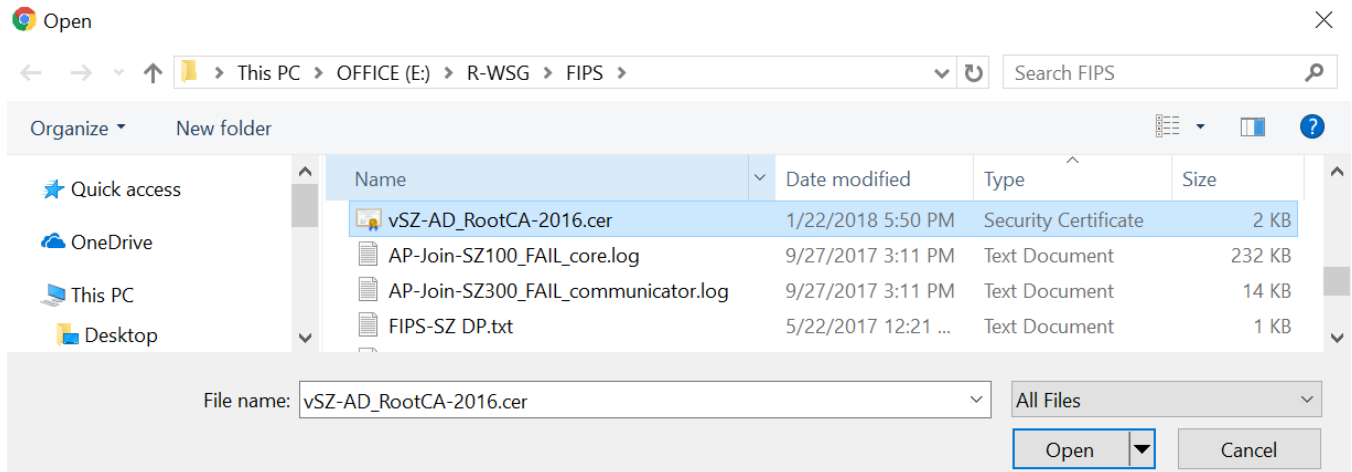
- Name:** A text input field with an asterisk (\*) indicating it is required.
- Description:** A text input field.
- Intermediate CA Certificates:** A section with the label "Intermediate CA Certificates:" followed by four rows. Each row consists of a checkbox, a text input field, a "Browse" button, and a "Clear" button.
- Root CA Certificate:** A section with the label "\* Root CA Certificate:" followed by a checkbox, a text input field, a "Browse" button, and a "Clear" button.

4. Select the root CA file from the local machine, and click **Open**.

**NOTE**

Only CER and PEM formats are supported for the CA certificates.

**FIGURE 25** Selecting the Certificate



A check mark is displayed next to the file name upon successful import of the certificate.

**FIGURE 26** Successful Certificate Import

## Import CA Certs (Chain)

The screenshot shows the "Import CA Certs (Chain)" configuration window. The "Name" field is set to "RadSec\_subCA-chain#1". The "Description" field is empty. Under "Intermediate CA Certificates", the first entry "ca-chain.cert.pem" is checked, with "Browse" and "Clear" buttons. Below it are three more empty entries, each with "Browse" and "Clear" buttons. Under "Root CA Certificate", the entry "ca.cert.pem" is checked, with "Browse" and "Clear" buttons.

# Enabling Other Secured Communication Services

The following secured communication services are available in FIPS:

- SFTP
- SNMP
- SMTP
- Syslog

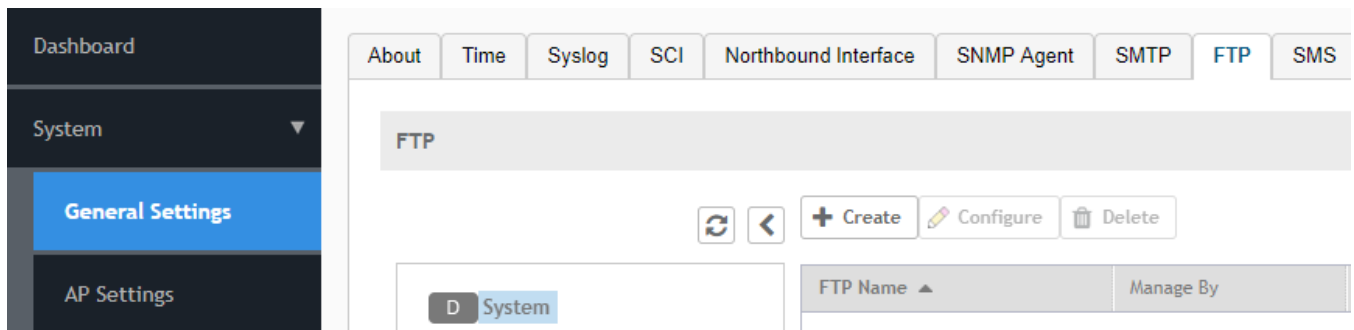
### NOTE

The secured communication service Syslog is a part of Common Criteria (CC) evaluation whereas the SFTP, SNMP, and SMTP services are not been evaluated as part of CC evaluation.

Perform the following steps to activate these services.

1. To enable SFTP, from the web interface, navigate to **System > General Settings > FTP**.

**FIGURE 27** Selecting FTP

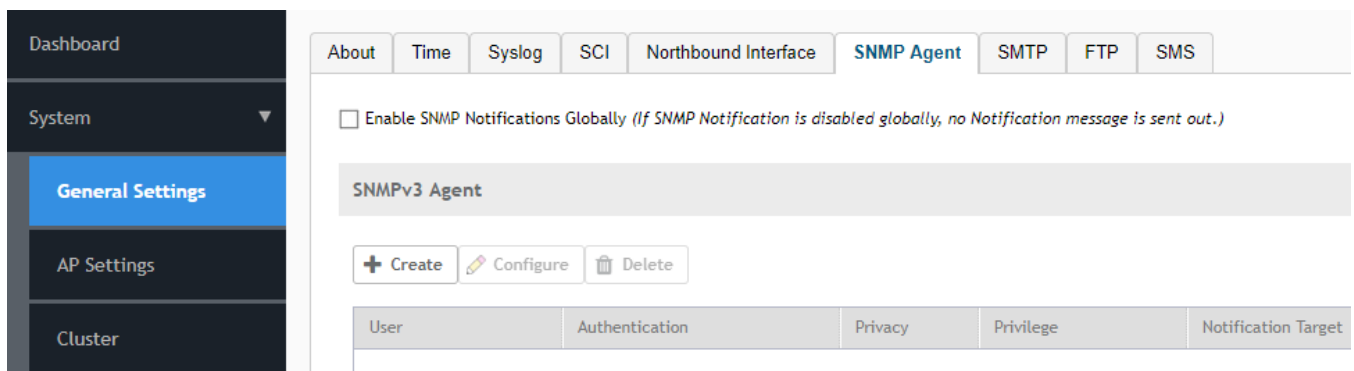


2. Select the required FTP or click **Create** to add a new FTP.
3. To enable the SNMP agent, in the web interface, navigate to **System > General Settings > SNMP Agent**. Enable the option for SNMP notifications.

### NOTE

The SNMPv3 Agent is valid for FIPS. The HASH algorithm is not user-configurable.

**FIGURE 28** Selecting the SNMP Agent



**Controller Configuration with FIPS Image**  
Enabling Other Secured Communication Services

4. To enable SMTP, in the web interface, navigate to **System > General Settings > SMTP**. Configure the SMTP server settings to enable email notifications.

**FIGURE 29** Selecting the SMTP Server

Dashboard

System

General Settings

AP Settings

Cluster

Maps

Certificates

Templates

About Time Syslog SCI Northbound Interface SNMP Agent **SMTP** FTP SMS

Configure the SMTP server settings. The system uses these SMTP server settings to send email notifications.

Enable SMTP Server

Logon Name:

Password:

\* SMTP Server Host:

\* SMTP Server Port:

\* Mail From:

From Display Name: Ruckus Support

\* Mail To:

Encryption Options:  TLS

Refresh OK Cancel Test

- To enable syslog, in the web interface, navigate to **System > General Settings > Syslog**.

**FIGURE 30** Selecting the Syslog Server

Configure the remote syslog server to which event logs will be sent. You can also configure the types of events to send, syslog facility, and event severity to log level mapping.

Enable logging to remote syslog server

\* Primary Syslog Server Address:  \* Port:  \* Protocol:

Secondary Syslog Server Address:  \* Port:  \* Protocol:

\* Application Logs Facility:  \* Filter Severity:

\* Administrator Activity Logs Facility:  \* Filter Severity:

\* Other Logs Filter Severity:

\* Event Facility:

\* Event Filter:  All events  
 All events except client association/disassociation events  
 All events above a severity

Priority:	Event Severity	=>	Syslog Priority
	Critical	=>	Error
	Major	=>	Error
	Minor	=>	Warning
	Warning	=>	Warning
	Informational	=>	Info
	Debug	=>	Debug

- Select **Enable logging to remote syslog server** to send event logs.

**NOTE**

Apart from the event logs, the controller also stores the audit logs on the local server, and sends them to the syslog servers. For AP and vSZ-D, the audit logs are not stored on the local server, they are buffered and sent to the controller in real-time. This buffer occurs in RAM. In the event buffer is full all new audits are discarded although there is an age out mechanism to prevent this from happening. Any audits in the buffer that cannot be sent to the controller within 30 minutes are deleted from the buffer. After the audits are sent the controller forwards them to the configured syslog server. The controller performs log rotation on both the file system and database. It stores system log files of the file system and the database. The permitted log files size is 100 MB and 14 archives of such application logs are allowed.

**NOTE**

The external syslog port number must be 514. When an external syslog server is configured, all the audit data or events are sent to the external syslog server simultaneously. The controller uses log rotation to overwrite the oldest audit records to prevent local storage space from becoming full.

## RadSec (RADIUS over TLS)

The latest RADIUS versions support the TLS interface and can be used in the SmartZone controller to support a TLS connection with the AAA server as a RadSec proxy.

## Controller Configuration with FIPS Image

### RadSec (RADIUS over TLS)

The RadSec proxy establishes the TLS connection with the RadSec AAA server using TLS over TCP. In the web interface, if TLS is enabled in the authentication or accounting service, RAC sends RADIUS messages to the RadSec proxy, and the RadSec proxy forwards the RADIUS messages over TLS to the configured RadSec server.

The connection between controller and RadSec Server lasts for a maximum of 30 seconds. As soon the controller receives a new Authentication Requests, it initiates a TLS handshake towards RadSec. If Network is down or RadSec server (process) itself is down, then UE authentications FAIL.

#### NOTE

If the connection between controller and RadSec is broken, by default the connection is resumed when the next message is received from the client. If the connection is not reestablished, the administrator should check if the network is down or RadSec server is down as noted above.

#### NOTE

TLS cipher suites are not user-configurable. The following cipher suites are supported by controller (RadSec client):

- ECDHE-RSA-AES128-SHA256
- ECDHE-RSA-AES256-GCM-SHA384
- ECDHE-RSA-AES256-SHA384
- ECDHE-RSA-AES128-GCM-SHA256
- DHE-RSA-AES128-SHA256
- DHE-RSA-AES256-SHA256

In FIPS mode, client authentication and accounting messages are exchanged through a TLS tunnel that is established between vSZ and the AAA server. This ensures that the user name, password, pass phrase, or any other sensitive information pertaining to the user or user session is encrypted.

## Configuring RadSec

Perform the following steps to configure and map RadSec in standard and WISPr WLANs.

1. Log in to the web interface using the URL <https://MGMT-interface-IP:8443>



2. To configure RadSec authentication service, navigate to **Services & Profiles > Authentication > Proxy (SZ Authenticator) > Configure**. The **Edit Authentication Service** page is displayed

FIGURE 31 Configuring RadSec Authentication Service

## Edit Authentication Service RadSec\_197

\* Name:

Friendly Name:

Description:

\* Service Protocol:  RADIUS  Active Directory  LDAP

RADIUS Service Options

Encryption:  ON  TLS

\* CN/SAN Identity:

OCSF Validation:  ON \* OCSF URL:

Client Certificate:

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

Primary Server

\* IP Address:

\* Port:

\* Shared Secret:

\* Confirm Secret:

Configure the following.

- a) **Name:** Enter the authentication service name.
- b) **Service Protocol:** Select the **RADIUS** option.

### NOTE

The connection between controller and RadSec Server lasts for maximum of 30 seconds. As soon the controller receives a new Authentication Requests, it initiates a TLS handshake towards RadSec. If Network is down or RadSec server (process) itself is down then UE authentications FAILS.

- c) In the RADIUS Service Options section, for the field **Encryption**, click **ON** to enable TLS encryption

**NOTE**

If **TLS** is enabled:

- Secondary server configuration is disabled.
- Only then the user can configure **OCSP Validation** and **CN/SAN Identity**.
- **OCSP Validation** is disabled by default.
- **CN/SAN** becomes a mandatory field. The validation is performed with the configured identity and is used by most of the certificates.

Refer to the following table to use the appropriate CN/SAN combination for a successful TLS connection.

**TABLE 3** Showing Appropriate Combination for TLS Connection

CN	SAN	Result
mismatch	mismatch	FAIL
match	mismatch	FAIL
empty	empty	FAIL
empty	mismatch	FAIL
empty	match	PASS
match	empty	PASS
mismatch	match	PASS
match	match	PASS

3. Enter **CA/SAN Identity**.

For CN/SAN Identity, enter an address (for example, bdc.commscope.com). The maximum length is 1024 characters.

When TLS encryption is enabled, CN/SAN Identity becomes a mandatory field. The validation is performed with the configured identity and is used by most of the certificates.

Refer to the following table to use the correct pattern for a successful TLS connection.

**TABLE 4** Showing Correct Pattern for TLS Connection

Wildcard (*.commscope.com) in the SAN of RadSec server certificate	Example	Result
Asterisk (*) is used other than at the beginning of the URL	bdc.*.commscope.com	FAIL
If configured as	bdc.commscope.com	PASS
If configured as	commscope.com	FAIL
If configured as	BRL.bdc.commscope.com	FAIL

4. For **OCSP Validation**, click **ON** to enable OCSP URL.

**NOTE**

If OCSP validation is enabled, SZ performs the validation; otherwise, the TLS connection is established without the OCSP validation.

5. Enter **OCSP URL** (for example, https://10.1.200.197:2561) Maximum length is 1024 characters.

When OCSP validation is enabled, OCSP URL becomes a mandatory field. If the server certificate contains OCSP attributes, RAC uses certificate-provided attributes for validation; otherwise, RAC uses the configured OCSP URL for validation.

6. For **Client Certificate**, select the certificate from the list.

For OSCP URL, enter a URL (for example, <https://10.1.200.197:2561>). The maximum length is 1024 characters.

The user can import the client certificate when SZ acts as a RadSec client. As a prerequisite to enabling the client certificate, complete the following steps:

- a) Navigate to **System > Certificates > SZ as Client Certificate** and click **Import**.
  - b) In the **Import Client Certificate** page, enter the certificate name.
  - c) For **Client Certification**, browse and select the certificate.
  - d) Click **Validate**. A validation message is displayed.
  - e) Click **OK** to complete the certificate validation.
7. Under **Primary Server**, enter the IP address and port number.

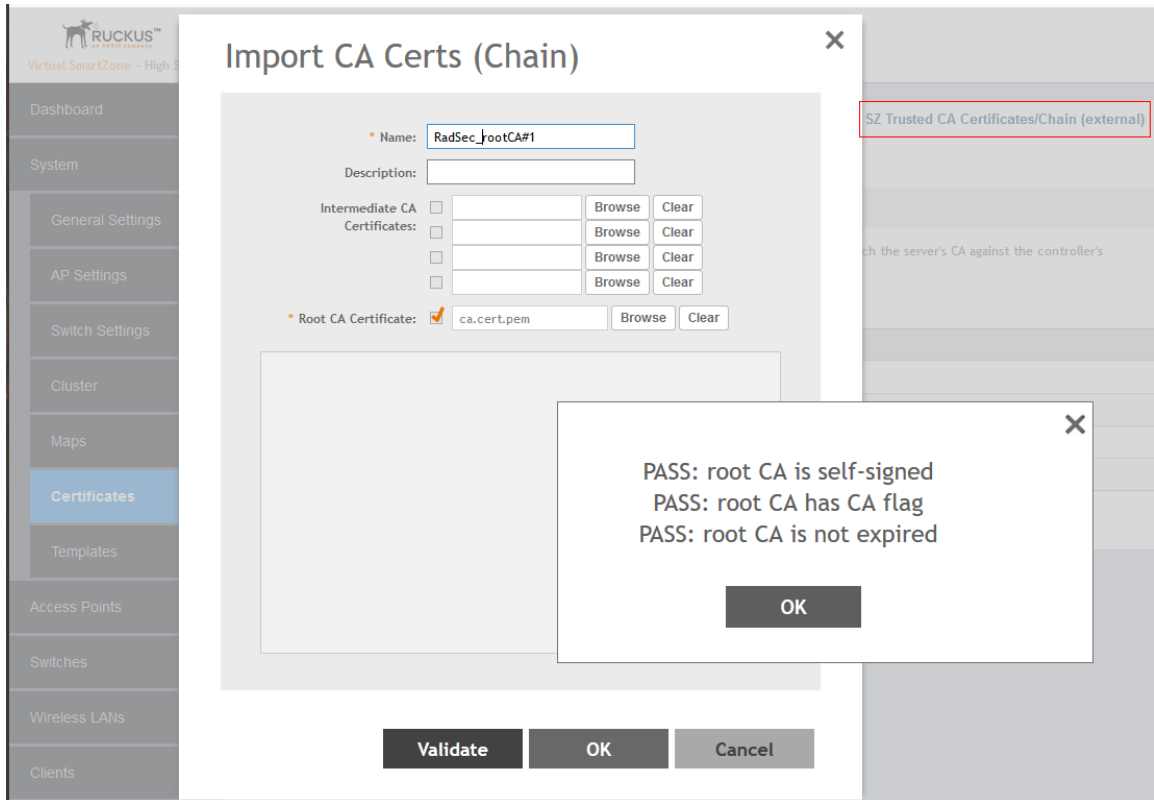
**NOTE**

You can use port number 2083, but ensure that the configured port is the same as that in the RadSec server.

8. Click **Save** to add the RadSec authentication service.

- To import the CA certificate for validation, navigate to **System > Certificates > Import CA Certs**.  
The **Import CA Certs (Chain)** page is displayed.

**FIGURE 32** Importing the CA Certificate



- Enter the CA certificate name.
- For **Root CA Certificate**, browse and select the certificate.

**NOTE**

RadSec supports only the Root CA certificate. Only the base64 certificate format is supported.

- Click **Validate**. A validation message is displayed.
- Click **OK** to complete the certificate validation.

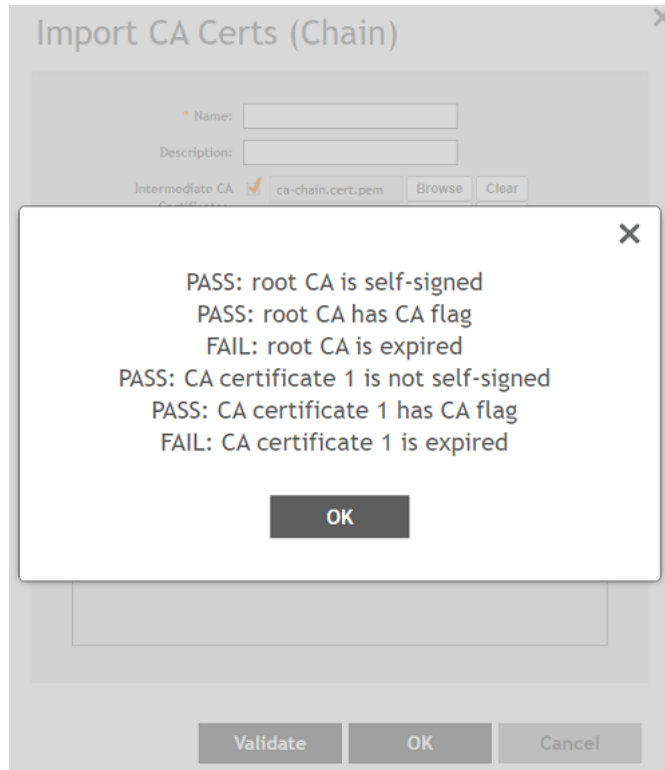
**NOTE**

The RadSec server certificate must contain the Server Authentication purpose in the **extendedKeyUsage** field for its successful validation.

**NOTE**

If the imported CA-Chain certificates are expired, invalid or corrupted then the GUI throws an error, the GUI still allows the user to upload the certificate, but after uploading the TLS/IPSec tunnel formation fails to get established.

FIGURE 33 Unable to Establish TLS/IPSec Tunnel



10. To configure a client certificate when SZ acts as a RadSec client, navigate to **System > Certificates > SZ as Client Certificate > Configure**.  
The **Edit Client Certificate** page is displayed.

**FIGURE 34** Configuring the Client Certificate

**Edit Client Certificate: clientcert**

Name:

Description:

Client Certificate

```
-----BEGIN CERTIFICATE-----
{
  Version: Y3
  Subject: EMAILADDRESS=radsecClient@commscope.com, CN=radsecClient.com,
  OU=QA, O=Commscope Ltd, ST=Bagalkot, C=IN
  Signature Algorithm: SHA256withRSA, OID = 1.2.840.113549.1.1.11

  Key: Sun RSA public key, 2048 bits
  modulus:
29688164683796986241515936074564691628864620188585989002299767140370846988
26638332793469582405289337620149806937469779525876683764905622192393261092
06414723534710242903535954575092588749528110351296755111911370231225850409
4701592383242172313501523680813499021431512337347101890884567277549980715
99955751652541522649550377121780713317392703498752332484428227897814931284
332949190668257660467235843079389548116869029774547659160763976356289835
1188483953457088988535133939662329501186151161520323197699121873844367073
86528844576138533743644315085090368545219630730591667639078695943562706257
0452250909455466533383337
}
```

Client Certificate:

Private Key:

- Enter the client certificate name.
- For **Client Certificate**, browse and select the certificate.
- For **Private Key**, browse and select the key.
- Click **Validate**. A validation message is displayed.
- Click **OK** to complete the certificate validation.

11. To configure a RadSec accounting service, navigate to **Services & Profiles > Accounting > Proxy (SZ Authenticator) > Configure**.

FIGURE 35 Configuring RadSec Accounting Service

## Edit Accounting Service: radsec\_10.1.200.197

\* Name:

Description:

Service Protocol:  RADIUS Accounting

RADIUS Service Options

Encryption:  ON TLS

\* CN/SAN Identity:

OCSP Validation:  ON \* OSCP URL:

Client Certificate:  ▼

Reload...

Disable

client\_cert

Primary Server

\* IP Address:

\* Port:

\* Shared Secret:

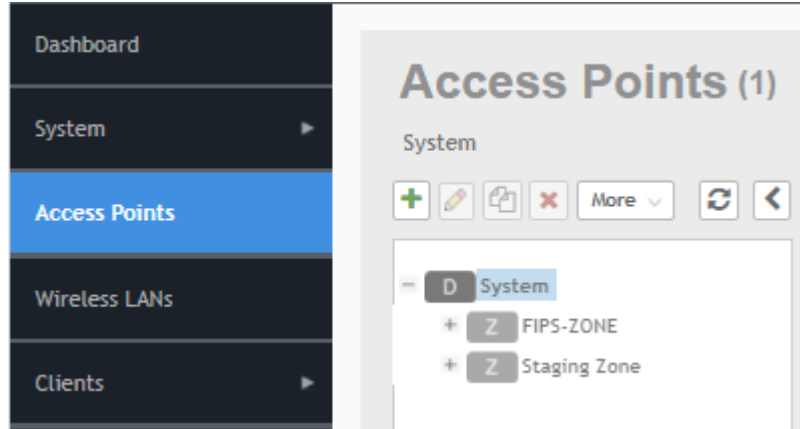
\* Confirm Secret:

12. On the **Edit Accounting Service** page, configure the following items:
  - Enter the accounting service name.
  - For **Service Protocol**, select **RADIUS Accounting**.
  - For **Encryption**, click **ON** to enable TLS Encryption. Repeat steps from 5 through 10.
13. Click **Save** to add the RadSec accounting service.

**Controller Configuration with FIPS Image**  
RadSec (RADIUS over TLS)

14. After creating RadSec authentication and accounting services, you must create a zone. In the web interface, navigate to **Access Points** and select **System** as the domain.

**FIGURE 36** Selecting System as the Domain





15. Click the plus (+) sign to create the AP group and configure the following fields on the **Create Group** page.

- Enter the AP group name.
- For **Type**, select **Zone**.
- Select **AP Firmware**.
- For **AP Admin Logon**, enter the username and password.

**FIGURE 37** Configuring an AP Group

The screenshot shows the 'Configure Group' web interface. At the top, there is a 'Name' field with the value 'FIPS-Zone' and a 'Description' field. Below this, the 'Type' is set to 'Zone' (selected with a radio button), and the 'Parent Group' is 'System'. A 'Configuration' tab is active, showing 'General Options'. The 'AP Firmware' is '5.1.1.3.1023'. The 'Country Code' is 'United States', with a note: '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.' The 'Location' is 'Ruckus HQ' and 'Location Additional Information' is '350 W Java Dr, Sunnyvale, CA, USA'. 'GPS Coordinates' includes fields for Latitude, Longitude, and Altitude (set to 'meters'). 'AP Admin Logon' has 'Logon ID' as 'mahan' and a masked password. 'AP Time Zone' is 'System defined' and '(GMT+0:00) GMT'. 'AP IP Mode' is 'IPv4 only'. 'Historical Connection Failures' is 'OFF'. 'DP Zone Affinity Profile' is 'Disable'. 'OK' and 'Cancel' buttons are at the bottom right.

16. Click **OK** to save the AP group.

**NOTE**

The WLAN authentication type for FIPS is either **Standard Usage with Authentication** or **Hotspot (WISPr)**.

17. Create a WLAN. In the web interface, navigate to **Wireless WLANs**. Click **Create**.

18. On the **Create WLAN Configuration** screen, configure the following items.

- Enter the WLAN name.
- Enter the SSID.

**NOTE**

If PSK is used, select **64 HEX PSK/PMK**.

- For **Zone**, select the zone created for FIPS.
- For **WLAN Group**, select **default**.
- For **Authentication Type**, select **Standard usage (for most regular wireless networks)**
- For **Method**, select **Open**.

**NOTE**

Other supported methods include **802.1X-EAP** and **802.1X-EAP & MAC**. For **802.1X-EAP** and **802.1X-EAP & MAC** authentication, the user must map the authentication and accounting services and the WLAN must reflect such a configuration.

- Click **OK** to save the configuration.

**FIGURE 38** Creating a WLAN with Open Method

The screenshot shows the 'Create WLAN Configuration' web interface. It features several input fields and sections:

- Name:** A text input field.
- SSID:** A text input field.
- Description:** A text input field.
- Zone:** A dropdown menu with 'FIPS-Zone' selected.
- WLAN Groups:** A dropdown menu with 'default' selected, and a '+ Create' button.
- Authentication Options:**
  - Authentication Type:** Radio buttons for 'Standard usage (for most regular wireless networks)' (selected), 'Hotspot (WSP)' (disabled), 'Hotspot 2.0 Access', and 'Hotspot 2.0 Onboarding'.
  - Method:** Radio buttons for 'Open' (selected), '802.1X EAP', and '802.1X EAP & MAC'.
- Encryption Options:**
  - Method:** Radio buttons for 'WPA2' (selected) and 'WPA3'.
  - Algorithm:** Radio buttons for 'AES' (selected) and 'TKIP'.
  - Passphrases:** A text input field with a 'Show' checkbox.

As an alternative, you can create a WLAN using the **802.1X EAP & MAC** method, as shown in the following figure.

FIGURE 39 Creating a WLAN with 802.1X EAP & MAC Method

The screenshot displays the 'Create WLAN Configuration' web interface. At the top, the 'Zones' dropdown is set to 'FIPS-Zone' and the 'WLAN Group' is 'default'. The 'Authentication Options' section includes: 'Authentication Type' with 'Standard usage (For most regular wireless networks)' selected; 'Method' with '802.1X EAP & MAC' selected; and 'MAC Authentication' with 'Use user-defined text as authentication password' checked. The 'MAC Address Format' dropdown is open, showing options: 'aabbccddeeff', 'AA-BB-CC-DD-EE-FF', 'AA BB CC DD EE FF', and 'AABBCCDDEEFF'. The 'Encryption Options' section includes: 'Method' with 'aabbccddeeff' selected; 'Algorithm' with 'aa-bb-cc-dd-ee-ff' selected; '802.11r Fast Roaming' with 'Enable 802.11r Fast BSS Transition' checked; and '802.11w WFP' with 'Disabled' selected.

19. The WLAN can be configured with the **Hotspot (WISPr)** authentication type. On the **Create WLAN Configuration** screen, configure the following items:
- Enter the WLAN name.
  - Enter the SSID.
  - For **Zone**, select the zone created for FIPS.
  - For **WLAN Group**, select **default**.
  - For **Authentication Type**, select **Hotspot (WISPr)**.
  - For **Method**, select **802.1X EAP**.
  - Click **OK** to save the configuration.

FIGURE 40 Creating a WLAN with Hotspot WISPr in 802.1X EAP Method

The screenshot shows the 'Create WLAN Configuration' interface. The 'Name' field is empty. The 'SSID' field is empty. The 'Description' field is empty. The 'Zone' dropdown menu is set to 'FIPPS-Zone'. The 'WLAN Group' dropdown menu is set to 'default'. The 'Authentication Options' section has 'Authentication Type' set to 'Hotspot (WISPr)' and 'Method' set to '802.1X EAP'. The 'Encryption Options' section has 'Method' set to 'WPA2' and 'Algorithm' set to 'AES'. There are checkboxes for '802.11r Fast Roaming' and 'Enable 802.11r Fast BSS Transition' at the bottom.

As an alternative, you can create a WLAN with **Hotspot WISPr** in the **Open** method, as shown in the following figure.

FIGURE 41 Creating a WLAN with Hotspot WISPr in Open Method

The screenshot shows the 'Create WLAN Configuration' interface. The 'Name' field is empty. The 'SSID' field is empty. The 'Description' field is empty. The 'Zone' dropdown menu is set to 'FIPPS-Zone'. The 'WLAN Group' dropdown menu is set to 'default'. The 'Authentication Options' section has 'Authentication Type' set to 'Hotspot (WISPr)' and 'Method' set to 'Open'. The 'Encryption Options' section has 'Method' set to 'WPA2' and 'Algorithm' set to 'AES'. There is a 'Passphrases' field and a 'Show' checkbox at the bottom.

## Mapping the Authentication Profile for the WLAN

1. When mapping the authentication profile for a WLAN configuration using Hotspot WISPr, be sure to map to the WISPr portal page. Confirm the Hotspot Portal settings. Click **OK** to save the mapping.

### NOTE

To map the authentication profile for a WLAN using a standard usage call, you need realm-based proxy profiles for authentication and accounting as described in the remaining steps of this procedure.

**FIGURE 42** Mapping to the Hotspot Portal

**Hotspot Portal**

\* Hotspot (WISPr) Portal:

Bypass CNA:  Enable

\* [?] Authentication Service:  Use the controller as proxy  Use Realm-based profile

Enable RFC 5580 Location Delivery Support

Accounting Service:  Use the controller as proxy  Use Realm-based profile

Send interim update every  Minutes (0-1440)

2. To map to a standard usage call WLAN profile, navigate to **Services & Profiles > Authentication > Realm Based Proxy** on the web interface.

The RadSec authentication profile is displayed.

**FIGURE 43** Configuring Realm-based Authentication Service

\* Name:

Description:

Enable Hosted AAA Support  Configure PLMN identifier

**Realm Based Authentication Service**

Realm	Protocol	Auth Service	Auth Method	Dynamic VLAN ID
No Match	RADIUS	RadSec Auth Service	NonGPPCallFlow	N/A
Unspecified	RADIUS	RadSec Auth Service	NonGPPCallFlow	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. Under **Realm**, click **No Match**.

4. Click **Configure**, and configure the following items:
  - For **Service**, select **RadSec Auth Service**.
  - For **Auth Method**, select **No data available**.
  - For **Dynamic VLAN ID**, select **Non-3GPP Call Flow**.
  - Click **OK** to save the configuration.

FIGURE 44 Editing Realm-based Authentication Service

## Edit Realm Based Authentication Service: No Match

Realms: No Match

Service: [RADIUS] RadSec Auth Serv + Create

Auth Method: No data available

Dynamic VLAN ID: Non-3GPP Call Flow

OK Cancel

5. Similarly, set the configuration for Unspecified.
6. To create a realm-based proxy for accounting to map to a standard usage call WLAN profile, navigate to **Services & Profiles > Accounting > Realm Based Proxy** on the web interface. The RadSec accounting profile is created and displayed.

FIGURE 45 Configuring Realm-based Accounting Service

Name: RadSec Acct Profile

Description:

Realm Based Accounting Service

+ Create Configure Delete

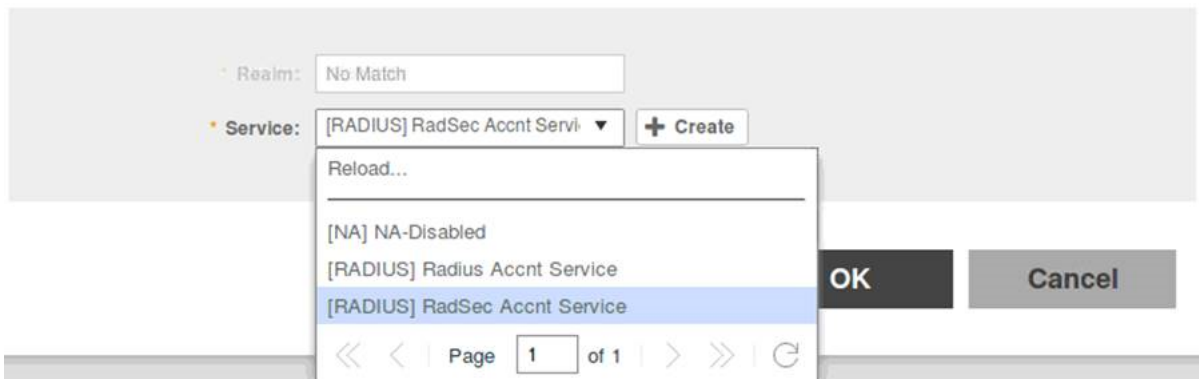
Realm	Protocol	Accounting Service
No Match	RADIUS	RadSec Account Service
Unspecified	RADIUS	RadSec Account Service

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.

7. Under **Realm**, click **No Match**.

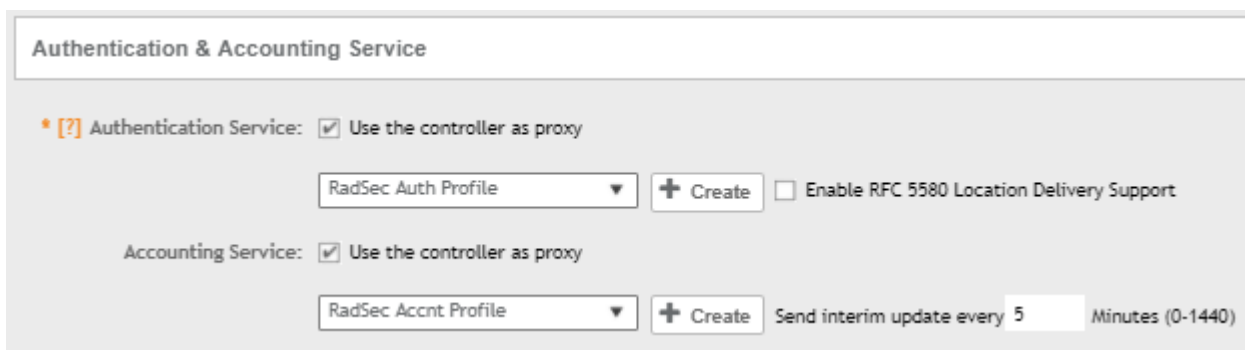
- Click **Configure**, and configure the following items:
  - For **Service**, select **RadSec Acctn Service**.
  - Click **OK** to save the configuration.

## Edit Realm Based Accounting Service: No Match



- Map the authentication and accounting profile to the WLAN as shown in the following figure.

**FIGURE 46** Mapping to Authentication & Accounting Service



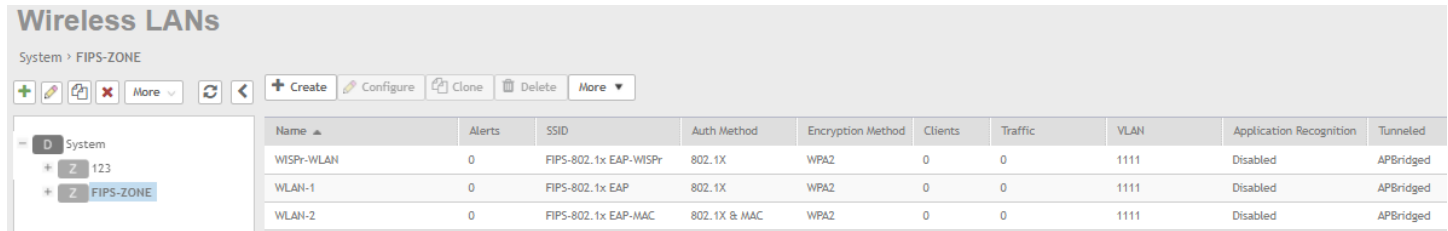
## Viewing the WLAN Configurations List

To view the WLAN configuration list, navigate to **Wireless LANs** in the web interface. As shown in the following figure, the left pane displays the FIPS Zone and its related WLAN.

## Controller Configuration with FIPS Image

### Upgrading the Software

FIGURE 47 Viewing FIPS zone WLANs



Name	Alerts	SSID	Auth Method	Encryption Method	Clients	Traffic	VLAN	Application Recognition	Tunneled
WISPr-WLAN	0	FIPS-802.1x EAP-WISPr	802.1X	WPA2	0	0	1111	Disabled	APBridged
WLAN-1	0	FIPS-802.1x EAP	802.1X	WPA2	0	0	1111	Disabled	APBridged
WLAN-2	0	FIPS-802.1x EAP-MAC	802.1X & MAC	WPA2	0	0	1111	Disabled	APBridged

#### NOTE

When TLS handshake fails between controller and RadSec Server during wireless client Authentication the controller triggers an event. To know more about this event refer to [Fails to establish TLS tunnel between SZ and External AAA Server](#) on page 275.

## Upgrading the Software

### Upgrading (v)SZ Software

RUCKUS periodically releases software updates which contains new feature enhancements or fixes for known issues.

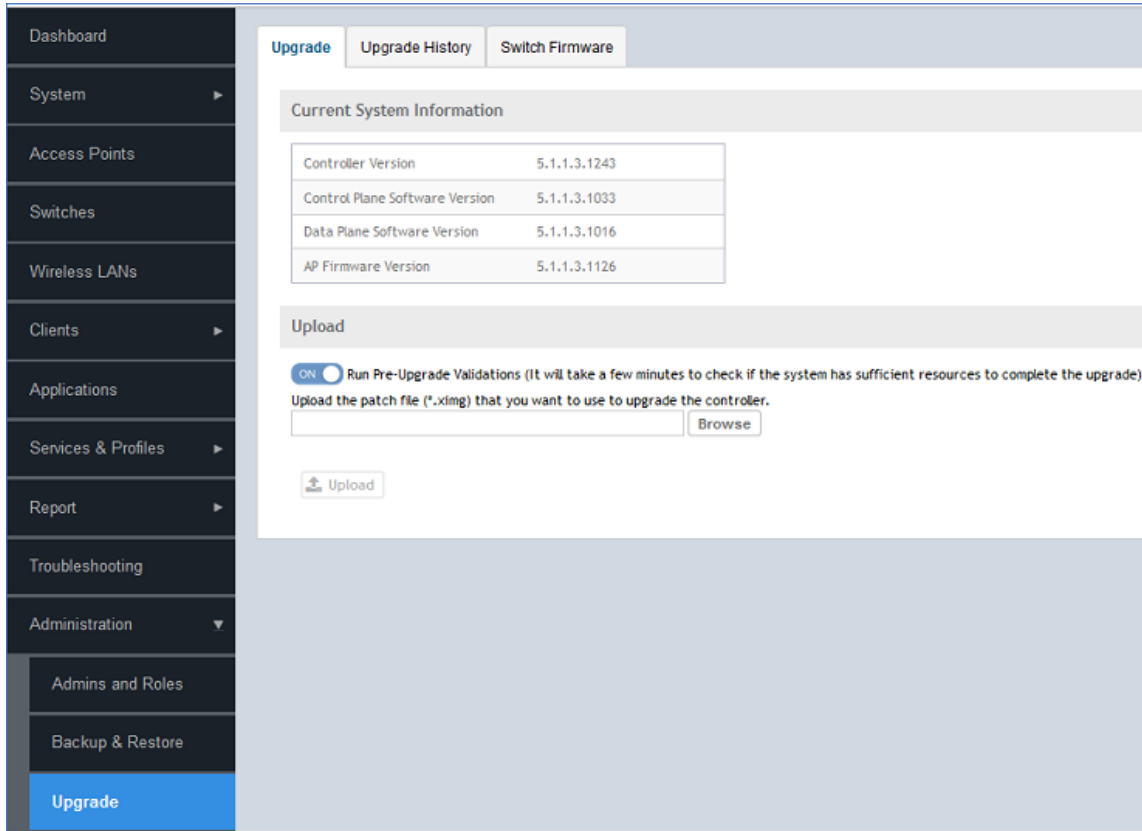
The software can be updated through GUI or CLI. Perform below steps to update the software:

1. Log-in to GUI and upload the image.



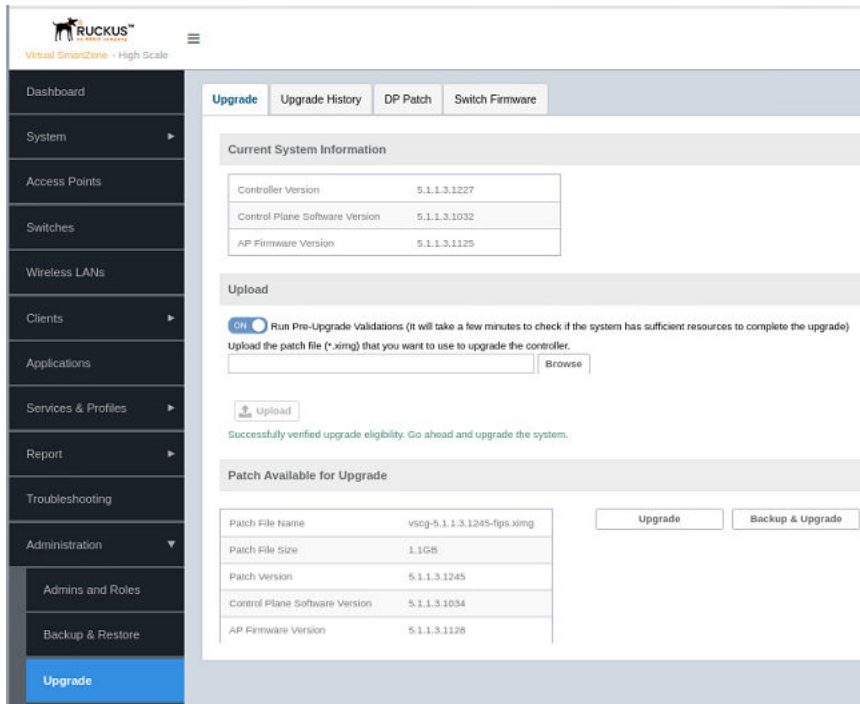
2. Download update/upgrade image from the RUCKUS Customer release site. Click **Upgrade** to view current version of the software.

**FIGURE 48** Upgrading the Software



3. After uploading the image, initiate **Upgrade** or **Backup & Upgrade**.

FIGURE 49 Initiating the Upgrade



**NOTE**

The upgrade package contains upgrade software/firmware, signatures and certificates of the signature signers. After upgrade package is uploaded to the controller, certificate chain is validated by the controller. If the certificate of signature signer passes the chain validation, then signatures of the upgrade software/firmware is verified. When upgrade package signature signer certificate chain validation error or the signature verification error occurs, the GUI shows a package decryption error. In such case, use validate upgrade package to continue system upgrading.

4. The web interface lists the active and inactive upgrade history.
5. After uploading, initiate delayed activation/upgrade.



**CAUTION**

Upgrading the (v)SZ software can force a restart and therefore, cause a temporary interruption in all the functionalities.

## Working with Application Signature Package

RUCKUS will periodically release and make new application signature packages available for download.

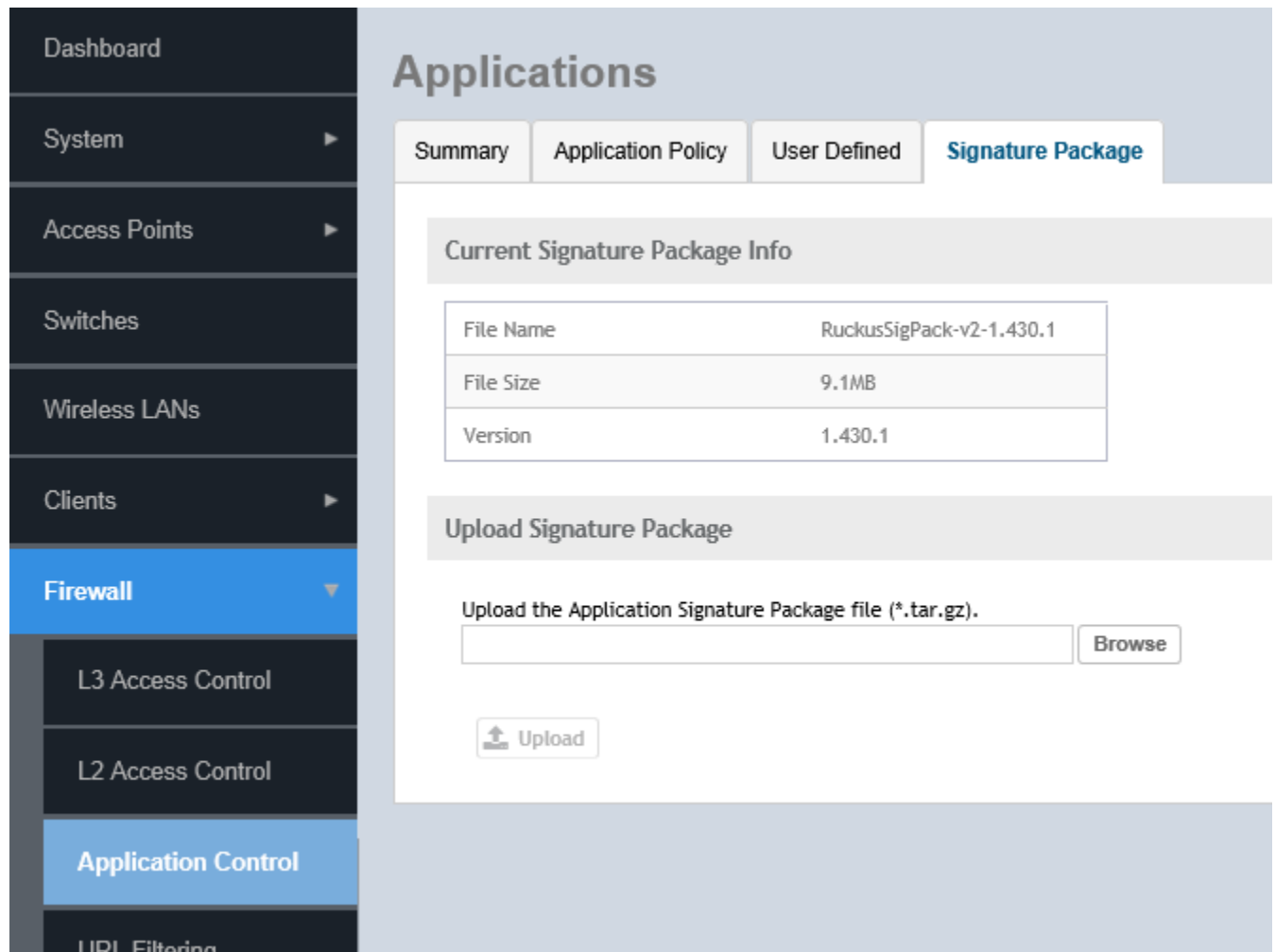
### Step 1: Uploading the Signature Package

Once you have downloaded a new signature package, you can import it into SmartZone using the following procedure:

1. Select **Firewall > Application Control**.

2. Select the **Signature Package** tab.

FIGURE 50 Viewing and Uploading Signature Package File Information



The **Current Signature Package Info** section displays the information about the file name, file size, and version of the signature package.

3. Under **Upload Signature Package**, click **Browse** to select the signature package file.
4. Click **Upload** to upload the signature package file.

Once the import is complete, the list of system-defined applications is updated immediately.

## Step 2: Validating the Signature Package

The application updates the latest signature package in all the connected APs. To validate the latest version follow the procedure:

1. In the Access Point, enter the Privileged EXEC mode using CLI.

## Controller Configuration with FIPS Image

### Upgrading the Software

2. Enter the following CLI command, which displays the latest version of the signature package.

#### NOTE

If AP is managed by SZ, then SSH will be disabled.

```
get qmdpi-version : get qmdpi-version
                  == get version details of DPI

rkscli: get qmdpi-version
DPI Signature Version : RuckusSigPack-v2-1.430.1
DPI Engine Version   : 5.4.0-68.052 (build date Jun  3 2019)
DPI Bundle Version   : 1.430.0-20 (build date Apr 15 2019)

OK
```

## Managing Signature Package Upgrading Conflicts

Upgrading a Signature package from lower version to a higher version fails when an Access Control Policy and an Application Control Policy already exists and the Application Signature in the AVC Policy of lower version conflicts with the one in higher version. In such a case, SZ displays an error message. Perform the following procedure to avoid this error.

To overcome Signature Package upgrade conflicts:

### Step 1: Delete the L3 Access Control Policy:

1. Go to **Firewall > L3 Access Control**.
2. Take a note of the policy details that you want to delete; click **Configure** to get more details of the profile for future reference.
3. Select the profile and click **Delete**.

### Step 2: Delete the Application Control Policy:

1. Go to **Firewall > Application Control > Application Policy**.
2. Take a note of the policy details that you want to delete; click **Configure** to get more details of the profile for future reference.
3. Select the policy and click **Delete**.

### Step 3: Upgrade the Signature Package

1. Go to **Firewall > Application Control -> Signature Package**.
2. Click **Browse**, and choose the Signature Package file.
3. Click **Upload**.

After the Signature Package is successfully applied the package file name, file size and the version will be visible in the UI.

Step 4: Create a new L3 Access Control Policy with the details of the policy deleted.

Step 5: Create a new Application Control Policy with the details of the policy deleted.

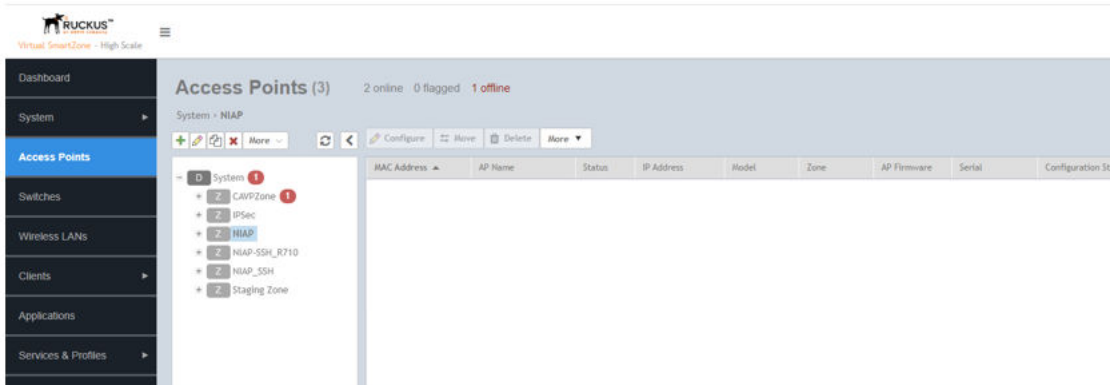
## Upgrading the AP Software

Feature enhancements or fixes or known issues pertaining to AP Software are addressed via AP firmware associated with a firmware version which is bundled part of (v) SZ Software upgrade image.

(v)SZ supports Multiple AP firmware . AP firmware version of a zone can be manually upgraded/downgraded. To change the AP Firmware of a zone, perform the following:

1. In web-interface, navigate to **Access Point**, the **Access Point** page displays. Locate the Zone for which you want to upgrade the AP firmware version.

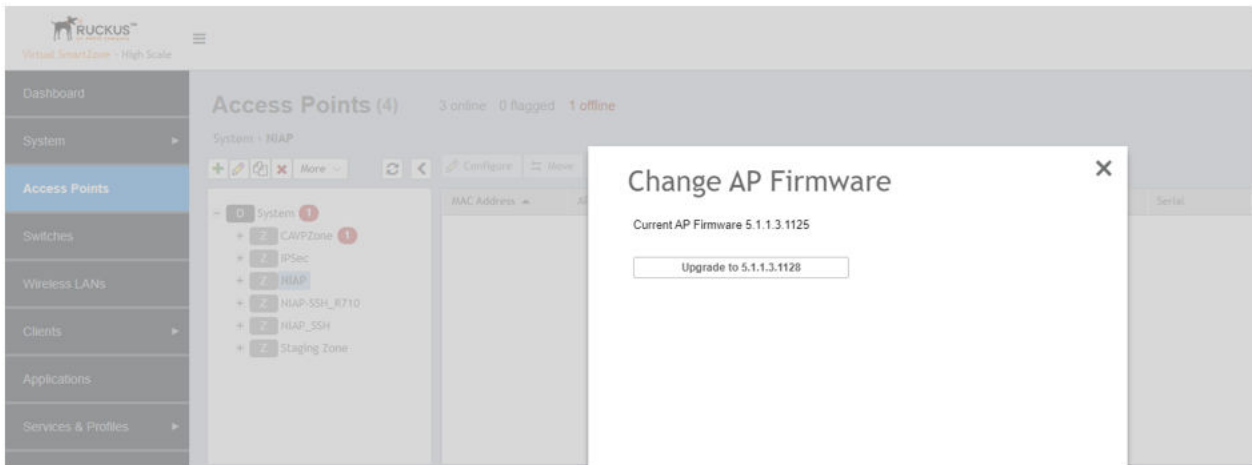
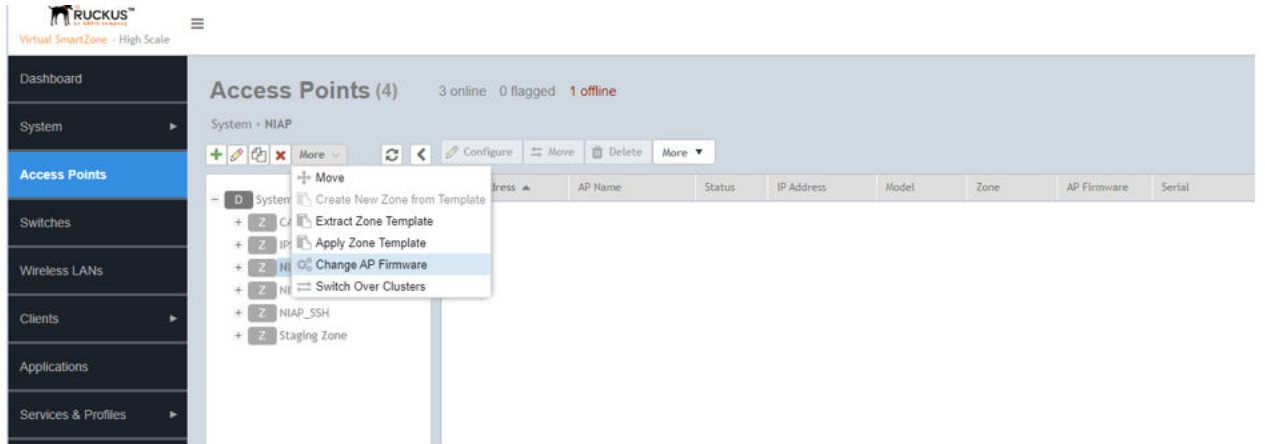
FIGURE 51 Locating the Zone



## Controller Configuration with FIPS Image Upgrading the Software

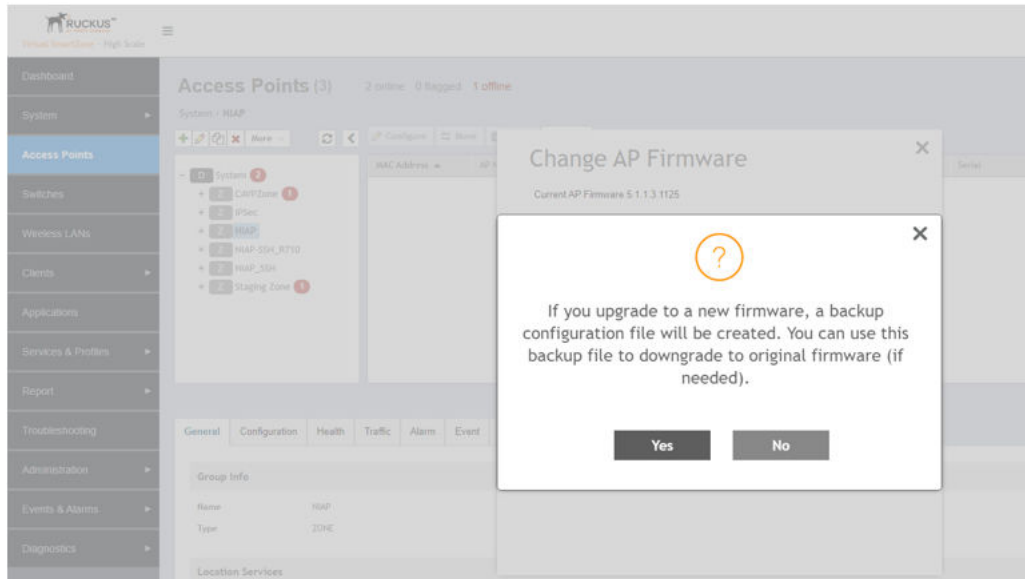
2. Click on **More** and select **Change AP Firmware**. The **Change AP Firmware** dialog box displays the current AP firmware version.

**FIGURE 52** Changing the AP Firmware



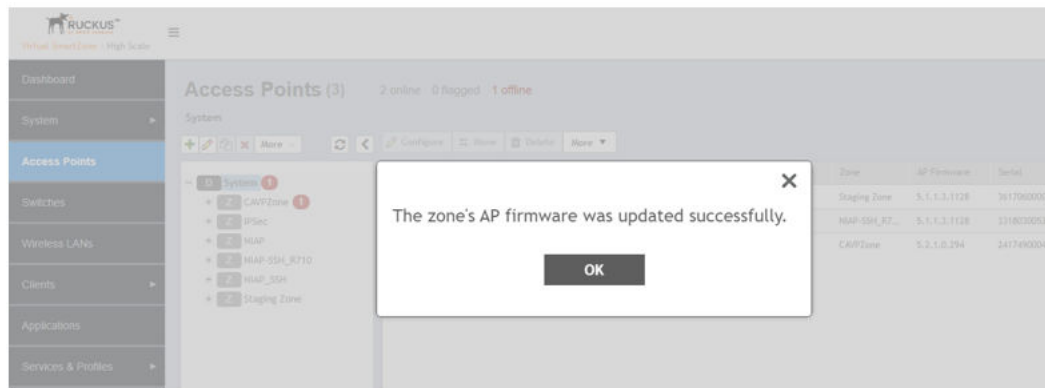
3. Select the firmware version. If upgraded to a new firmware version, backup configuration is created which can be used during firmware downgrade to original firmware.

FIGURE 53 Confirming the Upgrade



4. Click **Yes**, dialog box is displayed with the below message.

FIGURE 54 Upgrading Successfully



**NOTE**

If the zone fails to upgrade, a message is displayed to download the CSV file.

5. Click **OK** after successfully Upgrading the AP firmware of the zone.

**NOTE**

The Firmware software contains upgrade software, Signatures and certificates of the signature signers . When the Firmware is pushed to AP from (v)SZ . AP is validate the Certificate Chain first once the Chain validation goes through then AP validates the Signatures of upgrade firmware. If any of this validation fail first upgrade will and the corresponding status will be shown on UI and detailed info can be viewed through logs.



**CAUTION**

Upgrading the AP software can force a restart and therefore, cause a temporary interruption in all the functionalities.

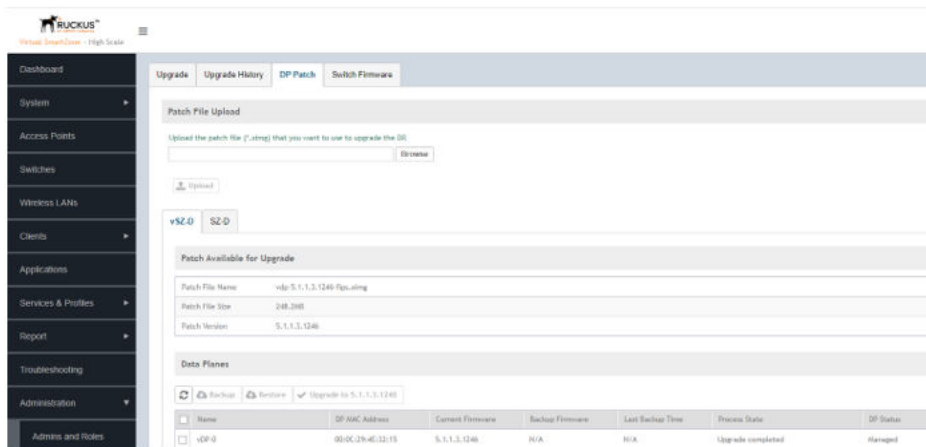
## Upgrading the vSZ-D Software

Feature enhancements or fixes or known issues pertaining to vSZ-D Software are addressed through VSZ-D Patch.

To upgrade the vSZ-D Software, perform the following steps:

1. In the web-interface, navigate to **Administration > Upgrade**.
2. Click DP Patch tab, the **DP Patch** page appears.

**FIGURE 55** DP Patch Page



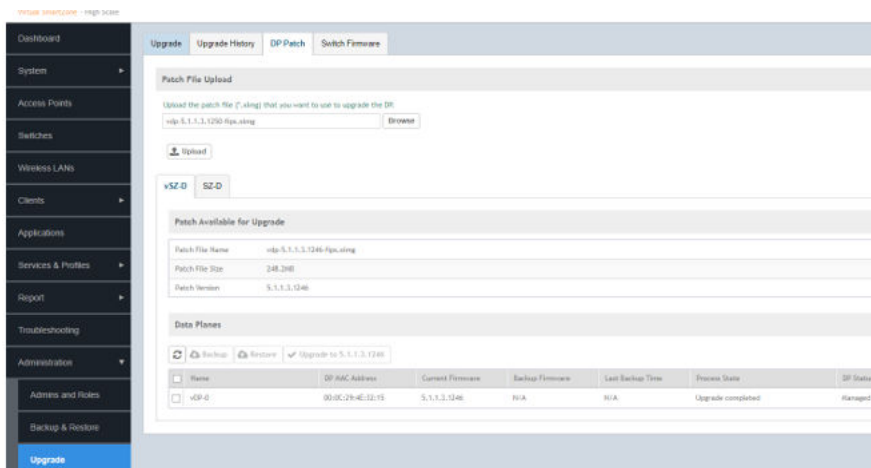
**NOTE**

The upgrade patch contains the upgrade software/firmware, signatures and the certificates of the signature signers. When the upgrade package is uploaded to the (v)SZ, (v)SZ will validate the certificate chain first. If the certificate of signature signer passes the chain validation, the (C)SZ then verifies the signatures of the upgrade software/firmware. )When the upgrade package signature signer certificate chain validation error or the signature verification error occur, the GUI shows a package decryption error .



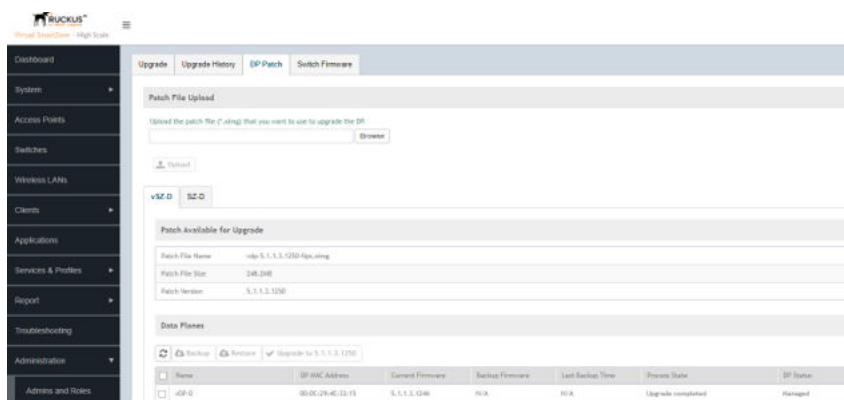
3. In Patch screen click **browse** and select the patch file to upgrade

FIGURE 56 Browsing the Patch File



4. Click **Upload** to upload the patch file.

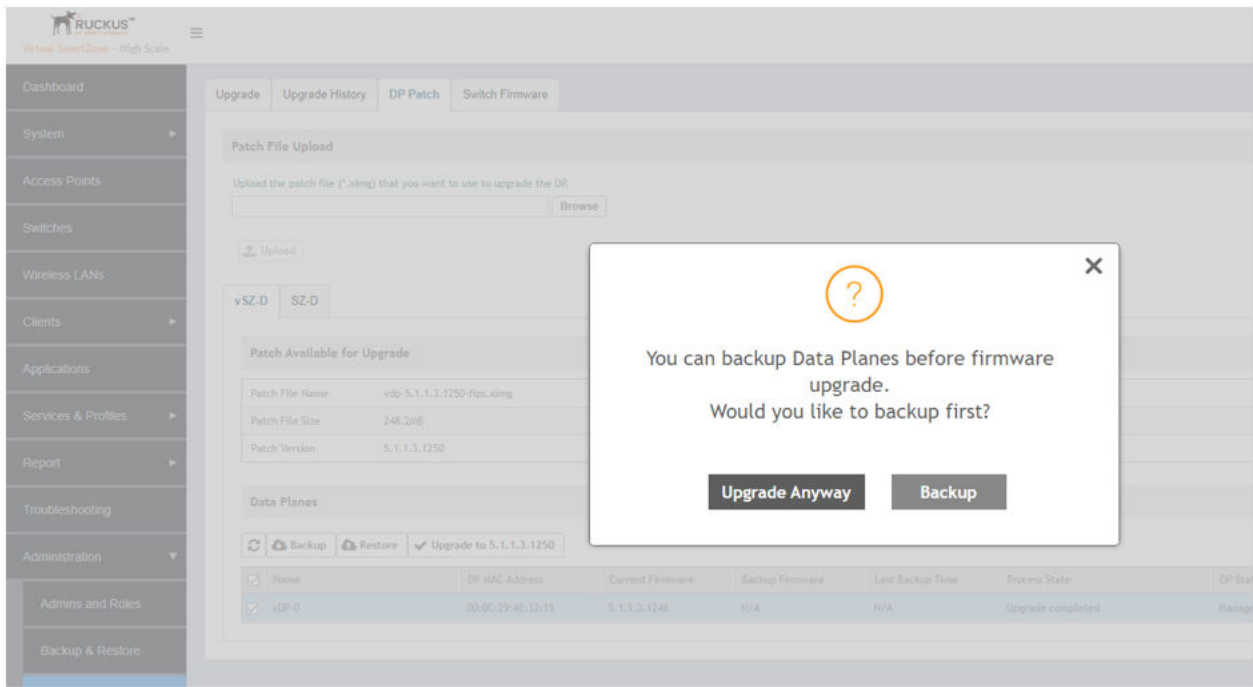
FIGURE 57 Uploading the patch file



## Controller Configuration with FIPS Image Upgrading the Software

- From the Data Plane section, select the vSZ-D to be upgraded and the patch file version to be upgraded.

**FIGURE 58** Backing up Data Plane Data

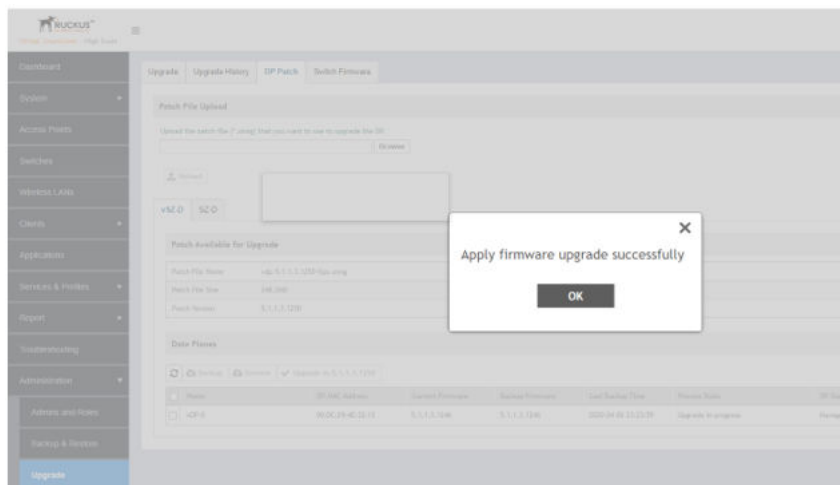


### NOTE

If you upgrade to new firmware version with a backup, a backup configuration will be created which can be used during firmware downgrade to original firmware

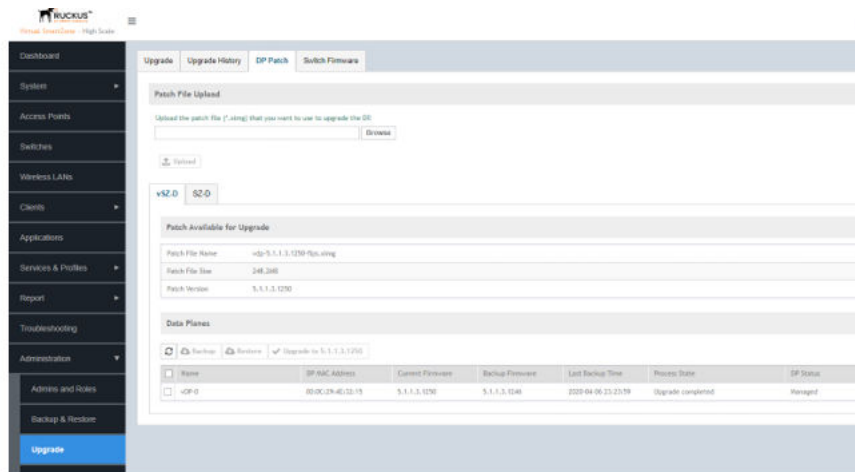
- Click on **Upgrade Anyway** to upgrade the vSZ-D to apply vSZ-D Patch

**FIGURE 59** Upgrading the vSZ-D



7. Click **OK** to Upgrade the vSZ-D patch/software.

**FIGURE 60** Successful Upgradation of vSZ-D Software



**CAUTION**

Upgrading the (v)SZ-D software can force a restart and therefore, cause a temporary interruption in all the functionalities.



# vSZ-D FIPS Installation with FIPS Image

- System Requirements..... 65
- vSZ-D FIPS Installation Prerequisites for FIPS..... 65
- Creating and Registering the Virtual Machine (vSZ-D)..... 65
- Joining vSZ-D to the vSZ Controller..... 71
- Using FIPS CLI Commands (vSZ-D)..... 75
- Downloading vSZ-D FIPS Logs..... 78

## System Requirements

The virtual platform (vSZ-D) installation can be performed on the following.

- RUCKUS virtual SmartZone - Data plane (vSZ-D)
  - ESXi 6.5
  - Running on hardware platform: (Intel(R) Xeon(R) CPU E5-2620 v4 @ 2.10GHz with AESNI).

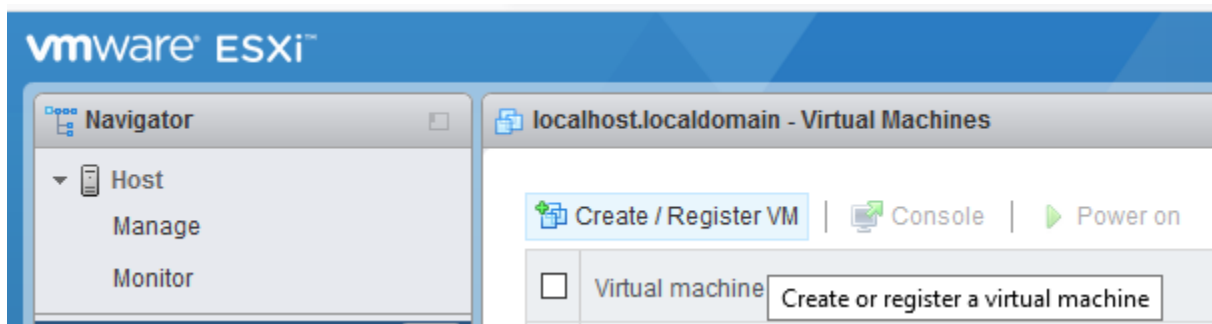
## vSZ-D FIPS Installation Prerequisites for FIPS

To comply with FIPS, you must have a new installation of vSZ-D 5.1.1.3 software. The installation will not work on a system upgraded to vSZ-D 5.1.1.3. The system validates the image before it is loaded.

## Creating and Registering the Virtual Machine (vSZ-D)

1. Install and deploy the .ova file on VMware ESXi using the **Create / Register VM** option, as shown in the following figure.

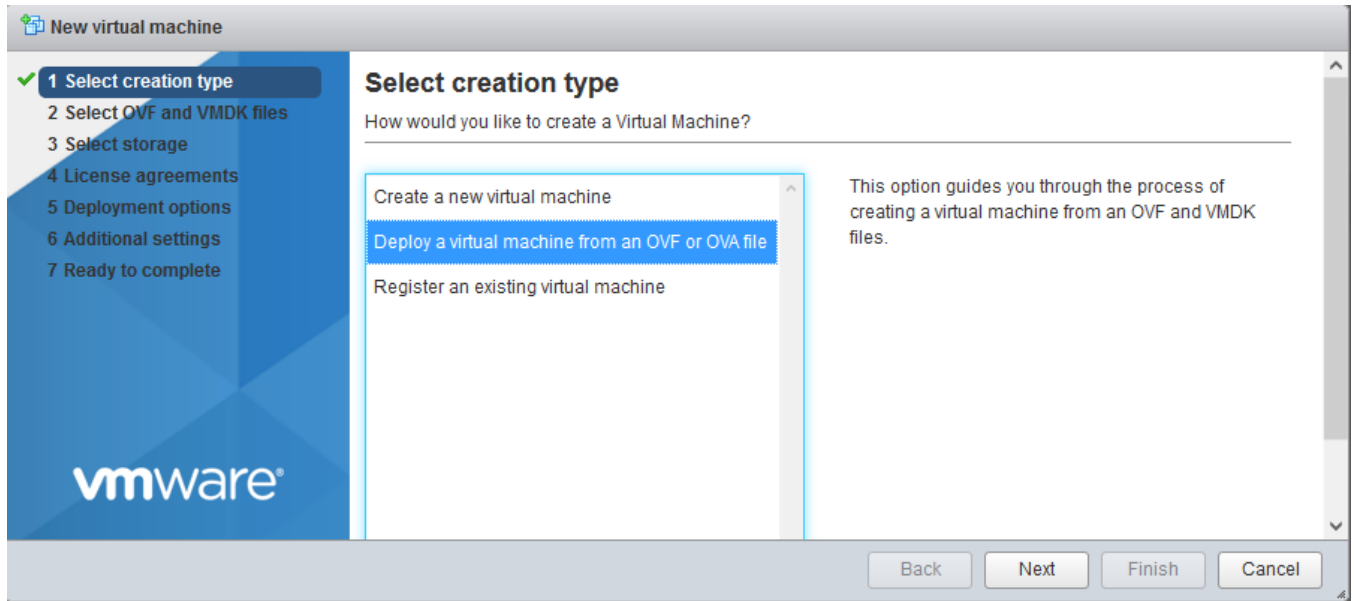
**FIGURE 61** Creating and register VM



**vSZ-D FIPS Installation with FIPS Image**  
Creating and Registering the Virtual Machine (vSZ-D)

2. Select **Deploy a virtual machine from an OVF or OVA file**.

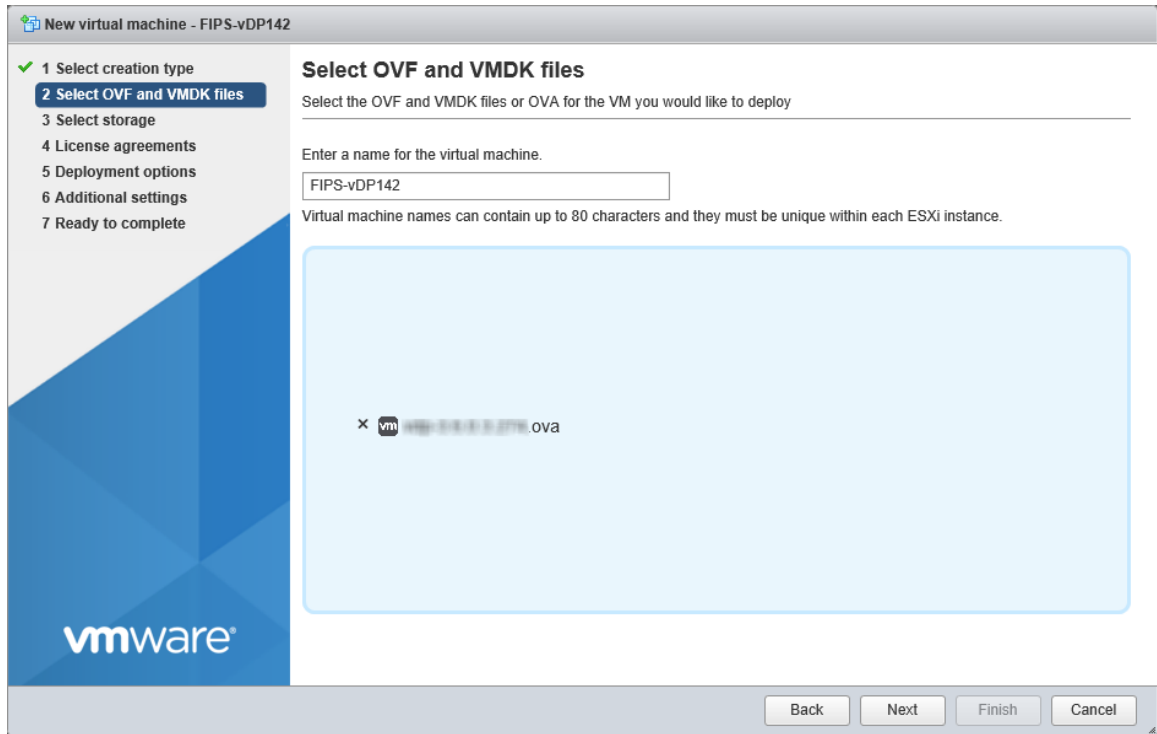
**FIGURE 62** Selecting the Creation Type



3. Click **Next** to select the OVF and VMDK files.

4. Enter the name of the VM and click the name of the OVF and VMDK file, as shown in the following figure.

**FIGURE 63** Selecting OVF and VMDK Files



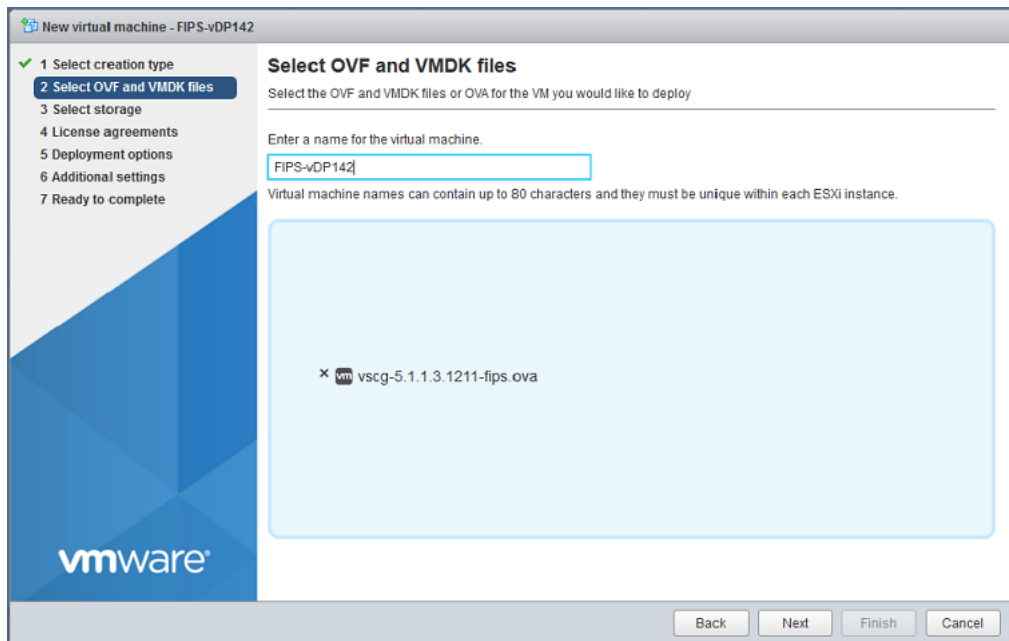
**vSZ-D FIPS Installation with FIPS Image**  
Creating and Registering the Virtual Machine (vSZ-D)

5. Select the .ova file from the browse window. The selected file is displayed in Select OVF and VMDK files screen

**FIGURE 64** Selecting the .ova File



**FIGURE 65** Selected file appears on screen

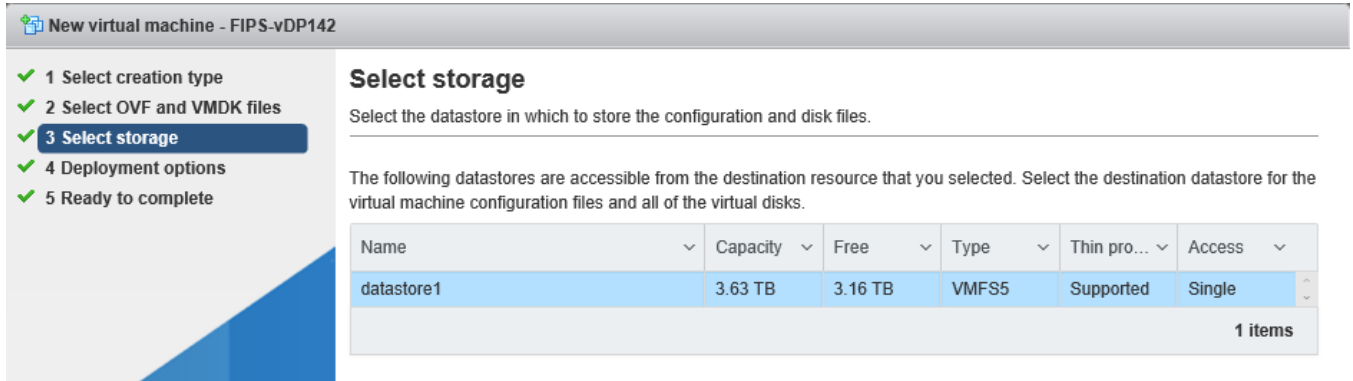


6. Click **Next** to select storage.



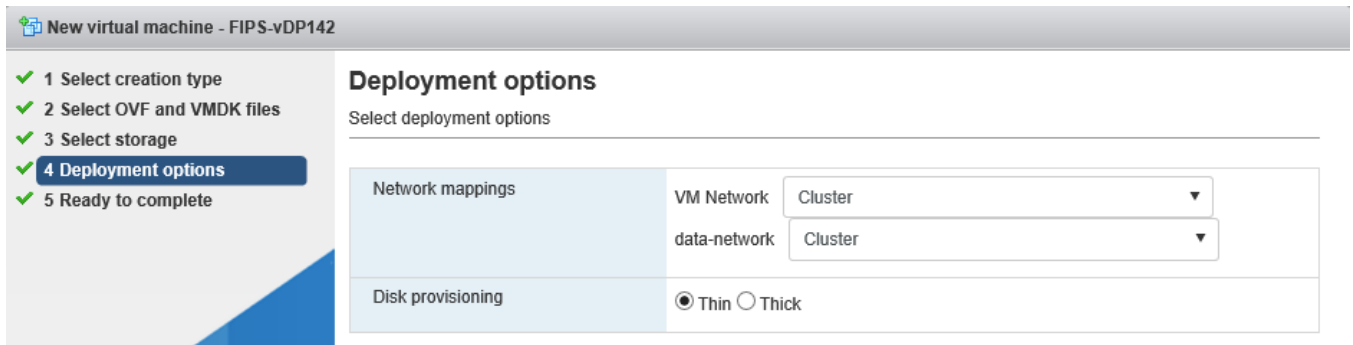
7. Select the required datastore.

FIGURE 66 Selecting the Datastore



8. Click **Next** to select deployment options.

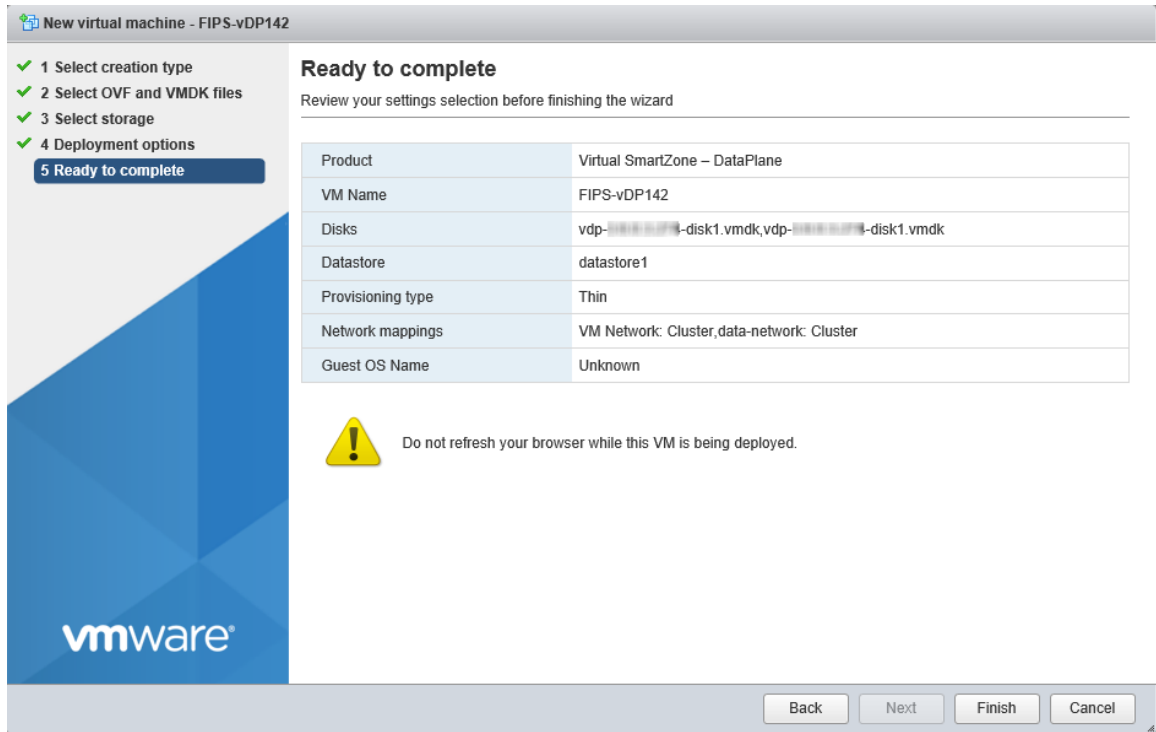
FIGURE 67 Selecting Deployment options



**vSZ-D FIPS Installation with FIPS Image**  
Creating and Registering the Virtual Machine (vSZ-D)

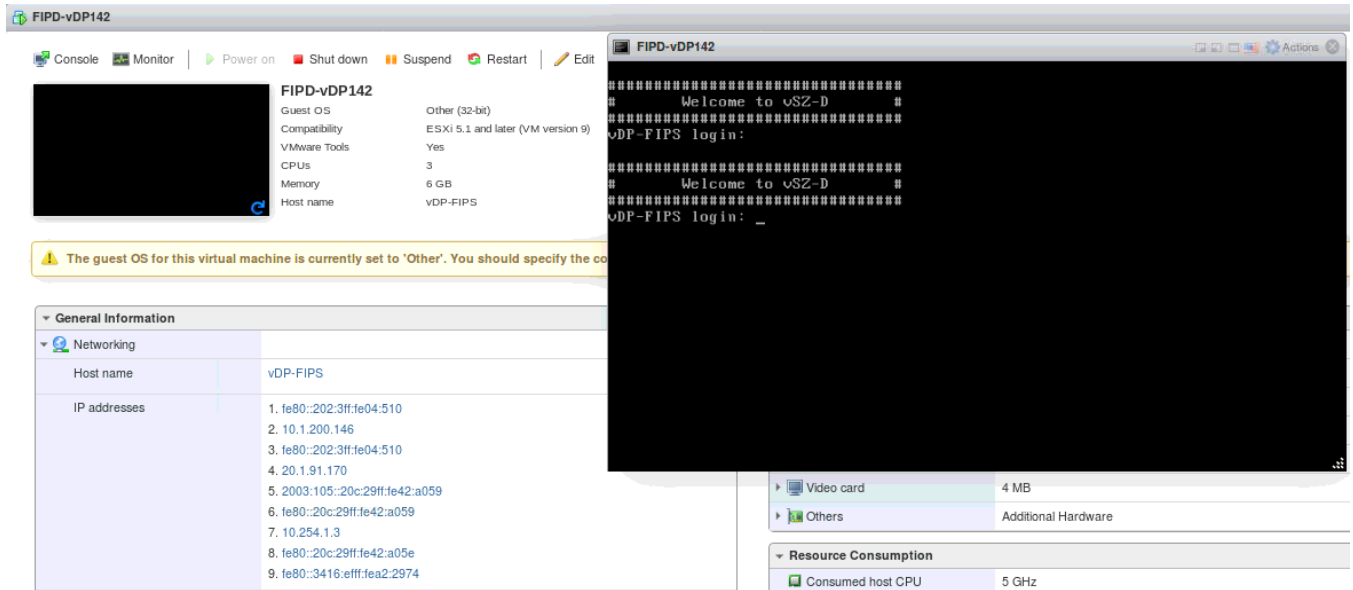
9. Click **Next** to review settings .

**FIGURE 68** Ready to Complete Installation



- Click **Finish** to complete the creation and registration of the virtual machine.  
The installation process shows the progress and displays the successfully completed tasks.

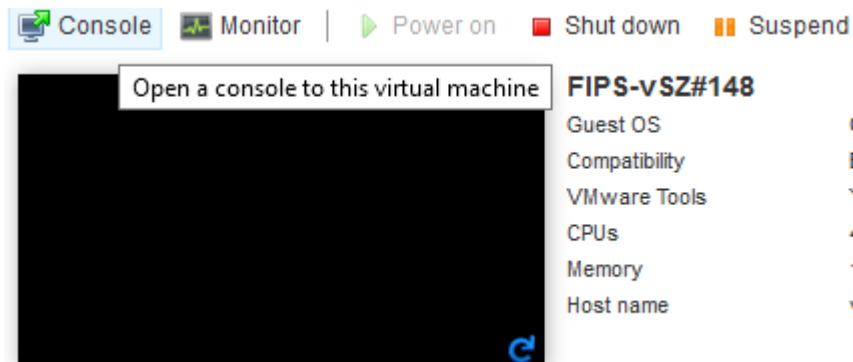
**FIGURE 69** Successful Installation



## Joining vSZ-D to the vSZ Controller

- After the VM is deployed, click **Power On** to start the vSZ-D.
- Open a console window to log in to the vSZ-D CLI.

**FIGURE 70** vSZ CLI Console

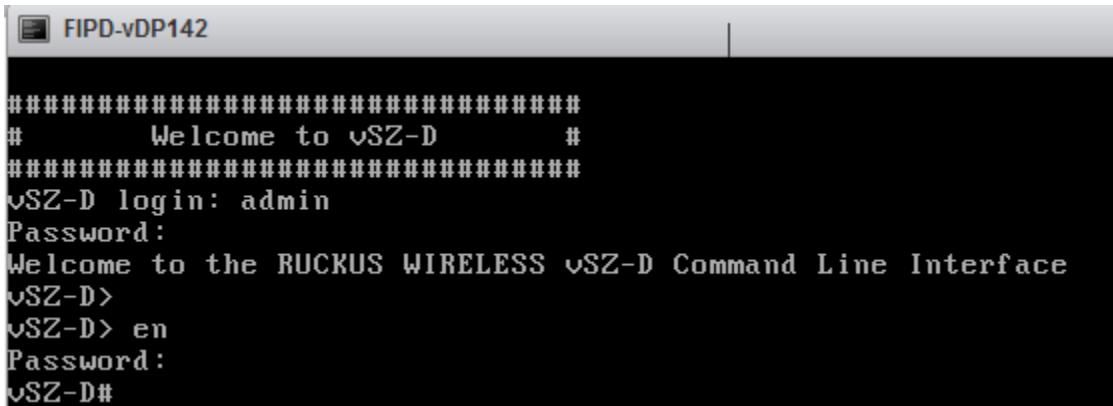


## vSZ-D FIPS Installation with FIPS Image

### Joining vSZ-D to the vSZ Controller

3. At the login prompt, log in using "administer" as the username and password.

**FIGURE 71** Logging In to Privileged EXEC Mode



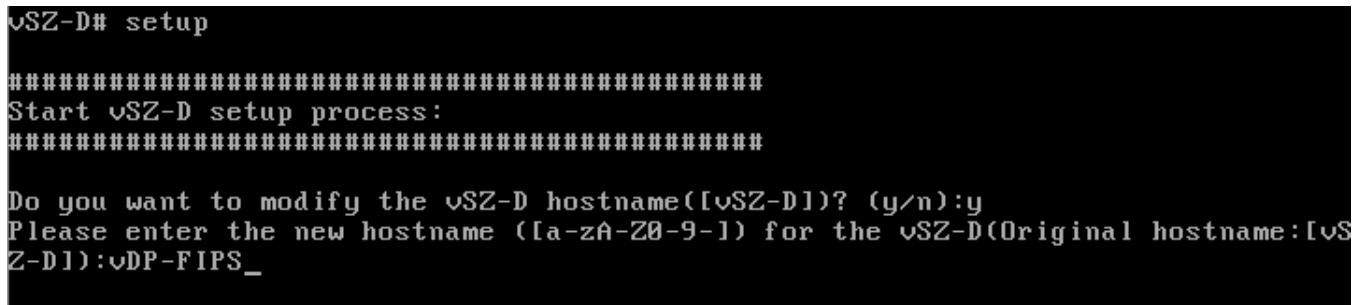
```
FIPD-vDP142
#####
#       Welcome to vSZ-D       #
#####
vSZ-D login: admin
Password:
Welcome to the RUCKUS WIRELESS vSZ-D Command Line Interface
vSZ-D>
vSZ-D> en
Password:
vSZ-D#
```

4. At the > prompt, enter the **enable (en)** command and the admin password to change to Privileged EXEC mode.
5. Use the **setup** command to configure the IP address for the management and data interfaces.

#### NOTE

It is recommended that you add a new host if you have multiple hosts for various configurations.

**FIGURE 72** Using the setup Command



```
vSZ-D# setup
#####
Start vSZ-D setup process:
#####
Do you want to modify the vSZ-D hostname([vSZ-D])? (y/n):y
Please enter the new hostname ([a-zA-Z0-9-]) for the vSZ-D(Original hostname:[vSZ-D]):vDP-FIPS_
```

6. Choose the IP address setup for the management and data interfaces by selecting either **MANUAL** or **DHCP**. Once you define the IP setup, the process of vSZ-D joining the vSZ controller starts.

FIGURE 73 Specifying IP Addresses for Management and Data Interfaces

```
#####
Start vSZ-D setup process:
#####

Do you want to modify the vSZ-D hostname([vSZ-D])? (y/n):y
Please enter the new hostname ([a-zA-Z0-9-]) for the vSZ-D(Original hostname
Z-D):vSZ-208
#####
IP Version Support
#####
1. IPv4 only
2. IPv4 and IPv6
#####
Select IP configuration (1/2):1
#####
IP address setup for Management interface
#####
1. MANUAL
2. DHCP
#####
Select IP configuration (1/2):1
IP Address:10.1.200.123
Netmask:2_

#####
IP address setup for Data interface
#####
1. MANUAL
2. DHCP
#####
Select IP configuration (1/2):1
IP Address:20.1.91.123
Netmask:255.255.255.0
Gateway:20.1.91.254
#####
Data Interface:
#####
IP Address : 20.1.91.123
Netmask : 255.255.255.0
Gateway : 20.1.91.254
#####
Do you want to apply this network configuration? (y/n):
```

**vSZ-D FIPS Installation with FIPS Image**  
 Joining vSZ-D to the vSZ Controller

- Follow the sequence of steps shown in the following figure to join vSZ-D to the vSZ controller. The process changes the FIPS mode for vSZ-D according to the FIPS mode state of vSZ.

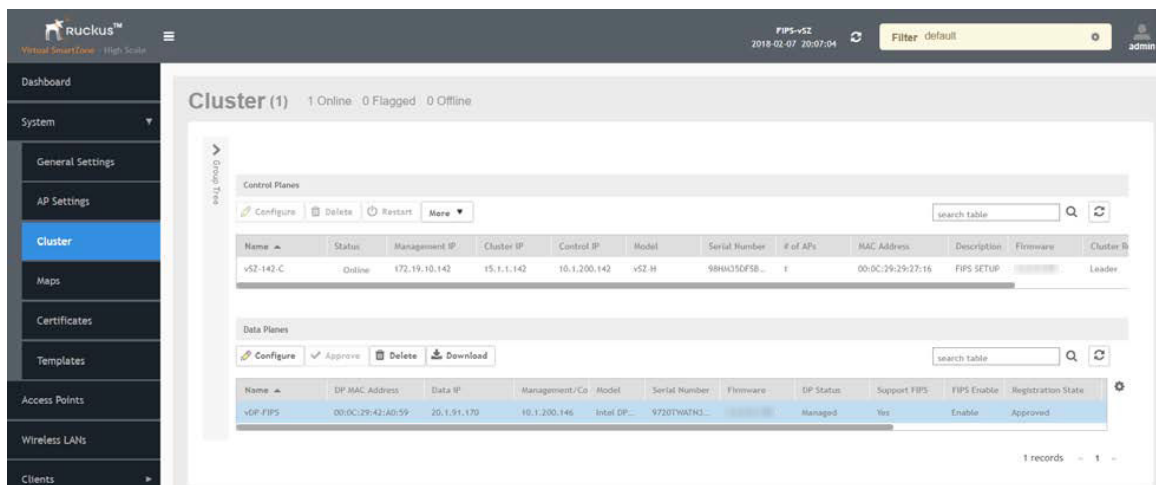
**FIGURE 74** vSZ-D Joining vSZ

```

Primary DNS:172.19.0.5
Secondary DNS:
Apply networking configuration ...
Save network configuration !
Data Interface external NAT IP:
Do you want to apply vSZ IP through DHCP Option 43 (y/n):n
Please input vSZ Control address:10.1.200.142
Do you want to connect vSZ (address:10.1.200.142) (y/n):y
Apply vSZ address ...
Save vSZ address
Please enter the new password for the local user "admin".....
Changing password for user admin.
New password:
BAD PASSWORD: it is based on a dictionary word
Retype new password:
passwd: all authentication tokens updated successfully.
Please enter CLI enable password that provides advance command.....
New password:
Retype:_
  
```

- To add the vSZ-D to vSZ controller, log in to the web interface of the vSZ. Navigate to **Clusters > Data planes**. Select the vSZ-D and click **Approve**. Upon approval, the status of the data plane appears dimmed.

**FIGURE 75** Approved vSZ-D FIPS image

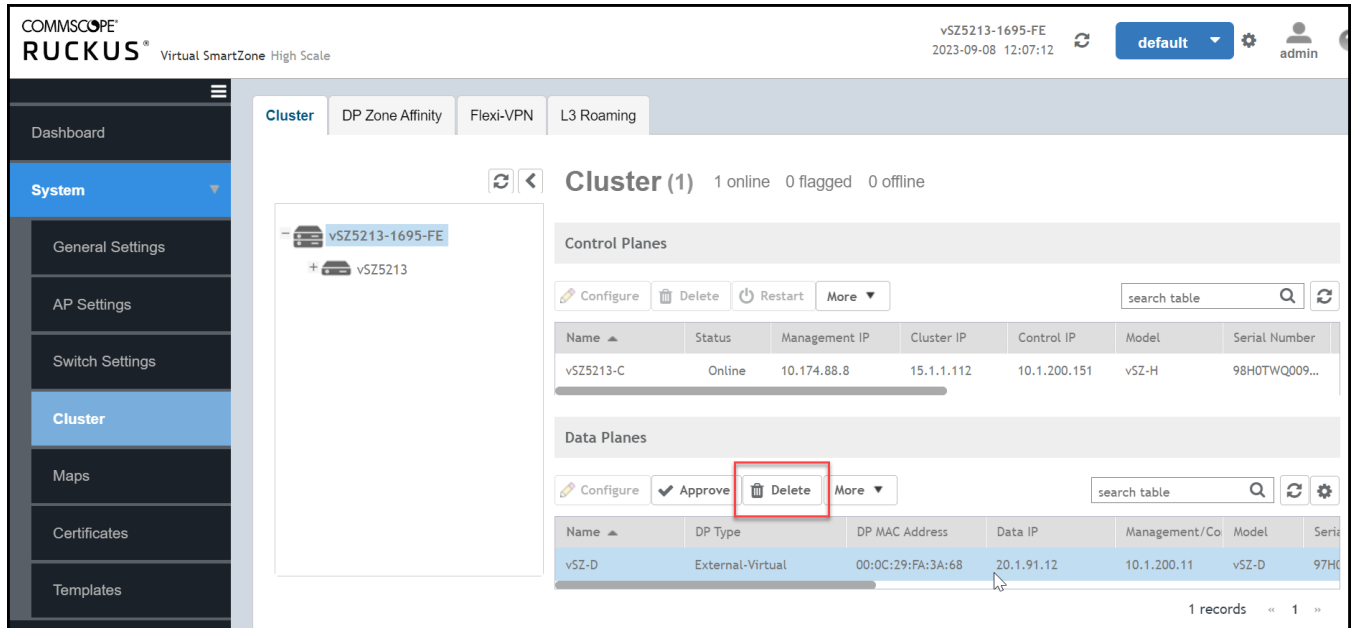


**NOTE**

After the vDP is joined to the vSZ, all management of the vDP is performed via the vSZ. SSH admin access to the vDP is stopped..

9. To delete the vSZ-D in vSZ controller, log in to the web interface of the vSZ. Navigate to **System > Clusters > Data Planes** . Select the vSZ-D and click **Delete**. Upon approval, the status of the data plane is removed from the **Data Planes** section.

FIGURE 76 Delete vSZ-D FIPS Image



**NOTE**

Deleting the vSZ-D from the controller prevents all other components from communicating with the vSZ-D.

**NOTE**

While the registration of components is done over a secure TLS channel, this part has not been claimed in the CC evaluation due to limited certificate verification capabilities during the registration. The TOE requires the use of a dedicated channel for the AP and vSZ-D to register with a Controller. The administrator must perform the registration of TOE components in a controlled environment in which there is a segregated network with only TOE components present. Further communication between AP/vSZ-D and (v)SZ is secured through the SSH connection.

## Using FIPS CLI Commands (vSZ-D)

1. Open a console window to log in to the vSZ-D CLI.
2. At the login prompt, log in using "administrator" as the username and password.
3. At the > prompt, enter the **enable (en)** command and the admin password.

4. Enter **fips status** to verify whether FIPS mode is enabled or disabled.

```
#####  
#      Welcome to vSZ-D      #  
#####  
vDP-FIPS login: admin  
Password:  
Last login: Tue Jan 23 17:26:49 on tty1  
Welcome to the RUCKUS WIRELESS vSZ-D Command Line Interface  
vDP-FIPS> en  
Password:  
vDP-FIPS# fips status  
FIPS compliance is Enable
```

5. Enter **fips ?** at the command prompt to display a list of available FIPS commands as shown.

```
vSP-FIPS# fips ?
```

The following figure provides a list of available FIPS commands.

**FIGURE 77** List of vSZ-D FIPS Commands

```
vDP-FIPS# fips  
selftest          FIPS Self Test  
showlog           Show Bootup Selftest Log  
status            Status of system FIPS compliance  
zeroization       Erase all configurations and security infor  
mation. This action will reboot the system.
```



6. Enter **fips selftest** to view and run the crypto module test for readiness.

FIGURE 78 Output of fips selftest Command

```
Starting auditd: [ OK ]
Starting FIPS Self Test:[ OK ]
Start Integrity Check:checking libXft.....
checking setup.....
checking device-mapper-persistent-data.....
checking basesystem.....
checking libffi.....
checking libX11-common.....
checking python-libs.....
checking kernel-headers.....
checking rks-net-config.....
checking kbd-misc.....
checking newt-python.....
checking fontpackages-filesystem.....
checking rks-dp-tunnelmgr.....
checking ncurses-base.....
checking rks-dp-dpm-udp.....
```

7. Enter **fips showlog** to display the results of an on-demand test of FIPS crypto modules.

FIGURE 79 Sample Output of the fips showlog Command

```
vSZ-D0# fips showlog
=====OpenSSL selftest=====
DRBG: PASSED
X931: PASSED
SHA1: PASSED
SHA2: PASSED
HMAC: PASSED
CMAC: PASSED
AES : PASSED
AES-CCM : PASSED
AES-GCM : PASSED
AES-XTS : PASSED
DES : PASSED
RSA : PASSED
ECDSA : PASSED
DSA : PASSED
DH : PASSED
ECDH : PASSED
ECP384 : PASSED
vSZ-D0# _
```

## vSZ-D FIPS Installation with FIPS Image

### Downloading vSZ-D FIPS Logs

8. Enter **fips zeroization** to delete or overwrite all system configuration, network configuration, private and public keys, certificates, passwords, pass phrases, and data. Enter **Y** to confirm the command or **N** to cancel the command. After the configuration and data are deleted, the zeroization process resets the vSZ to factory settings.

FIGURE 80 Using the fips zeroization Command

```
vDP-FIPS# fips zeroization
Are you sure you want to erase all configurations and security information, and
reboots the system[Y/N]Y_
```

## Downloading vSZ-D FIPS Logs

vSZ-D FIPS logs can be downloaded to the local machine. Only the CO (admin) can view and download the FIPS log from the web interface.

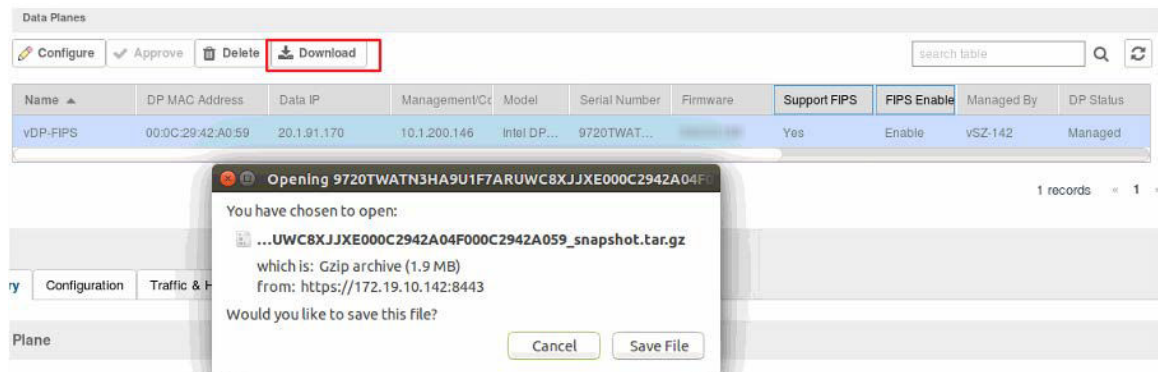
Perform the following steps to download vSZ-D FIPS logs.

1. In the web interface, navigate to **System > Clusters > Data Planes**.
2. Select the vSZ-D that has joined the controller.
3. Click the **Download** option.
4. In the displayed dialog, click **Save File**.

### NOTE

As an alternative, you can download the logs from **Diagnostics > Application Logs > DBlade** in the web interface.

FIGURE 81 Downloading vSZ-D FIPS Logs



5. Pay attention to the following considerations when downloading vSZ-D FIPS logs
  - Only a FIPS SKU vSZ-D can join a vSZ controller with a FIPS SKU set.
  - FIPS mode is replicated to vSZ-D after a successful join.
  - The zeroization effect on vSZ is not replicated on vSZ-D because it is an independent node that loses the network connection with vSZ.

# AP Configuration in FIPS Mode

- AP Models that Support FIPS Mode..... 79
- Joining AP to (v)SZ Controller..... 80
- Management Channel between AP/vSZ-D and Controller..... 81
- Configuring Regular Mesh..... 82
- FIPS AP Behavior.....85
- Crypto Officer Roles and Responsibilities for AP..... 86
- Quarantine State for AP.....86
- AP Features Not Supported in FIPS Mode..... 86
- Creating a WLAN WPA3 WLAN2/WPA3 Mixed Profile..... 91
- Recovery SSID..... 95
- SSH Public Key Authentication..... 98

## AP Models that Support FIPS Mode

The following 11ax AP models support FIPS mode.

**TABLE 5** 11ax AP Models supported on FIPS mode

Access Point Name	Hardware Part Number
R650-US Access Point	9F1 R650-US
R650-WW Access Point	9F1 R650-WW
R750 Access Point	9F1 R750
R850 Access Point	9F1 R850
T750SE Access Point	9F1 T750SE
T750SE Access Point	9F1 T750SE
T750-WW Access Point	9F1 T750-WW

The following controller models support FIPS mode.

- SZ144
- SZ300
- ESXi-6.7U1-10764712-A03 (VMware, Inc.)
- ESXi-6.5.0-20170702001-standard (VMware, Inc.)

**NOTE**

The peer node (server) selects the FIPS compliant ciphers while establishing a connection with the AP.

**NOTE**

While the registration of components is done over a secure TLS channel, this part has not been claimed in the CC evaluation due to limited certificate verification capabilities during the registration. The TOE requires the use of a dedicated channel for the AP and vSZ-D to register with a Controller. The administrator must perform the registration of TOE components in a controlled environment in which there is a segregated network with only TOE components present. Further communication between AP/vSZ-D and (v)SZ is secured through the SSH connection.

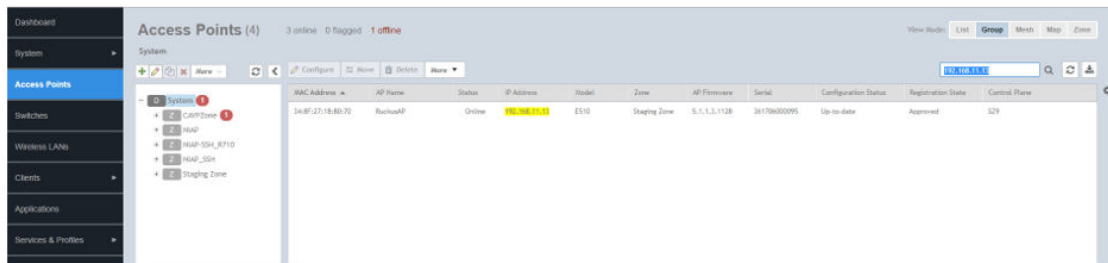
## Joining AP to (v)SZ Controller

AP can be made to discover the RUCKUS WLAN controller either by using DHCP option 43 or by setting WLAN controller IP address through AP CLI. For setting the WLAN controller IP address through AP CLI perform the following:

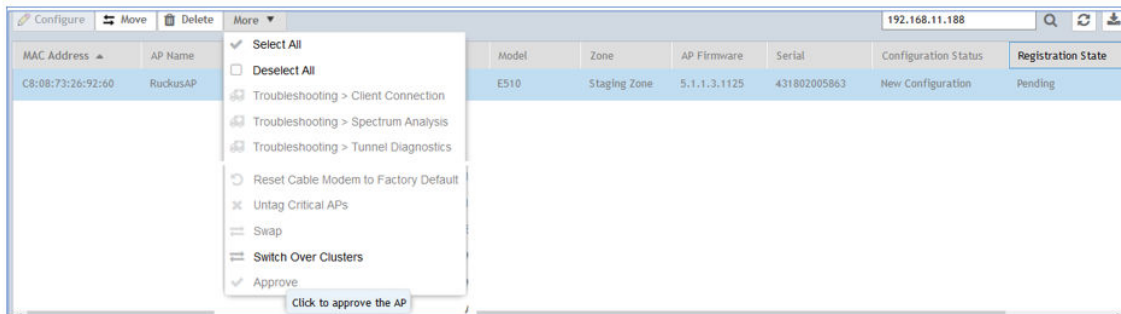
1. Logon to the AP through AP SSH using username and password as **super** and **sp-admin** and set the WLAN controller IP address. Follow the command to enable SSH communication towards WLAN controller.

```
rksccli:  
rksccli: set scg ip 10.1.200.143  
OK
```

2. Logon to the WLAN controller through web interface and navigate to **Access Points**.



3. Select the joined AP and click **More > Approve** to approve the AP.



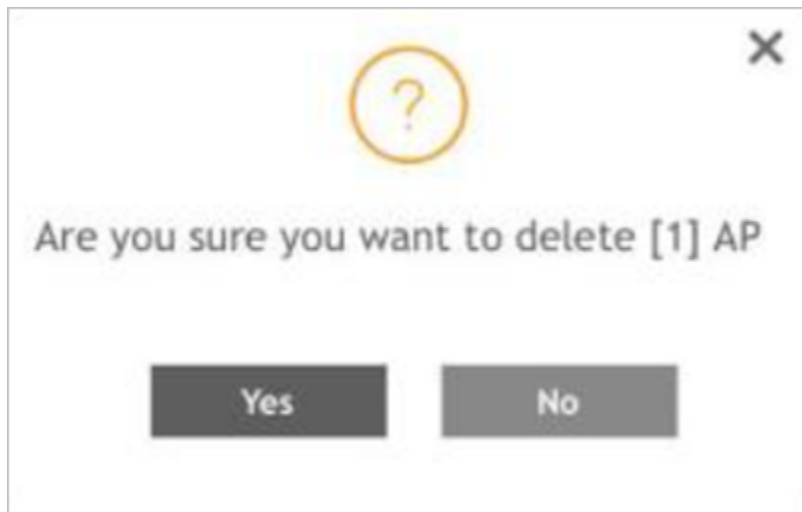
Once AP is approved, an SSH tunnel will be formed across AP and WLAN controller using public key authentication (without password - based authentication). This SSH tunnel will be utilized for management communication between AP and controller. If the connection is broken it will be resumed/re-attempted without any user intervention.

### NOTE

The SSH connection is established between AP and controller after the registration and without any user intervention.

4. To remove the AP from the controller, select the joined AP and click **Delete**.

**FIGURE 82** Deleting an Access Point



**NOTE**

Deleting the AP from the controller prevents all other components from communicating with the AP.

## Management Channel between AP/vSZ-D and Controller

The AP and vSZ-D are SSH clients which communicate to the SSH server which is the controller. This communication is only through public key auth (No password-based authentication). If the connection is broken it is resumed by default.

The following SSH parameters are non-configurable:

- SSH encryption algorithm
- SSH integrity MAC algorithm
- SSH client and server parameters
- Rekey limitation

**NOTE**

The rekey limitation is 1 hour or 1 GB of data traffic when the vSZ-D or AP connects to the SZ SSH server as an SSH client. The SSH client or server discards the data packets if the incoming packet size exceeds the packet size limitation; the maximum packet size is 256 KB.

# Configuring Regular Mesh

The Mesh topology feature is about the nature of the APs inside a venue and their relations. In this architecture, no user intervention required but user may constrain topology if desired. Multi-channel mesh paths are supported using wired mesh links.

## Creating an AP Zone

To create an AP zone, complete the following steps.

1. On the menu, select **Access Point > Access Point**.

FIGURE 83 Access Points Page


2. From the **System** tree hierarchy, select the location where you want to create the zone (for example, System or Domain), and click 
3. Configure the zone by completing the settings listed in the following table:

TABLE 6 AP Zone Details

Field	Description	Your Action
<b>Configuration &gt; General Options</b>		
<b>AP Admin Logon</b>	Indicates the administrator logon credentials.	Enter the <b>Logon ID</b> and <b>Password</b> .
<b>Configuration &gt; Mesh Options</b>		

TABLE 6 AP Zone Details (continued)

Field	Description	Your Action
<b>Enable mesh networking in this zone</b>	Enables managed APs to automatically form a wireless mesh network, in which participant nodes (APs) cooperate to route packets.  Dual-band APs can only mesh with other dual-band APs, while single-band APs can only mesh with other single-band APs.	Click the button.
<b>Zero Touch Mesh</b>	Enables a new AP to join the network using wireless connection.	Disable the option.
<b>Mesh Name (ESSID)</b>	Indicates the mesh name.	Enter a name for the mesh network. Alternatively, do nothing to accept the default mesh name that the controller has generated.
<b>Mesh Passphrase</b>	Indicates the passphrase used by the controller to secure the traffic between Mesh APs.	Enter a passphrase that contains at least 8 characters. Alternatively, click <b>Generate</b> to generate a random passphrase with 64 characters or more.
<b>Mesh Radio Option</b>	Indicates the channel range configured.	Select the channel option: 2.4 GHz or 5 GHz. Default value is 5 GHz.

4. Click **OK**.

For SZ300 and vSZ-H, you can also migrate the Zone configuration from a regular Domain to a Partner Domain.

5. If the controller is an **Enterprise** edition, then you must approve an AP in the **Default** zone and then move the AP to Mesh Zone. If the controller is **High Scale** edition then you must move an AP from **Staging Zone** to Mesh Zone and then approve the AP.

## AP Configuration in FIPS Mode

### Configuring Regular Mesh

- After moving the APs into the Mesh Zone, select an AP, and click **Configure**.

**FIGURE 84** Clicking Configure

The screenshot shows the Ruckus AP configuration interface. The top navigation bar includes 'Dashboard', 'System', 'Access Points', 'Monitoring APs', 'Switches', 'Wireless LANs', 'Clients', 'Firewall', 'Services & Profiles', 'Report', 'Troubleshooting', 'Administration', 'Events & Alarms', and 'Diagnostics'. The main content area is titled 'Access Points (4)' and shows a table of APs. The 'Configure' button is highlighted in red. Below the table, the 'Event' tab is selected, showing a list of events.

MAC Address	AP Name	Status	IP Address	Model	Mesh Role	AP Firmware	Serial	Configuration Status	Registration Status
28:B3:71:2F:28:70	RuckusAP	Online	192.168.0.105	R750	MAP	5.2.1.3.1101	212020007641	Up-to-date	Approved
70:CA:97:3A:09:10	RuckusAP	Online	192.168.0.107 / 1c95:1	R650	DISABLED	5.2.1.3.1101	142039004540	N/A	Pending
C8:03:F5:2C:88:D0	RuckusAP	Online	192.168.0.102	R850	RAP	5.2.1.3.1101	982072000787	Up-to-date	Approved

Date and Time	Code	Type	Severity	Activity
2021-05-07 14:40:00	303	AP disconnected	Major	AP [RuckusAP@70:CA:97:3A:09:10] disconnected.
2021-05-07 14:18:42	101	AP discovery succeeded	Informational	AP [RuckusAP@70:CA:97:3A:09:10] sent a discovery request to Virtual SmartZone [172.31.31.250].
2021-05-07 14:12:13	313	AP deleted	Major	AP [RuckusAP@70:CA:97:3A:09:10] has been deleted.
2021-05-07 13:56:00	303	AP disconnected	Major	AP [RuckusAP@70:CA:97:3A:09:10] disconnected.
2021-05-07 13:52:00	314	AP heartbeat lost	Informational	AP [RuckusAP@70:CA:97:3A:09:10] heartbeat lost.
2021-05-07 13:51:00	312	AP connected	Informational	AP [RuckusAP@70:CA:97:3A:09:10] connected because of [AP connected after discovery].

The **Mesh Options** page is displayed.

**FIGURE 85** Selecting Mesh Option

The screenshot shows the 'Mesh Options' configuration page. The 'Mesh Mode' section has 'Auto (Mesh role is assigned automatically)' selected. The 'Uplink Selection' section has 'Smart (Mesh APs automatically select the best uplink)' selected.

#### NOTE

In a Mesh network, there are several kinds of APs: Root APs (RAP), Mesh APs (MAP) and Ethernet Mesh APs (EAP). The RAPs are connected directly to the main network which activates on the venue in which they reside in. The first AP that is added to the Mesh is considered as RAP. The **Mesh APs** are connected indirectly to the main network. They are connected to the parent AP (Root AP or another e/Mesh AP) through wireless network which shares the connection to the main network. The **Ethernet Mesh APs** are connected indirectly to the main network. They are connected to the parent AP through ethernet. You can set the remaining APs as **Auto** or **MAP** as per the requirement.



- Select the Mesh zone, and click **Mesh** in the view mode.  
The APs that are configured for that specific Mesh are listed.

FIGURE 86 Viewing the Mesh Mode

Access Point	SNR	AP Name	AP Model	IP Address	External IP Address	Mesh Role	Channel	Client Count	Hop count
C8:03:F5:2C:88:D0		RuckusAP	R850	192.168.0.120	115.99.133.18:36915	Root AP	11 (auto),157 (11ax)	1	0
28:B3:71:2F:28:70	74 dB	RuckusAP	R750	192.168.0.100	115.99.171.18:36747	Mesh AP	11 (11ax),157 (11ax)	0	1
70:CA:97:3A:09...	76 dB	RuckusAP	R650	192.168.0.125	115.99.171.18:50483	Mesh AP	6 (11ax),157 (11ax)	0	2

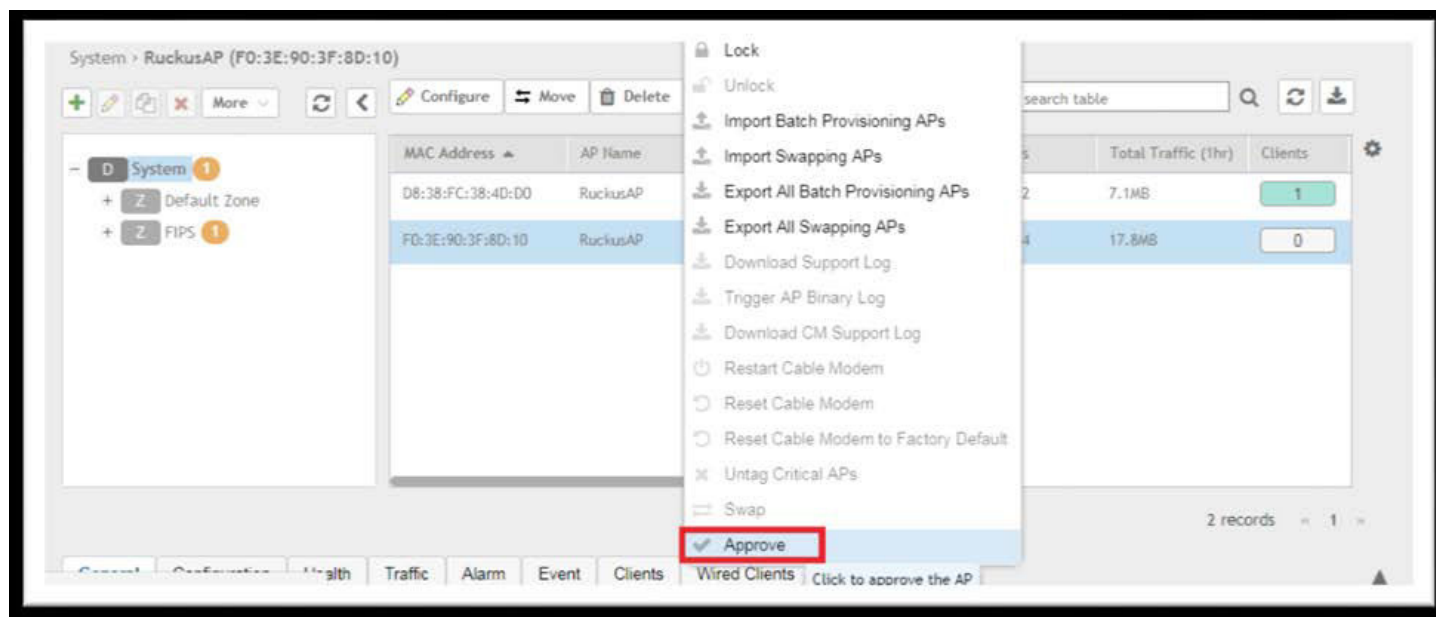
## FIPS AP Behavior

By default, FIPS mode on an AP is disabled. The FIPS state is displayed when you log in.

When a FIPS SKU AP joins a FIPS SKU SmartZone controller, it adopts the mode of the controller by default. Therefore, when an AP in FIPS mode joins a controller with a FIPS mode disabled, the FIPS mode in the AP is also disabled, and vice versa. If the AP and controller are running the same mode, then the AP mode remains unchanged. This implies that only a FIPS SKU AP can join FIPS SKU controller.

A FIPS SKU AP with FIPS mode disabled must be manually approved in the SmartZone interface whether auto-approval is enabled or disabled on SmartZone.

FIGURE 87 Manually Approving APs in the SmartZone Interface



FIPS AP with FIPS mode enabled is registered with SmartZone without any approval and is displayed in the default or staging zone  
Any non-FIPS AP is not able to join a FIPS-enabled SmartZone interface. A non-FIPS AP is not displayed in the default or staging zone.

## AP Configuration in FIPS Mode

### Crypto Officer Roles and Responsibilities for AP

#### NOTE

For Commercial Solutions for Classified Program (CSfC) compliance, run the following command to disable AP-to-AP communication and 802.11r on the AP or `rclient -d <ap-mac> -c "set ap2ap_dormant 1"` on the controller.

Ensure that 802.11r is disabled at each WLAN configuration if you disable AP-to-AP communication.

## Crypto Officer Roles and Responsibilities for AP

The AP has only one login (Crypto Officer). The default username is super, and the default password is sp-admin. These credentials are overwritten when the AP joins SmartZone, and the zone login credentials are applied to the AP. Only these login credentials have access to the AP CLI and can perform FIPS-related activities such as zeroization and FIPS mode changes.

## Quarantine State for AP

An AP goes into the quarantine state in either of the following situations:

- The AP is zeroized.
- The AP self-test has failed due to an error in the firmware.

In zeroized APs, the Crypto Officer (CO) is unable to access the AP CLI. The only way to recover the CO login is through a hard reset. A hard reset allows the CO to log in to the AP CLI; however, zeroization causes the AP to lose the web, user, and SSH certifications and keys permanently.

In APs that fail the self-test, network connectivity goes down and a hard reset cannot recover the AP; it must be sent back to the factory. You can determine the failure of the AP self-test only by physically examining the device.

The following LEDs on the AP (R720, R610, T610) display the quarantine status of the device:

- POWER : Solid red
- Wireless 2.4GHz: Solid amber
- Wireless 5GHz: Solid amber

The T610s and the T710s APs have similar LED patterns as the T610.

## AP Features Not Supported in FIPS Mode

The following AP features are not supported in FIPS mode:

- Recovery SSID
- Firmware upgrade options such as FTP, TFTP, and the web
- Telnet and HTTP management access
- Web interface access using HTTPS to the AP, once the AP has successfully joined SmartZone
- SNMPv1 and SNMPv2c (Only SNMPv3 is supported in FIPS mode.)
- Setting the WLAN interface state to up or down from the AP CLI

#### NOTE

The AVC feature is disabled by default in the SmartZone interface, however, ensure that the feature is disabled for end-to-end FIPS compliance.

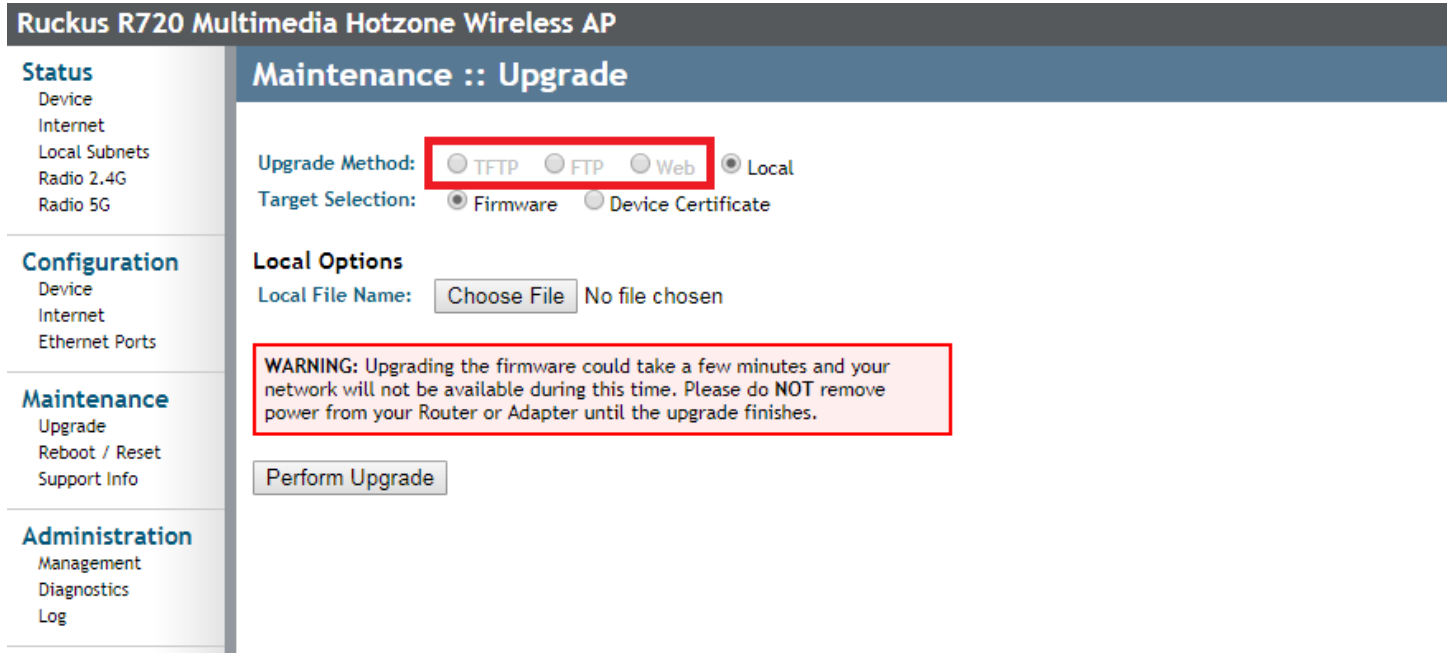
## Recovery SSID Not Supported.

FIGURE 88 Output to get wlanlist Command

```
rksccli: get wlanlist
name      status  type   wlanID  radioID  bssid          ssid
-----
wlan0     up      AP     wlan0   0        f0:3e:90:3f:8d:18 #Javeed
wlan1     down    AP     wlan1   0        00:00:00:00:00:00 Wireless2
wlan2     down    AP     wlan2   0        00:00:00:00:00:00 Wireless3
wlan3     down    AP     wlan3   0        00:00:00:00:00:00 Wireless4
wlan4     down    AP     wlan4   0        00:00:00:00:00:00 Wireless5
wlan5     down    AP     wlan5   0        00:00:00:00:00:00 Wireless6
wlan6     down    AP     wlan6   0        00:00:00:00:00:00 Wireless7
wlan7     down    AP     wlan7   0        00:00:00:00:00:00 Wireless8
wlan8     down    AP     wlan8   0        00:00:00:00:00:00 Wireless9
wlan9     down    AP     wlan9   0        00:00:00:00:00:00 Wireless10
wlan10    down    AP     wlan10  0        00:00:00:00:00:00 Wireless11
wlan11    down    AP     wlan11  0        00:00:00:00:00:00 Wireless12
wlan12    down    AP     wlan12  0        00:00:00:00:00:00 Wireless13
wlan13    down    AP     wlan13  0        00:00:00:00:00:00 Wireless14
wlan14    down    AP     wlan14  0        00:00:00:00:00:00 Wireless15
wlan32    up      AP     wlan32  1        f0:3e:90:3f:8d:1c #Javeed
wlan33    down    AP     wlan33  1        00:00:00:00:00:00 Wireless10
wlan34    down    AP     wlan34  1        00:00:00:00:00:00 Wireless11
wlan35    down    AP     wlan35  1        00:00:00:00:00:00 Wireless12
wlan36    down    AP     wlan36  1        00:00:00:00:00:00 Wireless13
wlan37    down    AP     wlan37  1        00:00:00:00:00:00 Wireless14
wlan38    down    AP     wlan38  1        00:00:00:00:00:00 Wireless15
wlan39    down    AP     wlan39  1        00:00:00:00:00:00 Wireless16
wlan40    down    AP     wlan40  1        00:00:00:00:00:00
wlan41    down    AP     wlan41  1        00:00:00:00:00:00
wlan42    down    AP     wlan42  1        00:00:00:00:00:00
wlan43    down    AP     wlan43  1        00:00:00:00:00:00
wlan44    down    AP     wlan44  1        00:00:00:00:00:00
wlan45    down    AP     wlan45  1        00:00:00:00:00:00
wlan46    down    AP     wlan46  1        00:00:00:00:00:00
wlan47    down    AP     wlan47  1        00:00:00:00:00:00
OK
```

## FTP, TFTP, and Web Not Supported

FIGURE 89 Unavailable Upgrade Methods in FIPS Mode



## HTTP and Telnet Management Access Not Supported

HTTP and Telnet management access is not supported in FIPS mode. The Telnet and HTTP access options are unavailable in the web interface when FIPS mode is enabled.

FIGURE 90 HTTP and Telnet Management Access Unavailable in FIPS Mode

The screenshot shows the 'Administration :: Management' page for a Ruckus R720 Multimedia Hotzone Wireless AP. The left sidebar contains navigation menus for Status, Configuration, Maintenance, and Administration. The main content area shows various settings:

- Network Profile: 4bss
- SSH Access?:  Enabled  Disabled
- SSH Port: 22
- HTTPS Access?:  Enabled  Disabled
- HTTPS Port: 443
- Certificate Verification: PASSED (Request to reissue a new Ruckus PKI certificate)
- PoE Operating Mode: AUTO
- Auto-provisioning?:  Enabled  Disabled
- SmartCellGateway Agent?:  Enabled  Disabled
- Cloud Discovery Agent (FQDN):  Enabled  Disabled
- Set Controller Address (Reboot to take effect):  Enabled  Disabled

Buttons at the bottom include 'Update Settings' and a link to 'Restore previous settings'. A red text message 'No Telnet & HTTP' is displayed in the center of the page.

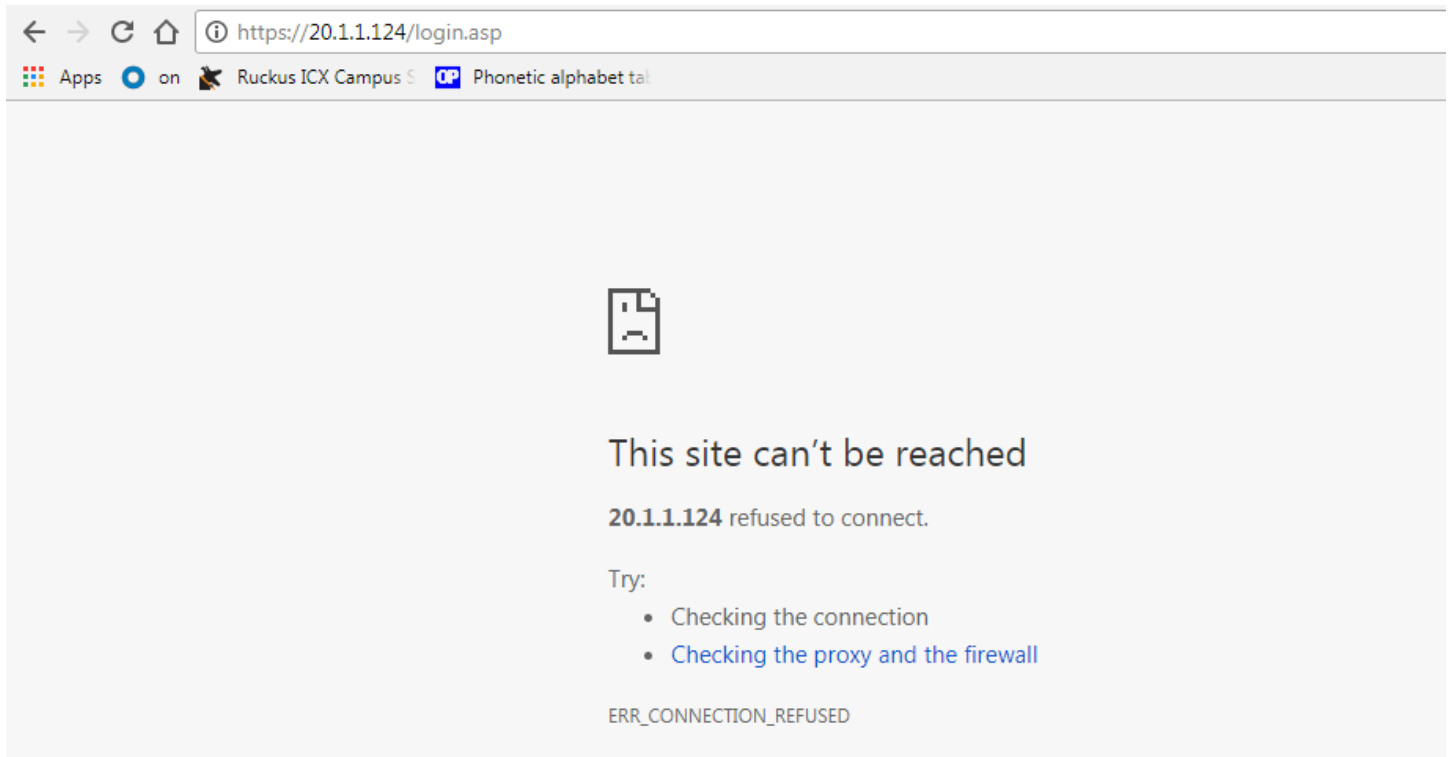
## Web Interface Access Through HTTPS Not Supported

The web interface through HTTPS is not accessible in FIPS mode when the AP has joined SmartZone.

## AP Configuration in FIPS Mode

AP Features Not Supported in FIPS Mode

**FIGURE 91** Web Access Through HTTPS Unavailable in FIPS Mode



## SNMPv1 and SNMPv2c Not Supported

SNMPv1 and SNMPv2c are not supported when FIPS mode is enabled. In FIPS mode, only SNMPv3 commands are included.

FIGURE 92 SNMPv3 Commands Allowed in FIPS Mode

```
rkscli: set snmp
Commands starting with 'set snmp' :
set snmp : set snmp {options}
           ->version <value>                SNMP version(v3)
           -- Modify SNMP Settings
set snmp-acl : set snmp-acl {options}
           -> {enable|disable}
           -> {add|del} <ipaddr>
           -> clear -- delete all entries
           -- Modify SNMP ACL Settings
set snmpv3 : set snmpv3 {options}
           ->ro username <name>,            SNMP v3 ro username
           ->ro auth <type>,                SNMP v3 auth type(SHA)
           ->ro auth-key <key>,            SNMP v3 auth key
           ->ro privacy <type>,            SNMP v3 privacy type(AES)
           ->ro privacy-key <key>,        SNMP v3 privacy key
           -----
           ->rw username <name>,            SNMP v3 ro username
           ->rw auth <type>,                SNMP v3 auth type(SHA)
           ->rw auth-key <key>,            SNMP v3 auth key
           ->rw privacy <type>,            SNMP v3 privacy type(AES)
           ->rw privacy-key <key>,        SNMP v3 privacy key
           -----
           ->trap {enable|disable},        SNMP V3 trap enable
           ->trap username <name>,        SNMP v3 trap username
           ->trap auth <type>,            SNMP v3 trap auth type(SHA)
           ->trap auth-key <key>,        SNMP v3 trap auth key
           ->trap privacy <type>,        SNMP v3 trap privacy type(AES)
           ->trap privacy-key <key>,    SNMP v3 trap privacy key
           ->trap-svr <ipaddr>,          SNMP V3 trap server ipaddr
           -- Modify SNMPv3 Settings
```

## WLAN Interface Up or Down from AP CLI Not Supported

When FIPS mode is enabled, you cannot set the WLAN interface state from the AP CLI.

FIGURE 93 WLAN Interface State Error Message.

```
rkscli: set state wlan33 up
Error: wlan33 state cannot be set 'up' with open network configuration in FIPS mode
rkscli: █
```

## Creating a WLAN WPA3 WLAN2/WPA3 Mixed Profile

Follow these steps to create a WLAN WPA3 WPA2/WPA3 mixed profile.

WPA3, WPA2/WPA3-Mixed and OWE are new WLAN service types added in this this release.

All the three WLAN types can be configured with

## AP Configuration in FIPS Mode

### Creating a WLAN WPA3 WLAN2/WPA3 Mixed Profile

Authentication Type 'Standard Usage' and Method 'Open'

Authentication Type 'Hotspot(WISPr)' and Method 'Open'

When WPA3 is selected, user has to configure SAE Passphrase. For WPA2/WPA3-Mixed, user has to configure Passphrase and SAE Passphrase respectively. For OWE (Opportunistic Wireless Encryption), encryption AES will be set automatically.

All three WLAN types support both Data tunnel n Non-tunnel WLAN traffic.

The configurations can be done following the steps below:

1. From the Wireless LANs zone, select the **Wireless LANS>Create WLAN Configuration> Encryption Option** for which you want to create a WLAN WPA3 WPA2/WPA3 profile.
2. Click **Create**, the Create WLAN Configuration page appears.
3. In the **Authentication Option**, select **standard usage/Hotspot(Wispr)** in Authentication Type and **Open** in **Method**.
4. Scroll down to the Encryption Options section.
5. In the **Encryption Option** field, select **WPA3**.

The screenshot shows the 'Create WLAN Configuration' window in the RUCKUS COMMScope interface. The window is titled 'Create WLAN Configuration' and has a close button (X) in the top right corner. On the left side, there is a navigation menu with the following items: Dashboard, System, Access Points, Switches, Wireless LANs (highlighted), Clients, Firewall, Services & Profiles, Report, Troubleshooting, Administration, and Events & Alarms. The main content area is divided into three sections: 'General Options', 'Authentication Options', and 'Encryption Options'. In the 'General Options' section, there are fields for Name, SSID, and Description, all of which are empty. There is also a 'Zone' dropdown menu set to '5.2.1.3.69' and a 'WLAN Group' dropdown menu set to 'default'. In the 'Authentication Options' section, there are four radio buttons for 'Authentication Type': 'Standard usage (For most regular wireless networks)' (selected), 'Hotspot (WISPr)', 'Hotspot 2.0 Access', and 'Hotspot 2.0 Onboarding'. Below these are three radio buttons for 'Method': 'Open' (selected), '802.1X EAP', and '802.1X EAP & MAC'. In the 'Encryption Options' section, there are four radio buttons for 'Method': 'WPA2', 'WPA3' (selected), 'WPA2/WPA3-Mixed', and 'OWE'. Below these are two radio buttons for 'Algorithm': 'AES' (selected) and another one that is not clearly visible. At the bottom of the window, there is a text input field for 'SAE Passphrase' and a '802.11w MFP' section with three radio buttons: 'Disabled', 'Capable', and 'Required' (selected). At the bottom right of the window, there are two buttons: 'OK' and 'Cancel'.

6. Enter **SAE Passphrase**, the SAE Passphrase should be minimum 8 characters in length and maximum 63 characters in length. (should only contain 1-9 numbers and A-F alphabets).
7. In the **Encryption Option**, select **WPA2**.



Enter **Passphrase**, the Passphrase should be minimum 8 characters in length and maximum 63 characters in length. (should only contain 1-9 numbers and A-F alphabets).

8. In the **Encryption Option**, select **WPA3**

Enter **SAE Passphrase**, the SAE Passphrase should be minimum 8 characters in length and maximum 63 characters in length. (should only contain 1-9 numbers and A-F alphabets).

**NOTE**

For WPA3, WPA2/WPA3 mixed configurations to be set, client should have access to WPA3 type.

## AP Configuration in FIPS Mode

### Creating a WLAN WPA3 WLAN2/WPA3 Mixed Profile

9. In the **Encryption Option**, select **WPA2/WPA3 Mixed**.

Enter **Passphrase** and **SAE Passphrase**, the Passphrase and SAE Passphrase should be minimum 8 characters in length and maximum 63 characters in length. (should only contain 1-9 numbers and A-F alphabets).

10. In the **Encryption Option**, select **OWE**

11. Save the configuration.

#### NOTE

WPA3, WPA2/WPA3 mixed configurations are not supported on 802.1X EAP and 802.1X EAP & MAC.

## Recovery SSID

Follow these steps for SSID recovery.

This enhancement is provided to make AP admin password available to federal release customers. Recovery SSID provides better security. SZ still needs to deliver the clear-text AP admin password to the AP. Recovery - SSID passphrase cannot be AP admin password in FIPS mode, so a custom passphrase is provided which is must, when recovery-ssid id is enabled.

By default, the Recovery SSID feature is disabled. Once the user enables it, the textbox is displayed. The user needs to input the passphrase. The validation rules of the passphrase should consider the Common Criteria and JITC requirement. The passphrase should be clear text stored in the database and deliver to the AP in GPB config via secure channel(SSH tunnel). The box is in clear text format as the passphrase is also used in WPA protocol.

1. AP page cannot override the recovery ssid or custom passphrase
2. AP group/page hide recovery ssid options.

After upgrade, Recovery SSID feature will be disabled. In the previous releases recovery ssid feature was malfunctioning due to the hashing of AP admin password and the AP side. The AP will not broadcast the ssid itself. Hence it is disabled and let the user enable it again, to make sure the functionality works as expected. Make sure all the APs receive the new config that disable Recovery SSID feature even those APs enabled previously..

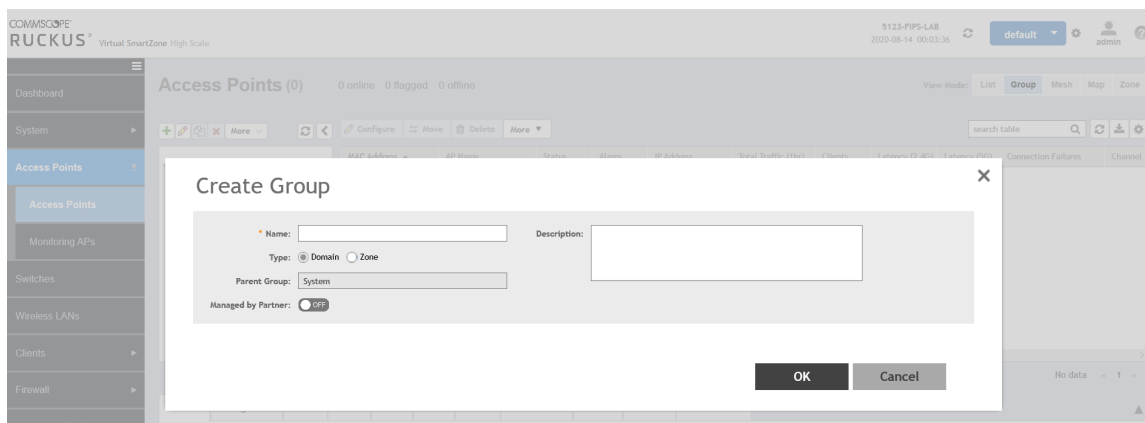
When AP loses connectivity from SmartZone and SmartZone Gateway, AP loses heartbeat (HB) and starts broadcasting the Recovery-SSID. Then user connects to the SSID and tries to recover or debug the issue.

If user has a console Access to AP, then Recovery-SSID can be identified as shown below:

```
wlan14      down    AP      wlan14    0      00:00:00:00:00:00 Wireless 14
recovery-ssid up      AP      wlan102   0      f0:3e:90:db:a7:7b Recover.Me-1BA770
wlan32      down    AP      wlan32    1      00:00:00:00:00:00 Wireless32
```

### GUI Configuration Page

1. Select the Access point tab.
2. Click **Create**, the Create Group page appears



3. Select the type **Zone** to configure.
4. In the **Advance Option** setting, Recovery SSID options is available.
5. Default Recovery SSID and custom passphrase filled will be in Disabled state.

## AP Configuration in FIPS Mode Recovery SSID

The screenshot shows the 'Create Group' configuration window in the RUCKUS interface. The 'Configuration' tab is active. Under the 'Recovery SSID' section, the 'Enable Broadcast' radio button is selected (ON), and the 'Custom Passphrase' radio button is selected (OFF). The 'Show' button next to the custom passphrase field is also disabled. The 'AP Reboot Timeout' is set to 30 minutes for gateway and 2 hours for controller. The 'Directed Multicast' section has three options: 'Multicast Traffic From Wired Client', 'Multicast Traffic From Wireless Client', and 'Multicast Traffic From Network', all of which are currently disabled (OFF).

6. Default Configuration of Recovery SSID can be enabled by clicking the ON/OFF button.

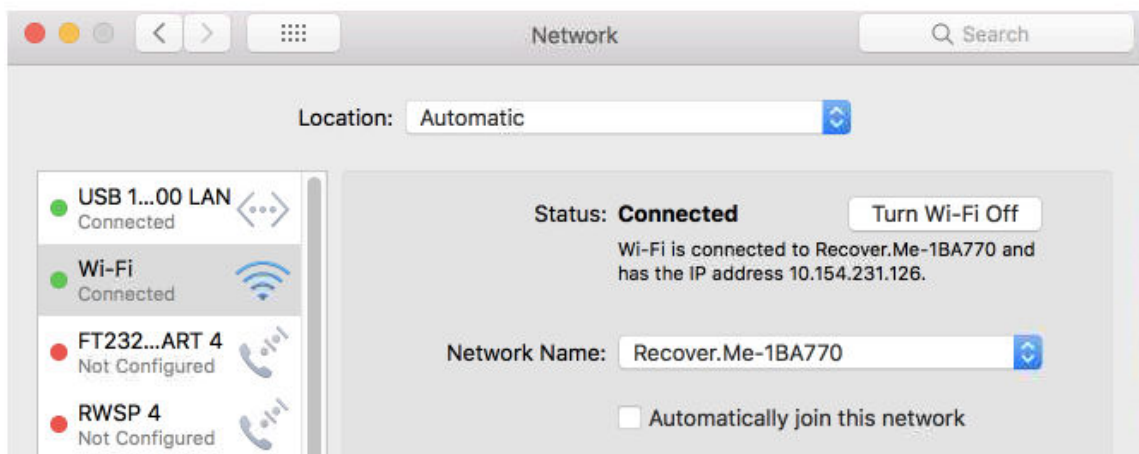
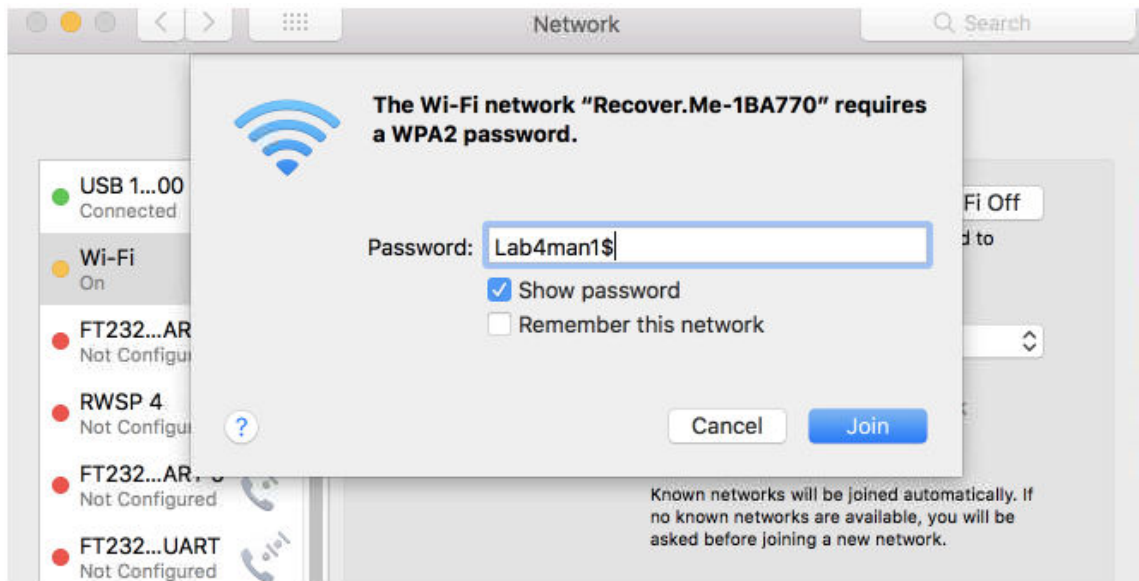
This screenshot is identical to the one above, showing the 'Create Group' configuration page. The 'Recovery SSID' section has 'Enable Broadcast' selected (ON) and 'Custom Passphrase' is disabled (OFF). The 'Show' button next to the custom passphrase field is also disabled. The 'AP Reboot Timeout' is set to 30 minutes for gateway and 2 hours for controller. The 'Directed Multicast' section has three options: 'Multicast Traffic From Wired Client', 'Multicast Traffic From Wireless Client', and 'Multicast Traffic From Network', all of which are currently disabled (OFF).

The "Show" option in the above image can let the user to see current passphrase, the design is just like another WLAN passphrase.

7. Enter **Custom Passphrase**, the Custom Passphrase should be 8-63 in characters (should only contain 1-9 , A-F). The Custom Passphrase should be different from the AP admin login password.
8. Configuration at the zone level is created.
9. Save the configuration.

How to connect to Recovery-SSID after AP loses its connectivity from SZ and its Gateway.

1. Configure a client with IP address 10.154.231.126 and connect to recovery-ssid with custom passphrase.



2. After successful connectivity, access the GUI as shown below:

The screenshot shows the web interface for a Ruckus T710 Multimedia Hotzone Wireless AP. The browser address bar shows `https://10.154.231.125/index.asp`. The page title is "Ruckus T710 Multimedia Hotzone Wireless AP".

**Status :: Device**

Device Name: RuckusAP  
Device Location:  
Coordinate Source: gps  
GPS Coordinates: 35.689501,139.691711  
PoE OUT Port: 'PoE OUT' port is disabled  
MAC Address: F0:3E:90:1B:A7:70  
Serial Number: 521504009382  
Software Version: 5.2.1.3.23  
Internal Temperature: 36(C) 96(F) Tue Jul 21 19:42:31 2020 (GMT)  
Uptime: 1 hr 28 mins 45 secs  
Current Time (GMT): Tue Jul 21 19:42:31 2020

**LAN Port Status** Refresh

Port	Interface	802.1X	Logical Link	Physical Link	Label
0	eth0	None	Up	Up 1000Mbps full	10/100/1000 PoE
1	eth1	None	Down	Down	10/100/1000
2	eth2	None	Down	Down	1000 SFP

**This AP is currently unable to provide wireless access. To resolve, connect to a Ruckus Controller. To function as a standalone AP, go to [Ruckus Support](#), navigate to the specific AP and download**

## SSH Public Key Authentication

Password authentication is known as less secure. However, it is the only authentication method for SZ remote administration via SSH. Public key authentication can provide cryptographic strength that even an extremely long and complex password cannot offer.

### SSH Public Key Authentication

This feature focuses on the SSH server on SZ/vSZ and this is a generic feature. No matter what the FIPS mode is, the SZ supports the SSH public key authentication. User "admin" can login to SZ Web GUI to configure up to **10 SSH public keys** and configure the SZ to use

- **Public key and password authentications (multi-factor)** : admin login with this combination has to pass public key and password authentications. SSH server authenticates the user with public key and follow by password. If user fails in public key or password authentication, the user is not authenticated and the connection breaks.
- **Public key authentication** : Admin login by public key authentication only.
- **Public key or password authentication** : Admin is authenticated by public key or password. User is authenticated either passing public key or password authentication.
- **Password authentication** : Admin login by password authentication only.

**Default AuthenticationMethod:** SSH login to SZ will be 'password' authentication. before n after setup procedure.

**Maximum Configurable Public Key:** Only 'admin' user can configure up to 10 public keys for SSH public key authentication with key format validation.

**Verification of Uploaded Public Key:** When admin user trying to upload/configure the SSH public key, SZ will prompt a notification if the key is invalid or duplicated

**Cluster Configuration:** The public key authentication method and the public keys, the configurations must be synchronized to all the nodes in the cluster

**Non-admin Accounts:** non-admin user cannot configure the SSH authentication methods or public keys settings.

**Weak Cryptographic Algorithms:** The public key that were generated by weak cryptographic algorithms, like DSA or ED25519 or RSA1.

**Uploaded Public Key Format:** When admin user trying to upload the SSH authentication public keys, SZ will prompt an error notification if the uploaded public key is not in SSH-format. The structure is "<algorithm> <key> [<comment>]", where the <key> part of the format is encoded with Base64. Although the format is not a standard in the cryptography world, but it is commonly adopted by most of the cloud applications. The comment part of the SSH-format public key is optional.

**Public Key Authentication Fail:**When admin user login from SSH and public key authentication fail, the failure count will not be increased. SSH client may try a lot of private keys for authentication, therefore, the public key authentication failure will not increase the authentication failure count on SZ

**Key Zeroization:** Those uploaded/configured public keys must be zeroized when the SZ FIPS mode changes from enable to disable, vice versa.

## Configuring SSH Authentication Method

1. In the controller web interface, navigate to GUI **Administration** > **Admin and Roles** > **Account Security** and choose AAH auth method.

FIGURE 94 Configuring SSH Authentication Method

The screenshot shows the 'Account Security' configuration page in the RUCKUS controller web interface. The left sidebar contains navigation options: Dashboard, System, Access Points, Switches, Wireless LANs, Clients, Firewall, Services & Profiles, Report, Troubleshooting, Administration (selected), and Admins and Roles. The main content area has tabs for Groups, Administrators, AAA, Access Control List, Account Security (selected), Session Management, and CAC/PIV Authentication. Under 'Global Security', there are settings for 'Captcha for Login' (OFF), 'Concurrent Session(s)' (OFF, 3 sessions), and 'Absolute Timeout Settings' (OFF, 30 minutes). The 'SSH Authentication Method' is highlighted with a red box and set to 'Public Key and Password'. Below this are 'Refresh', 'OK', and 'Cancel' buttons. The 'Account Security' section shows a table with columns for Name, Idle Timeout, Account Lockout, and Password Expiration. The 'System' account is listed with all these settings disabled.

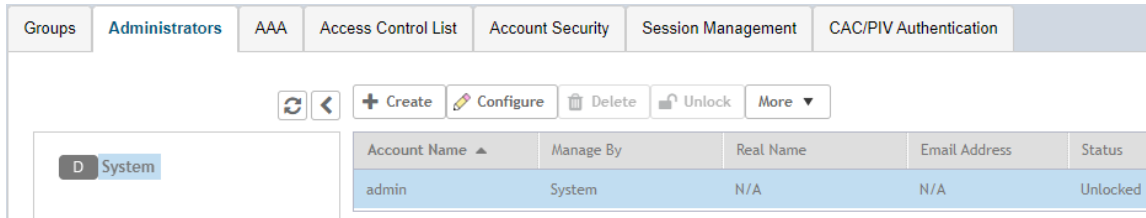
Name	Idle Timeout	Account Lockout	Password Ex
Default	Disabled	Disabled	Disabled

2. **Uploading SSH Authentication Public Keys**

Navigate to GUI>> Administration>> Admins and Roles>> Administrator

Choose 'admin' user and click on 'Configure'.

**FIGURE 95** Uploading SSH Authentication Public Keys





- 3. In 'admin' page navigate to 'SSH Keys' and click on Import button to upload the SSH Public Keys

FIGURE 96 Edit Administrator Account: Admin

## Edit Administrator Account: admin ✕

\* Account Name:

Real Name:

\* New Password:

\* Confirm New Password:

Phone:

Email:

Job Title:

Security Control ▶

**SSH Keys** ▼

Use SSH keys to connect simply and safely to CLI.

Label ▲	Key
<input type="text"/>	<input type="text"/>

FIGURE 97 Add Public Key

## Add Public Key



\* Key:

OK

Cancel

4. Enter the public key in the "Key" Textbox.
5. **ECDSA based public Key**

FIGURE 98 ECDSA Based Public Key

## Add Public Key



\* Key:

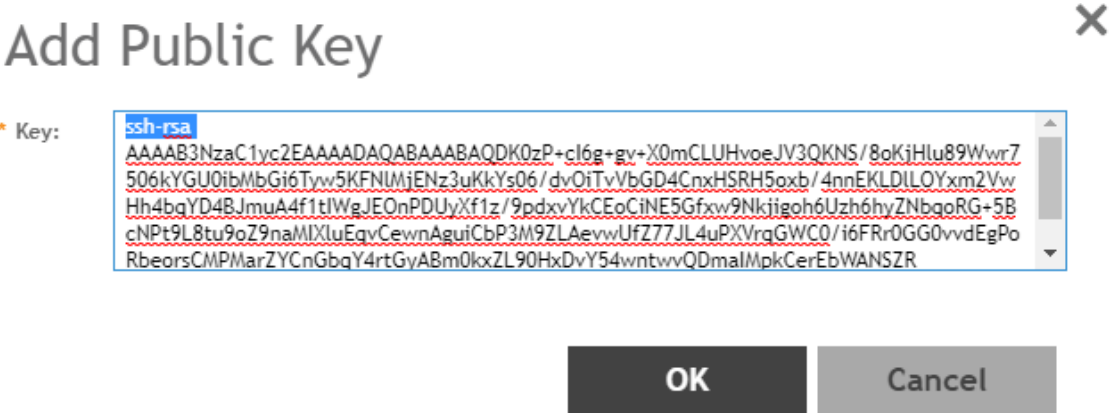
```
ecdsa-sha2-nistp256  
AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAIbmlzdHAyNTYAAABBBFRdOSEgcuAwrWDOMnX2rxLwU  
5qs0p6bM0XNfAbW8ZXfrUOVqCt4l/Fpf47ge+c10zuDTJUBNtEFhovZZDKDR60= ECDSA_keypair-1
```

OK

Cancel

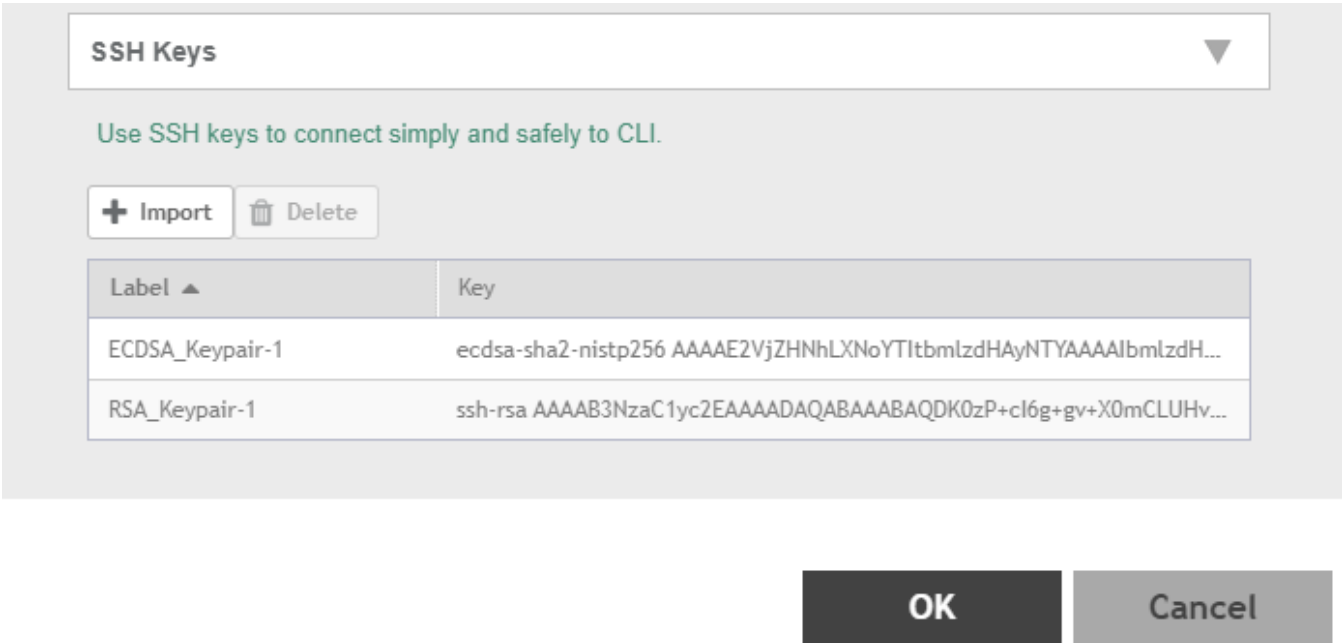
6. RSA based public Key

FIGURE 99 RSA Based Public Key



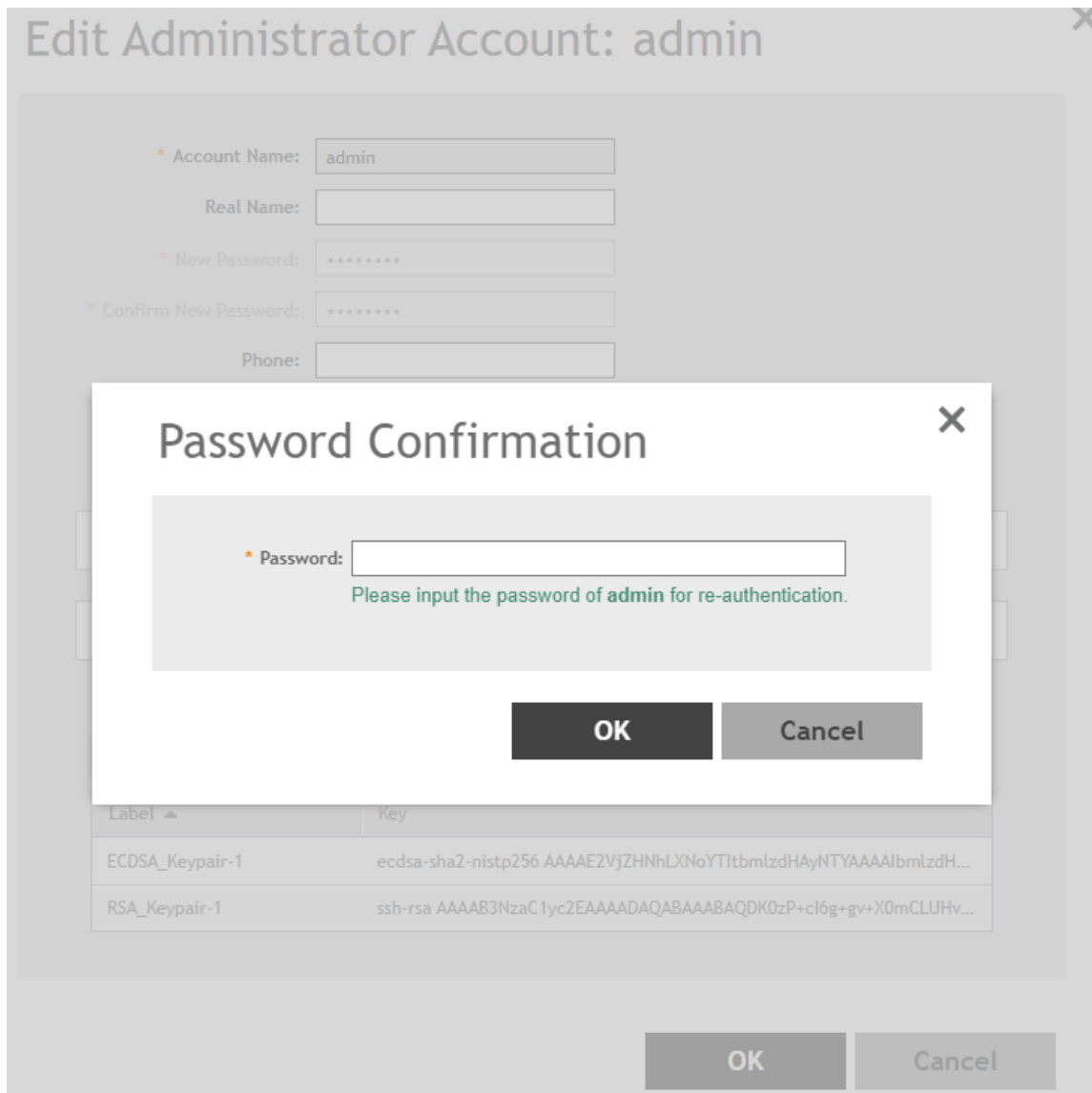
7. Uploaded Keys

FIGURE 100 Uploaded Keys



8. Click 'OK' button to save the uploaded keys. SZ will ask the admin user re-authentication to save the keys.

FIGURE 101 Password Confirmation for SSH Keys



SSH from Clients to SZ using each of the SSH public key Authentication

From any of the Linux machine user can generate RSA/ECDSA key pair [private n public]. Upload public key on SZ and use private key on the client from where SSH will be initiated towards SZ.

Use below command to generate key pair

- a. **ECDSA** `ssh-keygen -t ecdsa -C "ECDSA_Keypair-10" -f ecdsa1`

Files will be

1. **ecdsa1** Private key use in client
2. **ecdsa1.pub** Public key upload in SZ

b. **RSA > ssh-keygen -t rsa -C "RSA\_Keypair-1" -f rsa1**

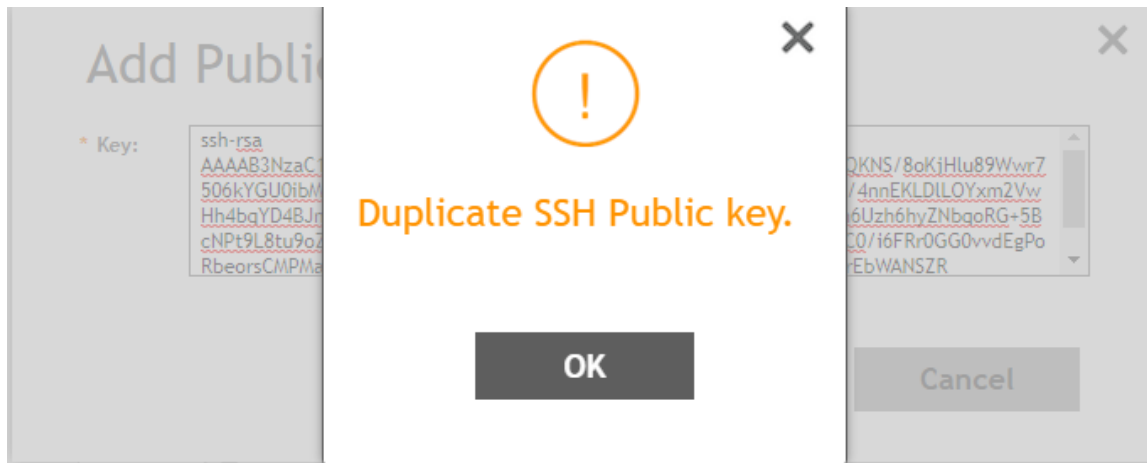
Files will be

1. **rsa1** Private key use in client
2. **rsa1.pub** Public key upload in SZ

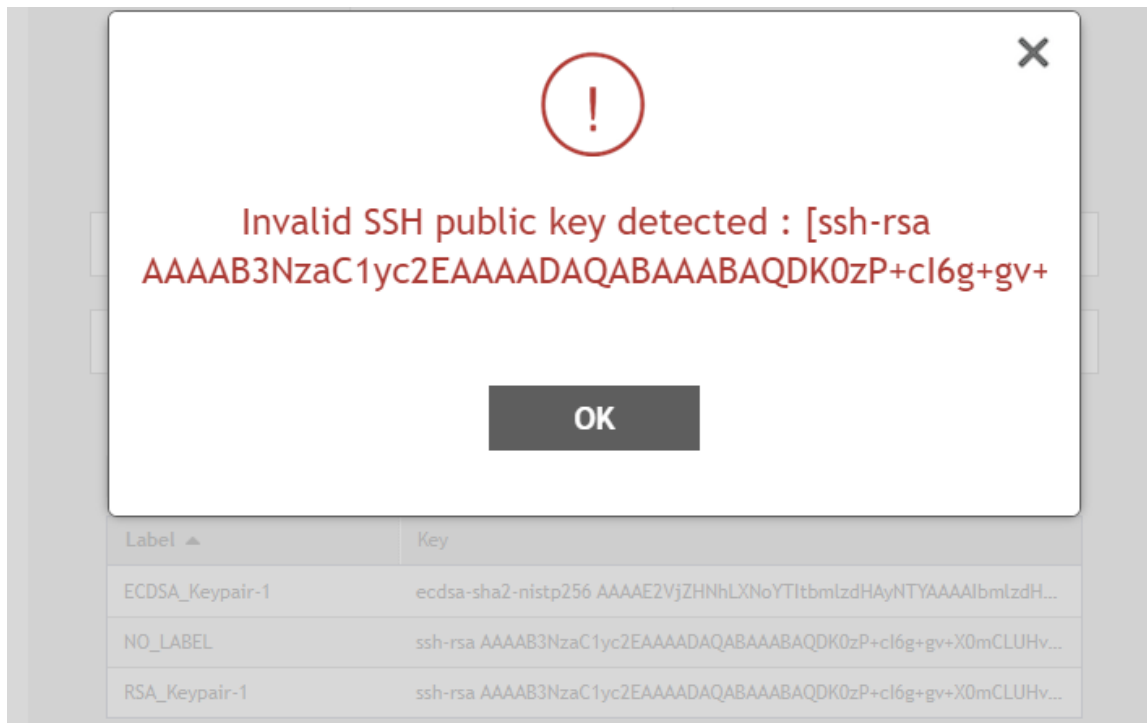
**Duplicate and Corrupt public keys Check during upload**

When admin user tries to upload the same/existing key GUI prompts an error dialogue

**FIGURE 102** Duplicate SSH Public Key



**FIGURE 103** Invalid SSH Public Key

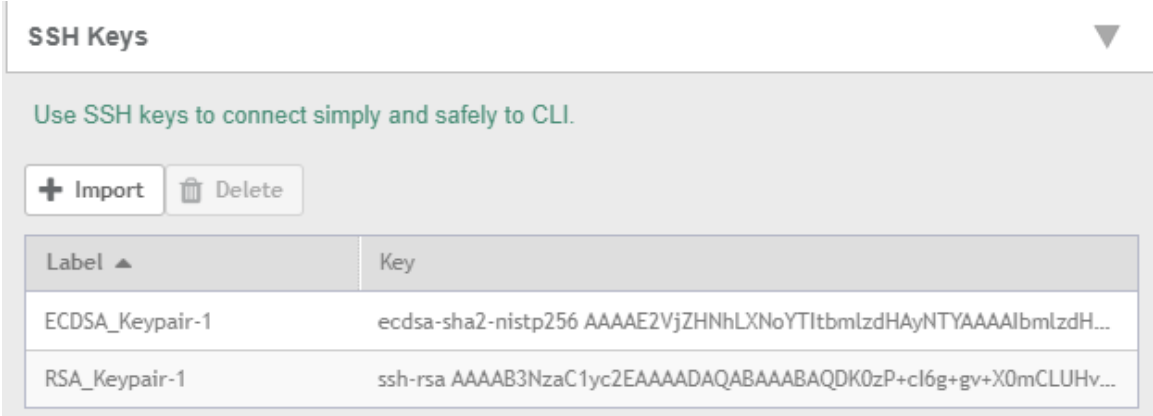


## Connecting to SZ using each of the methods from Linux Client

FIGURE 104 SSH Authentication Method Public Key and Password

\* SSH Authentication Method:  Password Only  Public Key Only  Public Key and Password  Public Key or Password

FIGURE 105 SSH Authentication Method Public Key and Password



1. **Public key and Password: Set the Authentication method and upload the public key**
  - a. Connect a client using ECDSA key based.

FIGURE 106 Connect a client using ECDSA key based

```
root@mahantesh:/home/mahantesh/Pubkeys/ECDSA# ssh -v -i ecdsa1 admin@10.174.89.149
OpenSSH_6.6.1, OpenSSL 1.0.1f 6 Jan 2014
debug1: Reading configuration data /etc/ssh/ssh_config
debug1: /etc/ssh/ssh_config line 19: Applying options for *
debug1: Connecting to 10.174.89.149 [10.174.89.149] port 22.
debug1: Connection established.
debug1: SSH2_MSG_SERVICE_REQUEST sent
debug1: SSH2_MSG_SERVICE_ACCEPT received
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
debug1: Authentications that can continue: publickey
debug1: Next authentication method: publickey
debug1: Offering ECDSA public key: ecdsa1
debug1: Server accepts key: pkalg ecdsa-sha2-nistp256 blen 104
debug1: key_parse_private2: missing begin marker
debug1: read PEM private key done: type ECDSA
Authenticated with partial success.
debug1: Authentications that can continue: password
debug1: Next authentication method: password
admin@10.174.89.149's password:
debug1: Authentication succeeded (password).
Authenticated to 10.174.89.149 ([10.174.89.149]:22).
debug1: channel 0: new [client-session]
debug1: Requesting no-more-sessions@openssh.com
debug1: Entering interactive session.
debug1: client_input_global_request: rtype hostkeys-00@openssh.com want_reply 0
debug1: Sending environment.
debug1: Sending env LANG = en_IN
Last successful login: 2020-08-19 13:52:54
Last successful login from: 10.174.89.254
Failed login attempts since last successful login: 0
Account privilege changes: No

Please wait. CLI initializing...

Welcome to the Ruckus Virtual SmartZone - High Scale Command Line Interface
Version: 5.2.1.3.1092

5113vSZ>
5113vSZ>
```

- b. Connect a client using RSA key based.



FIGURE 107 Connect a client using RSA key based

```
root@mahantesh:/home/mahantesh/Pubkeys/RSA# ssh -v -i rsa1 admin@10.174.89.149
OpenSSH_6.6.1, OpenSSL 1.0.1f 6 Jan 2014
debug1: Reading configuration data /etc/ssh/ssh_config
debug1: /etc/ssh/ssh_config line 19: Applying options for *
debug1: Connecting to 10.174.89.149 [10.174.89.149] port 22.
debug1: Connection established.
debug1: SSH2_MSG_SERVICE_REQUEST sent
debug1: SSH2_MSG_SERVICE_ACCEPT received
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
debug1: Authentications that can continue: publickey
debug1: Next authentication method: publickey
debug1: Offering RSA public key: rsa1
debug1: Server accepts key: pkalg ssh-rsa blen 279
debug1: key_parse_private2: missing begin marker
debug1: read PEM private key done: type RSA
Authenticated with partial success.
debug1: Authentications that can continue: password
debug1: Next authentication method: password
admin@10.174.89.149's password:
debug1: Authentication succeeded (password).
Authenticated to 10.174.89.149 ([10.174.89.149]:22).
debug1: channel 0: new [client-session]
debug1: Requesting no-more-sessions@openssh.com
debug1: Entering interactive session.
debug1: client_input_global_request: rtype hostkeys-00@openssh.com want_reply 0
debug1: Sending environment.
debug1: Sending env LANG = en_IN
Last successful login: 2020-08-19 13:53:21
Last successful login from: 10.174.89.254
Failed login attempts since last successful login: 0
Account privilege changes: No
Please wait. CLI initializing...

Welcome to the Ruckus Virtual SmartZone - High Scale Command Line Interface
Version: 5.2.1.3.1092

5113vSZ>
```

2. **Public key and Password: Set the Authentication method and the public key is already uploaded.**

**FIGURE 108** Authentication method and the public key is already uploaded

\* SSH Authentication Method:  Password Only  Public Key Only  Public Key and Password  Public Key or Password

a. Connect a client using public key based

**FIGURE 109** Authentication method and the public key is already uploaded

```
root@mahantesh:/home/mahantesh/Pubkeys/RSA# ssh -v -i rsa1 admin@10.174.89.149
OpenSSH_6.6.1, OpenSSL 1.0.1f 6 Jan 2014
debug1: Reading configuration data /etc/ssh/ssh_config
debug1: /etc/ssh/ssh_config line 19: Applying options for *
debug1: Connecting to 10.174.89.149 [10.174.89.149] port 22.
debug1: Connection established.
debug1: SSH2_MSG_SERVICE_REQUEST sent
debug1: SSH2_MSG_SERVICE_ACCEPT received
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
debug1: Authentications that can continue: publickey,password
debug1: Next authentication method: publickey
debug1: Offering RSA public key: rsa1
debug1: Server accepts key: pkalg ssh-rsa blen 279
debug1: key_parse_private2: missing begin marker
debug1: read PEM private key done: type RSA
debug1: Authentication succeeded (publickey).
Authenticated to 10.174.89.149 ([10.174.89.149]:22).
debug1: channel 0: new [client-session]
debug1: Requesting no-more-sessions@openssh.com
debug1: Entering interactive session.
debug1: client_input_global_request: rtype hostkeys-00@openssh.com want_reply 0
debug1: Sending environment.
debug1: Sending env LANG = en_IN
Last successful login: 2020-08-19 15:08:47
Last successful login from: 10.45.239.79
Failed login attempts since last successful login: 0
Account privilege changes: No
Please wait. CLI initializing...

Welcome to the Ruckus Virtual SmartZone - High Scale Command Line Interface
Version: 5.2.1.3.1092

5113vSZ>
```

b. Connect a client using password.

FIGURE 110 Connect a Client Using Password

```
root@mahantesh:/home/mahantesh/Pubkeys/ECDSA# ssh -v -j ecdsa1 admin@10.174.89.149
OpenSSH_6.6.1, OpenSSL 1.0.1f 6 Jan 2014
debug1: Reading configuration data /etc/ssh/ssh_config
debug1: /etc/ssh/ssh_config line 19: Applying options for *
debug1: Connecting to 10.174.89.149 [10.174.89.149] port 22.
debug1: Connection established.
debug1: SSH2_MSG_SERVICE_REQUEST sent
debug1: SSH2_MSG_SERVICE_ACCEPT received
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
debug1: Authentications that can continue: publickey
debug1: Next authentication method: publickey
debug1: Offering ECDSA public key: ecdsa1
debug1: Server accepts key: pkalg ecdsa-sha2-nistp256 blen 104
debug1: key_parse_private2: missing begin marker
debug1: read PEM private key done: type ECDSA
debug1: Authentication succeeded (publickey).
Authenticated to 10.174.89.149 ([10.174.89.149]:22).
debug1: channel 0: new [client-session]
debug1: Requesting no-more-sessions@openssh.com
debug1: Entering interactive session.
debug1: client_input_global_request: rtype hostkeys-00@openssh.com want_reply 0
debug1: Sending environment.
debug1: Sending env LANG = en_IN
Last successful login: 2020-08-19 15:17:32
Last successful login from: 10.174.89.254
Failed login attempts since last successful login: 0
Account privilege changes: No
Please wait. CLI initializing...

Welcome to the Ruckus Virtual SmartZone - High Scale Command Line Interface
Version: 5.2.1.3.1092

5113vSZ>
```

3. **Public key: Set the Authentication method and the public key are already uploaded.**

FIGURE 111 Add Public Key Only

\* SSH Authentication Method:  Password Only  Public Key Only  Public Key and Password  Public Key or Password

- a. Connect a client using public key based

FIGURE 112 Connect a client using public key based

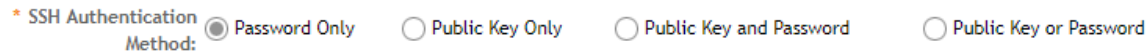
```
root@mahantesh:/home/mahantesh/Pubkeys/ECDSA# ssh -v -j ecdsa1 admin@10.174.89.149
OpenSSH_6.6.1, OpenSSL 1.0.1f 6 Jan 2014
debug1: Reading configuration data /etc/ssh/ssh_config
debug1: /etc/ssh/ssh_config line 19: Applying options for *
debug1: Connecting to 10.174.89.149 [10.174.89.149] port 22.
debug1: Connection established.
debug1: SSH2_MSG_SERVICE_REQUEST sent
debug1: SSH2_MSG_SERVICE_ACCEPT received
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
debug1: Authentications that can continue: publickey
debug1: Next authentication method: publickey
debug1: Offering ECDSA public key: ecdsa1
debug1: Server accepts key: pka1g ecdsa-sha2-nistp256 blen 104
debug1: key_parse_private2: missing begin marker
debug1: read PEM private key done: type ECDSA
debug1: Authentication succeeded (publickey).
Authenticated to 10.174.89.149 ([10.174.89.149]:22).
debug1: channel 0: new [client-session]
debug1: Requesting no-more-sessions@openssh.com
debug1: Entering interactive session.
debug1: client_input_global_request: rtype hostkeys-00@openssh.com want_reply 0
debug1: Sending environment.
debug1: Sending env LANG = en_IN
Last successful login: 2020-08-19 15:17:32
Last successful login from: 10.174.89.254
Failed login attempts since last successful login: 0
Account privilege changes: No
Please wait. CLI initializing...

Welcome to the Ruckus Virtual SmartZone - High Scale Command Line Interface
Version: 5.2.1.3.1092

5113vSZ>
```

4. Password: Set the Authentication method and the public key is already uploaded.

FIGURE 113 Add Password Only



a. Connect a client using password

FIGURE 114 Connect a client using password

```
root@mahantesh:/home/mahantesh/Pubkeys/ECDSA# ssh -v admin@10.174.89.149
OpenSSH_6.6.1, OpenSSL 1.0.1f 6 Jan 2014
debug1: Reading configuration data /etc/ssh/ssh_config
debug1: /etc/ssh/ssh_config line 19: Applying options for *
debug1: Connecting to 10.174.89.149 [10.174.89.149] port 22.
debug1: Connection established.
debug1: SSH2_MSG_SERVICE_REQUEST sent
debug1: SSH2_MSG_SERVICE_ACCEPT received
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
debug1: Authentications that can continue: password
debug1: Next authentication method: password
admin@10.174.89.149's password:
debug1: Authentication succeeded (password).
Authenticated to 10.174.89.149 ([10.174.89.149]:22).
debug1: channel 0: new [client-session]
debug1: Requesting no-more-sessions@openssh.com
debug1: Entering interactive session.
debug1: client_input_global_request: rtype hostkeys-00@openssh.com want_reply 0
debug1: Sending environment.
debug1: Sending env LANG = en_IN
Last successful login: 2020-08-19 15:22:53
Last successful login from: 10.174.89.254
Failed login attempts since last successful login: 0
Account privilege changes: No
Please wait. CLI initializing...

Welcome to the Ruckus Virtual SmartZone - High Scale Command Line Interface
Version: 5.2.1.3.1092

5113vSZ>
```



# X.509 Certificates

---

- [Generating Certificate Signing Request \(CSR\).....](#) 115
- [Configuring X.509 Server Certificates on the Controller.....](#) 116
- [Validating Certificates.....](#) 120
- [Uploading X.509 Certificates on AP.....](#) 122
- [Uploading X.509 Certificates on vSZ-D.....](#) 124

X.509 Certificates allows you to upload the CA certificates for the AP and the dataplane, verify the certificates, and validate the server certificates of the SmartZone controller.

Typically, the AP is deployed in two phases: the staging phase and the production phase. In the staging phase, the entire CA certificate chain of the production SZ server certificate and any other certificate validation settings are configured on the AP. After the AP goes to the production phase, the certificate validation and verification is completed.

## Generating Certificate Signing Request (CSR)

If you do not have an SSL certificate, you will need to create a certificate signing request (CSR) file and send it to an SSL certificate provider to purchase an SSL certificate.

To create a CSR file:

1. From the application select, **System > Certificates > CSR**.
2. Click **Generate**, the Generate CSR form appears.
3. Enter the following details:
  - **Name**—A name for this CSR.
  - **Description**— A short description for this CSR.
  - **Common Name**—A fully qualified domain name of your Web server. This must be an exact match (for example, **www.ruckuswireless.com**).
  - **Email**—An email address (for example, **joe@ruckuswireless.com**).
  - **Organization**—Complete legal name of your organization (for example, **Google, Inc.**). Do not abbreviate your organization name.
  - **Locality/City**—City where your organization is legally located (for example, **Sunnyvale**).
  - **State/Province**—State or province where your organization is legally located (for example, **California**) Do not abbreviate the state or province name.
4. Select the **Country**
5. Click **OK**, the controller generates the certificate request. When the certificate request file is ready, your web browser automatically downloads it.
6. Go to the default download folder of your Web browser and locate the certificate request file. The file name is **myreq.zip**.
7. Use a text editor (for example, Notepad) to open the certificate request file.
8. Go to the website of your preferred SSL certificate provider, and then follow the instructions for purchasing an SSL certificate.
9. When you are prompted for the certificate signing request, copy and paste the entire content of myreq.csr, and then complete the purchase.
10. After the SSL certificate provider approves your CSR, you will receive the signed certificate via email.







2. Select **Systems > Certificates > SZ as a Client Certificate** and upload the client certificate.

**FIGURE 116** Importing Client Certificate

Dashboard Certificate to Service Mapping CSR SZ as a Server Certificate **SZ as Client Certificate** SZ Trusted CA Certificates/Chain (external) AP Certificate Replacement Intra system (AP/SZ-D) T

### Import Client Certificate

Name:   
Description:

Client Certificate

Client Certificate:   Browse Clear  
Private Key:   Browse Clear

Validate OK Cancel

The **Import Client Certificate** page is displayed. Configure the following items:

- Client Certificate: Browse and select the certificate.
- Private Key: Browse and select the key to upload.

Select **Clear** if you want to remove a certificate that you selected.

## X.509 Certificates

### Configuring X.509 Server Certificates on the Controller

3. Select **Systems > Certificates > SZ Trusted CA Certificates/Chain (external)** to validate the server certificates from RadSec/IPSec.

The screenshot shows the 'Edit CA Chain Certificates: 4L\_subCAs' configuration window. The window title is 'Edit CA Chain Certificates: 4L\_subCAs'. The interface includes a sidebar on the left with navigation options: Dashboard, System, General Settings, AP Settings, Switch Settings, Cluster, Maps, Certificates (selected), Templates, Access Points, Switches, Wireless LANs, Clients, Applications, and Services & Profiles. The main content area has tabs for 'Certificate to Service Mapping', 'CSR', 'SZ as a Server Certificate', 'SZ as Client Certificate', and 'SZ Trusted CA Certificates/Chain (external)'. The configuration fields are as follows:

- Name:** 4L\_subCAs
- Description:** 4 Intermediate CAs
- Intermediate CA Certificates:** Three rows, each with a checkbox (checked), a text input field, and 'Browse' and 'Clear' buttons.
- Root CA Certificate:** One row with a checkbox (checked), a text input field, and 'Browse' and 'Clear' buttons.

Below the fields is a text area containing the following certificate details:

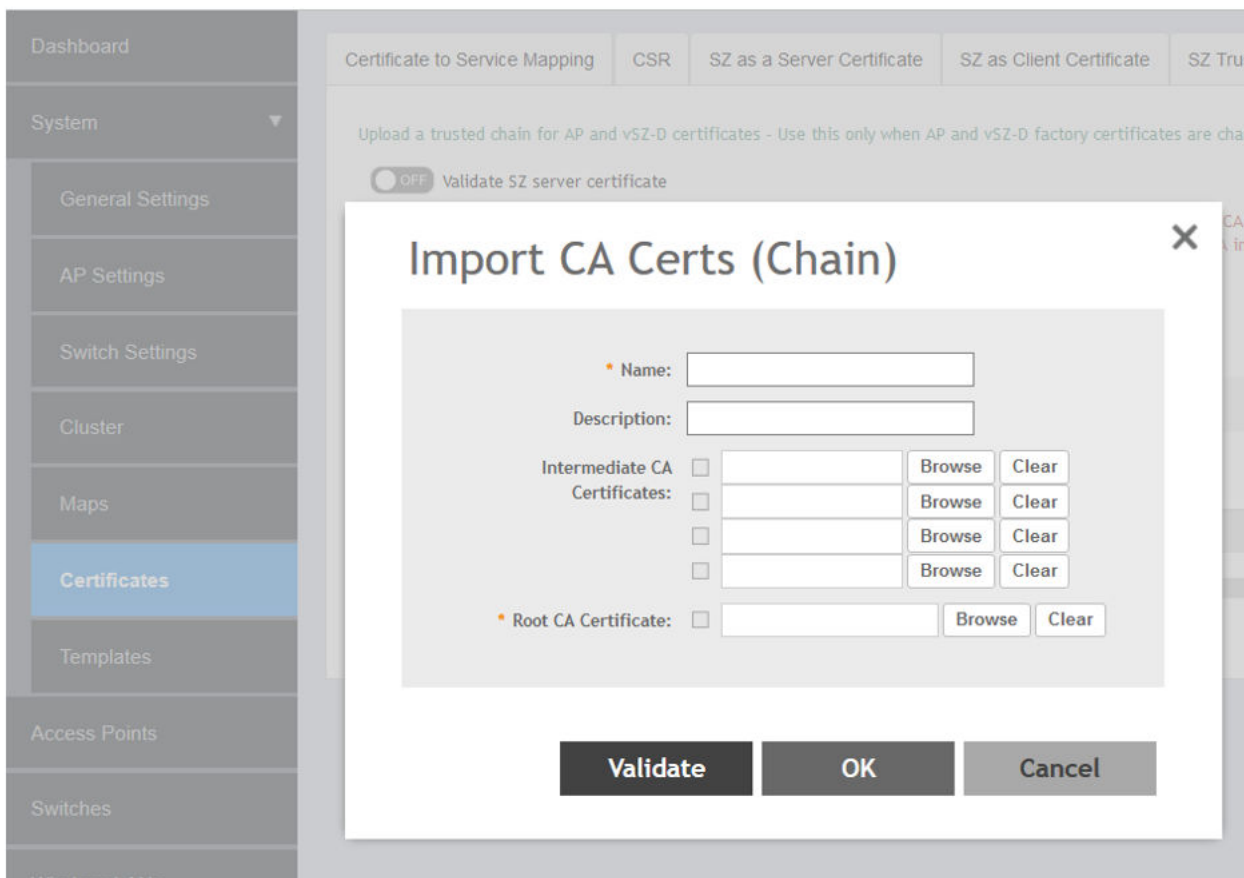
```
-----BEGIN INTERMEDIATE CERTIFICATE #1-----
[
  Version: V3
  Subject: EMAILADDRESS=intermediate01@ruckus.com, CN=1st, IntermediateCA,
  OU=FTQA Team, O=Comscope Ltd, ST=Karnataka, C=IN
  Signature Algorithm: SHA256withRSA, OID = 1.2.840.113549.1.1.11

  Key: Sun RSA public key, 4096 bits
  modulus:
  82708691118537840980215225898667375811895382100073008180376166749495831
  2418490360799555781151935564543372586632910942429212417850709686618241238
  922706912262946651474587461008386003833123702588526806957389820738805025
  41362854903111734734458536653951500596539849390733642018945722698474511
  900443644061688590489431259630332937599678015698510878517909576974807755
  9529489590376359685483353972119484025063516637861953289555566743978615801
  829507909667974520858847110734238599657578498056257052944196129235917638
```

At the bottom of the window are three buttons: 'Validate', 'OK', and 'Cancel'.

- Under the **Upload CA and CA-Chain Certificates for internal (AP/vDP)** used to push these certificates AP and vDP for server certificate validation. Configure the following:

**FIGURE 117** Uploading CA and CA-Chain Certificates for internal (AP/vDP)



The **Import CA Certs (Chain)** page is displayed. Configure the following items:

- **Name:** Enter the name of the certificate chain
- **Description:** Enter a short description about the imported certificate.
- **Intermediate CA Certificate:** browse and select the certificate. You can select up to four certificates.
- **Root CA Certificate:** Browse and select the certificate.

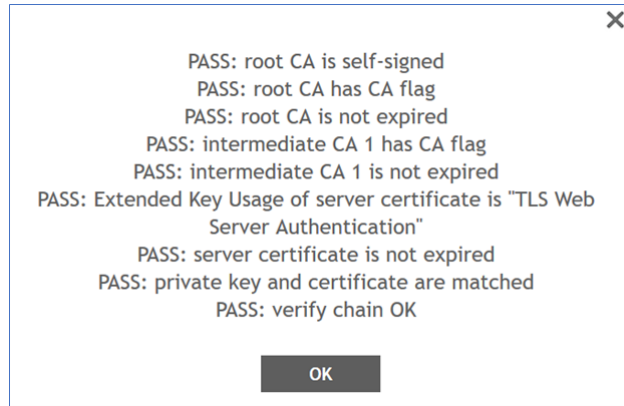
**NOTE**

You can select Clear if you want to remove a certificate that you selected.

5. Click **Validate**.

The results of the validation are displayed

**FIGURE 118** Validation Message



6. Click **OK**.

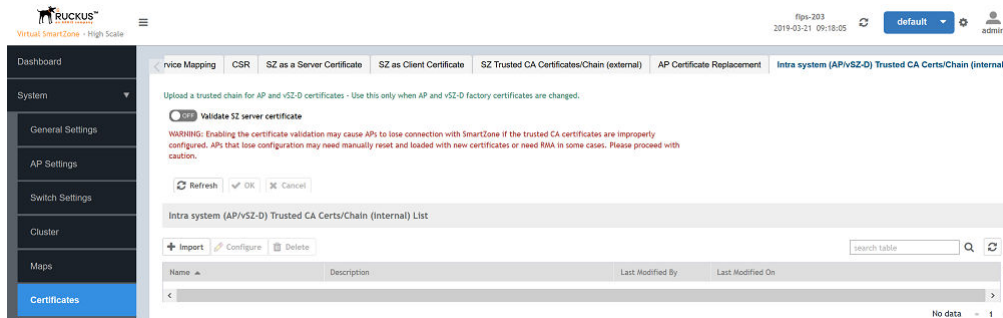
## Validating Certificates

You can validate CA certificates of the controller before assigning them to the AP.

1. **System > Certificates > Intra system (AP/vSZ-D) Trusted CA Certs/Chain (internal)**, and click **ON** to enable **Validate SZ Server Certificate** options.

This setting ensures the AP verifies and validates the server certificate of the controller. The AP or DP verifies if the SZ controller FQDN matches the DNS or common name of the SZ server certificate.

**FIGURE 119** Validating the Controller Server Certificates



2. From **Intra system (AP/vSZ-D) Trusted CA Certs/Chain (Internal) List**, click **Import**.

The **Import CA Certs (Chain)** page is displayed. Configure the following items:

- **Name:** Enter the name of the certificate chain
- **Description:** Enter a short description about the imported certificate.
- **Intermediate CA Certificate:** browse and select the certificate. You can select up to four certificates.
- **Root CA Certificate:** Browse and select the certificate.

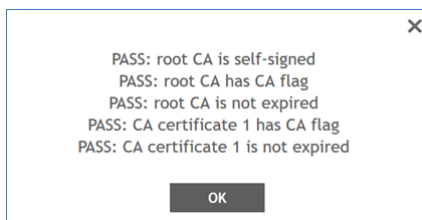
**NOTE**

You can select **Clear** if you want to remove a certificate that you selected.

3. Click **Validate**.

The results of the validation are displayed.

**FIGURE 120** Validation Message



## X.509 Certificates

### Uploading X.509 Certificates on AP

4. Click **OK**.

#### NOTE

When uploading the CA, the Sub-CA, Server Certificate, the Client Certificate and the Keys from the profiles **SZ as Server Certificate**, **SZ as Client Certificate**, **SZ Trusted CA Certificates/Chain (external)**, and **Intra system (AP/vSZ-D) Trusted CA Certs/Chain (internal)** if an error occurs an event is triggered. To know more about the event refer the **Events** section.

It takes some time for the certificate configurations to be applied to the AP. The AP must be turned off, moved to the production controller, and then powered on. The AP must be rediscovered by the controller. The discovery time is usually configured for 30 minutes. After this time, the AP establishes a connection with the controller. You can reconfigure this discovery time on the production controller to two hours from the controller interface (navigate to **Wireless LANs > Configure Group > Configuration > Advanced Options**). The settings highlighted must be configured for the same.

**FIGURE 121** Configuring AP Discovery Time

The screenshot shows the 'Configure Group' configuration page. The 'Name' field is set to 'aaaaaa' and the 'Type' is 'Zone'. Under the 'Configuration' tab, there are sections for '2.4 GHz Radio' and '5 GHz Radio', each with a 'Client Admission Control' toggle set to 'On'. Below these, the 'Protection Mode' for the 2.4 GHz radio is set to 'CTS ONLY'. At the bottom, the 'AP Reboot Timeout' section is highlighted with a red box, showing two dropdown menus: 'Reboot AP if it cannot reach default gateway after:' set to '30 minutes' and 'Reboot AP if it cannot reach the controller after:' set to '2 hours'. A 'Venue Code' field is also visible at the bottom.

## Uploading X.509 Certificates on AP

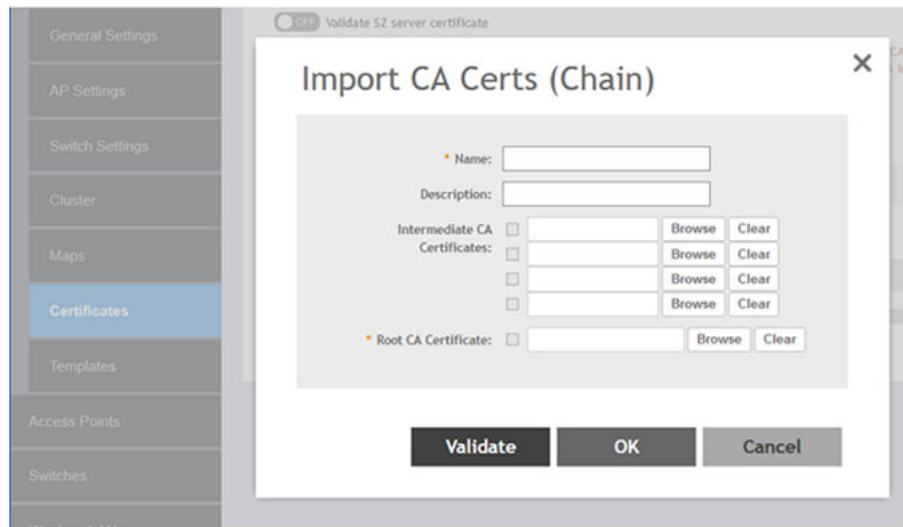
You can upload X.509 certificates to the AP using either SZ GUI or through CLI.

**NOTE**

It is not recommended to upload the certificates through AP CLI.

1. Click **System > Certificates > Intra system (AP/vSZ-D) Trusted CA Certs/Chain (internal)** to upload the CA/CA-chain certificates to the controller.

**FIGURE 122** Uploading CA/CA-chain certificate



2. Click **Validate**.

**FIGURE 123** Enabling Server Certificate Validation AP

Upload a trusted chain for AP and vSZ-D certificates - Use this only when AP and vSZ-D factory certificates are changed.

Validate SZ server certificate

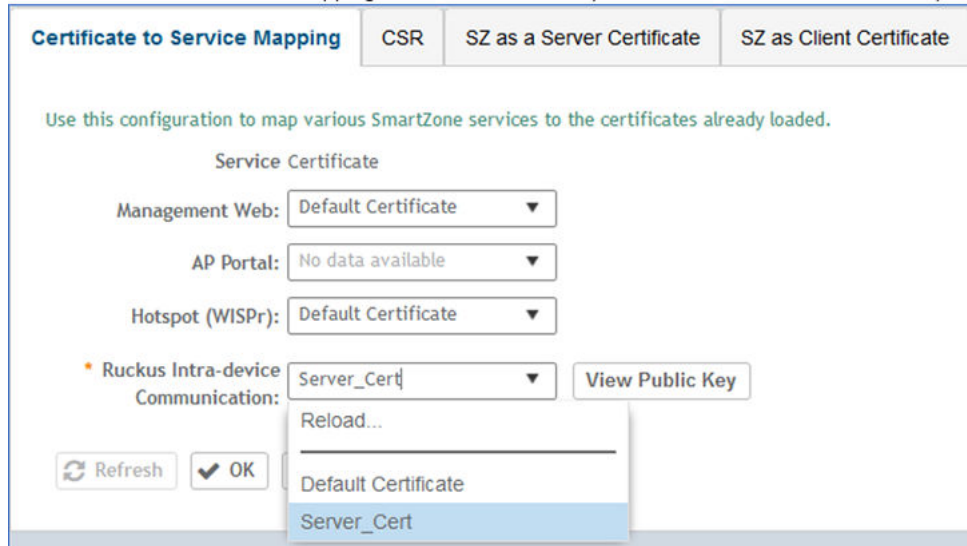
**WARNING:** Enabling the certificate validation may cause APs to lose connection with SmartZone if the trusted CA certificates are improperly configured. APs that lose configuration may need manually reset and loaded with new certificates or need RMA in some cases. Please proceed with caution.

## X.509 Certificates

### Uploading X.509 Certificates on vSZ-D

3. Select **Systems > Certificates > Certificate to Service Mapping**, and map the service certificate for AP-to-controller and & AP-to-dataplane communication by selecting the service certificate from the **Ruckus Intra-device Communication** list

FIGURE 124 Mapping Service Certificates



4. You can also upload certificate through CLI .

FIGURE 125 Uploading Certificate through AP CLI

```
rksccli: set scg dl-ctrlr-ca ctrlr_ca_cert 192.168.11.37 69 tftp
Updating controller CA cert ...
This is ARM platform
"reason"=" Manual FW update initiated"
v54_fw_update: download 192.168.11.37 section=ctrlr_ca_cert image=Image2 ctl_file=ctrlr_ca_cert (/writable/fw/cert/ctrlr_ca_cert.cnt1)
New controller ca certificates written to file
"reason"=" Manual FW:none update successful"
**/usr/bin/fw(3919) : Completed
"reason"=" rsm_fw_update(FW_TYPE_TDTS_RULE) ret=1 Successful update"
Update controller CA cert successfully.
rksccli:
rksccli: set scg dl-ctrlr-ca ctrlr_ca_cert 192.168.11.37 69 tftp
Updating controller CA cert ...
This is ARM platform
"reason"=" Manual FW update initiated"
v54_fw_update: download 192.168.11.37 section=ctrlr_ca_cert image=Image2 ctl_file=ctrlr_ca_cert (/writable/fw/cert/ctrlr_ca_cert.cnt1)
New controller ca certificates written to file
"reason"=" Manual FW:none update successful"
**/usr/bin/fw(3937) : Completed
"reason"=" rsm_fw_update(FW_TYPE_TDTS_RULE) ret=1 Successful update"
Update controller CA cert successfully.
rksccli:
```

## Uploading X.509 Certificates on vSZ-D

You can upload X.509 certificates to the vSZ-D either during initial setup or after initial setup through CLI.

1. Get contents of the *ca.pem* file, and copy the contents (from "Begin" to "End").







7. You can validate the CA certificate using the CLI

```
vDP-242(config-controller)# verify_cert_chain

vDP-242(config-controller)# ip scg.ruckuswireless.com
The command was executed successfully.
To save the changes, type 'end'.

vDP-242(config-controller)# exit

You have upload cert chain!
please type "end " to proceed end
Do you really want to exit (y/n) n
vDP-242(config-controller)# end

Server certificate chain upload was done!
Please reboot to take effect!
Save changes, and then exits the config context.

vDP-242# reboot
```

**NOTE**

For the RadSec server, SZ does not verify any identifier of the server certificate and therefore no configuration parameter is required.



# Management Certificate Check

---

- System Behaviour..... 129
- Viewing the Default Certificate using Controller Web Interface..... 129
- Modifying and Re-generating the Default Certificate using CLI..... 132

Management certificate check feature introduced in this release checks on the validity period or tracks the related operation change. This is specific to the controller (SmartZone) default server certificates especially for TLS server certificates in iOS 13 and macOS 10.15. This check shortens the validity period of the controller (SmartZone) certificates to a maximum of **825** days and a minimum of 124 days. This feature makes sure that the client can access the controller web user interface.

## System Behaviour

- If the user manually renews the default server certificate with a specific validity period in CLI mode and if the certificate is renewed automatically in the web user interface the next time, the controller will apply the previous validity period to generate default server certificate.
- The system automatically regenerates the default server certificate. Seven day prior to expiration a warning is displayed on the dashboard. This applies for third party user certificates.
- The validity period can be set to a minimum of 124 days (approximately four months) to a maximum of 1098 days (approximately three years).
- The controller renews the certificate with a default validity period 824 days if the user does not specify otherwise.

You can add the server certificate validity through the controller web user interface and or through CLI mode.

## Viewing the Default Certificate using Controller Web Interface

To view the Default certificate and Third party certificate perform the following steps.

## Management Certificate Check

Viewing the Default Certificate using Controller Web Interface

### NOTE

You cannot modify default certificate and the third party certificates from the controller web interface. To modify the default certificate for example, changing the day, you can make the changes in the CLI, the controller automatically renews the default certificate.

1. In the controller web interface, navigate to **System > Certificates > SZ as a Server Certificate**.

**FIGURE 126** Configuring and Checking the Default Certificate

The screenshot shows the RUCKUS Virtual SmartZone Essentials web interface. The top navigation bar includes the RUCKUS logo, the text 'Virtual SmartZone Essentials', the user 'admin', and the time '2020-08-14 11:54:45'. The main navigation menu on the left includes 'Dashboard', 'System', 'General Settings', 'AP Settings', 'Switch Settings', 'Cluster', 'Maps', 'Certificates', 'Templates', 'Access Points', 'Switches', and 'Wireless LANs'. The 'Certificates' section is active, and the sub-page is 'SZ as a Server Certificate'. The page title is 'Certificate to Service Mapping > CSR > SZ as a Server Certificate'. Below the title, there are tabs for 'Certificate to Service Mapping', 'CSR', 'SZ as a Server Certificate', 'SZ as Client Certificate', 'SZ Trusted CA Certificates/Chain (external)', 'AP Certificate Replacement', and 'Intra system (AP/VSZ-D) Trusted CA'. The main content area has a heading 'Use this configuration to upload a server certificate for SmartZone(SZ) itself.' and buttons for 'Import', 'Configure', and 'Delete'. Below this is a table with the following data:

Name	Description	Has Root CA	# of Inter Cert	Last Modified By	Last Modified On
Default Certificate	N/A	No	0	admin	2020/07/05 06:17:20

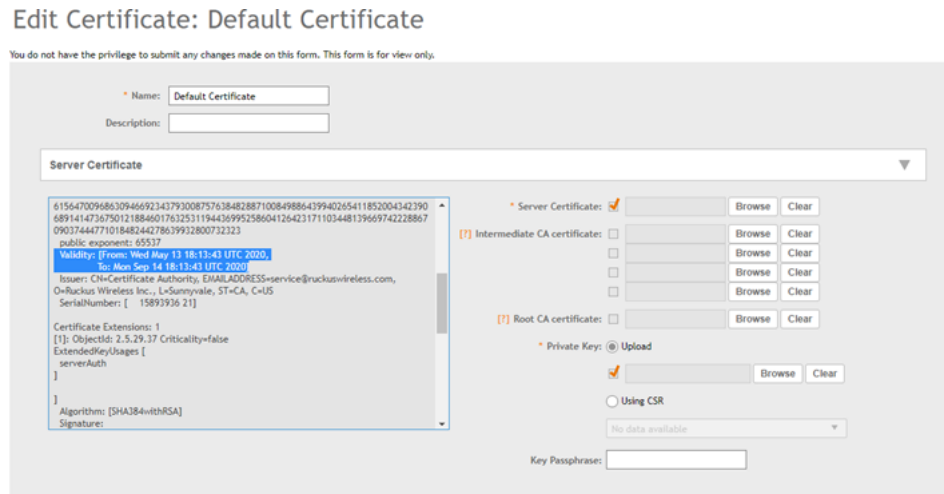
Below the table, there is a detailed view of the 'Default Certificate' with the following properties:

- Name: Default Certificate
- Description: N/A
- Has Root CA: No
- # of Inter Cert: 0
- Last Modified By: admin
- Last Modified On: 2020/07/05 06:17:20

- Click **Configure** to view the third-party and the default certificate validity period.

The **Edit Certificate** page is displayed.

**FIGURE 127** Viewing the Certificate Validity



**NOTE**

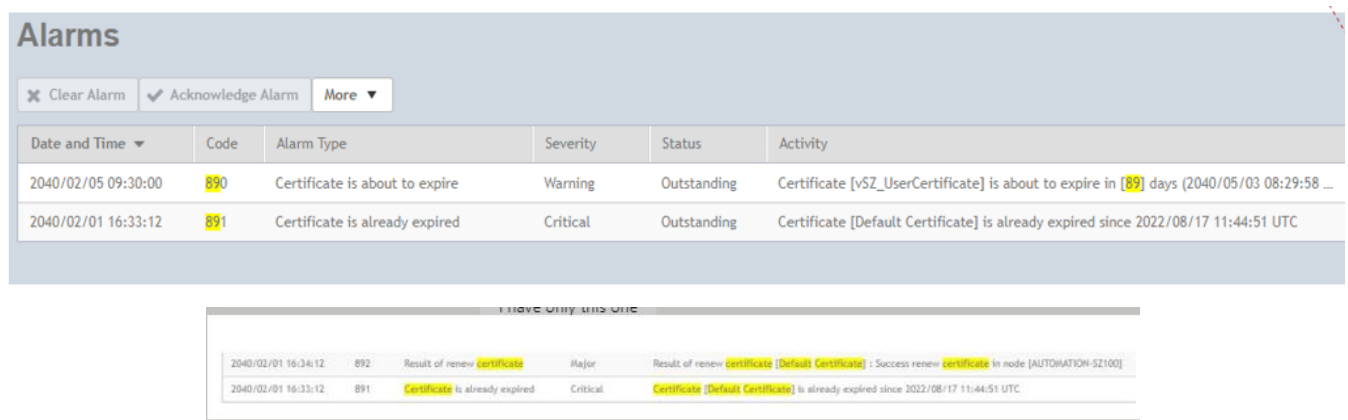
The third party certificates cannot be edited, you have to generate NEW one if want to modify the dates. Default Certificate validity can be modified using CLI by specifying the days ranging from 124 to 824.

- Click **Close**.
- The controller checks for valid certificates and triggers an alarm if the validity period is longer than 824 days. To view the alarm details, from the controller web interface, navigate to **Diagnostics > Events and Alarms >**

**NOTE**

Event 890 is thrown only for third party certificates.

**FIGURE 128** Viewing Events and Alarms

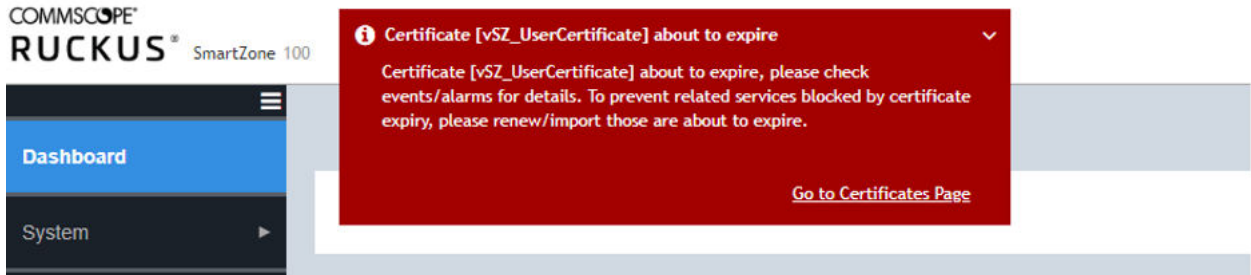


## Management Certificate Check

Modifying and Re-generating the Default Certificate using CLI

5. The controller dashboard displays the Global warning on certificate expiration.

**FIGURE 129** Global Warning on Certificate Expiration



## Modifying and Re-generating the Default Certificate using CLI

To modify and re-generate the server certificate through CLI, perform the following steps.

1. Login to CLI to set the validity for the **Default** server certificates.
2. In the configuration mode execute command **cert-store cert "Default Certificate" days <124 to 824>** to set the validity. The validity period can be set to a minimum of 124 days (approximately four months) to a maximum of 1098 days (approximately three years). After manually configuring the days for renewing the certificates, few of the services cannot be utilized for some time, but they resume within 7-10mins.



- To modify the default server certificate validity, execute the command `(config)# cert-store cert <days>`.

```
vSZ-01(config)# cert-store cert "Default Certificate"
```

```
vSZ-01(config-cert)# days
<days>      Expired days 124-1098, or default(824), works on Default Certificate only and other configuration will be ignored
vSZ-01(config-cert)# days 124
vSZ-01(config-cert)# end
```

```
vSZ-01_5213.339-F
0120: CD 05 00 F2 F5 2C A7 23 40 6E 9D 6C 23 EB ED CD .....#0n.l#...
0130: F0 FD F4 BC B9 55 E4 CA 4A 8F BE 2C DD AC 3D A3 .....U..J.....=
0140: 84 09 43 4A B6 2C 59 3B 97 7D E4 16 B6 4B 87 34 ..CJ.Y:....R.4
0150: B5 EB 2A 0E 53 D4 98 C5 21 8D 9F 4E DE 94 5E 70 ...S...t..N...^p
0160: 4C CB A8 FE 5D D4 A6 6C 7C 69 46 6F 0A CA 3E BB L...l..l..lFo...>
0170: 79 E2 4E CA DC 56 41 AE B3 75 E3 BE 8A BF ED 80 y.N..Ua..u.....

]
-----END CERTIFICATE-----

vSZ-01# config
vSZ-01(config)# cert-store cert "Default Certificate"
vSZ-01(config-cert)# days 123
% The last parameter should be between 124 and 1098 or default(824)
vSZ-01(config-cert)# days 124
vSZ-01(config-cert)# end
Do you want to update this context configuration? It will restart services because this certificate
used by Management Web or Hotspot. (or input 'no' to cancel)? [yes/no] yes

vSZ-01#
vSZ-01# show running-config cert-store cert "Default Certificate"
% Tomcat service error

vSZ-01# show service
```

No.	Application Name	Health Status	Log Level	# of Logs
1	AP Diagnostic Informati on			0
2	Cassandra	Online		4
3	Ccmd	Online	WARN	1
4	Collectd	Online		0
5	Communicator	Online	WARN	13
6	Configurer	Online	WARN	11

- Execute the command `show running-config cert-store cert` to view or check the certificate validity.

```
vSZ-01#
vSZ-01# show running-config cert-store cert
No. Name Description Has Root CA # of Inter Cert
-----
1 Default Certificat No 0
e

vSZ-01# show running-config cert-store cert "Default Certificate"
Name : Default Certificate
Description :
Server Certificate :
-----BEGIN CERTIFICATE-----
[
[
```



# Password Management

You can change the administrator password for AP and vSZ-D from the controller interface and from the command-line interface.

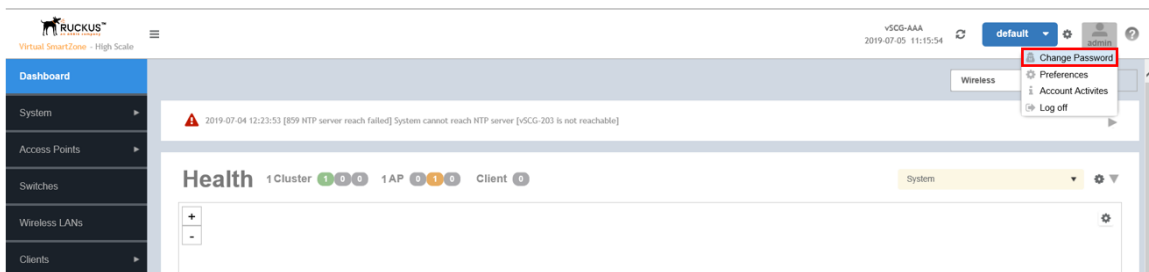
Passwords can be composed of any combination of uppercase and lowercase letters, numbers, and the following special characters: ! @ # \$ % ^ & \* ( ) - \_ = + [ ] { } ; ' " , < > / ?. (No other special characters are allowed.) The password length ranges from 8 to 64 characters.

The administrator login password of the AP zones is pushed from the controller. Therefore, the controller validates the administrator login password of AP zones before pushing it into the APs. The administrator login password of the dataplane is identical to that of the controller, so it need not be validated.

The administrator login password of the AP zones are pushed from the controller. Therefore, controller validates the admin login passwords length of AP zones before pushing them into APs. The administrator login password of the dataplane is identical to the controller so it need not be validated.

From the controller web interface, select **Admin > Change Password** to change the administrator password.

**FIGURE 130** Changing the Administrator Password



After the password is successfully changed, select **Administration > Admin Activities** to view the activity log. The account activity can be verified in the controller CLI by using the `/opt/ruckuswireless/wsg/log/web/activity.log` command.

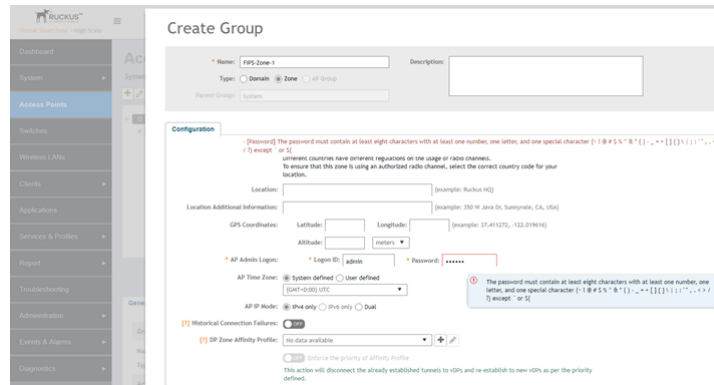
**FIGURE 131** Sample Verification Message

```
2019-02-05 05:41:21.564 Activity User [admin], Resource [10.32.139.171], Action [Log on], Resource [Administrator], Description [Administrator [admin] logged on from 10.32.139.171.]
2019-02-05 05:41:39.452 Activity User [admin], Resource [10.32.139.171], Action [Be authenticated], Resource [Administrator], Description [The user authentication is successful.]
2019-02-05 05:41:39.456 Activity User [admin], Resource [10.32.139.171], Action [Update], Resource [Administrator], Description [Administrator [admin] password changed.]
2019-02-05 05:41:39.456 Activity User [admin], Resource [10.32.139.171], Action [Update], Resource [Administrator], Description [Administrator [admin] updated.]
```

You can also configure the AP admin login password from **Access Points > Configure AP Zone** to configure the AP admin login password.. You can modify the settings for **AP Admin Logon**.

## Password Management

FIGURE 132 Modifying AP Admin Login



You can view changes to the data plane password from **System > Cluster- Data Planes > DP/vDP** . Click the **Event** tab to view the logs.

FIGURE 133 Dataplane Password Change Event Log

Name	DP Type	DP MAC Address	Data IP	Management/Co	Model	Serial Number	Firmware	Managed By	DP Status	Registration Stat
fips-vDP	External-Virtual	00:0C:29:6D:F5:90	20.1.91.203	10.1.200.41	v52-0	972032809...	5.1.1.0.222	fips-203	Managed	Approved

Date and Time	Code	Type	Severity	Activity
2019/01/04 15:34:41	504	Data plane configuration up...	Informational	Data plane [fips-vDP@97203280996A9V92L4N4Q4BRV000C296DF58000C296DF590] has been updated to dpciber configuration [4f3e6f0-0e81-1e9-82f4-00000a28a89].
2019/01/04 15:34:41	99203	Password Management	Informational	Data plane [97203280996A9V92L4N4Q4BRV000C296DF58000C296DF590] min password length changed, source: [DnsGUA], account: [admin].
2019/01/04 15:08:53	99214	Password Management	Informational	User logout to data plane [97203280996A9V92L4N4Q4BRV000C296DF58000C296DF590], source: [10.1.200.203], account: [admin].
2019/01/04 15:06:49	99205	Password Management	Informational	Data plane [97203280996A9V92L4N4Q4BRV000C296DF58000C296DF590] enable password changed, source: [10.1.200.203], account: [admin].
2019/01/04 15:05:50	99212	Password Management	Informational	User login into data plane [97203280996A9V92L4N4Q4BRV000C296DF58000C296DF590], source: [10.1.200.203], Account: [admin].
2019/01/04 15:05:42	99214	Password Management	Informational	User logout to data plane [97203280996A9V92L4N4Q4BRV000C296DF58000C296DF590], source: [10.1.200.203], account: [admin].
2019/01/04 15:05:40	99205	Password Management	Informational	Data plane [97203280996A9V92L4N4Q4BRV000C296DF58000C296DF590] enable password changed, source: [10.1.200.203], account: [admin].
2019/01/04 15:05:04	99205	Password Management	Informational	Data plane [97203280996A9V92L4N4Q4BRV000C296DF58000C296DF590] enable password changed, source: [10.1.200.203], account: [admin].

Refer to the *SmartZone Administrator Guide* for this release for more configuration information.

# Configuring the WLAN Scheduler

- [Setting the WLAN Scheduler from the CLI..... 138](#)

By configuring the WLAN scheduler, the controller can deny establishment of a wireless client session based on WLAN, time, day and so on. The controller can also control client access to the network by providing a time schedule within which the device can access the network. When the WLAN scheduler is disabled, SSID broadcasts are disabled and client connection is lost, including all clients that were connected earlier when the WLAN scheduler was enabled.

1. From the controller web interface, select **Wireless LANs** .
2. Select the zone for which you want to configure the WLAN scheduler and click the **Services** tab.
3. Select **WLAN Scheduler**.
4. Click **Create**.

The **Create Time SchedulesTable** page displays.

**FIGURE 134** Creating Time Schedules Table

General Options

\* Schedule Name:  ⓘ

Schedule Description:

Schedule Table

Time Zone: (GMT+0:00) UT1

	AM												PM										
Time	1	2	3	4	5	6	7	8	9	10	11	12	1	2	3	4	5	6	7	8	9	10	11
Sun																							
Mon																							
Tue																							
Wed																							
Thu																							
Fri																							
Sat																							

OK Cancel

5. Click **OK**.

The time schedule is configured.

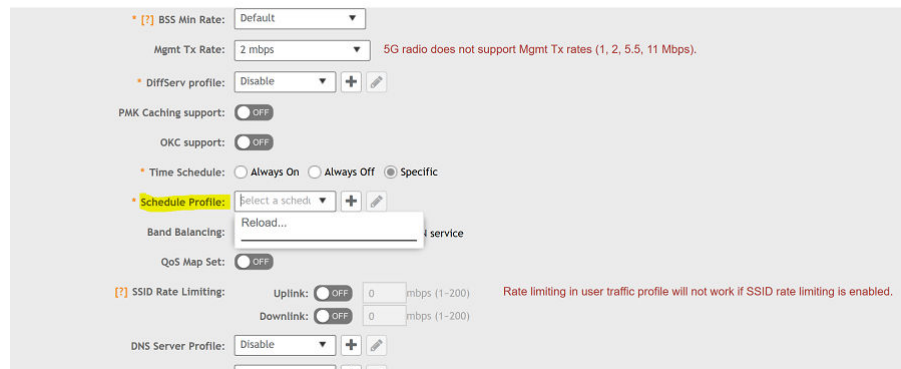
## Configuring the WLAN Scheduler

Setting the WLAN Scheduler from the CLI

- From the **Wireless LANs** page, select the scheduler profile from the **Advance Options** tab

**FIGURE 135** Selecting the Scheduler Profile

### Edit WLAN Config: 1@Eng\_Dar\_Man\_DBLBO\_Radsec



The screenshot shows the 'Edit WLAN Config' page for '1@Eng\_Dar\_Man\_DBLBO\_Radsec'. The 'Schedule Profile' dropdown menu is open, showing a list of profiles. The 'Schedule Profile' field is highlighted in yellow. Other configuration options visible include BSS Min Rate (Default), Mgmt Tx Rate (2 mbps), DiffServ profile (Disable), PMK Caching support (OFF), OKC support (OFF), Time Schedule (Always On, Always Off, Specific), Band Balancing (Reload...), QoS Map Set (OFF), and SSID Rate Limiting (Uplink and Downlink both OFF).

## Setting the WLAN Scheduler from the CLI

You can configure the WLAN scheduler from the command line interface as well.

- In the command prompt, go to the configuration issue the commands as shown in the figure.

**FIGURE 136** Sample Commands to Configure WLAN Scheduler from CLI

```
VSZ-206(config)# zone zone206
VSZ-206(config-zone)# wlan-scheduler 802.1x
VSZ-206(config-zone-wlan-scheduler)# schedule-data thur 01:15 02:30
VSZ-206(config-zone-wlan-scheduler)# exit
Do you want to save this context configuration (or input 'no' to cancel)? [yes/no] yes
VSZ-206(config-zone)# exit
Do you want to update this context configuration (or input 'no' to cancel)? [yes/no] yes
```

- To verify that the WLAN scheduler is configured, log in to the AP.
- Go to the **RKSLI** mode



## Configuring the WLAN Scheduler

### Setting the WLAN Scheduler from the CLI

FIGURE 139 WLAN down in AP and Not Broadcasting After the Scheduled Time

```
rksccli: get wlanlist
-----
name      status  type  wlanID  radioID  bssid          ssid
-----
wlan0     down   AP    wlan0   0         00:00:00:00:00:00  IgEng_Dar_Sz300_IPV6
wlan1     down   AP    wlan1   0         00:00:00:00:00:00  Wireless1
wlan2     down   AP    wlan2   0         00:00:00:00:00:00  Wireless3
wlan3     down   AP    wlan3   0         00:00:00:00:00:00  Wireless4
wlan4     down   AP    wlan4   0         00:00:00:00:00:00  Wireless5
wlan5     down   AP    wlan5   0         00:00:00:00:00:00  Wireless6
wlan6     down   AP    wlan6   0         00:00:00:00:00:00  Wireless7
wlan7     down   AP    wlan7   0         00:00:00:00:00:00  Wireless8
wlan100   down   MON   wlan100 0         00:00:00:00:00:00
recovery-ssid down   AP    wlan102 0         00:00:00:00:00:00  Recover_Me-07C270
wlan32    down   AP    wlan32   1         00:00:00:00:00:00  IgEng_Dar_Sz300_IPV6
wlan33    down   AP    wlan33   1         00:00:00:00:00:00  Wireless33
wlan34    down   AP    wlan34   1         00:00:00:00:00:00  Wireless11
wlan35    down   AP    wlan35   1         00:00:00:00:00:00  Wireless12
wlan36    down   AP    wlan36   1         00:00:00:00:00:00  Wireless13
wlan37    down   AP    wlan37   1         00:00:00:00:00:00  Wireless14
wlan38    down   AP    wlan38   1         00:00:00:00:00:00  Wireless15
wlan39    down   AP    wlan39   1         00:00:00:00:00:00  Wireless16
rksccli:
```

FIGURE 140 Event Raised for WLAN Scheduler

Date and Time	Code	Type	Severity	Activity
2020/04/01 13:...	522	AP WLAN state changed	Informati...	AP [RuckusAP@C8:08:73:26:92:60] enabled WLAN[!!!!!!WIPS/WIDS//OPEN+WPA2] of radio [11g/n] on [Wed Apr 1 07:51:04 2020]. Reason: [Administrator configure].
2020/04/01 13:...	522	AP WLAN state changed	Informati...	AP [RuckusAP@C8:08:73:26:92:60] enabled WLAN[!!!!!!WIPS/WIDS//OPEN+WPA2] of radio [11ac] on [Wed Apr 1 07:51:05 2020]. Reason: [Administrator configure].

- You can view logs of when the client joins the AP at the scheduled time.

FIGURE 141 Logs Showing Client Joining AP at the Scheduled Time

```
Apr 1 09:27:26 RuckusAP daemon.debug hostapd: wlan32: STA 98:46:0a:2:ba:74 WPA: wlan32: WPA: handle_sm_ue_context rsp
Apr 1 09:27:26 RuckusAP daemon.debug hostapd: wlan32: STA 98:46:0a:2:ba:74 IEEE 802.11: wlan32: IEEE 802.11: No static cache found
Apr 1 09:27:26 RuckusAP daemon.debug hostapd: wlan32: STA 98:46:0a:2:ba:74 WPA: wlan32: WPA: start authentication
Apr 1 09:27:26 RuckusAP daemon.debug hostapd: wlan32: STA 98:46:0a:2:ba:74 IEEE 802.1X: wlan32: IEEE 802.1X: unauthorized port
Apr 1 09:27:26 RuckusAP daemon.debug hostapd: wlan32: STA 98:46:0a:2:ba:74 WPA: wlan32: WPA: sending 1/4 msg of 4-Way Handshake
Apr 1 09:27:26 RuckusAP daemon.debug hostapd: wlan32: STA 98:46:0a:2:ba:74 WPA: wlan32: WPA: received EAPOL-Key frame (2/4 Pairwise)
Apr 1 09:27:26 RuckusAP daemon.debug hostapd: wlan32: STA 98:46:0a:2:ba:74 WPA: wlan32: WPA: UE connects using default PSK
Apr 1 09:27:26 RuckusAP daemon.debug hostapd: wlan32: STA 98:46:0a:2:ba:74 WPA: wlan32: WPA: sending 3/4 msg of 4-Way Handshake
Apr 1 09:27:26 RuckusAP daemon.debug hostapd: wlan32: STA 98:46:0a:2:ba:74 WPA: wlan32: WPA: received EAPOL-Key frame (4/4 Pairwise)
Apr 1 09:27:26 RuckusAP daemon.warn hostapd: STA 98:46:0a:2:ba:74 IEEE 802.11: IEEE 802.11: add station:98:46:0a:2:ba:74 to ruDb
Apr 1 09:27:26 RuckusAP daemon.debug hostapd: wlan32: STA 98:46:0a:2:ba:74 IEEE 802.11: wlan32: IEEE 802.11: rks_dot11_scache_update uplink_rate:0kbps, downlink_rate:0kbps
Apr 1 09:27:26 RuckusAP daemon.info hostapd: @!202,clientJoin,"apMac":"c8:08:73:26:92:60","clientMac":"98:46:0a:2:ba:74","ssid":"!!!!!!WIPS/WIDS//OPEN+WPA2","bssid":"c8:08:73:26:92:60","userid":"","wlanid":"1","face":"wlan32","tenantUUID":"839f87c6-d116-497e-afce-a8157abd30c","apName":"RuckusAP","vlanid":"1111","radio":"a/n/ac","encryption":"WPA2-AES","instantaneous rssi":"0","xput":"0"
Apr 1 09:27:26 RuckusAP daemon.debug hostapd: IEEE 802.11: Start to update ruDb entry
Apr 1 09:27:26 RuckusAP daemon.debug hostapd: STA 98:46:0a:2:ba:74 IEEE 802.11: IEEE 802.11: rks_set_sta_wlan32 set ac(lid:0) & firewall profile(lid:0) for station ok98:46:0a:2:ba:74
Apr 1 09:27:26 RuckusAP daemon.warn hostapd: STA 98:46:0a:2:ba:74 IEEE 802.11: IEEE 802.11: rsm_ruDb_setSTAPAttachedPolicies Firewall Index 1 applied for station
Apr 1 09:27:26 RuckusAP daemon.debug hostapd: STA 98:46:0a:2:ba:74 IEEE 802.11: IEEE 802.11: rks_set_sta_utp_ac wlan32 set utp ac(filter_id:0, conf->sta_utp_ac_list_id:1, firewall profile id:1) for station ok98:46:0a:2:ba:74
Apr 1 09:27:26 RuckusAP daemon.debug hostapd: wlan32: STA 98:46:0a:2:ba:74 IEEE 802.11: wlan32: IEEE 802.11: set sta_type = 2, roam_state = 1, auth_type = 0, auth_method = 1, uplink = 0, downlink = 0 to RUDB
Apr 1 09:27:26 RuckusAP daemon.notice hostapd: wlan32: AP-STA-CONNECTED 98:46:0a:2:ba:74
Apr 1 09:27:26 RuckusAP daemon.debug hostapd: wlan32: STA 98:46:0a:2:ba:74 IEEE 802.1X: wlan32: IEEE 802.1X: authorizing port
Apr 1 09:27:26 RuckusAP daemon.debug hostapd: wlan32: STA 98:46:0a:2:ba:74 IEEE 802.11: IEEE 802.11: ieee802_1x_set_sta_authorized:721, accounting start!
Apr 1 09:27:26 RuckusAP daemon.info hostapd: wlan32: STA 98:46:0a:2:ba:74 WPA: wlan32: WPA: pairwise key handshake completed (RSN)
Apr 1 09:27:27 RuckusAP kern.warn kernel: [8317.462634] FWLOG: [8560868] RATE: ChainMask 3, peer_mac: ba:74, phyMode 10, ni_flags 0x0621b006, vht_mcs_set 0x00fa, ht_mcs_set 0xffff, legacy_rate_set 0x82a0f8
Apr 1 09:27:28 RuckusAP local0.alert dpconfmgr: subject from server cert: /C=US/ST=CA/L=Sunmyale/O=Ruckus Wireless Inc./emailAddress=service@ruckuswireless.com/CN=97H0TWM7OXN24NN4IH02109P1CXQ00C29F64EE800C29F64EF5
Apr 1 09:27:28 RuckusAP local0.alert dpconfmgr: subject from server_list:
```



# Terminating Sessions

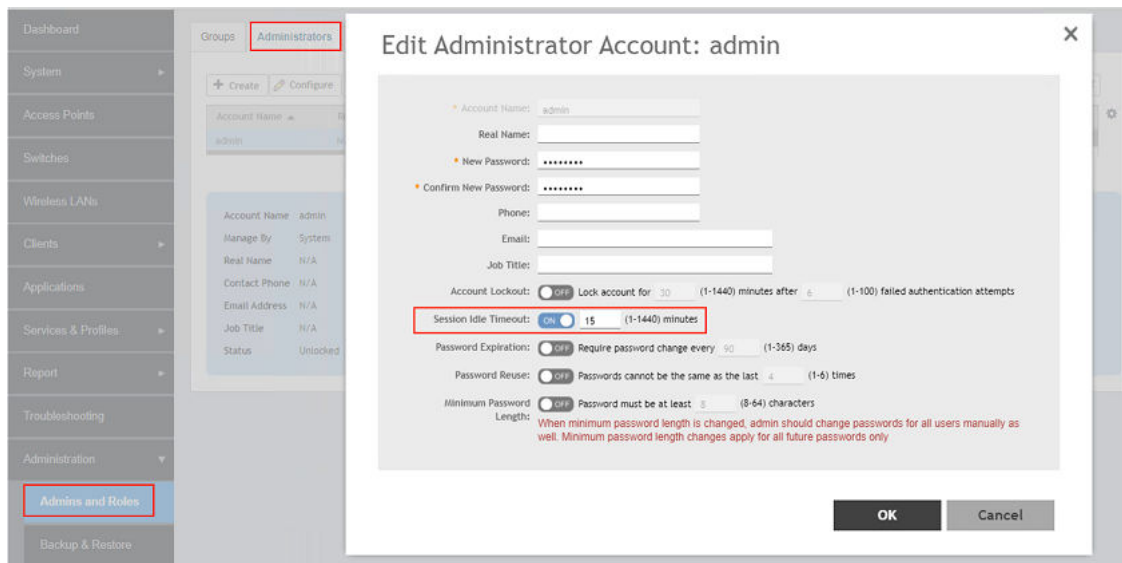
- Terminating Sessions for Non-Admin Users..... 142
- Terminating Administrator Sessions..... 143

The SmartZone controller can terminate a remote interactive session after it has exceeded the session timeout value configured by the security administrator.

## Terminating Sessions for Admin Users

1. To configure the timeout value on the controller web interface, select **Administration > Admin and Roles > Administrators**
2. Select the administrator account and click **Configure**.  
The **Edit Administrator Account** page displays.
3. Set the **Session Idle Timeout** value from 1 to 1440 minutes.

**FIGURE 142** Session Idle Timeout Configuration



The session idle timeout value is usually set to 30 minutes (default). You can also set the session idle timeout value from the command line interface.

## Terminating Sessions

### Terminating Sessions for Non-Admin Users

- From the command prompt, set the value as shown:

**FIGURE 143** Session Timeout Configuration via CLI

```
VSZ-NODE-208# session-timeout
<minutes> Minutes (Positive, max is 1440 and default is 30 minutes.)
<cr>

VSZ-NODE-208# session-timeout
Session timeout is 30 minutes
```

The session timeout configured via CLI is applied to the CLI and the local console.

For a CLI session, the default session idle timeout is 30 minutes.

For a GUI session, the default session idle timeout is 15 minutes.

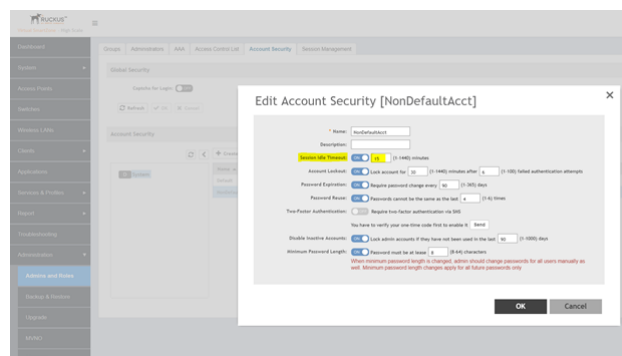
## Terminating Sessions for Non-Admin Users

You can terminate the remote interactive session for non administrator users by creating a non-admin user account, a non-admin security profile and mapping the profile with the user by creating a user group.

- Select **Administration > Admin and Roles > Account Security** to configure the timeout value on the controller web interface from the security profile.
- Click **Create**.
- Set the **Session Idle Timeout** value from 1 through 1440 minutes.

Because non-admin users cannot access the CLI, only the GUI session idle timeout is applicable.

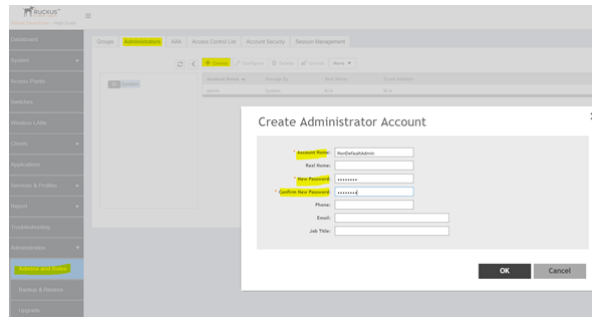
**FIGURE 144** Session Timeout Configuration from the Security Profile



The session timeout value is usually set to 30 minutes (default).

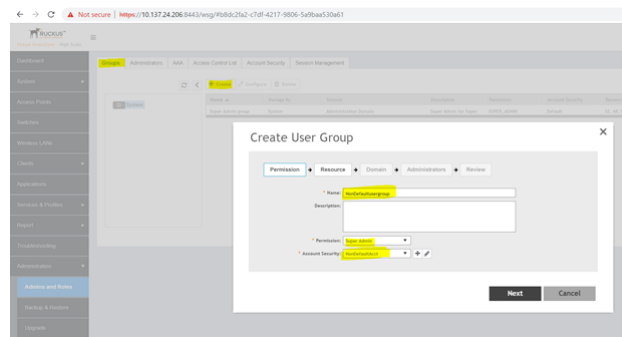
4. Select **Administration > Admin and Roles > Administrator** to create a non-admin user account.

FIGURE 145 Creating a Non-Admin Account



5. Select **Administration > Admin and Roles > Groups** to create the user group to map the non-admin user to the security profile.

FIGURE 146 Creating User Groups



After the session is terminated, an event is generated to notify the user. You can view the events from the **Events & Alarms** page on the controller interface.

## 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.

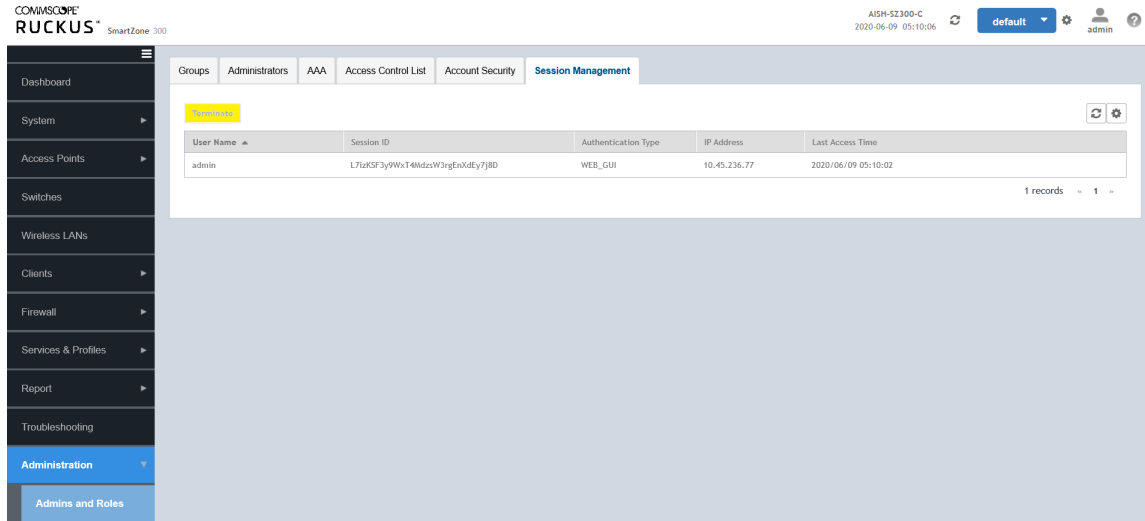
## Terminating Sessions

### Terminating Administrator Sessions

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 147** Sample Session Termination for Web Interface Session.



**FIGURE 148** 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

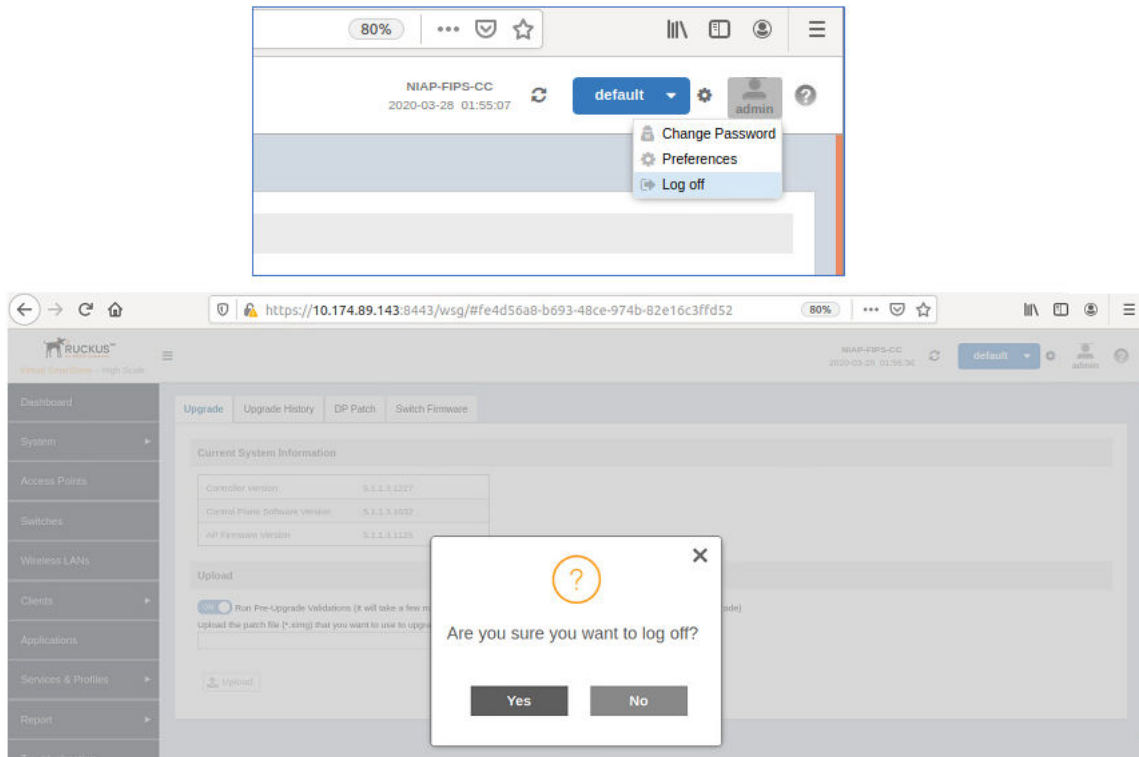
en
Please wait. CLI initializing...

Welcome to the Ruckus SmartZone 300 Command Line Interface
Version: 5.1.1.0.342

VSZ100>
VSZ100> en
VSZ100> 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 149** Logging out from the UI



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

**FIGURE 150** 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

S29> en
Password: *****

S29# exit

S29> 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:\>] █
```

## Terminating Sessions

### Terminating Administrator Sessions

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

FIGURE 151 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 152 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+J'.
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:\~]$
```

# Locking an Administrator Account

- [Locking Non-Administrator Accounts..... 148](#)

You can configure administrator accounts to be forcefully locked when there are repeated attempts to access the account by unauthorized users. This is typically applicable in situations when the user name entered is correct but password is wrong. You can configure the number of unsuccessful attempts that users can try to login to the account, after which the account will be locked.

1. From the controller web interface, go to **Administration > Admin and Roles > Administrators**.
2. Select the administrator account and click **Configure**.

The **Edit Administrator Account** page appears.

**FIGURE 153** Configuring the Account Lock

## Edit Administrator Account: admin

Account Name: admin

Real Name: [ ]

New Password: [ ]

Confirm New Password: [ ]

Phone: 68687886687

Email: [ ]

Job Title: Admin

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

Session Idle Timeout:  ON 60 (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 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

OK Cancel

3. Enable **Account Lockout** and configure the account lockout time and the number of failed authentication attempts. A user is locked out for the account lockout time after the configured number of failed login attempts.

### NOTE

The administrator must wait until the lockout period expires.

4. Click **OK**. The **Password Confirmation** screen appears.

## Locking an Administrator Account

### Locking Non-Administrator Accounts

5. Click **OK**.

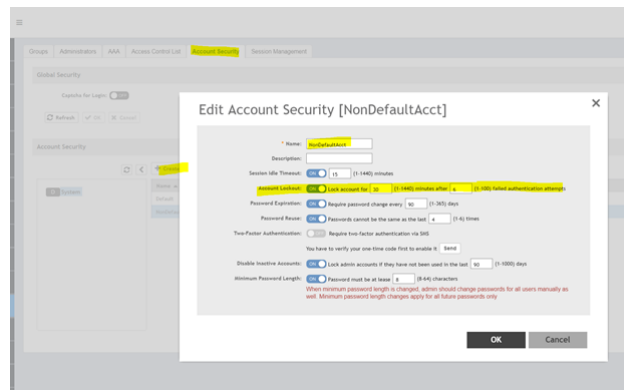
You can modify the account lock settings from the security profile also. Select **Administration > Admins and Roles > Account Security**, and click **Configure** to edit the value from within the selected profile.

## Locking Non-Administrator Accounts

You can configure non-administrator accounts to be forcefully locked when there are repeated attempts to access the account by unauthorized users. For this, you must create a non-admin user account, security profile, and user group mapping the account and profile.

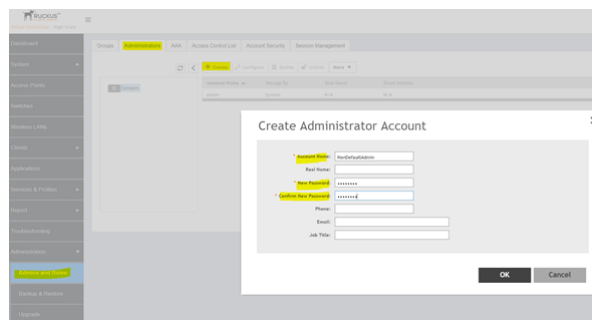
1. From the controller web interface, select **Administration > Admin and Roles > Account Security**.
2. Click **Configure**.
3. Click **ON** to enable **Account Lockout** and enter the account lockout time and number of failed authentication attempts.

**FIGURE 154** Account Lockout Configuration from the Security Profile



4. Select **Administration > Admin and Roles > Administrators** to create a non-administrator user account.

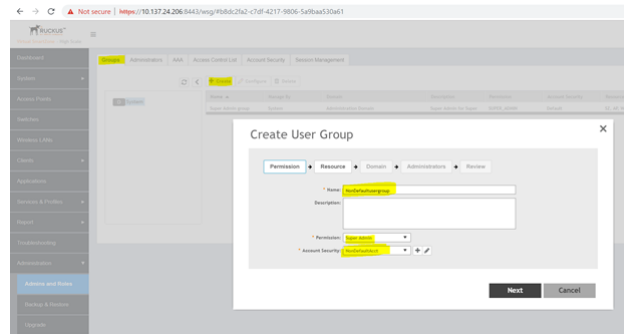
**FIGURE 155** Creating a Non-Administrator Account





5. Select **Administration > Admin and Roles > Groups** to create the user group to map the non administrator user to the security profile

FIGURE 156 Creating User Groups



When the number of login attempts exceeds the value configured, the user is locked and the following screen appears.

FIGURE 157 Locked User Account

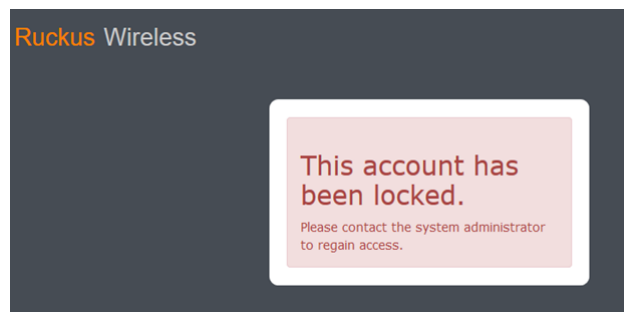


FIGURE 158 AP User Locked: Verification from CLI

```
[root@IRAWAT ~]# ssh 192.168.11.67
Please login: admin
password :
Login incorrect
Please login:
Please login: admin
password :
Login incorrect
Login failureConnection to 192.168.11.67 closed.
[root@IRAWAT ~]# ssh 192.168.11.67
Please login: admin
password :
kscli : Login failureConnection to 192.168.11.67 closed.
[root@IRAWAT ~]#
```

## Locking an Administrator Account

### Locking Non-Administrator Accounts

FIGURE 159 vSZ-D User Locked: Verification from CLI

```
[root@IRAWAT ~]# ssh admin@10.1.200.42
The authenticity of host '10.1.200.42 (10.1.200.42)' can't be established.
RSA key fingerprint is 57:fb:c5:ba:84:ab:5b:79:b6:ae:72:e2:5c:0b:90:6a.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.1.200.42' (RSA) to the list of known hosts.
#####
#           Welcome to vSZ-D           #
#####
admin@10.1.200.42's password:
Permission denied, please try again.
admin@10.1.200.42's password:
Permission denied, please try again.
admin@10.1.200.42's password:
Received disconnect from 10.1.200.42: 2: Too many authentication failures
[root@IRAWAT ~]#
[root@IRAWAT ~]# ssh admin@10.1.200.42
#####
#           Welcome to vSZ-D           #
#####
admin@10.1.200.42's password:
Permission denied, please try again.
admin@10.1.200.42's password:
Connection closed by 10.1.200.42
```

After the account is locked, an event is generated to notify the user. You can view the events from the **Events & Alarms** page on the controller interface.

# Setting Up the Login Banner

---

You can customize the message that appears in the login banner of the controller web interface.

1. From the controller web interface, Select **System > General Settings > Login Banner**.

## Setting Up the Login Banner

2. Configure the content of the login banner as required.

**FIGURE 160** Web Interface

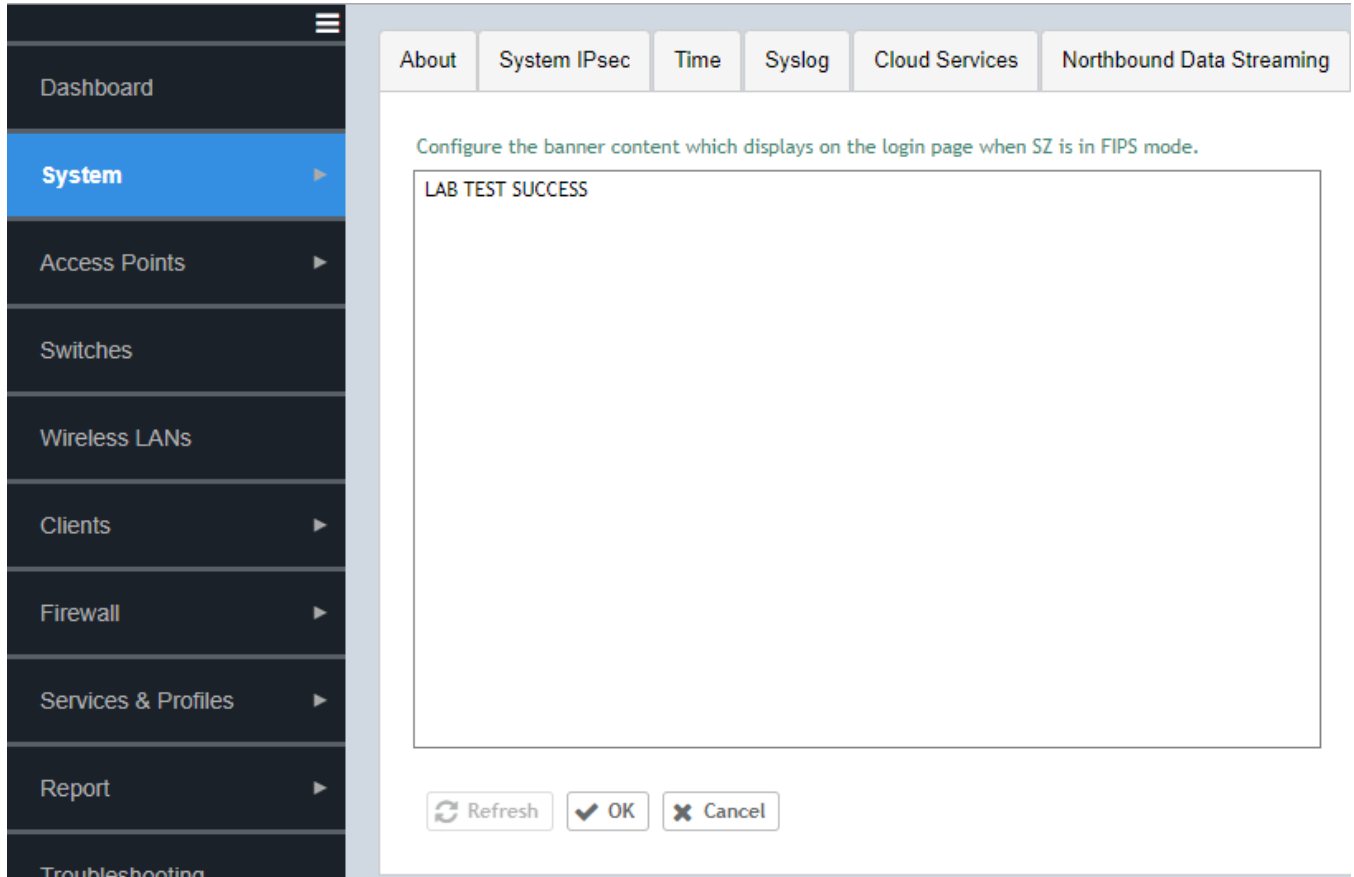


FIGURE 161 CLI Login

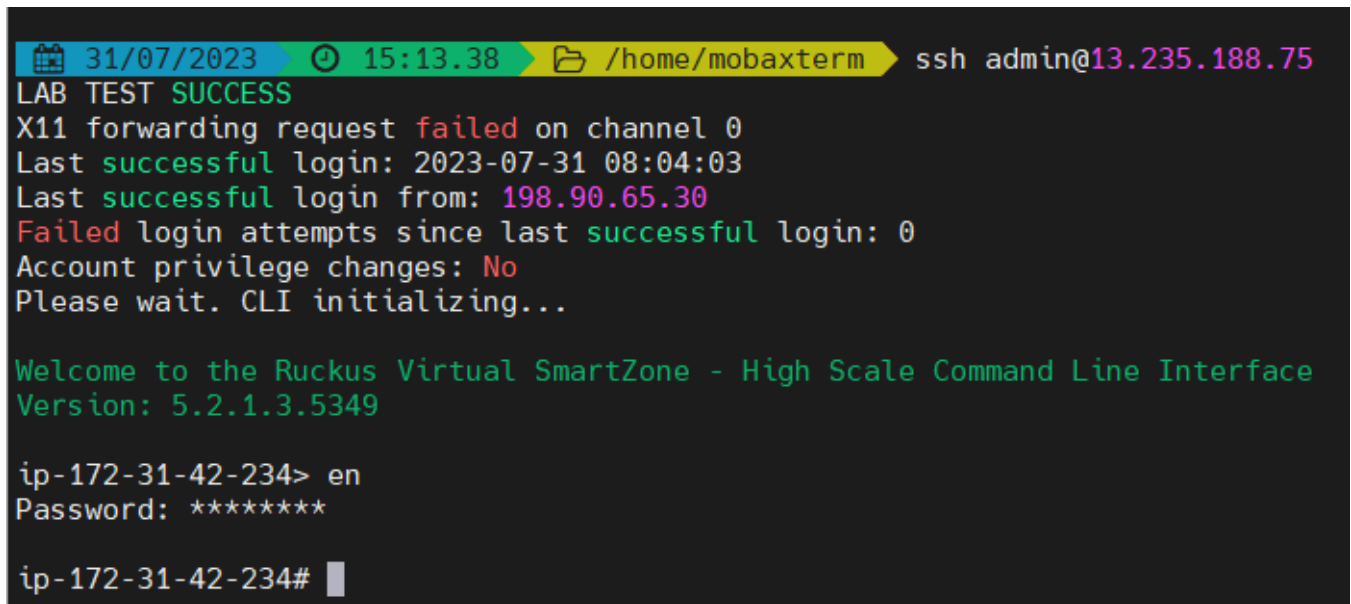
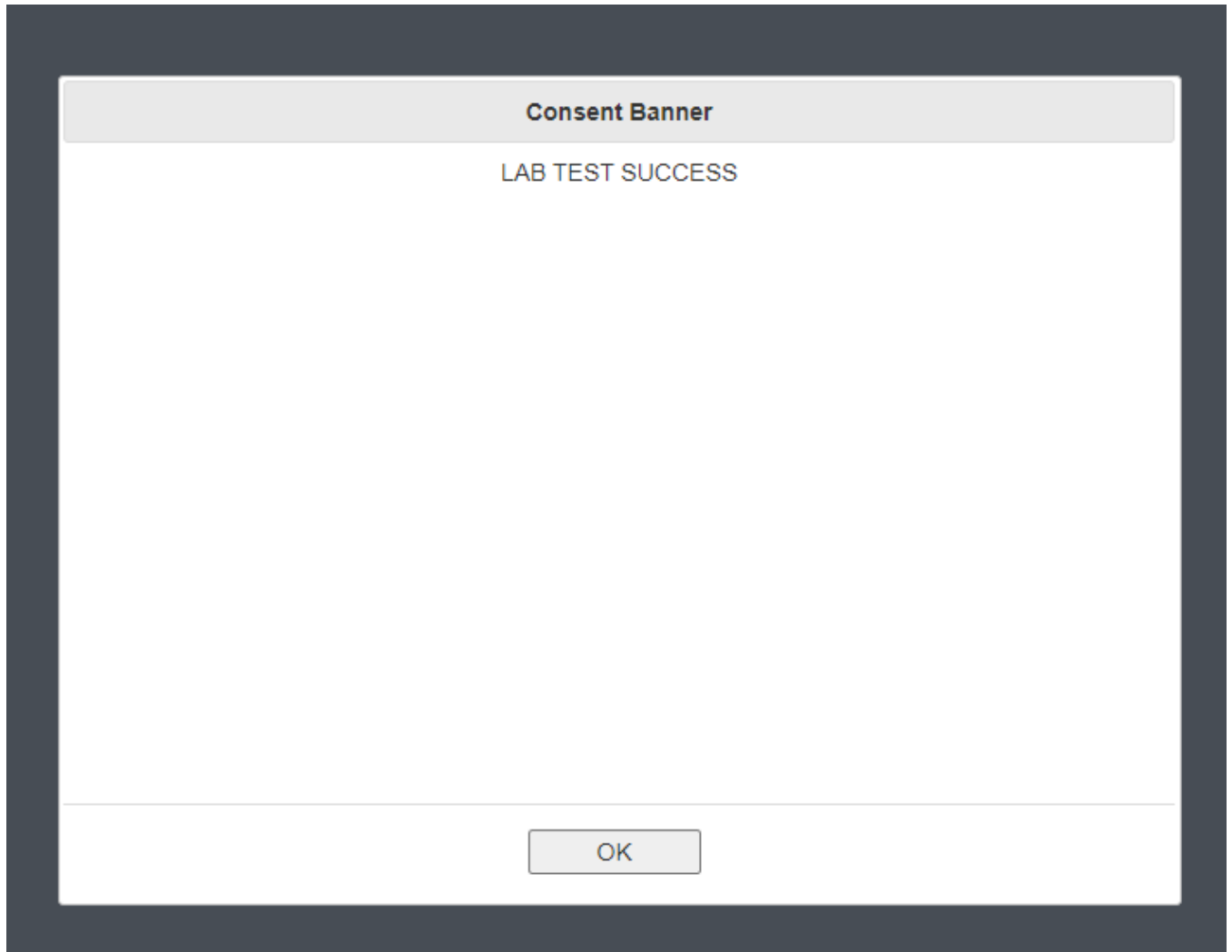
A screenshot of a terminal window with a dark background. At the top, there is a status bar with a calendar icon, the date '31/07/2023', a clock icon, the time '15:13.38', a folder icon, the path '/home/mobaxterm', and the connection 'ssh admin@13.235.188.75'. The main text shows a successful login: 'LAB TEST SUCCESS', followed by 'X11 forwarding request failed on channel 0', 'Last successful login: 2023-07-31 08:04:03', 'Last successful login from: 198.90.65.30', 'Failed login attempts since last successful login: 0', and 'Account privilege changes: No'. A message says 'Please wait. CLI initializing...'. The login banner reads 'Welcome to the Ruckus Virtual SmartZone - High Scale Command Line Interface' and 'Version: 5.2.1.3.5349'. The user enters 'ip-172-31-42-234> en' and 'Password: \*\*\*\*\*'. The prompt changes to 'ip-172-31-42-234#' with a cursor.

FIGURE 162 Consent Banner

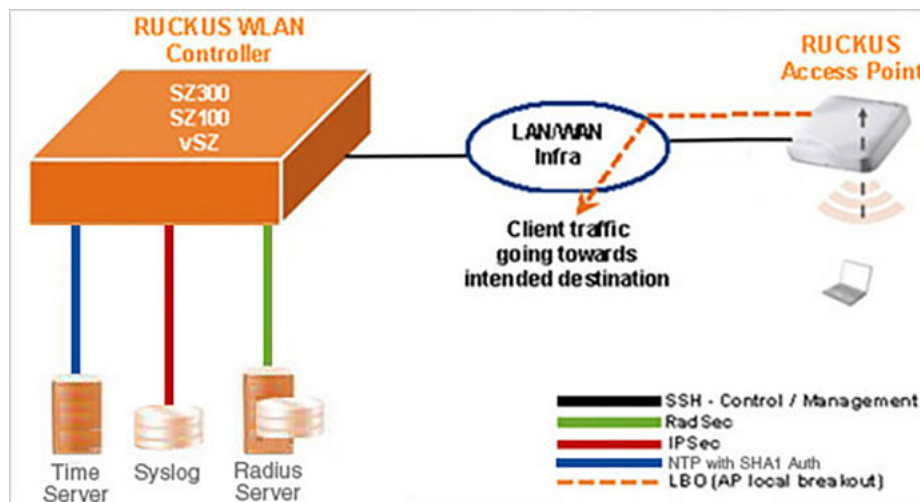


# Deployment Models

SZ and vSZ maintain different centralized deployment models for IPsec tunnel setup. RUCKUS Wireless Controllers and RUCKUS Smart Wi-Fi APs are deployed in two different models; distributed deployment model and centralized deployment model.

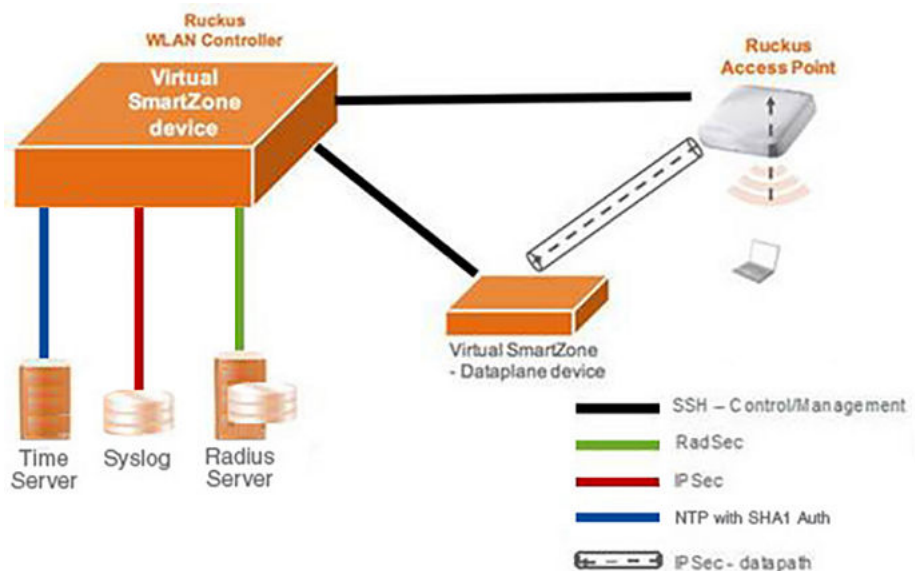
**Distributed Deployment Model** In distributed deployment model client traffic directly reaches the intended destination from the AP. All RUCKUS Wireless Controllers and APs support this deployment model as seen in the below figure.

FIGURE 163 Distributed Deployment Model



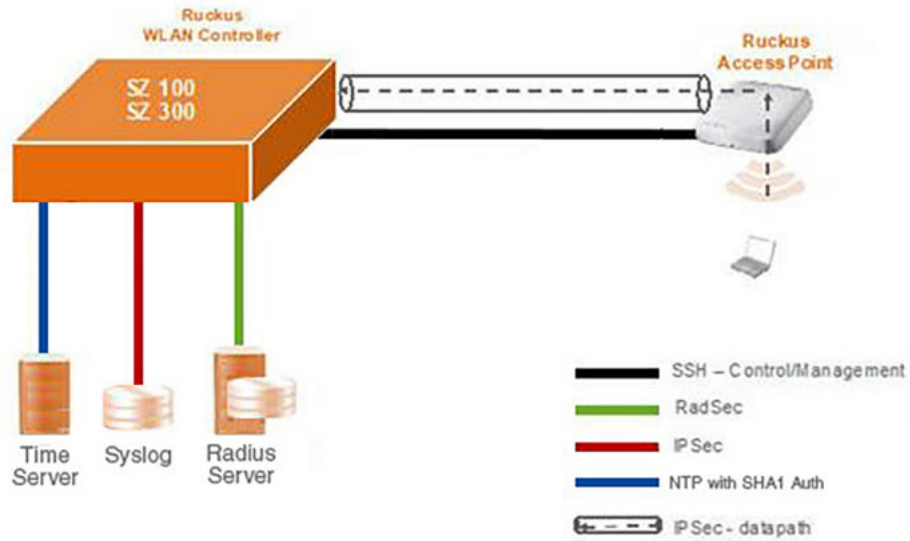
**Centralized Deployment Model** In centralized deployment model client traffic always reaches the WLAN controller first through the AP before going to intended destination as in the below figures.

FIGURE 164 Centralized Deployment Model with hardware



## Deployment Models

FIGURE 165 Centralized Deployment Model with Software



Once authenticated as trusted nodes on the wired infrastructure, the access points provide the encryption service on the wireless network between themselves and the wireless client. The APs also communicate directly with the wireless controller for management purposes. The management traffic between RUCKUS AP and RUCKUS Wireless Controller is encrypted



# Configuring RUCKUS GRE and IPSec in WLAN-Concept

---

- Creating an IPSec Profile..... 157
- Creating a RUCKUS GRE Profile..... 159
- Creating an AP Zone..... 160
- Creating AP GRE Tunnel Profile..... 167
- Creating WLAN Configuration..... 168

You can configure RUCKUS GRE tunnel profile and IPSec profile in WLAN to manage AP traffic. RUCKUS GRE and IPSec is a configuration of IPSec tunnel between AP and hardware (HW) controller (SmartZone) in centralize HW deployment, AP and vSZ-D in centralized virtualize deployment.

## Creating an IPSec Profile

Follow the below steps to create an IPSec profile.

On the controller web user interface:

1. Navigate to **Services & Profiles > Tunnels and Ports**.
2. Select the tab **IPSec** and select the required zone for creating the required profile.
3. Click on **Create** to view the *Create IPSec Profile* page.

## Create IPsec profile



**General Options**

Name:

Description:

Tunnel Mode:  SoftGRE  RuckusGRE

**Authentication**

Type:  Certificate

**Security Association**

IKE Proposal Type:  Specific

Algorithm Combinations:

ESP Proposal Type:  Specific

Algorithm Combinations:

**Rekey Options**

Internet Key Exchange: Rekey Time:

Encapsulating Security Payload: Rekey Time:

4. Configure the following:

- **Name:** Type the name of the profile.
- **Description:** Type the description of the profile.
- **Tunnel Mode :** Select Ruckus GRE.
- **Security Association:**
  - **IKE Proposal Type:** Select the proposal type as *AES128-SHA1-MODP2048* or *AES256-SHA384-ECP384*
  - **ESP Proposal Type :** Select the proposal type as *AES128-SHA1-MODP2048* or *AES256-SHA384-ECP384*.

**NOTE**

WLAN controller will not allow ESP proposal to be less secured than IKE Proposal . If *AES128-SHA1-MODP2048* is selected for IKE, WLAN controller will allow both *AES128-SHA1-MODP2048* and *AES256-SHA384-ECP384* for ESP. However, if *AES256-SHA384-ECP384* is selected for IKE only *AES256-SHA384-ECP384* will be allowed for ESP.

- **Rekey Options:** Configure the required duration for IKE and ESP keys.

5. Click OK.

You have created the IPSec GRE profile.

**NOTE**

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

**NOTE**

The IPSec connection between AP and vSZ-D is recovered automatically and manual intervention is not required.

## Creating a RUCKUS GRE Profile

Follow the below steps to create an GRE profile.

On the controller web user interface:

1. Navigate to **Services & Profiles > Tunnels and Ports**.
2. Select the tab **RUCKUS GRE** and select the required zone for creating the required profile.
3. Click on **Create** to view the *Create RUCKUS GRE Profile* page.

### Create Ruckus GRE Profile

The screenshot shows a web form titled "Create Ruckus GRE Profile". The form contains the following fields and options:

- Name:** A text input field.
- Description:** A text input field.
- Ruckus Tunnel Mode:** A dropdown menu with "GRE" selected.
- Tunnel Encryption:** Radio buttons for "Disable" (selected), "AES 128", and "AES 256".
- Tunnel MTU:** Radio buttons for "Auto" (selected) and "Manual". Next to "Manual" is a text input field containing "850" and the label "bytes (IPv4:850-9018, IPv6:1384-9018)".

At the bottom right of the form are two buttons: "OK" and "Cancel".

4. Configure the following:
  - **Name:** Type the name of the profile.
  - **Description:** Type the description of the profile.
  - **RUCKUS Tunnel Mode :** Select *Ruckus GRE*.
  - **Tunnel Encryption:** Select as *Disable*. This is the default option.
  - **Tunnel MTU :** MTU (Maximum Transmission Unit) is the size of the largest protocol data unit that can be passed on the controller network. Set the MTU for the tunnel using one of the 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.
5. Click OK.

## Configuring RUCKUS GRE and IPsec in WLAN-Concept Creating an AP Zone

You have created the RUCKUS GRE profile.

# Creating an AP Zone

Follow the below steps to create an AP Zone with the appropriate RUCKUS GRE and IPsec profiles.

On the controller web user interface:

1. Navigate to **Access Points** to create an AP Zone.
2. On the menu, click **Access Points** to view the below screen.

**FIGURE 166** Access Points

The screenshot shows the Ruckus controller web interface. At the top, there is a red banner with the message "No license to enable L3 Roaming." The page title is "Access Points (4)" with 0 Online, 0 Flagged, and 4 Offline. The interface includes a sidebar with navigation options like Dashboard, System, Access Points, Switches, Wireless LANs, Clients, Applications, Services & Profiles, and Report. The main content area displays a table of APs and a tree view of the System structure.

MAC Address	AP Name	Status	IP Address	Total Traffic (1hr)	Model	Clients	AP Firmware
EC:8C:A2:0C:A6:C0	RuckusAP	Offline	140.138.80.245	N/A	R610	0	5.1.0.99.263
F0:3E:90:3F:7F:80	RuckusAP	Offline		N/A	C110	0	5.1.0.0.563
F0:3E:90:3F:8B:00	RuckusAP	Offline		N/A	R720	0	5.1.0.0.579
F0:3E:90:3F:8C:80	RuckusAP	Offline		N/A	R720	0	5.1.0.0.563


3. From the **System tree**, select the location to create the zone (for example, System or Domain), and then click . You will be directed to the **Create Group** screen.

FIGURE 167 Create Group

- Configure the zone by typing the settings listed in the table below.

TABLE 7 AP Zone Details

Field	Description	Your Action
<b>Name</b>	Indicates the name of the zone/AP group.	Enter a name.
<b>Description</b>	Indicates the short description assigned to the zone or AP group.	Enter a brief description
<b>Type</b>	Indicates if you are creating a domain, zone or an AP group.	Appears by default. You can also choose the option.
<b>Parent Group</b>	Indicates the parent AP group.	Appears by default.
<b>Configuration &gt; General Options</b>		
<b>AP Firmware</b>	Indicates the firmware to which it applies.	Select the firmware.
<b>Country Code</b>	Indicates the country code. Using the correct country code helps ensure that APs use only authorized radio channels.	Select the country code.
<b>Location</b>	Indicates the generic location of the zone.	Enter the location.
<b>Location Additional Information</b>	Indicates detailed location.	Enter additional location information.
<b>GPS Coordinates</b>	Indicates the geographical location.	Enter the following coordinates: <ul style="list-style-type: none"> <li>• <b>Longitude</b></li> <li>• <b>Latitude</b></li> <li>• <b>Altitude</b></li> </ul>
<b>AP Admin Logon</b>	Indicates the admin logon credentials.	Enter the <b>Logon ID</b> and <b>Password</b> .
<b>AP Time Zone</b>	Indicates the time zone that applies.	Select a time zone, and the enter the details as required.
<b>AP IP Mode</b>	Indicates the IP version that applies.	Select the IP version. IPv6, IPv4 and dual addressing modes are supported.

TABLE 7 AP Zone Details (continued)

Field	Description	Your Action
<b>Historical Connection Failures</b>	Allows the zone APs to report client connection failures so that the administrator can view past connection problems from the Troubleshooting menu.	Click the button.
<b>DP Zone Affinity Profile</b>	Specifies the DP affinity profile for the zone.  <b>NOTE</b> This option is supported only on vSZ-H.	Select the zone affinity profile from the list.
<b>SSH Tunnel Encryption</b>	Specifies the encryption that reduces the load on controller control of SSH traffic.	Select the required option: <ul style="list-style-type: none"> <li>• <b>AES 128</b></li> <li>• <b>AES 256</b></li> </ul>
<b>Cluster Redundancy</b>	Provides cluster redundancy option for the zone.  <b>NOTE</b> Cluster redundancy is supported only on SZ300 and vSZ-H.	Select the required option: <ul style="list-style-type: none"> <li>• <b>Zone Enable</b></li> <li>• <b>Zone Disable</b></li> </ul>
<b>Configuration &gt; Radio Options</b>		
<b>Channel Range (2.4G)</b>	Indicates that you want to override the 2.4GHz channel range that has been configured for the zone to which this AP group belong.	Select <b>Select Channel Range (2.4G)</b> check boxes for the channels on which you want the 2.4GHz radios of managed APs to operate. Channel options include channels 1 to 11. By default, all channels are selected.
<b>DFS Channels</b>	Allows ZoneFlex APs to use DFS channels.	Select the check box.
<b>5.8 Ghz Channels</b>	Provides C-band support for all Outdoor APs and the following Indoor APs: R310, R510.  <b>NOTE</b> This feature is available only for countries that support 5.8Ghz channel. For example, UK provides indoor AP—5.8Ghz channel support.	Select the <b>Allow 5.8Ghz channels</b> check box.
<b>5.8 Ghz Channels License</b>	Enables full TX Power Adjustment for C-band channels.  <b>NOTE</b> This feature is supported only for UK.	Select the <b>Allow 5.8Ghz channels use full power</b> check box.
<b>Channel Range (5G) Indoor</b>	Indicates the channels on the 5GHz radio that you want managed indoor APs to operate.	Select the check boxes.
<b>Channel Range (5G) Outdoor</b>	Indicates the channels on the 5GHz radio that you want managed outdoor APs to operate.	Select the check boxes.

TABLE 7 AP Zone Details (continued)

Field	Description	Your Action
<p><b>Radio Options b/g/n (2.4 GHz)</b></p>	<p>Indicates the configuration options for the 2.4 GHz radio.</p>	<p>Select the following options:</p> <ul style="list-style-type: none"> <li> <p><b>Channelization</b>—Set the channel width used during transmission to either <b>20</b> or <b>40</b> (MHz), or select <b>Auto</b> to set it automatically.</p> </li> <li> <p><b>Channel</b>—Select the channel to use for the b/g/n (2.4GHz) radio, or select <b>Auto</b> to set it automatically.</p> </li> <li> <p><b>Auto cell sizing</b>— Select this option to enable APs to share information on interference seen by each other and dynamically adjust their radio Tx power and Rx parameters to minimize interference. Enabling this option, disables the TX Power Adjustment configuration.</p> <p style="text-align: center;"><b>NOTE</b> Ensure that <b>Background Scan</b> is enabled.</p> </li> <li> <p><b>TX Power Adjustment</b>—Select the preferred TX power, if you want to manually configure the transmit power on the 2.4GHz radio. By default, TX power is set to <b>Full</b> on the 2.4GHz radio.</p> <p style="text-align: center;"><b>NOTE</b> If you choose <b>Min</b>, the transmit power is set to 0dBm (1mW) per chain for 11n APs, and 2dBm per chain for 11ac APs. If you choose <b>Max</b>, the transmit power is set to the max allowable value according to the AP's capability and the operating country's regulations.</p> </li> </ul>

TABLE 7 AP Zone Details (continued)

Field	Description	Your Action
<b>Radio Options a/n/ac (5 GHz)</b>	Indicates the configuration options for the 5 GHz radio.	Select the following options: <ul style="list-style-type: none"> <li>● <b>Channelization</b>—Set the channel width used during transmission to either <b>20, 40, 80, 80+80, 160</b> (MHz), or select <b>Auto</b> to set it automatically.</li> <li>● <b>Channel</b>—For <b>Indoor</b> and <b>Outdoor</b>, select the channel to use for the a/n/c (5GHz) radio, or select <b>Auto</b> to set it automatically.</li> <li>● <b>Secondary Channel (80+80)</b>—For <b>Indoor</b> and <b>Outdoor</b>, the default secondary channel to use for the a/n/c (5GHz) radio, is set as <b>Auto</b>.</li> <li>● <b>Auto cell sizing</b>— Select this option to enable APs to share information on interference seen by each other and dynamically adjust their radio Tx power and Rx parameters to minimize interference. Enabling this option, disables the TX Power Adjustment configuration.                             <p style="text-align: center;"><b>NOTE</b> Ensure that <b>Background Scan</b> is enabled.</p> </li> <li>● <b>TX Power Adjustment</b>—Select the preferred TX power, if you want to manually configure the transmit power on the 5GHz radio. By default, TX power is set to <b>Full</b> on the 5GHz radio.                             <p style="text-align: center;"><b>NOTE</b> If you choose <b>Min</b>, the transmit power is set to 0dBm (1mW) per chain for 11n APs, and 2dBm per chain for 11ac APs. If you choose <b>Max</b>, the transmit power is set to the max allowable value according to the AP's capability and the operating country's regulations.</p> </li> </ul>
<b>Configuration &gt; AP GRE Tunnel Options</b>		
<b>Tunnel Type</b>	Indicates the supported tunnel type (Ruckus GRE, SoftGRE and SoftGRE+IPsec)	Choose : <ul style="list-style-type: none"> <li>● <b>Ruckus GRE</b> and select the <b>GRE Tunnel Profile</b>.</li> <li>● <b>SoftGRE</b> and                             <ul style="list-style-type: none"> <li>- select the <b>GRE Tunnel Profile</b></li> <li>- select <b>AAA Affinity</b>, which is applicable only for proxy AAA.                                     <p style="text-align: center;"><b>NOTE</b> If you select <b>AAA Affinity</b>, you must enable <b>Force Disassociate Client</b> while creating the Soft GRE Profile.</p> </li> </ul> </li> <li>● <b>SoftGRE+IPsec</b> and                             <ul style="list-style-type: none"> <li>- select the <b>GRE Tunnel Profile</b></li> <li>- select <b>SoftGRE+IPsec</b></li> </ul> </li> </ul>
<b>Configuration &gt; Advanced Options</b>		



TABLE 7 AP Zone Details (continued)

Field	Description	Your Action
<b>Channel Mode</b>	Indicates if location-based service is enabled. If you want to allow indoor APs that belong to this zone to use wireless channels that are Channel Mode regulated as indoor-use only.	Select the <b>Allow indoor channels</b> check box.
<b>Auto Channel Selection</b>	Indicates auto-channel settings.	Select the check box and choose the option.
<b>Background Scan</b>	Runs a background scan.	Select the respective check boxes and enter the duration in seconds: <ul style="list-style-type: none"> <li>● <b>Background Scanning</b>—Changes the AP channel if there is interference.</li> <li>● <b>ChannelFly</b>—Continuously monitors potential throughput and changes the AP channel to minimize interference and optimize throughput.</li> </ul>
<b>Smart Monitor</b>	Indicates AP interval check and retry threshold settings.	Select the check box and enter the interval and threshold.
<b>AP Ping Latency Interval</b>	Measures the latency between the controller and AP periodically, and send this data to SCI	Enable by moving the radio button to ON to measure latency.
<b>Rogue AP Detection</b>	Indicates rogue AP settings.	Enable the option.
<b>Rogue Classification Policy</b>	Indicates the parameters used to classify rogue APs. This option is available only if you enable the <b>Rogue AP Detection</b> option.	Select the options for rogue classification policy: <ul style="list-style-type: none"> <li>● - <b>Enable events and alarms for all rogue devices</b></li> <li>- <b>Enable events and alarms for malicious rogues only</b></li> <li>● <b>Report RSSI Threshold</b> - enter the threshold. Range: 0 through 100.</li> <li>● <b>Protect the network from malicious rogue access points</b> - Enable the option and choose one of the following:                             <ul style="list-style-type: none"> <li>- <b>Aggressive</b></li> <li>- <b>Auto</b></li> <li>- <b>Conservative</b></li> </ul> </li> <li>● <b>Radio Jamming Detection</b> - enable the option and enter the <b>Jamming Threshold</b> in percentage.</li> </ul>
<b>DoS Protection</b>	Indicates settings for blocking a client.	Select the check box and enter the duration in seconds.
<b>Client Load Balancing</b>	Balances the number of clients across APs.	Select the check box and enter the threshold.

TABLE 7 AP Zone Details (continued)

Field	Description	Your Action
<b>Band Balancing</b>	Balances the bandwidth of the clients.	<p>You can use the slider to actively control associated stations to meet certain band distribution requirements allowing for dynamic band balancing:</p> <ul style="list-style-type: none"> <li>● <b>Disable:</b> disables band balancing</li> <li>● <b>Basic (default):</b> during heavy load conditions, this option withholds probe and authentication responses in order to balance clients.</li> <li>● <b>Proactive:</b> this is a dynamic form of band balancing where the clients are re-balanced on the AP utilizing the 802.11v BTM standard. The AP sends a BTM message to the client to change the bands and it is left to the client's discretion to make a decision on changing the bands.</li> <li>● <b>Strict:</b> this is an aggressive form of band balancing where the clients are forced to re-balance utilizing the 802.11v BTM standard. The AP sends a BTM message to the client to change the bands. If the client does not change the band, the client is forced to disconnect after 10 seconds.</li> </ul> <p><b>NOTE</b>                      The band change is applicable only for those connected clients that support 802.11v standard.</p> <p>Enter the percentage of client load on the 2.4 GHz band.</p>
<b>Location Based Service</b>	Indicates that the location based service is enabled.	<ul style="list-style-type: none"> <li>● Select the check box and choose the options.</li> <li>● Click Create, In the Create LBS Server form:                             <ol style="list-style-type: none"> <li>Enter the <b>Venue Name</b>.</li> <li>Enter the <b>Server Address</b>.</li> <li>Enter the <b>Port number</b>.</li> <li>Enter the <b>Password</b>.</li> </ol> </li> </ul>
<b>Client Admission Control</b>	Indicates the load thresholds on the AP at which it will stop accepting new clients.	<p>Select the check box and update the following settings:</p> <ul style="list-style-type: none"> <li>● <b>Min Client Count</b></li> <li>● <b>Max Radio Load</b></li> <li>● <b>Min Client Throughput</b></li> </ul>
<b>Protection Mode</b>	Indicates the mechanism to reduce frame collision.	<p>Choose one of the following options:</p> <ul style="list-style-type: none"> <li>● None</li> <li>● RTS/CTS</li> <li>● CTS Only</li> </ul>
<b>AP Reboot Timeout</b>	Indicates the AP reboot settings.	<p>Choose the required option for:</p> <ul style="list-style-type: none"> <li>● <b>Reboot AP if it cannot reach default gateway after</b></li> <li>● <b>Reboot AP if it cannot reach the controller after</b></li> </ul>
<b>Recovery SSID</b>	Allows you to enable or disable the Recovery(Island) SSID broadcast on the controller.	Enable <b>Recovery SSID Broadcast</b>

5. Click **OK**.

You have created the AP Zone.


**NOTE**

RUCKUS GRE over IPsec is supported in transport mode only. It provides RSA support.

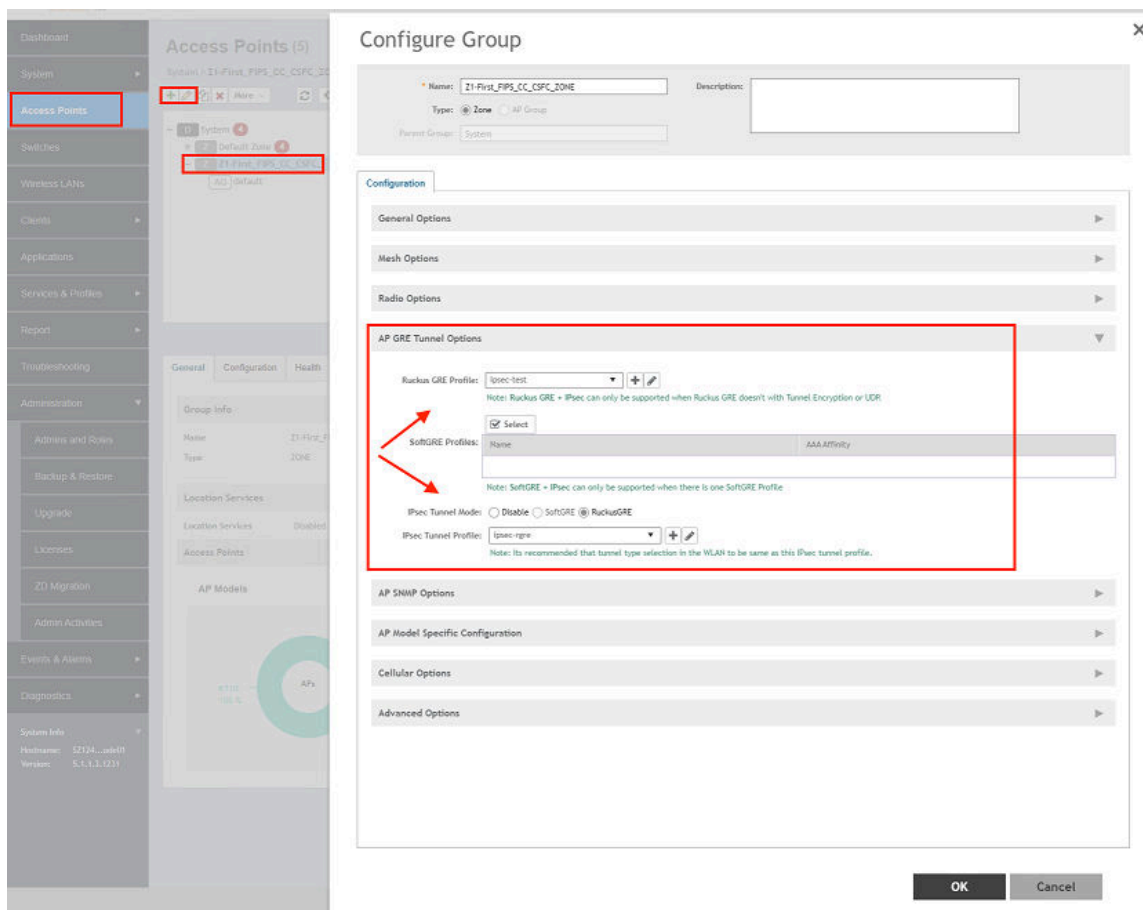
## Creating AP GRE Tunnel Profile

Follow the below steps to create an AP GRE Tunnel profile.

On the controller web user interface in the **Create Group** screen:

1. Select the **FIPS Zone** and click the  icon to configure the **AP GRE Tunnel Options** from the **Configuration** tab.
2. Configure the following:
  - **RUCKUS GRE Profile** : Select the GRE profile configured previously.
  - **IPsec Tunnel Mode**: Select the radio button RuckusGRE.
  - **IPsec Tunnel Profile**: Select the configured IPsec tunnel profile.

**FIGURE 168** AP GRE Tunnel Configurations



3. Click OK.

You have created the options for AP GRE Tunnel.

## Creating WLAN Configuration

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

On the controller web user interface:

1. In the **Wireless LANs** page, from the System tree hierarchy, select the Zone where you want to create a WLAN.
2. Click the option **Create**. to view the *Creating WLAN Configuration* page.
3. Go to **Data Plan Options** and select the RUCKUS GRE tunnel profile. By default, RUCKUS GRE and IPsec are enabled and attached at the zone level to the WLAN.
4. Click **OK**.

You have created the WLAN configuration.

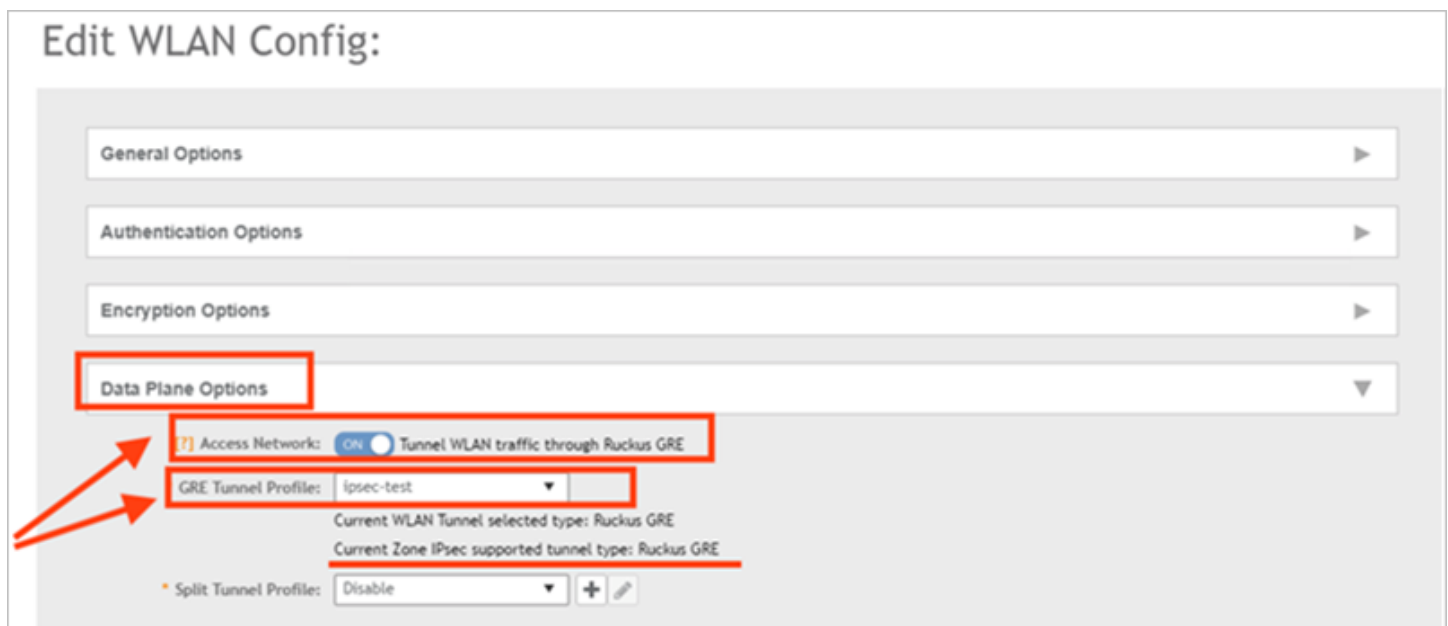
### NOTE

Peer reference identifiers are not configurable. The controller auto generates the reference identifiers to AP and DP.

## Mapping RUCKUS GRE and IPsec Profile to WLAN

1. Navigate to **Wireless LANs** page.
2. Select the Zone to either create a new WLAN or edit an existing WLAN.
3. Within WLAN configuration, in the **Data Plane Option**stab:
  - a. Select to enable the Access Networks.
  - b. Map to the RUCKUS GRE profile created.

Once you enable and select RUCKUS GRE, IPsec profile is applied based on AP Zone configuration.



# System IPsec

---

- [Configuring System IPsec using Preshared Key.....](#) 170
- [Configuring System IPsec using Certificates.....](#) 173
- [Configuring IKE and ESP Rekeying Separately.....](#) 176
- [Configuring System IPsec OCSF Settings.....](#) 179

System IPsec is the IPsec tunnel between SZ and external syslog server. All IPsec tunnels are NAT traversal.

If the connection between SZ and the IPsec gateway is unintentionally broken then:

- The user may need to re-connect using the **Re-connect** button from GUI to re-establish the connection.
- If the connection broken period is over the IKE rekey timeout, the system IPsec will go down and a system event #99104 will be triggered to notify users.
- If the connection broken period is within the IKE rekey timeout, the system IPsec sends retransmission request to the gateway every 10 seconds until the IKE rekey timeout or 360 retransmission tries.

# Configuring System IPsec using Preshared Key

You can configure the system IPsec settings by using preshared keys.

1. From the controller web interface, select **General Settings > System IPsec**.

**NOTE**

System IPsec Settings allows user to directly configure IPsec to Protect (Encrypt) the syslog data. IF System IPsec is not enabled syslog data will be in plain text. By default, discard packets from different subnets and are dropped/not handled.

Configure the following options:

- Security Gateway: Enter the security gateway endpoint IP address.
- Subnet: Enter the subnet that must be reachable by way of the IPsec tunnel
- Type: Click "Preshared Key"
- Preshared key: Enter the key

**ATTENTION**

The preshared key text ranges from 8 through 64 ASCII characters or 44 through 128 bit-based characters and any combination of upper and lower case letters, numbers, and special characters (that include: '!', '@', '#', '\$', '%', '^', '&', '\*', '(', and ')', except " or ' or \$( characters. For example, **Pa\$\$wOrd4F!rst%!P\$\*c#**.

- Under **IKE**, select the encryption algorithm, the integrity algorithm, and the rekey time.

**NOTE**

The supported encryption algorithms are AES128, AES192, and AES256. The supported integrity algorithms are SHA1, SHA256, SHA384, and SHA512. The IKE encryption proposals should be greater than or equal to the ESP encryption proposal. System IPsec supports IKEv2 only.

- Under **ESP**, select the encryption algorithm, the integrity algorithm, and the rekey time.

**NOTE**

The supported encryption algorithms are AES128, AES192, and AES256. The supported integrity algorithms are SHA1, SHA256, SHA384, and SHA512. By default, DH group is DH-20 [ECP-384], which cannot be changed.

- Under **Tunnel State**, view the status of the IPsec tunnel.

**NOTE**

System IPsec supports tunnel mode only.

FIGURE 169 System IPsec Settings

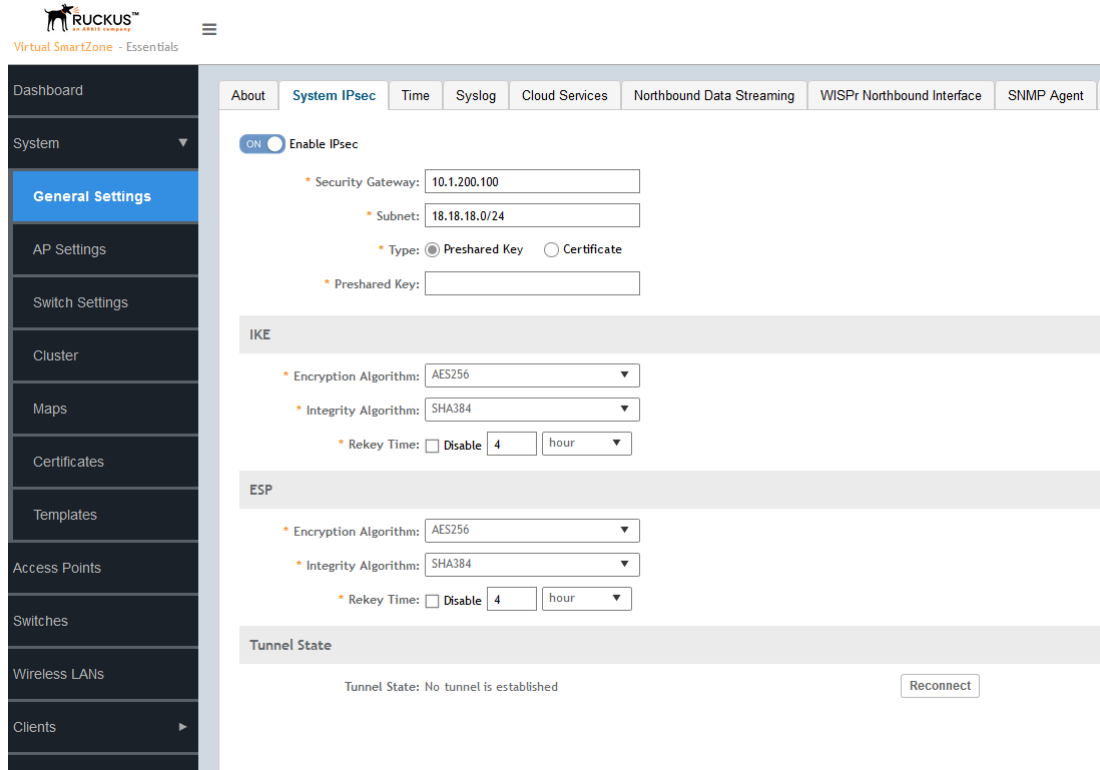
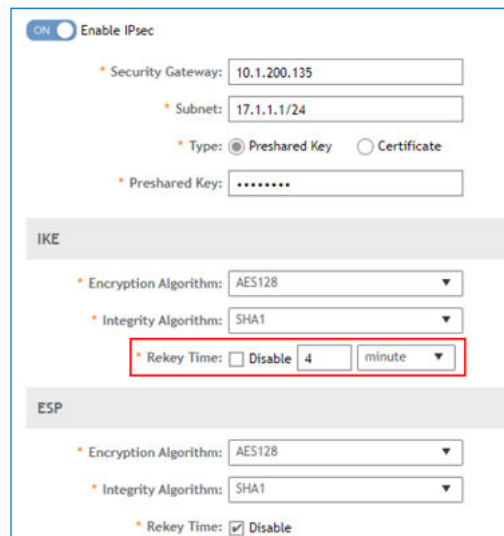


FIGURE 170 Enabling IKE Rekeying



## System IPsec

### Configuring System IPsec using Preshared Key

**FIGURE 171** Enabling ESP Rekeying

The screenshot shows the 'Enable IPsec' configuration window. At the top, there is a 'GUI' button and a radio button labeled 'Enable IPsec'. Below this, there are fields for 'Security Gateway' (10.1.200.135), 'Subnet' (17.1.1.1/24), and 'Type' (radio buttons for 'Preshared Key' and 'Certificate', with 'Preshared Key' selected). A 'Preshared Key' field contains several asterisks. The 'IKE' section has 'Encryption Algorithm' set to 'AES192', 'Integrity Algorithm' set to 'SHA1', and 'Rekey Time' checked with 'Disable'. The 'ESP' section has 'Encryption Algorithm' set to 'AES192', 'Integrity Algorithm' set to 'SHA1', and 'Rekey Time' set to '4' hours. A red box highlights the 'Rekey Time' field in the ESP section.

2. Click **OK**.

#### **NOTE**

If the connection is unintentionally broken then user has to re-connect using the 'Re-connect' button from GUI to re-establishes the connection.



# Configuring System IPsec using Certificates

You can configure the system IPsec settings by using certificates.

1. From the controller web interface, select **General Settings > System IPsec**.

Configure the following options:

- **Security Gateway:** Enter the security gateway endpoint IP address.
- **Subnet:** Enter the subnet that is reachable via IPsec tunnel
- **Type:** Click **Certificate**

**NOTE**

Both RSA and ECDSA private keys are supported.

- **Remote ID:** Enter the remote ID for certificate authentication.

**NOTE**

The Remote ID must be a distinguished name and the identifier to the external IPsec gateway.

- **Certificate:** Select a previously imported client certificate.
- **OCSP:** If the CA certificate has the OCSP [authorityinfoaccess] by default, the system IPsec CA certifications will be validated using the information certificates. Click **ON** to enable the OCSP as necessary and enter the OCSP validator URL, trusted certificate, and subject of the certifications that need to be validated.
- Under **IKE**, select the encryption algorithm, the integrity algorithm, and the rekey time.

**NOTE**

The supported encryption algorithms are AES128, AES192, and AES256. The supported integrity algorithms are SHA1, SHA256, SHA384, and SHA512. The IKE encryption proposals should be greater than or equal to the ESP encryption proposal. System IPsec supports IKEv2 authentication by X.509 certificate only.

- Under **ESP**, select the encryption algorithm, the integrity algorithm, and the rekey time.

**NOTE**

The supported encryption algorithms are AES128, AES192, and AES256. The supported integrity algorithms are SHA1, SHA256, SHA384, and SHA512. By default DH group will be DH-20 [ECP-384], which cannot be changed. System IPsec supports DH-20 only.

- Under **Tunnel State**, view the status of the IPsec tunnel.

**NOTE**

System IPsec supports tunnel mode only.

**System IPsec**  
Configuring System IPsec using Certificates

**FIGURE 172** System IPsec Settings

ON Enable IPsec

\* Security Gateway:

\* Subnet:

\* Type:  Preshared Key  Certificate

\* Remote ID:

\* Certificate:

\* OCSP:  OFF

---

**IKE**

\* Encryption Algorithm:

\* Integrity Algorithm:

\* Rekey Time:  Disable

---

**ESP**

\* Encryption Algorithm:

\* Integrity Algorithm:

\* Rekey Time:  Disable

2. Click **OK**.

You can import the System IPsec certificates from **System > Certificates > Import** . You can import the trusted CA certificates from **System > Trusted CA Certs > Import**.

Following is an example showing server certificate details:

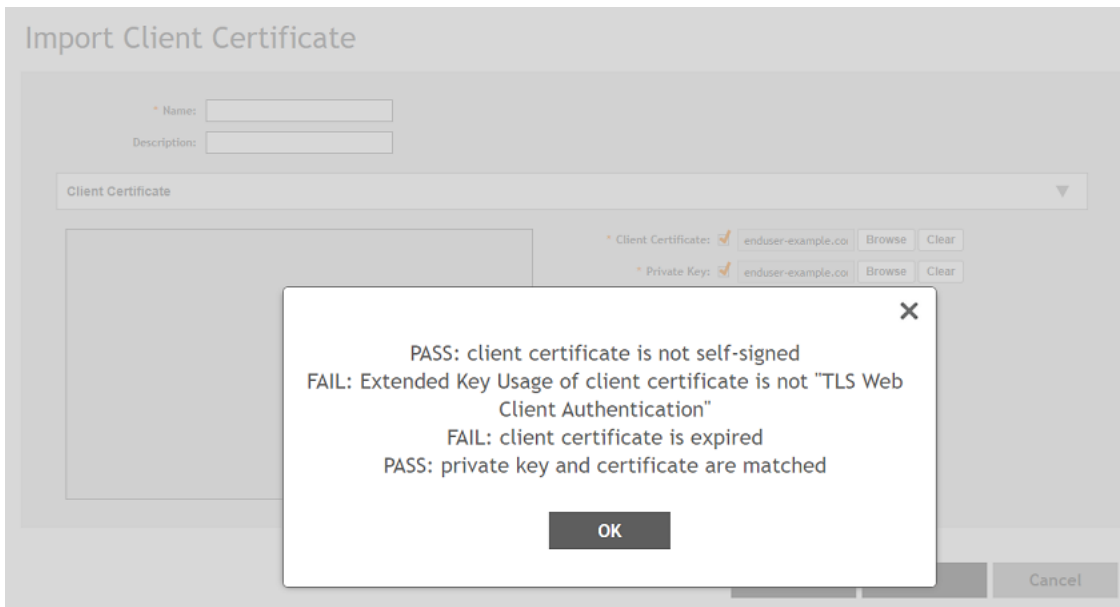
**FIGURE 173** Server Certificate Details

```
[root@IPSEC-CENTOS x509]# openssl x509 -in aaa.cert.pem -text -noout
Certificate:
  Data:
    Version: 3 (0x2)
    Serial Number: 4099 (0x1003)
    Signature Algorithm: sha384WithRSAEncryption
    Issuer: C=US, ST=CA, O=Arris, OU=RuckusNetwork, CN=IntermediateCA
    Validity
      Not Before: May 29 11:30:12 2019 GMT
      Not After : May 28 11:30:12 2020 GMT
    Subject: C=US, ST=aaa, L=aaa, O=aaa, OU=aaa, CN=aaa
    Subject Public Key Info:
      Public Key Algorithm: rsaEncryption
      Public-Key: (4096 bit)
      Modulus:
```

**NOTE**

For IPsec, for CA- Chain certificate validation refer [Configuring RadSec](#) on page 36.

The Client certificate also known as SZ's certificate must be uploaded, validated and saved for IPsec tunnel formation. The controller allows user to upload the client certificate eventhough the certificates fail to pass the certificate validation. The validation failed Import Client Certificate results in the failure of establishing the IPsec/TLS tunnel formation.



## Configuring IKE and ESP Rekeying Separately

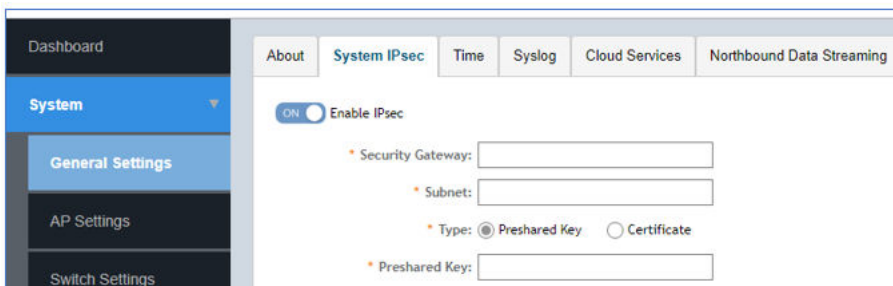
IKE and ESP Rekeying can be configured independently to initiate the rekeying on the established IPsec tunnel.

Perform the following steps to configure.

1. In the web interface, navigate to **System > General Settings > System IPsec Tab**
2. From the **Type** field, select either **Preshared Key** or **Certificate**.

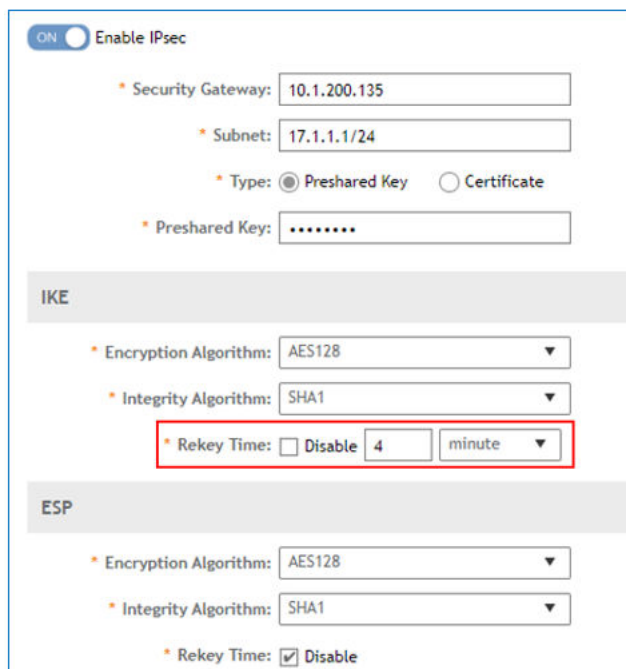
3. If **Preshared Key** is selected, perform the following.
  - a) Enable IPsec.

**FIGURE 174** Enabling IPsec



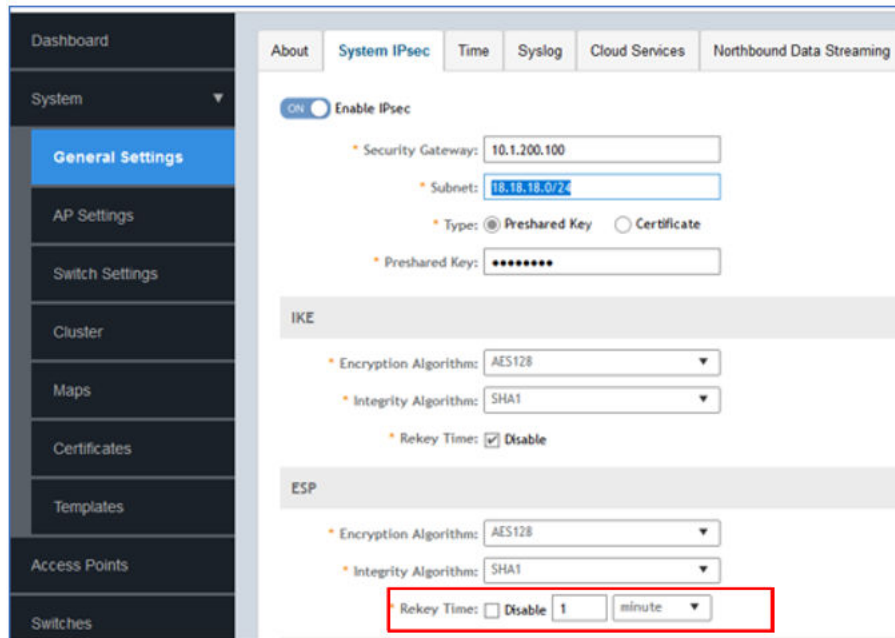
- b) In the IKE section, enable IKE Rekeying.

**FIGURE 175** Enabling IKE Rekeying



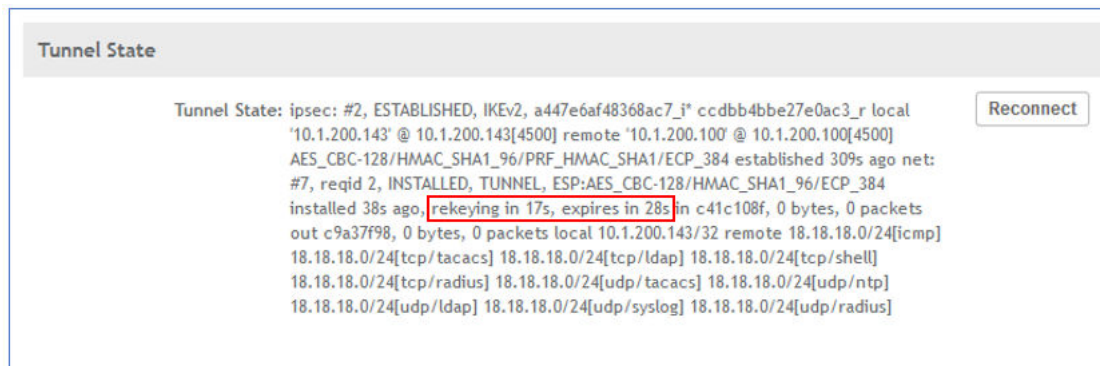
- c) In the ESP section, enable ESP Rekeying

FIGURE 176 Enabling ESP Rekeying



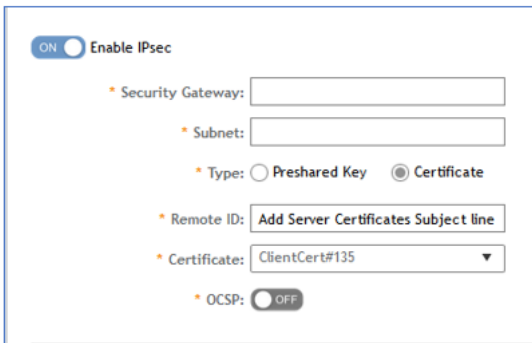
- d) After you click OK, the following message is displayed Successful IPsec tunnel creation with Rekeying information

FIGURE 177 Successful IPsec Tunnel Creation



4. If **Certificates** is selected, perform the following.
  - a) In the Certificate field, upload 'SZ as Client Certificate' and 'CA n sub-CA Certificate'.
  - b) In the Remote ID fiels, enter the IPsec GW certificates Subject line.  
For example, C=US, ST=CA, O=Ruckus Wireless Inc., CN=scg.ruckuswireless.com, EMAILADDRESS=service@ruckuswireless.com.

**FIGURE 178** Adding Certificate



The screenshot shows a configuration panel for IPsec. At the top, there is a toggle switch labeled 'Enable IPsec' which is currently turned 'ON'. Below this are several fields:

- 'Security Gateway': an empty text input field.
- 'Subnet': an empty text input field.
- 'Type': two radio buttons, 'Preshared Key' (unselected) and 'Certificate' (selected).
- 'Remote ID': a text input field containing the text 'Add Server Certificates Subject line'.
- 'Certificate': a dropdown menu with 'ClientCert#135' selected.
- 'OCSP': a toggle switch currently set to 'OFF'.

## Configuring System IPsec OCSP Settings

This feature assists you to check the status of the server certificates by configuring the OCSP settings.

If the OCSP is off, the system IPsec does not check the status of certificates. If OCSP is turned on, the controller asks you to complete the OCSP server information. At times, this is contradictory as you already have the authority access information in the peer and the CA certificates.

For example, the X.509 certificate indicates an OCSP server that can be accessed through URL. In such a case, if you want to access the OCSP server that is described in the peer or CA certificate, you should be able to skip the OCSP server settings. In some cases, you might want to use your own OCSP server, then the controller must allow you to configure the OCSP server.

You can configure the OCSP server settings in the following ways.

- Disabling OCSP
- Enabling the OCSP certificate status checking using the authority information embedded in the peer/CA certificate, this can be achieved by selecting the option **Prioritized with cert.**
- Enabling the OCSP certificate status checking using user specified OCSP server, this can be achieved by selecting the option **Prioritized with user specified.**

## System IPsec

### Configuring System IPsec OCSF Settings

To configure the OCSF settings, perform the following steps.

1. From the controller web interface, navigate to **System > General Settings > System IPsec**.

**FIGURE 179** Configuring System IPsec OCSF Settings

The screenshot shows the 'System IPsec' configuration page in the controller web interface. The left sidebar contains a navigation menu with 'System' selected, and 'General Settings' highlighted. The main content area has tabs for 'About', 'System IPsec', 'Time', 'Syslog', 'Cloud Services', and 'Northbound Data Streaming'. The 'System IPsec' tab is active. The configuration is as follows:

- Enable IPsec:** ON (toggle)
- Security Gateway:** 10.1.200.100
- Subnet:** 18.18.18.18/24
- Type:** Certificate (radio button selected)
- Remote ID:** CN=ruckuswireless.com
- Certificate:** IPSec\_Clientcertificate (dropdown)
- OCSP:** ON (toggle)
- OCSP action:** Prioritized with cert (radio button selected)

Below these are sections for 'IKE' and 'ESP':

- IKE:**
  - Encryption Algorithm: AES128 (dropdown)
  - Integrity Algorithm: SHA1 (dropdown)
  - Rekey Time:  Disable
- ESP:**
  - Encryption Algorithm: AES128 (dropdown)
  - Integrity Algorithm: SHA1 (dropdown)
  - Rekey Time:  Disable

A 'Tunnel State' section is visible at the bottom of the configuration area.

2. Click **Enable IPsec**.
3. Choose **Certificate** option in the **Type** field.
4. In the **Remote ID** field, type the subject line of the server certificate.
5. Select the peer/CA Certificate from the **Certificate** drop-down



6. You can enable or disable **OCSP**.

If you disable OCSP, you cannot view the status of the certificates.

The screenshot shows a configuration panel for IPsec. At the top, there is a toggle switch labeled "Enable IPsec" which is currently turned "ON". Below this, several fields are listed, each with an asterisk indicating it is required:

- Security Gateway:** 10.1.200.100
- Subnet:** 18.18.18.18/24
- Type:** Radio buttons for "Preshared Key" and "Certificate". "Certificate" is selected.
- Remote ID:** C=IN, ST=Karnataka, L=Bengal
- Certificate:** A dropdown menu showing "IPSec\_ocspURL".
- OCSP:** A toggle switch currently set to "OFF".

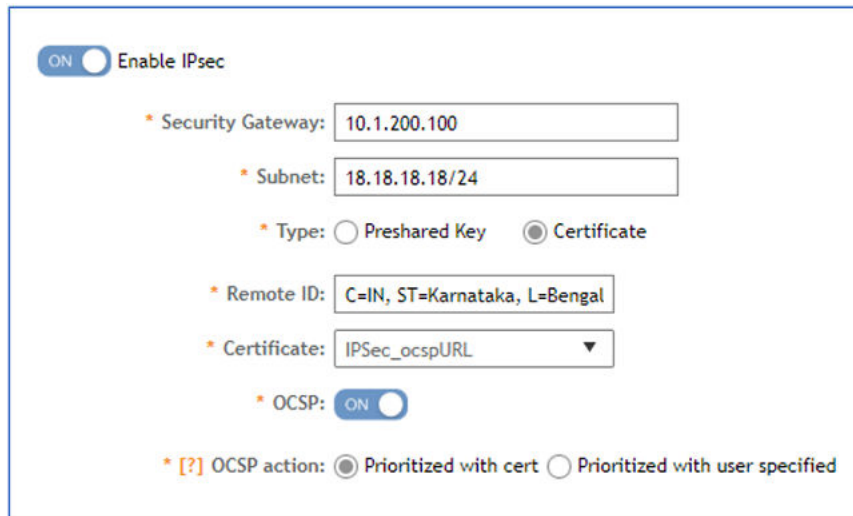
## System IPsec

### Configuring System IPsec OCSP Settings

7. To enable OCSP, select either **Prioritized with cert** or **Prioritized with user defined OCSP action** .

When OCSP on with the option **Prioritized with cert**, certificate authority information is chosen, the system checks the certificate status with certificate status server through OCSP. The system uses the OCSP server that is given by the authority information in the peer certificate. If there is no OCSP server information in peer certificate, the system IPsec will skip the certificate status checking.

**FIGURE 180** Enabling OCSP with Prioritized with cert OCSP action

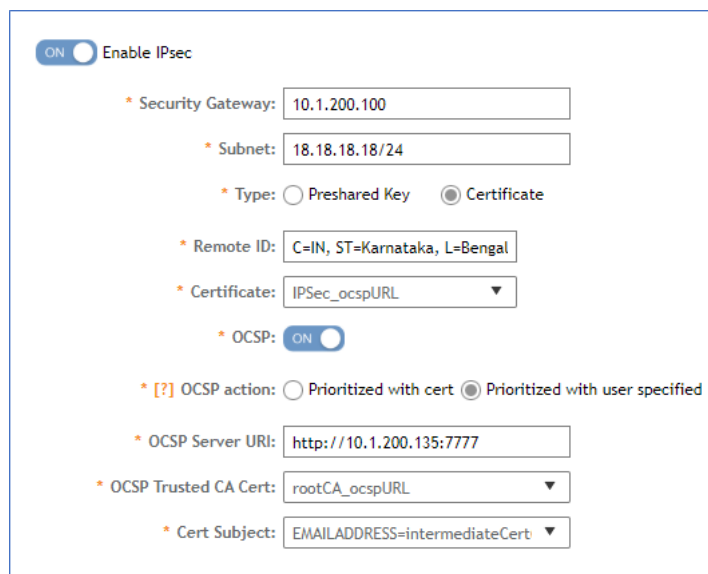


The screenshot shows the IPsec configuration interface with the following settings:

- Enable IPsec:** ON (checked)
- Security Gateway:** 10.1.200.100
- Subnet:** 18.18.18.18/24
- Type:** Certificate (selected)
- Remote ID:** C=IN, ST=Karnataka, L=Bengal
- Certificate:** IPSec\_ocspURL
- OCSP:** ON (checked)
- OCSP action:** Prioritized with cert (selected)

The user can configure additional OCSP server information using the option **Prioritized with user defined OCSP** where the user can give the OCSP server URL. This is useful in case of absence of OCSP setting of authority information embedded in the peer certificate. When system checks the certificate status, it uses the user specified OCSP server as higher priority.

**FIGURE 181** Enabling OCSP with Prioritized with user specified OCSP action



The screenshot shows the IPsec configuration interface with the following settings:

- Enable IPsec:** ON (checked)
- Security Gateway:** 10.1.200.100
- Subnet:** 18.18.18.18/24
- Type:** Certificate (selected)
- Remote ID:** C=IN, ST=Karnataka, L=Bengal
- Certificate:** IPSec\_ocspURL
- OCSP:** ON (checked)
- OCSP action:** Prioritized with user specified (selected)
- OCSP Server URI:** http://10.1.200.135:7777
- OCSP Trusted CA Cert:** rootCA\_ocspURL
- Cert Subject:** EMAILADDRESS=intermediateCert

8. In the **OCSP Server URL** field, enter the user defined OCSP Server URL

9. From the **OCSF Trusted CA Cert** drop-down, select the OCSF trusted certificate.

If the peer certificate authority information has OCSF server information, and user has manually configured the OCSF server, then the status of the certificate can be summarized as follows:

**TABLE 8** Checking the Staus of Server Certificate

Prioritized with user specified	Prioritized with cert	Final Result of Server Certificate Validation
PASS	PASS	PASS
OCSF server unreachable	PASS	PASS
PASS	OCSF server unreachable	PASS
OCSF server unreachable	OCSF server unreachable	FAIL
FAIL	PASS	FAIL
PASS	FAIL	PASS
FAIL	FAIL	FAIL



# Configuring System Time

The controller has three external Network Time Protocol (NTP) servers that are used to synchronize the time across Access Points, Cluster nodes, and vDPs.

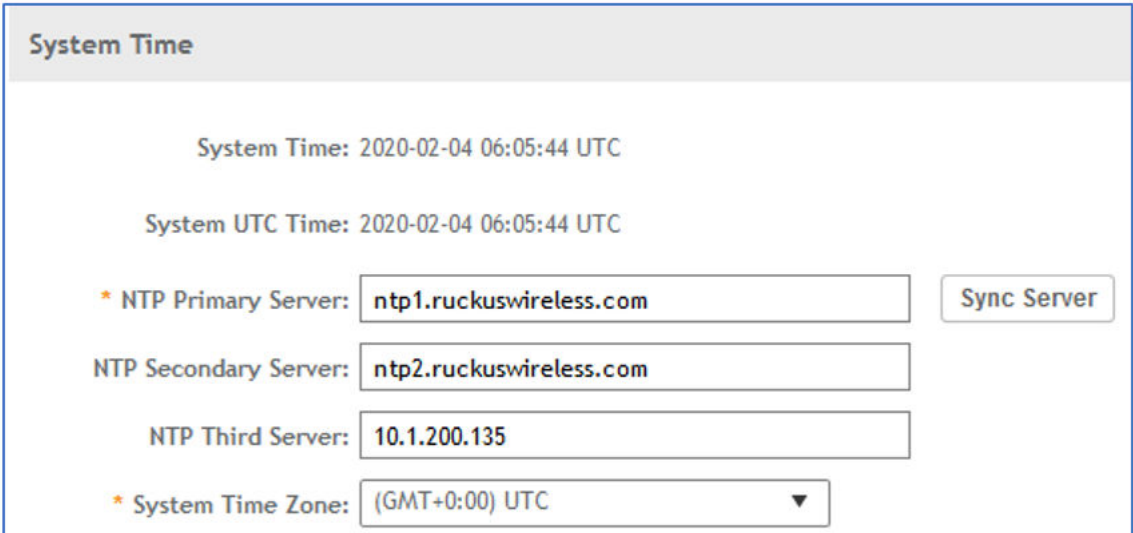
The controller synchronizes its time with that of the configured NTP server.

## NOTE

The controller supports version 4.2.6p5 of NTP. The SZ controllers and AP does not accept broadcast and multicast NTP packets that would result in the timestamp, these packets are ignored by default.

1. Go to **System > General Settings > Time**.

**FIGURE 182** Setting System Time



The screenshot shows the 'System Time' configuration page. At the top, the current system time is displayed as '2020-02-04 06:05:44 UTC'. Below this, the system UTC time is also shown as '2020-02-04 06:05:44 UTC'. There are three input fields for NTP servers: 'NTP Primary Server' with the value 'ntp1.ruckuswireless.com', 'NTP Secondary Server' with 'ntp2.ruckuswireless.com', and 'NTP Third Server' with '10.1.200.135'. A 'Sync Server' button is located to the right of the primary server field. At the bottom, the 'System Time Zone' is set to '(GMT+0:00) UTC' via a dropdown menu.

## Configuring System Time

- For **NTP Primary Server**, enter the NTP Server address that you want to use. By default, the controller uses its own clock to synchronize its time.

### NOTE

It is mandatory to configure the Primary Server. You can configure secondary and tertiary NTP server depending on the requirement.

**FIGURE 183** Configuring System Time for Secondary Server and Tertiary Servers

**System Time**

System Time: 2020-02-04 06:05:44 UTC

System UTC Time: 2020-02-04 06:05:44 UTC

\* NTP Primary Server:

NTP Secondary Server:

NTP Third Server:

\* System Time Zone: (GMT+0:00) UTC

**NTP Primary Server Authentication**

Key Type: SHA1

Key ID: 9

Key:  The PSK is provided by the NTP server, please fill it accordingly

**NTP Secondary Server Authentication**

Key Type: None

Key ID: 1 - 65534

Key:  The PSK is provided by the NTP server, please fill it accordingly

**NTP Third Server Authentication**

Key Type: SHA1

Key ID: 7

Key:  The PSK is provided by the NTP server, please fill it accordingly

- For **System Time Zone**, select the time zone from the list that you want the controller to use. The default time zone is (GMT +0:00) UTC.

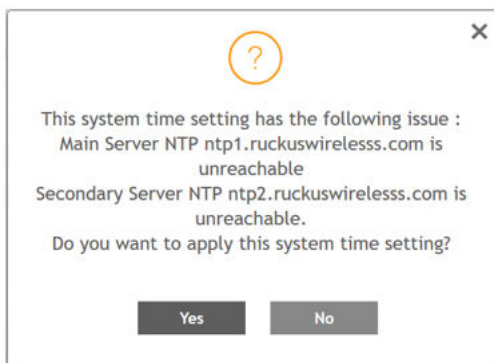
- Click **Sync Server** to enable an AP to join the controller and automatically synchronize its time every day.

If the **NTP Primary Server** is unreachable then secondary and tertiary NTP servers can be reached for synchronizing time. When primary and secondary NTPs are not reachable then the tertiary NTP server is used to sync the controller time.

**NOTE**

When the NTP Servers are unreachable, an event is triggered.

**FIGURE 184** Message when the NTP Servers are unreachable



- Under **NTP Authentication**, provide the NTP authentication (which includes the **Key Type** as **SHA1** and **Key ID** as [ranges from 1 through 65534], and **Key**).

**NOTE**

By enabling the NTP Server Authentication in FIPS mode, you can configure the NTP (Primary, Secondary and Tertiary) servers.

- Click **OK**.





# Administrating the Controller

- Administrating the Controller using CLI Console..... 189
- Administrating the Controller Remotely..... 190

## Administrating the Controller using CLI Console

All hardware platforms have console port which can be connected to CLI console switch to access the controller (SmartZone) console.

1. User can telnet to console switch using the **NewSZ300 Properties** to establish connection.

FIGURE 185 Establishing connection with SZ 300

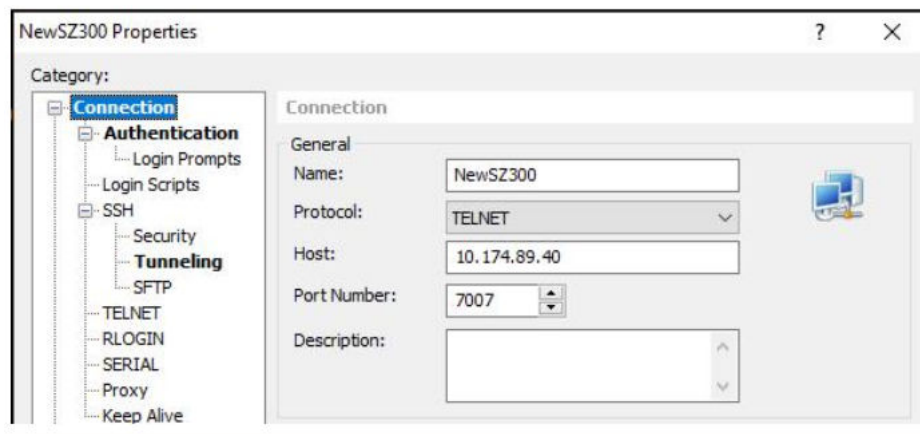


FIGURE 186 Logging into CLI

```
Connecting to 10.174.89.40:7007...
Connection established.
To escape to local shell, press 'Ctrl+Alt+].

Type the hot key to suspend the connection: <CTRL>Z

Login incorrect

login: root
Password:

Login incorrec
#####
#   Welcome to SmartZone 300   #
#####
SCG login: admin
Password:
Login incorrect

login: admin
Password:
Last login: Wed Mar 18 09:38:40 on ttyS0
Please wait. CLI initializing...

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

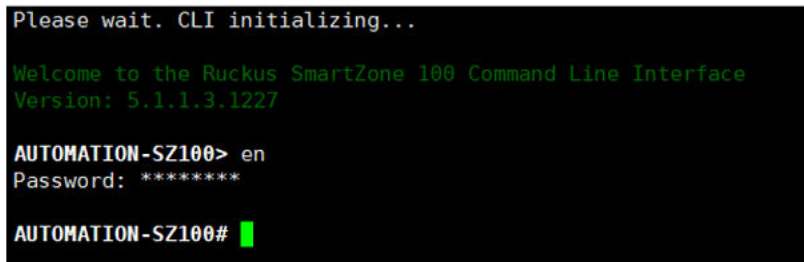
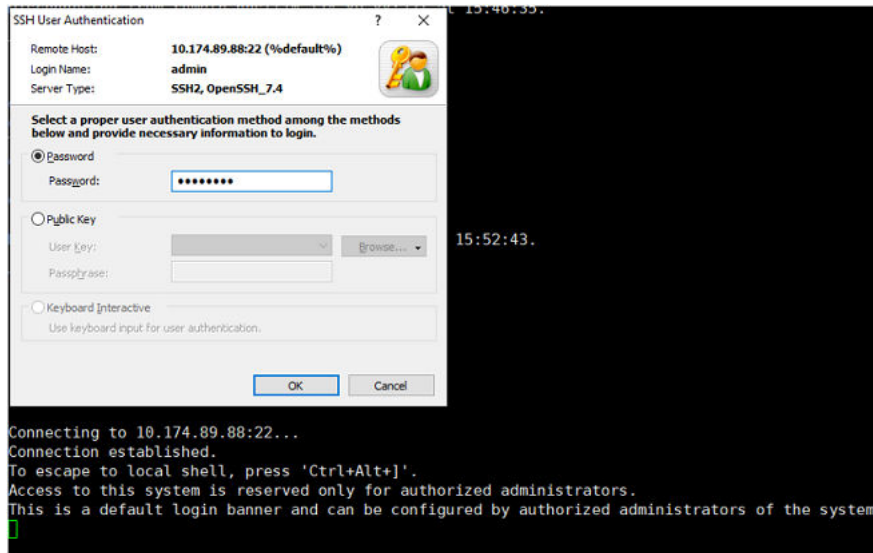
# Adminstrating the Controller Remotely

Controller (SmartZone) can be accessed remotely using SSH or Web UI.

1. Using controller (SmartZone) management IP address, user can SSH and login to CLI console.

For example, ssh admin@<SZ management IP>

FIGURE 187 Logging into CLI



The SSHv2 supports the following algorithms:

- a. **Encryption Algorithms (client and server):** aes128-ctr, aes256-ctr, <http://aes256-gcm@openssh.com>
- b. **Public and Host Key Algorithms (client):** ssh-rsa
- c. **Public Key Algorithms (server):** ssh-rsa, rsa-sha2-256, rsa-sha2-512, ecdsa-sha2-nistp384
- d. **Host Key Algorithms (Server):** ssh-rsa, ecdsa-sha2-nistp384
- e. **Data Integrity/MAC algorithms (client and server):** hmac-sha1, hmac-sha2-256, hmac-sha2-512

### NOTE

Per the PP, 'implicit' is included when [http://aes\\*-gcm@openssh.com](http://aes*-gcm@openssh.com) is selected as an encryption algorithm. When [http://aes\\*-gcm@openssh.com](http://aes*-gcm@openssh.com) is negotiated as the encryption algorithm, the MAC algorithm field is ignored and GCM is implicitly used as the MAC. "implicit" is not an SSH algorithm identifier and will not be seen on the wire; however, the negotiated MAC might be decoded as "implicit".

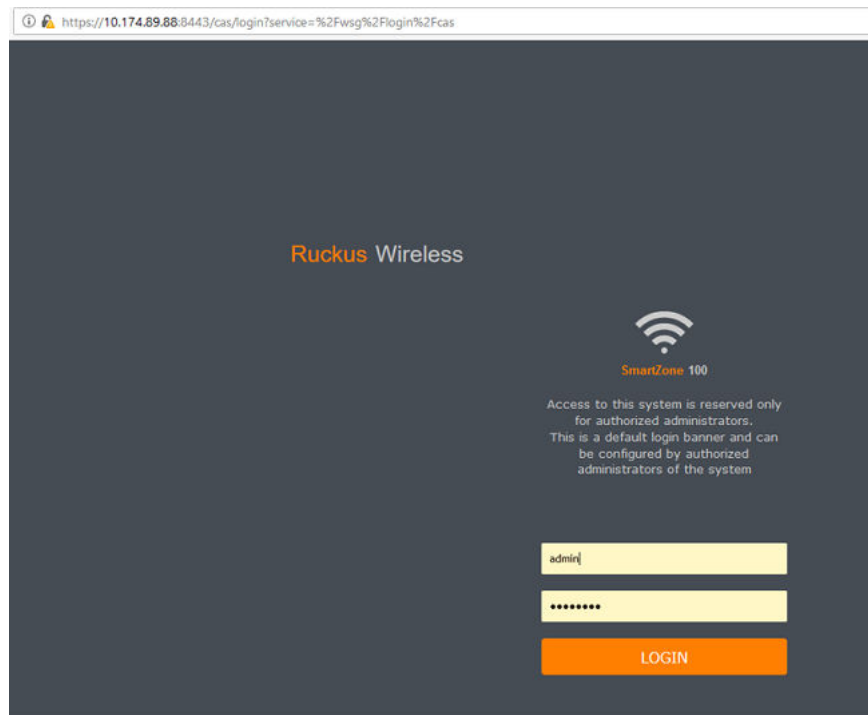
- f. **Key Exchange Methods (client and server):** diffie-hellman-group14-sha1, ecdh-sha2-nistp256, ecdh-sha2-nistp384 and ecdh-sha2-nistp521]

**NOTE**

If the SSH connection is broken then it can be manually re-established.

- 2. Enter the IP address `https://MGMT-INTERFACE-IP:8443` in the browser to access the controller Web UI.

**FIGURE 188** Logging using Web UI



Specific configuration is not required to access the SSH and Web UI session, its enabled by default. The controller provides remote administration of the system through secure communication channel (Web UI via HTTPS and CLI via SSH) . Accordingly, TLS version 1.2 is supported and the following cipher suites are supported for TLS/HTTPS:

- a. DHE-RSA-AES128-SHA256
- b. DHE-RSA-AES256-SHA256
- c. ECDHE-RSA-AES128-GCM-SHA256
- d. ECDHE-RSA-AES256-GCM-SHA384
- e. ECDHE-RSA-AES128-SHA256
- f. ECDHE-RSA-AES256-SHA384

**NOTE**

If the HTTPS/ Web UI connection is broken due to any issues then it can be manually re-established.

**NOTE**

Wireless clients connecting to a managed AP are communicating on the TOE's data channel and not via the management interface and therefore, cannot perform remote administration of the SZ.



# Configuring FIPS Disable Mode

- [Configuring the FIPS Disable Mode.....](#) 193
- [FIPS Disable Mode Matrix.....](#) 196
- [Features in FIPS Disable Mode.....](#) 197

## Configuring the FIPS Disable Mode

By default, SZ with FIPS build installed and ready for 'setup', has FIPS mode set to **DISABLE**.

1. User can choose the mode as **ENABLE** or can keep the default during initial setup.

**FIGURE 189** Initial Setup with FIPS Disable Mode

```
vSZ# setup

#####
Start vSZ setup process:
#####

*****
FIPS Setting
Current Status : Disable
*****

1. Enable FIPS
2. Keep Current Mode
*****

Select FIPS Mode (1/2): 2
```

2. Enter **fips status** to verify whether FIPS mode is enabled or disabled.

**FIGURE 190** Using the FIPS Status Command

```
vSZ# fips status
FIPS compliance is Disable
```

**NOTE**

When FIPS mode is enabled or disabled, vSZ is initiated with set-factory to clean up the configuration.

## Configuring FIPS Disable Mode

### Configuring the FIPS Disable Mode

3. Enter **fips disable** to disable FIPS mode, and enter **yes** to confirm.

**FIGURE 191** Using the FIPS Disable Command

```
Node1# fips disable
Zeroization will be initiated using set factory and the FIPS mode will be set to
Disable (or input 'no' to cancel)? [yes/no]
```

4. Enter **fips enable** to enable FIPS mode, and enter **yes** to confirm.

**FIGURE 192** Using FIPS Enable Command

```
Node2# fips status
FIPS compliance is Enable

Node2# fips disable
Zeroization will be initiated using set factory and the FIPS mode will be set to
Disable (or input 'no' to cancel)? [yes/no] yes
```

5. If the mode entered is same as current mode, then the warning is shown and no action can be taken further.

**FIGURE 193** Showing Warning Message

```
Node1# fips status
FIPS compliance is Disable

Node1# fips disable
Zeroization will be initiated using set factory and the FIPS mode will be set to
Disable (or input 'no' to cancel)? [yes/no] yes
FIPS compliance was already disabled

Node1#
```

6. Performing the **POST** and integrity tests in the fips disable mode.

**FIGURE 194** Performing the POST and Integrity Test

```
Bringing up interface br-tun: [ OK ]
Starting FIPS Self Test:[ OK ]
Start Integrity Check: Integrity test starts
Verifying system files ...
It takes a few minutes ...
RSA verify SUCCESS!
Integrity check failure file count: 0
[ OK ]
Starting irqbalance: [ OK ]
```

**NOTE**

SZ in FIPS disable mode is same as Regular SZ with POST operation during boot-up.

7. Enter **fips showlog** to display the results of an on-demand test of FIPS crypto modules.

FIGURE 195 Using the FIPS Showlog Command

```

vSZ# fips status
FIPS compliance is Disable

vSZ# fips showlog
=====OpenSSL selftest=====
DRBG: PASSED
X931: PASSED
SHA1: PASSED
SHA2: PASSED
HMAC: PASSED
CMAC: PASSED
AES : PASSED
AES-CCM : PASSED
AES-GCM : PASSED
AES-XTS : PASSED
DES : PASSED
RSA : PASSED
ECDSA : PASSED
DSA : PASSED
DH : PASSED
ECDH : PASSED
ECP384 : PASSED

vSZ#
  
```

## FIPS Disable Mode Matrix

### FIPS Disable Mode Matrix for Access Point (AP)

	FIPS Disable SZ	Regular SZ
FIPS AP	Supported	Rejected
Regular AP	Supported	Supported

### FIPS Disable Mode Matrix for Virtual Data Plane (vDP)

	FIPS Disable SZ	Regular SZ
FIPS vDP	Supported	Rejected
Regular vDP	Supported	Supported



## Upgrade Matrix in FIPS Disable Mode

### Upgrade Matrix in FIPS Disable Mode for Access Point (AP)

	FIPS Disable SZ	Regular SZ
FIPS ximg	Supported	Not Supported
Regular ximg	Not supported	Supported

### Upgrade Matrix in FIPS Disable Mode for Virtual Data Plane (vDP)

	FIPS Disable vDP	Regular vDP
FIPS ximg	Supported	Not Supported
Regular ximg	Not supported	Supported

## Features in FIPS Disable Mode

The features listed below are available in FIPS DISABLE mode and are NOT available in FIPS Enable Mode.

- FTP
- SNMPv2
- SNMPv3 with MD5 authentication
- SNMPv3 with NONE and DES privacy
- WLAN types Guest Access, Web Authentication, Std-MAC Authentication, Std OPEN NONE and WeChat.
- Encryption methods such as WPA-Mixed, WEP-64 (40 bits), WEP-128 (104 bits).
- On AP, http, tftp, ftp, snmpv2, snmpv3 with DES & MD5.



# Wireless Intrusion Detection and Prevention System

---

- Allowed Device Profile..... 199
- Monitoring Access Points (APs)..... 203
- Rogue Devices..... 206
- Audit/Event Alert..... 215
- Reports..... 217
- External Syslog Server..... 221
- Signature Based Detection Rule..... 223
- AP MAC OUI Address..... 228
- Different Rule types and Classification..... 228

Wireless Intrusion Detection and Prevention System (WIDS/WIPS) is a security structure that monitors a WLAN for any threats from rogue devices.

A user can create rogue classification policy with rules at the zone and monitoring group level. This helps in automatic classification behavior when a specific-rogue detection criteria are met.

## Allowed Device Profile

Allowed device profile contains list of MAC addresses of APs and EUDs that are part of the profile and considered as **authorized** devices.

This is a system-wide (Global) configuration. The MAC addresses can be imported via .CSV file or through user input.

To view a list of Allowed Device Profiles, go to **Services & Profiles > WIDS & WIPS > Allowed Device Profile**.

A user with **Administrator** privileges can **Create** a new allowed device, **Configure/Modify**, **Clone/Replicate** or **Delete** an allowed device profile of an AP/EUD.

A user should start the configuration with new Allowed Device Profile by adding MAC of an AP or EUD or both to the list.

## Configuring Allowed Device Profile

To create an allowed device profile, perform the following -

1. Go to **Services & Profiles > WIDS & WIPS > Allowed Device Profile** and click **Create**.  
This displays the **Create Allowed Device Profile** screen.

**FIGURE 196** Create Allowed Device Profile

**Edit Allowed Device Profile**

\* Name:

Description:

\* [?] Allowed Devices: \* Allowed AP MAC Entry  **+ Add** **Import CSV** **Cancel** **Delete**

Allowed AP MAC Entry ▲

C8:03:F5:2C:88:D0

1 records « 1 »

\* Allowed Client MAC Entry  **+ Add** **Import CSV** **Cancel** **Delete**

Allowed Client MAC Entry ▲

2C:33:61:56:CE:6B

1 records « 1 »

**OK** **Cancel**

2. Enter the following information in the respective fields. These are mandatory fields.
  - a. **Name:** Enter the name for the new Allowed Device Profile.
  - b. **Description:** Enter short description for the new Allowed Device Profile.
  - c. **Allowed Devices:** The allowed devices has two sections -
    - **Allowed AP MAC Entry:** Enter the MAC address of an AP to include in the allowed devices profile. User can enter the MAC address manually and click **Add**.

Or

To add multiple MAC addresses, click **Import CSV** the application navigates to the local file system.
    - **Allowed Client MAC Entry:** Enter the MAC address of the client to include in the allowed devices profile. User can enter the MAC address manually and click **Add**.

Or

To add multiple MAC addresses, click **Import CSV** this navigates to the local file system.

**NOTE**

To **Import CSV** file, refer [Import .csv file](#) on page 201.

3. After entering all the fields, click **OK**.

The newly created profile (EUD or AP or both) is displayed in the **Allowed Device Profile** list.
4. The **Allowed Device Profile** in the list can be **Configured** or **Cloned** or **Deleted**.

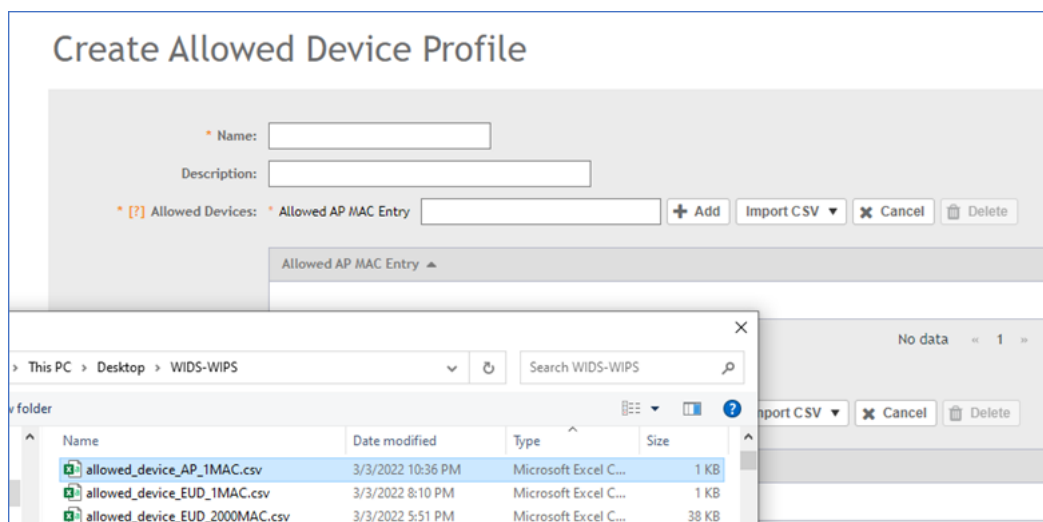
To perform any of the above action, select an **Allowed Device Profile** from the list and click the corresponding button.

**Import .csv file**

To import a .csv file in the **Allowed AP MAC Entry** and **Allowed Client MAC Entry**, perform the following -

1. Click **Import CSV**, the application navigates to the local file system.

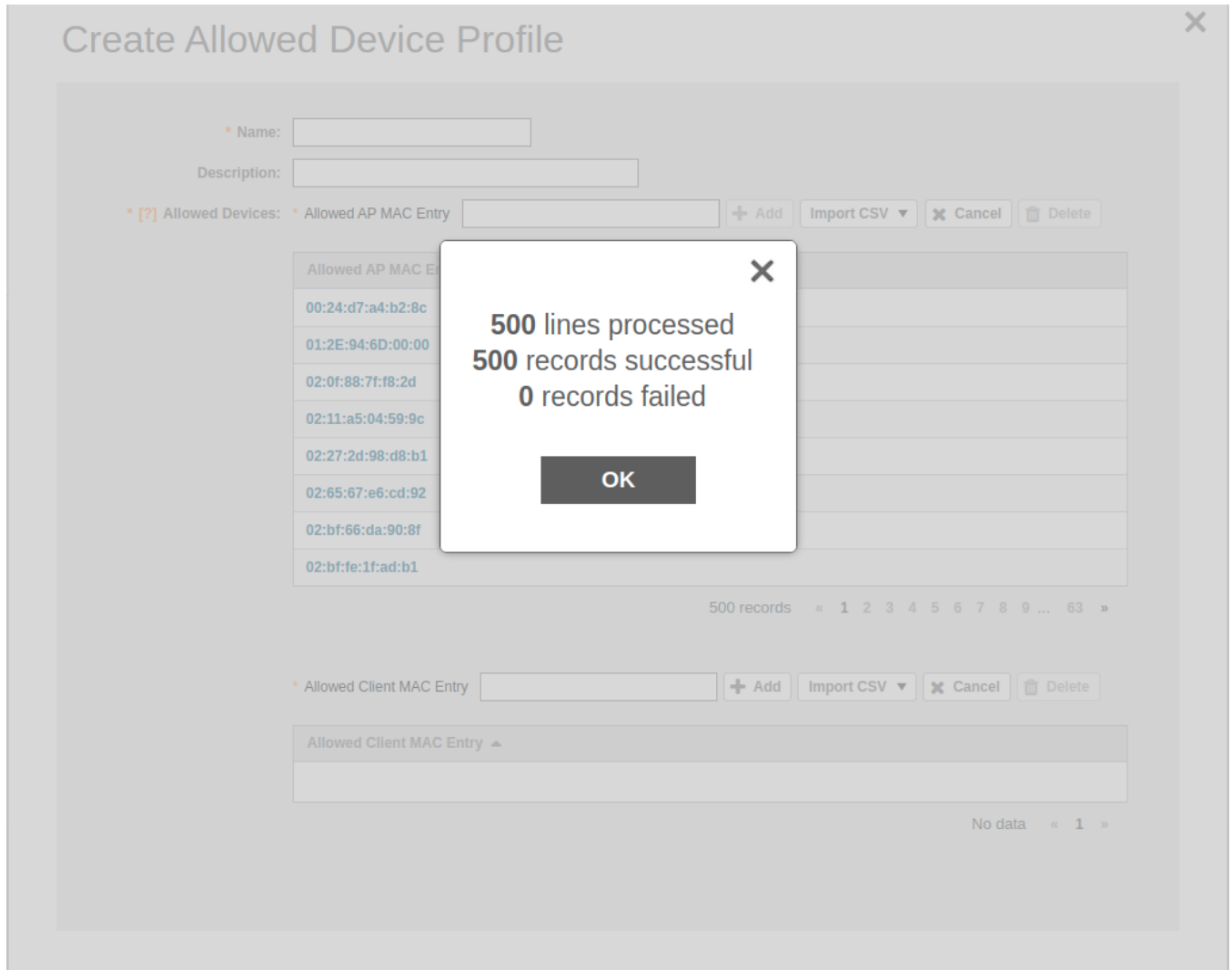
**FIGURE 197** .csv file upload



**Wireless Intrusion Detection and Prevention System**  
Allowed Device Profile

2. Map the location and select the .CSV file and click **Open**.

**FIGURE 198** .csv files\_uploaded



The list of MAC addresses is displayed in the **Allowed AP MAC Entry** table.

**NOTE**

Perform the above steps to import **Allowed MAC Client Entry**.

3. Click **Cancel** to abort the upload or select any of the MAC address in the **Allowed AP MAC Entry** or **Allowed Client MAC Entry** list and click **Delete** to erase the MAC address.

**NOTE**

The maximum number of **Allowed AP MAC Entry** is 500 and for **Allowed Client MAC Entry** is 2000 per profile. Maximum profiles for the system is 100.

## Monitoring Access Points (APs)

Monitoring AP can be deployed in 3 modes.

- Integrated Mode
- Overlay Mode
- Hybrid Mode

### Integrated Mode

Sensor and Service Mode - In service AP mode, Ruckus AP serving client detects rogue activities through background scanning and reports alerts to the SmartZone controller. It also contains threats by targeting de-authentication to the relevant devices. Service AP can be configured to scan the background in variable intervals.

### Overlay Mode

Monitoring AP mode - In monitor mode, Ruckus AP operates in continuous receive mode and performs forensic analysis on all the frames for different classes of threat and reports alerts to the SmartZone controller. Monitoring AP can be configured to monitor in 3 levels based on network deployment -

- Low - Scans every 120 seconds for rogue devices (AP/EUD).
- Medium - Scans every 60 seconds for rogue devices (AP/EUD).
- High - Scans every 20 seconds for rogue devices (AP/EUD).

### Hybrid Mode

Hybrid mode helps the user to incorporate integrated and overlay mode and supports the scanning of rogue devices and WLAN service to the Client/UEs. This enables WIDS at the zone level with a dedicated monitoring mode AP.

## Creating a Monitoring Access Point (AP)

As a prerequisite, the monitoring Access Point (AP) must be connected to the SmartZone controller.

The configuration starts with creating a new zone followed by enabling rogue detection and mapping a rogue policy. The new zone is mapped with default rogue classification policy. This default rogue classification policy can be modified by the user.

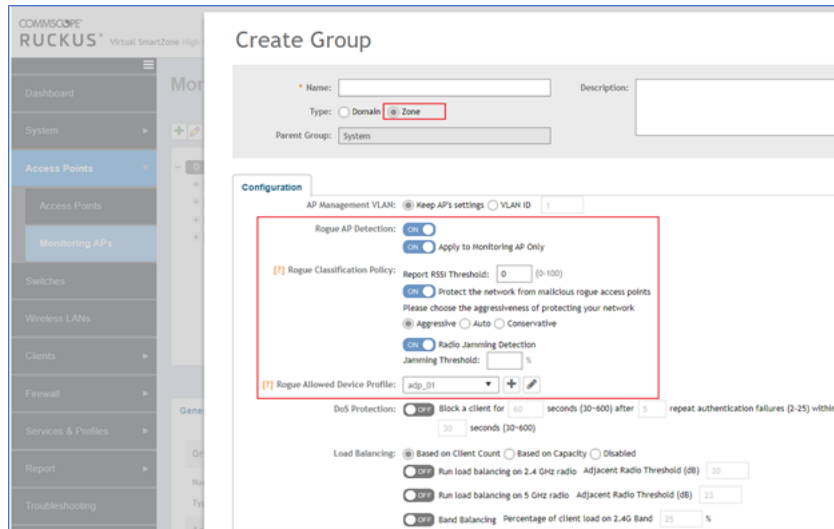
Perform the following procedure to create a new zone for the monitoring AP and enabling rogue detection and mapping the Allowed Device policy:

1. From the left pane, select **Access Points > Monitoring APs** to create a zone.

## Wireless Intrusion Detection and Prevention System Monitoring Access Points (APs)

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

**FIGURE 199** Create a Zone and Rogue AP Detection



3. Select **Type** as **Zone**.
4. Navigate to **Advanced Options**, enable **Rogue AP Detection**.
5. For **Rogue Classification Policy**, configure the following options:
  - a) In the **Report RSSI Threshold** field, enter the threshold (the threshold ranges from 0 through 100).
  - b) Enable **Protect the network from malicious rogue access points** and select one of the following options:
    - **Aggressive**
    - **Auto**
    - **Conservative**

### NOTE

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

- c) Enable **Radio Jamming Session** and enter the jamming threshold as a percentage.
- d) Map Rogue Allowed Device Profile from the drop-down list (refer Configuration of Allowed Device Profile)
- e) Click **OK**.



- On the **Access Points > Monitoring APs** page, select the created zone and click **+** to create the AP monitoring group.

**FIGURE 200** Creating an AP Monitoring Group

- Enter the group name.

To move an AP to the **Monitoring APs** group, perform the following steps -

- In the Access Points page, select the AP from the default/staging zone and click **Move**.
- In the **Select Destination AP Zone** management domain window, select the AP monitoring group and click **OK**.
- Viewing Associated Events
  - From the left pane, select **Monitoring APs**.
  - Select the zone and the corresponding monitoring AP and click **Event**.

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

**FIGURE 201** List of Events

Date and Time	Code	Type	Severity	Activity
2022/12/30 10:59:42	186	Classified rogue AP	Warning	AP [RuckusAP-M@20:58:69:38:D6:50] has detected a rogue AP[B4:3D:08:5A:97:30] with SSID[sagar katti 4g] and RSSI [1] on channel[7] classified as [Rogue] because of rogue classification policy (policy[No p...
2022/12/30 10:26:38	186	Classified rogue AP	Warning	AP [RuckusAP-M@20:58:69:38:D6:50] has detected a rogue AP[70:CA:97:BA:09:17] with SSID[] and RSSI [82] on channel[44] classified as [Rogue] because of rogue classification policy (policy[No policy matc...
2022/12/30 10:26:38	186	Classified rogue AP	Warning	AP [RuckusAP-M@20:58:69:38:D6:50] has detected a rogue AP[32:42:40:EA:9D:94] with SSID[Hathway_mallikarjun] and RSSI [18] on channel[7] classified as [Rogue] because of rogue classification policy (po...
2022/12/30 10:23:37	186	Classified rogue AP	Warning	AP [RuckusAP-M@20:58:69:38:D6:50] has detected a rogue AP[32:42:40:EA:9D:94] with SSID[Hathway_mallikarjun] and RSSI [17] on channel[7] classified as [Rogue] because of rogue classification policy (po...
2022/12/30 10:17:36	186	Classified rogue AP	Warning	AP [RuckusAP-M@20:58:69:38:D6:50] has detected a rogue AP[64:FB:92:60:21:E5] with SSID[www.excitel.com] and RSSI [0] on channel[7] classified as [Rogue] because of rogue classification policy (policy[...
2022/12/30 10:05:35	186	Classified rogue AP	Warning	AP [RuckusAP-M@20:58:69:38:D6:50] has detected a rogue AP[C2:94:AD:EB:7D:CE] with SSID[Vinuta K Shetty] and RSSI [1] on channel[7] classified as [Rogue] because of rogue classification policy (policy[NL...
2022/12/30 09:56:33	186	Classified rogue AP	Warning	AP [RuckusAP-M@20:58:69:38:D6:50] has detected a rogue AP[70:CA:97:3A:09:18] with SSID[WLAN_Mesh] and RSSI [61] on channel[7] classified as [Rogue] because of rogue classification policy (policy[No p...
2022/12/30 09:41:31	186	Classified rogue AP	Warning	AP [RuckusAP-M@20:58:69:38:D6:50] has detected a rogue AP[30:42:40:CA:9D:96] with SSID[] and RSSI [1] on channel[7] classified as [Rogue] because of rogue classification policy (policy[No rule matche...

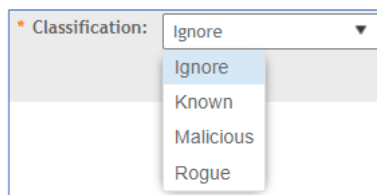
## Rogue Devices

Rogue APs and clients are unauthorized devices that may pose potential threats to a wireless network. Their activities can significantly impact the performance of a wireless network, or even cause serious security issues. The SmartZone's rogue device detection identifies the presence of rogue APs or clients, their behavior, and categorize them accordingly. The system can detect a wide range of wireless threats with the various configurable parameters.

To view rogue device, from the left pane, navigate to **Reports** and select **Rogue Devices**. This displays the **Rogue Devices** screen.

Ruckus APs can detect a wide range of wireless threats with configurable parameters. Rogue devices can be Classified into the following parameters

FIGURE 202 Classification Types



Below is the list of detection types supported for each classification policy.

FIGURE 203 Detection Types

Active Probing	Failed Attempts WLAN	RTS Abuse
Ad Hoc	ICS Connection	Same Network
Allowlisted AP	Long SSID	Signature Based
Allowlisted Client	Low RSSI	SSID
Auth Flood	MAC OUI	SSID Spoofing
Client MAC Spoofing	MAC Spoofing	Unauthorized Ap Broadcast Authorized SSID
Connected Unauthorized SSID	Max Clients	Unauthorized Auth Scheme
CTS Abuse	Mesh Network	Unauthorized Encryption Scheme
Deauth Flood	Non-Allowlisted AP	Unauthorized SSID
Disassoc Flood	Non-Allowlisted Client	Unencrypted Traffic
EAP Flood	Null SSID	Weak/Outdated Protocol
Excessive Power	Packet Flood	Weak/Unsupported/Disallowed Encryption Schem
		Windows Hosted Network

## Classifying a Rogue Policy

You can create rogue classification policy with rules at the zone and monitoring group level. This helps in automatic classification behavior when a specific-rogue detection criteria are met.

Complete the following steps to create a rogue classification policy.

1. Select **Services & Profiles > WIPS**.

- Under **Policy**, select the zone for which you want to create the policy and click **Create**.

**FIGURE 204** Creating a Rogue Classification Policy

Create Rogue Classification Policy

Name:

Description:

Rogue Classification Rules

+ Create Configure Delete Up Down search table Q

Priority ▲	Name	Type and Criteria	Classification
------------	------	-------------------	----------------

OK Cancel

- Enter the policy name and description.

4. Under **Rogue Classification Rules**, click **Create** and complete the following steps to create a rogue classification rule.
  - a) In the **Name** field, enter the rule name.
  - b) Under **Rule Type**, select one from the following rule type for classification:
    - **Ad Hoc**: The monitoring AP is able to detect the ad hoc network as a rogue.
    - **Clear to Send (CTS) Abuse**: Reported when the number of CTS frames per second to a specific receiver MAC address exceeds the specific threshold. The default number of frames per second is 50.
    - **Authentication Flood**: Reported when the number of Authentication frames per second exceeds the specific threshold from a specific transmitter. The default number of frames per second is 50.
    - **EAP Handshake Flood**: Reported when the number of EAPOL frames per second exceeds the specific threshold from a specific transmitter. The default number of frames per second is 50.
    - **Deauth Flood**: Reported when the number of deauthentication frames per second exceeds the specific threshold from a specific transmitter. The default number of frames per second is 50.
    - **Disassoc Flood**: Reported when the number of disassociation frames per second exceeds the specific threshold from specific transmitter. The default number of frames per second is 50.
    - **Request to Send (RTS) Abuse**: Reported when the number of RTS frames per second to a specific receiver MAC address exceeds the specific threshold. The default number of frames per second is 50.
    - **Excessive Power**
    - **Low RSSI**: In the **Signal Threshold** field, enter the RSSI threshold in dBm.
    - **MAC OUI**: In the **MAC OUI** field, enter the first three octets of the MAC address. For example, for a MAC address 11:22:33:44:55:66, the MAC OUI is 11:22:33.
    - **MAC (BSSID) Spoofing**
    - **Same Network**
    - **SSID**: Enter the partial or complete SSID string regardless of the zone being configured with the specific SSID.
    - **NULL SSID**
    - **SSID Spoofing**: Enter the SSID that is configured in a specific zone from a non-managed AP.
    - **Auth Flood**: Reported when the number of Auth flood frames per second exceeds the specific threshold from a specific transmitter. The default number of frames per second is 50.
    - **EAP Flood**: Reported when the number of EAP flood frames per second exceeds the specific threshold from a specific transmitter. The default number of frames per second is 50.
  - c) Under **Classification**, select one of the following actions to be taken for the selected rule type:
    - **Ignore**
    - **Know**
    - **Malicious**
    - **Rogue**
  - d) Click **OK** to save the changes.
5. Click **OK**.

**NOTE**

Click **Configure** or **Delete** to edit or delete a rogue classification policy respectively. To prioritize a classification rule, select the rule from the list and click **Up** or **Down** to position the rule.

**NOTE**

You can use CLI option in SZ to disable or change threshold packets per seconds for CTS abuse, RTS abuse, Deauth flood and disassociation flood.

- To change the threshold detection follow the CLI command: remote ap-cli <ap-mac> "set rogued <attack-type> <number pf packets>". Example: remote ap-cli 8c:fe:74:1c:d6:b8 "set rogued rtsthreshold 10"
- To enable / disable flood detection follow the CLI command : remote ap-cli <ap-mac> "set rogued <attack-type> enable/disable". Example: remote ap-cli 8c:fe:74:1c:d6:b8 "set rogued rtsdetect enable"

**FIGURE 205** CLI Commands for Disabling the Threshold Packets

```
Usage: set rogued
-> debug {level}          <level: 0-7>
-> rtsdetect {enable|disable} <enable or disable RTS frame detection>
-> rtsthreshold {value}    <value >= 1, num of frames per second>
-> ctsdetect {enable|disable} <enable or disable CTS frame detection>
-> ctsthreshold {value}    <value >= 1, num of frames per second>
-> deauthdetect {enable|disable} <enable or disable DEAUTH frame detection>
-> deauththreshold {value} <value >= 1, num of frames per second>
-> disassocdetect {enable|disable} <enable or disable DISASSOC frame detection>
-> disassocthreshold {value} <value >= 1, num of frames per second>
-> authdetect {enable|disable} <enable or disable AUTH frame detection>
-> auththreshold {value}  <value >= 1, num of frames per second>
-> eapdetect {enable|disable} <enable or disable EAP frame detection>
-> eapthreshold {value}   <value >= 1, num of frames per second>
```

## Viewing Rogue Devices

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

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

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

## Filtering Rogue Devices

From the list of rogue APs or rogue clients, you can filter the required rogue AP or rogue client based on rogue MAC address, type, or SSID.

Perform the following procedure to filter the rogue devices.

1. Select **Report > Rogue Devices**.
2. In the **Rogue Devices** page, select **Access Point** from the **Device Type** list and click **Settings** (⚙️).
3. In the **Apply Filters** page, enter the rogue MAC address for **Rogue MAC**.
4. Select **Type** from the list.

If **Device Type** is **Access Point**, select **Ignore**, **Known**, **Rogue**, or **Malicious**.

If **Device Type** is client, select **Active Probing**, **CTS Abuse**, **Data Encrypted**, **Deauth Flood**, **Disassoc Flood**, **Excessive Power**, **Known**, **Rogue Client**, and **RTS Abuse**, **Auth Flood** and **EAP Flood**.

5. Enter **SSID**.
6. Click **OK**.

### NOTE

You can click **Filter On** or **Filter Off** to add or remove the filters.

## Marking Rogue Access Points

You can mark a rogue (or unauthorized) AP as known.

To mark a rogue AP as known:

1. From the left pane, click **Report > Rogue Devices**. The **Rogue Devices** page is displayed.
2. Select the rogue AP from the list and click **Mark as Known**. The classification **Type** of the rogue AP changes to **Known**. You can also select the rogue AP from the list and click **Unmark** to change the classification.

## Locating a Rogue Device

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

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

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

3. Click **Locate Rogue**.

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

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

**FIGURE 206** Map View

### Home\_Office

Rogue AP is approximately located at position shown.

Rogue APs			
MAC: 8C:FE:74:23:55:38	Type: Rogue	SSID: FD_WPA2-PSK	Allow

Detecting APs		
MAC: 28:B3:71:2F:74:80	Name: M-R750	RSSI: 86
MAC: 20:58:69:3B:D6:50	Name: M-R650	RSSI: 81
MAC: C8:03:F5:2C:88:D0	Name: M-R850	RSSI: 66

OK

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

FIGURE 207 Satellite View

MAC Address	AP Name	Status	IP Address	Model	Channel (2.4G)	Channel (5G)	AP Firmware	Serial	Configuration Status	Registration State
28:83:71:2F:74:80	M-R750	Online	192.168.1.3	R750	1 (20MHz)	36 (80MHz)	5.2.1.3.1195	212002008858	Up-to-date	Approved

General Configuration Health Traffic Alarm Event **GPS Location**

M-R750		28:83:71:2F:74:80
AP Name	M-R750	
IP Address	192.168.1.3	
Channel	1 (20MHz), 36 (80MHz)	
Clients	0	
Traffic (1hr)	0	
Latency	N/A (2.4G)	N/A (5G)
Airtime Utilization	27% (2.4G)	2% (5G)
Connection Failure	0%	
<a href="#">See this AP in AP page</a>		

- +: Zoom in on the location.
- -: Zoom out of the location.

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

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

4. Click **OK**.

### Upload a Map

Upload map to a zone.

To upload a map, perform the following:

1. From the left pane, select **System > Maps**.  
This displays **Maps** screen.



2. To upload a map, click +.

This displays **Add Map** screen. In the **Details** section, enter the following:

- **Name** - Enter name of the map.
- **Description** - Describe the map in few words.
- **Location** - Enter the location details.
- **GPS Co-ordinates** - Latitude and Longitude details.
- **Map Image** - Upload the map image by clicking **Browse** button.

FIGURE 208 Add Map

**Add Map**

Details → Scale Map → Place APs

Name: HOME\_OFFICE\_MAP

Description:

Location: OFFICE Space at Home

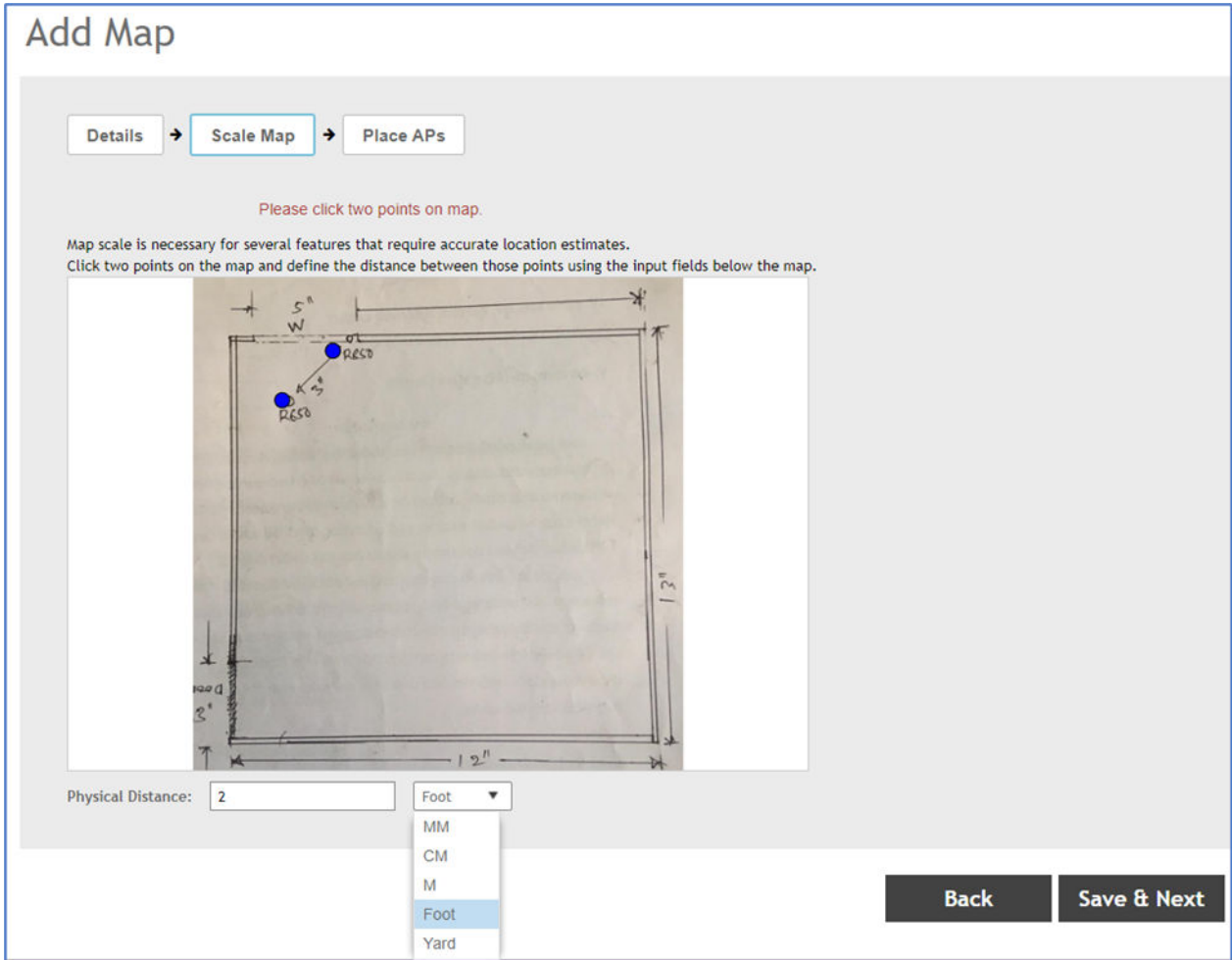
GPS Coordinates: Latitude: 25.07858 Longitude: 121.57141 example: 25.07858, 121.57141

Map Image: Home\_office\_floorplan.jpeg Browse

Next

3. Click **Next** and enter the **Physical Distance** and click on the two points of the map to define distance between those points.

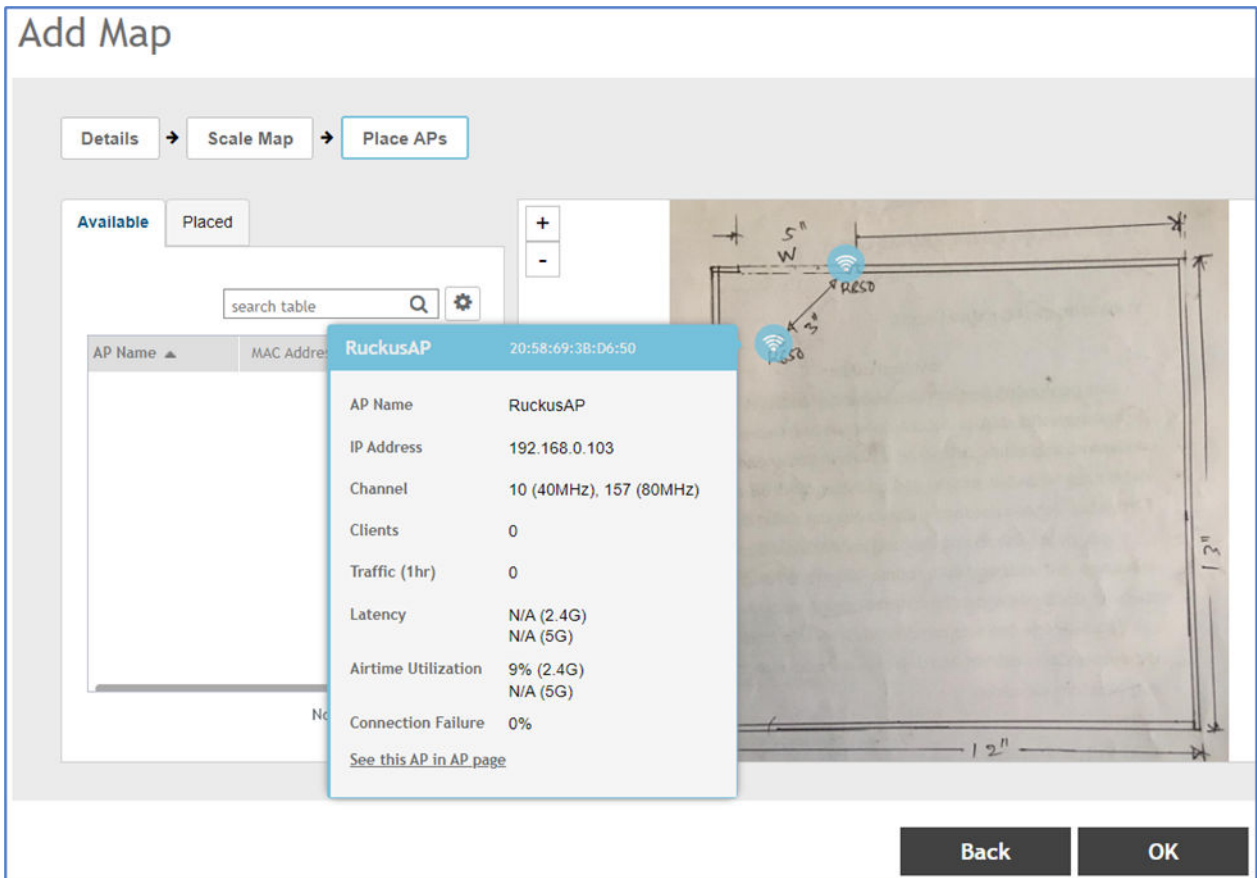
FIGURE 209 Physical Distance



4. Click **Save and Next**.

This displays **Place APs** list. Choose from the list of APs in the **Available** or **Placed** tab.

**FIGURE 210** Place APs



5. Click **Ok**.

The new map is uploaded to the zone.

**NOTE**

To view signal coverage of both the bands, click **Show Signal Coverage On** or **Off** button.

## Audit/Event Alert

After the successful detection of rogue devices, alerts are generated and reported to SmartZone controller. These alerts can be viewed by an Administrator.

The Audit alert/event report can be generated or viewed in two ways.

- System level Audit/Event Alert
- Zone level Audit/Event Alert

## System level Audit/Event Alert

To generate system level audit/event alerts, in the home page, navigate to **Event & Alarms**. Select **Events**. This displays the list of events available in the system.

FIGURE 211 Enable/Disable Zone Level Audit Alert

The screenshot shows the 'Events Management' interface. At the top, there are tabs for 'Events', 'Event Management', 'Event Threshold', and 'Switch Custom Events'. The 'Email Notification' section is active, showing a message: 'The SMTP server is currently disabled. You must enable and configure the SMTP server (Go to System >> General Settings >> SMTP) so notification emails can be delivered successfully.' Below this, there is a 'Notification Email for Events:' section with a radio button for 'Enable' selected and a 'Mail To:' input field. There are 'Refresh', 'OK', and 'Cancel' buttons. Below the email notification section is the 'Events' table. The table has columns for 'Category', 'Type', 'SNMP Notification', 'Email', 'DB Persistence', 'OID', and 'Description'. The table contains several rows of event data, including 'Classified rogue AP', 'AP image signing failed', 'AP service on standby cluster is expir...', 'Jamming attack', 'Classified Rogue Client', 'Client authentication failed', 'Client joined', and 'Client failed to join'.

Category	Type	SNMP Notification	Email	DB Persistence	OID	Description
AP Communication	Classified rogue AP	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	1.3.6.1.4.1.25053.2.10.1.59	This event occurs when AP detects a rogue AP(malicious/known/rogue) that is classified ...
AP Communication	AP image signing failed	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	1.3.6.1.4.1.25053.2.10.1.20	This event occurs when a AP image signing failed.
AP Communication	AP service on standby cluster is expir...	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	1.3.6.1.4.1.25053.2.10.1.20	This event occurs when a AP is connected to standby cluster over the expiration date
Warning	AP Communication	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	1.3.6.1.4.1.25053.2.10.1.20	This event occurs when a AP detects a radio jamming attack.
Warning	AP Communication	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	1.3.6.1.4.1.25053.2.10.1.20	This event occurs when a AP detects a rogue client.
Informational	Client	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	1.3.6.1.4.1.25053.2.10.1.100	This event occurs when a client fails to join WLAN on the AP due to authentication failur...
Informational	Client	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	1.3.6.1.4.1.25053.2.10.1.100	This event occurs when a client successfully joins WLAN on the AP.
Informational	Client	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	1.3.6.1.4.1.25053.2.10.1.100	This event occurs when the client is unable to connect to WLAN on AP.

### NOTE

Make sure to enable **DB Persistence** with this data is not written permanently and after 7 days the data is purged and the new events are written.

## Zone Level Audit/Event Alert

1. In the home page, navigate to **Access Points**. Select **Monitoring APs** and select any specific **Zone**. This displays the list of **Access Points** available in that particular zone.
2. Select the **Access Point** and click the **Event** tab. This displays the events and alerts specific to that access point.

FIGURE 212 Zone Level Audit Alerts

The screenshot shows the 'Monitoring Access Points' interface. On the left is a navigation menu with options like Dashboard, System, Access Points, Services & Profiles, Report, Troubleshooting, Administration, and Events & Alarms. The main area is titled 'Monitoring Access Points' and contains a table of access points and a list of events.

MAC Address	Status	IP Address	Model	Channel (2.4G)	Channel (5G)	AP Group
20:58:69:3B:D6:50	Online	192.168.0.103	R650	6 (20MHz)	44 (80MHz)	agp_Mahan

Date and Time	Code	Type	Severity	Activity
2022/11/30 14:50:40	194	Classified Rogue Client	Warning	Rogue client[DE:BA:CA:ED:00:00] with SSID[], BSSID[00:00:00:00:00:00] and RSSI [4] on ...
2022/11/30 14:50:40	194	Classified Rogue Client	Warning	Rogue client[42:4E:D7:CD:00:00] with SSID[], BSSID[00:00:00:00:00:00] and RSSI [4] on ...
2022/11/30 14:50:40	194	Classified Rogue Client	Warning	Rogue client[1D:17:94:06:00:00] with SSID[], BSSID[00:00:00:00:00:00] and RSSI [5] on ...
2022/11/30 14:50:40	194	Classified Rogue Client	Warning	Rogue client[F2:D4:5B:A8:00:00] with SSID[], BSSID[00:00:00:00:00:00] and RSSI [6] on ...
2022/11/30 14:50:40	194	Classified Rogue Client	Warning	Rogue client[1B:96:26:FC:00:00] with SSID[], BSSID[00:00:00:00:00:00] and RSSI [3] on ...

**NOTE**  
There are 4 types of severity level, Critical, Warning, Major and Info.

## Reports

Reports display a list of rogue devices that were detected in a specific zone containing one or more monitor APs.

Two types of reports are generated:

1. Access Point or AP reports
2. Client reports

### Access Points or AP Reports

Access Point or AP reports can be viewed by selecting a zone and device type as **Access Point**.

1. In the home page, navigate to **Report**. Select **Rogue Devices**. This displays system level **Rogue Devices** and by default **Access Point** is selected as **Device Type** on the top right hand corner.
2. To view list of zone level access points, select a specific zone under the **System** tree.

FIGURE 213 Viewing Access Point Report

The screenshot shows the 'Rogue Devices' report interface. On the left is a navigation sidebar with options like System, Access Points, Switches, Wireless LANs, Clients, Firewall, Services & Profiles, Report, Report Generation, Rogue Devices, Historical Client Stats, Ruckus AP Tunnel Stats, and Core Network Tunnel Stats. The main area displays a table of detected rogue devices with columns for Rogue MAC, Type, Allow Listed, Classification Policy, Channel (Last seen), Radio, SSID, Detecting AP Name, Zone, and RSSI. Below the table is a 'General' section providing details for the selected device (Rogue MAC: 8C:FE:74:23:55:3C).

Rogue MAC	Type	Allow Listed	Classification Policy	Channel (Last seen)	Radio	SSID	Detecting AP Name	Zone	RSSI
20:58:69:38:D6:5C	Rogue	Yes	No policy rule matched	44	802.11 ac	WPA2-Enterprise	AP-R850	MONITOR ZONE	70
20:58:69:7B:D6:5C	Rogue	Yes	No policy rule matched	44	802.11 ac	WAP3-Personal	AP-R850	MONITOR ZONE	70
20:58:69:8B:D6:5C	Rogue	Yes	No policy rule matched	44	802.11 ac	WPA3-Enterprise	AP-R850	MONITOR ZONE	70
28:B3:71:3F:2C:EC	Rogue	No	No policy rule matched	44	802.11 ac	JioPrivateNet	AP-R850	MONITOR ZONE	7
30:42:40:CA:9D:96	Rogue	No	No policy rule matched	44	802.11 a	N/A	AP-R850	MONITOR ZONE	12
3C:84:6A:7B:46:D6	Rogue	No	No policy rule matched	44	802.11 a	N/A	AP-R850	MONITOR ZONE	8
8C:FE:74:23:55:3C	Rogue	No	Matched by apLocation, rule [1]ssid, CustomSidRule	44	802.11 ac	AP_Location	AP-R850	MONITOR ZONE	75
8C:FE:74:63:55:3C	Rogue	No	No policy rule matched	44	802.11 ac	UEspool_SSID	AP-R850	MONITOR ZONE	75

**General**

Rogue MAC: 8C:FE:74:23:55:3C  
 Type: Rogue  
 Allow Listed: No  
 Classification Policy: Matched by apLocation, rule [1]ssid, CustomSidRule  
 Other Detected: N/A  
 Channel: 44  
 Radio Band: 5G  
 Radio: 802.11 ac  
 SSID: AP\_Location

FIGURE 214 Access Point (AP) Report Filters

The 'Apply Filters' dialog box contains the following fields:

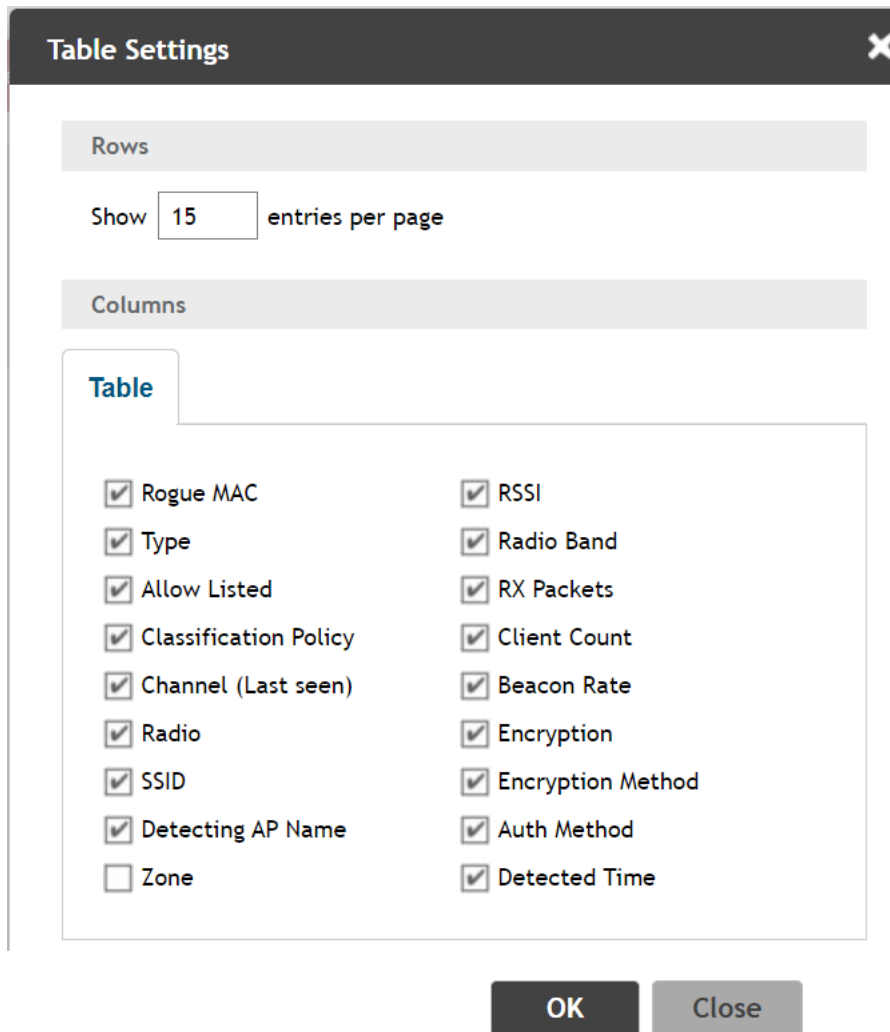
- Rogue MAC:
- Type:
- Allow Listed:
- SSID:

Buttons:   [Reset Filters](#)

**NOTE**

Click  icon to filter rogue devices based on the Rogue MAC, Type, Allow Listed and SSID. The AP report can be filtered and viewed only by the administrator user.

**FIGURE 215** Table Settings for Access Point (AP) Reports



**NOTE**

The tabs in the columns can be customized by clicking  icon and select the checkbox corresponding to the tab names.

## Client Report

Client reports can be viewed by selecting a zone and device type as **Client**.

1. In the home page, navigate to **Report**. Select **Rogue Devices**. This displays system level **Rogue Devices** and by default **Device Type** is selected as **Access Point** on the top right hand corner. Click the device type drop-down list and select **Client**.

## Wireless Intrusion Detection and Prevention System Reports

- To view list of zone level client list, select a specific zone under the **System** tree.

**FIGURE 216** Client Report

F4:D6:20:F4:75:E0	Rogue	No	Matched by Wi-Fi_Direct, rule [1]Ad Hoc, AdhocRule	48	JioPrivateNet	28:B3:71:3F:29:5C	RuckusAP	Z-MAHAN	11	5G	Encrypted	2022/12/12 12:35:42
F6:AD:D5:A9:F4:73	Rogue	No	No policy rule matched	6	N/A	00:00:00:00:00:00	RuckusAP	Z-MAHAN	14	2.4G	None	2022/12/12 12:33:02
F7:55:CF:27:00:00	Rogue	No	No policy rule matched	6	N/A	00:00:00:00:00:00	RuckusAP	Z-MAHAN	17	2.4G	None	2022/12/12 12:26:22
F8:20:39:00:00:00	Rogue	No	No policy rule matched	48	N/A	00:00:00:00:00:00	RuckusAP	Z-MAHAN	12	5G	None	2022/12/12 12:26:22
FE:FD:C9:DE:D3:90	Rogue	No	No policy rule matched	48	N/A	00:00:00:00:00:00	RuckusAP	Z-MAHAN	5	5G	None	2022/12/12 12:39:42

77 records

**General**

Rogue MAC: F4:D6:20:F4:75:E0

Type: Rogue

Allow Listed: No

Classification Policy: Matched by Wi-Fi\_Direct, rule [1]Ad Hoc, AdhocRule

Other Detected: N/A

Channel: 48

Radio Band: 5G

SSID: JioPrivateNet

BSSID: 28:B3:71:3F:29:5C

IP Address: N/A

Subnet Mask: N/A

Default Gateway: N/A

DHCP Server IP: N/A

DNS Server List: N/A

Encryption: Encrypted

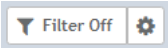
Encryption Method: WPA2

Auth Method: EAP

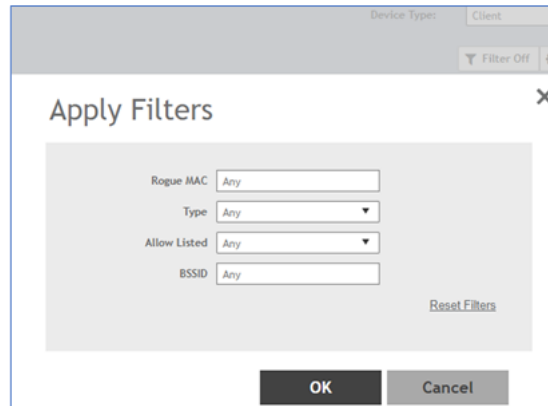
Last Detected: 2022-12-12 12:35:42



**NOTE**

Click  icon to filter rogue devices based on the Rogue MAC, Type, Allow Listed and BSSID. The Client report can be filtered and viewed only by an administrator.

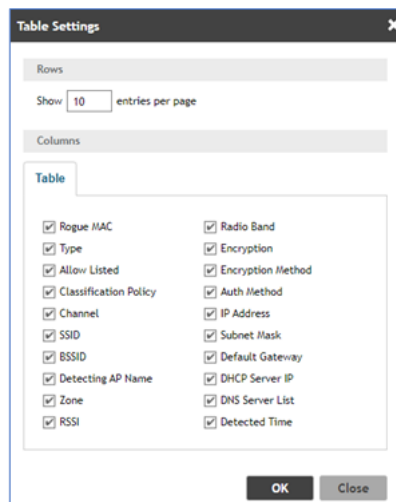
**FIGURE 217** Apply Filters Client Reports



**NOTE**

The tabs in the columns can be customized by clicking  icon and select the checkbox corresponding to the tab names.

**FIGURE 218** Table Settings for Client Reports



## External Syslog Server

System logging is a method where network devices use standard message format to communicate with a logging server. Configure an external syslog server to send the event logs from the SmartZone.

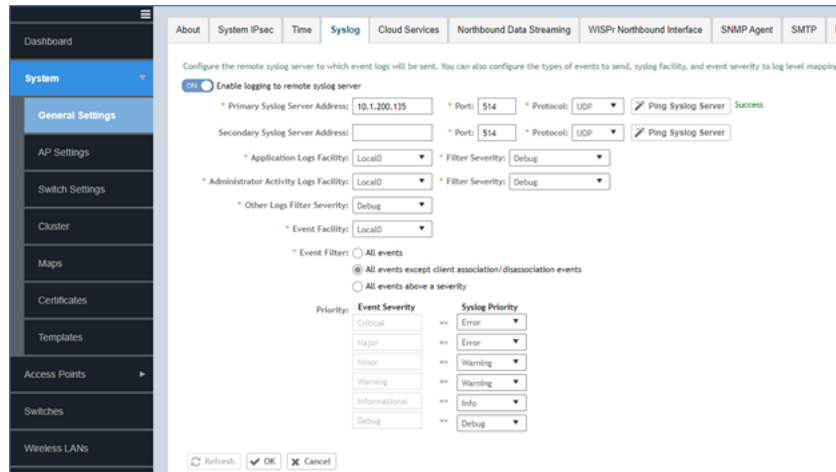
The alert/audit events are also forwarded to configured log server via secured way. User must configure an external log server to receive the alert/audit events.

## Configuring External Syslog Server

To configure an external syslog server, perform the following:

1. In the home page, navigate to **System** and select **General Settings**. This displays system information.
2. Click the **Syslog** tab. By default, **Enable logging to remote syslog server** is turned off. Click the button to turn **On** the remote server and configure the system log server and enter required details in the screen.
3. Click **Ok**.

FIGURE 219 External System Log Server



Test the reachability of external system log server using **ping syslog server**, **success** indicates it is ready to receive the alert/audit events. After the successful reception of the alerts, external system log server displays the message in the below format.

FIGURE 220 External System Log Server

```
Aug 19 06:43:58 ip-172-31-42-234 Core c.r.w.e.w.EventWriterThread - Got msg:
1660891438000,@@186,generalRogueAPDetected,"zoneUUID"="991ea315-bdbe-4601-a4f8-f0d70d4bf39d", "apMac"="20:58:69:38:D6:50",
"apName"="RuckusAP", "rogueMac"="34:E3:80:41:D7:00", "ssid"="SHRIKANTH", "wlanId"="11", "radio"="802.11g/n", "channel"="11", "timestamp"
="1660891426000", "rogueType"="Malicious", "roguePolicyName"="Default Policy", "rogueRuleName"="RTS Abuse Rule",
"rogueDetectedInfos"="Other detected: Rule[CTS Abuse Rule];", "rssi"="9", "rogueMatchedRuleDetectedMessage"="", "bssid"="",
"rfband"="2.4G", "serialNumber"="351939000263", "timeZone"="", "apLocation"="", "zoneName"="SBD_ZONE-7"

Aug 19 06:43:58 ip-172-31-42-234 Core: @@186,generalRogueAPDetected,"zoneUUID"="991ea315-bdbe-4601a4f8f0d70d4bf39d",
"apMac"="20:58:69:38:D6:50", "apName"="RuckusAP", "rogueMac"="34:E3:80:41:D7:00", "ssid"="SHRIKANTH", "wlanId"="11", "radio"="802.11
g/n", "channel"="11", "timestamp"="1660891426000", "rogueType"="Malicious", "roguePolicyName"="Default Policy", "rogueRuleName"="RTS
Abuse Rule", "rogueDetectedInfos"="Other detected: Rule[CTS Abuse Rule];", "rssi"="9", "rogueMatchedRuleDetectedMessage"="",
"bssid"="", "rfband"="2.4G", "serialNumber"="351939000263", "timeZone"="", "apLocation"="", "zoneName"="SBD_ZONE-7"

Aug 19 06:50:21 ip-172-31-42-234 Core c.r.w.e.w.EventWriterThread - Got msg:
1660891821000,@@194,classifiedRogueClientDiscovered,"zoneUUID"="991ea315-bdbe-4601-a4f8-f0d70d4bf39d",
"apMac"="20:58:69:38:D6:50", "apName"="RuckusAP", "rogueMac"="FE:4A:0B:B9:BF", "ssid"="", "wlanId"="0", "radio"="Unknown", "channel"
="11", "timestamp"="1660891565000", "rogueType"="Rogue", "roguePolicyName"="No policy matched", "rogueRuleName"="No rule
matched", "rogueDetectedInfos"="", "rssi"="1", "rogueMatchedRuleDetectedMessage"="null", "bssid"="00:00:00:00:00:00",
"rfband"="2.4G", "serialNumber"="351939000263", "timeZone"="", "apLocation"="", "zoneName"="SBD_ZONE-7"
```

The SmartZone user interface displays the events as shown in the below screen.

FIGURE 221 Testing External System Log Server

Timestamp	Severity	Source	Message
2022-08-19 12:07:58	Warning	AP [RuckusAP020586938 DK 50]	has detected a rogue AP(S4 E3 80 41 D7 00) with SSID [XXXXXXXXXX] and RSSI [0] on channel[1] classified as [Rogue] because of rogue classification policy [policy/No policy matched], rule[No rule matched].
2022-08-19 11:07:58	Warning	AP [RuckusAP020586938 DK 50]	has detected a rogue AP(S4 E3 80 41 D7 00) with SSID [XXXXXXXXXX] and RSSI [0] on channel[1] classified as [Malicious] because of rogue classification policy [policy/Default Policy], rule[No rule matched].
2022-08-19 09:50:08	Warning	Rogue client[90 0F 9C AF 8E 8F]	with SSID [XXXXXXXXXX], BSSID(S4 E3 80 41 D7 00) and RSSI [0] on channel[1] detected by [RuckusAP020586938 DK 50] and classified as [Rogue] because of rogue classification policy [policy/No policy matched], rule[No rule matched].
2022-08-19 09:35:08	Warning	Rogue client[90 0F 9C AF 8E 8F]	with SSID [XXXXXXXXXX], BSSID(S4 E3 80 41 D7 00) and RSSI [0] on channel[1] detected by [RuckusAP020586938 DK 50] and classified as [Rogue] because of rogue classification policy [policy/No policy matched], rule[No rule matched].
2022-08-19 08:37:05	Warning	AP [RuckusAP020586938 DK 50]	has detected a rogue AP(S4 E3 80 41 D7 00) with SSID [XXXXXXXXXX] and RSSI [0] on channel[1] classified as [Malicious] because of rogue classification policy [policy/Default Policy], rule[No rule matched]. Other detected: Rule[No rule matched].
2022-08-19 04:31:02	Warning	Rogue client[92 5A 48 10 F3 D4]	with SSID [XXXXXXXXXX], BSSID(S4 E3 80 41 D7 00) and RSSI [0] on channel[1] detected by [RuckusAP020586938 DK 50] and classified as [Rogue] because of rogue classification policy [policy/No policy matched], rule[No rule matched].

## Signature Based Detection Rule

Signature-based (SB) detection rules are global configuration. User can create signature-based rules once and use them in a zone or multiple zones. A set of signature-based rules form a signature based profile which can be mapped at a zone level. The same signature based profile can be mapped to different Zones. At a time, only one signature based profile can be mapped to a zone.

As part of the Wireless Intrusion Detection monitoring system (AP and EUD), monitoring AP scans for a specific pattern in the received frames from the EUDs (clients). The received frame (from EUD) is matched against the configured signatures. After successful detection an alert is triggered by SmartZone controller.

To view the list of signatures, go to **Services & Profiles > WIDS & WIPS > Signature-Based Rule**.

A user can **Create** a new Signature-based rule, **Configure/Modify**, **Clone/Replicate** or **Delete** an existing signature-based rule.

## Creating a Signature-Based Detection Profile

To create Signature-Based Rule, perform the following:

1. Go to **Services & Profiles > WIDS & WIPS > Signature-Based Rule** and click **Create**.

This displays the **Create Signature-Based Detection Profile** screen.

**FIGURE 222** Create Signature-Based Detection Profile

### Create Signature-Based Detection Profile

Name:

Description:

Rules ▼

**+ Create** Configure Delete

Name	Description	Scope	SignatureItems

**OK** **Cancel**

2. Enter the following information in the respective fields.
  - a. **Name:** Enter the name for the new Signature-Based Detection Profile.
  - b. **Description:** Enter a short description for the new Signature-Based Detection Profile.
  - c. **Rules:** User can **Create**, **Configure** and **Delete** a rule. To create a rule, perform the following:
    1. Click **Create**. This displays **Create Signature-Based Detection Rule** screen. Enter the information in fields:

FIGURE 223 Create Signature-Based Detection Rule

The screenshot shows a dialog box titled "Create Signature-Based Detection Rule". It has a close button (X) in the top right corner. The form contains the following elements:

- Name:** A text input field.
- Description:** A text input field.
- Scope:** Radio buttons for "Header" (selected) and "Body".
- Items:** A dropdown menu currently showing "Items".
- Buttons:** "+ Create", "Configure", and "Delete" buttons.
- Detail:** A text input field.
- Text:** "The operator for the rows of the grid is always the logical AND. The final rule will be:"
- Field:** A text input field containing "N/A".
- Bottom:** "OK" and "Cancel" buttons.

- **Name:** Enter a name for the rule.
- **Description:** Enter a short description for the rule.
- **Scope:** Select **Header** or **Body** for the rule.
- Click **Create** in the **Items** section. This displays **Create Signature-Based Detection Rule Item** screen.

FIGURE 224 Create Signature-Based Detection Rule Item

The screenshot shows a dialog box titled "Create Signature-Based Detection Rule Item". It has a close button (X) in the top right corner. The form contains the following elements:

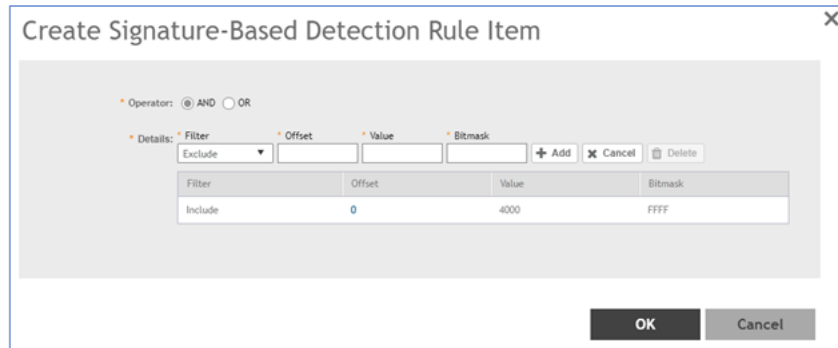
- Operator:** Radio buttons for "AND" (selected) and "OR".
- Details:** A table with columns: Filter, Offset, Value, Bitmask.
  - Filter:** A dropdown menu with "Include" selected.
  - Offset:** A text input field with "0".
  - Value:** A text input field with "4000".
  - Bitmask:** A text input field with "FFFF".
- Buttons:** "+ Add", "Cancel", and "Delete" buttons.
- Bottom:** "OK" and "Cancel" buttons.

- In this screen, select **Operator** options between **AND**, **OR**.
- In the **Details** column, select or enter the following fields:

**Wireless Intrusion Detection and Prevention System**  
Signature Based Detection Rule

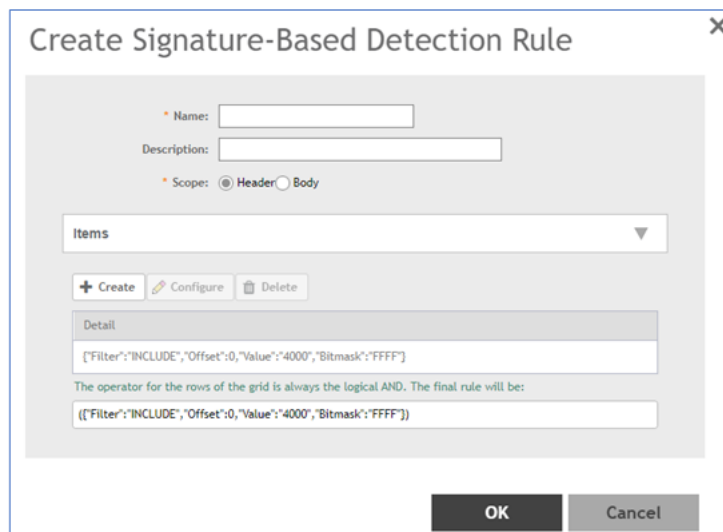
- **Filter:** Click on the drop-down menu and select the option to filter the rules.
- **Offset:** Enter an offset valid range, for **Header 0~31** and **Body 0~2311**
- **Value:** Enter a 64 bit value in hex format.
- **Bitmask:** As the value field is a 64 bit hex format, the **Bitmask** should be entered between F and FFFFFFFFFFFFFFFF hex range. Value and Bitmask field length should be equal, (for example, value=2e ; Bitmask = FF), here, value = 2;Bitmask = F.
- After entering the above fields, click **Add**. The new rule is displayed in the below table. Click **OK**.

**FIGURE 225** Signature-Based Detection Rule Item Added



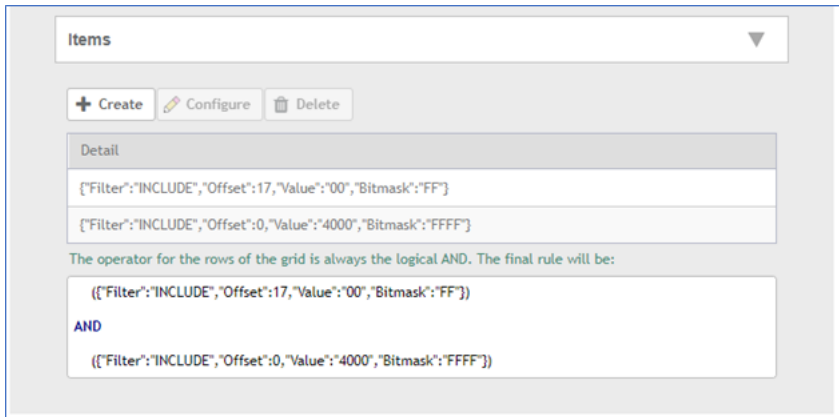
- The newly created Signature-Based Detection Rule/Item is displayed in the **Detail** table as per the configured items. Click **OK**.

**FIGURE 226** Create Signature-Based Detection Rules Details



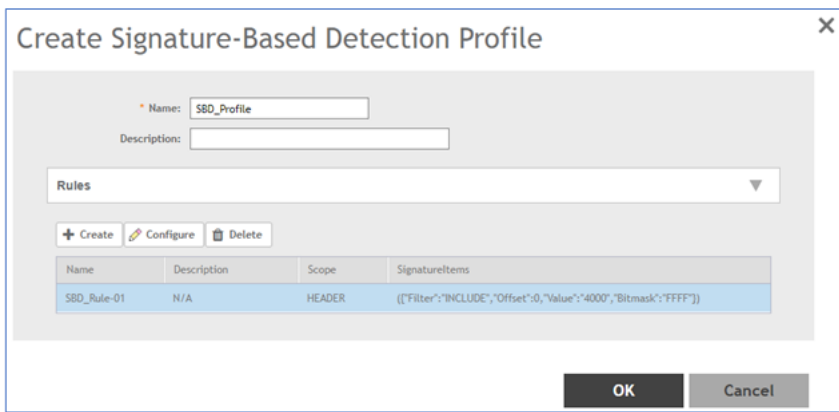
2. User can add multiple rule items with AND-OR, AND-AND & OR-OR operations under one rule in a SB profile.

FIGURE 227 AND-OR Rule



3. The new rule for the **Signature-Based Detection Profile** is created. Click **OK**.

FIGURE 228 One Rule Item



4. In case of multiple rules in one rule. The application displays the below screen.

FIGURE 229 Multiple Items in One Rule



## AP MAC OUI Address

User must enable the AP MAC OUI validation with specific Organizationally Unique Identifier (OUI) to allow an AP to connect to SmartZone. If the Access Point is not in the OUI list and it connects to the SmartZone, then the AP is rejected and event code 1294 is generated.

### Creating an AP MAC OUI Address

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

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

1. Select **System > AP Settings > AP MAC OUI Validation**.
2. Select **Enable AP MAC OUI Validation**.
3. Click **Create** to create the MAC OUI settings for an AP.

FIGURE 230 Creating an AP MAC OUI Address



The screenshot shows a dialog box titled "Create MAC OUI" with a close button (X) in the top right corner. The dialog contains two input fields: "MAC OUI:" (with a red asterisk indicating a required field) and "Description:". Below the input fields are two buttons: "OK" and "Cancel".

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

## Different Rule types and Classification

Rogue Classification Policy is configured to Detect and Report the rogues devices in the network.

Rogue classification policy has two main configurations for Detection and Reporting -

- Rule Type
- Classification

Rule type defines the type of rule to match the classification policy. The supported list is described in the below sections -



## Active Probing

The Monitoring AP detects active scanning (transmission of Probe Request Frames) by the EUDs and reports to the SmartZone.

FIGURE 231 Active Probing

A screenshot of a configuration interface for an 'Active Probing' rule. It features three fields: 'Name' with the value 'Active\_Probing', 'Rule Type' with a dropdown menu set to 'Active Probing', and 'Classification' with a dropdown menu set to 'Malicious'. Each field is preceded by an asterisk and followed by a descriptive text: 'Defines the type of rule to match for this classification policy' for Rule Type, and 'Defines the classification when the above criteria is matched' for Classification.

## Ad Hoc

Detect and report authorized clients establishing peer-to-peer connection with any other allowed/non-allowed client.

The following connection types are supported -

- Windows Ad Hoc Connection
- Mac OS Ad Hoc
- Linux Ad Hoc
- Wi-Fi Direct

FIGURE 232 Ad Hoc

A screenshot of a configuration interface for an 'Ad Hoc' rule. It features three fields: 'Name' with the value 'Ad\_Hoc', 'Rule Type' with a dropdown menu set to 'Ad Hoc', and 'Classification' with a dropdown menu set to 'Rogue'. Each field is preceded by an asterisk and followed by a descriptive text: 'Defines the type of rule to match for this classification policy' for Rule Type, and 'Defines the classification when the above criteria is matched' for Classification.

## AllowListed AP

Detect and report allowlisted AP. Allowlisted AP are those configured in the Allowed Device Profile associated with the Monitoring AP Zone.

FIGURE 233 AllowListed AP

A screenshot of a configuration interface for an 'Allowlisted AP' rule. It features three fields: 'Name' with the value 'Allowlisted\_AP', 'Rule Type' with a dropdown menu set to 'Allowlisted AP', and 'Classification' with a dropdown menu set to 'Rogue'. Each field is preceded by an asterisk and followed by a descriptive text: 'Defines the type of rule to match for this classification policy' for Rule Type, and 'Defines the classification when the above criteria is matched' for Classification.

## AllowListed Client

Detect and report allowlisted Client. Allowlisted Client are those configured in the Allowed Device Profile associated with the Monitoring AP Zone.

FIGURE 234 AllowListed Client

The screenshot shows a configuration form for the 'AllowListed Client' rule. It includes three fields: 'Name' with the value 'Allowlisted\_Client', 'Rule Type' set to 'Allowlisted Client' with a dropdown arrow, and 'Classification' set to 'Rogue' with a dropdown arrow. Each field has a small asterisk icon to its left. To the right of the 'Rule Type' and 'Classification' fields, there is explanatory text: 'Defines the type of rule to match for this classification policy' and 'Defines the classification when the above criteria is matched' respectively.

## Auth Flood

Detect and report if the number of authentication frames per second exceeds the specific threshold from a specific transmitter. The default number of frames per second is 50.

FIGURE 235 Auth Flood

The screenshot shows a configuration form for the 'Auth Flood' rule. It includes three fields: 'Name' with the value 'Auth\_Flood', 'Rule Type' set to 'Auth Flood' with a dropdown arrow, and 'Classification' set to 'Rogue' with a dropdown arrow. Each field has a small asterisk icon to its left. To the right of the 'Rule Type' and 'Classification' fields, there is explanatory text: 'Defines the type of rule to match for this classification policy' and 'Defines the classification when the above criteria is matched' respectively.

## Client MAC Spoofing

Detect and report the spoofing of MAC address of an allowListed client. The detection is possible when the client is connected to an allowlisted AP, and when the spoofing device is in a geographically distant area.

FIGURE 236 Client MAC Spoofing

The screenshot shows a configuration form for the 'Client MAC Spoofing' rule. It includes three fields: 'Name' with the value 'Client\_MAC\_Spoofing', 'Rule Type' set to 'Client MAC Spoofing' with a dropdown arrow, and 'Classification' set to 'Rogue' with a dropdown arrow. Each field has a small asterisk icon to its left. To the right of the 'Rule Type' and 'Classification' fields, there is explanatory text: 'Defines the type of rule to match for this classification policy' and 'Defines the classification when the above criteria is matched' respectively.

## Connected Unauthorized SSID

Detect and report authorized AP broadcasting a unauthorized SSID utilizing 2.4 GHz and 5GHz bands.

FIGURE 237 Connected Unauthorized SSID

The screenshot shows a configuration form for the 'Connected Unauthorized SSID' rule. It includes three fields: 'Name' with the value 'Unauthorized\_SSID', 'Rule Type' set to 'Connected Unauthorized SSID' with a dropdown arrow, and 'Classification' set to 'Rogue' with a dropdown arrow. Each field has a small asterisk icon to its left. To the right of the 'Rule Type' and 'Classification' fields, there is explanatory text: 'Defines the type of rule to match for this classification policy' and 'Defines the classification when the above criteria is matched' respectively.

## CTS Abuse

Detect and report if the number of CTS frames per second to a specific receiver MAC address exceeds the specific threshold. The default number of frames per second is 50.

FIGURE 238 CTS Abuse

A screenshot of a configuration interface for a rule named "CTS\_Abuse". It features three fields: "Name" with the value "CTS\_Abuse", "Rule Type" with a dropdown menu set to "CTS Abuse", and "Classification" with a dropdown menu set to "Rogue". Each field has a small asterisk icon to its left. To the right of the "Rule Type" and "Classification" dropdowns is a small text label: "Defines the type of rule to match for this classification policy" and "Defines the classification when the above criteria is matched" respectively.

## Deauth Flood

Detect and report if the number of deauthentication frames per second exceeds the specific threshold from a specific transmitter. The default number of frames per second is 50.

FIGURE 239 Deauth Flood

A screenshot of a configuration interface for a rule named "Deauth\_Flood". It features three fields: "Name" with the value "Deauth\_Flood", "Rule Type" with a dropdown menu set to "Deauth Flood", and "Classification" with a dropdown menu set to "Rogue". Each field has a small asterisk icon to its left. To the right of the "Rule Type" and "Classification" dropdowns is a small text label: "Defines the type of rule to match for this classification policy" and "Defines the classification when the above criteria is matched" respectively.

## Disassoc Flood

Detect and report if the number of disassociation frames per second exceeds the specific threshold from specific transmitter. The default number of frames per second is 50.

FIGURE 240 Disassoc Flood

A screenshot of a configuration interface for a rule named "Disassoc\_Flood". It features three fields: "Name" with the value "Disassoc\_Flood", "Rule Type" with a dropdown menu set to "Disassoc Flood", and "Classification" with a dropdown menu set to "Rogue". Each field has a small asterisk icon to its left. To the right of the "Rule Type" and "Classification" dropdowns is a small text label: "Defines the type of rule to match for this classification policy" and "Defines the classification when the above criteria is matched" respectively.

## EAP Flood

Detect and report if the number of disassociation frames per second exceeds the specific threshold from specific transmitter. The default number of frames per second is 50.

FIGURE 241 EAP Flood

A screenshot of a configuration interface for a rule named "EAP\_Flood". It features three fields: "Name" with the value "EAP\_Flood", "Rule Type" with a dropdown menu set to "EAP Flood", and "Classification" with a dropdown menu set to "Rogue". Each field has a small asterisk icon to its left. To the right of the "Rule Type" and "Classification" dropdowns is a small text label: "Defines the type of rule to match for this classification policy" and "Defines the classification when the above criteria is matched" respectively.

## Excessive Power

Detect and report if the traffic with excessive transmit power level exceeds the maximum.

## Wireless Intrusion Detection and Prevention System

### Different Rule types and Classification

FIGURE 242 Excessive Power

A screenshot of a configuration form for a rule named 'Excessive\_Power'. The form has three main sections: 'Name' with a text input field containing 'Excessive\_Power'; 'Rule Type' with a dropdown menu set to 'Excessive Power' and a descriptive text 'Defines the type of rule to match for this classification policy'; and 'Classification' with a dropdown menu set to 'Rogue' and a descriptive text 'Defines the classification when the above criteria is matched'.

## Failed Attempts WLAN

Detect and report high number of failed attempts to join the WLAN in a short period of time.

FIGURE 243 Failed Attempts

A screenshot of a configuration form for a rule named 'Failed\_Attempts'. The form has four main sections: 'Name' with a text input field containing 'Failed\_Attempts'; 'Rule Type' with a dropdown menu set to 'Failed Attempts WLAN' and a descriptive text 'Defines the type of rule to match for this classification policy'; 'Failed Attempts WLAN' with two input fields, the first containing '3' and the second containing '300', followed by the text '(times/seconds) Fail attempt times within the period'; and 'Classification' with a dropdown menu set to 'Rogue' and a descriptive text 'Defines the classification when the above criteria is matched'.

Failed attempts range is 3-20 times within 300-900 secs.

## ICS Connection

Detect and report the establishment of the ICS connection (Internet Connection Sharing).

FIGURE 244 ICS Connection

A screenshot of a configuration form for a rule named 'Failed\_Attempts'. The form has three main sections: 'Name' with a text input field containing 'Failed\_Attempts'; 'Rule Type' with a dropdown menu set to 'ICS Connection' and a descriptive text 'Defines the type of rule to match for this classification policy'; and 'Classification' with a dropdown menu set to 'Rogue' and a descriptive text 'Defines the classification when the above criteria is matched'.

## Long SSID

Detect and report when the SSID is larger than 32 bytes.

FIGURE 245 Long SSID

A screenshot of a configuration form for a rule named 'Failed\_Attempts'. The form has three main sections: 'Name' with a text input field containing 'Failed\_Attempts'; 'Rule Type' with a dropdown menu set to 'Long SSID' and a descriptive text 'Defines the type of rule to match for this classification policy'; and 'Classification' with a dropdown menu set to 'Rogue' and a descriptive text 'Defines the classification when the above criteria is matched'.

## Low RSSI

Detect and report Low RSSI when configured Signal Threshold is crossed.

FIGURE 246 Low RSSI

A screenshot of a configuration form for a 'Low RSSI' rule. The form has a light gray background and contains the following fields: 'Name' (empty text box), 'Rule Type' (dropdown menu with 'Low RSSI' selected), 'Signal Threshold' (text box with '10' and '(dBm) RSSI cutoff for rogue classification' to its right), and 'Classification' (dropdown menu with 'Rogue' selected). Each field is preceded by a red asterisk and a label.

## MAC OUI

Detect and report if the configured MAC is matched. In the MAC OUI field, enter the first three octets of the MAC address. For example, for a MAC address 11:22:33:44:55:66, the MAC OUI is 11:22:33.

FIGURE 247 MAC OUI

A screenshot of a configuration form for a 'MAC OUI' rule. The form has a light gray background and contains the following fields: 'Name' (empty text box), 'Rule Type' (dropdown menu with 'MAC OUI' selected), 'MAC OUI' (text box with '11:22:33' and 'Defines the MAC OUI (e.g. 11:22:33) to match for this classification rule' to its right), and 'Classification' (dropdown menu with 'Rogue' selected). Each field is preceded by a red asterisk and a label.

## MAC Spoofing

Detect and report the spoofing of the MAC address of an allowListed AP. It is also known as AP MAC (BSSID) spoofing .

FIGURE 248 MAC Spoofing BSSID

A screenshot of a configuration form for a 'MAC Spoofing' rule. The form has a light gray background and contains the following fields: 'Name' (empty text box), 'Rule Type' (dropdown menu with 'MAC Spoofing' selected), and 'Classification' (dropdown menu with 'Rogue' selected). Each field is preceded by a red asterisk and a label.

## Max Clients

Detect and report when the number of client connected to particular allowListed AP exceed the configured threshold (1-1024).

FIGURE 249 Max Clients

A screenshot of a configuration form for a 'Max Clients' rule. The form has a light gray background and contains the following fields: 'Name' (empty text box), 'Rule Type' (dropdown menu with 'Max Clients' selected), 'Client Maximum' (text box with '3'), and 'Classification' (dropdown menu with 'Rogue' selected). Each field is preceded by a red asterisk and a label.

## Mesh Network

Detect and report the establishment of point-to-point wireless bridge with an allowListed APs.

FIGURE 250 Mesh Network

A screenshot of a configuration interface for a 'Mesh Network' rule. It features three fields: 'Name' (a text input), 'Rule Type' (a dropdown menu set to 'Mesh Network'), and 'Classification' (a dropdown menu set to 'Rogue'). Each field is preceded by a red asterisk. To the right of the 'Rule Type' and 'Classification' dropdowns, there is explanatory text: 'Defines the type of rule to match for this classification policy' and 'Defines the classification when the above criteria is matched' respectively.

## Non-Allowlisted AP

Detect and report the deployed non-allowListed AP that are not part of the configured Allowed Device profile.

FIGURE 251 Non-Allowlisted AP

A screenshot of a configuration interface for a 'Non-Allowlisted AP' rule. It features three fields: 'Name' (a text input), 'Rule Type' (a dropdown menu set to 'Non-Allowlisted AP'), and 'Classification' (a dropdown menu set to 'Rogue'). Each field is preceded by a red asterisk. To the right of the 'Rule Type' and 'Classification' dropdowns, there is explanatory text: 'Defines the type of rule to match for this classification policy' and 'Defines the classification when the above criteria is matched' respectively.

## Non-Allowlisted Client

Detect and report the Deployed non-allowListed client that are not part of the configured Allowed Device profile and connected to AP.

FIGURE 252 Non-Allowlisted Client

A screenshot of a configuration interface for a 'Non-Allowlisted Client' rule. It features three fields: 'Name' (a text input), 'Rule Type' (a dropdown menu set to 'Non-Allowlisted Client'), and 'Classification' (a dropdown menu set to 'Rogue'). Each field is preceded by a red asterisk. To the right of the 'Rule Type' and 'Classification' dropdowns, there is explanatory text: 'Defines the type of rule to match for this classification policy' and 'Defines the classification when the above criteria is matched' respectively.

## Null SSID

Configure the AP to have null SSID. In WLAN config Advanced option turn 'ON' the 'Hide SSID'. Attempt to connect an allowListed EUD to the AP without supplying the correct AP SSID. Mon AP should detect & report this.

FIGURE 253 Null SSID

A screenshot of a configuration interface for a 'Null SSID' rule. It features three fields: 'Name' (a text input), 'Rule Type' (a dropdown menu set to 'Null SSID'), and 'Classification' (a dropdown menu set to 'Rogue'). Each field is preceded by a red asterisk. To the right of the 'Rule Type' and 'Classification' dropdowns, there is explanatory text: 'Defines the type of rule to match for this classification policy' and 'Defines the classification when the above criteria is matched' respectively.

## Packet Flood

Detect and report the Generation a large amount of TCP/UDP traffic from a given client(s).

FIGURE 254 Packet Flood

A screenshot of a configuration form for a 'Packet Flood' rule. It features three main fields: 'Name' (a text input), 'Rule Type' (a dropdown menu set to 'Packet Flood'), and 'Classification' (a dropdown menu set to 'Rogue'). Each field is accompanied by a small asterisk icon and a descriptive text label: 'Name: [input]', '\* Rule Type: Packet Flood [dropdown] Defines the type of rule to match for this classification policy', and '\* Classification: Rogue [dropdown] Defines the classification when the above criteria is matched'.

## RTS Abuse

Reported when the number of RTS frames per second to a specific receiver MAC address exceeds the specific threshold. The default number of frames per second is 50. Range is 1 to 50.

FIGURE 255 RTS Abuse

A screenshot of a configuration form for an 'RTS Abuse' rule. It features three main fields: 'Name' (a text input), 'Rule Type' (a dropdown menu set to 'RTS Abuse'), and 'Classification' (a dropdown menu set to 'Rogue'). Each field is accompanied by a small asterisk icon and a descriptive text label: 'Name: [input]', '\* Rule Type: RTS Abuse [dropdown] Defines the type of rule to match for this classification policy', and '\* Classification: Rogue [dropdown] Defines the classification when the above criteria is matched'.

## Same Network

Detect and report the AP that is part of the same network SZ.

FIGURE 256 Same Network

A screenshot of a configuration form for a 'Same Network' rule. It features three main fields: 'Name' (a text input), 'Rule Type' (a dropdown menu set to 'Same Network'), and 'Classification' (a dropdown menu set to 'Rogue'). Each field is accompanied by a small asterisk icon and a descriptive text label: 'Name: [input]', '\* Rule Type: Same Network [dropdown] Defines the type of rule to match for this classification policy', and '\* Classification: Rogue [dropdown] Defines the classification when the above criteria is matched'.

## Signature Based

Detect and report when a client sends WIFI packets, matching the configured signature/pattern, to an authorized AP.

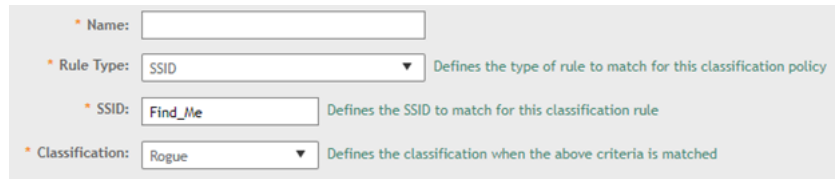
FIGURE 257 Signature Based

A screenshot of a configuration form for a 'Signature Based' rule. It features four main fields: 'Name' (a text input), 'Rule Type' (a dropdown menu set to 'Signature Based'), 'Signature-Based Profile' (a dropdown menu set to 'SBD\_Profile'), and 'Classification' (a dropdown menu set to 'Rogue'). Each field is accompanied by a small asterisk icon and a descriptive text label: 'Name: [input]', '\* Rule Type: Signature Based [dropdown] Defines the type of rule to match for this classification policy', 'Signature-Based Profile: SBD\_Profile [dropdown]', and '\* Classification: Rogue [dropdown] Defines the classification when the above criteria is matched'.

## SSID

Detect and report the partially or completely configured SSID string regardless of the zone being configured with the specific SSID.

FIGURE 258 SSID

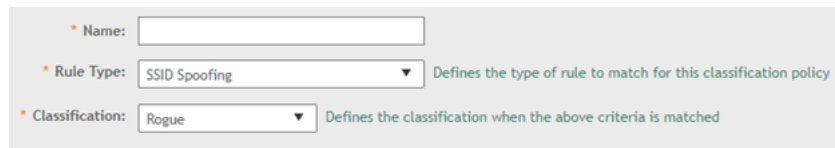


A screenshot of a configuration form for an SSID rule. It contains four fields: 'Name' (text input), 'Rule Type' (dropdown menu set to 'SSID'), 'SSID' (text input set to 'Find\_Me'), and 'Classification' (dropdown menu set to 'Rogue'). Each field has a small asterisk icon and a descriptive text label to its right.

## SSID Spoofing

Detect and report the SSID that is configured in a specific zone from a non-managed AP.

FIGURE 259 SSID Spoofing

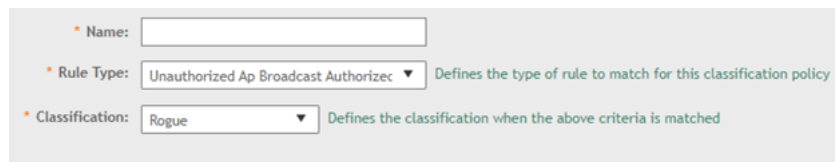


A screenshot of a configuration form for an SSID Spoofing rule. It contains three fields: 'Name' (text input), 'Rule Type' (dropdown menu set to 'SSID Spoofing'), and 'Classification' (dropdown menu set to 'Rogue'). Each field has a small asterisk icon and a descriptive text label to its right.

## Unauthorized Ap Broadcast Authorized SSID

Detect and report a non-allowListed service AP broadcasting a SSID (part of the same SZ).

FIGURE 260 Unauthorized Ap Broadcast Authorized SSID



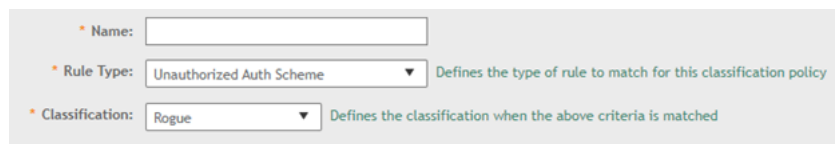
A screenshot of a configuration form for an Unauthorized Ap Broadcast Authorized SSID rule. It contains three fields: 'Name' (text input), 'Rule Type' (dropdown menu set to 'Unauthorized Ap Broadcast Authorized'), and 'Classification' (dropdown menu set to 'Rogue'). Each field has a small asterisk icon and a descriptive text label to its right.

## Unauthorized Auth Scheme

Auth scheme that is not part/configured of the AP are considered as unauthorized auth scheme. Authorized Auth scheme is 802.1x EAP and all other Auth scheme are considered as unauthorized.

Detect and report when an allowlisted AP utilizing unauthorized authorization scheme.

FIGURE 261 Unauthorized Auth Scheme



A screenshot of a configuration form for an Unauthorized Auth Scheme rule. It contains three fields: 'Name' (text input), 'Rule Type' (dropdown menu set to 'Unauthorized Auth Scheme'), and 'Classification' (dropdown menu set to 'Rogue'). Each field has a small asterisk icon and a descriptive text label to its right.

## Unauthorized Encryption Scheme

AES encryption type is the only allowed encryption scheme. TKIP and none are considered as unauthorized.



Detect and report when an AP or EUD uses unauthorized authentication scheme.

FIGURE 262 Unauthorized Encryption Scheme

The screenshot shows a configuration form for an 'Unauthorized Encryption Scheme' rule. It includes three fields: 'Name' (empty), 'Rule Type' (set to 'Unauthorized Encryption Scheme'), and 'Classification' (set to 'Rogue'). Each field has a small asterisk icon to its left. To the right of the 'Rule Type' and 'Classification' dropdowns, there is explanatory text: 'Defines the type of rule to match for this classification policy' and 'Defines the classification when the above criteria is matched' respectively.

## Unauthorized SSID

Detect and report the allowListed AP broadcasting an unauthorized SSID.

SSID is considered authorized only if configured to be used by a managed WLAN.

FIGURE 263 Unauthorized SSID

The screenshot shows a configuration form for an 'Unauthorized SSID' rule. The 'Name' field is filled with 'Unauthorized\_SSID'. The 'Rule Type' dropdown is set to 'Connected Unauthorized SSID', and the 'Classification' dropdown is set to 'Rogue'. Explanatory text is provided for the 'Rule Type' and 'Classification' fields.

## Unencrypted Traffic

Detect and report unencrypted data frames being sent between AP (both allowlisted and nonallowlisted) and EUD (both allowlisted and nonallowlisted).

FIGURE 264 Unencrypted Traffic

The screenshot shows a configuration form for an 'Unencrypted Traffic' rule. The 'Name' field is empty, the 'Rule Type' dropdown is set to 'Unencrypted Traffic', and the 'Classification' dropdown is set to 'Rogue'. Explanatory text is provided for the 'Rule Type' and 'Classification' fields.

## Weak/Outdated Protocol

Detect and Report weak/outdated WLAN protocol to generate an alert when allowlisted AP uses/utilizes the 802.11g or older WLAN protocol.

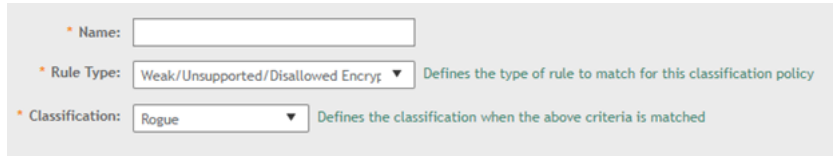
FIGURE 265 Weak and Outdated Protocol

The screenshot shows a configuration form for a 'Weak/Outdated Protocol' rule. The 'Name' field is empty, the 'Rule Type' dropdown is set to 'Weak/Outdated Protocol', and the 'Classification' dropdown is set to 'Rogue'. Explanatory text is provided for the 'Rule Type' and 'Classification' fields.

## Weak/Unsupported/Disallowed Encryption Scheme

Detect and Report an allowed AP advertising a SSID configured/changed with weak/unsupported/disallowed encryption options.

FIGURE 266 Weak/Unsupported/Disallowed Encryption Scheme

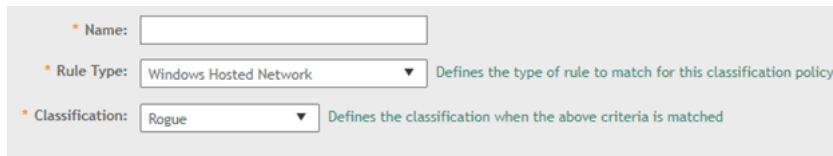


A screenshot of a configuration form for a rule. It contains three fields: a text input for 'Name', a dropdown menu for 'Rule Type' with the value 'Weak/Unsupported/Disallowed Encry...', and a dropdown menu for 'Classification' with the value 'Rogue'. Each field has a small asterisk icon to its left and a descriptive text label to its right.

## Windows Hosted Network

Detect and report a windows hosted network established with an allowlisted client.

FIGURE 267 Windows Hosted Network



A screenshot of a configuration form for a rule. It contains three fields: a text input for 'Name', a dropdown menu for 'Rule Type' with the value 'Windows Hosted Network', and a dropdown menu for 'Classification' with the value 'Rogue'. Each field has a small asterisk icon to its left and a descriptive text label to its right.

# Tamper-Evident Seals

- General Information about Tamper-Evident Seals..... 239
- Tamper-Evident Seals on SmartZone144 Devices.....239
- Tamper-Evident Seals on SmartZone 300 Devices..... 243
- Tamper-Evident Seals on T610 AP Devices..... 245
- Tamper-Evident Seals on R610 AP Devices..... 245
- Tamper-Evident Seals on R720 AP Devices..... 246

## General Information about Tamper-Evident Seals

The tamper-evident custom security labels are FIPS-certified for SmartZone and AP products. The following sections include photos showing locations where the seals must be applied by product type.

For all seal applications, ensure that the following instructions are observed:

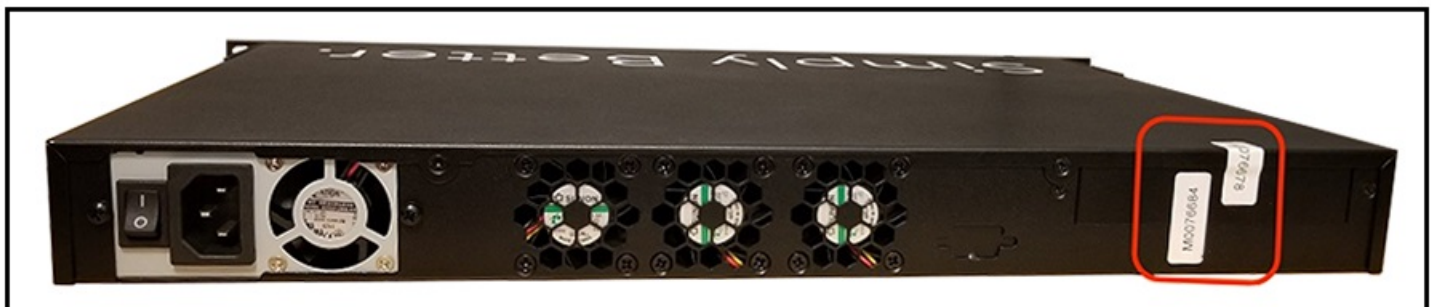
- All surfaces to which the seals will be applied must be clean and dry. Use alcohol to clean the surfaces. Do not use other solvents.
- Do not cut, trim, punch, or otherwise alter the tamper-evident seal.
- Do not use bare fingers to handle the labels. Slowly peel the packing from each seal, taking care not to touch the adhesive.
- Use very firm pressure across the entire seal surface to ensure maximum adhesion.
- Allow a minimum of 24 hours for the adhesive to cure. Tamper evidence may not be apparent until the adhesive cures.

When a tamper-evident seal is removed from the surface to which it has been applied, several tamper indications are apparent. The removed seal shows a checkerboard destruct pattern. The graphics printed within the seal are uniquely split between the removed seal and the residue left on the surface.

## Tamper-Evident Seals on SmartZone144 Devices

The following images show locations where FIPS tamper-evident seals must be placed on SmartZone144 devices.

**FIGURE 268** SmartZone144 Rear Seals



## Tamper-Evident Seals

Tamper-Evident Seals on SmartZone144 Devices

**FIGURE 269** SmartZone144 Rear Seals (vertical)



FIGURE 270 SmartZone144 Side Seal (Horizontal View)



FIGURE 271 SmartZone144 Side Seal (Vertical View)



## Tamper-Evident Seals

Tamper-Evident Seals on SmartZone144 Devices

FIGURE 272 SmartZone144 Bottom Seals



FIGURE 273 SmartZone144 Top View



## Tamper-Evident Seals on SmartZone 300 Devices

The following images show locations where FIPS tamper-evident seals must be placed on SmartZone 300 devices.

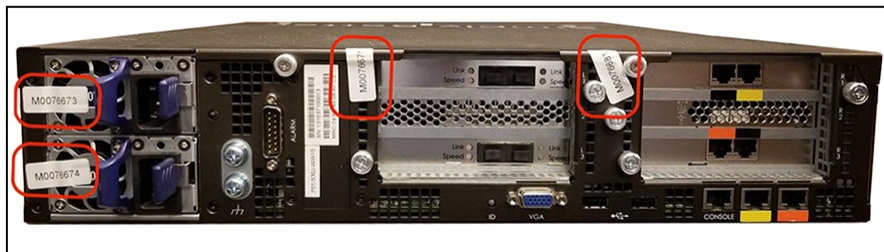
**Tamper-Evident Seals**

Tamper-Evident Seals on SmartZone 300 Devices

**FIGURE 274** SmartZone 300 Top Seals



**FIGURE 275** SmartZone 300 Rear Seals



**FIGURE 276** SmartZone 300 Front Seals





## Tamper-Evident Seals on T610 AP Devices

The following images show locations where FIPS tamper-evident seals must be placed on T610 AP devices.

FIGURE 277 T610 AP Side Seals



FIGURE 278 T610 AP Side Seal Detail



## Tamper-Evident Seals on R610 AP Devices

The following images show locations where FIPS tamper-evident seals must be placed on R610 AP devices.

## Tamper-Evident Seals

### Tamper-Evident Seals on R720 AP Devices

**FIGURE 279** R610 AP Side Seal



**FIGURE 280** R610 AP Side Seal (Opposite Side)



## Tamper-Evident Seals on R720 AP Devices

The following images show locations where FIPS tamper-evident seals must be placed on R720 AP devices.

FIGURE 281 R720 AP Right Side Seal



FIGURE 282 R720 AP Left Side Seal





# Trusted Channels Through TSF

- Trusted Communication Channels..... 249
- Enabling Trusted Channel Using IEEE 802.11-2012 (WPA2) Standards ..... 249
- Enabling Trusted Channel Using IEEE 802.1X and IPsec..... 250

## Trusted Communication Channels

TSF uses standards and protocols such as IEEE 802.11-2012 (WPA2), IEEE 802.1X, IPsec, SSH, TLS, and HTTPS to provide a trusted communication channel between itself and authorized IT entities supporting WLAN clients, audit servers, and 802.1X authentication servers. TSF also identifies endpoints for channel data, and protects channel data. It also ensures that the communication between authorized IT entities in the network only occurs through the trusted channel.

## Enabling Trusted Channel Using IEEE 802.11-2012 (WPA2) Standards

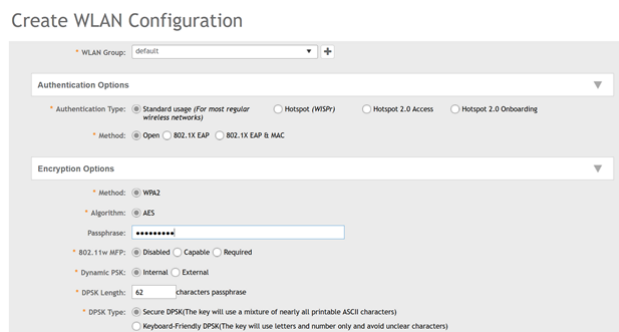
You can enable a secure and trusted channel for communication by using IEEE 802.11-2012 (WPA2) standards. This connection is initiated from the beginning by itself with WPA2 four-way handshake. This is as per WPA2 standard, and no manual intervention needed. IF the Wireless communication is interrupted/Broken user needs to reauthenticate via wireless device to reestablish the connection

1. In the controller interface, select **Wireless LANs**
2. Select the zone that you want to configure and click **Create**.

The **Create WLAN Configuration** page is displayed. Configure the settings as necessary.

Under Authentication Options, for Method, select **Open**. Under Encryption Options, for Method, select **WPA2**.

**FIGURE 283** Configuring the WLAN



### ATTENTION

The Hexadecimal (0 to 9 and A to F) characters are only allowed, no other ASCII characters. You have to use exactly 64 hexadecimal characters. 22 to 63 text-based characters are also supported For example, **f!rstwPa2%PSK-WI@nPa\$w0rd** or **abcdefghijklmnopqrstuvwxyz0123456789\$@abcdefghijklmnopqrstuvwxyz**.

## Trusted Channels Through TSF

Enabling Trusted Channel Using IEEE 802.1X and IPsec

# Enabling Trusted Channel Using IEEE 802.1X and IPsec

You can enable a secure and trusted channel for communication by using IEEE 802.1X and IPsec standards.

1. Follow the steps listed in [Configuring RadSec](#) on page 36 to configure a RadSec profile.
2. Follow the steps listed in [Creating a RUCKUS GRE Profile](#) on page 159 and [Creating an IPsec Profile](#) on page 157 to configure RUCKUS GRE and IPsec for a WLAN.

# FIPS-Compliant Products

- [AP Controller Matrix.....](#) 251
- [FIPS-Compliant Product SKUs and Descriptions.....](#) 251

## AP Controller Matrix

The AP and SmartZone cannot be in different FIPS modes at the same time. The AP acquires the FIPS mode from vSZ as soon as it is managed by the controller. The following table describes the FIPS capabilities of the AP and vSZ during the join process.

**TABLE 9** AP and vSZ FIPS Support Matrix

		FIPS SKU SmartZone (-F)		Regular SmartZone
		FIPS Enable	FIPS Disable	
FIPS SKU AP (-F)	FIPS enable	Supported	Not supported	X
	FIPS disable	Not supported	Supported (factory reset)	X
Regular AP		X	Supported	Supported

## FIPS-Compliant Product SKUs and Descriptions

The following tables describe FIPS-compliant AP, and controller products by SKU.

**TABLE 10** FIPS-Compliant AP Products

SKU	Long Description	Short Description
9F1-R720-US00	TAA/FIPS - compliant RUCKUS R720 dual-band 802.11abgn/ac (802.11ac Wave 2) Wireless Access Point with Multi-Gigabit Ethernet backhaul, 4x4:4 streams, MU-MIMO, BeamFlex+, dual ports, 802.3af/at PoE support. Does not include power adapter or PoE injector. Includes Limited Lifetime Warranty.	TAA R720 xx dual 11ac indoor AP 4x4:4
9F1-R610-US00	TAA/FIPS - compliant RUCKUS R610 dual-band 802.11abgn/ac (802.11ac Wave 2) Wireless Access Point, 3x3:3 streams, MU-MIMO, BeamFlex+, dual ports, 802.3af/at PoE support. Does not include power adapter or PoE injector. Includes Limited Lifetime Warranty.	TAA R610 XX dual 11ac indoor AP 3x3:3
9F1-T610-US01	TAA/FIPS - compliant RUCKUS T610 802.11ac Wave 2 Outdoor Wireless Access Point, 4x4:4 Stream, MU-MIMO, Omnidirectional Beamflex+ coverage, 2.4-GHz and 5-GHz concurrent dual band, Dual 10/100/1000 Ethernet ports, POE in, IP-67 Outdoor enclosure, -40 to 65C Operating Temperature. Includes standard 1-year warranty. Mounting kit sold as separate accessory (902-0125-0000). For box contents, see Shipping Container Contents.	TAA T610 xx Dual AC W2 outdoor AP 4x4
9F1-T610-US51	TAA/FIPS - compliant RUCKUS T610s 802.11ac Wave 2 Outdoor Wireless Access Point, 4x4:4 Stream, MU-MIMO, 120 degree sector Beamflex+ coverage, 2.4-GHz and 5-GHz concurrent dual band, Dual 10/100/1000 Ethernet ports, POE in, IP-67 Outdoor enclosure, -40 to 65C Operating Temperature. Includes standard 1-year warranty. Mounting kit sold as separate accessory (902-0125-0000). For box contents, see Shipping Container Contents.	TAA T610s xx Dual AC W2 outdoor AP 4x4

## FIPS-Compliant Products

### FIPS-Compliant Product SKUs and Descriptions

**TABLE 11** FIPS-Compliant Controller Products

SKU	Long description	Short description
PF1-S124-US00	TAA/FIPS - compliant SmartZone144 with 2x10GigE and 4 GigE ports, 90-day temporary access to licenses.	TAA SZ144-2x10GE & 4xGE, XX power cord
PF1-S104-US00	TAA/FIPS - compliant SmartZone144 with 4 GigE ports, 90-day temporary access to licenses.	TAA SZ144-4xGE ports, XX power cord
PF1-S300-WW10	SmartZone300 (SZ300) with redundant AC power, six (6) Fans, two (2) 10 Gbps data cards, and six (6) 1 GigE ports. Does not include power cords. 90-day temporary access to licenses.	TAA SZ300, 4x10GE-SFP+, 6x1GE, 2xPS, AC
PF1-S300-WW00	SmartZone300 (SZ300) with redundant DC power, six (6) Fans, two (2) 10 Gbps data cards and six (6) 1 GigE ports. Includes two DC power pigtail cables. 90-day temporary access to licenses.	TAA SZ300, 4x10GE-SFP+, 6x1GE, 2xPS, DC
LF9-VSCG-WW00	TAA/FIPS - compliant Virtual SmartZone 3.0 or newer software virtual appliance, 1 Instance, includes 1 AP license.	TAA vSCG 3.0 or newer virtual appliance
LF9-vSZD-WW00	TAA/FIPS -compliant Virtual Data Plane 3.2 or newer software virtual appliance, 1 instance (includes throughput up to 1 Gbps)	TAA Virtual Data Plane 1Gbps capacity

#### NOTE

vSZ-SKU is common for both the vSZ-E and vSZ-H product platforms.



# Connecting the Switches to Controller

- [Configuring the Switches to Connect to Controller.....](#) 253
- [Configuring the Controller to Access the Switch.....](#) 257
- [Viewing Switch from the Controller.....](#) 258
- [Deleting Switch from the Controller.....](#) 259

## Configuring the Switches to Connect to Controller

The FIPS 5.2.1.3 release allows the switches to join the FIPS enabled vSZ controller, and the hardware platforms. To establish this connection you must ensure that the port 987 on the controller must be opened for the switch to register.

You must perform the following steps to configure switch.

1. Telnet to switch

```
Telnet <IP Address>
```

2. Enter the below command to access the configure terminal mode.

```
telnet@switch-new#configure terminal
```

3. Enter **sz disable** to disable the controller.

```
telnet@swtch-new(config)#
telnet@swtch-new(config)#sz d
disable                               Disable SZ On Premise Management
telnet@swtch-new(config)#sz disable
SZ is already disabled via configurtion...
```

4. Enter **sz port-list 987** to open the port 987.

```
telnet@swtch-new(config)#
telnet@swtch-new(config)#
telnet@swtch-new(config)#sz port-list 987
telnet@swtch-new(config)#
```

## Connecting the Switches to Controller

### Configuring the Switches to Connect to Controller

5. Enter **show sz status** to confirm if the value for the **Port list** and the **Server Port** used is 987.

```
telnet@swtch-new(config)#show sz status
===== MGMT Agent State Info =====
Config Status: Disabled Operation Status: Disabled
State: DISABLED Prev State: QUERY Event: NONE

SWR List      : None
Active List   : 10.1.200.193, 10.1.200.198
DHCP Option 43 : No
DHCP Opt 43 List : None
Passive List  : None
Merged List   : 10.1.200.193, 10.1.200.198

SZ IP Used    : 10.1.200.193
Port List     : 987
Server Port Used : 987
Query Status  :
                Not Initiated

SSH Tunnel Status - :
Tunnel Status  : Not Initiated
CLI IP/Port    : /0
SNMP IP/Port   : /0
Syslog IP/Port : /0
HTTP SERVER IP/Port: /0
HTTP CLIENT IP/Port: /0

Timer Status   : Not Running
telnet@swtch-new(config)#
```

6. Remove the current SmartZone active list by executing the command **no sz active-list 10.1.200.193 10.1.200.198**

```
telnet@new-switch(config)#no sz ac
active-list Active SZ List
telnet@new-switch(config)#no sz active-list 10.1.200.193 10.1.200.198
REGISTERED VERSION - Please support MobaXterm by subscribing to the professional edition here: https://mobax
```

7. Execute the command **sz active -list 10.1.200.215** where IP address is the IP address of the controller.

```
telnet@new-switch(config)#sz active-list 10.1.200.215
telnet@new-switch(config)#
```

8. Execute **no sz disable** to enable SmartZone discovery for switch.

```
telnet@new-switch(config)#no sz disable
telnet@new-switch(config)#
telnet@new-switch(config)#
telnet@new-switch(config)#
telnet@new-switch(config)#
telnet@new-switch(config)#
```

- Show **show sz status** to view the current connection status of switch and SmartZone.

```

===== NGMT Agent State Info =====
Config Status: None      Operation Status: Enabled
State: QUERY           Prev State: INIT          Event: QUERY RESPONSE

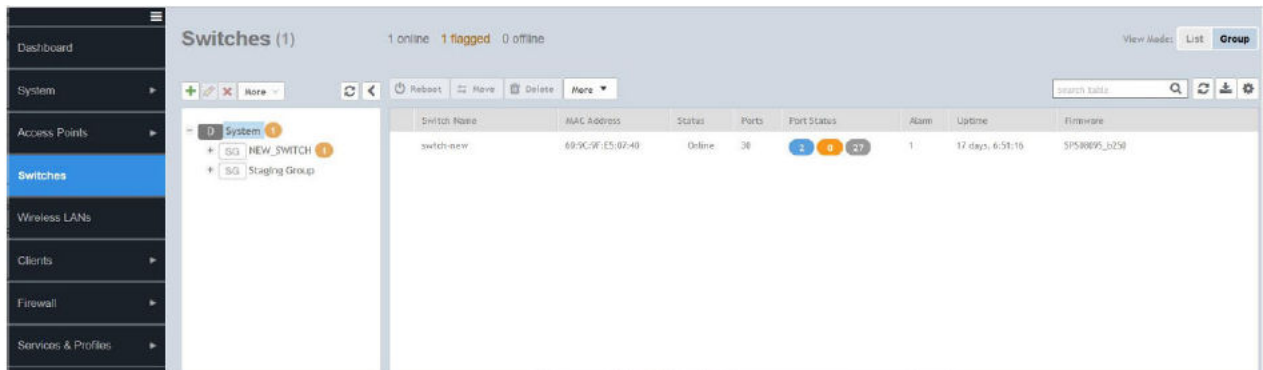
SWR List      : None
Active List   : 10.1.200.215
DHCP Option 43 : No
DHCP Opt 43 List : None
Backup List   : None
Merged List   : 10.1.200.215

SZ IP Used    : 10.1.200.215
Port List     : 987
Server Port Used : 987
Query Status  : In Progress. Response Not Received.

SSH Tunnel Status - :
Tunnel Status : Not Initiated
CLI IP/Port    : /0
SNMP IP/Port   : /0
Syslog IP/Port : /0
HTTP SERVER IP/Port: /0
HTTP CLIENT IP/Port: /0

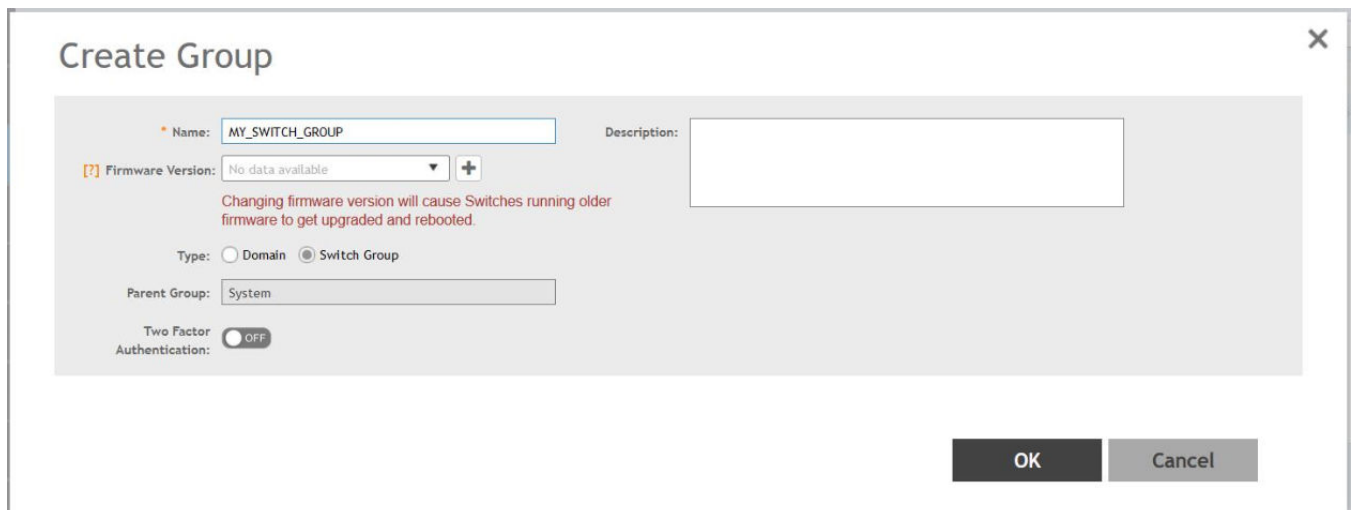
Timer Status : Running
Timer Details in msec
Start Time Stamp : 77565322
Duration         : 15000
Current Time Stamp: 77566063
Time Left        : 14259
telnet(new-switch(config)#
    
```

- Switch will come under staging group in offline state.



- Click .

FIGURE 284 Creating Switch Group



## Connecting the Switches to Controller

### Configuring the Switches to Connect to Controller

12. Configure the following.

- **Name:** Type the name of the switch group that you want to create.
- **Description:** Enter a brief description for the switch group
- **Type:** Select **Switch Group**
- **Parent Group:** Displays the parent group under which the switch group resides
- **Two Factor Authorization:** Disables the SSH and tenet connection for the switch.

#### NOTE

By default, the **Two Factor Authorization** is disabled.

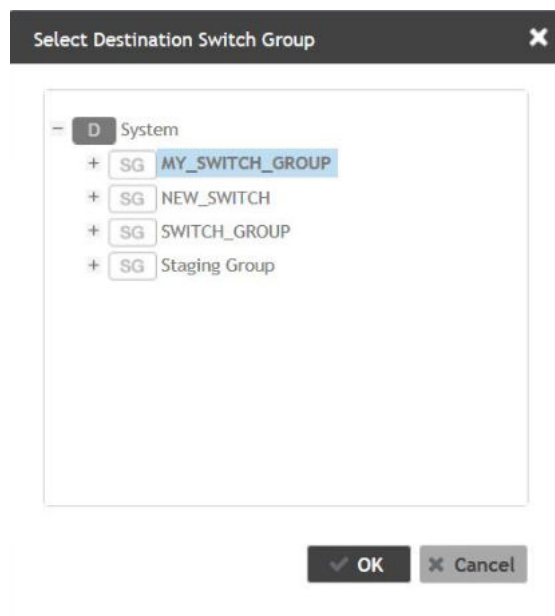
13. Click **OK**.

The switch group is created under the selected parent group.

14. Select the switch in the staging group, and click the **Move** tab.

The **Select Destination Switch Group** page is displayed. Select the switch group to which you want to move the selected switch.

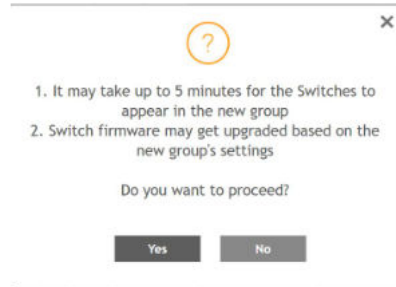
**FIGURE 285** Moving the switch to Destination Switch Group



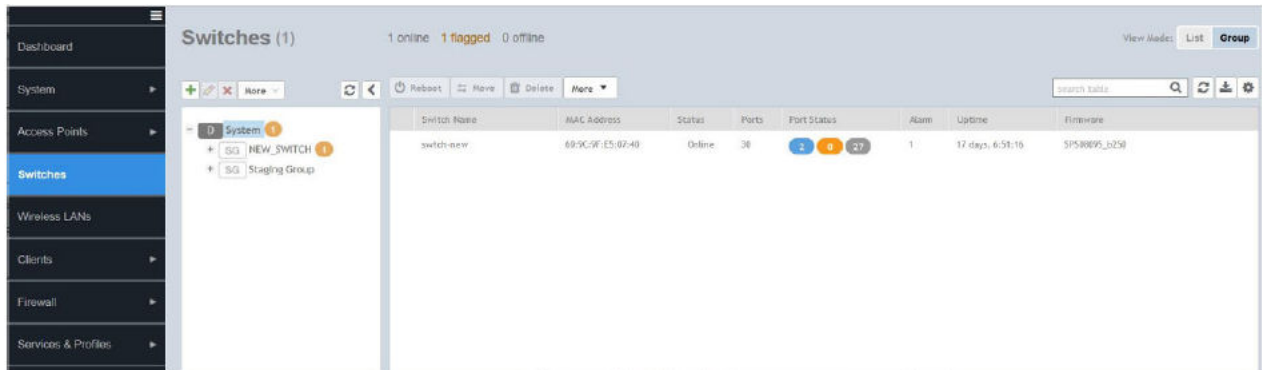
15. Click **OK**.

A dialogue box is displayed.

**FIGURE 286** Waiting for Switch to get Added



16. Click **Yes** to add the switch to the newly created group.



## Configuring the Controller to Access the Switch

You must perform the following steps to configure the controller to access the switch connectivity.

1. SSH to FIPS enabled controller.

```
SSH username@ <IP Address>
```

## Connecting the Switches to Controller

### Viewing Switch from the Controller

2. Go to configuration mode, and enter `open-icx-management`.

```
[shubham@IRAWAT ~]$ ssh admin@10.174.89.192
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.
#####Welcome to the FIPS Build#####
admin@10.174.89.192's password:
Last successful login: 2020-05-15 07:12:35
Last successful login from: 10.174.88.51
Failed login attempts since last successful login: 0
Account privilege changes: No
Please wait. CLI initializing...

Welcome to the Ruckus Virtual SmartZone - High Scale Command Line Interface
Version: 5.2.1.0.335

FIPS-ICXM> en
Password: *****

FIPS-ICXM# config

FIPS-ICXM(config)# open-icx-management
Successful operation

FIPS-ICXM(config)# █
```

## Viewing Switch from the Controller

After the switch is connected to the FIPS enabled controller, you can view it from the controller web user interface .

### NOTE

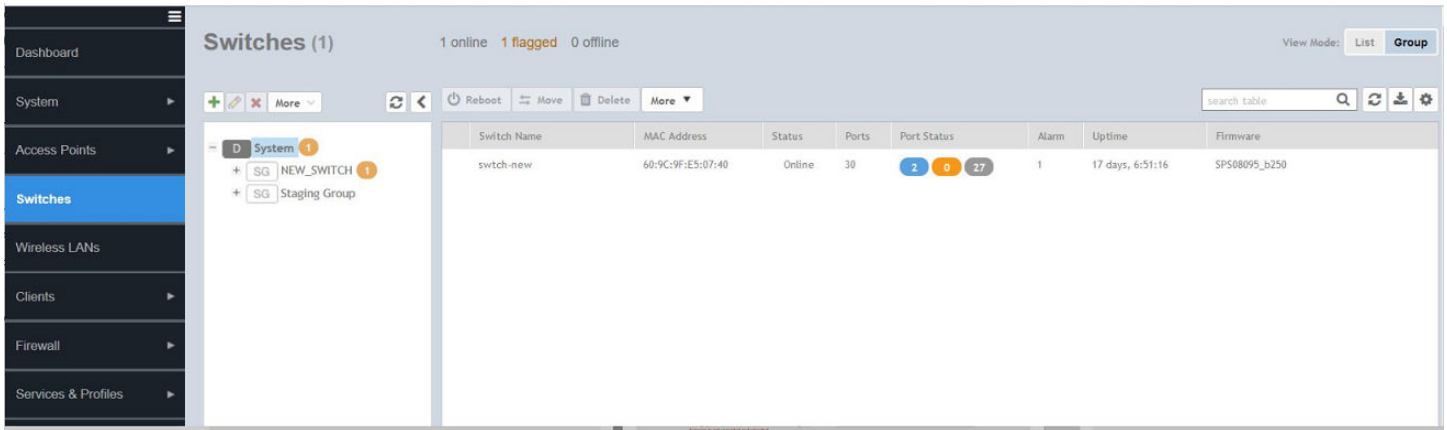
To configure the switch, and the FIPS enabled controller, refer the topics below . By default, the switch gets added in the staging group.

You must perform the following steps to view the switch on the controller.

From the controller web interface, select **Switches** on the left pane.

The **Switches** page is displayed.

**FIGURE 287** Accessing the Switch Tab



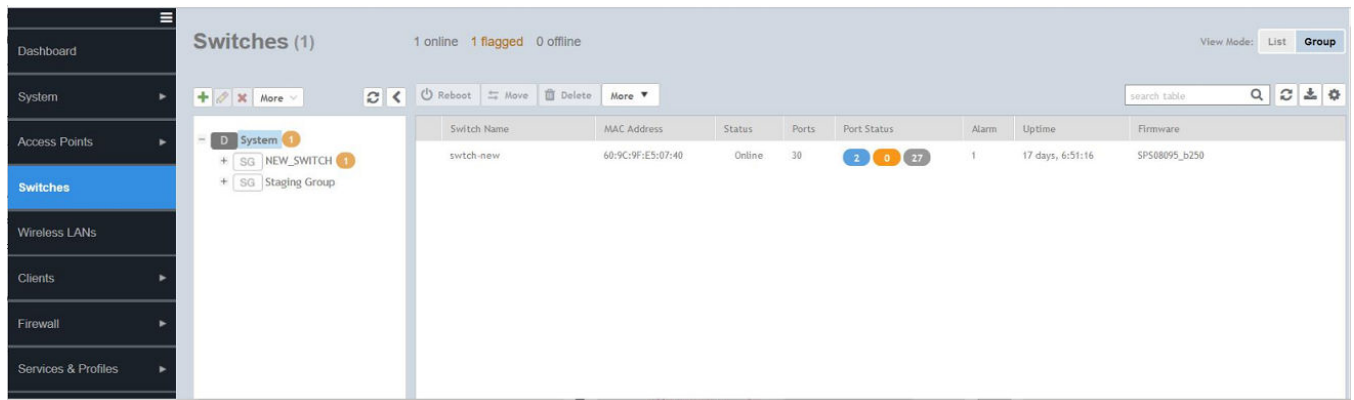
## Deleting Switch from the Controller

You can delete the switch when the ICX service is no longer needed by the controller.

You must perform the following steps to delete a switch.

1. From the controller web user interface, select **Switches** on the left pane.  
The **Switches** page appears.

**FIGURE 288** Selecting Switch

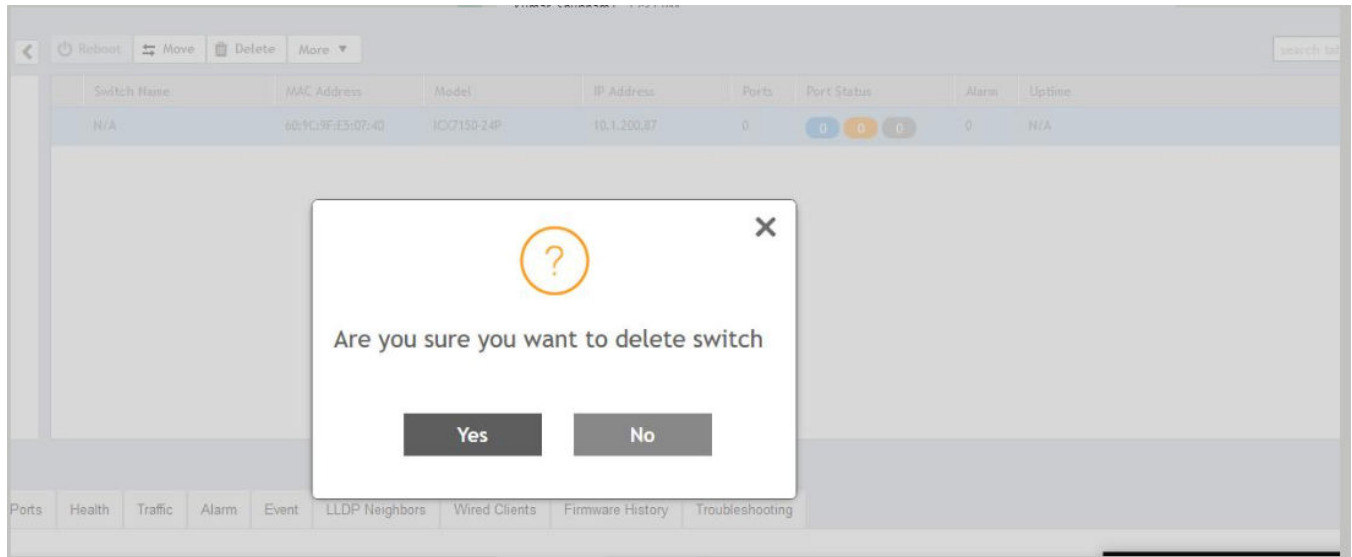


## Connecting the Switches to Controller

### Deleting Switch from the Controller

2. Select a switch, and click **Delete**.

**FIGURE 289** Deleting a Switch



3. Click **Yes**.



# Two-Factor Authentication

---

Two-factor authentication provides stronger security for non-admin users by enforcing two level of authentication. One is by CAC card, and the other followed by PAP/CHAP authentication [username & password] which will be mapped to one of the user groups.

To perform two-factor authentication, you must configure the below items, and enable the CAC-PIV Authentication.

Configure the following.

- [Creating Switch Groups](#) on page 263
- [Creating User Groups \(FIPS\)](#) on page 265
- [Configuring SZ Admin AAA Servers](#) on page 269
- [Importing New Certificates](#) on page 267
- [Enabling Common Access Card or Personal Identity Verification Authentication](#) on page 273

## NOTE

1. SSH 2 factor auth (2FA) has become a mandatory for Security Technical Implementation Guide (STIG). If the two-factor authentication mode is applied on ICX by SmartZone, ICX will lock down all incoming SSH requests. The Switch CLI can be accessed through remote CLI feature on SmartZone.
2. If telnet authentication is enabled on ICX, user will be prompted to enter the login credentials for ICX.



# Creating Switch Groups

You can group switches based on your need, for example, you can group switches based on their size or their location.

You can only create a maximum of two levels within the group hierarchy. By default, all the switches are placed under the default switch group. You can create a group or sub-group and then move the switch under it. You can also modify or delete a group at any time.

After the switch is registered with the controller interface, you can monitor, view status or usage, and perform some basic management, including configuration backups and firmware management. However, you cannot configure the switch from the controller web user interface.

## NOTE

To configure the switch, refer steps 1 to 9 in the topic *Configuring the ICX Switches to Connect to the Controller*.

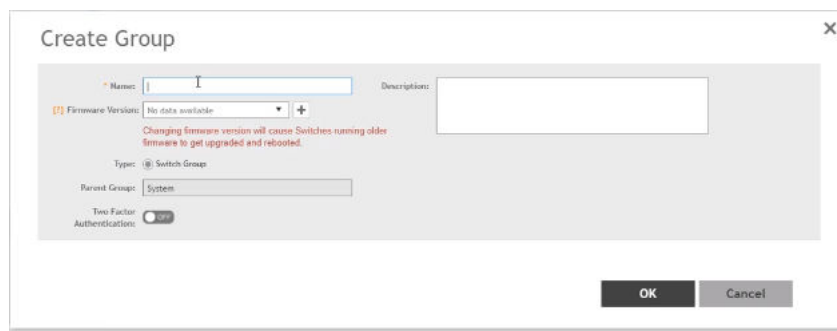
1. From the left pane, select **Switches**.

The **Switches** page appears.

2. Click .

The **Create Group** page appears.

**FIGURE 290** Creating Switch Group



3. Configure the following.
  - a) **Name:** Type the name of the switch group that you want to create.
  - b) **Description:** Enter a brief description for the switch group.
  - c) **Type:** Select Switch Group. For enterprise devices such as SZ-300 and vSZ-H, you also have the option to select Domain.
  - d) **Parent Group:** Displays the parent group under which the switch group resides.
  - e) **Two Factor Authorization:** You can slide the radio button to ON or OFF to enable or disable two factor authorization.
4. Click **OK**.

The switch group is created under the selected parent group.



# Creating User Groups (FIPS)




---

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

1. Go to **Administration > Admins and Roles**.
2. Select the **Groups** tab.
3. Click **Create** after selecting the system domain.  
The **Create User Group** page appears.
4. Configure the following:
  - a. Permission
    1. Name: Type the name of the user group you want to create.
    2. Description: Type a short description for the user group you plan to create.
    3. Permission: Select one of the access permission for the user group, from the drop-down menu. You can also grant admin permission to generate guest passes. Select the **Custom** option to manually assign role-based permission in the **Resource** tab page.
    4. Account Security: Select the account security profile that you created to manage the administrator accounts.
    5. Click **Next**.
  - b. Resource: From **Select Resources**, choose the resources that you want to assign to this user group. If you have selected **ICX Switch** 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.
  - c. Click **Next**.

## NOTE

Domain Option is unavailable in SZ144 and vSZ-E.

- 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**, do not select any user. Click the .
- 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.



# Importing New Certificates

---

When you have an SSL certificate issued by an SSL certificate provider, you can import it into the controller and use it for HTTPS communication.

To complete this procedure, you will need the following:

- The signed server certificate
- The intermediate CA certificate (at least one)
- The private key file

## NOTE

The file size of each signed certificate and intermediate certificate must not exceed 8192 bytes. If a certificate exceeds 8192 bytes, you will be unable to import it into the controller.

Follow these steps to import a signed server certificate:

1. Copy the signed certificate file, intermediate CA certificate file, and private key file to a location (either on the local drive or a network share) that you can access from the controller web interface.
2. From the application select, **System > Certificates > Installed Certs**.
3. Click **Import**, the Import Certificate form appears.
4. Enter a **Name** to identify the certificate.
5. Enter a **Description** about the certificate.
6. For **Service Certificates**, click **Browse** and select the location where the certificate is saved.
7. For **Intermediate CA certificates**, click **Browse** and select the location where the certificate is saved. If you need to upload additional intermediate CA certificates to establish a chain of trust to the signed certificate, you can select up to four certificates.
8. If you are using this SSL certificate for a Hotspot 2.0 configuration, you must also import a root CA certificate. To import **Root CA Certificate**, click **Browse** and select the location where the certificate is saved.
9. You can import the **Private Key** file either by
  - uploading file—choose **Upload** and click **Browse** to select the location.
  - using CSR—choose **Using CSR** and select the CSR that you generated earlier.
10. Enter the **Key Passphrase** that has been assigned to the private key file.
11. Click **OK**.

## NOTE

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

## NOTE

only CRT or PEM format is supported for the CA certificate.





# Configuring SZ Admin AAA Servers

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

1. Select **Administration > Admins and Roles > AAA**.
2. From **AP AAA Servers**, click **Create**.

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

**FIGURE 291** Creating an Administrator AAA Server

## Edit Administrator AAA Server: Radius-136

\* Name: Radius-136

\* Type:  RADIUS  TACACS+  Active Directory  LDAP

\* Realm: commscope.com  
Multiple realms supported. Use a comma (,) to separate realms (for example, home1,home2).

TLS Encryption:  ON

\* CN/SAN Identity: sz124.commscope.com

OCSP Validation:  OFF \* OCSP URL: [ ]

Client Certificate: IPSec\_clientCert

[?] Default Role Mapping:  ON

User Group: auto-mapping

Administrator: [Auto-generate]

Backup RADIUS:  OFF Enable Secondary Server

\* IP Address: 10.1.200.136

\* Port: 2083

\* Protocol:  PAP  CHAP  PEAP

\* Shared Secret: [ ]

\* Confirm Secret: [ ]

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

## Configuring SZ Admin AAA Servers

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 **Ruckus-WSG-User-{SZUSER}** (for example, **Ruckus-WSG-User-{SZUSER}**), depending on the SZ users or permissions you want the Active Directory or LDAP user to map.

### NOTE

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

7. For **Backup RADIUS**, select **Enable Secondary Server** if a secondary RADIUS server exists on the network. Refer to step 9 for configuration settings.

8. Under **Primary Server**, configure the settings of the primary AAA server.

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

**NOTE**

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

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

For **Active Directory**, configure the settings for the **Proxy Agent**.

- **User Principal Name:** Enter the Windows domain Administrator name
- **Password:** Enter the administrator password.
- **Confirm Password:** Re-enter the password to confirm.

9. Under **Secondary Server**, configure the settings of the secondary RADIUS server.

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

**NOTE**

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

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

10. Under **Failover Policy at NAS**, configure the settings of the secondary RADIUS server.

- **Request Timeout:** Enter the timeout period in seconds. After the timeout period, an expected RADIUS response message is considered to have failed.
- **Max Number of Retries:** Enter the number of failed connection attempts. After the maximum number of attempts, the controller tries to connect to the backup RADIUS server.
- **Reconnect Primary:** Enter the time in minutes, after that the controller connects to the primary server.

11. Click **OK**.

**NOTE**

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



# Enabling Common Access Card or Personal Identity Verification Authentication

Perform the following procedure to enable CAC/PIV authentication.

1. Select **Administration > Admins and Roles > CAC/PIV Authentication**.
2. Select **Enable CAC/PIV Authentication**.

**FIGURE 292** Enabling CAC/PIV Authentication

The screenshot shows the configuration page for CAC/PIV Authentication. The navigation bar includes tabs for Groups, Administrators, AAA, Access Control List, Account Security, Session Management, and CAC/PIV Authentication. The CAC/PIV Authentication tab is selected. The main content area features a toggle switch for 'Enable CAC/PIV Authentication' which is currently turned ON. Below this, there are four configuration fields: 'Authorization Server' (dropdown menu showing 'AD-242 (Single Step Authenticatic'), 'CA Chain Certificates' (dropdown menu showing 'OSCP'), 'User Name Mapping' (dropdown menu showing 'User Principal Name'), and 'OCSP Server URI' (text input field containing 'http://10.1.200.16:2560'). At the bottom of the form, there are three buttons: 'Refresh', 'OK', and 'Cancel'.

3. Select the AAA authorization server from the list.

#### NOTE

For RADIUS, the login flow changes to three-factor authentication.

The CAC/PIV login prompts the user to insert the CAC/PIV smart card. The operating system and browser in conjunction with card reader drive support verifies the client certification using a personal identification number (PIN). Only after the PIN is verified as correct, the client certificate is sent to SZ for verification.

4. Select the CA chain certificate from the list.

#### NOTE

To upload the certificates refer [Importing New Certificates](#) on page 267

5. For **User Name Mapping**, select the **User Principal Name** or **RFC822 Name** from the drop-down list.
6. Enter the OCSP server URL.
7. Click **OK**.



# Events

- Fails to establish TLS tunnel between SZ and External AAA Server..... 275
- SZ Login fail..... 275
- SZ Login ..... 276
- SZ Logout ..... 276
- Unsync NTP time..... 276
- SZ Failure of Certificate..... 276
- NodeRebooted..... 277
- NodeShutdown..... 277
- Auditable Events in AP and DP for Common Criteria..... 277

## Fails to establish TLS tunnel between SZ and External AAA Server

**TABLE 12** Fails to establish TLS tunnel between SZ and External AAA Server Event

Event	Fails to establish TLS tunnel between SZ and External AAA Server
Event Type	racTLSEstablishmentFailedBetweenSZandExternalAAAServer
Event Code	1763
Severity	Major
Attribute	"ctrlBladeMac"="aa:bb:cc:dd:ee:ff" "srcProcess"="radiusd" "SCGMgmtIp"="2.2.2.2" "desc"="Fails to establish "
Displayed on the web interface	[[srcProcess]] Establishes the TLS connection fails between SZ and external AAA Server from SCG[[SCGMgmtIp]]
Description	This event occurs when TLS establishment fails between the controller and the external AAA Server.

## SZ Login fail

**TABLE 13** SZ Login fail Event

Event	SZ Login fail
Event Type	szLoginFail
Event Code	8007
Severity	-
Attribute	userName = "x", ip="xxx.xxx.xxx.xxx"
Displayed on the web interface	Administrator [[userName]] logged on failed from [[ip]]
Description	This event occurs when the administrator fails to log into the controller.

## SZ Login

TABLE 14 SZ Login Event

Event	SZ Login
Event Type	szLogin
Event Code	8008
Severity	-
Attribute	userName = "x", ip="xxx.xxx.xxx.xxx"
Displayed on the web interface	Administrator [{userName}] logged on from [{ip}]
Description	This event occurs when the administrator is logged on to the controller.

## SZ Logout

TABLE 15 SZ Logout Event

Event	SZ Logout
Event Type	szLogout
Event Code	8009
Severity	-
Attribute	userName = "x", ip="xxx.xxx.xxx.xxx"
Displayed on the web interface	Administrator [{userName}] logged off from [{ip}]
Description	This event occurs when the administrator logged off the controller.

## Unsync NTP time

TABLE 16 SZ Logout Event

Event	Unsync NTP time
Event Type	Unsync NTP time
Event Code	855
Severity	Major
Attribute	Cluster Node name = "X" timedifference "xxxx" seconds
Displayed on the web interface	Node [Cluster-Node] time is not synchronized because of [NTP Server]. The time difference is "timedifference" seconds.
Description	This event occurs when cluster time is unsynchronized.

## SZ Failure of Certificate

TABLE 17 SZ Failure of Certificate

Event	SZ Failure of Certificate
Event Type	SZ Failure of Certificate



**TABLE 17** SZ Failure of Certificate (continued)

Event	SZ Failure of Certificate
Event Code	99102
Severity	Majority
Displayed on the web interface	Common name {{SubrootCA}}, root CA is not self-signed.
Description	<p>This event occurs when SZ server certificate validation fails.</p> <p><b>NOTE</b> The validation can fail due to :</p> <ul style="list-style-type: none"> <li>• Invalid server certificate</li> <li>• Server certificate expired</li> <li>• Extended key usage of server certificate is not " TLS Web Server Authentication".</li> </ul>

## NodeRebooted

**TABLE 18** NodeRebooted Event

Event	NodeRebooted
Event Type	nodeRebooted
Event Code	826
Severity	Major
Attribute	"nodeName"="xxx", "nodeMac"="xxx"
Displayed on the web interface	Node {{nodeName}} in cluster {{clusterName}} rebooted.
Description	This event occurs when the node is rebooted.

## NodeShutdown

**TABLE 19** NodeShutdown Event

Event	NodeShutdown
Event Type	nodeShutdown
Event Code	828
Severity	Major
Attribute	"nodeName"="xxx", "nodeMac"="xxx"
Displayed on the web interface	Node {{nodeName}} has been shut down
Description	This event occurs when the node is shut down.

## Auditable Events in AP and DP for Common Criteria

The following table lists the auditable events in the access point (AP) for Common Criteria (CC).

## Events

### Auditable Events in AP and DP for Common Criteria

**TABLE 20** Auditable Events in AP for CC

Event Code	Event Type	Description
99000	keyGenFail	This event occurs when PMK is not available to derive PTK
99001	keyDisFail	This event occurs when 4-way handshake fails
99002	keyDisFailGTK	This event occurs when 4-way handshake fails
99003	wpaEnDecFail	This event occurs when WPA encryption and decryption fails
99004	ipsecSesFail	This event occurs when there is an IPsec session establishment and termination due to SA failure
99005	authAttempts	This event occurs when the number of failed attempts to switch to trusted channel is exceeded
99006	authUnsucces	This event occurs when a user has tried maximum number of unsuccessful login attempts
99007	authReauth	This event occurs once the user is blocked and waits for specified amount of time before getting login prompt
99008	auth8021xClient	This event occurs when receiving data frame before client is authorized
99009	fwManualInitiation	This event occurs when there is manual firmware update
99010	apMGMNTTSFData	This event occurs when there is all management activities of TSF data initiated/started/executed
99011	apTSFFailure	This event occurs whenever there is Failure of all or any management TSF
99012	apSelfTests	This event occurs when all self-tests are passed for fips_sku builds
99013	fwInitiationUpdate	This event occurs when there is firmware update
99014	disContiChan	This event occurs when AP syncs its time with SZ
99015	apLocalSessionTimeout	This event occurs when local AP session terminates due to session timeout
99016	apRemoteSessionTimeout	This event occurs when remote AP session terminates due to session timeout
99017	apSessionExit	This event occurs on user-initiated termination of an interactive AP session
99018	sshInitiation	This event occurs when the SSH session started with successful authentication
99019	sshTermination	This event occurs when there is exit from an established SSH session
99020	sshFailure	This event occurs when there is SSH session initiation with failed authentication
99021	tlsInitiation	This event occurs when there is a successful login through AP web-GUI or AP establishes a trusted TLS connection
99022	tlsTermination	This event occurs when there is logout from AP web-GUI session or AP gracefully terminates a trusted TLS connection
99023	tlsFailure	This event occurs whenever there is a failed login through AP web-GUI or AP fails to establish a trusted TLS connection
99024	ipsecInitiation	This event occurs when there is an IPsec session initiation
99025	ipsecTermination	This event occurs when there is an IPsec session terminated or exited
99026	ipsecFailure	This event occurs when there is IPsec session attempt failure

The following table lists the auditable events in the data plane (DP) for Common Criteria (CC).

**TABLE 21** Auditable Events in DP for CC

Event Code	Event Type	Description
552	dpUpgradeSuccess	This event occurs whenever DP upgrade is successful
553	dpUpgradeFailed	This event occurs whenever DP upgrade fails
600	dpCompleteTunnelRequest	This event occurs whenever there is a TLS termination of AP tunmgr connect to DP tunmgr
601	dpAcceptTunnelRequest	This event occurs whenever there is a TLS initiation of AP tunmgr connect to DP tunmgr
602	dpRejectTunnelRequest	This event occurs whenever there is a TLS failure of AP tunmgr connect to DP tunmgr
99200	dpIntegrityTestFailed	This event occurs whenever the DP self-integrity test fails
99201	dpCliEnableFailed	This event occurs whenever <b>vSZ-D_cli enabled</b> fails

**TABLE 21** Auditable Events in DP for CC (continued)

Event Code	Event Type	Description
99202	dpReAuth	This event occurs whenever the DP attempts to re-authenticate
99203	dpPasswordMinLengthUpdated	This event occurs whenever the DP minimum password length changed
99204	dpPasswordChanged	This event occurs whenever the DP password changed
99205	dpEnablePasswordChanged	This event occurs whenever the DP enable password changed
99206	dpHttpsAuthFailed	This event occurs whenever X.509 certificate verification failed
99207	dpCertUploaded	This event occurs whenever X.509 certificate is uploaded
99208	dpScgFqdnUpdated	This event occurs whenever SZ FQDN setting is updated on DP
99210	dpInitUpgrade	This event occurs whenever there is an attempt to initiate a manual update
99211	dpDiscontinuousTimeChangeNTPServerd pNtpTimeSync	This event occurs whenever there are discontinuous changes to time, either initiated by administrator or changed by an automated process
99212	dpUserLogin	This is an administrative login event.
99213	dpUserLogin	This event occurs whenever an administrator login is successful
99214	dpUserLoginFailed	This event occurs whenever an administrator login fails
	dpUserLogout	This event occurs whenever there is a termination of an interactive session
99215	dpAccountLocked	This event occurs whenever the maximum number of unsuccessful user authentications has been exceeded with subsequent actions taken and restoration of the account
99220	dpSessionIdleUpdated	This event occurs whenever a remote session is terminated by the session locking mechanism
99221	dpSessionIdleTerminated	This event occurs whenever a remote session is terminated by the session locking mechanism
99230	dpSshTunnFailed	This event occurs whenever there is initiation and termination of trusted path and subsequent failure of the trusted path functions
99231	dpHttpsConnFailed	This event occurs whenever there is initiation and termination of trusted path and subsequent failure of the trusted path functions
99240	dpIPsecTunnCreateFailed	This event occurs whenever attempts to establish a trusted channel (including IEEE 802.11) fails
99241	dpIPsecTunnInitiate	This event occurs whenever attempts to establish a trusted channel (including IEEE 802.11) fails
99242	dpIPsecTunnTerminated	This event occurs whenever attempts to establish a trusted channel (including IEEE 802.11) fails
99243	dpIPsecSaFailed	This event occurs whenever there is an establishment or termination of an IPsec SA connection
99244	dpIPsecSaUpdated	This event occurs whenever cryptographic keys are generated, imported, changed, or deleted

The following table lists the events in the SZ.

**TABLE 22** Events in SZ

Event Code	Event Type	Description
1763	Fails to establish TLS tunnel between SZ and External AAA Serve	This event occurs when Fails to establish TLS tunnel between SZ and External AAA Server.
859	NTP server reach failed	This event occurs when the user is unable to reach the NTP Server.
827	NTP time synchronized	This event occurs when the date and time settings on node are not synchronized with the NTP Server.
99102	SZ Failure of Certificate	This event occurs when the user fails to upload the CA, Sub-CA, Server Certificate, Client Certificate and keys to the controller.
99013	System IPsec IKE is UP	This event occurs when System IPsec IKE is up.
99014	System IPsec IKE is Down	This event occurs when System IPsec IKE is down(terminated).

## Events

Auditable Events in AP and DP for Common Criteria

**TABLE 22** Events in SZ (continued)

Event Code	Event Type	Description
99102	SZ Failure of Certificate	This event occurs when sz server certificate validation failed.

# Audit Records

- Viewing the Events and Alarms..... 281
- Downloading the Logs from the Controller..... 282
- Viewing the Audit Records..... 283

## Viewing the Events and Alarms

You can view the events and alarms on the controller by performing the following steps.

- In the web interface, navigate to **Events and Alarms > Events**.
- Click the **Events** tab

FIGURE 293 Viewing Events

Date and Time	Code	Type	Activity
2020/04/04 00:15:18	204	Client disconnected	Client [r
2020/04/04 00:15:18	186	Classified rogue AP	AP [Out
2020/04/04 00:15:18	186	Classified rogue AP	AP [Out
2020/04/04 00:15:18	186	Classified rogue AP	AP [Out
2020/04/04 00:15:18	186	Classified rogue AP	AP [Out
2020/04/04 00:15:18	186	Classified rogue AP	AP [Out
2020/04/04 00:15:18	186	Classified rogue AP	AP [Out
2020/04/04 00:15:18	186	Classified rogue AP	AP [Out
2020/04/04 00:15:18	186	Classified rogue AP	AP [Out
2020/04/04 00:15:17	186	Classified rogue AP	AP [Out
2020/04/04 00:15:17	186	Classified rogue AP	AP [Out
2020/04/04 00:15:17	186	Classified rogue AP	AP [Out
2020/04/04 00:15:17	186	Classified rogue AP	AP [Out
2020/04/04 00:15:17	186	Classified rogue AP	AP [Out
2020/04/04 00:15:17	186	Classified rogue AP	AP [Out
2020/04/04 00:15:17	186	Classified rogue AP	AP [Out
2020/04/04 00:15:17	186	Classified rogue AP	AP [Out
2020/04/04 00:15:17	186	Classified rogue AP	AP [Out
2020/04/04 00:15:17	186	Classified rogue AP	AP [Out
2020/04/04 00:15:17	186	Classified rogue AP	AP [Out
2020/04/04 00:15:15	186	Classified rogue AP	AP [E11-
2020/04/04 00:15:15	186	Classified rogue AP	AP [E11-

- To view alarms, navigate to **Events and Alarms > Alarms**.
- The **Alarm** page appears.

## Audit Records

### Downloading the Logs from the Controller

FIGURE 294 Viewing Alarms

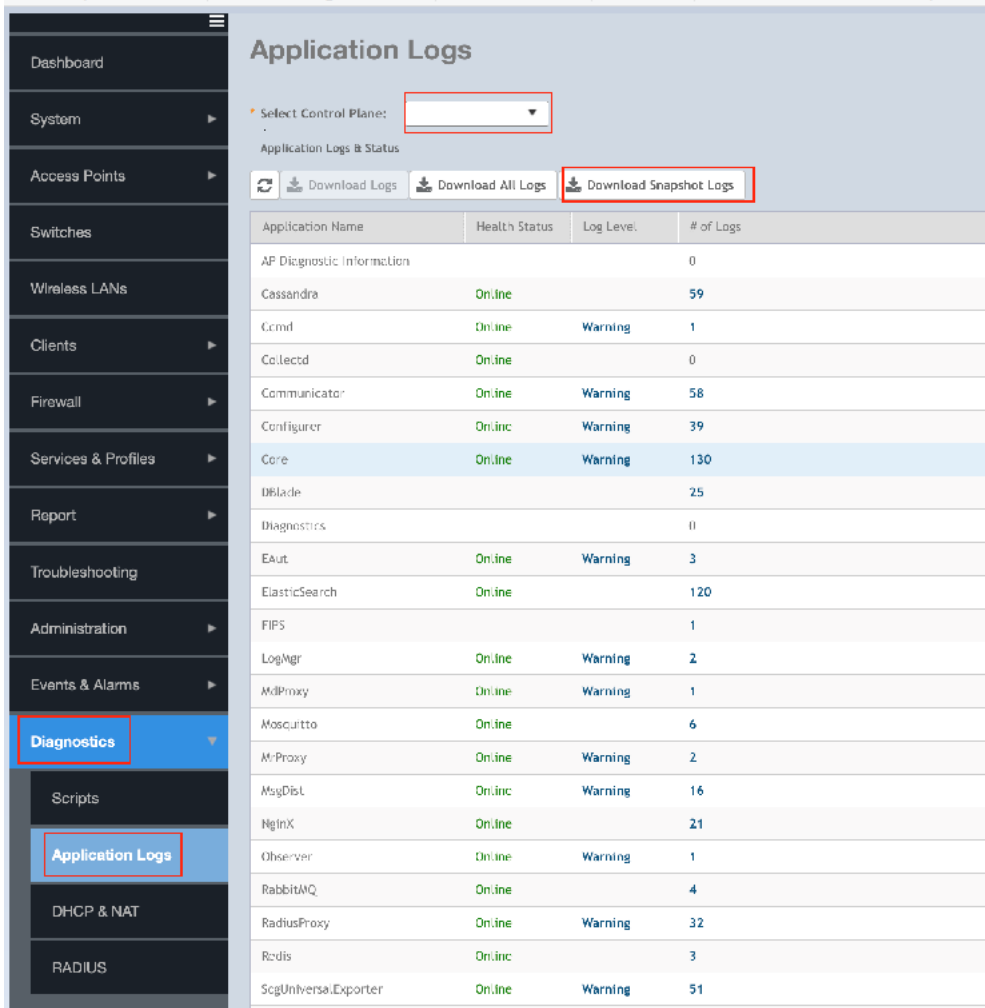
Date and Time	Alarm Type	Severity	Status	Activity	Acknowledged On	Cleared By	Cleared On	Comments
2020/04/01 13:24:30	AP disconnected	Major	Cleared	AP E08	N/A	System	2020/04/01 13:25:01	Auto Cleared
2020/04/01 13:24:12	AP rebooted by system	Major	Outstanding	AP E08	N/A	N/A	N/A	N/A
2020/04/01 13:24:12	AP failed to connect to LS	Major	Outstanding	AP E08	N/A	N/A	N/A	N/A
2020/04/01 12:31:04	AP failed to connect to LS	Major	Outstanding	AP E04C	N/A	N/A	N/A	N/A
2020/04/03 06:45:20	Radius server unreachable	Major	Cleared	AP E08	N/A	System	2020/04/03 06:45:28	Auto Cleared
2020/04/01 06:45:18	AP rebooted by system	Major	Outstanding	AP E08	N/A	N/A	N/A	N/A
2020/04/03 06:17:00	AP disconnected	Major	Cleared	AP E03	N/A	System	2020/04/03 06:17:30	Auto Cleared
2020/04/01 06:16:58	AP rebooted by system	Major	Outstanding	AP E03	N/A	N/A	N/A	N/A
2020/04/01 06:16:38	AP failed to connect to LS	Major	Outstanding	AP E03	N/A	N/A	N/A	N/A
2020/04/03 06:16:58	No LS responses	Major	Outstanding	AP E03	N/A	N/A	N/A	N/A
2020/04/01 02:32:48	AP failed to connect to LS	Major	Outstanding	AP E04C	N/A	N/A	N/A	N/A
2020/04/01 02:03:54	AP rebooted by system	Major	Outstanding	AP E08	N/A	N/A	N/A	N/A
2020/04/02 20:13:29	AP rebooted by system	Major	Outstanding	AP E03	N/A	N/A	N/A	N/A
2020/04/02 15:06:16	Connect to data streamin...	Critical	Cleared	Node Id	N/A	System	2020/04/02 15:11:41	Auto Cleared
2020/04/02 12:15:08	No LS responses	Major	Outstanding	AP E04C	N/A	N/A	N/A	N/A
2020/04/01 23:00:47	AP rebooted by system	Major	Outstanding	AP E08	N/A	N/A	N/A	N/A
2020/04/01 20:21:52	AP failed to connect to LS	Major	Outstanding	AP E05	N/A	N/A	N/A	N/A
2020/04/01 19:39:51	AP rebooted by system	Major	Outstanding	AP E08	N/A	N/A	N/A	N/A
2020/04/01 19:38:13	AP rebooted by system	Major	Outstanding	AP E08	N/A	N/A	N/A	N/A
2020/04/01 19:06:05	No LS responses	Major	Outstanding	AP E04C	N/A	N/A	N/A	N/A
2020/04/01 19:01:38	AP rebooted by system	Major	Outstanding	AP E08	N/A	N/A	N/A	N/A
2020/04/01 19:01:38	No LS responses	Major	Outstanding	AP E08	N/A	N/A	N/A	N/A

## Downloading the Logs from the Controller

You can download the logs from the controller by performing the following.

- In the web interface, navigate to **Diagnostics > Application Logs**.

FIGURE 295 Downloading the Logs form the Controller



- The **Application log** page appears. In the **Select Control Plane** field, select the control plane form the drop-down list.
- Click **Download Snapshot Logs** and save it.

## Viewing the Audit Records

The audit records are listed below.

<b>Auditable Events</b>	Start-up and shut-down of audit functions
<b>Additional Content</b>	None

## Audit Records

### Viewing the Audit Records

<b>SZ144 (Physical)</b>	<p>The audit functions correspond with the startup and shutdown of the device.</p> <p><b>Start Up</b> 2021-01-01T12:00:00+00:00 SZ144 Core: @@835,nodeBackToInService,"sourceBladeUUID"="44743360-244d-4dcc-b722-8fdd45e30cf3","nodeMac"="B4:79:C8:25:82:30","clusterName"="SZ144Test","wsgMgmtIp"="172.16.16.244","nodeName"="SZ144"</p> <p><b>Shut Down</b> 2021-01-01T12:00:00+00:00 SZ144-CC Core: @@826,nodeRebooted,"toVersion"="5.2.1.3.1228","reason"="Normal Boot!","sourceBladeUUID"="1e4f2602-c4f8-4293-8511-e33324a51089","nodeName"="SZ144-CC","wsgMgmtIp"="172.16.16.144","clusterName"="SZ144-CC","nodeMac"="70:CA:97:25:01:80"</p>
<b>vsZ-H (Virtual)</b>	<p>The audit functions correspond with the startup and shutdown of the device</p> <p><b>Start Up</b> 2021-01-01T12:00:00+00:00 vszh Core: @@835,nodeBackToInService,"nodeName"="vszh","clusterName"="HighScale","sourceBladeUUID"="c8b436f2-eb54-495d-ab10-1212190c891a","wsgMgmtIp"="172.16.16.230","nodeMac"="00:0C:29:13:08:76"</p> <p><b>Shut Down</b> 2021-01-01T12:00:00+00:00 vszh Core: c.r.w.d.u.s.ForwardErrorEventUtils - @@826,nodeRebooted,"reason"="Normal reboot!","wsgMgmtIp"="172.16.16.230","clusterName"="HighScale","nodeMac"="00:0C:29:13:08:76","toVersion"="5.1.1.3.1231","nodeName"="vszh","sourceBladeUUID"="c8b436f2-eb54-495d-ab10-1212190c891a"</p>
<b>vsZ-D</b>	<p>The audit functions correspond with the startup and shutdown of the device</p> <p><b>Start Up</b> 2021-01-01T12:00:00+00:00 vszh Core: @515,dpPhyInterfaceUp,"dpKey"="97HM3WVA5234U0JPM34HJEU1XTA000C29B4693A000C29B46944","portID"="0"</p> <p><b>Shutdown</b> 2021-01-01T12:00:00+00:00 vszh Core: @513,dpDisconnected,"dpKey"="97HM3WVA5234U0JPM34HJEU1XTA000C29B4693A000C29B46944","timestamp"="1585584738918","cpName"="vszh","wsgIP"="172.16.8.230","reason"="1, NMI problem."</p>
<b>AP</b>	<p>The audit functions correspond with the startup and reboot of the device .</p> <p><b>Start Up</b> 2021-01-01T12:00:00+00:00 vszh Core: @312,apConnected,"idealEventVersion"="3.5.1","domainId"="8b2081d5-9662-40d9-a3db-2a3cf4dde3f7","zoneUUID"="7079e8e4-ac46-4086-803b-6b4bc3a46de2","zoneName"="TestZone","apGroupUUID"="35f4aa9e-6b5c-4a05-8035-bdc2ac8674ea","apMac"="94:BF:C4:22:75:00","apName"="T710","apLocation"="", "apDescription"=null,"apGps"="39.232527,-76.822969","apIpAddress"="172.16.8.248","apIpv6Address"="", "timeZone"="EST +5EDT,M3.2.0/02","serialNumber"="521803001443","domainName"="Administration Domain","timestamp"="1585584010186","reason"="AP connected after rebooting"</p> <p><b>Reboot</b></p> <p>2021-01-01T12:00:00+00:00 SZ144-CC Core: @826,nodeRebooted,"toVersion"="5.2.1.3.1228","reason"="Normal Boot!","sourceBladeUUID"="1e4f2602-c4f8-4293-8511-e33324a51089","nodeName"="SZ144-CC","wsgMgmtIp"="172.16.16.144","clusterName"="SZ144-CC","nodeMac"="70:CA:97:25:01:80"</p> <p>2021-01-01T12:00:00+00:00 vszh Core: c.r.w.d.u.s.ForwardErrorEventUtils - @826,nodeRebooted,"reason"="Normal reboot!","wsgMgmtIp"="172.16.16.230","clusterName"="HighScale","nodeMac"="00:0C:29:13:08:76","toVersion"="5.1.1.3.1231","nodeName"="vszh","sourceBladeUUID"="c8b436f2-eb54-495d-ab10-1212190c891a"</p>

<b>Auditable Events</b>	Enabling communications between a pair of components. Disabling communications between a pair of components.
<b>Additional Content</b>	Identities of the endpoints pairs enabled or disabled.



<b>SZ144 (Physical)</b>	<p><b>Enabled</b> 2021-01-01T12:00:00+00:00 Core:                  @@312,apConnected,"idealEventVersion"="3.5.1","domainId"="8b2081d5-9662-40d9-a3db-2a3cf4dde3f7","zoneUUID"="f77a8816-3049-40cd-8484-82919275ddc3","zoneName"="Default Zone","apGroupUUID"="18e2a1fc-fdee-475d-950d-6eda1f6f5ab7","apMac"="C8:08:73:30:F2:90","apName"="R610","apLocation"="", "apDescription"=null,"apGps"="", "apIpAddress"="172.16.16.245",                  "apIpv6Address"="fc00::1","timeZone"=null,"serialNumber"="501849000776","domainName"="Administration Domain","timestamp"="1582558656170","reason"="AP connected after rebooting"</p> <p><b>Disabled</b> 2021-01-01T12:00:00+00:00 Core:                  @@313,apDeleted,"apName"="R610","apMac"="C8:08:73:30:F2:90","model"="R610","zoneUUID"="f77a8816-3049-40cd-8484-82919275ddc3","fwVersion"="5.1.1.3.1124","apGps"="", "apDescription"="", "apIpAddress"="172.16.16.245",                  "zoneName"="Default Zone", "domainName"="Administration Domain", "serialNumber"="501849000776",                  "timeZone"="", "apLocation"=""</p>
<b>vsZ-H (Virtual)</b>	<p><b>Enabled</b> 2021-01-01T12:00:00+00:00 vszh Core:                  @@312,apConnected,"idealEventVersion"="3.5.1","domainId"="8b2081d5-9662-40d9-a3db-2a3cf4dde3f7","zoneUUID"="7079e8e4-ac46-4086-803b-6b4bc3a46de2","zoneName"="TestZone", "apGroupUUID"="35f4aa9e-6b5c-4a05-8035-bdc2ac8674ea", "apMac"="94C4:22:75:00", "apName"="T710", "apLocation"="", "apDescription"=null, "apGps"="39.295598,-76.754107", "apIpAddress"="172.16.8.248", "apIpv6Address"="fc00::1", "timeZone"=null, "serialNumber"="521803001443", "domainName"="Administration Domain", "timestamp"="1585498034724", "reason"="AP connected after rebooting"</p> <p><b>Disabled</b> 2021-01-01T12:00:00+00:00 vszh Core:                  @@313,apDeleted,"apName"="T710", "apMac"="94:BF:C4:22:75:00", "model"="T710", "zoneUUID"="7079e8e4-ac46-4086-803b-6b4bc3a46de2", "fwVersion"="5.1.1.3.1126", "apGps"="39.295598,-76.754107", "apDescription"="", "apIpAddress"="172.16.8.248", "zoneName"="TestZone", "domainName"="Administration Domain", "serialNumber"="521803001443", "timeZone"="", "apLocation"=""</p>
<b>vsZ-D</b>	<p><b>Enabled</b> 2021-01-01T12:00:00+00:00 vszh Core:                  @@512,dpConnected,"dpKey"="97HM3WVA5234U0JPM34HJEU1XTA000C29B4693A000C29B46944", "timestamp"="1585498710059", "cpName"="vszh", "wsgiP"="172.16.8.230"</p> <p><b>Disabled</b> 2021-01-01T12:00:00+00:00 vszh Core:                  @@513,dpDisconnected,"dpKey"="97HM3WVA5234U0JPM34HJEU1XTA000C29B4693A000C29B46944", "timestamp"="1585001239636", "cpName"="vszh", "wsgiP"="172.16.8.230", "reason"="1, NMI problem."</p>
<b>AP</b>	<p><b>Enabled</b></p> <p>2021-01-01T12:00:00+00:00 vszh Core: @@99018,sshInitiation, "apMac"="94:BF:C4:22:75:00", "reason"="SSH Login successful with IP 172.16.8.254 username admin", "fwVersion"="5.1.1.3.1125", "model"="T710", "zoneUUID"="7079e8e4-ac46-4086-803b-6b4bc3a46de2", "zoneName"="TestZone", "timeZone"="EST +5EDT,M3.2.0/02:00,M11.1.0/02:00", "apLocation"="", "apGps"="39.295072,-76.7", "apIpAddress"="172.16.8.248", "apIpv6Address"="2001::172:16:8:248", "apGroupUUID"="35f4aa9e-6b5c-4a05-8035-bdc2ac8674ea", "domainId"="8b2081d5-9662-40d9-a3db-2a3cf4dde3f7", "serialNumber"="521803001443", "domainName"="Administration Domain", "idealEventVersion"="3.5.1", "apDescription"=""</p> <p><b>Disabled</b></p> <p>2021-01-01T12:00:00+00:00 vszh Core: @@99019,sshTermination, "apMac"="", "reason"="SSH session exited", "fwVersion"="5.1.1.3.1128", "model"="T710", "zoneUUID"="7079e8e4-ac46-4086-803b-6b4bc3a46de2", "zoneName"="TestZone", "timeZone"="EST +5EDT,M3.2.0/02:00,M11.1.0/02:00", "apLocation"="", "apGps"="39.295598,-76.7", "apIpAddress"="172.16.8.248", "apIpv6Address"="fc00::1", "apGroupUUID"="35f4aa9e-6b5c-4a05-8035-bdc2ac8674ea", "domainId"="8b2081d5-9662-40d9-a3db-2a3cf4dde3f7", "serialNumber"="521803001443", "domainName"="Administration Domain", "idealEventVersion"="3.5.1", "apDescription"=""</p>

<b>Auditable Events</b>	Failure to establish a HTTPS Session
<b>Additional Content</b>	Reason for failure.
<b>SZ144 (Physical)</b>	2021-01-01T12:00:00+00:00 SZ144 Web Activity: "User:[admin],Browser IP:[172.16.16.153],Action:[Log on failed],Resource:[Administrator],Description:[Administrator [admin] logged on failed from [172.16.16.153].]"
<b>vsZ-H (Virtual)</b>	2021-01-01T12:00:00+00:00 vszh Web Activity: "User:[admin],Browser IP:[172.16.16.253],Action:[Log on failed],Resource:[Administrator],Description:[Administrator [admin] logged on failed from [172.16.16.253].]"

## Audit Records

### Viewing the Audit Records

vSZ-D	N/A
AP	N/A

<b>Auditable Events</b>	Failure to establish anIPSec SA.
<b>Additional Content</b>	Reason for failure.
<b>SZ144 (Physical)</b>	<p><b>Invalid IKE Proposal</b> 2021-01-01T12:00:00+00:00 SZ144 strongswan: 16[IKE] received proposals unacceptable</p> <p><b>Invalid ESP Proposal</b> 2021-01-01T12:00:00+00:00 SZ144 strongswan: 05[IKE] no acceptable proposal found</p> <p><b>Invalid Cert Identifier</b> 2021-01-01T12:00:00+00:00 SZ144 strongswan: 10[CFG] no matching peer config found</p>
<b>vSZ-H (Virtual)</b>	<p><b>Invalid IKE Proposal</b> 2021-01-01T12:00:00+00:00 vszh strongswan: 07[IKE] received proposals unacceptable</p> <p><b>Invalid ESP Proposal</b> 2021-01-01T12:00:00+00:00 vszh strongswan: 12[IKE] no acceptable proposal found</p> <p><b>Invalid Cert Identifier</b> 2021-01-01T12:00:00+00:00 vszh strongswan: 09[CFG] no matching peer config found</p>
<b>vSZ-D</b>	2021-01-01T12:00:00+00:00 vszh Core: @99243,dplPsecSaFailed,"dpKey"="97HM3WVA5234U0JPM34HJEUJ1XTA000C29B4693A000C29B46944","dstIP"="172.16.8.31","apiP"="172.16.8.248","reason"="spi 0x7a010000 SA not found"
<b>AP</b>	2021-01-01T12:00:00+00:00 vszh Core: @99026,ipsecFailure,"apMac"="94:BF:C4:22:75:00","reason"="IPSec session for apiP= 172.16.8.248 with dpIP= 172.16.8.31 tunnelType:Ruckus GRE Failed,"fwVersion"="5.1.1.3.1125","model"="T710","zoneUUID"="7079e8e4-ac46-4086-803b-6b4bc3a46de2","zoneName"="TestZone","timeZone"="EST +5EDT,M3.2.0/02:00,M11.1.0/02:00","apLocation"="", "apGps"="39.295072,-76.7","apIpAddress"="172.16.8.248","apIpv6Address"="2001::172:16:8:248","apGroupUUID"="35f4aa9e-6b5c-4a05-8035-bdc2ac8674ea","domainId"="8b2081d5-9662-40d9-a3db-2a3cf4dde3f7","serialNumber"="521803001443","domainName"="Administration Domain","idealEventVersion"="3.5.1","apDescription"=""

<b>Auditable Events</b>	Configuration of a new time server Removal of configured time server.
<b>Additional Content</b>	Identity if new/removed time server.
<b>SZ144 (Physical)</b>	2021-01-01T12:00:00+00:00 SZ144 Core: @99301,disContTimeChange, "before"="Mon Feb 17 16:00:19 2020", "after"="Mon Feb 17 19:07:35 2020", "server"="172.16.16.254", "local_ip"="172.16.16.244"
<b>vSZ-H (Virtual)</b>	2021-01-01T12:00:00+00:00 vszh Core: @99301,disContTimeChange, "before"="Fri Feb 21 16:57:58 2020", "after"="Fri Feb 21 22:57:42 2020", "server"="172.16.16.254", "local_ip"="172.16.16.230"
<b>vSZ-D</b>	N/A
<b>AP</b>	N/A

<b>Auditable Events</b>	Protocol failures. Establishment/Termination of anIPSec SA. Negotiation "down" from an IKEv2 to IKEv1 exchange.
<b>Additional Content</b>	Reason for failure. Non-TOE endpoint of connection (IP address) for both successes and failures.
<b>SZ144 (Physical)</b>	<p><b>Protocol Failures</b> Failure to establish an IPSec SA</p> <p><b>Establishment</b> 2021-01-01T12:00:00+00:00 SZ144 strongswan: 07[IKE] IKE_SA ipsec[1] established between 172.16.16.244[172.16.16.244]...172.16.16.254[172.16.16.254]</p> <p><b>Termination</b> 2021-01-01T12:00:00+00:00 SZ144 strongswan: 09[IKE] deleting IKE_SA ipsec[8] between 172.16.16.244[172.16.16.244]...172.16.16.254[172.16.16.254]</p>
<b>vSZ-H (Virtual)</b>	<p><b>Protocol Failures</b> Failure to establish an IPSec SA</p> <p><b>Establishment</b> 2021-01-01T12:00:00+00:00 vszh strongswan: 08[IKE] IKE_SA ipsec[1] established between 172.16.8.230[C=US, ST=MD, L=Catonsville, O=GSS, CN=SZ144.example.com, E=server-SZ144-IPsec-rsa@gossamersec.com]...172.16.8.254[C=US, ST=MD, L=Catonsville, O=GSS, CN=t14-16x.example.com, E=server-rsa@gossamersec.com]</p> <p><b>Termination</b> 2021-01-01T12:00:00+00:00 vszh strongswan: 15[IKE] deleting IKE_SA ipsec[2] between 172.16.8.230[C=US, ST=MD, L=Catonsville, O=GSS, CN=SZ144.example.com, E=server-SZ144-IPsec-rsa@gossamersec.com]...172.16.8.254[C=US, ST=MD, L=Catonsville, O=GSS, CN=t14-16x.example.com, E=server-rsa@gossamersec.com]</p>

<b>vsZ-D</b>	<p><b>Protocol Failures</b> Failure to establish an IPsec SA</p> <p><b>Establishment</b> 2021-01-01T12:00:00+00:00 vszh Core: @@99244,dplPsecSaUpdated,"dpKey"="97HM3WVA5234U0JPM34HJEU1XTA000C29B4693A000C29B46944","dstIP"="172.16.8.248","apIP"="172.16.8.248","action"="spi 0xc52b4656 insert SA"</p> <p><b>Termination</b> 2021-01-01T12:00:00+00:00 vszh Core: @@99242,dplPsecTunnTerminated,"dpKey"="97HM3WVA5234U0JPM34HJEU1XTA000C29B4693A000C29B46944","apIP"="172.16.8.248"</p>
<b>AP</b>	<p><b>Protocol Failures</b> Failure to establish an IPsec SA</p> <p><b>Establishment</b> 2021-01-01T12:00:00+00:00 vszh Core: @608,apBuildTunnelSuccess,"apMac"="94:bf:c4:22:75:00","dpIP"="[172.16.8.31]:0","fwVersion"="5.1.1.3.1125","model"="T710","zoneUUID"="7079e8e4-ac46-4086-803b-6b4bc3a46de2","zoneName"="TestZone","timeZone"="EST+5EDT,M3.2.0/02:00,M11.1.0/02:00","apLocation"="","apGps"="39.295072,-76.7","apIpAddress"="172.16.8.248","apIpv6Address"="2001::172:16:8:248","apGroupUUID"="35f4aa9e-6b5c-4a05-8035-bdc2ac8674ea","domainId"="8b2081d5-9662-40d9-a3db-2a3cf4dde3f7","serialNumber"="521803001443","domainName"="Administration Domain","idealEventVersion"="3.5.1","apDescription"=""</p> <p><b>Termination</b> 2021-01-01T12:00:00+00:00 vszh Core: @99025,ipsecTermination,"apMac"="94:BF:C4:22:75:00","reason"="IPsec session for apIP= 172.16.8.248 with dpIP= 172.16.8.31 tunnelType:Ruckus GRE Terminated","fwVersion"="5.1.1.3.1125","model"="T710","zoneUUID"="7079e8e4-ac46-4086-803b-6b4bc3a46de2","zoneName"="TestZone","timeZone"="EST+5EDT,M3.2.0/02:00,M11.1.0/02:00","apLocation"="","apGps"="39.295072,-76.7","apIpAddress"="172.16.8.248","apIpv6Address"="2001::172:16:8:248","apGroupUUID"="35f4aa9e-6b5c-4a05-8035-bdc2ac8674ea","domainId"="8b2081d5-9662-40d9-a3db-2a3cf4dde3f7","serialNumber"="521803001443","domainName"="Administration Domain","idealEventVersion"="3.5.1","apDescription"=""</p>

<b>Auditable Events</b>	Failure to establish an SSH client session.
<b>Additional Content</b>	Reason for failure.
<b>SZ144 (Physical)</b>	N/A
<b>vsZ-H (Virtual)</b>	N/A
<b>vsZ-D</b>	The vsZ-D wont log to the SZ controller if the ITT connection fails. A local log can be pulled from the vsZ-D if required:  2021-01-01T12:00:00+00:00 esxidp dpm[3987]: @@99230,dpSshTunnFailed,"dpKey"="97HM3WVA5234U0JPM34HJEU1XTA000C29B4693A000C29B46944","scgIP"="172.16.8.230"
<b>AP</b>	The AP wont log to the SZ controller if the ITT connection fails. A local log can be pulled from the AP if required:  Apr 2 00:39:20 T710 daemon.err rsm_d_func[13975]: SShTunnel start Failed ServerIP=172.16.8.230

<b>Auditable Events</b>	Failure to establish an SSH server session
<b>Additional Content</b>	Reason for failure.
<b>SZ144 (Physical)</b>	<p><b>Failed Password</b> 2021-01-01T12:00:00+00:00 SZ144 sshd[16052]: Failed password for admin from 172.16.16.254 port 33578 ssh2</p> <p><b>Invalid Public Key Algorithm</b> 2021-01-01T12:00:00+00:00 SZ144 sshd[7138]: Unable to negotiate with 172.16.16.254 port 33620: no matching host key type found. Their offer: ssh-dss</p> <p><b>Invalid HMAC</b> 2021-01-01T12:00:00+00:00 SZ144 sshd[3644]: Unable to negotiate with 172.16.16.254 port 33744: no matching MAC found. Their offer: hmac-md5</p> <p><b>Invalid Key Exchange</b> 2021-01-01T12:00:00+00:00 SZ144 sshd[14509]: Unable to negotiate with 172.16.16.254 port 33826: no matching key exchange method found. Their offer: diffie-hellman-group1-sha1,ext-info-c</p>

## Audit Records

### Viewing the Audit Records

<b>vSZ-H (Virtual)</b>	<p><b>Failed Password</b> 2021-01-01T12:00:00+00:00 vszh sshd[10124]: Failed password for admin from 172.16.16.154 port 60940 ssh2</p> <p><b>Invalid Public Key Algorithm</b> 2021-01-01T12:00:00+00:00 vszh sshd[4241]: Unable to negotiate with 172.16.8.254 port 45354: no matching host key type found. Their offer: ssh-dss</p> <p><b>Invalid HMAC</b> 2021-01-01T12:00:00+00:00 vszh sshd[19379]: Unable to negotiate with 172.16.8.254 port 45436: no matching MAC found. Their offer: hmac-md5</p> <p><b>Invalid Key Exchange</b> 2021-01-01T12:00:00+00:00 vszh sshd[30431]: Unable to negotiate with 172.16.8.254 port 45518: no matching key exchange method found. Their offer: diffie-hellman-group1-sha1,ext-info-c</p>
<b>vSZ-D</b>	N/A
<b>AP</b>	N/A

<b>Auditable Events</b>	Failure to establish a TLS Session (HTTPS)
<b>Additional Content</b>	Reason for failure.
<b>SZ144 (Physical)</b>	<p>2021-01-01T12:00:00+00:00 [info] 2501#2501: *6041 SSL_do_handshake() failed (SSL: error:1408A0C1:SSL routines:SSL3_GET_CLIENT_HELLO:no shared cipher) while SSL handshaking, client: ::ffff:172.16.16.254, server: [::]:8443</p> <p>2021-01-01T12:00:00+00:00 [crit] 2501#2501: *6042 SSL_do_handshake() failed (SSL: error:1408B010:SSL routines:SSL3_GET_CLIENT_KEY_EXCHANGE:EC lib) while SSL handshaking, client: ::ffff:172.16.16.254, server: [::]:8443</p> <p>2021-01-01T12:00:00+00:00 [info] 2501#2501: *6043 SSL_do_handshake() failed (SSL: error:1408C095:SSL routines:SSL3_GET_FINISHED:digest check failed) while SSL handshaking, client: ::ffff:172.16.16.254, server: [::]:8443</p> <p>2021-01-01T12:00:00+00:00 [info] 2501#2501: *6044 SSL_do_handshake() failed (SSL: error:1408E098:SSL routines:SSL3_GET_MESSAGE:excessive message size) while SSL handshaking, client: ::ffff:172.16.16.254, server: [::]:8443</p> <p>2021-01-01T12:00:00+00:00 [info] 2501#2501: *6045 SSL_do_handshake() failed (SSL: error:1408F081:SSL routines:SSL3_GET_RECORD:block cipher pad is wrong) while SSL handshaking, client: ::ffff:172.16.16.254, server: [::]:8443</p> <p>2021-01-01T12:00:00+00:00 [info] 2500#2500: *6046 SSL_do_handshake() failed (SSL: error:140760FC:SSL routines:SSL23_GET_CLIENT_HELLO:unknown protocol) while SSL handshaking, client: ::ffff:172.16.16.254, server: [::]:8443</p>
<b>vSZ-H (Virtual)</b>	<p>2021-01-01T12:00:00+00:00 [info] 13797#13797: *7604 SSL_do_handshake() failed (SSL: error:1408A0C1:SSL routines:SSL3_GET_CLIENT_HELLO:no shared cipher) while SSL handshaking, client: ::ffff:172.16.16.254, server: [::]:8443</p> <p>2021-01-01T12:00:00+00:00 [crit] 13796#13796: *7605 SSL_do_handshake() failed (SSL: error:1408B010:SSL routines:SSL3_GET_CLIENT_KEY_EXCHANGE:EC lib) while SSL handshaking, client: ::ffff:172.16.16.254, server: [::]:8443</p> <p>2021-01-01T12:00:00+00:00 [info] 13797#13797: *7606 SSL_do_handshake() failed (SSL: error:1408C095:SSL routines:SSL3_GET_FINISHED:digest check failed) while SSL handshaking, client: ::ffff:172.16.16.254, server: [::]:8443</p> <p>2021-01-01T12:00:00+00:00 [info] 13796#13796: *7607 SSL_do_handshake() failed (SSL: error:1408E098:SSL routines:SSL3_GET_MESSAGE:excessive message size) while SSL handshaking, client: ::ffff:172.16.16.254, server: [::]:8443</p> <p>2021-01-01T12:00:00+00:00 [info] 13796#13796: *7609 SSL_do_handshake() failed (SSL: error:1408F081:SSL routines:SSL3_GET_RECORD:block cipher pad is wrong) while SSL handshaking, client: ::ffff:172.16.16.254, server: [::]:8443</p> <p>2021-01-01T12:00:00+00:00 [info] 13797#13797: *7610 SSL_do_handshake() failed (SSL: error:140760FC:SSL routines:SSL23_GET_CLIENT_HELLO:unknown protocol) while SSL handshaking, client: ::ffff:172.16.16.254, server: [::]:8443</p>
<b>vSZ-D</b>	N/A
<b>AP</b>	N/A

<b>Auditable Events</b>	Attempts to access the 802.1X controlled port prior to successful completion of the authentication exchange.
<b>Additional Content</b>	Provided client identity (MAC address).
<b>SZ144 (Physical)</b>	N/A
<b>vSZ-H (Virtual)</b>	N/A
<b>vSZ-D</b>	N/A

AP	2021-01-01T12:00:00+00:00 vszh Core: @@203,clientJoinFailure,"apMac"="94:bf:c4:22:75:00","clientMac"="70:18:8b:02:f2:f3","ssid"="VSZHWLAN","bssid"="94:bf:c4:22:75:08","userId"="", "wlanId"="1","iface"="wlan0","tenantUUID"="839f87c6-d116-497e-afce-aa8157abd30c","apName"="T710","apGps"="39.295655,-76.753728","userName"="", "vlanId"="1","radio"="b/g/n","encryption"="WPA2-AES","fwVersion"="5.1.1.3.1125","model"="T710","zoneUUID"="7079e8e4-ac46-4086-803b-6b4bc3a46de2","zoneName"="TestZone","timeZone"="UTC+0","apLocation"="", "apGps"="39.295655,-76.7","apIpAddress"="172.16.8.248","apIpv6Address"="2001::172:16:8:248","apGroupUUID"="35f4aa9e-6b5c-4a05-8035-bdc2ac8674ea","domainId"="8b2081d5-9662-40d9-a3db-2a3cf4dde3f7","serialNumber"="521803001443","domainName"="Administration Domain","wlanGroupUUID"="4a0d08e0-5e34-11ea-8d1d-fa23a50db6e8","idealEventVersion"="3.5.1","apDescription"=""
----	---

Auditable Events	Unsuccessful login attempt limit is met or exceeded.
Additional Content	Origin of the attempt (e.g., IP address).
SZ144 (Physical)	N/A 2021-01-01T12:00:00+00:00 SZ144 Core: @@8011,adminAccountLockout,"userName"="admin","ip"="172.16.16.153","lockoutDuration"="5"
vSZ-H (Virtual)	2021-01-01T12:00:00+00:00 vszh Core: @@8011,adminAccountLockout,"userName"="admin","ip"="172.16.16.153","lockoutDuration"="5"
vSZ-D	N/A
AP	N/A

Auditable Events	The reaching of the threshold for the unsuccessful authentication attempts and the actions taken (e.g., disabling of an account) and the subsequent, if appropriate, restoration to the normal state (e.g., re-enabling of a terminal)..
Additional Content	
SZ144 (Physical)	See Unsuccessful login attempt limit is met or exceeded
vSZ-H (Virtual)	See Unsuccessful login attempt limit is met or exceeded
vSZ-D	N/A
AP	N/A

Auditable Events	Attempts to re-authenticate.
Additional Content	Origin of the attempt (e.g., IP address).
SZ144 (Physical)	2021-01-01T12:00:00+00:00 SZ144 Web Activity: "User:[admin],Browser IP:[172.16.16.253],Action:[Re-authenticate],Resource:[Administrator],Description:[The re-authentication is successful.]"
vSZ-H (Virtual)	2021-01-01T12:00:00+00:00 vszh Web Activity: "User:[admin],Browser IP:[172.16.16.253],Action:[Re-authenticate],Resource:[Administrator],Description:[The re-authentication is successful.]"
vSZ-D	N/A
AP	N/A

Auditable Events	All use of identification and authentication mechanism.
Additional Content	Origin of the attempt (e.g., IP address).

## Audit Records

### Viewing the Audit Records

<b>SZ144 (Physical)</b>	<p><b>Logon success</b></p> <p><b>Web UI</b> 2021-01-01T12:00:00+00:00 SZ144 Web Activity: "User:[admin],Browser IP:[172.16.16.253],Action:[Log on],Resource:[Administrator],Description:[Administrator [admin] logged on from [172.16.16.253].]"</p> <p><b>CLI</b> 2021-01-01T12:00:00+00:00 SZ144 Web Activity: "User:[admin],Browser IP:[127.0.0.1],Action:[Log on],Resource:[Administrator],Description:[Administrator [admin] logged on from CLI.]"</p> <p><b>SSH</b> 2021-01-01T12:00:00+00:00 SZ144 Core: @@8008,szLogin,"userName"="admin","ip"="172.16.16.254"</p> <p><b>Logon Failure</b></p> <p><b>WebUi</b> See Failure to establish a HTTPS Session</p> <p><b>CLI</b> 2021-01-01T12:00:00+00:00 SZ144 login: FAILED LOGIN 2 FROM (null) FOR admin, Authentication failure</p> <p><b>SSH</b> 2021-01-01T12:00:00+00:00 SZ144 Core: @@8007,szLoginFail,"userName"="admin","ip"="172.16.16.254"</p>
<b>vsZ-H (Virtual)</b>	<p><b>Logon success</b></p> <p><b>Web UI</b> 2021-01-01T12:00:00+00:00 vszh Web Activity: "User:[admin],Browser IP:[172.16.16.153],Action:[Log on],Resource:[Administrator],Description:[Administrator [admin] logged on from [172.16.16.153].]"</p> <p><b>CLI</b> 2021-01-01T12:00:00+00:00 vszh Web Activity: "User:[admin],Browser IP:[172.16.16.254],Action:[Log on],Resource:[Administrator],Description:[Administrator [admin] logged on from CLI.]"</p> <p><b>SSH</b> 2021-01-01T12:00:00+00:00 vszh Core: @@8008,szLogin,"userName"="admin","ip"="172.16.16.254"</p> <p><b>Logon Failure</b></p> <p><b>WebUi</b> See Failure to establish a HTTPS Session</p> <p><b>CLI</b> 2021-01-01T12:00:00+00:00 vszh login: FAILED LOGIN 3 FROM (null) FOR admin, Authentication failure</p> <p><b>SSH</b> 2021-01-01T12:00:00+00:00 vszh Core: @@8007,szLoginFail,"userName"="admin","ip"="172.16.16.254"</p>
<b>vsZ-D</b>	N/A
<b>AP</b>	N/A

<b>Auditable Events</b>	Failure to establish TLS Connection (Radsec)
<b>Additional Content</b>	Reason for TLS failure due to key exchange failure, certificate verification failed, invalid encoding, wrong ssl version and CN/SAN mismatch.
<b>SZ144 (Physical)</b>	<p><b>Radsec</b></p> <p>2021-01-01T12:00:00+00:00[SZ144-CC][RADIUS][ERR][TID=780125952][src/main/cb.c:70]#012tls: TLS_connect: Error in SSLv3 read server key exchange B</p> <p>2021-01-01T12:00:00+00:00[SZ144-CC][RADIUS][ERR][TID=780125952][src/main/tls.c:326]#012tls: error:1408D07B:SSL routines:SSL3_GET_KEY_EXCHANGE:bad signature</p> <p>2021-01-01T12:00:00+00:00[SZ144-CC][RADIUS][ERR][TID=260040448][src/main/tls.c:326]#012tls: error:10067066:elliptic curve routines:ec_GFp_simple_oct2point:invalid encoding</p> <p>2021-01-01T12:00:00+00:00[SZ144-CC][RADIUS][ERR][TID=754947840][src/main/tls.c:300]#012tls: Failed in __FUNCTION__ (SSL_connect): error:1408C095:SSL routines:SSL3_GET_FINISHED:digest check failed</p> <p>2021-01-01T12:00:00+00:00[SZ144-CC][RADIUS][ERR][TID=754947840][src/main/tls.c:300]#012tls: Failed in __FUNCTION__ (SSL_connect): error:1408C095:SSL routines:SSL3_GET_FINISHED:digest check failed</p> <p>2021-01-01T12:00:00+00:00 [SZ144-CC][RADIUS][ERR][TID=771733248][src/main/tls.c:300]#012tls: Failed in __FUNCTION__ (SSL_connect): error:1408F081:SSL routines:SSL3_GET_RECORD:block cipher pad is wrong</p> <p>2021-01-01T12:00:00+00:00 [SZ144-CC][RADIUS][ERR][TID=268433152][src/main/tls.c:300]#012tls: Failed in __FUNCTION__ (SSL_connect): error:1409210A:SSL routines:SSL3_GET_SERVER_HELLO:wrong ssl version</p> <p>2021-01-01T12:00:00+00:00 [SZ144-CC][RADIUS][ERR][TID=1291818752][src/main/tls.c:2943]#012 Certificate SAN-DNS doesn't match with SAN Identifier: (Bad CN identifier)</p>

<p><b>vSZ-H (Virtual)</b></p>	<p><b>Radsec</b></p> <p>2021-01-01T12:00:00+00:00 [vSZ-H][RADIUS][ERR][TID=447129344][src/main/tls.c:300]#012tls: Failed in __FUNCTION__ (SSL_connect): error:14090086:SSL routines:SSL3_GET_SERVER_CERTIFICATE:certificate verify failed</p> <p>2021-01-01T12:00:00+00:00 [vSZ-H][RADIUS][ERR][TID=405165824][src/main/cb.c:70]#012tls: TLS_connect: Error in SSLv3 read server key exchange B</p> <p>2021-01-01T12:00:00+00:00 [vSZ-H][RADIUS][ERR][TID=405165824][src/main/tls.c:326]#012tls: error:1408D07B:SSL routines:SSL3_GET_KEY_EXCHANGE:bad signature</p> <p>2021-01-01T12:00:00+00:00 [vSZ-H][RADIUS][ERR][TID=388380416][src/main/tls.c:300]#012tls: Failed in __FUNCTION__ (SSL_connect): error:1408C095:SSL routines:SSL3_GET_FINISHED:digest check failed</p> <p>2021-01-01T12:00:00+00:00 [vSZ-H][RADIUS][ERR][TID=396773120][src/main/tls.c:300]#012tls: Failed in __FUNCTION__ (SSL_connect): error:1408F081:SSL routines:SSL3_GET_RECORD:block cipher pad is wrong</p> <p>2021-01-01T12:00:00+00:00 [vSZ-H][RADIUS][ERR][TID=363202304][src/main/tls.c:326]#012tls: error:10067066:elliptic curve routines:ec_GFp_simple_oct2point:invalid encoding</p> <p>2021-01-01T12:00:00+00:00 [vSZ-H][RADIUS][ERR][TID=480700160][src/main/tls.c:300]#012tls: Failed in __FUNCTION__ (SSL_connect): error:140920F8:SSL routines:SSL3_GET_SERVER_HELLO:unknown cipher returned</p> <p>2021-01-01T12:00:00+00:00 [vSZ-H][RADIUS][ERR][TID=371595008][src/main/tls.c:300]#012tls: Failed in __FUNCTION__ (SSL_connect): error:1409210A:SSL routines:SSL3_GET_SERVER_HELLO:wrong ssl version</p> <p>2021-01-01T12:00:00+00:00 [vSZ-H][RADIUS][ERR][TID=556234496][src/main/tls.c:2943]#012 Certificate SAN-DNS doesn't match with SAN Identifier: (Bad CN Identifier)</p>
<p><b>vSZ-D</b></p>	<p>N/A</p>
<p><b>AP</b></p>	<p>N/A</p>

<p><b>Auditable Events</b></p>	<p>Unsuccessful attempt to validate a certificate. Any addition, replacement or removal of trust anchors in the TOE's trust store</p>
<p><b>Additional Content</b></p>	<p>Reason for failure of certificate validation Identification of certificates added, replaced or removed as trust anchor in the TOE's trust store.</p>

## Audit Records

### Viewing the Audit Records

<b>SZ144 (Physical)</b>	<b>IPsec</b>  2021-01-01T12:00:00+00:00 SZ144 strongswan: 13[CFG] no issuer certificate found for "C=US, ST=MD, L=Catonsville, O=GSS, CN=subca-rsa, E=subcarsa@gossamersec.com"  2021-01-01T12:00:00+00:00 SZ144 strongswan: 05[CFG] subject certificate invalid (valid from Dec 23 13:07:29 2019 to Dec 23 13:12:00 2019)  2021-01-01T12:00:00+00:00 SZ144 strongswan: 08[CFG] certificate was revoked on Dec 23 13:08:41 UTC 2019, reason: unspecified  2021-01-01T12:00:00+00:00 SZ144 strongswan: 07[CFG] ocsrp response verification failed, no signer certificate 'C=US, ST=MD, L=Catonsville, O=GSS, CN=serverocsp-subca-ecdsa,E=server-ocsp-subcaecdsa@gossamersec.com' found  2021-01-01T12:00:00+00:00 SZ144 strongswan: 09[LIB] OpenSSL X.509 parsing failed  2021-01-01T12:00:00+00:00 SZ144 strongswan: 12[IKE] no trusted RSA public key found for 'C=US,ST=MD, L=Catonsville,O=GSS, CN=tl4-16x.example.com,E=serverrsa@gossamersec.com'  2021-01-01T12:00:00+00:00 SZ144 strongswan: 08[CFG]ocsp request to http://172.16.161.1:7777 failed  <b>RadSec</b> 2021-01-01T12:00:00+00:00[SZ144-CC][RADIUS][ERR][TID=788518656][src/main/tls.c:2409]#012ocsp: Certificate has been expired/revoked  2021-01-01T12:00:00+00:00[SZ144-CC][RADIUS][ERR][TID=805304064][src/main/tls.c:326]#012tls: error:OD0680A8:asn1 encoding routines:ASN1_CHECK_TLEN:wrong tag  2021-01-01T12:00:00+00:00[SZ144-CC][RADIUS][ERR][TID=1291818752][src/main/tls.c:326]#012tls: error:0407006A:rsa routines:RSA_padding_check_PKCS1_type_1:block type is not 01  2021-01-01T12:00:00+00:00 [SZ144-CC][RADIUS][ERR][TID=1325389568][src/main/tls.c:326]#012tls: error:04091068:rsa routines:INT_RSA_VERIFY:bad signature  2021-01-01T12:00:00+00:00 [SZ144-CC][RADIUS][ERR][TID=-1325426944][src/main/tls.c:2343]#012Extension Key usage(OCSP SIGNING) is not present, Terminating TLS connect  2021-01-01T12:00:00+00:00 [SZ144-CC][RADIUS][ERR][TID=1325389568][src/main/tls.c:326]#012tls: error:14090086:SSL routines:SSL3_GET_SERVER_CERTIFICATE:certificate verify failed  <b>Add Cert to Trust Store</b> 2021-01-01T12:00:00+00:00 SZ144 Web Activity: "User:[admin],Browser IP:[172.16.16.253],Action:[Create],Resource:[Trusted CA Chain],Description:[Trusted CA Chain [ECDSA_New] created.]"  <b>Update Chain in Trust store</b> 2021-01-01T12:00:00+00:00 SZ144 Web Activity: "User:[admin],Browser IP:[172.16.16.253],Action:[Update],Resource:[Trusted CA Chain],Description:[Trusted CA Chain [RSA_New] updated.]"  <b>Delete Cert from Trust Store</b> 2021-01-01T12:00:00+00:00 SZ144 Web Activity: "User:[admin],Browser IP:[172.16.16.153],Action:[Delete],Resource:[Trusted CA Chain],Description:[Trusted CA Chain [ECDSA_New] deleted.]"
-------------------------	---



<p><b>vsZ-H (Virtual)</b></p>	<p><b>IPSec</b></p> <p>2021-01-01T12:00:00+00:00 vszh strongswan: 08[CFG] no issuer certificate found for "C=US, ST=MD, L=Catonsville, O=GSS, CN=tl4-16x.example.com, E=server-ecdasa@gossamersec.com"</p> <p>2021-01-01T12:00:00+00:00 vszh strongswan: 13[CFG] subject certificate invalid (valid from Jan 22 13:07:31 2020 to Jan 22 13:12:00 2020)</p> <p>2021-01-01T12:00:00+00:00 vszh strongswan: 05[CFG] certificate was revoked on Jan 22 13:08:38 UTC 2020, reason: unspecified</p> <p>2021-01-01T12:00:00+00:00 vszh strongswan: 05[CFG] ocp response verification failed, no signer certificate 'C=US, ST=MD, L=Catonsville, O=GSS, CN=server-ocsp-subca-rsa, E=server-ocsp-subca-rsa@gossamersec.com' found</p> <p>2021-01-01T12:00:00+00:00 vszh strongswan: 08[LIB] OpenSSL X.509 parsing failed</p> <p>2021-01-01T12:00:00+00:00 vszh strongswan: 15[IKE] no trusted RSA public key found for 'C=US, ST=MD, L=Catonsville, O=GSS, CN=tl4-16x.example.com, E=server-rsa@gossamersec.com'</p> <p>2021-01-01T12:00:00+00:00 vszh strongswan: 16[CFG] ocp request to http://172.16.16.1:7778 failed</p> <p><b>RadSec</b>2021-01-01T12:00:00+00:00 [vsZ-H][RADIUS][ERR][TID=1912551168][src/main/tls.c:2399]#012ocsp: Certificate has been expired/revoked</p> <p>2021-01-01T12:00:00+00:00 [vsZ-H][RADIUS][ERR][TID=573019904][src/main/tls.c:326]#012tls: error:0D0680A8:asn1 encoding routines:ASN1_CHECK_TLEN:wrong tag</p> <p>2021-01-01T12:00:00+00:00 [vsZ-H][RADIUS][ERR][TID=598198016][src/main/tls.c:326]#012tls: error:0407006A:rsa routines:RSA_padding_check_PKCS1_type_1:block type is not 01</p> <p>2021-01-01T12:00:00+00:00 [vsZ-H][RADIUS][ERR][TID=346416896][src/main/tls.c:326]#012tls: error:04091068:rsa routines:INT_RSA_VERIFY:bad signature</p> <p>2021-01-01T12:00:00+00:00 vsZ-H radiusd[20866]: [Tue Sep 29 2020 14:46:29:999][vsZ-H][RADIUS][ERR][TID=2114295552][src/main/tls.c:2333]#012Extension Key usage(OCSP SIGNING) is not present, Terminating TLS connect</p> <p>2021-01-01T12:00:00+00:00[vsZ-H][RADIUS][ERR][TID=447129344][src/main/tls.c:300]#012tls: Failed in __FUNCTION__ (SSL_connect): error:14090086:SSL routines:SSL3_GET_SERVER_CERTIFICATE:certificate verify failed</p> <p><b>Add Cert to Trust Store</b> 2021-01-01T12:00:00+00:00 vszh Web Activity: "User:[admin],Browser IP:[172.16.16.253],Action:[Create],Resource:[Trusted CA Chain],Description:[Trusted CA Chain [RSA_ECDSA] created.]"</p> <p><b>Update Chain in Trust store</b> 2021-01-01T12:00:00+00:00 vszh Web Activity: "User:[admin],Browser IP:[172.16.16.253],Action:[Update],Resource:[Trusted CA Chain],Description:[Trusted CA Chain [RSA-New] updated.]"</p> <p><b>Delete Cert from Trust Store</b> 2021-01-01T12:00:00+00:00 vszh Web Activity: "User:[admin],Browser IP:[172.16.16.153],Action:[Delete],Resource:[Trusted CA Chain],Description:[Trusted CA Chain [ECDSA] deleted.]"</p>
<p><b>IPSec</b></p>	<p>See Failure to establish an IPSec SA</p>
<p><b>Radsec</b></p>	<p>N/A</p>
<p><b>Updates to TrustStore</b></p>	<p>N/A</p>

<p><b>Auditable Events</b></p>	<p>Any attempt to initiate a manual update.</p>
<p><b>Additional Content</b></p>	<p>None</p>
<p><b>SZ144 (Physical)</b></p>	<p>2021-01-01T12:00:00+00:00 SZ144 Configurer: c.r.w.c.o.ClusterUpgradeOperationService - &lt;OPT&gt; [Upgrade] generate upgrade history:UpgradeHistory [key=null, startTime=1584992373902, creatorUUID=null, cbVersion=5.1.1.3.1033, dpVersion=5.1.1.3.1016, apFwVersion=5.1.1.3.1126, oldCbVersion=5.1.1.3.1032, oldDpVersion=5.1.1.3.1016, oldApFwVersion=5.1.1.3.1126, fileName=5.1.1.3.1243-fips.ximg, elapsedSeconds=null]</p>
<p><b>vsZ-H (Virtual)</b></p>	<p>2021-01-01T12:00:00+00:00 vszh Configurer: c.r.w.c.o.ClusterUpgradeOperationService - &lt;OPT&gt; [Upgrade] generate upgrade history:UpgradeHistory [key=null, startTime=1580130324305, creatorUUID=null, cbVersion=5.1.1.3.1032, dpVersion=, apFwVersion=5.1.1.3.1124, oldCbVersion=5.1.1.3.1026, oldDpVersion=0.0.0.0, oldApFwVersion=5.1.1.3.1115, fileName=vscg-5.1.1.3.1166-fips.ximg, elapsedSeconds=null]</p>
<p><b>vsZ-D</b></p>	<p>2021-01-01T12:00:00+00:00 vszh Configurer: c.r.w.c.o.ClusterUploadVdpOperationService - &lt;OPT&gt; [UploadVDPFirmware] =&gt; patch info : fileName=vdp-5.1.1.3.1245-fips.ximg, fileSize=260247492, versionInfo=version: {"platformType":"vdp","version":"5.1.1.3.1245"}, fileUploadPath=/opt/ruckuswireless/wsg/data/vDPfirmwareContent/</p>

## Audit Records

### Viewing the Audit Records

AP	2021-01-01T12:00:00+00:00 vszh Core: @99009.fwManualInitiation,"apMac"="94:BF:C4:22:75:00","reason"=" Manual FW:dpi-rule update initiated","fwVersion"="5.1.1.3.1124","model"="T710","zoneUUID"="8f13ef2d-71c9-4d3c-a860-4381b01822a8","zoneName"="TestZone","timeZone"="EST +5","apLocation"="", "apGps"="39.295438,-76.7","apIpAddress"="172.16.8.248","apIpv6Address"="", "apGroupUUID"="f0593dad-007d-4d5d-900c-843e963e2192","domainId"="8b2081d5-9662-40d9-a3db-2a3cf4dde3f7","serialNumber"="521803001443","domainName"="Administration Domain","idealEventVersion"="3.5.1","apDescription"=""
----	---

Auditable Events	All management activities of TSF data.
Additional Content	None
SZ144 (Physical)	<p><b>Ability to administer the TOE locally and remotely</b></p> <p>See All use of identification and authentication mechanism</p> <p><b>Configure the access banner</b></p> <p>2021-01-01T12:00:00+00:00 SZ144 Web Activity: "User:[admin],Browser IP:[172.16.16.153],Action:[Update],Resource:[Security Warning Message],Description:[Security warning message updated]"</p> <p><b>Configure the session inactivity time before session termination or locking and configure the authentication failure parameters for FIA_AFL.1</b></p> <p>2021-01-01T12:00:00+00:00 SZ144 Web Activity: "User:[admin],Browser IP:[172.16.16.153],Action:[Update],Resource:[Account Security Profile],Description:[Account Security Profile [Default] updated.]</p> <p><b>Ability to update the TOE, and to verify the updates using [digital signature] capability prior to installing those updates</b></p> <p>See Any attempt to initiate a manual update.</p> <p><b>Configure Audit Behavior</b></p> <p>2021-01-01T12:00:00+00:00 SZ144 Configurer: c.r.w.c.c.MainChannelPeerRemoteProxy - Apply new log config[{syslogPort=514, applog_syslog_facility=LOCAL0, applog_syslog_severity=Debug, redundancyMode=active_active, other_syslog_severity=Debug, syslogHost=172.16.16.254, applog_syslog_enable=true, audit_syslog_facility=LOCAL0, audit_syslog_severity=Debug, syslogSecondaryHost=, event_syslog_facility=LOCAL0, event_syslog_enable=true, syslogSecondaryPort=514}]</p> <p><b>Configure IPsec (lifetimes and reference identifier)</b>2021-01-01T12:00:00+00:00 SZ144 Web Activity: "User:[admin],Browser IP:[172.16.16.153],Action:[Update],Resource:[System IPsec],Description:[System IPsec [SystemIPsec] updated.]"</p> <p><b>Ability to configure the interaction between TOE components</b> See Enabling communications between a pair of components. Disabling communications between a pair of components</p> <p><b>Ability to set the time which is used for time-stamps</b></p> <p>See Discontinuous changes to time - either Administrator actuated or changed via an automated process</p> <p><b>Configure RadSec (reference identifier)</b> 2021-01-01T12:00:00+00:00 SZ144 Web Activity: "User:[admin],Browser IP:[172.16.16.153],Action:[Update],Resource:[Authentication Service],Description:[Authentication service [Radsec] updated.]"</p> <p><b>Resetting Passwords</b> 2021-01-01T12:00:00+00:00 SZ144 Web Activity: "User:[admin],Browser IP:[172.16.16.253],Action:[Update],Resource:[Administrator],Description:[Administrator [admin] password changed.]"</p> <p><b>Importing/Creation of Keys</b></p> <p>2021-01-01T12:00:00+00:00 SZ144 Web Activity: "User:[admin],Browser IP:[172.16.16.253],Action:[Create],Resource:[Client Cert],Description:[Client Cert [IPsec-ECDSA] created.]"</p> <p><b>Deletion of Keys</b></p> <p>2021-01-01T12:00:00+00:00 SZ144 Web Activity: "User:[admin],Browser IP:[172.16.16.153],Action:[Delete],Resource:[Client Cert],Description:[Client Cert [Client] deleted.]"</p>

<p>vsZ-H (Virtual)</p>	<p><b>Ability to administer the TOE locally and remotely</b></p> <p>See All use of identification and authentication mechanism</p> <p><b>Configure the access banner</b></p> <p>2021-01-01T12:00:00+00:00 vszh Web Activity: "User:[admin],Browser IP:[172.16.16.153],Action:[Update],Resource:[Security Warning Message],Description:[Security warning message updated]"</p> <p><b>Configure the session inactivity time before session termination or locking and configure the authentication failure parameters for FIA_AFL.1</b></p> <p>2021-01-01T12:00:00+00:00 vszh Web Activity: "User:[admin],Browser IP:[172.16.16.153],Action:[Update],Resource:[Account Security Profile],Description:[Account Security Profile [Default] updated.]"</p> <p><b>Ability to update the TOE, and to verify the updates using [digital signature] capability prior to installing those updates</b></p> <p>See Any attempt to initiate a manual update</p> <p><b>Configure Audit Behavior</b></p> <p>2021-01-01T12:00:00+00:00 vszh Configurer: c.r.w.c.c.MainChannelPeerRemoteProxy - Apply new log config[{syslogPort=514, applog_syslog_facility=LOCAL0, applog_syslog_severity=Debug, redundancyMode=active_active, other_syslog_severity=Debug, syslogHost=172.16.8.254, applog_syslog_enable=true, audit_syslog_facility=LOCAL0, audit_syslog_severity=Debug, syslogSecondaryHost=, event_syslog_facility=LOCAL0, event_syslog_enable=true, syslogSecondaryPort=514}]</p> <p><b>Configure IPsec (lifetimes and reference identifier)</b> 2021-01-01T12:00:00+00:00 vszh Web Activity: "User:[admin],Browser IP:[172.16.16.153],Action:[Update],Resource:[System IPsec],Description:[System IPsec [SystemIPsec] updated.]"</p> <p><b>Ability to configure the interaction between TOE components</b> See Enabling communications between a pair of components. Disabling communications between a pair of components.</p> <p><b>Ability to set the time which is used for time-stamps</b> See Discontinuous changes to time - either Administrator actuated or changed via an automated process.</p> <p><b>Configure RadSec (reference identifier)</b> 2021-01-01T12:00:00+00:00 vszh Web Activity: "User:[admin],Browser IP:[172.16.16.253],Action:[Update],Resource:[Authentication Service],Description:[Authentication service [Radsec] updated.]"</p> <p><b>Resetting Passwords</b> 2021-01-01T12:00:00+00:00 vszh Web Activity: "User:[admin],Browser IP:[172.16.16.253],Action:[Update],Resource:[Administrator],Description:[Administrator [admin] password changed.]"</p> <p><b>Importing/Creation of Keys</b></p> <p>2021-01-01T12:00:00+00:00 vszh Web Activity: "User:[admin],Browser IP:[172.16.16.253],Action:[Create],Resource:[Client Cert],Description:[Client Cert [Client-RSA] created.]"</p> <p><b>Deletion of Keys</b></p> <p>2021-01-01T12:00:00+00:00 vszh Web Activity: "User:[admin],Browser IP:[172.16.16.153],Action:[Delete],Resource:[Client Cert],Description:[Client Cert [ECDSA_Client] deleted.]"</p>
<p>vsZ-D</p>	<p>N/A</p>
<p>AP</p>	<p>N/A</p>

<p><b>Auditable Events</b></p>	<p>Failure of the TSF.</p>
<p><b>Additional Content</b></p>	<p>Indication that the TSF has failed with the type of failure that occurred.</p>
<p><b>SZ144 (Physical)</b></p>	<p>The logging service is not initiated in a fail state. An error will be presented at the detection of the fail state.</p>
<p><b>vsZ-H (Virtual)</b></p>	<p>The logging service is not initiated in a fail state. An error will be presented at the detection of the fail state.</p>
<p><b>vsZ-D</b></p>	<p>The logging service is not initiated in a fail state. An error will be presented at the detection of the fail state.</p>
<p><b>AP</b></p>	<p>The logging service is not initiated in a fail state. An error will be presented at the detection of the fail state.</p>

<p><b>Auditable Events</b></p>	<p>Initiation of the trusted channel. Termination of the trusted channel. Failure of the trusted channel functions. (Internal Communication)</p>
<p><b>Additional Content</b></p>	<p>Identification of the initiator and target of failed trusted channels establishment attempt.</p>

## Audit Records

### Viewing the Audit Records

<b>SZ144 (Physical)</b>	<p><b>IPsec</b> See Protocol failures. Establishment/Termination of anIPSec SA. Negotiation "down" from an IKEv2 to IKEv1 exchange.</p> <p><b>SSH Failure</b> See Failure to establish an SSH server session</p> <p><b>Establishment</b> 2021-01-01T12:00:00+00:00 SZ144 sshd[27340]: Accepted publickey for sstunnel from 172.16.16.249 port 37194 ssh2: RSA SHA256:Rf7WBKnCLNVor1D4R5paZQQTWInl7cwoQheehcoGRMY</p> <p><b>Termination</b> 2021-01-01T12:00:00+00:00 SZ144 sshd[27340]: pam_unix(sshd:session): session closed for user sstunnel</p>
<b>vsZ-H (Virtual)</b>	<p><b>SSH Failure</b> See Failure to establish an SSH server session</p> <p><b>Establishment</b> 2021-01-01T12:00:00+00:00 vszh sshd[30619]: Accepted publickey for sstunnel from 172.16.8.248 port 50644 ssh2: RSA SHA256:ioKMgn7kIMOybsZQWANI43f04L1KHio/Zalq82nOqRM</p> <p><b>Termination</b> 2021-01-01T12:00:00+00:00 vszh sshd[30619]: pam_unix(sshd:session): session closed for user sstunnel</p>
<b>vsZ-D</b>	<p><b>IPsec</b> See Protocol failures. Establishment/Termination of anIPSec SA. Negotiation "down" from an IKEv2 to IKEv1 exchange.</p> <p><b>SSH Failure</b> See Failure to establish an SSH server session</p> <p><b>Establishment</b> 2021-01-01T12:00:00+00:00 vszh Core: @ @512,dpConnected,"dpKey"="97HM3WVA5234U0JPM34HJEU1XTA000C29B4693A000C29B46944","timestamp"="1585498710059","cpName"="vszh","wsgIP"="172.16.8.230"</p> <p><b>Termination</b> 2021-01-01T12:00:00+00:00 vszh Core: @ @513,dpDisconnected,"dpKey"="97HM3WVA5234U0JPM34HJEU1XTA000C29B4693A000C29B46944","timestamp"="1585001239636","cpName"="vszh","wsgIP"="172.16.8.230","reason"="1, NMI problem."</p>
<b>AP</b>	<p><b>IPsec</b> See Protocol failures. Establishment/Termination of anIPSec SA. Negotiation "down" from an IKEv2 to IKEv1 exchange.</p> <p><b>SSH Failure</b> See Failure to establish an SSH server session</p> <p><b>Establishment</b> 2021-01-01T12:00:00+00:00 vszh Core: @ @99018,sshInitiation, "apMac"="94:BF:C4:22:75:00", "reason"="SSH Login successful with IP 172.16.8.254 username admin","fwVersion"="5.1.1.3.1125","model"="T710","zoneUUID"="7079e8e4-ac46-4086-803b-6b4bc3a46de2","zoneName"="TestZone","timeZone"="EST+5EDT,M3.2.0/02:00,M11.1.0/02:00","apLocation"="", "apGps"="39.295072,-76.7","apIpAddress"="172.16.8.248","apIpv6Address"="2001::172:16:8:248","apGroupUUID"="35f4aa9e-6b5c-4a05-8035-bdc2ac8674ea","domainId"="8b2081d5-9662-40d9-a3db-2a3cf4dde3f7","serialNumber"="521803001443","domainName"="Administration Domain","idealEventVersion"="3.5.1","apDescription"=""</p> <p><b>Termination</b> 2021-01-01T12:00:00+00:00 vszh Core: @ @99019,sshTermination, "apMac"="", "reason"="SSH session exited","fwVersion"="5.1.1.3.1128","model"="T710","zoneUUID"="7079e8e4-ac46-4086-803b-6b4bc3a46de2","zoneName"="TestZone","timeZone"="EST+5EDT,M3.2.0/02:00,M11.1.0/02:00","apLocation"="", "apGps"="39.295598,-76.7","apIpAddress"="172.16.8.248","apIpv6Address"="fc00::1","apGroupUUID"="35f4aa9e-6b5c-4a05-8035-bdc2ac8674ea","domainId"="8b2081d5-9662-40d9-a3db-2a3cf4dde3f7","serialNumber"="521803001443","domainName"="Administration Domain","idealEventVersion"="3.5.1","apDescription"=""</p>

<b>Auditable Events</b>	Discontinuous changes to time - either Administrator actuated or changed via an automated process. (Note that no continuous changes to time need to be logged. See also application note on FPT_STM_EXT.1).
<b>Additional Content</b>	For discontinuous changes to time: The old and new values for the time. Origin of the attempt to change time for success and failure (e.g., IP address).
<b>SZ144 (Physical)</b>	2021-01-01T12:00:00+00:00 SZ144 Core: @ @99301,disContTimeChange, "before"="Mon Feb 17 16:00:19 2020", "after"="Mon Feb 17 19:07:35 2020", "server"="172.16.16.254", "local_ip"="172.16.16.244"
<b>vsZ-H (Virtual)</b>	2021-01-01T12:00:00+00:00 vszh Core: @ @99301,disContTimeChange, "before"="Fri Feb 21 16:57:58 2020", "after"="Fri Feb 21 22:57:42 2020", "server"="172.16.16.254", "local_ip"="172.16.16.230"
<b>vsZ-D</b>	2021-01-01T12:00:00+00:00 vszh Core: @ @99211,dpDiscontinuousTimeChangeNTPServerdpNtpTimeSync,"dpKey"="97HM3WVA5234U0JPM34HJEU1XTA000C29B4693A000C29B46944","before"="02/21/2020-04:59:01 PM","after"="02/21/2020-10:58:45 PM","source"="10.254.1.1"

AP	2021-01-01T12:00:00+00:00 vszh Core: @@99014,disContiChan,"apMac"="94:BF:C4:22:75:00","reason"="Discontinuous change of time through NTP server from SZ.The time got from SCG: Wed Mar 4 15:32:20 2020 , the Current time in AP: Wed Mar 4 15:30:42 2020","fwVersion"="5.1.1.3.1124","model"="T710","zoneUUID"="8f13ef2d-71c9-4d3c-a860-4381b01822a8","zoneName"="TestZone","timeZone"="EST +5","apLocation"="", "apGps"="39.295438,-76.7", "apIpAddress"="172.16.8.248", "apIpv6Address"="", "apGroupUUID"="f0593dad-007d-4d5d-900c-843e963e2192", "domainId"="8b2081d5-9662-40d9-a3db-2a3cf4dde3f7", "serialNumber"="521803001443", "domainName"="Administration Domain", "idealEventVersion"="3.5.1", "apDescription"=""
----	---

<b>Auditable Events</b>	Execution of this set of TSF self-tests. Detected integrity violations.
<b>Additional Content</b>	For integrity violations, the TSF code file that caused the integrity violation.
<b>SZ144 (Physical)</b>	The logging service is not initiated in a fail state. An error will be presented at the detection of the fail state.
<b>vsZ-H (Virtual)</b>	The logging service is not initiated in a fail state. An error will be presented at the detection of the fail state.
<b>vsZ-D</b>	The logging service is not initiated in a fail state. An error will be presented at the detection of the fail state.
<b>AP</b>	The logging service is not initiated in a fail state. An error will be presented at the detection of the fail state.

<b>Auditable Events</b>	Initiation of update; result of the update attempt (success or failure).
<b>Additional Content</b>	None
<b>SZ144 (Physical)</b>	<b>Initiation</b> See Any attempt to initiate a manual update  <b>Update Result</b> 2021-01-01T12:00:00+00:00 SZ144 Core: c.r.w.s.c.MainChannelDirectiveListener - received Admin_UpgradeHistory_Update! history: {"dpVersion":"5.1.1.3.1016", "apFwVersion":"5.1.1.3.1126", "fileName": "5.1.1.3.1243-fips.ximg", "oldDpVersion":"5.1.1.3.1016", "oldApFwVersion":"5.1.1.3.1126", "startTime": "1584992373902", "oldVersion":"5.1.1.3.1234", "version":"5.1.1.3.1243", "elapsedSeconds": "2121", "cbVersion":"5.1.1.3.1033", "oldCbVersion":"5.1.1.3.1032"}
<b>vsZ-H (Virtual)</b>	<b>Initiation</b> See Any attempt to initiate a manual update  <b>Update Result</b> 2021-01-01T12:00:00+00:00 vszh Core: c.r.w.s.c.MainChannelDirectiveListener - received Admin_UpgradeHistory_Update! history: {"dpVersion":""," apFwVersion":"5.1.1.3.1124", "fileName": "vscg-5.1.1.3.1166-fips.ximg", "oldDpVersion":"0.0.0.0", "oldApFwVersion":"5.1.1.3.1115", "startTime": "1580130324305", "oldVersion":"5.1.1.3.1120", "version":"5.1.1.3.1166", "elapsedSeconds": "1696", "cbVersion":"5.1.1.3.1032", "oldCbVersion":"5.1.1.3.1026"}
<b>vsZ-D</b>	<b>Initiation</b> See Any attempt to initiate a manual update  <b>Update Result</b> 2021-01-01T12:00:00+00:00 vszh Configurer: c.r.w.c.o.ClusterUploadVdpOperationService - <OPT> [UploadVDPFirmware] => patch info : fileName=vdp-5.1.1.3.1245-fips.ximg, fileSize=260247492, versionInfo=version: {"platformType":"vdp", "version":"5.1.1.3.1245"}, fileUploadPath=/opt/ruckuswireless/wsg/data/vDPfirmwareContent/
<b>AP</b>	<b>Initiation</b> See Any attempt to initiate a manual update  <b>Update Result</b> 2021-01-01T12:00:00+00:00 SZ144 Core: @@99013,fwInitiationUpdate,"apMac"="C8:08:73:30:F2:90","reason"=" FW: dpi-rule update, ret=1, Successful update", "fwVersion"="5.1.1.3.1126", "model"="R610", "zoneUUID"="f77a8816-3049-40cd-8484-82919275ddc3", "zoneName"="Default Zone", "timeZone"="EST +5EDT,M3.2.0/02:00,M11.1.0/02:00", "apLocation"="", "apGps"="", "apIpAddress"="172.16.16.245", "apIpv6Address"="fc00::1", "apGroupUUID"="18e2a1fc-fdee-475d-950d-6eda1f6f5ab7", "domainId"="8b2081d5-9662-40d9-a3db-2a3cf4dde3f7", "serialNumber"="501849000776", "domainName"="Administration Domain", "idealEventVersion"="3.5.1", "apDescription"=""

<b>Auditable Events</b>	The termination of a remote session by the session locking mechanism.
<b>Additional Content</b>	None
<b>SZ144 (Physical)</b>	<b>Web UI</b> 2021-01-01T12:00:00+00:00 SZ144 Web Activity: "User:[admin],Browser IP:[172.16.16.153],Action:[Log off],Resource:[Administrator],Description:[Administrator [admin] session timeout to logged off from [172.16.16.153].]  <b>SSH</b> 2021-01-01T12:00:00+00:00 SZ144 sshd[21178]: pam_unix(sshd:session): session closed for user admin

## Audit Records

### Viewing the Audit Records

<b>vSZ-H (Virtual)</b>	<b>Web UI</b> 2021-01-01T12:00:00+00:00 vszh Web Activity: "User:[admin],Browser IP:[172.16.16.253],Action:[Log off],Resource:[Administrator],Description:[Administrator [admin] session timeout to logged off from [172.16.16.253].]" <b>SSH</b> 2021-01-01T12:00:00+00:00 SZ144 sshd[21178]: pam_unix(sshd:session): session closed for user admin
<b>vSZ-D</b>	N/A
<b>AP</b>	N/A

<b>Auditable Events</b>	The termination of an interactive session.
<b>Additional Content</b>	None
<b>SZ144 (Physical)</b>	<b>Web UI</b> 2021-01-01T12:00:00+00:00 SZ144 Web Activity: "User:[admin],Browser IP:[172.16.16.253],Action:[Log off],Resource:[Administrator],Description:[Administrator [admin] logged off from [172.16.16.253].]" <b>SSH</b> 2021-01-01T12:00:00+00:00 SZ144 Web Activity: "User:[admin],Browser IP:[172.16.16.253],Action:[Log off],Resource:[Administrator],Description:[Administrator [admin] logged off from CLI.]" <b>CLI</b> 2021-01-01T12:00:00+00:00 SZ144 Web Activity: "User:[admin],Browser IP:[127.0.0.1],Action:[Log off],Resource:[Administrator],Description:[Administrator [admin] logged off from CLI.]"
<b>vSZ-H (Virtual)</b>	<b>Web UI</b> 2021-01-01T12:00:00+00:00 vszh Web Activity: "User:[admin],Browser IP:[172.16.16.153],Action:[Log off],Resource:[Administrator],Description:[Administrator [admin] session timeout to logged off from [172.16.16.153].]" <b>SSH</b> 2021-01-01T12:00:00+00:00 vszh Web Activity: "User:[admin],Browser IP:[172.16.16.253],Action:[Log off],Resource:[Administrator],Description:[Administrator [admin] session timeout to logged off from CLI.]" <b>CLI</b> 2021-01-01T12:00:00+00:00 vszh Web Activity: "User:[admin],Browser IP:[127.0.0.1],Action:[Log off],Resource:[Administrator],Description:[Administrator [admin] logged off from CLI.]"
<b>vSZ-D</b>	N/A
<b>AP</b>	N/A

<b>Auditable Events</b>	The termination of a local session by the session locking mechanism.
<b>Additional Content</b>	None
<b>SZ144 (Physical)</b>	2021-01-01T12:00:00+00:00 SZ144 Web Activity: "User:[admin],Browser IP:[127.0.0.1],Action:[Log off],Resource:[Administrator],Description:[Administrator [admin] logged off from CLI.]"
<b>vSZ-H (Virtual)</b>	2021-01-01T12:00:00+00:00 vszh Web Activity: "User:[admin],Browser IP:[172.16.16.153],Action:[Log off],Resource:[Administrator],Description:[Administrator [admin] logged off from CLI.]"
<b>vSZ-D</b>	N/A
<b>AP</b>	N/A

<b>Auditable Events</b>	Denial of a session establishment due to the session establishment mechanism.
<b>Additional Content</b>	Reason for denial, origin of establishment attempt
<b>SZ144 (Physical)</b>	N/A
<b>vSZ-H (Virtual)</b>	N/A
<b>vSZ-D</b>	N/A
<b>AP</b>	The TOE uses a time scheduler to enable and disable the SSID. Thus the SSID is unable to be connected to and no failure log is generated as no connection attempt is made. The following log is the result of the time scheduler disabling the SSID:  2021-01-01T12:00:00+00:00 SZ300 Eventreader: @@322,apWLANStateChanged,"apMac"="18:7C:0B:10:10:80","ssid"="SZ300WLAN","state"="disabled","radio"="11ac","apTime"="Wed Apr 22 11:22:03 2020","reason"="Service schedule","fwVersion"="5.1.1.3.1128","model"="R720","zoneUUID"="64620dea-4fa6-4121-9e2e-6f0717279a79","zoneName"="Test Zone","timeZone"="EST +5EDT,M3.2.0/02:00,M11.1.0/02:00","apLocation"="", "apGps"="", "apIpAddress"="172.16.8.249", "apIpv6Address"="", "apGroupUUID"="2beb1a92-4009-47d8-a25c-0f2665ac4f47", "domainId"="8b2081d5-9662-40d9-a3db-2a3cf4dde3f7", "serialNumber"="491803002384", "domainName"="Administration Domain", "idealEventVersion"="3.5.1", "apDescription"="

<b>Auditable Events</b>	Initiation of the trusted channel. Termination of the trusted channel. Failure of the trusted channel functions. (External Communication)
<b>Additional Content</b>	Identification of the initiator and target of failed trusted channels establishment attempt.
<b>SZ144 (Physical)</b>	<b>IPSec</b> See Protocol failures. Establishment/Termination of anIPSec SA. Negotiation "down" from an IKEv2 to IKEv1 exchange.
<b>vSZ-H (Virtual)</b>	<b>IPSec</b> See Protocol failures. Establishment/Termination of anIPSec SA. Negotiation "down" from an IKEv2 to IKEv1 exchange.
<b>vSZ-D</b>	N/A
<b>AP</b>	N/A

<b>Auditable Events</b>	Failed attempts to establish a trusted channel (including IEEE 802.11). Detection of modification of channel data.
<b>Additional Content</b>	Identification of the initiator and target of channel.
<b>SZ144 (Physical)</b>	<b>IPSec</b> See Protocol failures. Establishment/Termination of anIPSec SA. Negotiation "down" from an IKEv2 to IKEv1 exchange <b>RadSec</b> See Failure to establish TLS Connection (Radsec)
<b>vSZ-H (Virtual)</b>	<b>IPSec</b> See Protocol failures. Establishment/Termination of anIPSec SA. Negotiation "down" from an IKEv2 to IKEv1 exchange <b>RadSec</b> See Failure to establish TLS Connection (Radsec)
<b>vSZ-D</b>	<b>IPSec</b> See Protocol failures. Establishment/Termination of anIPSec SA. Negotiation "down" from an IKEv2 to IKEv1 exchange
<b>AP</b>	<b>IEEE 802.11-2012 (WPA2) / IEEE 802.1X</b> 2021-01-01T12:00:00+00:00 vszh Core: @ @203,clientJoinFailure,"apMac"="94:bf:c4:22:75:00","clientMac"="70:18:8b:02:f2:f3","ssid"="VSZHWLAN","bssid"="94:bf:c4:22:75:08","userId"="", "wlanId"="1", "iface"="wlan0", "tenantUUID"="839f87c6-d116-497e-afce-aa8157abd30c", "apName"="T710", "apGps"="39.295655,-76.753728", "userName"="", "vlanId"="1", "radio"="b/g/n", "encryption"="WPA2-AES", "fwVersion"="5.1.1.3.1125", "model"="T710", "zoneUUID"="7079e8e4-ac46-4086-803b-6b4bc3a46de2", "zoneName"="TestZone", "timeZone"="UTC+0", "apLocation"="", "apGps"="39.295655,-76.7", "apIpAddress"="172.16.8.248", "apIpv6Address"="2001::172:16:8:248", "apGroupUUID"="35f4aa9e-6b5c-4a05-8035-bdc2ac8674ea", "domainId"="8b2081d5-9662-40d9-a3db-2a3cf4dde3f7", "serialNumber"="521803001443", "domainName"="Administration Domain", "wlanGroupUUID"="4a0d08e0-5e34-11ea-8d1d-fa23a50db6e8", "idealEventVersion"="3.5.1", "apDescription"=""

<b>Auditable Events</b>	Initiation of the trusted path. Termination of the trusted path. Failure of the trusted path functions.
<b>Additional Content</b>	None
<b>SZ144 (Physical)</b>	<b>Initiation</b> See All use of identification and authentication mechanism <b>Termination</b> See The termination of an interactive session. <b>Failure Web UI</b> See Failure to establish a HTTPS Session and Failure to establish a TLS Session (HTTPS) <b>SSH</b> See Failure to establish an SSH server session
<b>vSZ-H (Virtual)</b>	<b>Initiation</b> See All use of identification and authentication mechanism <b>Termination</b> See The termination of an interactive session. <b>Failure Web UI</b> See Failure to establish a HTTPS Session and Failure to establish a TLS Session (HTTPS) <b>SSH</b> See Failure to establish an SSH server session
<b>vSZ-D</b>	N/A
<b>AP</b>	N/A

<b>Auditable Events</b>	Action taken due to potential security violations.
<b>Additional Content</b>	None
<b>SZ144 (Physical)</b>	N/A
<b>vSZ-H (Virtual)</b>	N/A
<b>vSZ-D</b>	N/A



## Audit Records

### Viewing the Audit Records

AP	See Detection of rogue AP or EUD
<b>Auditable Events</b>	Presence of allowedlisted device.
<b>Additional Content</b>	Type of device (AP or EUD), MAC Address
<b>SZ144 (Physical)</b>	2021-01-01T12:00:00+00:00 SZ144 Core c.r.s.d.r.r.PolicyMatcherImpl - DetectedInfos : WIDS-[ rogueMac:18:7C:0B:10:10:88; rogueTypeInfo: 0 (Rogue Device); encrypt_type: WPA2-PSK; auth_type: Open; beacon_intval: 100; rx_packet_count: 0; sta_count: 0; allowListed: Yes; mesh_formed: no; mesh_root_mac: ; eud_ap_mac: ; sbd_matched_rule_name: ; sbd_scope_type: 0; eud_ssid: ; rf_band: 2.4G;
<b>vsZ-H (Virtual)</b>	2021-01-01T12:00:00+00:00 SZ144 Core c.r.s.d.r.r.PolicyMatcherImpl - DetectedInfos : WIDS-[ rogueMac:18:7C:0B:10:10:88; rogueTypeInfo: 0 (Rogue Device); encrypt_type: WPA2-PSK; auth_type: Open; beacon_intval: 100; rx_packet_count: 0; sta_count: 0; allowListed: Yes; mesh_formed: no; mesh_root_mac: ; eud_ap_mac: ; sbd_matched_rule_name: ; sbd_scope_type: 0; eud_ssid: ; rf_band: 2.4G;
<b>vsZ-D</b>	2021-01-01T12:00:00+00:00 SZ144 Core c.r.s.d.r.r.PolicyMatcherImpl - DetectedInfos : WIDS-[ rogueMac:18:7C:0B:10:10:88; rogueTypeInfo: 0 (Rogue Device); encrypt_type: WPA2-PSK; auth_type: Open; beacon_intval: 100; rx_packet_count: 0; sta_count: 0; allowListed: Yes; mesh_formed: no; mesh_root_mac: ; eud_ap_mac: ; sbd_matched_rule_name: ; sbd_scope_type: 0; eud_ssid: ; rf_band: 2.4G;
AP	N/A

<b>Auditable Events</b>	Location of AP or EUD.
<b>Additional Content</b>	MAC Address, device type, classification of device, sensor(s) that detected device, signal strength as received by detecting sensor(s), proximity to detecting sensor(s).
<b>SZ144 (Physical)</b>	<b>Client Location:</b> 2021-01-01T12:00:00+00:00 SZ144 WebActivity: "User:[admin],Browser IP:[172.16.16.253],Action:[Locate],Resource:[Rogue Client],Description:[Locate the Rogue Client[70:18:8B:02:F2:F3 (x:182.7924,y:243.63966)] classified as [Rogue] on Map[TestMap]. It is detected and located by the following monitoring APs: [R750@70:CA:97:2C:66:00 (x:210.01047,y:221.14757) RSSI:59; R850@34:20:E3:28:9E:20 (x:151.30484,y:269.65994) RSSI:51]" <b>AP Location:</b> 2021-01-01T12:00:00+00:00 SZ144 WebActivity: "User:[admin],Browser IP:[172.16.16.253],Action:[Locate],Resource:[Rogue AP],Description:[Locate the Rogue AP[18:7C:0B:10:10:88 (x:183.57053,y:242.99666)] classified as [Rogue] on Map[TestMap]. It is detected and located by the following monitoring APs: [R750@70:CA:97:2C:66:00 (x:210.01047,y:221.14757) RSSI:72; R850@34:20:E3:28:9E:20 (x:151.30484,y:269.65994) RSSI:59]"
<b>vsZ-H (Virtual)</b>	<b>Client Location:</b> 2021-01-01T12:00:00+00:00 SZ144 WebActivity: "User:[admin],Browser IP:[172.16.16.253],Action:[Locate],Resource:[Rogue Client],Description:[Locate the Rogue Client[70:18:8B:02:F2:F3 (x:182.7924,y:243.63966)] classified as [Rogue] on Map[TestMap]. It is detected and located by the following monitoring APs: [R750@70:CA:97:2C:66:00 (x:210.01047,y:221.14757) RSSI:59; R850@34:20:E3:28:9E:20 (x:151.30484,y:269.65994) RSSI:51]" <b>AP Location:</b> 2021-01-01T12:00:00+00:00 SZ144 WebActivity: "User:[admin],Browser IP:[172.16.16.253],Action:[Locate],Resource:[Rogue AP],Description:[Locate the Rogue AP[18:7C:0B:10:10:88 (x:183.57053,y:242.99666)] classified as [Rogue] on Map[TestMap]. It is detected and located by the following monitoring APs: [R750@70:CA:97:2C:66:00 (x:210.01047,y:221.14757) RSSI:72; R850@34:20:E3:28:9E:20 (x:151.30484,y:269.65994) RSSI:59]"
<b>vsZ-D</b>	<b>Client Location:</b> 2021-01-01T12:00:00+00:00 SZ144 WebActivity: "User:[admin],Browser IP:[172.16.16.253],Action:[Locate],Resource:[Rogue Client],Description:[Locate the Rogue Client[70:18:8B:02:F2:F3 (x:182.7924,y:243.63966)] classified as [Rogue] on Map[TestMap]. It is detected and located by the following monitoring APs: [R750@70:CA:97:2C:66:00 (x:210.01047,y:221.14757) RSSI:59; R850@34:20:E3:28:9E:20 (x:151.30484,y:269.65994) RSSI:51]" <b>AP Location:</b> 2021-01-01T12:00:00+00:00 SZ144 WebActivity: "User:[admin],Browser IP:[172.16.16.253],Action:[Locate],Resource:[Rogue AP],Description:[Locate the Rogue AP[18:7C:0B:10:10:88 (x:183.57053,y:242.99666)] classified as [Rogue] on Map[TestMap]. It is detected and located by the following monitoring APs: [R750@70:CA:97:2C:66:00 (x:210.01047,y:221.14757) RSSI:72; R850@34:20:E3:28:9E:20 (x:151.30484,y:269.65994) RSSI:59]"
AP	N/A

<b>Auditable Events</b>	Detection of rogue AP or EUD.
<b>Additional Content</b>	None
<b>SZ144 (Physical)</b>	N/A
<b>vsZ-H (Virtual)</b>	N/A
<b>vsZ-D</b>	N/A



<b>AP</b>	2021-01-01T12:00:00+00:00 SZ144 Core: @@194,classifiedRogueClientDiscovered,"zoneUUID"="16643bf0-1632-40b1-9540-f8025dea3b79","apMac"="70:CA:97:2C:66:00","apName"="R750-CC","rogueMac"="E6:B1:9F:3A:39:7F","ssid"="Linux_Ad_Hoc","wlanId"="0","radio"="Unknown","channel"="6","timestamp"="1669832496000","rogueType"="Malicious","roguePolicyName"="WIDS_Policy","rogueRuleName"="Ad Hoc Rule","rogueDetectedInfos"="", "rssi"="62","rogueMatchedRuleDetectedMessage"="", "bssid"="2A:48:05:85:92:CD","rfband"="2.4G","serialNumber"="262072001548","timeZone"="", "apLocation"="", "zoneName"="Test_Zone_2"
-----------	--

<b>Auditable Events</b>	Detection of unauthorized SSID
<b>Additional Content</b>	None
<b>SZ144 (Physical)</b>	N/A
<b>vSZ-H (Virtual)</b>	N/A
<b>vSZ-D</b>	N/A
<b>AP</b>	2021-01-01T12:00:00+00:00 SZ144 Core: @@186,generalRogueAPDetected,"zoneUUID"="16643bf0-1632-40b1-9540-f8025dea3b79","apMac"="70:CA:97:2C:66:00","apName"="R750-CC","rogueMac"="18:7C:0B:10:10:8C","ssid"="Rogue_WLAN","wlanId"="2","radio"="802.11ac","channel"="149","timestamp"="1627932663000","rogueType"="Malicious","roguePolicyName"="WIDS_Policy","rogueRuleName"="Unauth_SSID","rogueDetectedInfos"="", "rssi"="73","rogueMatchedRuleDetectedMessage"="", "bssid"="", "rfband"="5G","serialNumber"="262072001548","timeZone"="", "apLocation"="", "zoneName"="Test_Zone_2"

<b>Auditable Events</b>	Sensor wireless transmission capabilities
<b>Additional Content</b>	Wireless transmission capabilities are turned on
<b>SZ144 (Physical)</b>	N/A
<b>vSZ-H (Virtual)</b>	N/A
<b>vSZ-D</b>	N/A
<b>AP</b>	Refer to Start-up and shut-down of audit functions as this demonstrates the AP booting up



© 2023 CommScope, Inc. All rights reserved.  
350 West Java Dr., Sunnyvale, CA 94089 USA  
<https://www.commscope.com>