

RUCKUS FIPS and Common Criteria Configuration Guide for SmartZone and APs, 5.1.1.3

Supporting SmartZone Release 5.1.1.3

Copyright, Trademark and Proprietary Rights Information

© 2020 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

ARRIS, the ARRIS logo, COMMSCOPE, RUCKUS, RUCKUS WIRELESS, the Ruckus logo, the Big Dog design, BEAMFLEX, CHANNELFLY, FASTIRON, ICX, SMARTCELL and UNLEASHED are trademarks of CommScope, Inc. and/or its affiliates. Wi-Fi Alliance, Wi-Fi, the Wi-Fi logo, Wi-Fi Certified, the Wi-Fi CERTIFIED logo, Wi-Fi Protected Access, the Wi-Fi Protected Setup logo, Wi-Fi Protected Setup, Wi-Fi Multimedia and WPA2 and WMM are trademarks or registered trademarks of Wi-Fi Alliance. All other trademarks are the property of their respective owners.

Contents

Preface.....	6
Document Conventions.....	6
Command Syntax Conventions.....	6
Document Feedback.....	7
RUCKUS Product Documentation Resources.....	7
Online Training Resources.....	7
Contacting RUCKUS Customer Services and Support.....	7
What's New in This Document.....	8
Federal Information Processing Standards.....	9
FIPS Mode Overview.....	9
Crypto Officer Roles and Responsibilities.....	10
Zeroization Process.....	10
Quarantine State.....	10
vSZ Installation with FIPS Image.....	11
System Requirements	11
vSZ Installation Prerequisites for FIPS.....	11
Creating and Registering the Virtual Machine.....	11
Hardware Configuration with FIPS Image	15
Controller Configuration with FIPS Image	16
Using FIPS-Related CLI Commands.....	16
Viewing and Downloading FIPS Logs.....	19
Uploading Certificates to SmartZone OS.....	21
Enabling Other Secured Communication Services.....	23
RadSec (RADIUS over TLS).....	25
Upgrading the Software.....	41
vSZ-D FIPS Installation with FIPS Image.....	49
System Requirements.....	49
vSZ-D FIPS Installation Prerequisites for FIPS.....	49
Creating and Registering the Virtual Machine (vSZ-D).....	50
Joining vSZ-D to the vSZ Controller.....	55
Using FIPS CLI Commands (vSZ-D).....	60
Downloading vSZ-D FIPS Logs.....	62
AP Configuration in FIPS Mode.....	63
AP Models that Support FIPS Mode.....	63
Joining AP to the (v)SZ Controller.....	64
Management Channel between AP/vSZ-D and Controller.....	65
FIPS AP Behavior.....	65
Crypto Officer Roles and Responsibilities for AP.....	66
Quarantine State for AP.....	66
AP Features Not Supported in FIPS Mode.....	67
X.509 Certificates.....	73
Generating Certificate Signing Request (CSR).....	73

Configuring X.509 Server Certificates on the Controller.....	74
Validating Certificates.....	78
Uploading X.509 Certificates on AP.....	80
Uploading X.509 Certificates on vSZ-D.....	82
Password Management.....	85
Configuring the WLAN Scheduler.....	87
Setting the WLAN Scheduler from the CLI.....	89
Terminating Sessions.....	91
Terminating Sessions for Non-Admin Users.....	92
Terminating Administrator Sessions.....	94
Locking Accounts.....	97
Locking Non-Administrator Accounts.....	97
Setting Up the Login Banner.....	100
Deployment Models.....	102
Configuring Ruckus GRE and IPsec in the WLAN.....	103
System IPsec.....	113
Configuring System IPsec using Preshared Key.....	115
Configuring System IPsec using Certificates.....	118
Configuring IKE and ESP Rekeying Separately.....	119
Configuring System Time.....	122
Administering the Controller.....	125
Administering the controller using console.....	125
Administering the controller remotely.....	127
Tamper-Evident Seals.....	129
General Information about Tamper-Evident Seals.....	129
Tamper-Evident Seals on SmartZone 100 Devices.....	129
Tamper-Evident Seals on SmartZone 300 Devices.....	133
Tamper-Evident Seals on T610 AP Devices.....	134
Tamper-Evident Seals on T710 AP Devices.....	135
Tamper-Evident Seals on R610 AP Devices.....	137
Tamper-Evident Seals on R710 AP Devices.....	138
Tamper-Evident Seals on R720 AP Devices.....	140
Trusted Channels Through TSF.....	141
Trusted Communication Channels.....	141
Enabling Trusted Channel Using IEEE 802.11-2012 (WPA2) Standards	142
Enabling Trusted Channel Using IEEE 802.1X and IPsec.....	142
FIPS-Compliant Products.....	142
AP Controller Matrix.....	142
FIPS-Compliant Product SKUs and Descriptions.....	143
Auditable Events in AP and DP for Common Criteria.....	144
Audit Records.....	146
Viewing the Events and Alarms.....	146
Downloading the Logs from the Controller.....	148

Viewing the Audit Records..... 148

Preface

Document Conventions

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

TABLE 1 Text Conventions

Convention	Description	Example
monospace	Identifies command syntax examples	device(config)# interface ethernet 1/1/6
bold	User interface (UI) components such as screen or page names, keyboard keys, software buttons, and field names	On the Start menu, click All Programs .
<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
bold text	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.

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.ruckuswireless.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://training.ruckuswireless.com>.

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.ruckuswireless.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.

What's New in This Document

- 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://forums.ruckuswireless.com/ruckuswireless/categories>
- Knowledge Base Articles—<https://support.ruckuswireless.com/answers>
- Software Downloads and Release Notes—https://support.ruckuswireless.com/#products_grid
- Security Bulletins—<https://support.ruckuswireless.com/security>

Using these resources will help you to resolve some issues, and will provide TAC with additional data from your troubleshooting analysis if you still require assistance through a support case or RMA. If you still require help, open and manage your case at https://support.ruckuswireless.com/case_management.

What's New in This Document

TABLE 2 Summary of Enhancements in Ruckus FIPS and Common Criteria Configuration Guide for SmartZone and AP 5.1.1.3

Feature	Description	Location
Administrating the Controller	Instructions on administrating the controller.	Refer to Administrating the Controller on page 125 for more information.
Upgrading the Software	Instructions on upgrading the software.	Refer to Upgrading the Software on page 41 for more information.
Configuring the IKE and ESP Rekeying Separately	Instructions on configuring the IKE and ESP Rekeying.	Refer to Configuring IKE and ESP Rekeying Separately on page 119 for more information.
Controller Configuration with FIPS Image	Information on controller configuration.	Refer to Controller Configuration with FIPS Image on page 16 for more details.
Joining AP to (v)SZ Controller	Instruction on joining AP to controller	Refer to Joining AP to the (v)SZ Controller on page 64 for more details.

TABLE 2 Summary of Enhancements in Ruckus FIPS and Common Criteria Configuration Guide for SmartZone and AP 5.1.1.3 (continued)

Feature	Description	Location
Management Channel Between Between AP/vSZ-D and SZ	Instructions on establishing communication between AP and controller.	Refer to Management Channel between AP/vSZ-D and Controller on page 65 for more details.
Generating Certificate Signing Request (CSR)	Instructions on generating CSR.	Refer to Generating Certificate Signing Request (CSR) on page 73
Hardware Configuration with FIPS Image	Instructions on installation of FIPS on hardware devices	Refer to Hardware Configuration with FIPS Image on page 15
Audit Records	Instructions on viewing/downloading audit logs. List of audit records.	Refer to Audit Records on page 146
Various edits	Minor editorial updates made throughout the Configuration Guide.	All chapters.

Federal Information Processing Standards

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 an agreed-upon security standard for government deployments via 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 met:

- 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.
- Tamper-evident security seals labels are applied to the device according to the instructions included in [Tamper-Evident Seals](#) on page 129. 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>.

Crypto Officer Roles and Responsibilities

The administrator (admin) is treated as a Crypto Officer (CO) and is the default user created during the SmartZone installation. The admin role is the only user role available on the vSZ-D and the access point (AP). Only 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 SmartZone, the vSZ-D and the AP only have a single admin login which is the CO role.

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 SZ controller, zeroization is achieved by changing the FIPS mode 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

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 hardware platform: (Intel(R) Xeon(R) CPU E5-2620 v4 @ 2.10GHz with AES-NI).

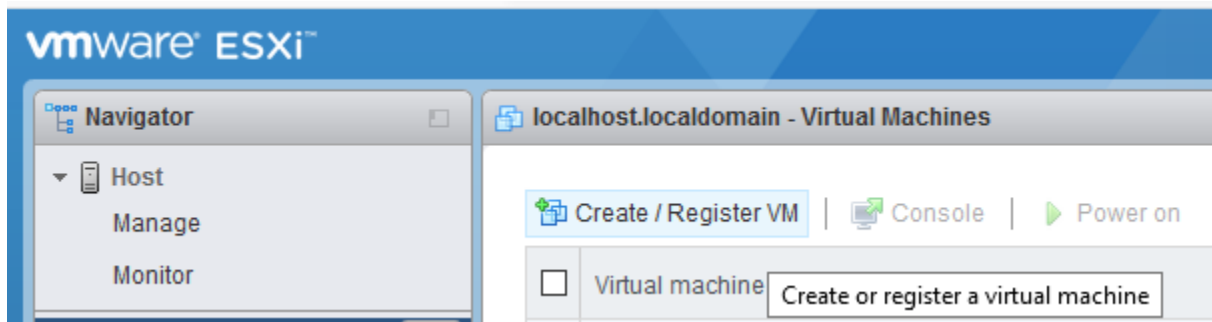
vSZ Installation Prerequisites for FIPS

To comply with FIPS, you must have a new installation of SmartZone 5.1.1.3 and a corresponding AP. The installation will not work on a system upgraded to SmartZone 5.1.1.3. The system validates the image before it is loaded.

Creating and Registering the Virtual Machine

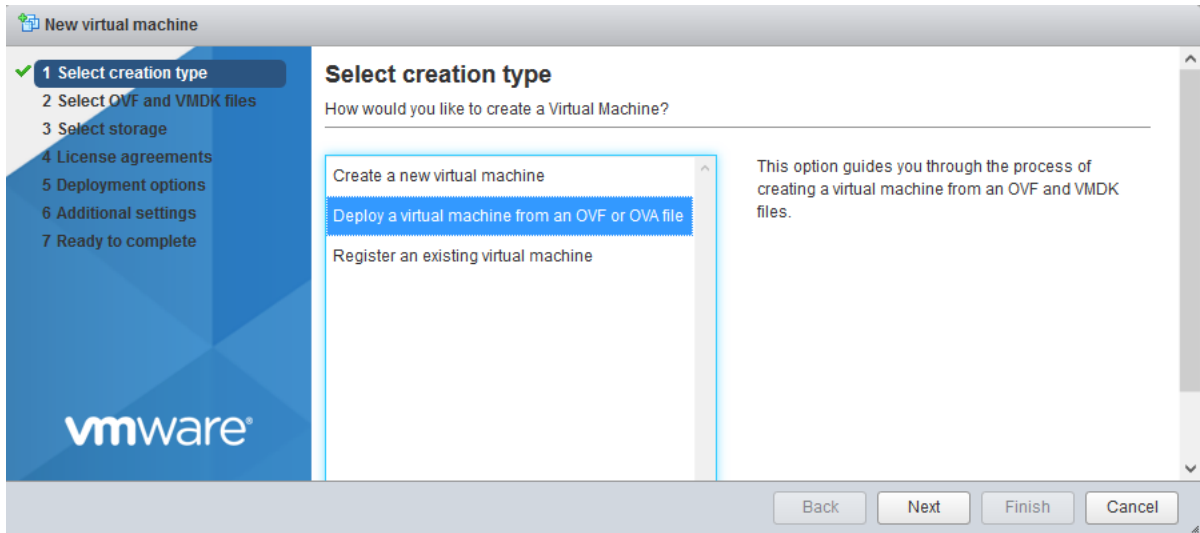
1. Install and deploy the .ova file on VMware ESXi using the **Create/Register VM** option, as shown in the following figure.

FIGURE 3 Create and register VM



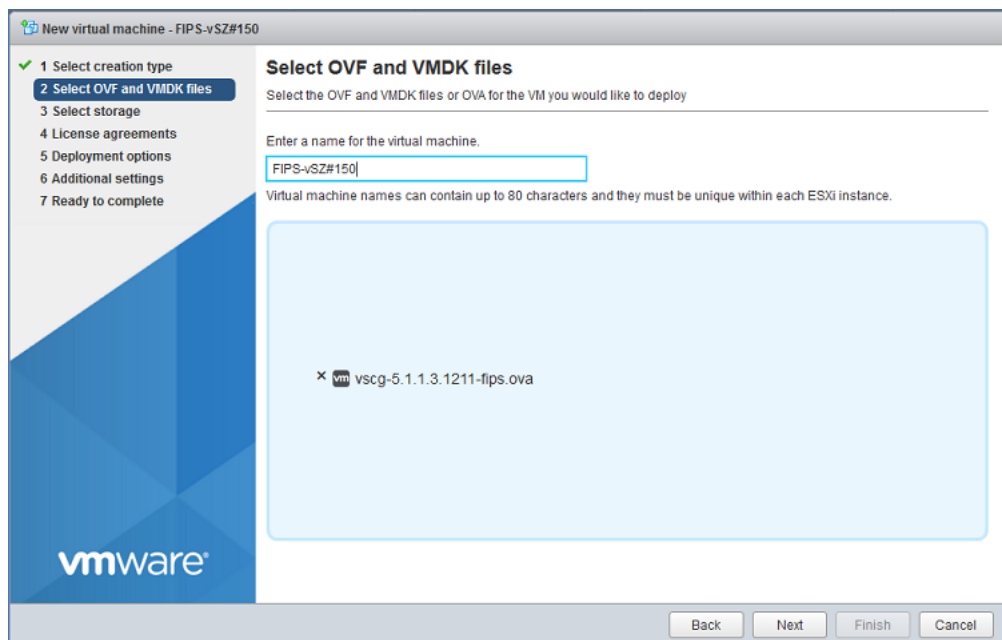
2. Select **Deploy a virtual machine from an OVF or OVA file**.

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

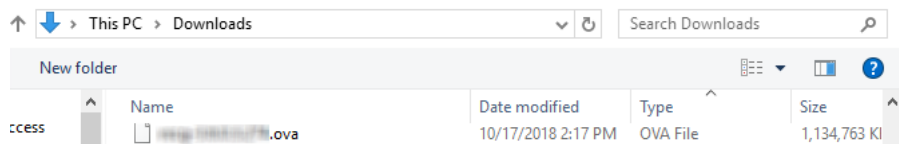
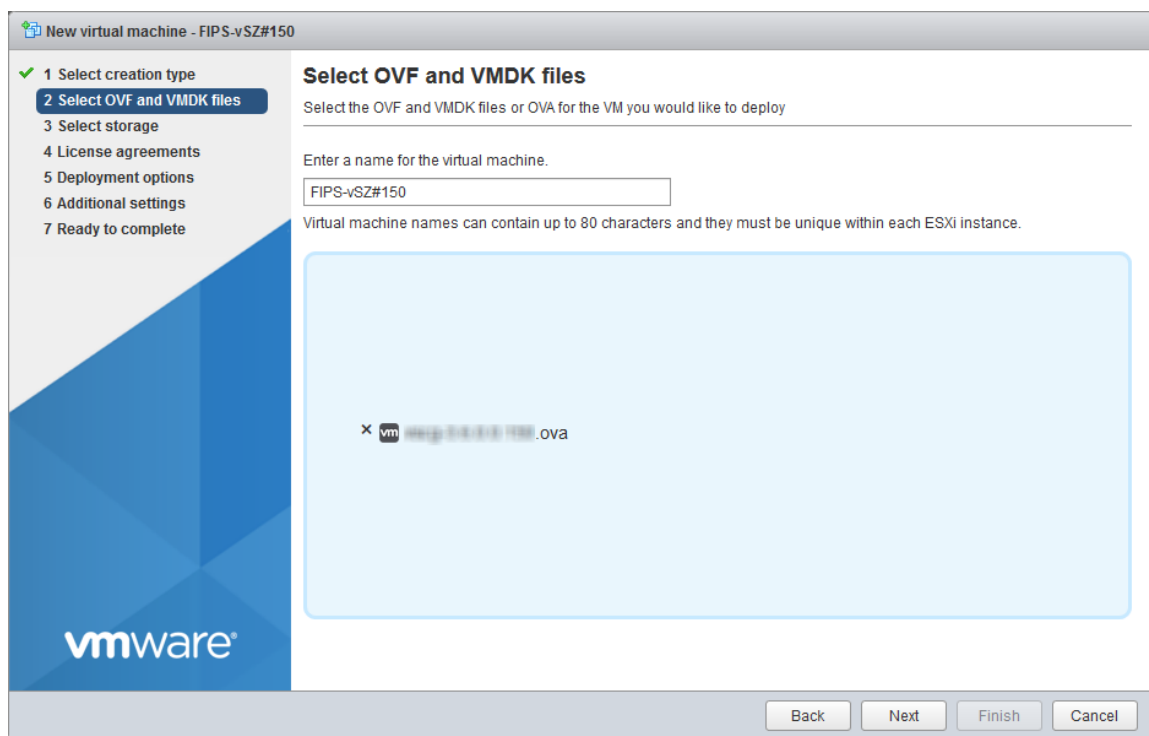


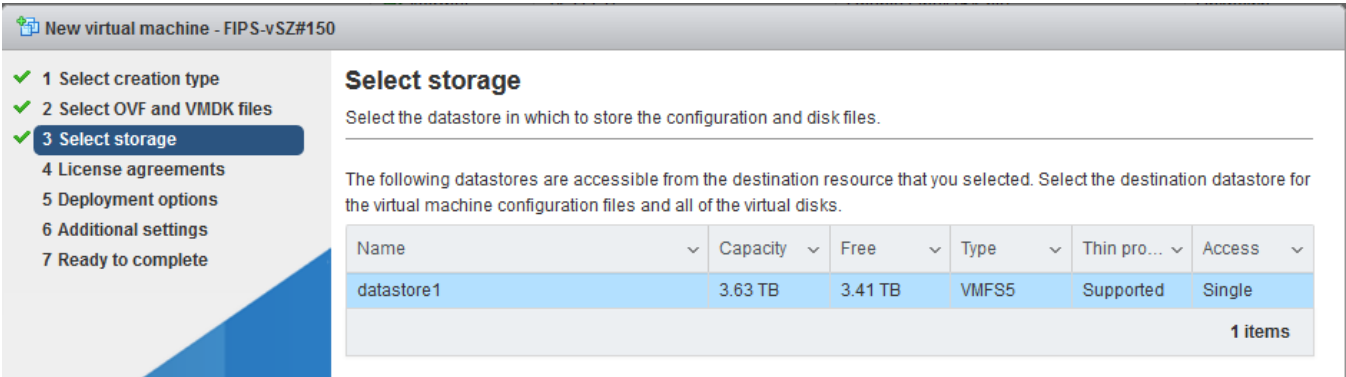
FIGURE 7 Selected .ova File



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

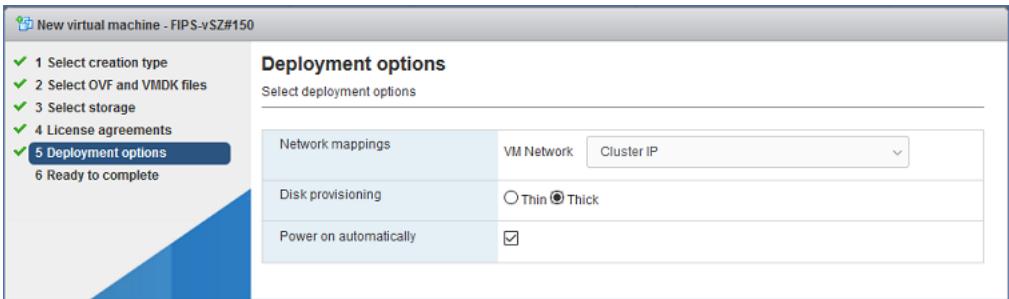
7. Select the required datastore.

FIGURE 8 Selecting the Datastore



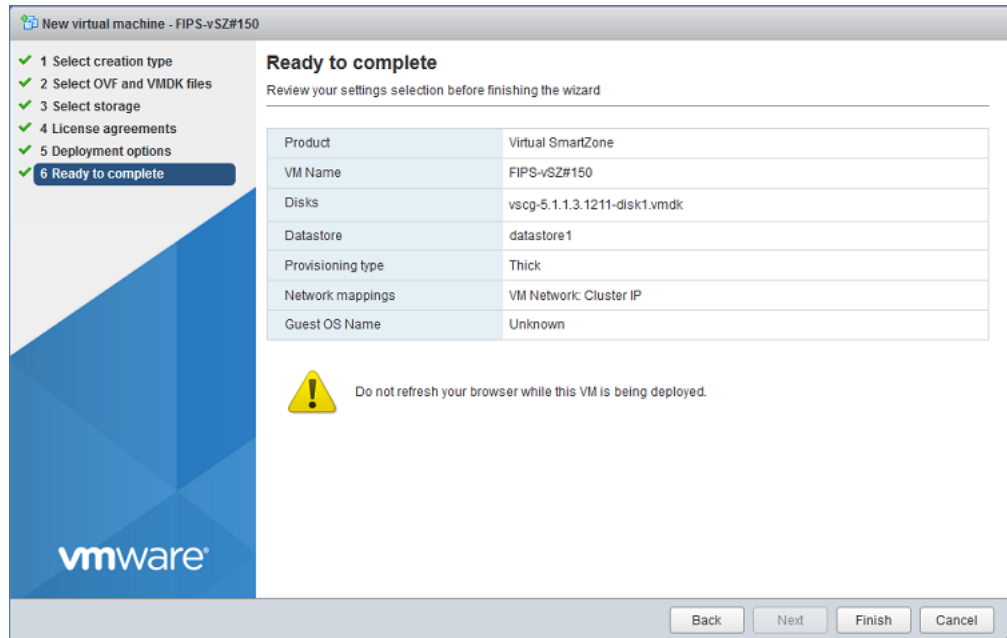
8. Click **Next** to select deployment options.

FIGURE 9 Selecting Deployment Options



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

FIGURE 10 Ready to complete installation



10. 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

Recent tasks			
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 Zone 100 (includes SZ-104 and SZ-124 models)
- Smart Zone 300 (SZ 300)

NOTE

The installation is carried out for the hardware plat forms at Ruckus facility.

Controller Configuration with FIPS Image

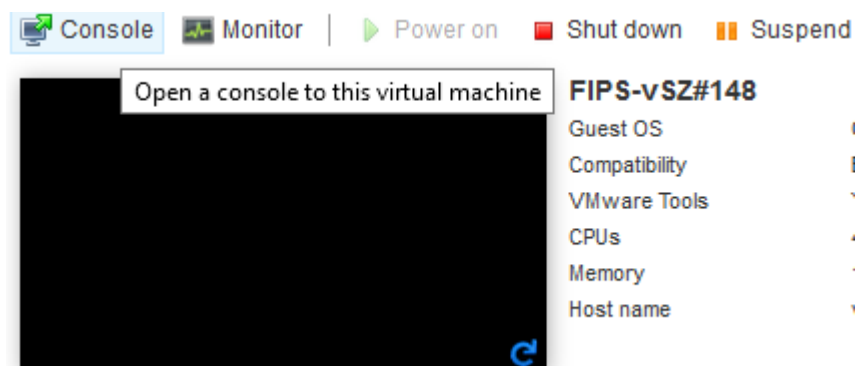
The controller configuration commands are applicable for installation of FIPS across all the platforms such as SZ100, SZ300 and vSZ.

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



3. At the login prompt, log in using "administrator" 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 SZ100 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 (SZ100)

```
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: 3.4.0.3.2009

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

```
VSZ-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.

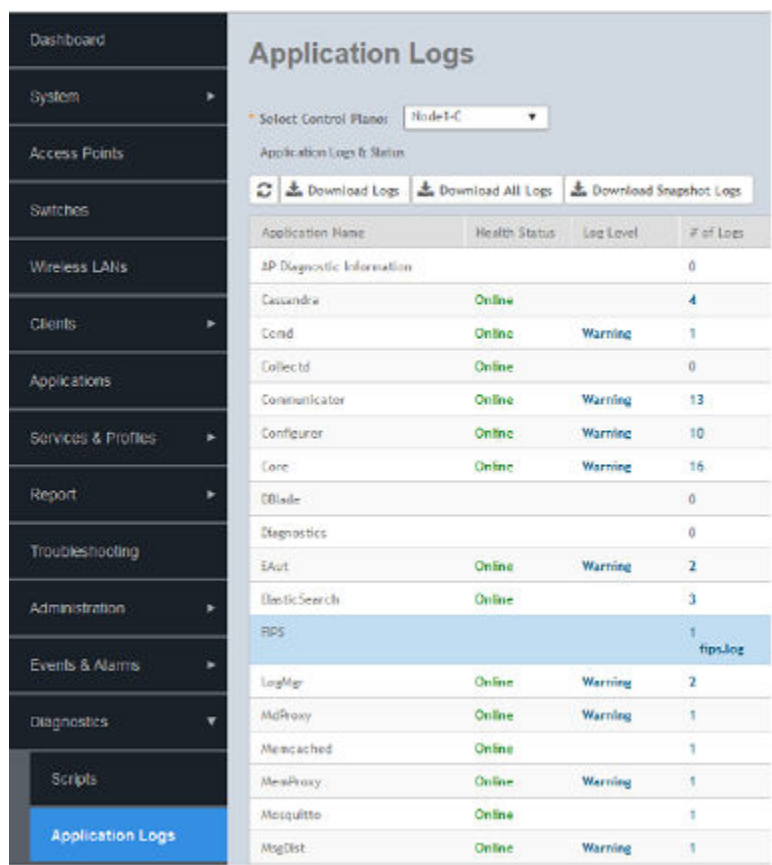
Viewing and Downloading FIPS Logs

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

Controller Configuration with FIPS Image
Viewing and Downloading FIPS Logs

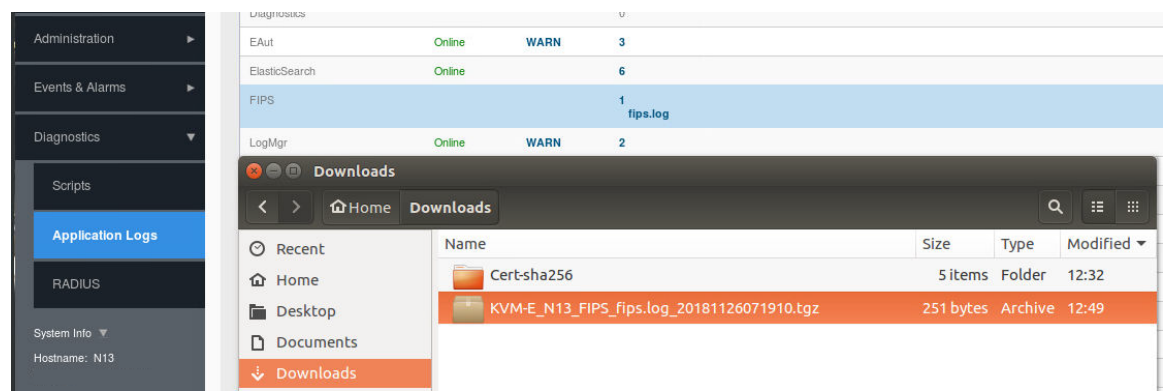
In the web interface, navigate to **Diagnostics > Application Logs > FIPS** to download the logs to the local machine.

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

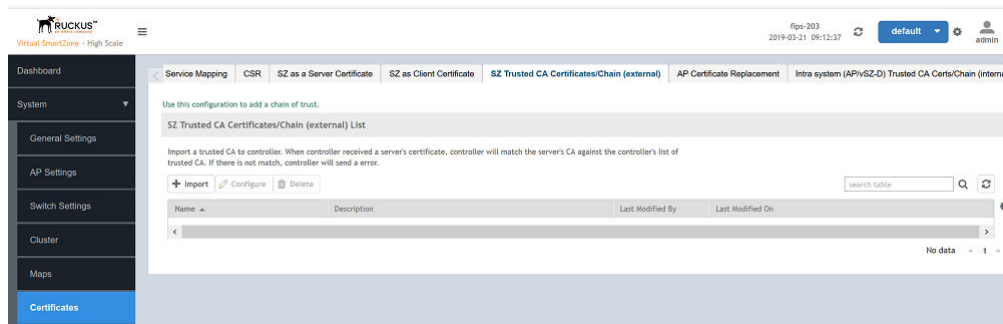


Uploading Certificates to SmartZone OS

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 > Certification > SZ Trusted CA Certificates/Chain (external)**. Click the **Import** option.

FIGURE 23 Selecting the Import Option



2. 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)

*** Name:**

Description:

Intermediate CA Certificates:

<input type="checkbox"/>	<input type="text"/>	Browse	Clear
<input type="checkbox"/>	<input type="text"/>	Browse	Clear
<input type="checkbox"/>	<input type="text"/>	Browse	Clear
<input type="checkbox"/>	<input type="text"/>	Browse	Clear

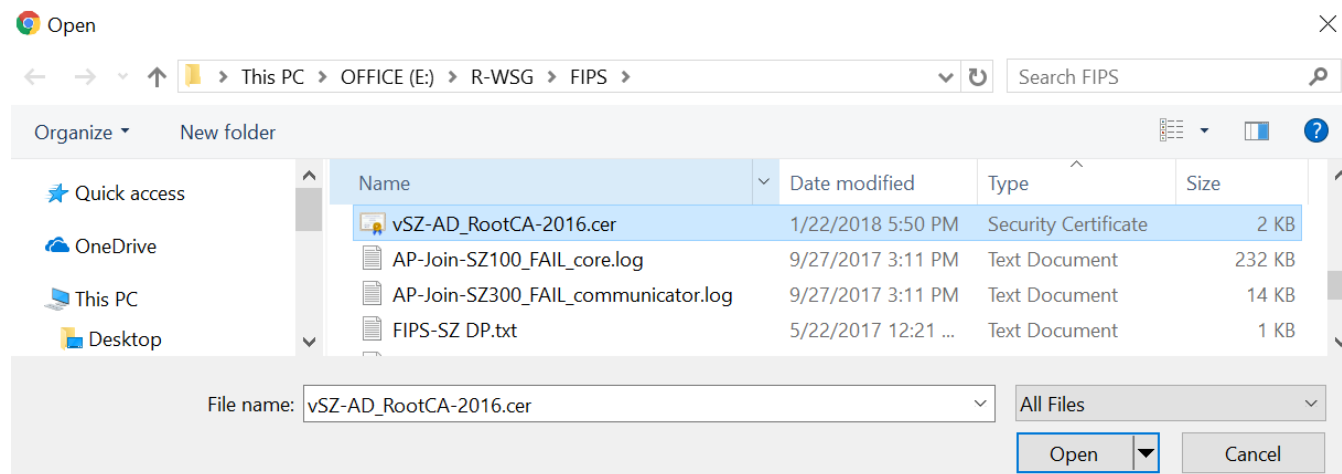
*** Root CA Certificate:** ☐ **Browse** **Clear**

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

NOTE

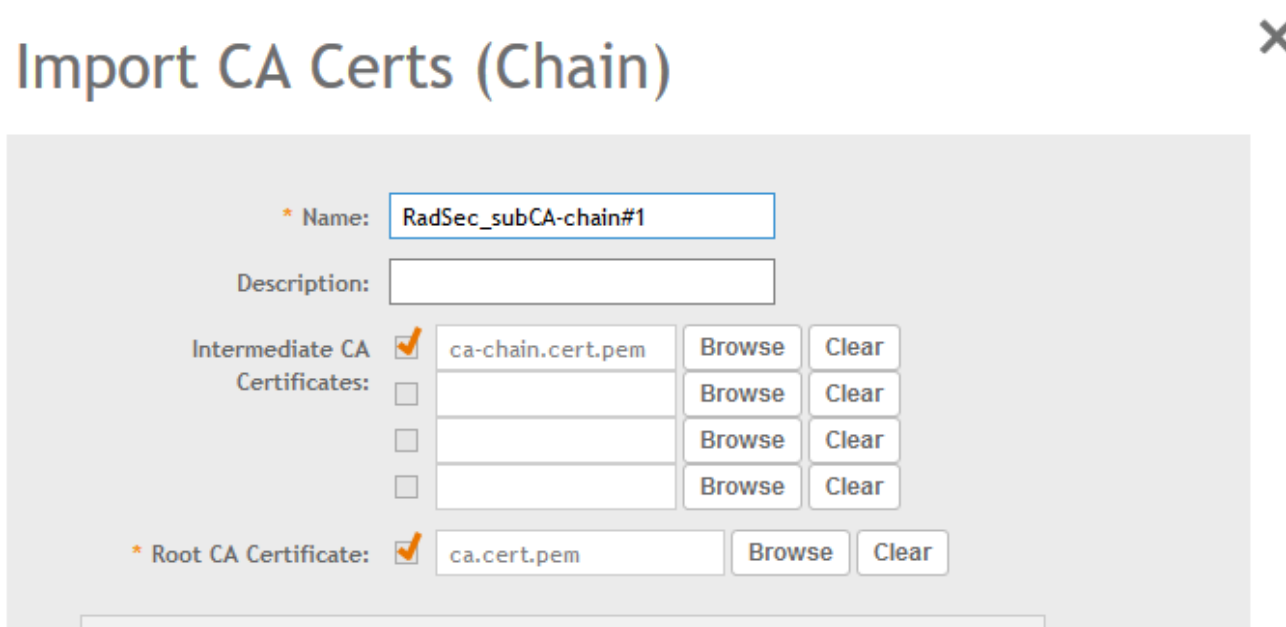
Only CER and PEM formats are supported for the CA certificates.

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



Enabling Other Secured Communication Services

The following secured communication services are available in FIPS:

- SFTP
- SNMP
- SMTP
- Syslog

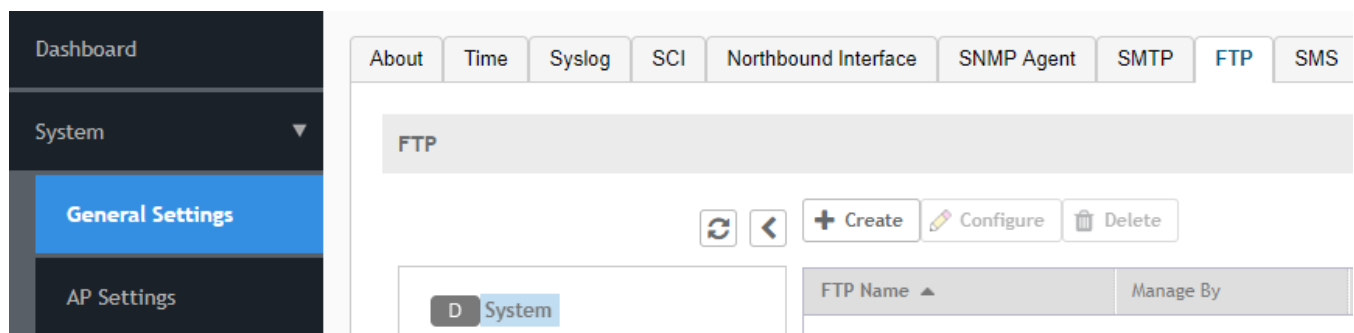
NOTE

The secured communication service Syslog is a part of 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, in the web interface, navigate to **System > General Settings > FTP**. Select the required FTP or click **Create** to add a new FTP.

FIGURE 27 Selecting FTP

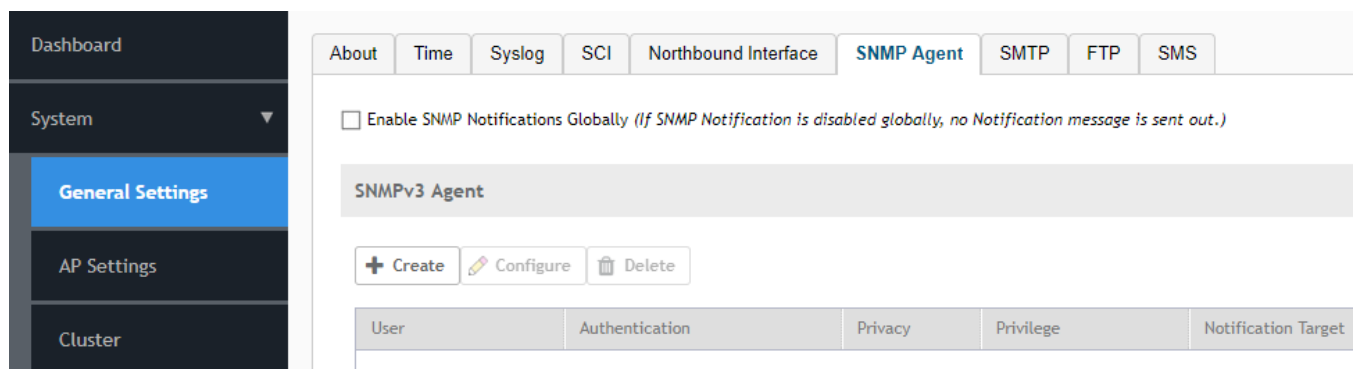


2. To enable the SNMP agent, in the web interface, navigate to **System > General Settings > SNMP Agent**. Enable the option for SNMP notifications.

NOTE

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

FIGURE 28 Selecting the SNMP Agent



3. 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:

* Mail To:

Encryption Options: ☐ TLS

- To enable syslog, in the web interface, navigate to **System > General Settings > Syslog** . Select **Enable logging to remote syslog server** to send event logs.

FIGURE 30 Selecting the Syslog Server

The screenshot shows the 'Syslog' configuration page in the SmartZone web interface. The left sidebar has a dark theme with 'General Settings' highlighted. The main area has a light theme with tabs for 'About', 'Time', 'Syslog', 'SCI', 'Northbound Interface', 'SNMP Agent', 'SMTP', 'FTP', and 'SMS'. The 'Syslog' tab is active, displaying configuration options for remote syslog servers. The 'Enable logging to remote syslog server' checkbox is checked. Below it, there are fields for 'Primary Syslog Server Address', 'Secondary Syslog Server Address', 'Application Logs Facility', 'Administrator Activity Logs Facility', 'Other Logs Filter Severity', and 'Event Facility'. Each of these has a dropdown menu. There are also 'Port' and 'Protocol' fields for each server, with '514' and 'UDP' pre-filled. 'Ping Syslog Server' buttons are next to each server configuration. At the bottom, there is an 'Event Filter' section with three radio button options: 'All events', 'All events except client association/disassociation events' (which is selected), and 'All events above a severity'. Below this is a table mapping 'Event Severity' to 'Syslog Priority'.

Event Severity	Event Filter	Syslog Priority
Critical	All events except client association/disassociation events	Error
Major		Error
Minor		Warning
Warning		Warning
Informational		Info
Debug		Debug

At the bottom of the page, there are 'Refresh', 'OK', and 'Cancel' buttons.

NOTE

The Controller can also store the audit logs locally and send it to syslog servers. The audit logs from AP and vSZ-D are also collected from the controller and sent to the configured syslog server. These audit logs are not stored locally on AP or vSZ-D. The controller performs log rotation for both the file system and database. For the file system log file, max 10 archives of application logs with each log size of up to 10 MB.

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. SmartZone 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.

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.

Connection between SZ and RadSec Server will last for 30 Sec Max. As soon SZ receives a new Authentication Request, it will initiate a TLS handshake towards RadSec. If Network is down or RadSec server (process) itself is down then UE authentications FAIL.

NOTE

If the connection is broken, then it resumes by default when the next radius message is received from the client.

NOTE

TLS cipher suites are not user-configurable. The following cipher suites are supported by SZ (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:

OCSP Validation: ☒ ON ☐ OFF * OSCP 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:

3. Enter the authentication service name.
4. For **Service Protocol**, select **RADIUS**.

NOTE

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

5. For **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

6. 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

7. 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.

8. 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.

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

For OCSP 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.

10. 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.

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

12. 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.

- 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 33 Configuring the Client Certificate

Edit Client Certificate: clientcert

Name:

Description:

Client Certificate

Client Certificate: Browse Clear

Private Key: Browse Clear

-----BEGIN CERTIFICATE-----
Version: V3
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:
2968816468379698624151593607456469162886462018858598902299767140370846988
2663833279346958245289337620149806937469779525876683764905622192393261092
06414723534710242903535954575092588749528110351296755111911370231225850409
47019923832421723135015236808134390214313123373471018908084967277549980715
9995575165254152264959037712178071331739270349875232484428227897814931284
33529491906682576604672358430793895483116869029774547659160763976356289835
118483595345708898835133939662329501186151161520323197699121873844367073
86528844576138533743644315085090368545219630730591667639078695943562706257
0452250909455466533383337

Validate OK Cancel

- 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.

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

FIGURE 34 Configuring RadSec Accounting Service

Edit Accounting Service: radsec_10.1.200.197

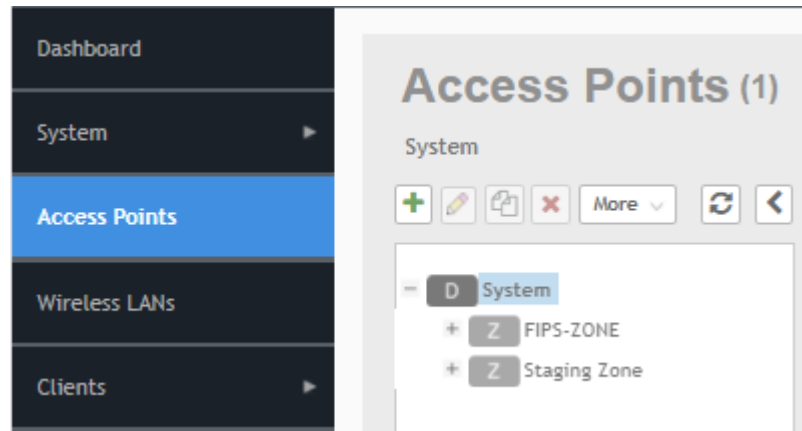
The screenshot displays the 'Edit Accounting Service' configuration page for a service named 'radsec_10.1.200.197'. The page is divided into several sections:

- Name:** radsec_10.1.200.197
- Description:** (empty field)
- Service Protocol:** RADIUS Accounting (selected with a radio button)
- RADIUS Service Options:**
 - Encryption:** ON TLS (toggle switch)
 - CN/SAN Identity:** sz1.commscope.com
 - OCSP Validation:** ON (toggle switch)
 - OCSP URL:** http://10.1.200.135:7777
 - Client Certificate:** client_cert (dropdown menu)
- Primary Server:** client_cert (dropdown menu)
- IP Address:** (empty field)
- Port:** 2083
- Shared Secret:** (empty field)
- Confirm Secret:** (empty field)

15. 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.
16. Click **Save** to add the RadSec accounting service.

17. 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 35 Selecting System as the Domain



18. 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 36 Configuring an AP Group

Configure Group

Name: Description:

Type: ☐ Domain ☒ Zone ☐ AP Group

Parent Group:

Configuration

General Options

* AP Firmware:

Country Code:

Different countries have different regulations on the usage of radio channels.
To ensure that this zone is using an authorized radio channel, select the correct country code for your location.

Location: (example: Ruckus HQ)

Location Additional Information: (example: 350 W Java Dr, Sunnyvale, CA, USA)

GPS Coordinates: Latitude: Longitude: (example: 37.411272, -122.019616)

Altitude: meters

* AP Admin Logon: * Logon ID: * Password:

AP Time Zone: ☒ System defined ☐ User defined

AP IP Mode: ☒ IPv4 only ☐ IPv6 only ☐ Dual

[?] Historical Connection Failures: ☐ OFF

[?] DP Zone Affinity Profile: +

OK **Cancel**

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

NOTE

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

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

21. 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 37 Creating a WLAN with Open Method

The screenshot shows the 'Create WLAN Configuration' web page. It has several input fields and dropdown menus. The 'Name' field is empty. The 'SSID' field is empty. The 'Description' field is empty. The 'Zone' dropdown is set to 'FIPS-Zone'. The 'WLAN Group' dropdown is set to 'default'. There is a 'Create' button next to the WLAN Group dropdown. Below these fields are two sections: 'Authentication Options' and 'Encryption Options'. In the 'Authentication Options' section, under 'Authentication Type', the radio button for 'Standard usage (For most regular wireless networks)' is selected. Under 'Method', the radio button for 'Open' is selected. In the 'Encryption Options' section, under 'Method', the radio button for 'WPA2' is selected. Under 'Algorithm', the radio button for 'AES' is selected. At the bottom, there is a 'Passphrase' field and 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 38 Creating a WLAN with 802.1X EAP & MAC Method

Create WLAN Configuration

Zone: FIPS-Zone

WLAN Group: default

Create

Authentication Options

Authentication Type: ☒ Standard usage (For most regular wireless networks) ☐ Hotspot (WISPs) ☐ Hotspot 2.0 Access ☐ Hotspot 2.0 Onboarding

Method: ☐ Open ☐ 802.1X EAP ☒ 802.1X EAP & MAC

MAC Authentication: ☐ Use user-defined text as authentication password (default is device MAC address):

MAC Address Format:

aabbccddeeff
aabbccddeeff
AA-BB-CC-DD-EE-FF
AA-BB-CC-DD-EE-FF
AABBCCDDEEFF
aa-bb-cc-dd-ee-ff

Encryption Options

Method:

AA-BB-CC-DD-EE-FF
AA-BB-CC-DD-EE-FF
AABBCCDDEEFF
aa-bb-cc-dd-ee-ff

Algorithm:

aa-bb-cc-dd-ee-ff

802.11r Fast Roaming: ☐ Enable 802.11r Fast BSS Transition

802.11w WEP: ☒ Disabled ☐ Capable ☐ Required

22. 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 39 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 'FIPS-Zone'. The 'WLAN Group' dropdown menu is set to 'default'. The 'Create' button is visible. Under 'Authentication Options', 'Authentication Types' has 'Hotspot (WISPr)' selected. Under 'Methods', '802.1X EAP' is selected. Under 'Encryption Options', 'Method' is set to 'WPA2' and 'Algorithm' is 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 40 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 'FIPS-Zone'. The 'WLAN Group' dropdown menu is set to 'default'. The 'Create' button is visible. Under 'Authentication Options', 'Authentication Types' has 'Hotspot (WISPr)' selected. Under 'Methods', 'Open' is selected. Under 'Encryption Options', 'Method' is set to 'WPA2' and 'Algorithm' is set to 'AES'. There is a 'Passphrases' field and a 'Show' button 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 41 Mapping to the Hotspot Porta

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 42 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 43 Editing Realm-based Authentication Service

Edit Realm Based Authentication Service: No Match

* Realm: 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 44 Configuring Realm-based Accounting Service

* Name: RadSec Acct Profile
 Description:

Realm Based Accounting Service

+ Create Configure Delete

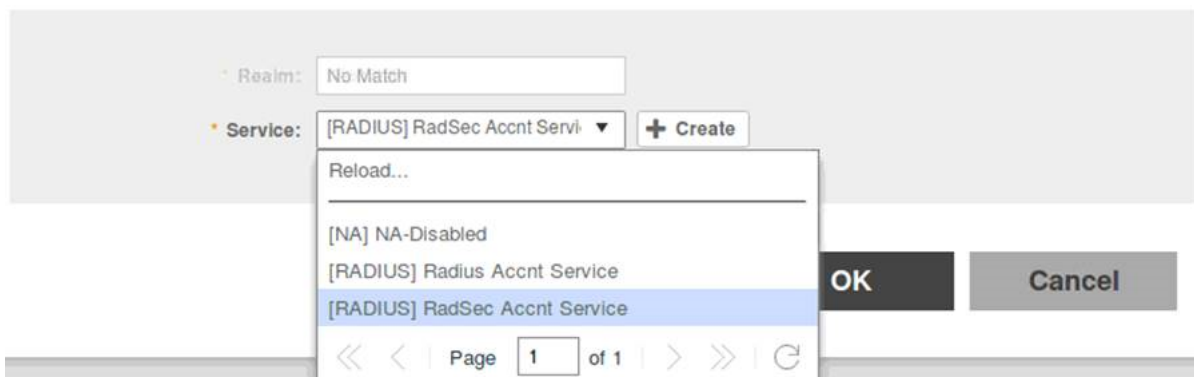
Realm	Protocol	Accounting Service
No Match	RADIUS	RadSec Account Service
Unspecified	RADIUS	RadSec Account Service

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**.

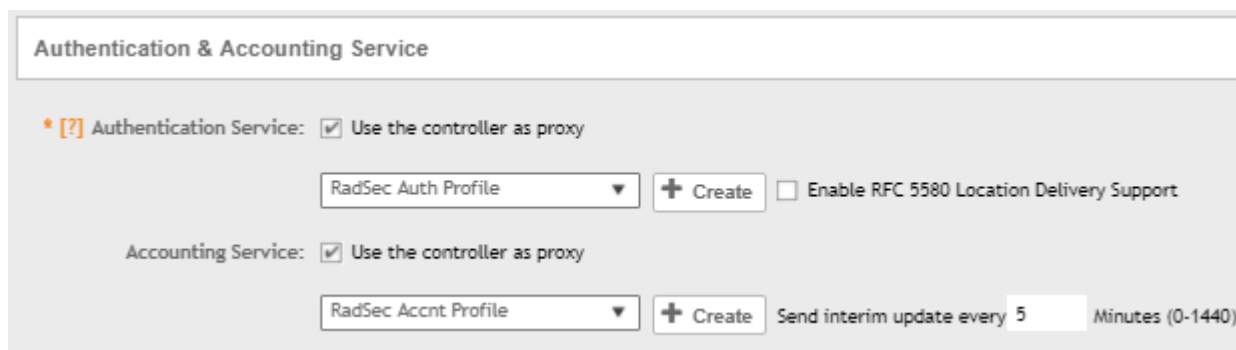
8. Click **Configure**, and configure the following items:
 - For **Service**, select **RadSec Acctnt Service**.
 - Click **OK** to save the configuration.

Edit Realm Based Accounting Service: No Match



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

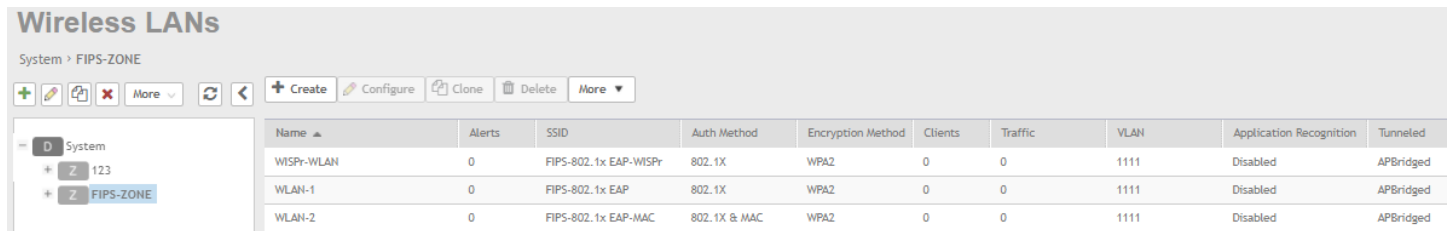
FIGURE 45 Mapping to Authentication & Accounting Service



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.

FIGURE 46 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 SZ and RadSec Server during wireless client Authentication then SZ triggers an event. To know more about the event refer to the Events section.

Upgrading the Software

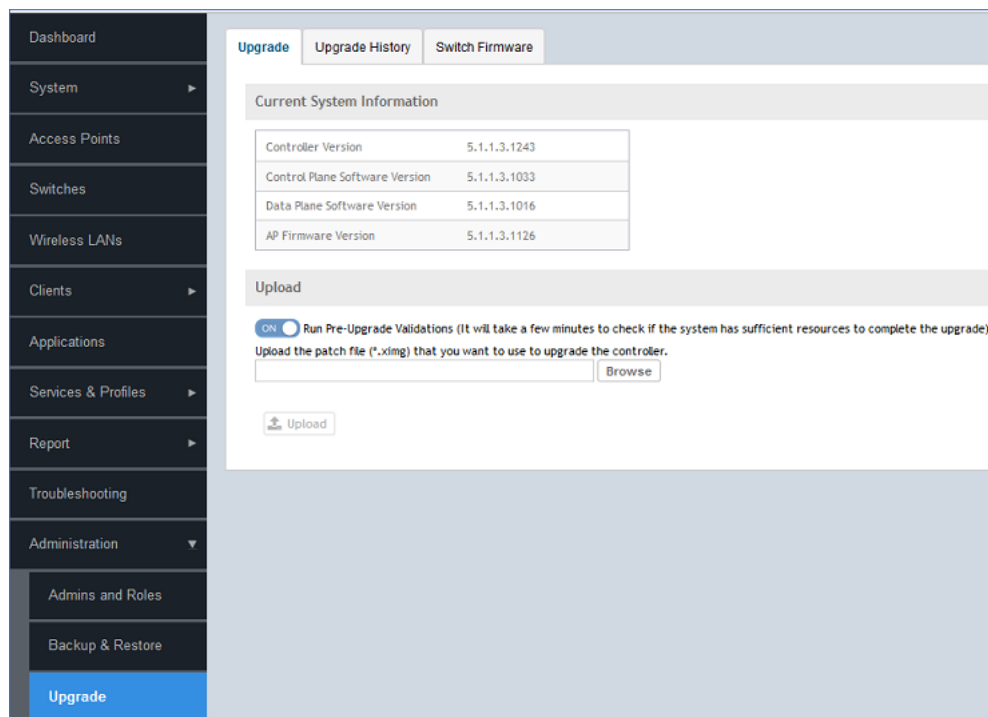
Ruckus periodically releases software updates which contains new feature enhancements or fixes for known issues.

Upgrading (v)SZ Software

The software updates can be done through GUI or CLI. To perform the updates, follow the below steps.

1. Login to the GUI and upload the image.
2. Download the update/upgrade image from the Ruckus Customer release site. Click **Upgrade** to view the current version of the software.

FIGURE 47 Upgrading the Software



Dashboard
System
Access Points
Switches
Wireless LANs
Clients
Applications
Services & Profiles
Report
Troubleshooting
Administration
Admins and Roles
Backup & Restore
Upgrade

Upgrade Upgrade History Switch Firmware

Current System Information

Controller Version	5.1.1.3.1243
Control Plane Software Version	5.1.1.3.1033
Data Plane Software Version	5.1.1.3.1016
AP Firmware Version	5.1.1.3.1126

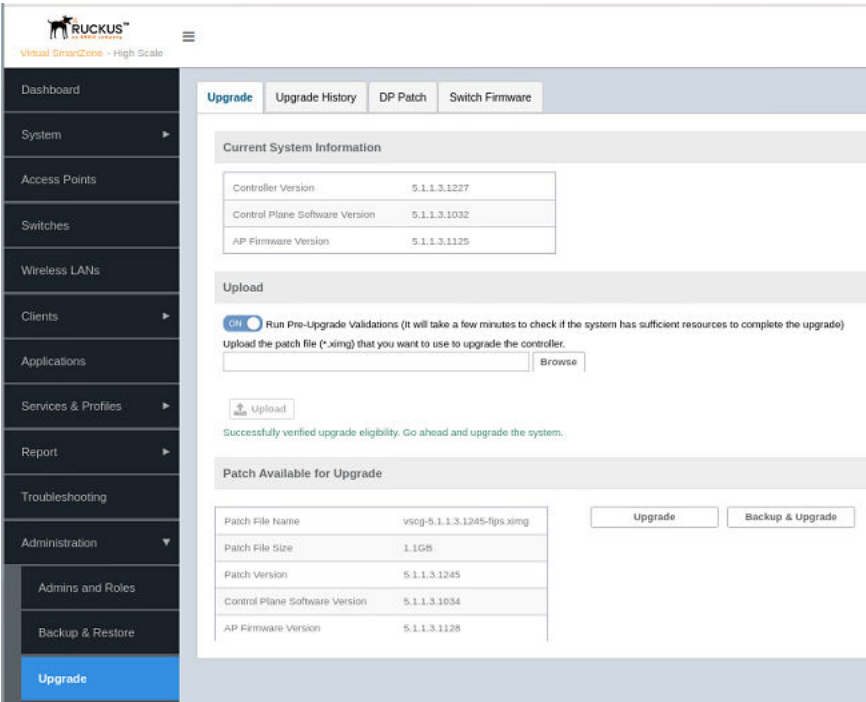
Upload

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

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

3. After uploading, the user has to initiate **Upgrade** or **Backup & Upgrade**.

FIGURE 48 Initiating the Upgrade



NOTE

The upgrade package contains the upgrade software/firmware, signatures and the certificates of the signature signers. When the upgrade package is uploaded to the controller, the controller will validate the certificate chain first. If the certificate of signature signer passes the chain validation, the controller 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. In such case, use a validate upgrade package to continue system upgrading.

4. The web interface lists the active and inactive upgrade history.
5. Once uploaded, delayed activation/upgrade can be initiated.

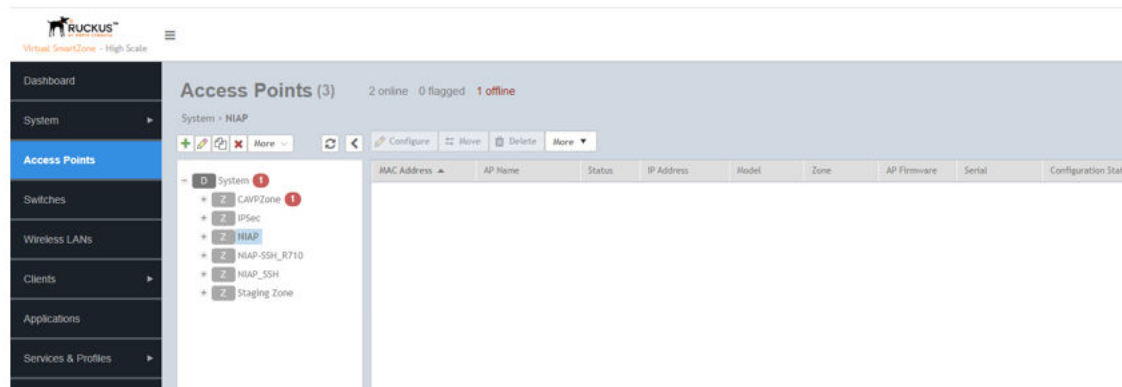
Upgrading the AP Software

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 . You can manually upgrade or downgrade AP firmware version of a Zone. Perform the following to change the AP Firmware of the Zone

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

FIGURE 49 Locating the Zone

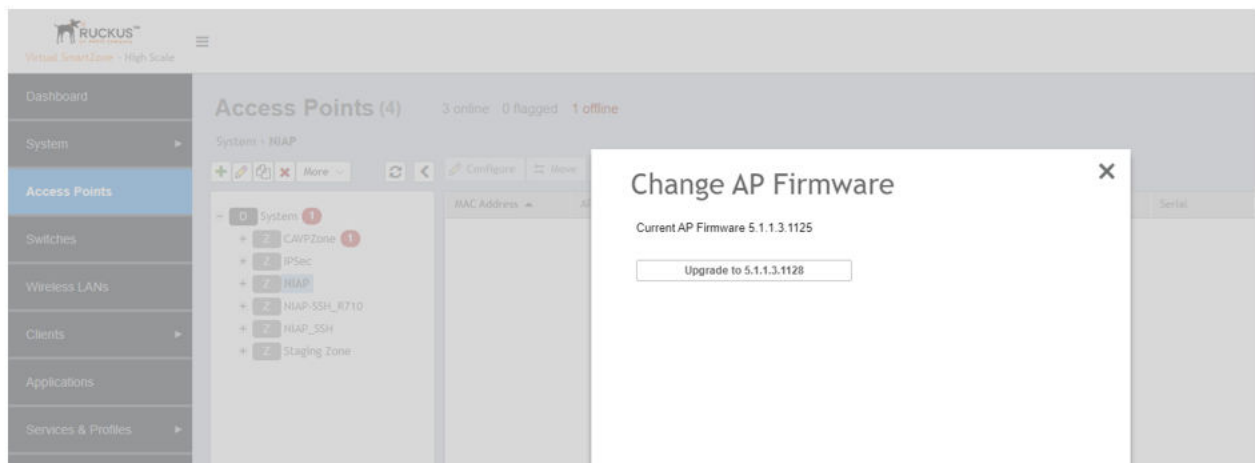
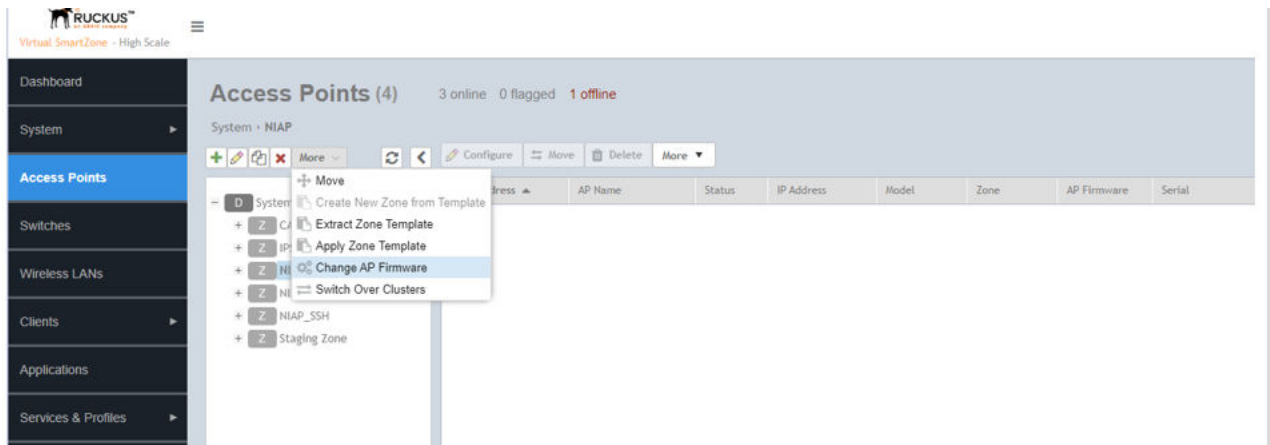


Controller Configuration with FIPS Image

Upgrading the Software

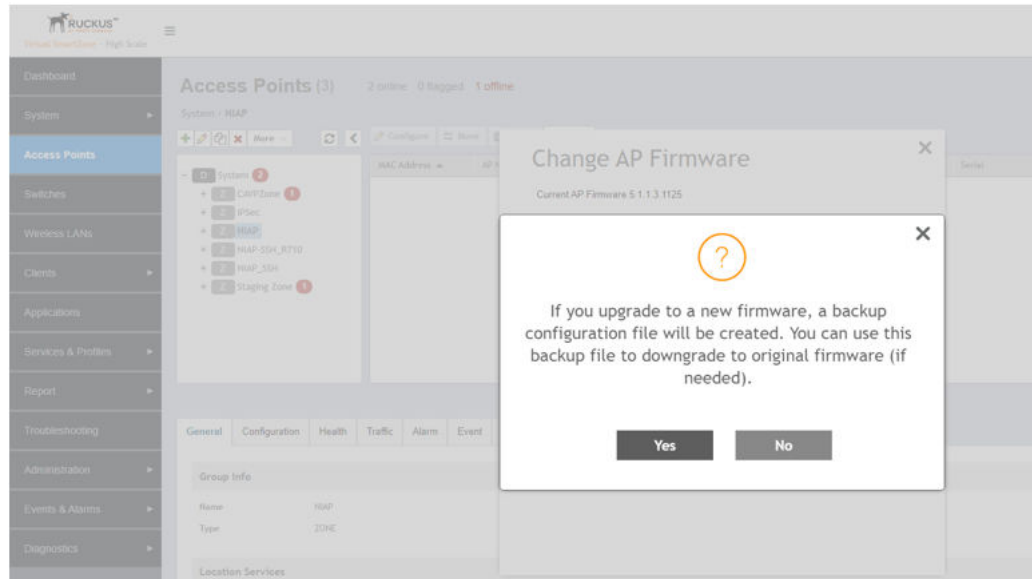
2. Click on **More** and select **Change AP Firmware**. The Change AP Firmware dialog box displays the current AP firmware version.

FIGURE 50 Changing the AP Firmware



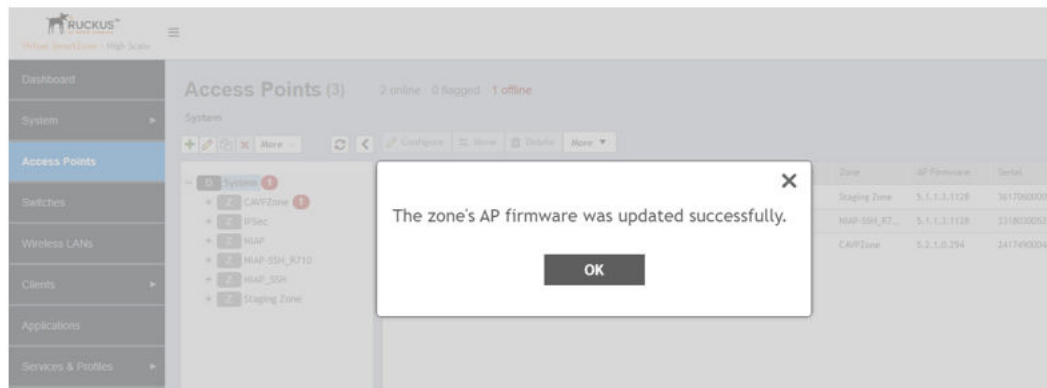
3. Select the firmware version you needed. If you upgrade to new firmware version a backup configuration will be created which can be used during firmware downgrade to original firmware.

FIGURE 51 Confirming the Upgrade



4. Click **Yes**, a dialogue box appears displaying the below message.

FIGURE 52 Upgrading Successfully



NOTE

If the zone fails to upgrade a dialogue box displays to download a 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 will 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.

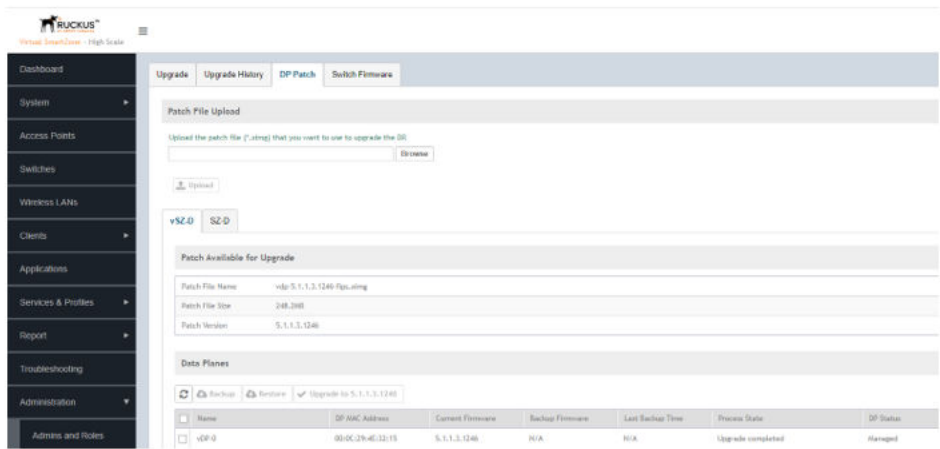
Upgrading the vSZ-D Software

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

Perform the following steps to upgrade the vSZ-D Software.

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

FIGURE 53 DP Patch Page

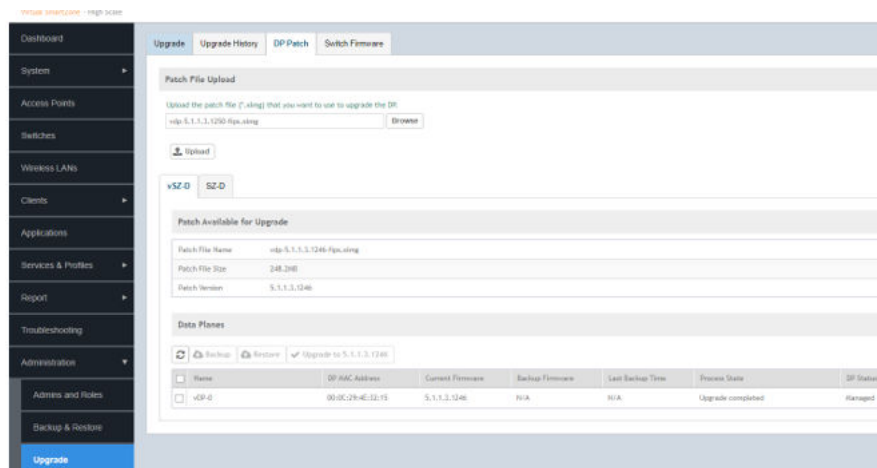


NOTE

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 .

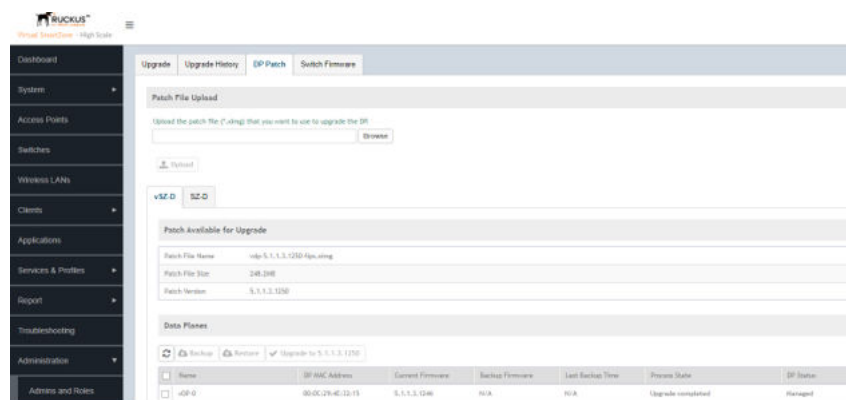
3. In Patch screen click **browse** and select the patch file to upgrade

FIGURE 54 Browsing the Patch File



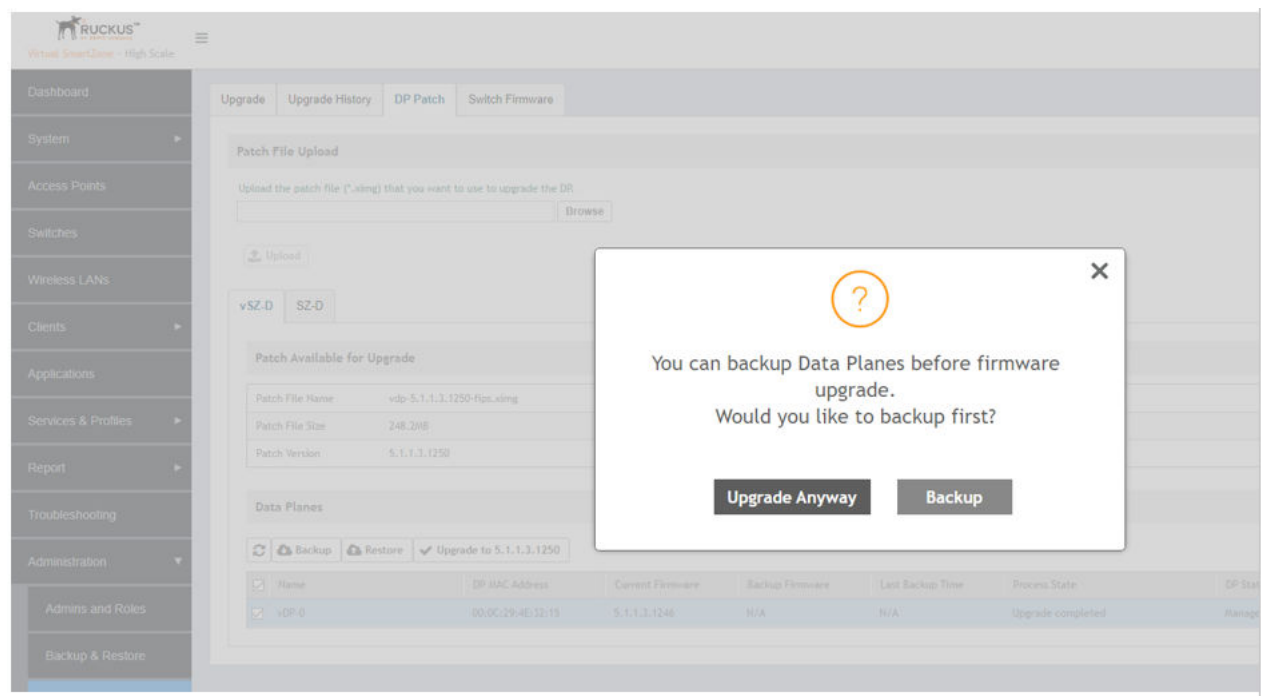
4. Click **Upload** to upload the patch file.

FIGURE 55 Uploading the patch file



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

FIGURE 56 Backing up Data Plane Data

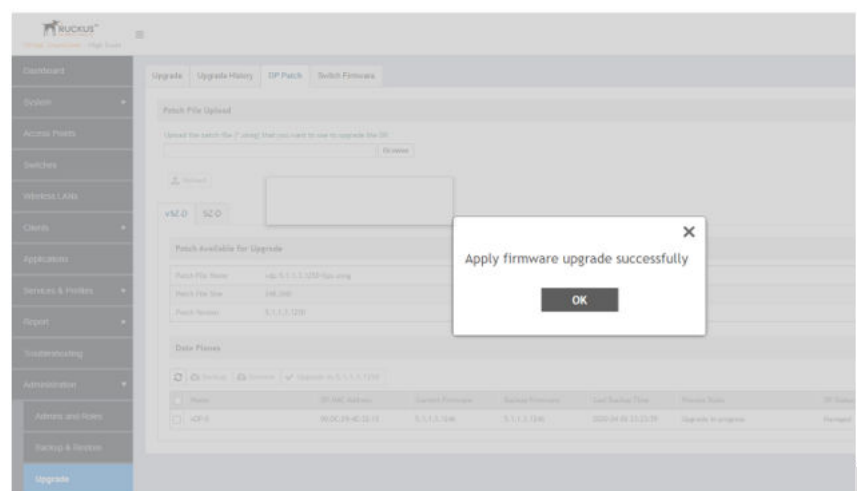


NOTE

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

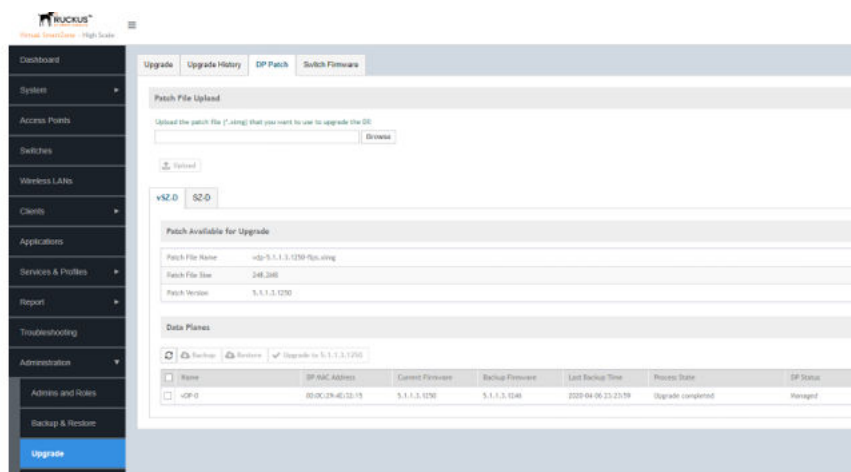
6. Click on **Upgrade Anyway** to upgrade the vSZ-D to apply vSZ-D Patch

FIGURE 57 Upgrading the vSZ-D



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

FIGURE 58 Successful Upgradation of vSZ-D Software



vSZ-D FIPS Installation with FIPS Image

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).

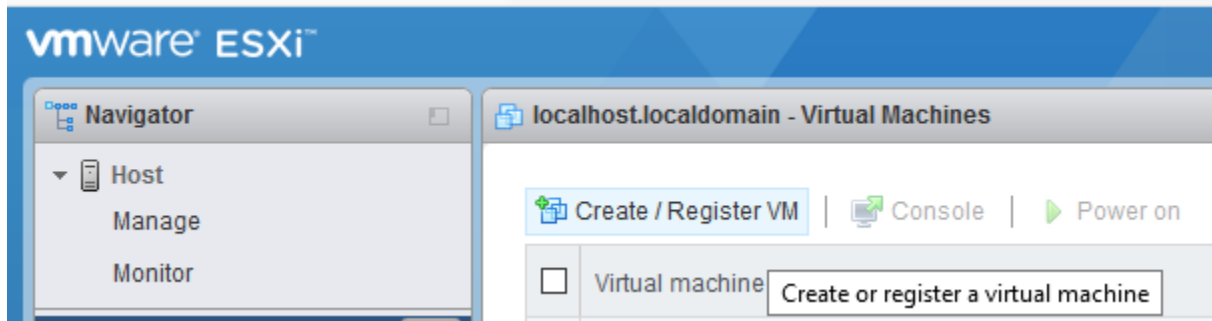
vSZ-D FIPS Installation Prerequisites for FIPS

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)

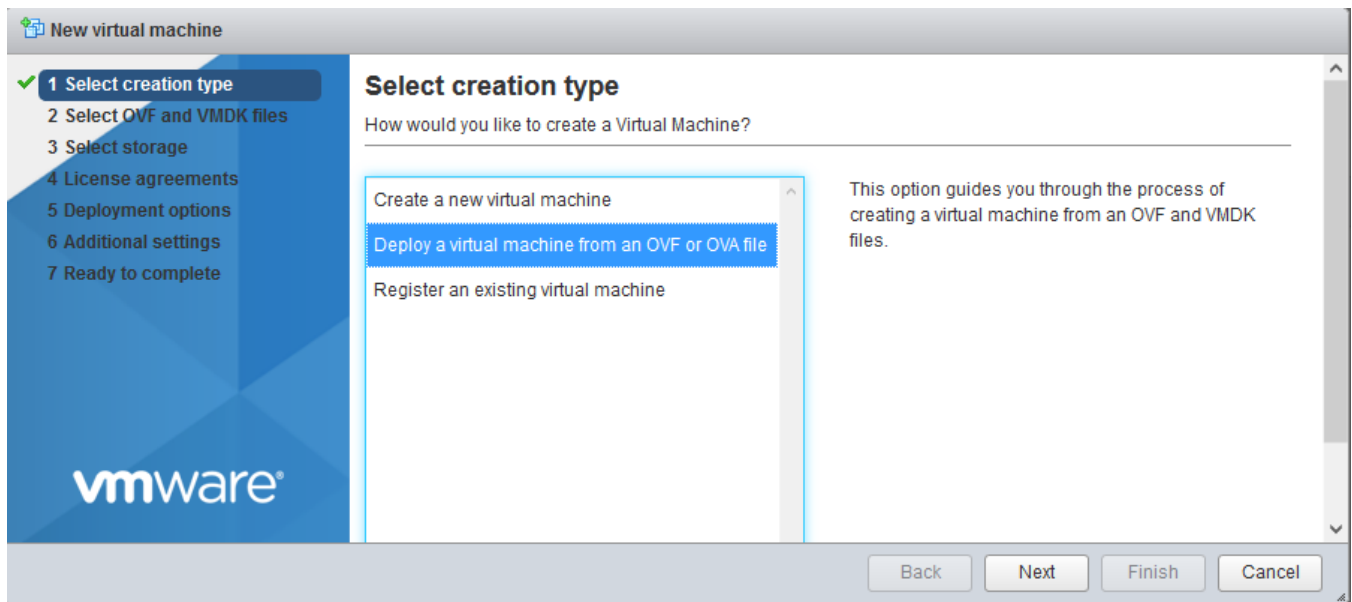
1. Install and deploy the .ova file on VMware ESXi using the **Create / Register VM** option, as shown in the following figure.

FIGURE 59 Creating and register VM



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

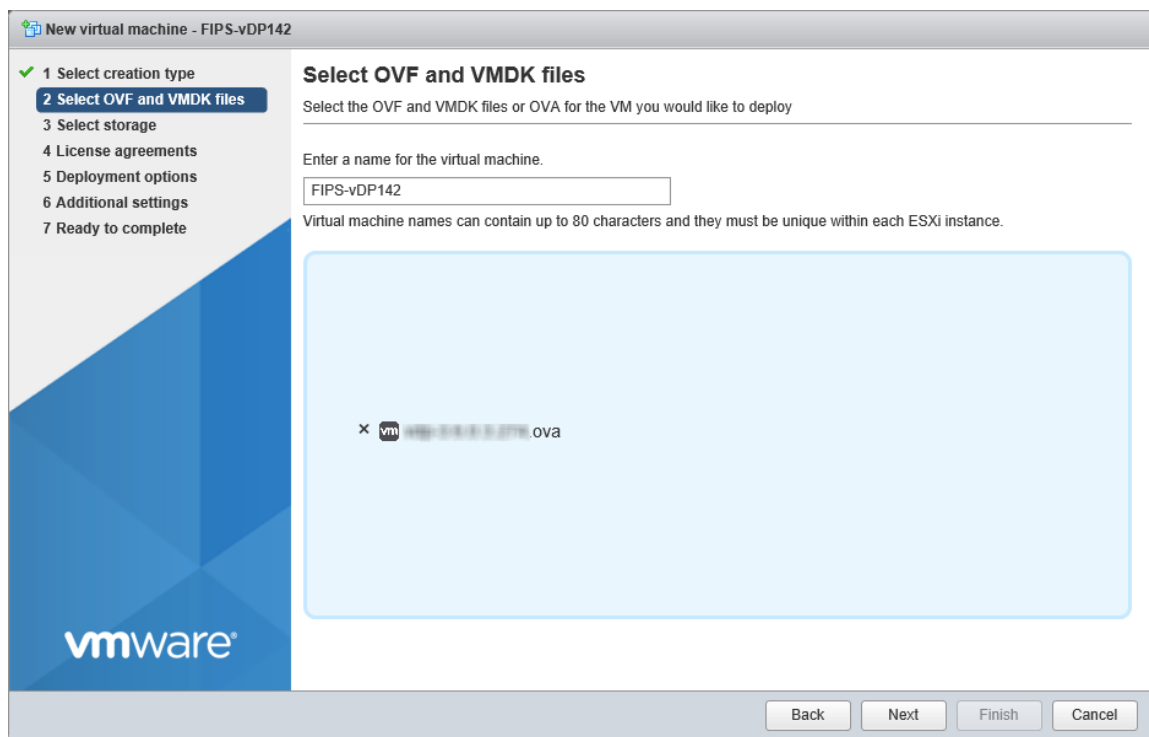
FIGURE 60 Selecting the Creation Type



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 61 Selecting OVF and VMDK Files

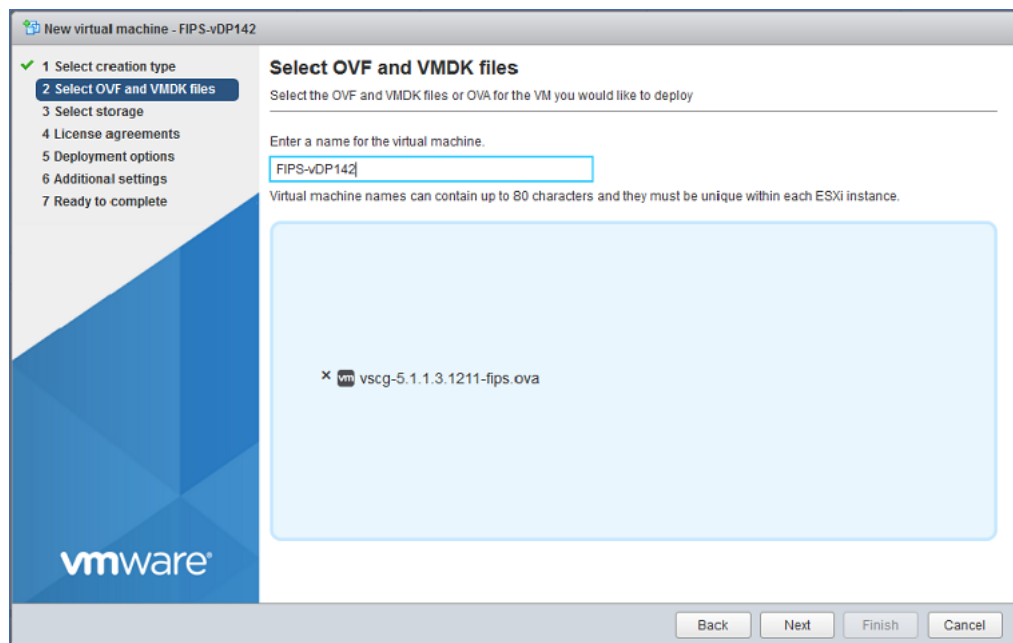


5. Select the .ova file from the browse window. The selected file is displayed in Select OVF and VMDK files screen

FIGURE 62 Selecting the .ova File



FIGURE 63 Selected file appears on screen



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

7. Select the required datastore.

FIGURE 64 Selecting the Datastore

New virtual machine - FIPS-vDP142

- ✓ 1 Select creation type
- ✓ 2 Select OVF and VMDK files
- ✓ 3 Select storage
- ✓ 4 Deployment options
- ✓ 5 Ready to complete

Select storage

Select the datastore in which to store the configuration and disk files.

The following datastores are accessible from the destination resource that you selected. Select the destination datastore for the virtual machine configuration files and all of the virtual disks.

Name	Capacity	Free	Type	Thin pro...	Access
datastore1	3.63 TB	3.16 TB	VMFS5	Supported	Single

1 items

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

FIGURE 65 Selecting Deployment options

New virtual machine - FIPS-vDP142

- ✓ 1 Select creation type
- ✓ 2 Select OVF and VMDK files
- ✓ 3 Select storage
- ✓ 4 Deployment options
- ✓ 5 Ready to complete

Deployment options

Select deployment options

Network mappings	<div>VM Network Cluster</div> <div>data-network Cluster</div>
Disk provisioning	<input checked="" type="radio"/> Thin <input type="radio"/> Thick

vSZ-D FIPS Installation with FIPS Image

Creating and Registering the Virtual Machine (vSZ-D)

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

FIGURE 66 Ready to Complete Installation

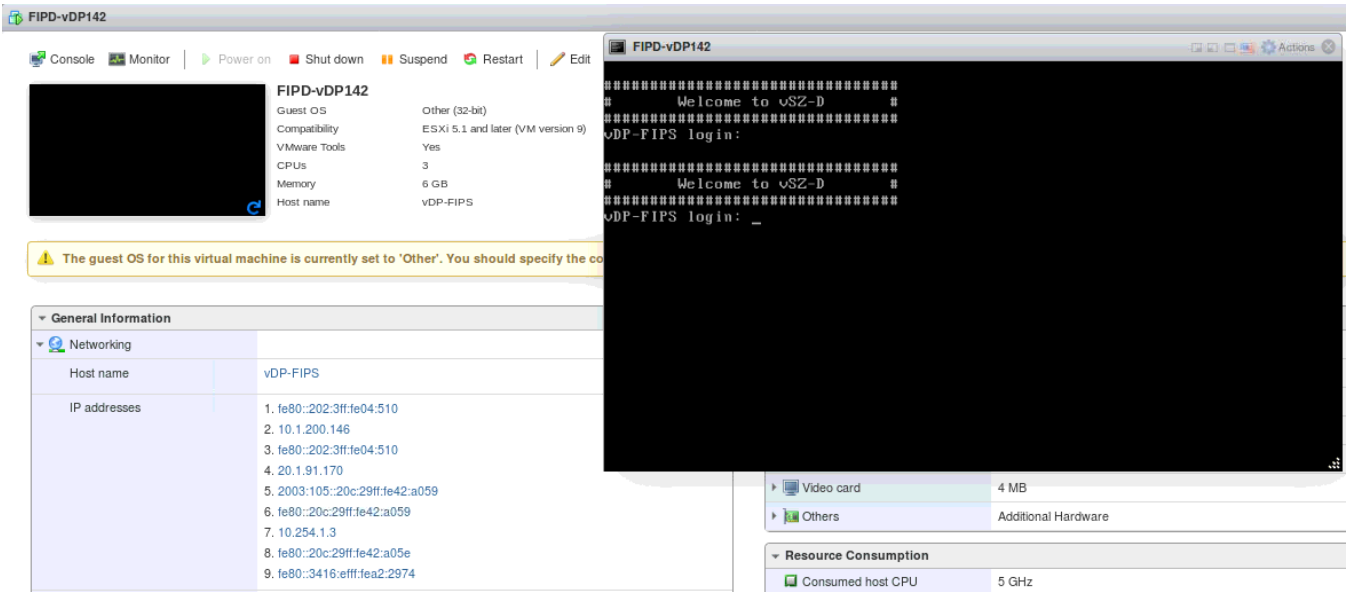
The screenshot shows the 'New virtual machine - FIPS-vDP142' wizard in VMware vSphere. The left sidebar shows five steps: 1 Select creation type, 2 Select OVF and VMDK files, 3 Select storage, 4 Deployment options, and 5 Ready to complete (highlighted). The main area is titled 'Ready to complete' and instructs the user to 'Review your settings selection before finishing the wizard'. A table lists the configuration details:

Product	Virtual SmartZone – DataPlane
VM Name	FIPS-vDP142
Disks	vdp-[redacted]-disk1.vmdk, vdp-[redacted]-disk1.vmdk
Datastore	datastore1
Provisioning type	Thin
Network mappings	VM Network: Cluster, data-network: Cluster
Guest OS Name	Unknown

Below the table is a yellow warning icon and the text: 'Do not refresh your browser while this VM is being deployed.' At the bottom right are four buttons: 'Back', 'Next', 'Finish', and 'Cancel'. The VMware logo is visible in the bottom left corner of the wizard window.

10. 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 67 Successful Installation



Joining vSZ-D to the vSZ Controller

TLS is used to perform the initial discovery of SZ controller. Once vSZ-D discovers and approves SZ controller, a SSH connection is established. Any communication between vSZ and vSZ-D is through SSH only. Before placing any wireless client call, IPsec and RGRE tunnel is formed between AP and vSZ-D. Once UE is authenticated user data traffic is through IPsec. For more information, refer [Configuring Ruckus GRE and IPsec in the WLAN](#) on page 103. vSZ-D keeps polling the SZ and it's reachability, and once controller is reachable the registration process is completed and it proceeds with SSH re-establishment.

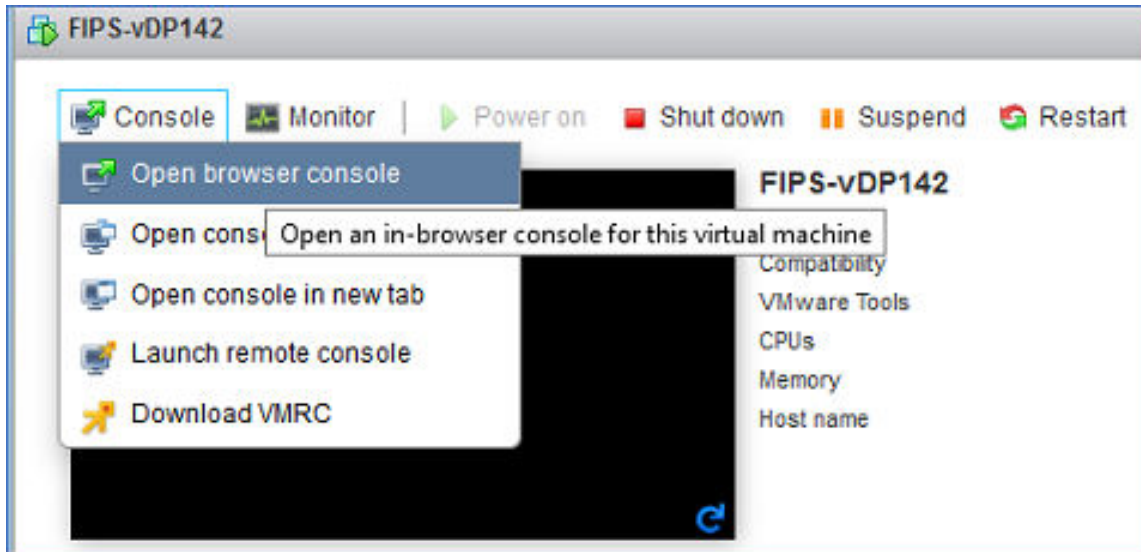
NOTE

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.

1. Once the VM has been deployed, click **Power On** to start the vSZ-D.

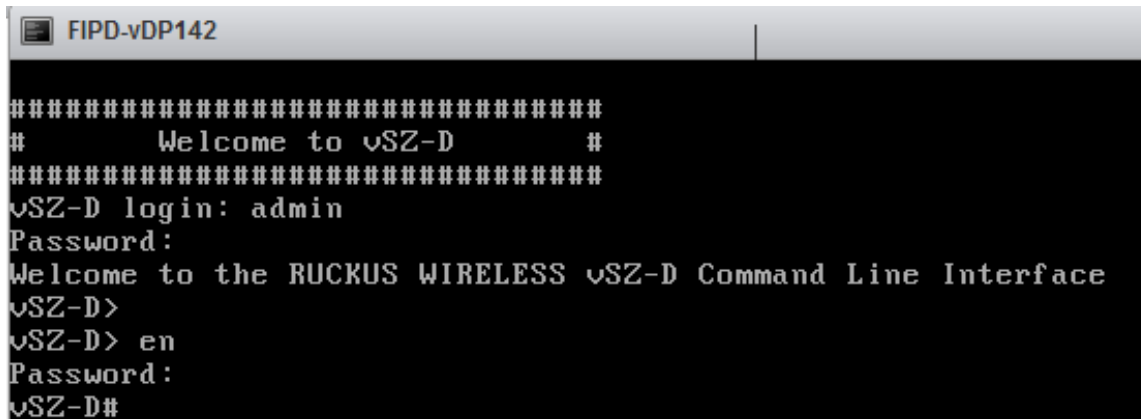
2. Open a console window to log in to the vSZ-D CLI.

FIGURE 68 vSZ CLI Console



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

FIGURE 69 Logging In to Privileged EXEC Mode



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 70 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 71 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):
```

- 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 72 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 73 vSZ-D FIPS image approved

The screenshot shows the Ruckus vSZ web interface. The left sidebar contains navigation links: Dashboard, System, General Settings, AP Settings, Cluster (selected), Maps, Certificates, Templates, Access Points, Wireless LANs, and Clients. The main content area is titled 'Cluster (1)' and shows '1 Online, 0 Flagged, 0 Offline'. Below this, there are two sections: 'Control Planes' and 'Data Planes'. The 'Data Planes' section has buttons for 'Configure', 'Approve', 'Delete', and 'Download'. A table lists the data planes, with one entry 'vGP-FIPS' highlighted in blue. The table columns are: Name, DP MAC Address, Data IP, Management IP, Model, Serial Number, Firmware, DP Status, Support FIPS, FIPS Enable, and Registration State. The 'vGP-FIPS' entry shows 'Managed' status, 'Support FIPS: Yes', 'FIPS Enable: Enable', and 'Registration State: Approved'.

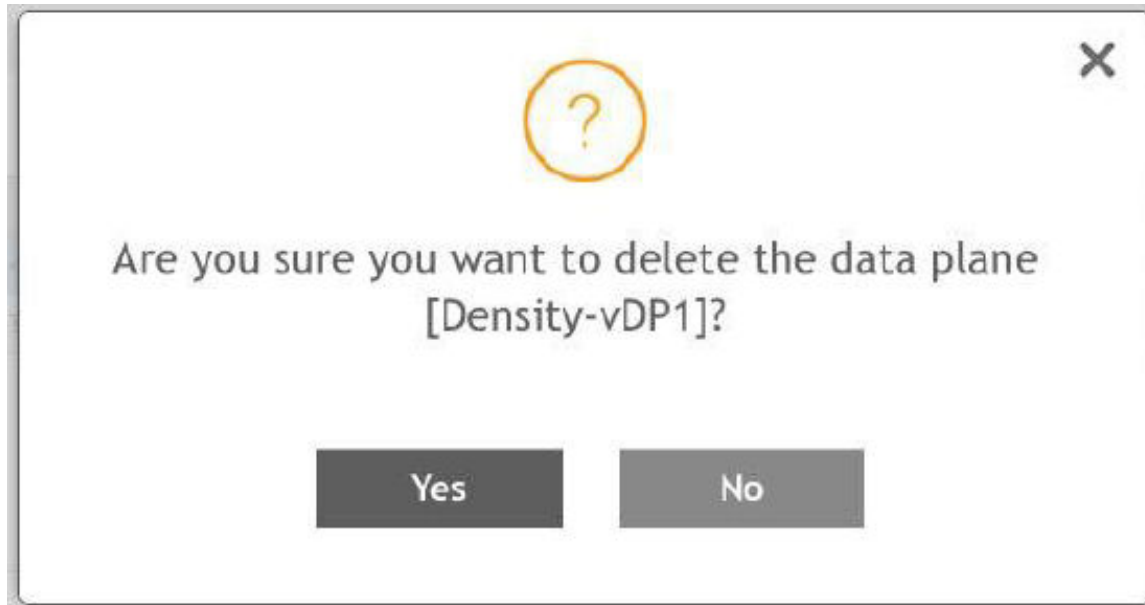
Name	DP MAC Address	Data IP	Management IP	Model	Serial Number	Firmware	DP Status	Support FIPS	FIPS Enable	Registration State
vGP-FIPS	00:0C:29:42:A0:59	20.1.51.170	10.1.200.146	Intel DP...	9720T0A7N3...		Managed	Yes	Enable	Approved

NOTE

If the connection between vSZ-D and vSZ is broken then it resumes back automatically and no manual intervention is required.

9. To remove the vSZ-D from vSZ controller, log in to the web interface of the vSZ. Navigate to **Clusters > Data Planes**, select the vSZ-D, and click **Delete**. The Data Plane entry is deleted.

FIGURE 74 Deleting Data Plane Entry



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.

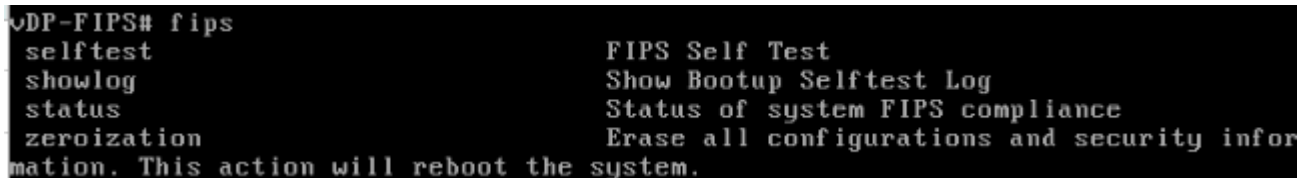
```
#####
#      Welcome to vSZ-D      #
#####
vDP-FIPS login: admin
Password:
Last login: Tue Jan 23 17:26:49 on tty1
Welcome to the RUCKUS WIRELESS vSZ-D Command Line Interface
vDP-FIPS> en
Password:
vDP-FIPS# fips status
FIPS compliance is Enable
```


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.

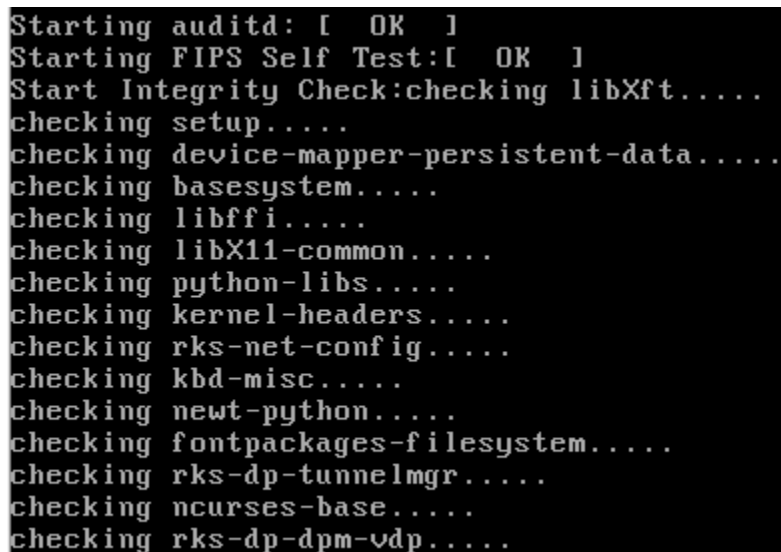
FIGURE 75 List of vSZ-D FIPS Commands



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

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

FIGURE 76 Output of fips selftest Command



```
vSP-FIPS# fips selftest
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-vdp.....
```

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

FIGURE 77 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# _
```

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 78 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.

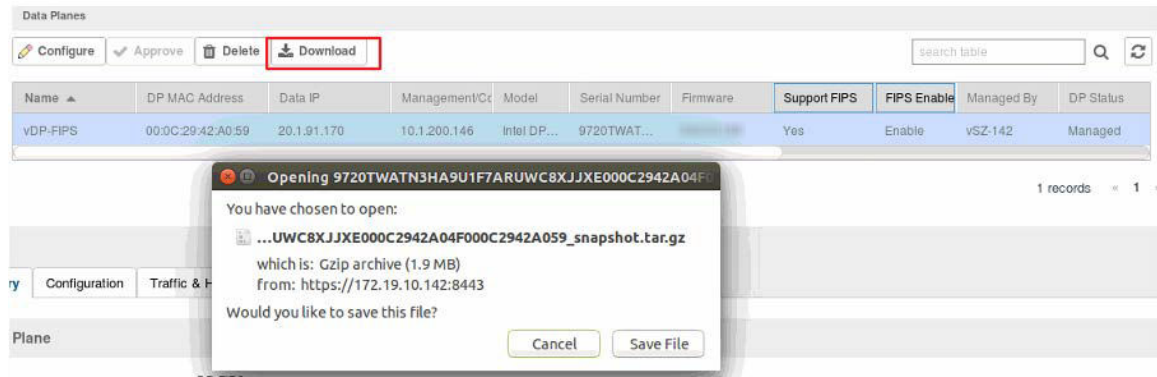
1. In the web interface, navigate to **System > Clusters > Data Planes**.
2. Select the vSZ-D that has joined the controller.
3. Click the **Download** option.

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 79 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

The following AP models support FIPS mode:

- R610
- R710
- R720
- T610
- T610s
- T710
- T710s

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.

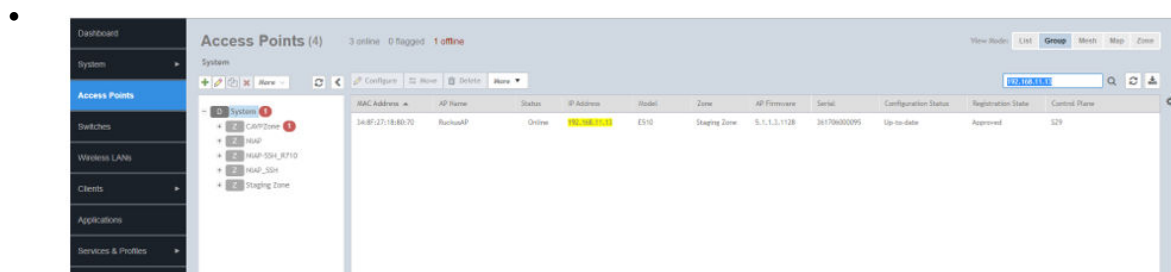
Joining AP to the (v)SZ Controller

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

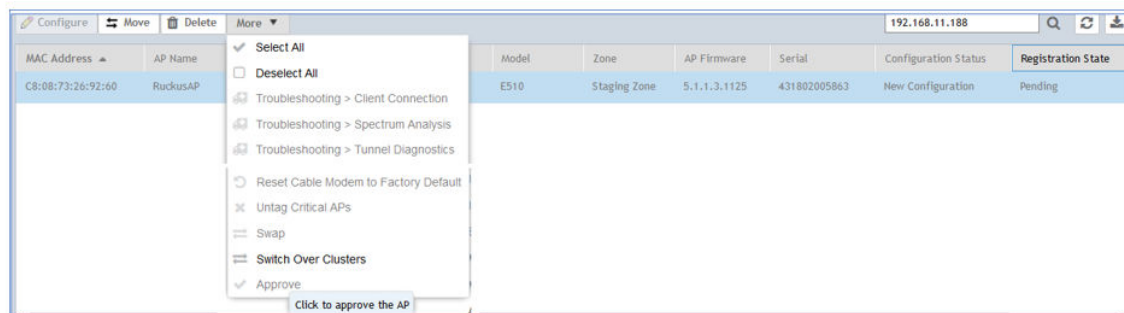
- Log on to the AP through AP SSH using username and password as super and sp-admin and set the WLAN Controller IP. Follow the commands to enable SSH communication towards WLAN Controller.

- ```
rkscli:
rkscli: set scg ip 10.1.200.143
OK
```

- Log on to the WLAN Controller through web interface and navigate to **Access Points**.



- Select the Access point that is being joined, and click **More > Approve** to approve the AP.



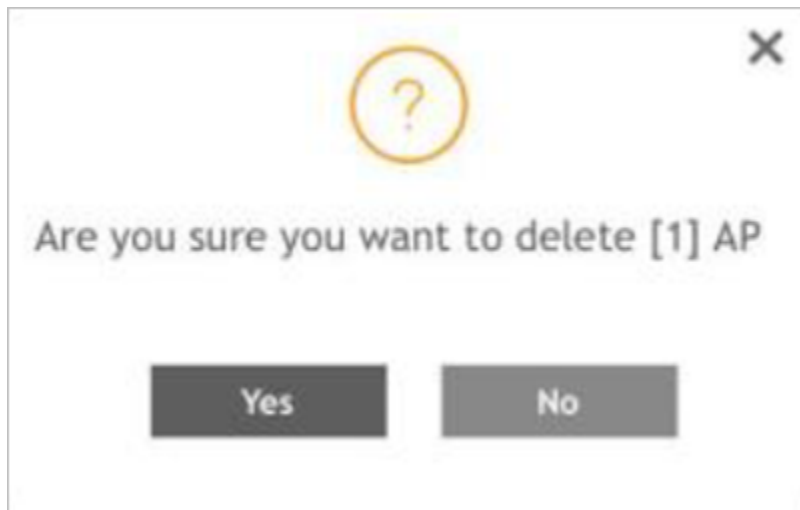
Once AP is approved an SSH tunnel will be formed across AP and WLAN Controller using public key authentication (without password - based authentication). This SSH tunnel will be utilized for management communication between AP and controller. If the connection is broken it will be resumed/reattempted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

#### NOTE

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

- To remove the Access Point from the controller, select the Access Point that is joined and click **Delete**.

**FIGURE 80** Deleting an Access Point



## 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.

## FIPS AP Behavior

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

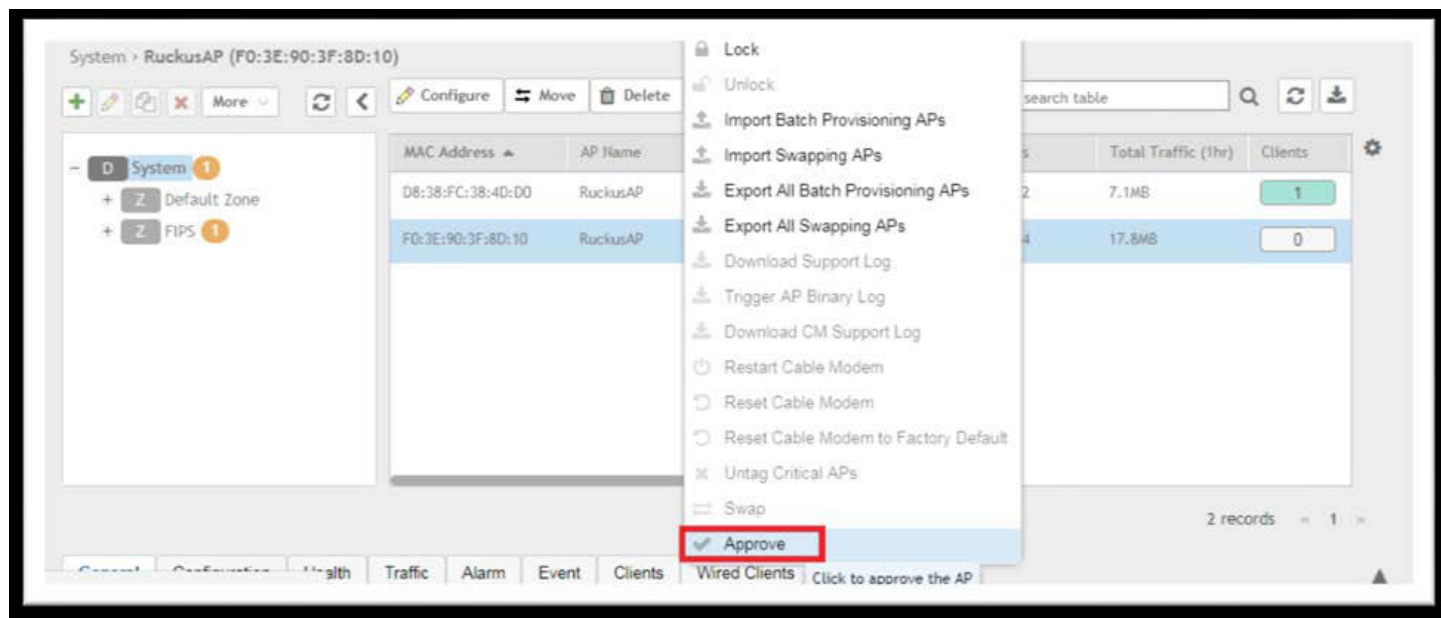
When a FIPS SKU AP joins a FIPS SKU SmartZone controller, it adopts the mode of the controller by default. Therefore, when an AP in FIPS mode joins a controller with a FIPS mode disabled, the FIPS mode in the AP is also disabled, and vice versa. If the AP and controller are running the same mode, then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

## AP Configuration in FIPS Mode

### Crypto Officer Roles and Responsibilities for AP

**FIGURE 81** 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.

#### 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 `rlclient -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, R710, R610, T610, and T710) 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 and the T710 respectively.

## 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 82** 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 83 Unavailable Upgrade Methods in FIPS Mode

**Ruckus R720 Multimedia Hotzone Wireless AP**

**Status**  
Device  
Internet  
Local Subnets  
Radio 2.4G  
Radio 5G

**Configuration**  
Device  
Internet  
Ethernet Ports

**Maintenance**  
Upgrade  
Reboot / Reset  
Support Info

**Administration**  
Management  
Diagnostics  
Log

**Maintenance :: Upgrade**

Upgrade Method: ☐ TFTP ☐ FTP ☐ Web ☒ Local

Target Selection: ☒ Firmware ☐ Device Certificate

**Local Options**  
Local File Name:  No file chosen

**WARNING:** Upgrading the firmware could take a few minutes and your network will not be available during this time. Please do NOT remove power from your Router or Adapter until the upgrade finishes.

### 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 84 HTTP and Telnet Management Access Unavailable in FIPS Mode

Status

Device

Internet

Local Subnets

Radio 2.4G

Radio 5G

Configuration

Device

Internet

Ethernet Ports

Maintenance

Upgrade

Reboot / Reset

Support Info

Administration

Management

Diagnostics

Log

Administration :: Management

Network Profile:4bss

SSH Access?☒ Enabled ☐ Disabled

SSH Port:22

No Telnet & HTTP

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

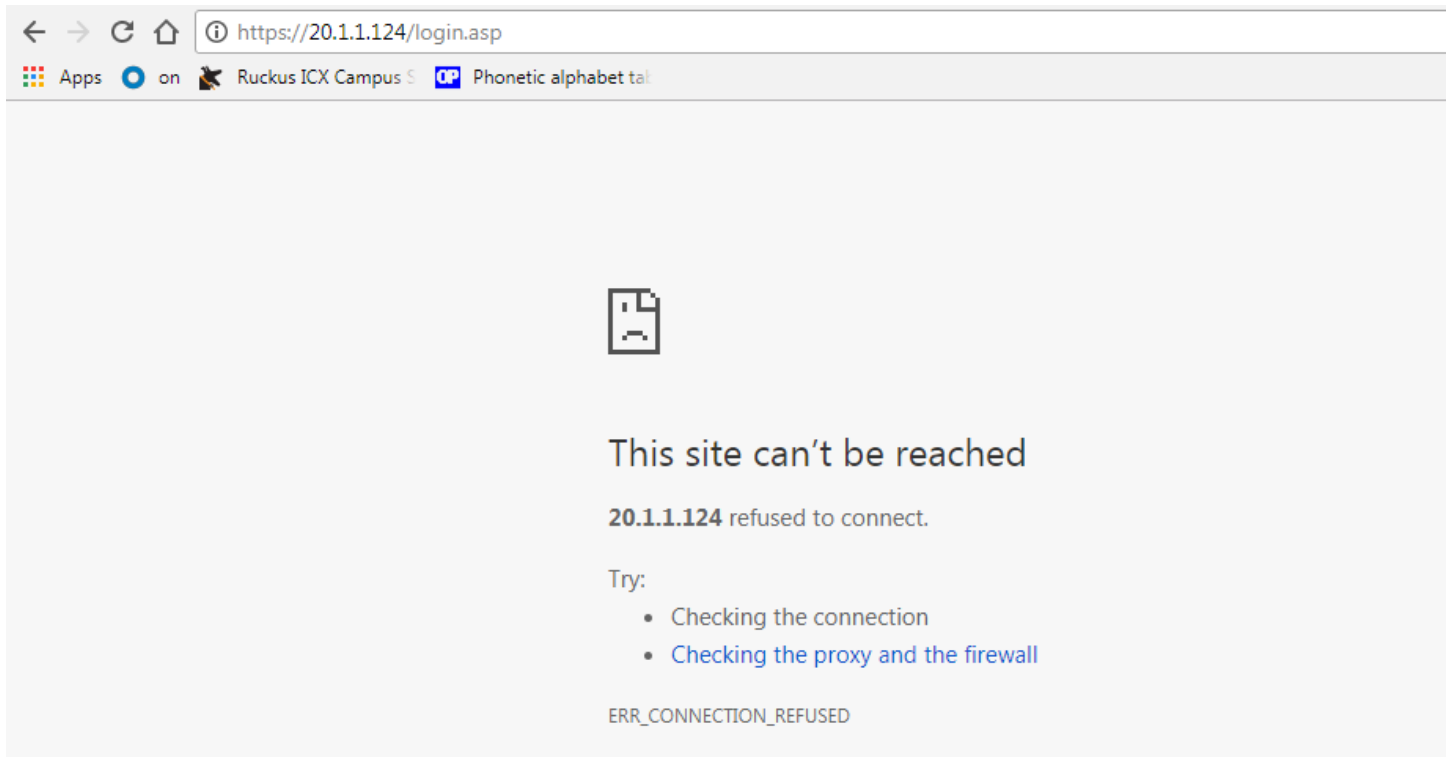
Update Settings

Restore previous settings

Web Interface Access Through HTTPS Not Supported

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

**FIGURE 85** 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 86** 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 87** 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: █

```

# X.509 Certificates

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.
  - **Organization Unit**—Name of the division, department, or section in your organization that manages network security (for example, **Network Management**).
  - **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.
11. Copy the content of the signed certificate, and then paste it into a text file.
12. Save the file.

### NOTE

You can also edit, clone, download or delete a CSR by selecting the options **Configure**, **Clone**, **Download** or **Delete** respectively.

You can configure the X.509 server certificates from a controller in a production environment.

1. Select **Systems > Certificates > SZ as a Server Certificate**, and upload the server certificate.

The **Edit Certificate** page is displayed. Configure the following.

- **Server Certificate:** Browse and select the certificate.
- **Intermediate CA Certificate:** Browse and select the certificate. You can select up to four certificates.
- **Root CA Certificate:** Browse and select the certificate.
- **Private Key:** Browse and select the key to upload.
- **Key Passphrase:** Enter the pass phrase.

**FIGURE 88** Uploading Server Certificate

Dashboard

System

General Settings

AP Settings

Switch Settings

Cluster

Maps

Certificates

Templates

Access Points

Switches

Wireless LANs

Clients

Certificate to Service Mapping

CSR

is as a Server Certificate

is as Client Certificate

is Trusted CA Certificates/Chain (external)

AP Certificate Replacement

Intra system (AP/WiFi)

## Edit Certificate: Default Certificate

You do not have the privilege to submit any changes made on this form. This form is for view only.

\* Name:

Default Certificate

Description:

Server Certificate

-----BEGIN CERTIFICATE-----

```
-----BEGIN CERTIFICATE-----
[
Version: V3
Subject: EMAILADDRESS=service@ruckuswireless.com, CN=ruckuswireless.com,
O=Ruckus Wireless, Inc., ST=CA, C=US
Signature Algorithm: SHA384withRSA, OID = 1.2.846.1.13549.1.1.12

Key: RS RSA public key: 3072 bits
modulus:
25483125299165395638256589796077986291604925002184367295564312610732381
18375399552958644360191905129763436169279608002779943891441415874782934970
111004954638618439227527026634436147621661462409917796331587193830246956
23387402114835679893508581358402317943230499625054844200190130546819344
77336010495300708991936223120127743468645212168856475566297921852345973
99156205879952145046886177246484761597876628042800162311820891545241141
7952706053901853991112948287847908135199854282974524032268284230525469388
71902899594944236282147796845028386367551623279060712850031062164854017
842746436088612684431587148865851879627993831326966568816667425649305870
```

\* Server Certificate:

Browse

Clear

[?] Intermediate CA Certificate:

Browse

Clear

[?] Root CA Certificate:

Browse

Clear

\* Private Key:

Upload

Browse

Clear

☐ Using CSR

No data available

Key Password:

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

**FIGURE 89** Importing Client Certificate

The screenshot shows the 'Import Client Certificate' page in a web application. The left sidebar contains a navigation menu with the following items: Dashboard, System, General Settings, API Settings, Switch Settings, Cluster, Maps, Certificates (highlighted in blue), Templates, Access Points, Switches, Wireless LANs, and Clients. The main content area has a breadcrumb trail: Certificate to Service Mapping > CSR > SZ as a Server Certificate > **SZ as Client Certificate** > SZ Trusted CA Certificates/Chain (external) > AP Certificate Replacement > Infra system (API/SZ-D). The main title is 'Import Client Certificate'. The form includes: a 'Name' field with a red asterisk; a 'Description' field; a 'Client Certificate' dropdown menu; a large empty rectangular box for the certificate content; a 'Client Certificate' label with a red asterisk and a checkbox; a 'Private Key' label with a red asterisk and a checkbox; 'Browse' and 'Clear' buttons for both the Client Certificate and Private Key fields; and 'Validate', 'OK', and 'Cancel' buttons at the bottom right.

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 Ruckus Controller web interface with the 'Certificates' menu item selected in the left sidebar. The main content area displays the 'Edit CA Chain Certificates: 4L\_subCAs' dialog box. The dialog has the following fields and controls:

- Name:** 4L\_subCAs
- Description:** 4 Intermediate CAs
- Intermediate CA Certificates:** A table with three rows, each containing a checkbox (checked), a 'Browse' button, and a 'Clear' button.
- Root CA Certificate:** A checkbox (checked), a 'Browse' button, and a 'Clear' button.
- Text Area:** Contains the following text:

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

 Key: Sun RSA public key, 4096 bits
 modulus:
8270869111853784099802152258986673758118953832100073008180376166749495831
2418490360799555781151935564543372586632910942429212417850709686618241238
9227069122629466514745874610083860038331237025885268069573898820738805025
4136285490313117347344585366539515005596539849390733642018945722698474511
9000423644061688590489431259630333937599678015698510878517959576974807755
9529489590376359685483353972119494025063516637861953289555566743978615801
8295079096679745208588471107342385996575784986056257052944196129235917638
```

At the bottom of the dialog 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 90** 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.

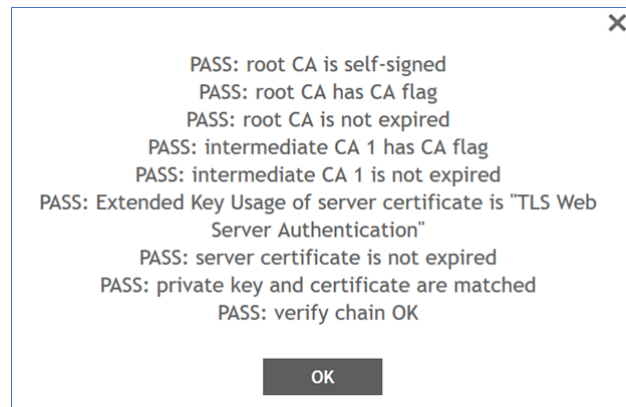
**NOTE**

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 91** Validation Message



6. Click **OK**.

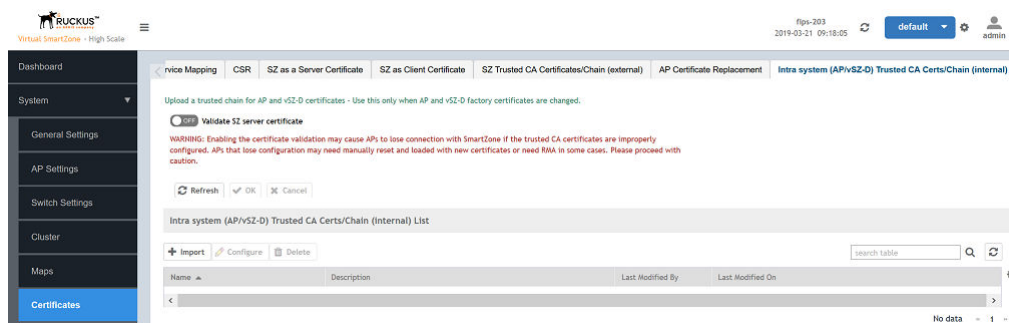
## Validating Certificates

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 92** 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.

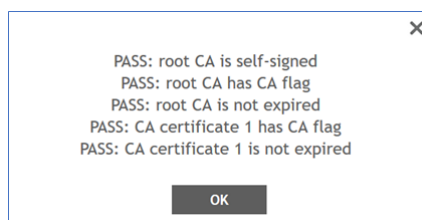
**NOTE**

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 93** 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 94** Configuring AP Discovery Time

The screenshot shows the 'Configure Group' interface. The 'Configuration' tab is selected. Under 'Client Admission Control', there are sections for '2.4 GHz Radio' and '5 GHz Radio'. Below these, the 'Protection Mode' section is highlighted with a red box. It contains two dropdown menus for 'AP Reboot Timeout': 'Reboot AP if it cannot reach default gateway after: 30 minutes' and 'Reboot AP if it cannot reach the controller after: 2 hours'. The '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 95** Uploading CA/CA-chain certificate

General Settings  
AP Settings  
Switch Settings  
Cluster  
Maps  
**Certificates**  
Templates  
Access Points  
Switches

Validate SZ server certificate

### Import CA Certs (Chain)

Name:

Description:

Intermediate CA Certificates:

|                          |                      |        |       |
|--------------------------|----------------------|--------|-------|
| <input type="checkbox"/> | <input type="text"/> | Browse | Clear |
| <input type="checkbox"/> | <input type="text"/> | Browse | Clear |
| <input type="checkbox"/> | <input type="text"/> | Browse | Clear |
| <input type="checkbox"/> | <input type="text"/> | Browse | Clear |

Root CA Certificate: ☐  Browse Clear

Validate OK Cancel

2. Click **Validate**.

**FIGURE 96** 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.

ON

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 97** Mapping Service Certificates

4. You can also upload certificate through CLI .

**FIGURE 98** 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").
2. In the command prompt, the following is displayed: Do you want to upload vSZ server certificate chain (y/n):. Enter **y** to upload the vSZ server certificate chain.

4. Press **Enter** to finish.

5. In the command prompt, the following message is displayed: Do you want to verify vSZ server certificate chain (y/n) :. Enter **y**.

## X.509 Certificates

Uploading X.509 Certificates on vSZ-D

### 6. You can upload the certificate using the CLI

```
Welcome to the RUCKUS WIRELESS vSZ-D Command Line Interface

vDP-242> en

Password:

vDP-242# config

vDP-242(config)# controller

vDP-242(config-controller) set_cert_chain

Paste your certificate sentence including BEGIN/END CERTIFICATE:

Example: -----BEGIN CERTIFICATE-----
XX
-----END CERTIFICATE-----

When you input "-----END CERTIFICATE-----" press enter to finish
Or you can type "###" and press enter to stop

-----BEGIN CERTIFICATE-----
MIIETzCCA5+gAwIBAgIJAP38SkXhlwnzMA0GCSqGSIb3DQEBCwUAMIGYMQswCQYD
VQQGEwJVUzELMAkGA1UECBMCQ0ExEjAQBgNVBAcTCVN1bm55dmFsZTEdMBSGA1UE
ChMUUnVja3VzIEdpcmcVsZXNzIEluYy4xKTAnBgkqhkiG9w0BCQEWGnNlcnpY2VA
cnVja3VzZ2lyZWxlcn3MuY29tMR4wHAYDVQQDExVDXJ0aWZpY2F0ZSBDbXR0b3Jp
dHkwHhcNMjgwOTE3MDMzNjQ1WWhcNMzMwOTEzMDMzNjQ1WjCBMDELMAkGA1UEBhMC
VVMxCzAJBgNVBAGTAkNBMRlweAYDVQQHEw1TdW5ueXZhbGUxHTAbBgNVBAoTFFJ1
Y2t1cyBXaXJlbGVzcyBJbmMuMSkwJwYJKoZIhvcNAQkBFhpzZXJ2aWNlQHJ1Y2t1
c3dpcmcVsZXNzLmNvbTEeMBwGA1UEAxMVQ2VydGhmaWNhdGUgQXV0aG9yaXR5MIIB
IjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAp3BM7P3ZEuWwuFT8+ejJ+UP0
kODr+RDMl6u9kBJqsURYpw+hRZnpN56LfeNp+GBBTBlJgKJ3RdTmK22zs9gj2JeD
AZZ72K72GEiYMikfoXXY5Nrl6Dat2MrZmxOtpqZkKtwG6SyTywtpxUnlpgzQcHx4
rXvr4ikoxKaNWYXAXJcGXMMWrPhQ91Bm3XjgB/6W8Zch+axh1jL5kPnhWLzuzLqLV
Q9+EmVE6eyc2TzMZBu0qlyciN9KgMipGluIDjZwWa7PUwnPjU12CpT4rFtWbl6W5
AyrXqAAbP0W+vLObVyQkaytkSldR9qhaC398WljHmM5mz90Cb+i4yTOcbINi8QID
AQABO4IBADCB/TAdBgNVHQ4EFgQUdJcnbgqRCKN2B/mDGYy6w12gSvkgwc0GA1Ud
IwSBxTCBwoAUDJcnbgqRCKN2B/mDGYy6w12gSvmhgZ6kgZswgZgxCzAJBgNVBAYT
AIVTMQswCQYDVQQIEwJDQTESMBAGA1UEBxMJU3Vubnl2YWxlMR0wGwYDVQQKEwRS
dWNrdXMGV2lyZWxlcn3MgSW5jLjEpMCCGCSqGSIb3DQEJARYac2VydmljZUBydWNR
dXN3aXJlbGVzcy5jb20xHjAcBgNVBAMTFUNlcnpZmljYXRlIEF1dGhvcml0eYUJ
AP38SkXhlwnzMAwGA1UdEwQFMAMBAf8wDQYJKoZIhvcNAQELBQADggEBAEUv3Kns

GJ5uNLoXWDIr2Mrt8Doh50cxRbOPHtWaxyrQyNKZpY+I08p9ET1hJD++2/7e6ES
YgtiwlwR8iZHsn1GdXgFVhz55d8pJZ2NZtbADdvhR1AJGkJ5hEclw+oX1eeKql
wrkoYjGF/+O5O24+sWfftZb1HJDrEoGeQGSOLR+iBOB0yhHQHdvR9dozcZk37aD7
Hix74KlqDRhZ5xDIRYEGSg/joXGjh9tW4Bhe3sPgX195IHCKZycs+rknyu3SfLX

Verify your certificate format now, wait a moment.

Verify certificate format done please type "end" to finish
```



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.

## Password Management

The admin password can be changed for an AP and vSZ-D from the controller interface and 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). To cover FIPS and CC password length range, the minimum password length should be 8 characters and the maximum length ranges from 8-64 characters. For example, **c@ntro!!erAdm!n#123**.

The admin 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 admin login password of the data plane is identical to the controller, so it need not be validated.

From the controller web interface go to **Administration > Admin and Roles > Administrators** and click **Configure** to modify the password.

**FIGURE 99** Configuring the Password

Name:

Default

Description:

Default Account Security

Session Idle Timeout:

OFF

15

(1-1440) minutes

Account Lockout:

OFF

Lock account for

30

(1-1440) minutes after

6

(1-100) failed authentication attempts

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

Two-Factor Authentication:

OFF

Require two-factor authentication via SMS

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

Send

Disable Inactive Accounts:

OFF

Lock admin accounts if they have not been used in the last

90

(1-1000) days

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

OK

Cancel

After the password is successfully changed, you can view the activity log from **Administration > Admin Activities**.

The account activity can be verified in the controller CLI by using the `/opt/ruckuswireless/wsg/log/web/activity.log` command.

**FIGURE 100** Sample Verification Message

|                         |                                                                                                                                         |                                                                                                                                                          |
|-------------------------|-----------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------|
| 2019-02-08 05:14:28,182 | Activity                                                                                                                                | User:[admin], Browser:[IP:10.32.138.173], Action:[Log on], Resource:[Administrator], Description:[Administrator (admin) logged on from [10.32.138.173].] |
| 2019-02-08 05:14:28,182 | User:[admin], Browser:[IP:10.32.138.173], Action:[Log on], Resource:[Administrator], Description:[The re-authentication is successful.] |                                                                                                                                                          |
| 2019-02-08 05:14:30,655 | Activity                                                                                                                                | User:[admin], Browser:[IP:10.32.138.173], Action:[Update], Resource:[Administrator], Description:[Administrator (admin) password changed.]               |
| 2019-02-08 05:14:33,635 | Activity                                                                                                                                | User:[admin], Browser:[IP:10.32.138.173], Action:[Update], Resource:[Administrator], Description:[Administrator (admin) updated.]                        |

Select **Access PointsConfigure AP Zone** to configure the AP admin login password. You can modify the settings for **AP Admin Logon**.

**FIGURE 101** Modifying AP Admin Login

[illegible]

Select **SystemCluster- Data PlanesDP/vSZ-D** to view changes to the dataplane password. . Click the **Event** tab to view the logs.

FIGURE 102 Dataplane Password Change Event Log

| Data Planes                                                                                                                                                                                                  |                  |                     |               |                                                                                                                                    |       |               |              |            |           |                    |            |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------|---------------------|---------------|------------------------------------------------------------------------------------------------------------------------------------|-------|---------------|--------------|------------|-----------|--------------------|------------|
| <div> <span>Configure</span> <span>Approve</span> <span>Delete</span> <span>More</span> </div> <div>search table</div>                                                                                       |                  |                     |               |                                                                                                                                    |       |               |              |            |           |                    |            |
| Name                                                                                                                                                                                                         | DP Type          | DP MAC Address      | Data IP       | Management/Co                                                                                                                      | Model | Serial Number | Firmware     | Managed By | DP Status | Registration State | Uptime     |
| vDP-0                                                                                                                                                                                                        | External-Virtual | 00:0C:29:4E:32:15   | 20.1.91.84    | 10.1.200.147                                                                                                                       | v5Z-D | 9720TSU6RL... | 5.1.1.3.1245 | SZ9        | Managed   | Approved           | 1d 18h 29m |
| 1 records                                                                                                                                                                                                    |                  |                     |               |                                                                                                                                    |       |               |              |            |           |                    |            |
| <div> <span>Summary</span> <span>Configuration</span> <span>Traffic &amp; Health</span> <span>DHCP/NAT</span> <span>System</span> <span>Alarm</span> <span>Event</span> <span>DP Zone Affinity</span> </div> |                  |                     |               |                                                                                                                                    |       |               |              |            |           |                    |            |
| <div> <div>Filter Off</div> <div>Password</div> </div>                                                                                                                                                       |                  |                     |               |                                                                                                                                    |       |               |              |            |           |                    |            |
| Date and Time                                                                                                                                                                                                | Code             | Type                | Severity      | Activity                                                                                                                           |       |               |              |            |           |                    |            |
| 2020/03/31 02:23:47                                                                                                                                                                                          | 99203            | Password Management | Informational | Data plane [9720TSU6RL6VXLBNTQCBMNAJLAPQ000C294E320B000C294E3215] min password length changed, source: [WebGUI], account: [admin]. |       |               |              |            |           |                    |            |
| 2020/03/31 02:18:40                                                                                                                                                                                          | 99212            | Password Management | Informational | User login into data plane [9720TSU6RL6VXLBNTQCBMNAJLAPQ000C294E320B000C294E3215], source: [10.1.200.135], Account: [admin].       |       |               |              |            |           |                    |            |
| 2020/03/31 02:18:32                                                                                                                                                                                          | 99214            | Password Management | Informational | User logout to data plane [9720TSU6RL6VXLBNTQCBMNAJLAPQ000C294E320B000C294E3215], source: [10.1.200.135], account: [admin].        |       |               |              |            |           |                    |            |
| 2020/03/31 02:17:28                                                                                                                                                                                          | 99212            | Password Management | Informational | User login into data plane [9720TSU6RL6VXLBNTQCBMNAJLAPQ000C294E320B000C294E3215], source: [10.1.200.135], Account: [admin].       |       |               |              |            |           |                    |            |
| 2020/03/31 02:17:05                                                                                                                                                                                          | 99212            | Password Management | Informational | User login into data plane [9720TSU6RL6VXLBNTQCBMNAJLAPQ000C294E320B000C294E3215], source: [Console], Account: [admin].            |       |               |              |            |           |                    |            |
| 2020/03/31 02:02:38                                                                                                                                                                                          | 99203            | Password Management | Informational | Data plane [9720TSU6RL6VXLBNTQCBMNAJLAPQ000C294E320B000C294E3215] min password length changed, source: [WebGUI], account: [admin]. |       |               |              |            |           |                    |            |
| 2020/03/31 01:58:39                                                                                                                                                                                          | 99212            | Password Management | Informational | User login into data plane [9720TSU6RL6VXLBNTQCBMNAJLAPQ000C294E320B000C294E3215], source: [Console], Account: [admin].            |       |               |              |            |           |                    |            |
| 2020/03/31 01:50:43                                                                                                                                                                                          | 99214            | Password Management | Informational | User logout to data plane [9720TSU6RL6VXLBNTQCBMNAJLAPQ000C294E320B000C294E3215], source: [Console], account: [admin].             |       |               |              |            |           |                    |            |

**NOTE**

The default username and password for controller and vSZ/vDP is admin/admin. The default username and password for AP is super/sp-admin.

## Configuring the WLAN Scheduler

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 103** Creating Time Schedules Table

Create Time Schedules Table

General Options

Schedule Name:

Schedule Description:

Schedule Table

Time Zone: (GMT+0:00) UT

|      | 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.

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

**FIGURE 104** Selecting the Scheduler Profile

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

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

Schedule Profiles: Select a sched

Band Balancing: Reload... service

QoS Map Set: OFF

SSID Rate Limiting: Uplink: 0 mbps (1-200) Downlink: 0 mbps (1-200)

DNS Server Profile: Disable

## Setting the WLAN Scheduler from the CLI

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

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

**FIGURE 105** 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
```

2. To verify that the WLAN scheduler is configured, log in to the AP.
3. Go to the *RKSCLI* mode

## Configuring the WLAN Scheduler

Setting the WLAN Scheduler from the CLI

4. Use the **get wlanlist** command to review the status of the WLANs.

**FIGURE 106** WLAN Scheduler Enabled on WLAN32

```
rkscli: get scheduler wlan32
WLAN Scheduler (Profile ID=1)
Timezone = GMT+0
Current UTC time = Thu Jan 10 09:09:29 2019
Current local time = Thu Jan 10 09:09:29 2019
Scheduler Table:
+-----+
| | 0|1|2|3|4|5|6|7|8|9|10|11|12|13|14|15|16|17|18|19|20|21|22|23|
+-----+
|Sun|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|
+-----+
|Mon|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|
+-----+
|Tue|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|
+-----+
|Wed|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|
+-----+
|Thu|0|0|0|0|0|0|0|0|0|0|1|0|0|0|0|0|0|0|0|0|0|0|0|
+-----+
|Fri|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|
+-----+
|Sat|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|
+-----+
There are four bits in one hour to control the WLAN interface's state.
Each bit represents a quarter of an hour and converted to a hex value.
For example: 'A' => '1010' means WLAN is available in the 2nd and the 4th quarter.
OK

rkscli: get wlanlist
name status type wlanID radioID bssid ssid

wlan0 up AP wlan0 0 0c:f4:d5:07:c2:78 1@Eng_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 up AP wlan32 1 0c:f4:d5:07:c2:7c 1@Eng_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
OK
rkscli:
```

**FIGURE 107** WLAN Scheduler Disabled on WLAN32

```
rkscli: get scheduler wlan32
WLAN Scheduler (Profile ID=1)
Timezone = GMT+0
Current UTC time = Thu Jan 10 09:15:24 2019
Current local time = Thu Jan 10 09:15:24 2019
Scheduler Table:
+-----+
| | 0|1|2|3|4|5|6|7|8|9|10|11|12|13|14|15|16|17|18|19|20|21|22|23|
+-----+
|Sun|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|
+-----+
|Mon|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|
+-----+
|Tue|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|
+-----+
|Wed|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|
+-----+
|Thu|0|0|0|0|0|0|0|0|0|0|1|0|0|0|0|0|0|0|0|0|0|0|0|
+-----+
|Fri|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|
+-----+
|Sat|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|
+-----+
There are four bits in one hour to control the WLAN interface's state.
Each bit represents a quarter of an hour and converted to a hex value.
For example: 'A' => '1010' means WLAN is available in the 2nd and the 4th quarter.
OK
```

**FIGURE 108** WLAN down in AP and Not Broadcasting After the Scheduled Time

```
rksccli: get wlanlist
```

| name          | status | type | wlanID  | radioID | ssid                                   |
|---------------|--------|------|---------|---------|----------------------------------------|
| wlan0         | down   | AP   | wlan0   | 0       | 00:00:00:00:00:00 lqEng_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 lqEng_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           |

**FIGURE 109** Event Raised for WLAN Scheduler

| Date and Time     | Code | Type                  | Severity     | Activity                                                                                                                                                   |
|-------------------|------|-----------------------|--------------|------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 2020/04/01 13:... | 122  | 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:... | 122  | 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 110** Logs Showing Client Joining AP at the Scheduled Time

```
Apr 1 09:27:26 RuckusAP daemon.debug hostapd: wlan32: STA 98:46:0a:a2:ba:74 WPA: wlan32: WPA: handle_sm_ue_context rsp
Apr 1 09:27:26 RuckusAP daemon.debug hostapd: wlan32: STA 98:46:0a:a2: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:a2:ba:74 WPA: wlan32: WPA: start authentication
Apr 1 09:27:26 RuckusAP daemon.debug hostapd: wlan32: STA 98:46:0a:a2: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:a2: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:a2: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:a2:ba:74 WPA: wlan32: WPA: UE connects using default PSK
Apr 1 09:27:26 RuckusAP daemon.debug hostapd: wlan32: STA 98:46:0a:a2: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:a2: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:a2:ba:74 IEEE 802.11: IEEE 802.11: add station:98:46:0a:a2:ba:74 to ruob
Apr 1 09:27:26 RuckusAP daemon.debug hostapd: wlan32: STA 98:46:0a:a2:ba:74 IEEE 802.11: wlan32: IEEE 802.11: rks_dot11_scache_update uplink_ratelimit:0kbps, downlink_ratelimit:0kbps
Apr 1 09:27:26 RuckusAP daemon.info hostapd: @202,clientJoin,"apMac":"c8:08:73:26:92:60","clientMac":"98:46:0a:a2:ba:74","ssid":"!!!!!!WIPS/WIDS//OPEN+WPA2","bssid":"c8:08:73:26:92:60","userid":"","wlanid":"1","iface":"wlan32","tenantUUID":"839f87c6-d116-497e-afce-aa8157abd30c","apName":"RuckusAP","vlanid":"1111","radio":"a/n/ac","encryption":"WPA2-AES","instantaneous_rssi":"0","Xpwt":"0"
Apr 1 09:27:26 RuckusAP daemon.debug hostapd: IEEE 802.11: Start to update ruob entry
Apr 1 09:27:26 RuckusAP daemon.debug hostapd: STA 98:46:0a:a2:ba:74 IEEE 802.11: IEEE 802.11: rks_set_sta_wlan32 set ac(lid:0) & firewall profile(lid:0) for station ok:98:46:0a:a2:ba:74
Apr 1 09:27:26 RuckusAP daemon.warn hostapd: STA 98:46:0a:a2:ba:74 IEEE 802.11: IEEE 802.11: rsmc_ruob_setSTAAttachedPolicies Firewall index 1 applied for station
Apr 1 09:27:26 RuckusAP daemon.debug hostapd: STA 98:46:0a:a2:ba:74 IEEE 802.11: IEEE 802.11: rks_set_sta_utp_acl wlan32 set utp_acl(filter_id:0, conf->sta_utp_acl_list_id:1, firewall profile id:1) for station ok:98:46:0a:a2:ba:74
Apr 1 09:27:26 RuckusAP daemon.debug hostapd: wlan32: STA 98:46:0a:a2: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 RUOB
Apr 1 09:27:26 RuckusAP daemon.notice hostapd: wlan32: AP-STA-CONNECTED 98:46:0a:a2:ba:74
Apr 1 09:27:26 RuckusAP daemon.debug hostapd: wlan32: STA 98:46:0a:a2: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:a2:ba:74 IEEE 802.11: wlan32: 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:a2: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, phy mode 10, ni_flags 0x0621b006, vht_mcs_set 0x00fa, ht_mcs_set 0x0fff, legacy_rate_set 0x02a0f8
Apr 1 09:27:28 RuckusAP local0.alert dpconfmgr: subject from server cert: /C=US/ST=CA/L=Sunnyvale/O=Ruckus Wireless Inc./emailAddress=service@ruckuswireless.com/CN=97H0TW7QXN24NN4IH02109P1CKQ00C29F64EEB000C29F64EFS
Apr 1 09:27:28 RuckusAP local0.alert dpconfmgr: subject from server_list:
```

## Terminating Sessions

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

- To configure the timeout value on the controller web interface, select **Administration > Admin and Roles > Administrators**
- Select the administrator account and click **Configure**.

The **Edit Administrator Account** page displays.

## Terminating Sessions

### Terminating Sessions for Non-Admin Users

3. Set the **Session Idle Timeout** value from 1 to 1440 minutes.

**FIGURE 111** Session Idle Timeout Configuration

The screenshot shows the Ruckus SmartZone GUI. On the left, the 'Administration' menu is expanded, and 'Admins and Roles' is selected. The 'Administrators' tab is active, showing a list of administrators. The 'admin' user is selected, and the 'Edit Administrator Account: admin' dialog is open. In the dialog, the 'Session Idle Timeout' is set to 15 minutes, which is highlighted with a red box. Other settings like 'Account Lockout' and 'Password Expiration' are also visible.

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.

4. From the command prompt, set the value as shown:

**FIGURE 112** 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.

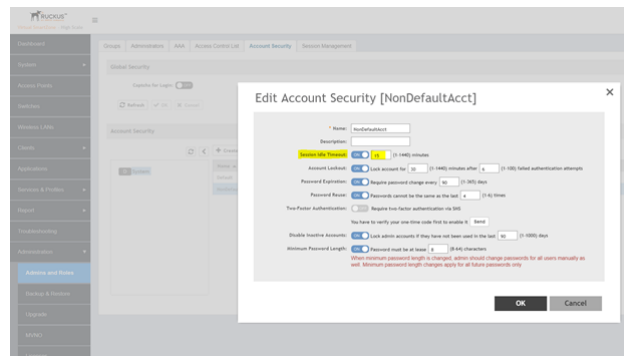
1. Select **Administration > Admin and Roles > Account Security** to configure the timeout value on the controller web interface from the security profile.
2. Click **Create**.



3. 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.

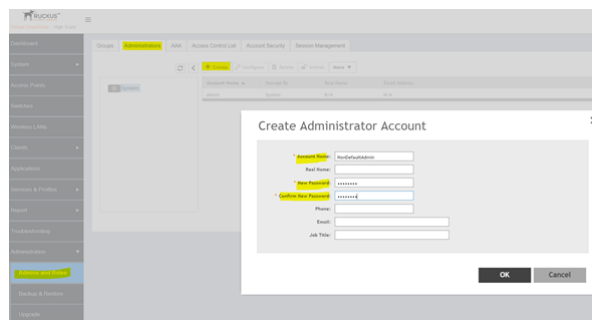
**FIGURE 113** Session Timeout Configuration from the Security Profile



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

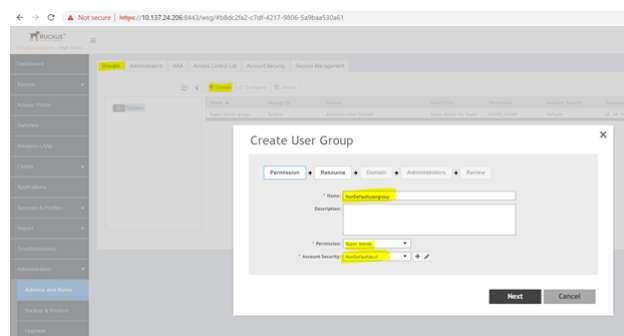
4. Select **Administration > Admin and Roles > Administrator** to create a non-admin user account.

**FIGURE 114** 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 115** 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.

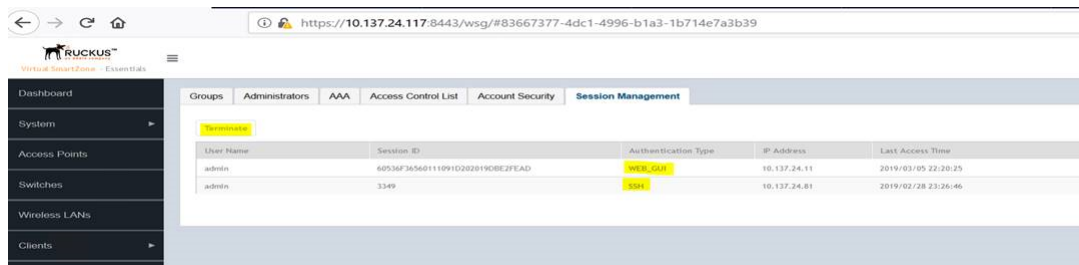
1. From the controller web interface, select **Administration > Admin and Roles > Session Management**
2. Select the administrator session you want to discontinue and click **Terminate**.

The **Password Confirmation** page displays.

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 116** Sample Session Termination for Web Interface Session.



**FIGURE 117** Sample Session Termination for CLI Session.

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

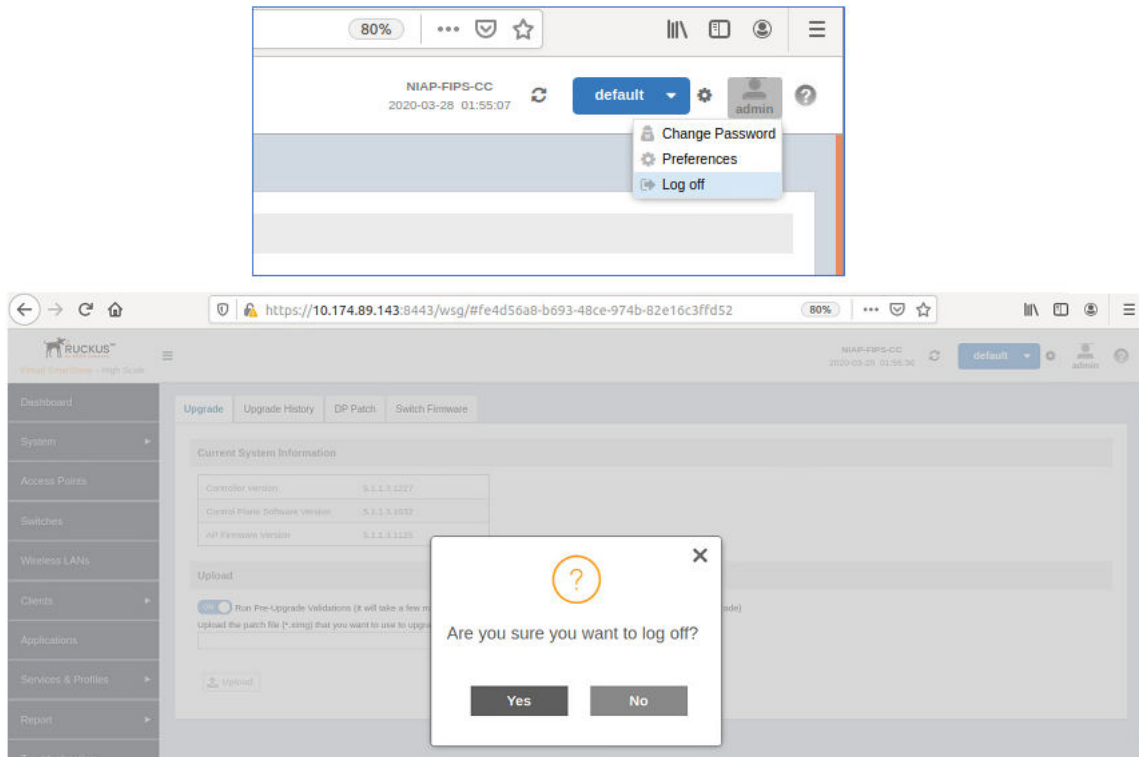
en
Please wait. CLI initializing...

Welcome to the Ruckus SmartZone 100 Command Line Interface
Version: 5.1.1.0.342

VSZ100>
VSZ100> en
VSZ100> Password: *****
VSZ100# Connection to 10.1.200.102 closed by remote host.
Connection to 10.1.200.102 closed.
```

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

**FIGURE 118** Logging out from the UI



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

**FIGURE 119** Logging out from the SSH session

```
[C:\>] ssh admin@10.174.89.143

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

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

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

SZ9> en
Password: *****

SZ9# exit

SZ9> exit

Connection closing...Socket close.
Connection closed by foreign host.

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

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

## Terminating Sessions

### Terminating Administrator Sessions

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

**FIGURE 120** 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 121** 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 Accounts

Administrator accounts can be forcefully locked when there are repeated attempts to access the account by unauthorized users. This situation typically applies when the entered user name is correct, but the password is incorrect. You can configure the number of unsuccessful attempts a user can try to log in to the account before the account is 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 displays.

**FIGURE 122** Configuring the Account Lock

3. Click **ON** to 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 is displayed.
5. Click **OK**.

You can modify the account lock settings from the security profile also. Select **Administration > Admins and Roles > Account Security**, 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.

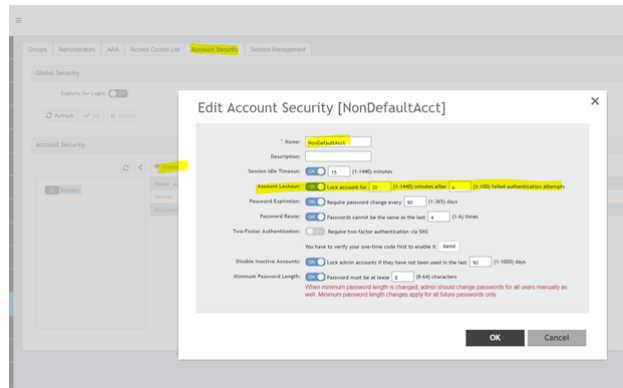
1. From the controller web interface, select **Administration > Admin and Roles > Account Security**.
2. Click **Configure**.

## Locking Accounts

### Locking Non-Administrator Accounts

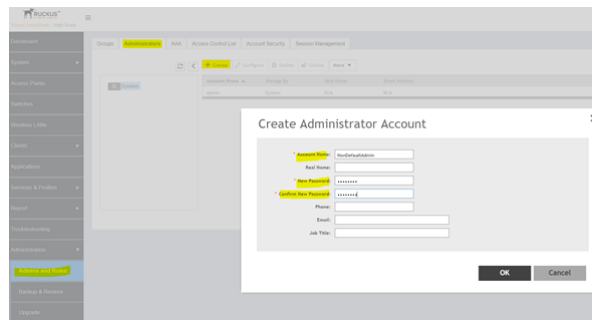
3. Click **ON** to enable **Account Lockout** and enter the account lockout time and number of failed authentication attempts.

**FIGURE 123** Account Lockout Configuration from the Security Profile



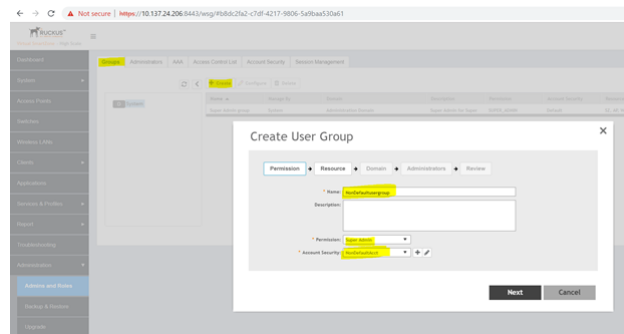
4. Select **Administration > Admin and Roles > Administrators** to create a non-administrator user account.

**FIGURE 124** Creating a Non-Administrator Account



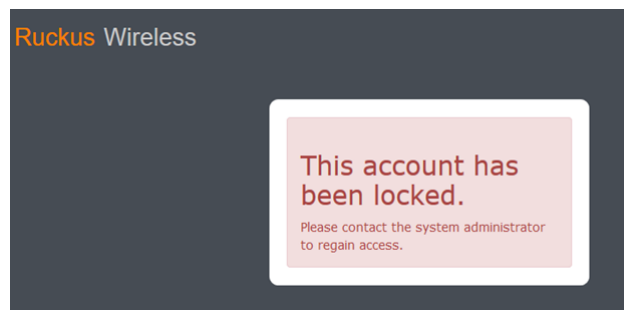
5. Select **Administration > Admin and Roles > Groups** to create the user group to map the non administrator user to the security profile

**FIGURE 125** Creating User Groups



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

**FIGURE 126** Locked User Account



**FIGURE 127** 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 :
Login failureConnection to 192.168.11.67 closed.
[root@IRAWAT ~]#
```

**FIGURE 128** 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 and CLI.

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

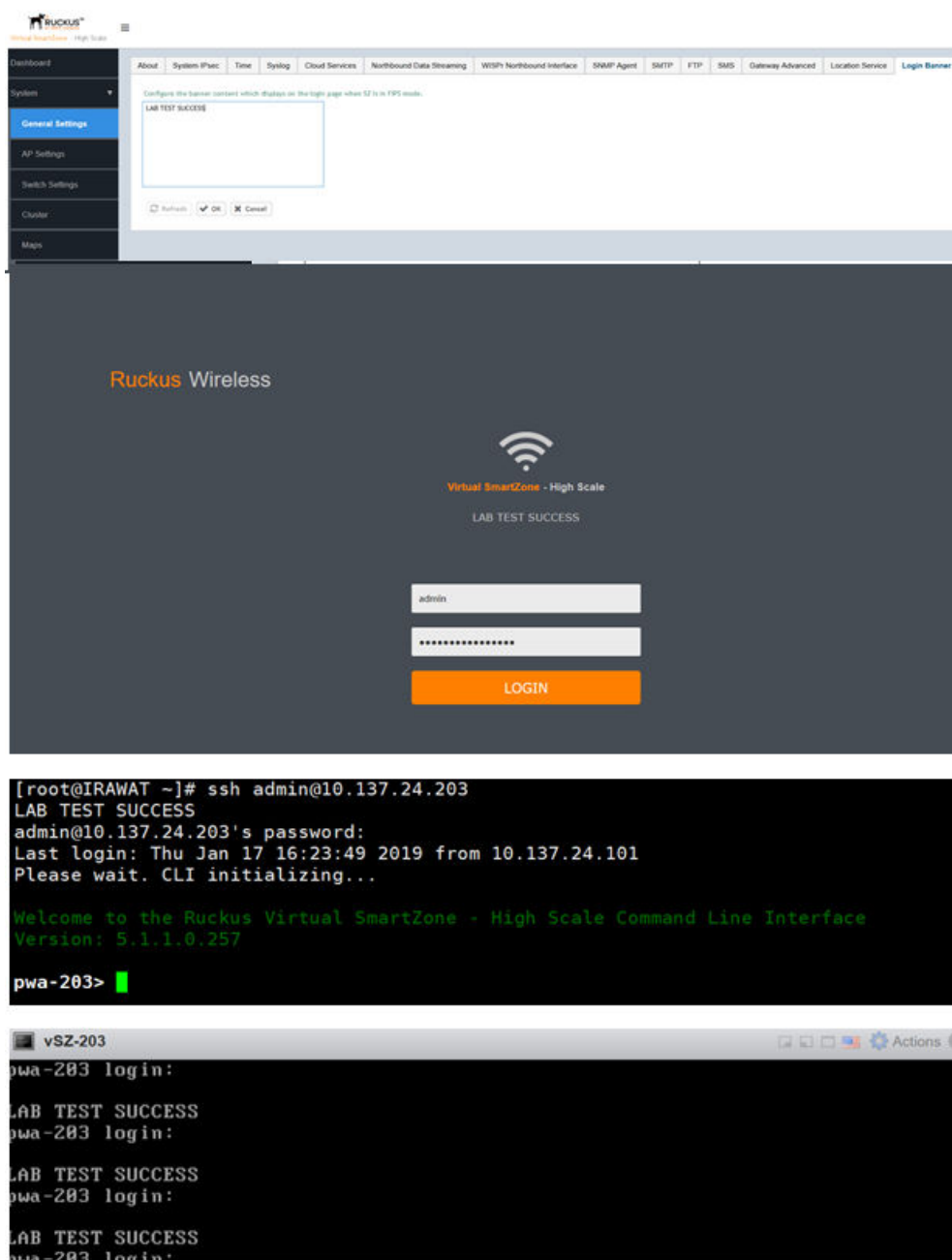
### NOTE

The **Setting Up the Login Banner** is not applicable to Dataplane.



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

**FIGURE 129** Login Banner: Web Interface and CLI

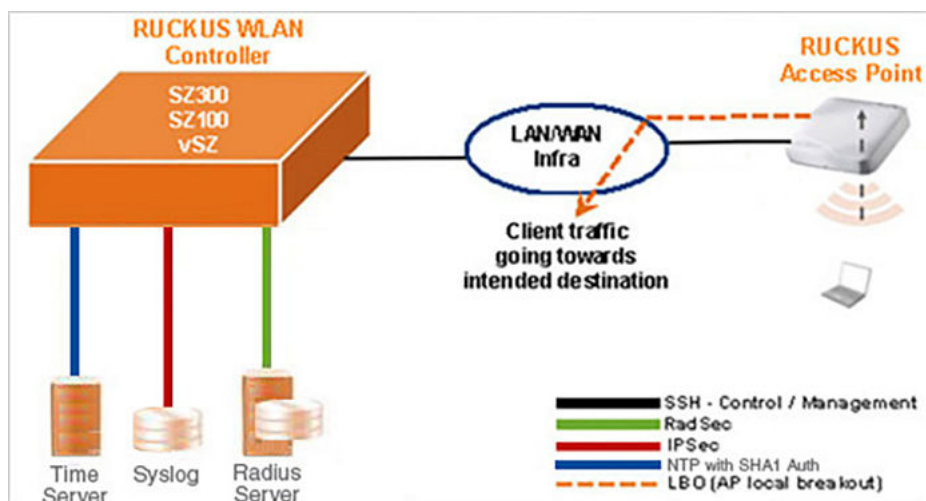


## Deployment Models

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.

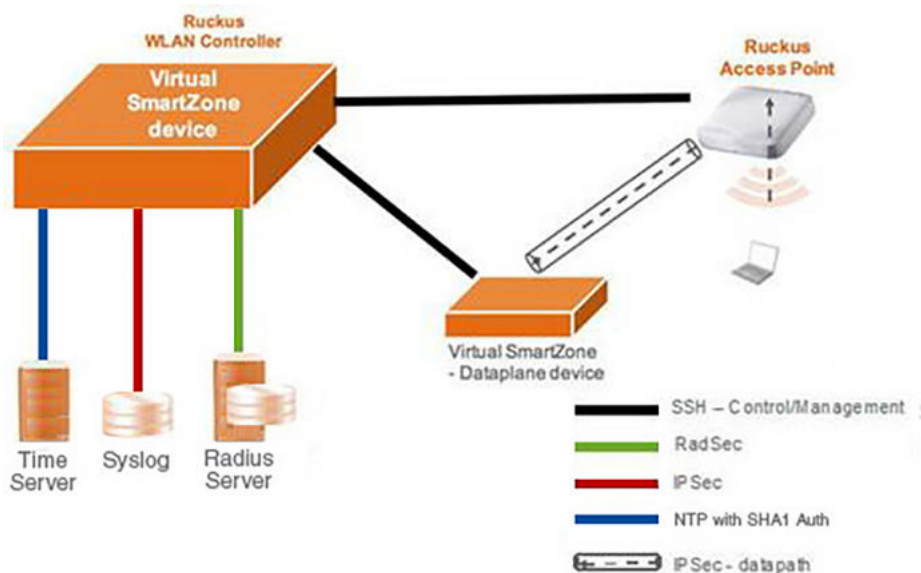
**Distributed Deployment Model** In distributed deployment model client traffic directly reaches the intended destination from the AP. All Ruckus Wireless Controllers and APs support this deployment model as seen in the below figure.

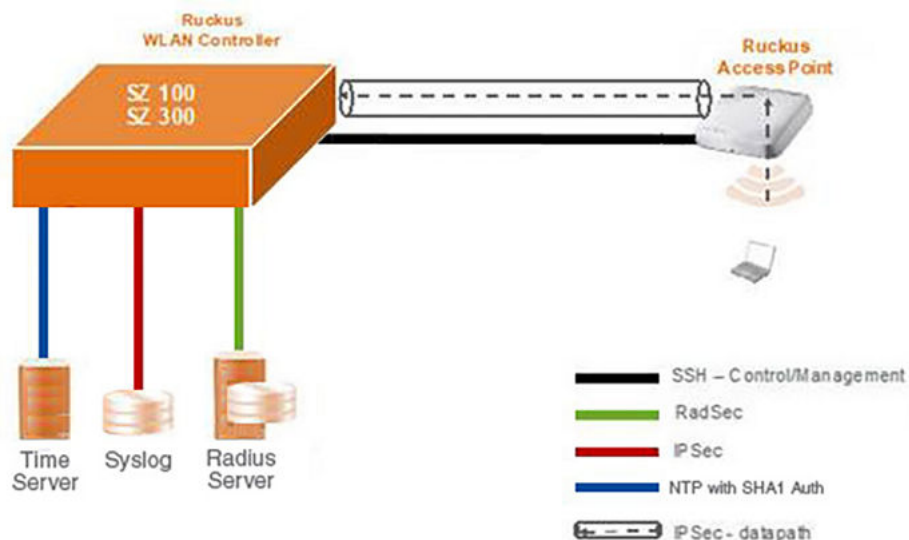
**FIGURE 130** Distributed Deployment Model



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

**FIGURE 131** Centralized Deployment Model with hardware



**FIGURE 132** 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 the WLAN

You can configure the Ruckus GRE tunnel profile and IPsec profile in the WLAN to manage AP traffic. Ruckus GRE and IPsec is a configuration of IPsec tunnel between AP and HW SZ in centralize HW deployment, AP and vSZ-D in centralize virtualize deployment.

### Creating an IPsec Profile

1. Go to **Services & Profiles > Tunnels and Ports**
2. Select the **IPsec** tab, and then select the zone for which you want to create the profile.

3. Click **Create**.

The **Create IPsec Profile** page appears.

**FIGURE 133** Creating an IPsec Profile

**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 description of the profile.
- Tunnel Mode : select Ruckus GRE.
- Under Security Association select either the required option for IKE Proposal Type: AES128-SHA1-MODP2048 or AES256-SHA384-ECP384.
- Under Security Association select either one of the supported options for ESP Proposal Type : 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, AES256-SHA384-ECP384 for ESP however if AES256-SHA384-ECP384 selected for IKE only AES256-SHA384-ECP384 will be allowed for ESP.

- Configure the required duration for IKE and ESP Key's under Rekey options.

5. Click **OK**.

### Creating a Ruckus GRE Profile

6. Go to **Services & Profiles > Tunnels and Ports**.
7. Select the **Ruckus GRE** tab, and then select the zone for which you want to create the profile.
8. Click **Create**.

The **Create Ruckus GRE Profile** page appears.

**FIGURE 134** Creating a Ruckus GRE Profile

9. Type a name for the profile in the **Name** box.
10. Type a description for the profile in the **Description** box.
11. Select Ruckus Tunnel mode as GRE.
12. Select Tunnel encryption as Disable. Select Tunnel MTU as Auto  
MTU is the size of the largest protocol data unit that can be passed on the controller network.
13. Set the maximum transmission unit (MTU) for the tunnel using one of the **Tunnel MTU** options:
  - Click the **Auto** radio button. This is the default option.
  - Click the **Manual** radio button and enter the maximum number of bytes. For IPv4 traffic the range is from 850-1500 bytes, for IPv6 traffic the range is from 1384 to 1500 bytes.

MTU is the size of the largest protocol data unit that can be passed on the controller network.

14. Click **OK**.

You have created the Ruckus GRE profile.

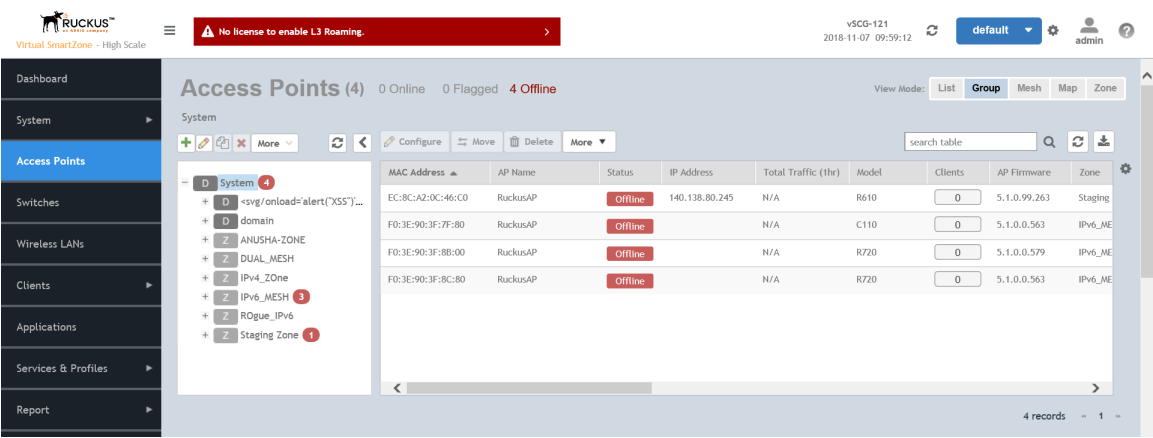
### Creating an AP Zone

15. Create an AP zone with the appropriate Ruckus GRE and IPsec profiles. Go to **Access Points**.

To create an AP zone

- a. On the menu, click **Access Points**. The figure below appears.

FIGURE 135 Access Points




- b. From the **System** tree, select the location where you want to create the zone (for example, System or Domain), and then click .

FIGURE 136 Create Groups

Create Group

Name:

Description:

Type: ☐ Zone ☒ AP Group

Parent Group: zone1

Configuration

General Options

Location: ☐ override  (example: Starbucks)

Location Additional ☐ override  (example: 440 N. 1st St. Suite 100, San Jose, CA 95131)

OK

Cancel

- c. Configure the zone by completing the settings listed in the table below.
- d. Click **OK**.

TABLE 5 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 then 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.                                                                                                                                             |
| <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. <p><b>NOTE</b><br/>This option is supported only on vSZ-H.</p>                                      | 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. <p><b>NOTE</b><br/>Cluster redundancy is supported only on SZ300 and vSZ-H.</p>                    | 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 belongs.                  | 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.                                                                                                                                                                                                  |

**TABLE 5** AP Zone Details (continued)

| Field                                | Description                                                                                                                                                                                                                                                     | Your Action                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|--------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>5.8 Ghz Channels</b>              | <p>Provides C-band support for all Outdoor APs and the following Indoor APs: R310, R510, R710 .</p> <p><b>NOTE</b><br/>This feature is available only for countries that support 5.8Ghz channel. For example, UK provides indoor AP—5.8Ghz channel support.</p> | Select the <b>Allow 5.8Ghz channels</b> check box.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>5.8 Ghz Channels License</b>      | <p>Enables full TX Power Adjustment for C-band channels.</p> <p><b>NOTE</b><br/>This feature is supported only for UK.</p>                                                                                                                                      | 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.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>Radio Options b/g/n (2.4 GHz)</b> | Indicates the configuration options for the 2.4 GHz radio.                                                                                                                                                                                                      | <p>Select the following options:</p> <ul style="list-style-type: none"> <li>• <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.</li> <li>• <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.</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.</li> </ul> <p><b>NOTE</b><br/>Ensure that <b>Background Scan</b> is enabled.</p> <ul style="list-style-type: none"> <li>• <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.</li> </ul> <p><b>NOTE</b><br/>If you choose Min, the transmit power is set to 0dBm (1mW) per chain for 11n APs, and 2dBm per chain for 11ac APs. If you choose Max, the transmit power is set to the max allowable value according to the AP's capability and the operating country's regulations.</p> |



TABLE 5 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.                    | <p>Select the following options:</p> <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.</li> </ul> <p><b>NOTE</b><br/>Ensure that <b>Background Scan</b> is enabled.</p> <ul style="list-style-type: none"> <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.</li> </ul> <p><b>NOTE</b><br/>If you choose Min, the transmit power is set to 0dBm (1mW) per chain for 11n APs, and 2dBm per chain for 11ac APs. If you choose Max, the transmit power is set to the max allowable value according to the AP's capability and the operating country's regulations.</p> |
| <b>Configuration &gt; AP GRE Tunnel Options</b> |                                                                             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>Tunnel Type</b>                              | Indicates the supported tunnel type (Ruckus GRE, SoftGRE and SoftGRE+IPsec) | <p>Choose :</p> <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.</li> </ul> </li> </ul> <p><b>NOTE</b><br/>If you select <b>AAA Affinity</b>, you must enable <b>Force Disassociate Client</b> while creating the Soft GRE Profile.</p> <ul style="list-style-type: none"> <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 5** 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: <b>0</b> through <b>100</b>.</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 5** 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><br/>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: <ul style="list-style-type: none"> <li>a. Enter the <b>Venue Name</b>.</li> <li>b. Enter the <b>Server Address</b>.</li> <li>c. Enter the <b>Port number</b>.</li> <li>d. Enter the <b>Password</b>.</li> </ul> </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>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |

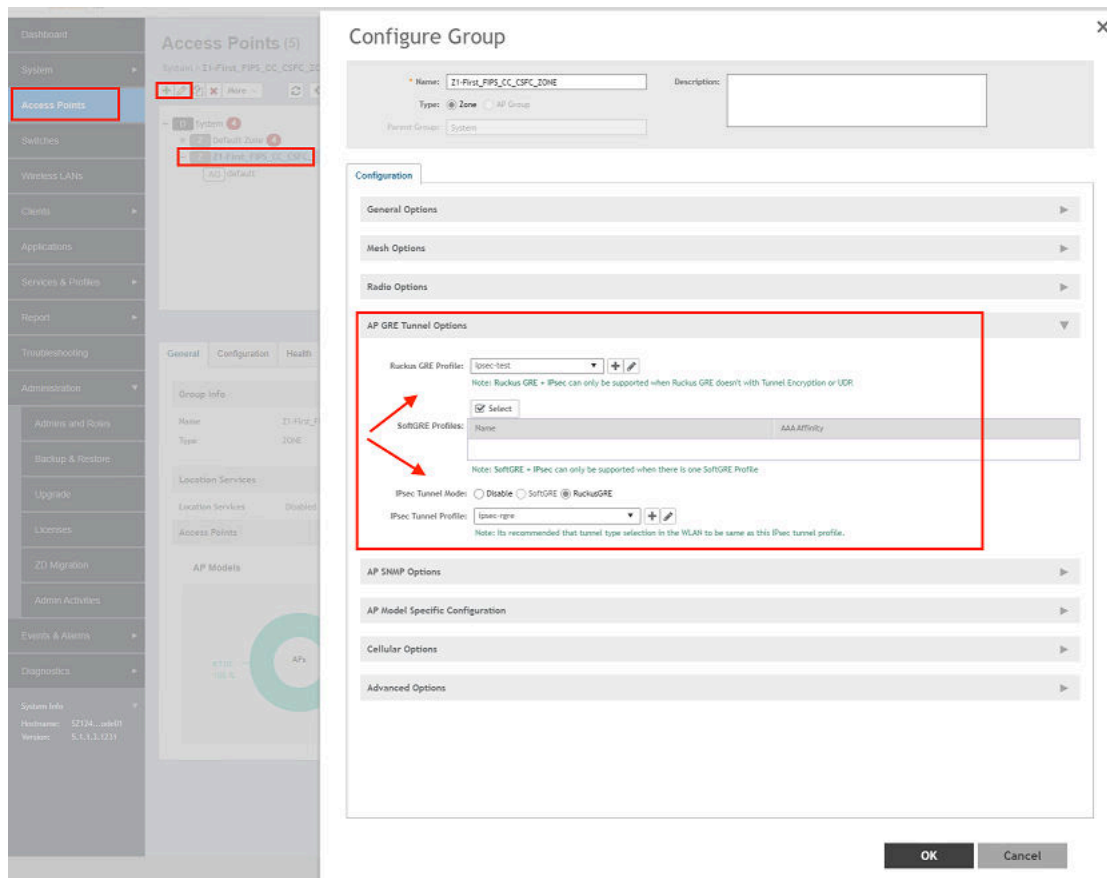
**NOTE**

RuckusGRE over IPsec is supported in transport mode only. It provide support of RSA.

16. Select the FIPS zone and click the + icon to configure the AP GRE Tunnel Options from the **Configuration** tab.

- For Ruckus GRE Profile select proper GRE profile configured previously.
- Select Ruckus GRE option for IPSEC tunnel mode.
- Select proper configured IPSEC tunnel profile for Ipsec Tunnel profile option.

**FIGURE 137** AP GRE Tunnel Configurations



17. Go to **Wireless LAN**.

18. Select the zone. The **Creating WLAN Configuration** page displays.

19. 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.

### NOTE

Peer reference identifiers are not configurable, SZ will autogenerate reference identifiers to AP and DP.

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.

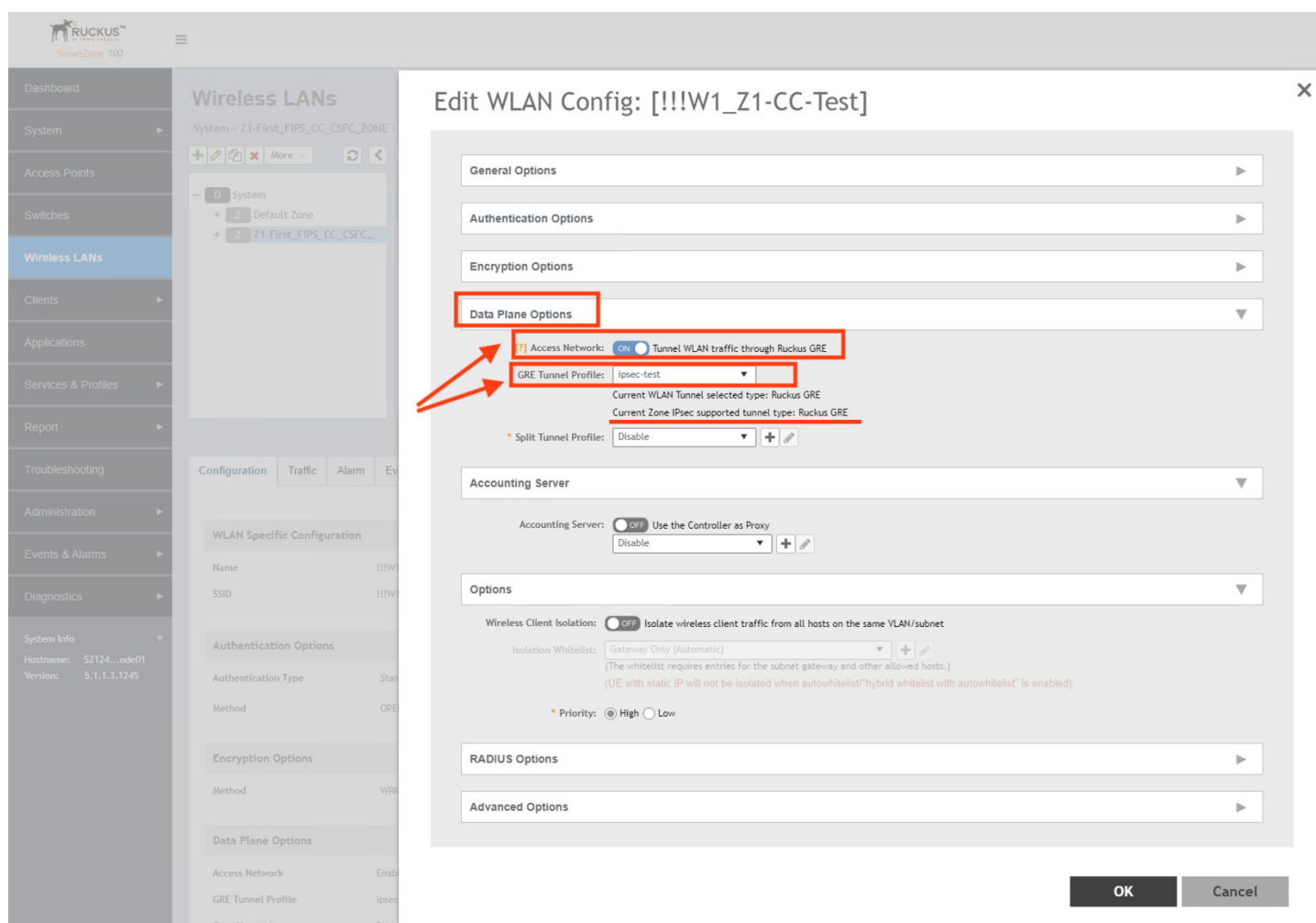
### NOTE

The IPsec connection between AP and vSZ-D is recovered automatically and no manual intervention required

### Map Ruckus GRE and IPsec profile to Wlan

- Go to Wireless LANs
- Select the Zone and either create a new WLAN or edit the existing WLAN.
- Within WLAN config, under the Data Plane Options:
  - Select to enable the Access Networks.
  - Map the Ruckus GRE profile created in above steps.
  - Once you enable and select Ruckus GRE, IPsec profile is applied based on AP zone configuration.

**FIGURE 138** WLAN configuration



## System IPsec

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:

- 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 139 System IPsec Settings

RUCKUS™

an AXIOM company

Virtual SmartZone - Essentials

Dashboard

System

General Settings

AP Settings

Switch Settings

Cluster

Maps

Certificates

Templates

Access Points

Switches

Wireless LANs

Clients

AboutSystem IPsecTimeSyslogCloud ServicesNorthbound Data StreamingWISPr Northbound InterfaceSNMP Agent

ONEnable IPsec

\* Security Gateway:10.1.200.100

\* Subnet:18.18.18.0/24

\* Type: ☒ Preshared Key ☐ Certificate

\* Preshared Key:

IKE

\* Encryption Algorithm: AES256

\* Integrity Algorithm: SHA384

\* Rekey Time: ☐ Disable 4 hour

ESP

\* Encryption Algorithm: AES256

\* Integrity Algorithm: SHA384

\* Rekey Time: ☐ Disable 4 hour

Tunnel State

Tunnel State: No tunnel is established

Reconnect

FIGURE 140 Enabling IKE Rekeying

ONEnable IPsec

\* Security Gateway:10.1.200.135

\* Subnet:17.1.1.1/24

\* Type: ☒ Preshared Key ☐ Certificate

\* Preshared Key: .....

IKE

\* Encryption Algorithm: AES128

\* Integrity Algorithm: SHA1

\* Rekey Time: ☐ Disable 4 minute

ESP

\* Encryption Algorithm: AES128

\* Integrity Algorithm: SHA1

\* Rekey Time: ☒ Disable



**FIGURE 141** Enabling ESP Rekeying

The screenshot shows the 'Enable IPsec' configuration window. At the top, there is a 'GUI' tab and an 'Enable IPsec' toggle. Below this, the 'Security Gateway' is set to '10.1.200.135' and the 'Subnet' is '17.1.1.1/24'. The 'Type' is set to 'Preshared Key' (selected with a radio button) and 'Certificate' (unselected). The 'Preshared Key' field contains a series of dots. The 'IKE' section has 'Encryption Algorithm' set to 'AES192', 'Integrity Algorithm' set to 'SHA1', and 'Rekey Time' set to 'Disable' (checked). The 'ESP' section has 'Encryption Algorithm' set to 'AES192', 'Integrity Algorithm' set to 'SHA1', and 'Rekey Time' set to '4 hour' (unchecked). The 'Rekey Time' field in the ESP section is highlighted with a red rectangle.

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.

**FIGURE 142** System IPsec Settings

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 143** 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:
```

## 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**.

## System IPsec

### Configuring IKE and ESP Rekeying Separately

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

**FIGURE 144** Enabling IPsec

The screenshot shows the 'System IPsec' configuration page. On the left is a navigation menu with 'Dashboard', 'System' (selected), 'General Settings', 'AP Settings', and 'Switch Settings'. The main content area has tabs for 'About', 'System IPsec' (active), 'Time', 'Syslog', 'Cloud Services', and 'Northbound Data Streaming'. Under the 'System IPsec' tab, there is a toggle for 'Enable IPsec' which is turned 'ON'. Below this are fields for 'Security Gateway', 'Subnet', 'Type' (with radio buttons for 'Preshared Key' and 'Certificate'), and 'Preshared Key'.

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

**FIGURE 145** Enabling IKE Rekeying

This screenshot is a zoomed-in view of the 'System IPsec' configuration page, focusing on the 'IKE' and 'ESP' sections. The 'Enable IPsec' toggle is 'ON'. The 'Security Gateway' is '10.1.200.135' and the 'Subnet' is '17.1.1.1/24'. The 'Type' is 'Preshared Key'. The 'Preshared Key' field contains seven dots. The 'IKE' section has 'Encryption Algorithm' set to 'AES128' and 'Integrity Algorithm' set to 'SHA1'. The 'Rekey Time' for IKE is set to '4' minutes, with a red box highlighting the '4' and 'minute' dropdown. The 'ESP' section has 'Encryption Algorithm' set to 'AES128' and 'Integrity Algorithm' set to 'SHA1'. The 'Rekey Time' for ESP is set to 'Disable'.

- c) In the ESP section, enable ESP Rekeying

**FIGURE 146** Enabling ESP Rekeying

The screenshot shows the 'System IPsec' configuration page. The 'Enable IPsec' toggle is turned on. Under the 'IKE' section, the 'Rekey Time' is set to 'Disable'. Under the 'ESP' section, the 'Rekey Time' is set to '1 minute', which is highlighted with a red rectangle.

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

**FIGURE 147** Successful IPsec Tunnel Creation

The screenshot shows the 'Tunnel State' page. The tunnel state is 'ipsec: #2, ESTABLISHED, IKEv2, a447e6af48368ac7\_i\* cddb4bbe27e0ac3\_r local '10.1.200.143' @ 10.1.200.143[4500] remote '10.1.200.100' @ 10.1.200.100[4500] AES\_CBC-128/HMAC\_SHA1\_96/PRF\_HMAC\_SHA1/ECP\_384 established 309s ago net: #7, reqid 2, INSTALLED, TUNNEL, ESP:AES\_CBC-128/HMAC\_SHA1\_96/ECP\_384 installed 38s ago, rekeying in 17s, expires in 28s'. The text 'rekeying in 17s, expires in 28s' is highlighted with a red rectangle. A 'Reconnect' button is visible in the top right corner.

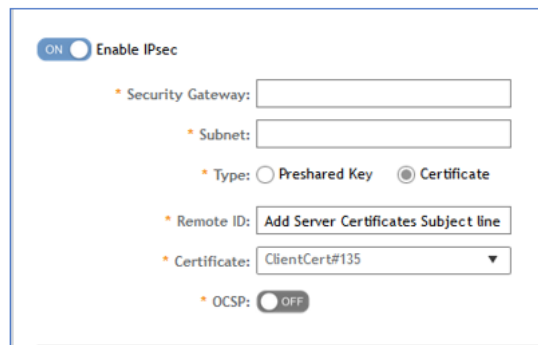
4. If **Certificates** is selected, perform the following.

a) In the Certificate field, upload 'SZ as Client Certificate' and 'CA n sub-CA Certificate'.

b) In the Remote ID field, 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 148** Adding Certificate



The screenshot shows the IPsec configuration interface. At the top, there is a toggle switch labeled "ON" and "Enable IPsec". Below this, there are several fields and options:

- \* Security Gateway: [Empty text box]
- \* Subnet: [Empty text box]
- \* Type: ☐ Preshared Key ☒ Certificate
- \* Remote ID: [Add Server Certificates Subject line]
- \* Certificate: [ClientCert#135]
- \* OCSP: ☐ OFF

## Configuring System Time

The controller uses three external Network Time Protocol (NTP) servers to synchronize the times across cluster nodes and managed access points.

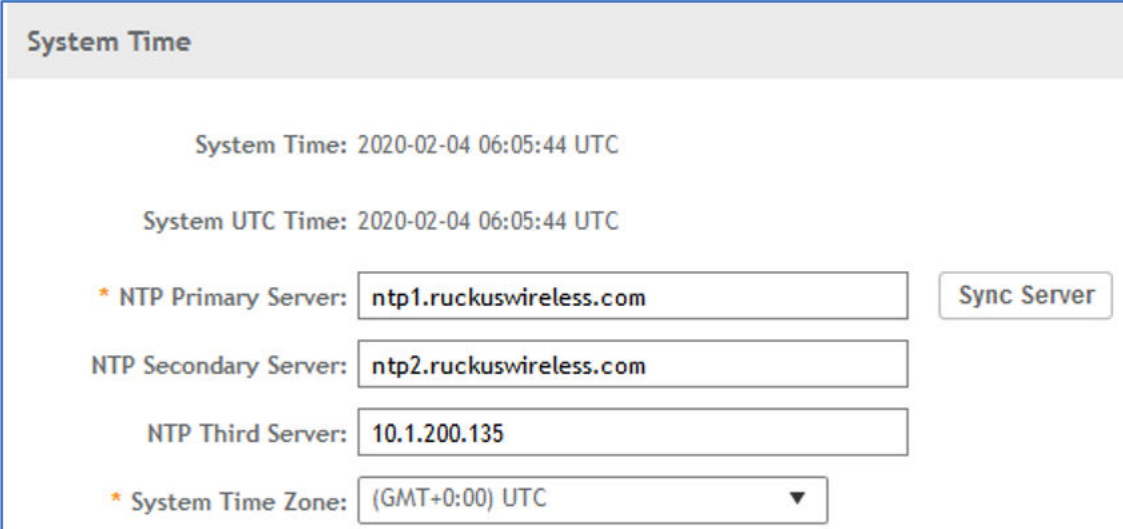
The NTP server synchronizes its time with that of the controller.

**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 149** 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'. The configuration section includes three NTP server fields: '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. The 'System Time Zone' is set to '(GMT+0:00) UTC' via a dropdown menu.

| System Time                              |                                                  |
|------------------------------------------|--------------------------------------------------|
| System Time: 2020-02-04 06:05:44 UTC     |                                                  |
| System UTC Time: 2020-02-04 06:05:44 UTC |                                                  |
| * NTP Primary Server:                    | ntp1.ruckuswireless.com <span>Sync Server</span> |
| NTP Secondary Server:                    | ntp2.ruckuswireless.com                          |
| NTP Third Server:                        | 10.1.200.135                                     |
| * System Time Zone:                      | (GMT+0:00) UTC ▼                                 |

- For **NTP Primary Server**, enter the NTP Server address that you want to use. The default NTP server address is `ntp.ruckuswireless.com`.

### NOTE

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

**FIGURE 150** Configuring System Time for Secondary Server

The screenshot displays the 'System Time' configuration page. At the top, it shows the current 'System Time' and 'System UTC Time' as '2020-02-04 06:05:44 UTC'. Below this, there are input fields for 'NTP Primary Server' (ntp.ruckuswireless.com), 'NTP Secondary Server' (10.1.200.135), and 'NTP Third Server' (3rdNTPserver.com). A 'Sync Server' button is next to the primary server field. The 'System Time Zone' is set to '(GMT+0:00) UTC'. The page is divided into three sections for authentication: 'NTP Primary Server Authentication' (Key Type: SHA1, Key ID: 9, Key: masked), 'NTP Secondary Server Authentication' (Key Type: None, Key ID: 1 - 65534, Key: masked), and 'NTP Third Server Authentication' (Key Type: SHA1, Key ID: 7, Key: masked). Each authentication section has a red note: 'The PSK is provided by the NTP server, please fill it accordingly'. At the bottom, there are 'Refresh', 'OK', and 'Cancel' buttons.

- 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.



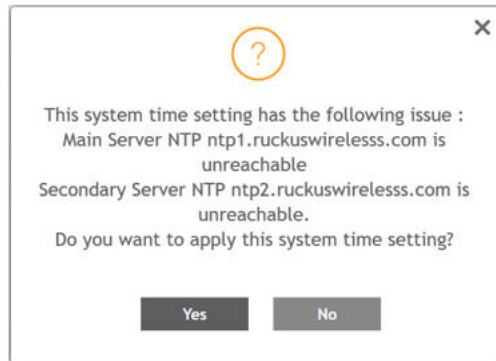
- Click **Sync Server** to enable an AP to join the controller and automatically synchronize its time every day.

If the **NTP Primary Server** is unreachable then secondary and tertiary NTP servers can be reached for synching 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. To know more about the event refer the

**FIGURE 151** 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**.
- Click **OK**.

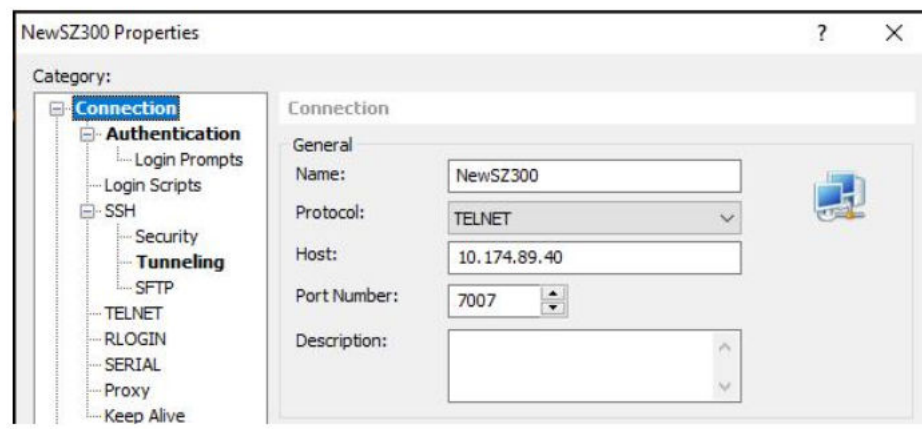
## Administrating the Controller

### Administrating the controller using console

All hardware platforms have console port which can be connected to Console switch to access the SZ console.

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

**FIGURE 152** Establishing connection with SZ 300



## Administrating the Controller

Administrating the controller using console

**FIGURE 153** Logging into CLI

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

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

Login incorrect

login: root
Password:

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

login: admin
Password:
Last login: Wed Mar 18 09:38:40 on tty50
Please wait. CLI initializing...

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

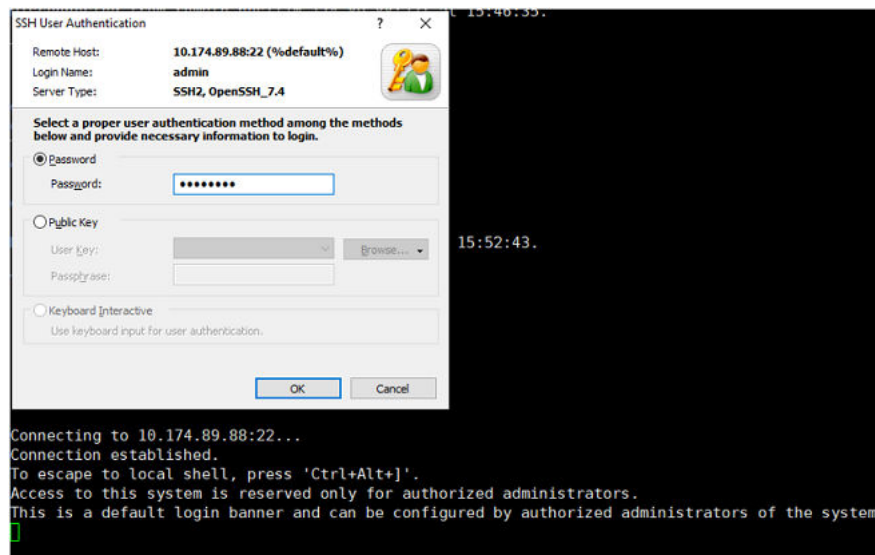
## Administrating the controller remotely

SZ Controller can be accessed remotely using SSH or WebUI.

1. Using SZ management IP, user can do ssh and login to CLI.

For example, ssh admin@<SZ management IP>

**FIGURE 154** Logging into CLI



```
Please wait. CLI initializing...

Welcome to the Ruckus SmartZone 100 Command Line Interface
Version: 5.1.1.3.1227

AUTOMATION-SZ100> en
Password: *****

AUTOMATION-SZ100#
```

The SSHv2 supports the following algorithms:

- a. Encryption Algorithms (client & server): aes128-ctr, aes256-ctr, [aes256-gcm@openssh.com](https://openssh.com)
- b. Public Key Algorithms (client): ssh-rsa
- c. Public Key Algorithms (server): ssh-rsa, ecdsa-sha2-nistp256, ecdsa-sha2-nistp384, ecdsa-sha2-nistp521
- d. Data Integrity/MAC algorithms (client & server): hmac-sha1, hmac-sha2-256, hmac-sha2-512 (Note:

### NOTE

Per the PP, 'implicit' is included when [aes\\*-gcm@openssh.com](https://openssh.com) is selected as an encryption algorithm. When [aes\\*-gcm@openssh.com](https://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".

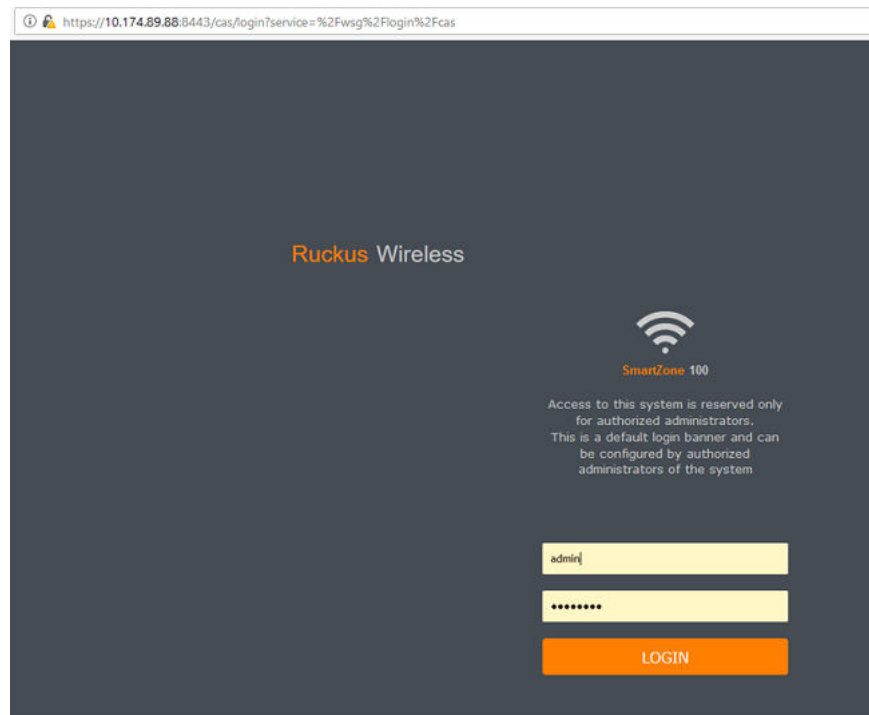
- e. Key Exchange Methods (client & server): diffie-hellman-group14-sha1, ecdh-sha2-nistp256, ecdh-sha2-nistp384 and ecdh-sha2-nistp521]

**NOTE**

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

2. Enter the IP address [HTTPS://MGMT-INTERFACE-IP:8443](https://MGMT-INTERFACE-IP:8443) in the browser to access the SZ Controller UI.

**FIGURE 155** Logging using Web Browser



There is no specific configuration needed to access the SSH and WebUI session, its enabled by default. The Controller provides remote administration of the system through secure communication channel (WebGUI 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/ WebUI connection is broken due to any issues then it can be manually re-established.

# Tamper-Evident Seals

## 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:

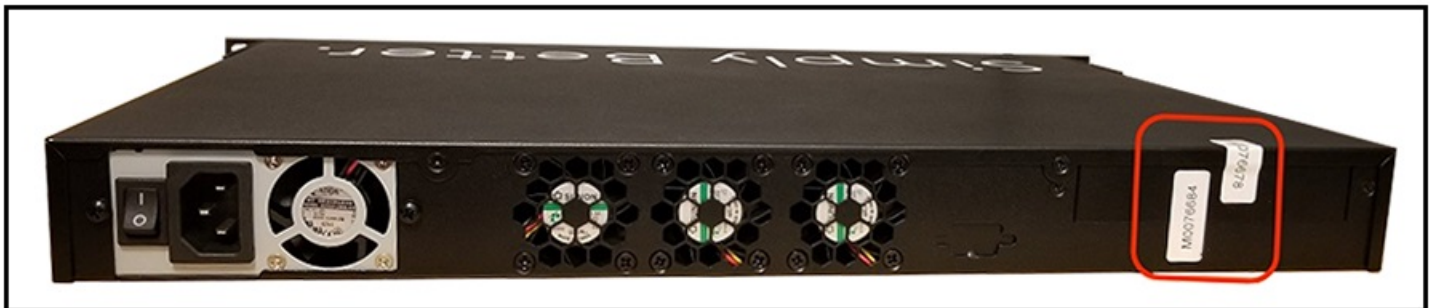
- All surfaces to which the seals will be applied must be clean and dry. Use alcohol to clean the surfaces. Do not use other solvents.
- Do not cut, trim, punch, or otherwise alter the tamper-evident seal.
- Do not use bare fingers to handle the labels. Slowly peel the packing from each seal, taking 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 SmartZone 100 Devices

The following images show locations where FIPS tamper-evident seals must be placed on SmartZone 100 devices.

**FIGURE 156** SmartZone 100 Rear Seals



## Tamper-Evident Seals

Tamper-Evident Seals on SmartZone 100 Devices

**FIGURE 157** SmartZone 100 Rear Seals (vertical)



**FIGURE 158** SmartZone 100 Side Seal (Horizontal View)



**FIGURE 159** SmartZone 100 Side Seal (Vertical View)



## Tamper-Evident Seals

Tamper-Evident Seals on SmartZone 100 Devices

**FIGURE 160** SmartZone 100 Bottom Seals





**FIGURE 161** SmartZone 100 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.

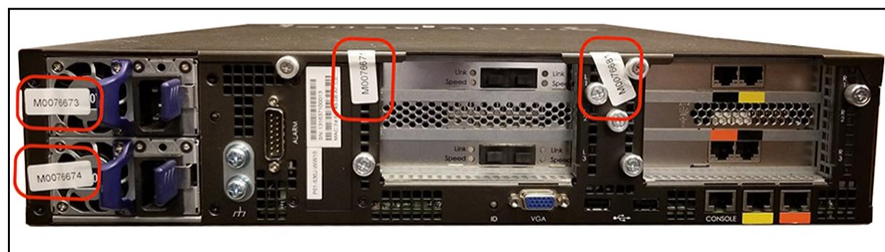
## Tamper-Evident Seals

### Tamper-Evident Seals on T610 AP Devices

**FIGURE 162** SmartZone 300 Top Seals



**FIGURE 163** SmartZone 300 Rear Seals



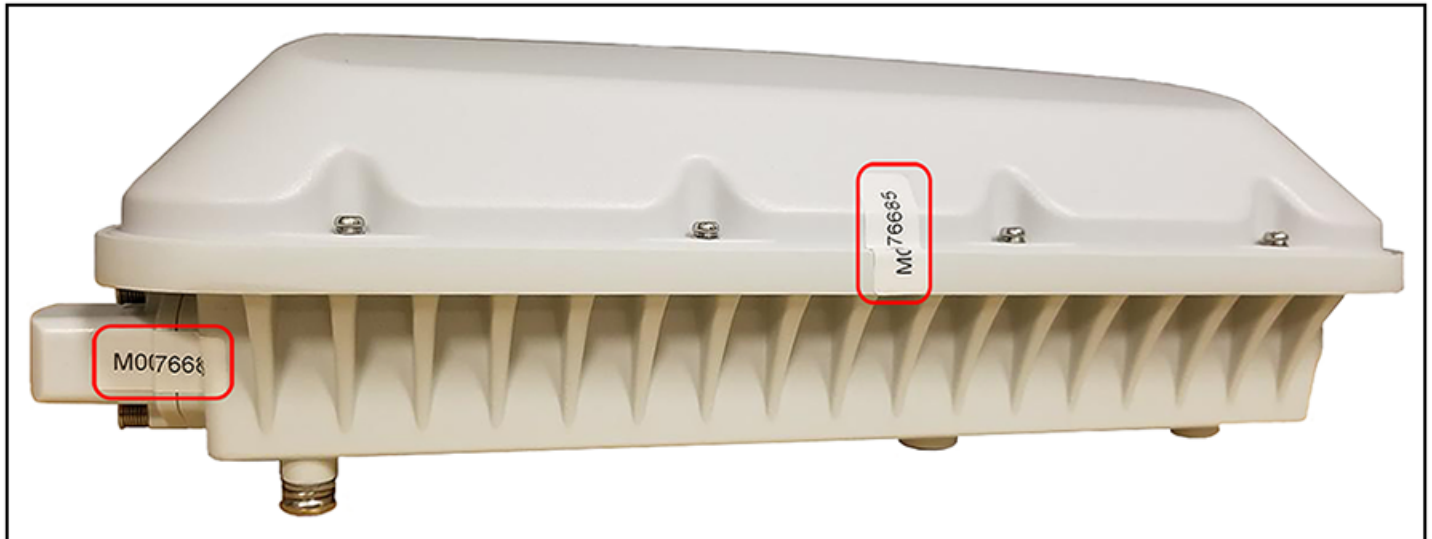
**FIGURE 164** SmartZone 300 Front Seals



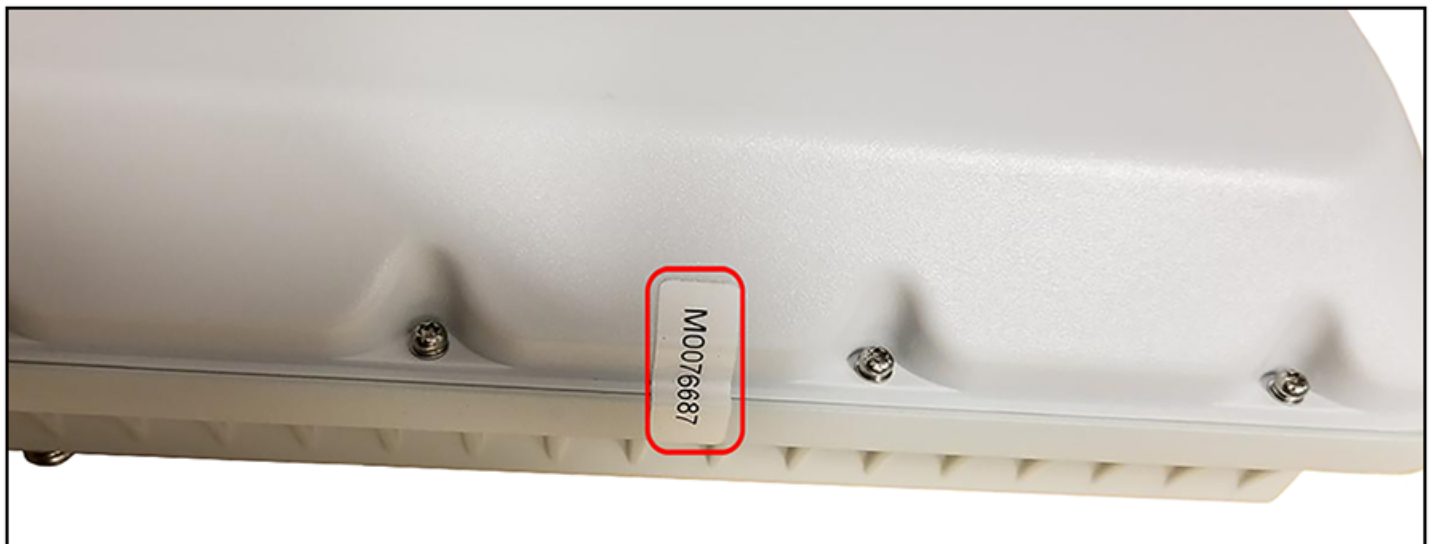
## Tamper-Evident Seals on T610 AP Devices

The following images show locations where FIPS tamper-evident seals must be placed on T610 AP devices.

**FIGURE 165** T610 AP Side Seals



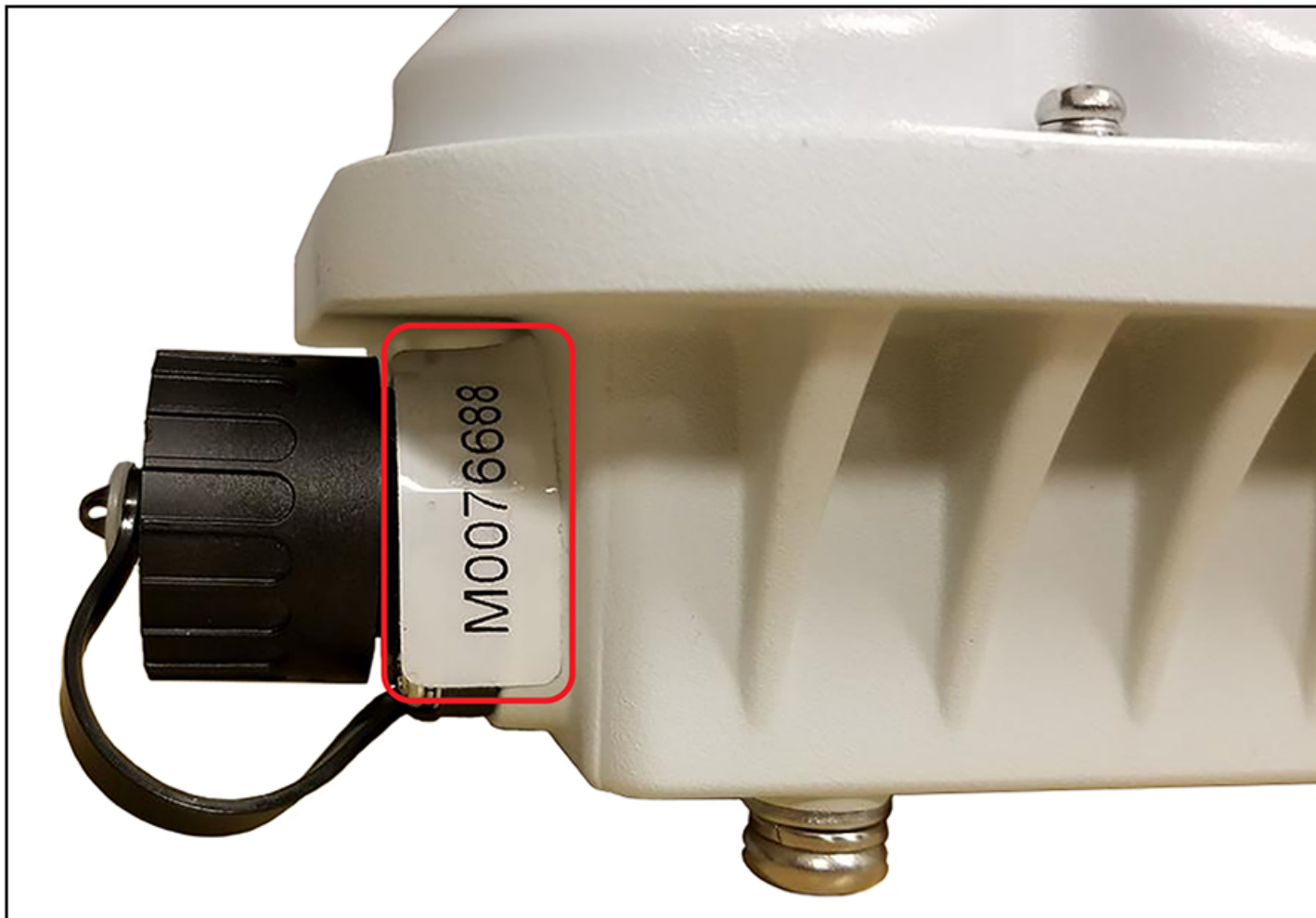
**FIGURE 166** T610 AP Side Seal Detail



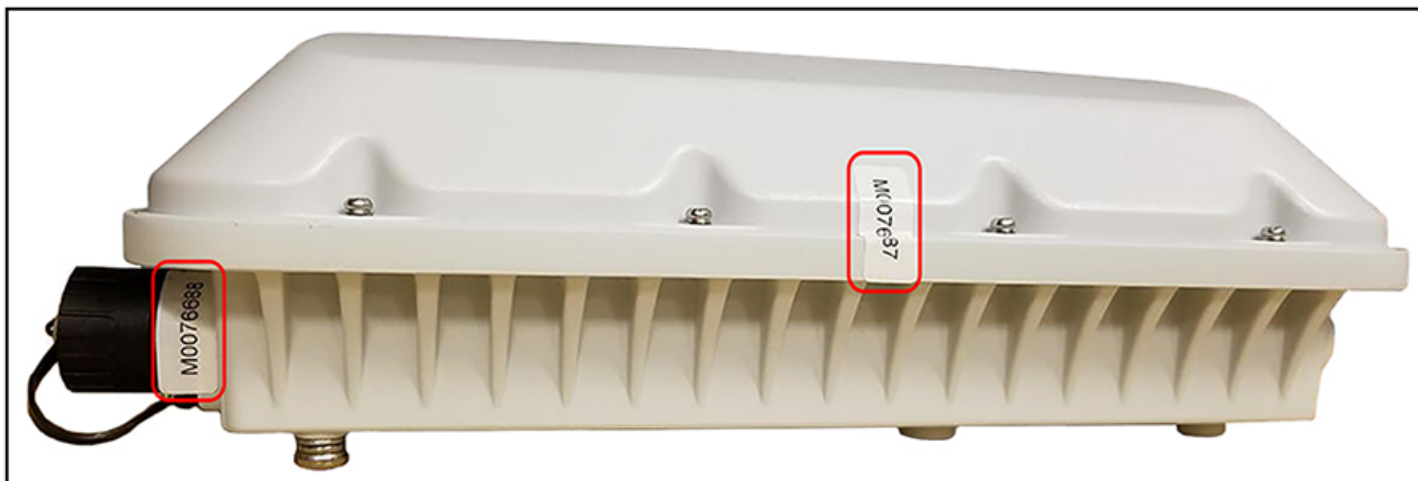
## Tamper-Evident Seals on T710 AP Devices

The following images show locations where FIPS tamper-evident seals must be placed on T710 AP devices.

**FIGURE 167** T710 AP Collar Seal



**FIGURE 168** T710 AP Side Seals



**FIGURE 169** T710 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.

**FIGURE 170** R610 AP Side Seal





## Tamper-Evident Seals

### Tamper-Evident Seals on R710 AP Devices

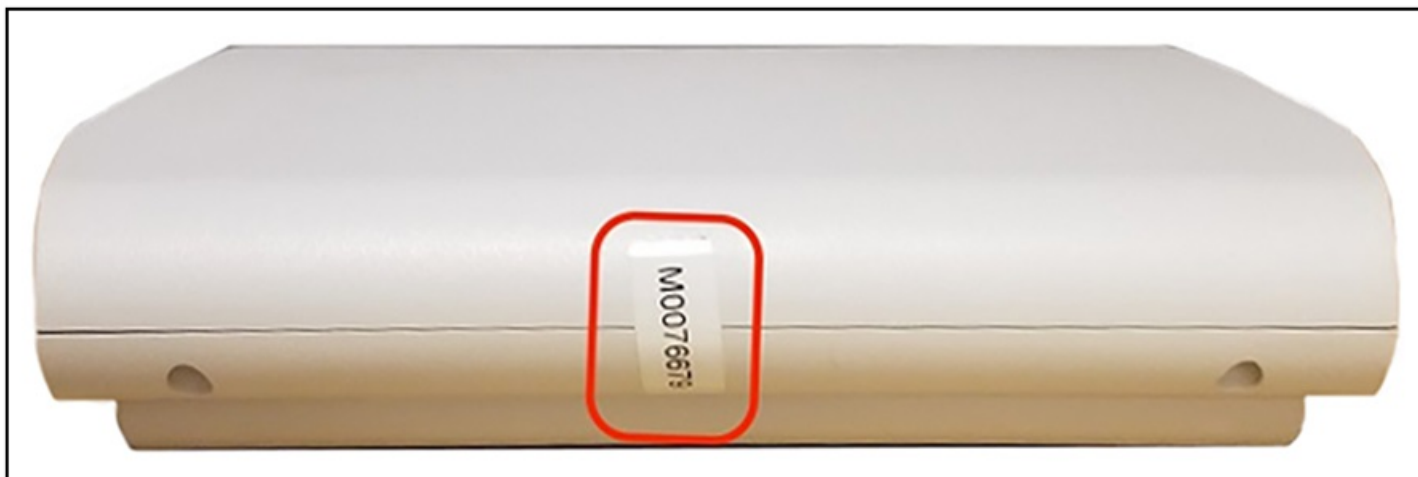
**FIGURE 171** R610 AP Side Seal (Opposite Side)



## Tamper-Evident Seals on R710 AP Devices

The following images show locations where FIPS tamper-evident seals must be placed on R710 AP devices.

**FIGURE 172** R710 AP Side Seal



**FIGURE 173** R710 AP Side Seal (Opposite Side)



## Tamper-Evident Seals

### Tamper-Evident Seals on R720 AP Devices

**FIGURE 174** R710 AP Seals (Bottom View)

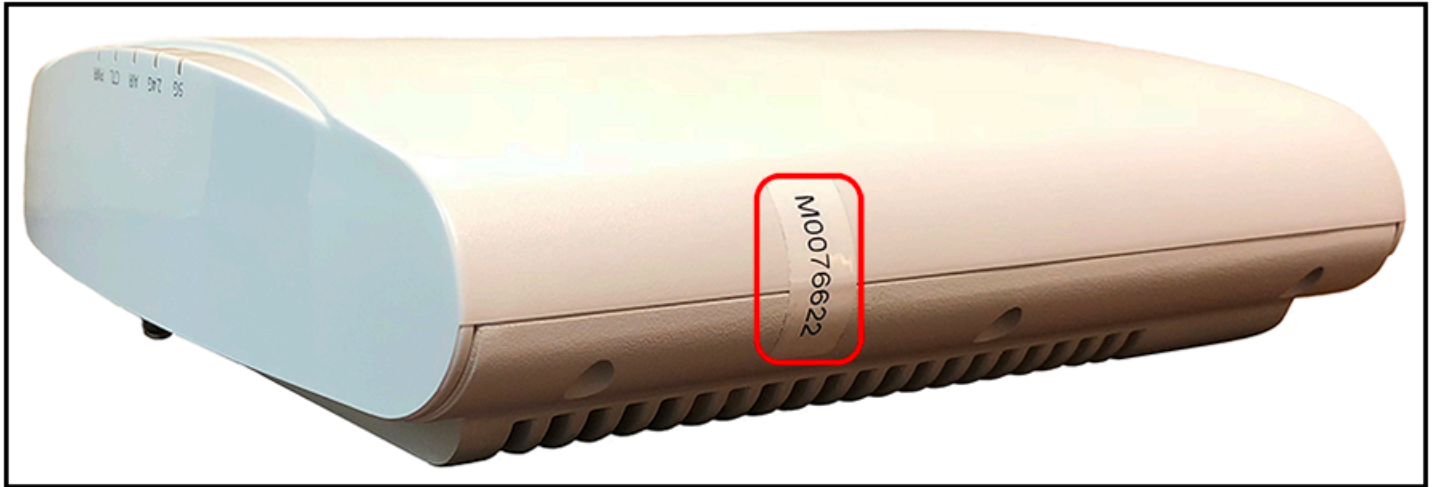


## Tamper-Evident Seals on R720 AP Devices

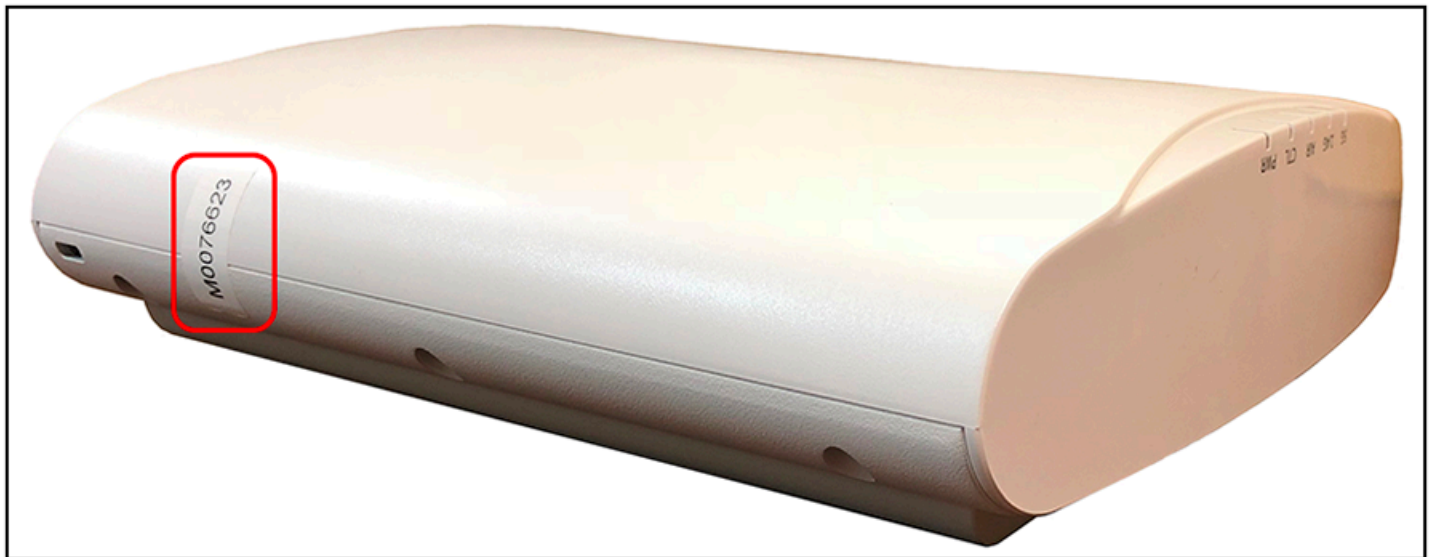
The following images show locations where FIPS tamper-evident seals must be placed on R720 AP devices.



**FIGURE 175** R720 AP Right Side Seal



**FIGURE 176** R720 AP Left Side Seal



## Trusted Channels Through TSF

### 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 177** 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, **flrstwPa2%PSK-Wl@nPa\$\$w0rd** or **abcdefghijklmnopqrstuvwxyz0123456789\$@Abcdefghijklmnopqrstuvwxyz**.

## 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 26 to configure a RadSec profile.
2. Follow the steps listed in [Configuring Ruckus GRE and IPsec in the WLAN](#) on page 103 to configure Ruckus GRE and IPsec for a WLAN.

## FIPS-Compliant Products

### 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 6** 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 7** 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-R710-US00 | TAA/FIPS - compliant Ruckus R710 dual-band 802.11abgn/ac (802.11ac Wave 2) Wireless Access Point, 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 R710 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-T710-US01 | TAA/FIPS - compliant Ruckus T710 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, 90-264 VAC, POE in and POE out, Fiber SFP, GPS, IP-67 Outdoor enclosure, -40 to 65C Operating Temperature. Includes standard 1-year warranty. For box contents, see Shipping Container Contents.                     | TAA T710 XX 11ac dual outdoor AP 4x4:4  |
| 9F1-T710-US51 | TAA/FIPS - compliant Ruckus T710s 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, 90-264 VAC, POE in and POE out, Fiber SFP, GPS, IP-67 Outdoor enclosure, -40 to 65C Operating Temperature. Includes standard 1-year warranty. For box contents, see Shipping Container Contents.                  | TAA T710s XX 11ac dual outdoor AP 4x4:4 |
| 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  |

**TABLE 8** FIPS-Compliant Controller Products

| SKU           | Long description                                                                                                                                                                              | Short description                       |
|---------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------|
| PF1-S124-US00 | TAA/FIPS - compliant SmartZone 100 with 2x10GigE and 4 GigE ports, 90-day temporary access to licenses.                                                                                       | TAA SZ 100-2x10GE & 4xGE, XX power cord |
| PF1-S104-US00 | TAA/FIPS - compliant SmartZone 100 with 4 GigE ports, 90-day temporary access to licenses.                                                                                                    | TAA SZ 100-4xGE ports, XX power cord    |
| PF1-S300-WW10 | SmartZone 300 (SZ 300) 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 | SmartZone 300 (SZ 300) 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.

## 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).

**TABLE 9** 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      | authReauththe          | 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                                          |

**TABLE 9** Auditable Events in AP for CC (continued)

| Event Code | Event Type       | Description                                                                                                             |
|------------|------------------|-------------------------------------------------------------------------------------------------------------------------|
| 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 10** 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                                                                                                         |
| 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      | dpDiscontinuousTimeChangeNTPServerdpNtpTimeSync | 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                               |

**TABLE 10** Auditable Events in DP for CC (continued)

| Event Code | Event Type              | Description                                                                                      |
|------------|-------------------------|--------------------------------------------------------------------------------------------------|
| 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 11** 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).                                                                       |
| 99102      | SZ Failure of Certificate                                       | This event occurs when sz server certificate validation failed.                                                                    |

## Audit Records

### 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 178 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 00:15:15 | 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.

FIGURE 179 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 [Out  | N/A             | N/A        | N/A                 | N/A          |
| 2020/04/01 06:45:20 | Radius server unreachable   | Major    | Cleared     | AP [E08  | N/A             | System     | 2020/04/01 06:45:28 | Auto Cleared |
| 2020/04/01 06:45:16 | AP rebooted by system       | Major    | Outstanding | AP [E08  | N/A             | N/A        | N/A                 | N/A          |
| 2020/04/01 06:17:00 | AP disconnected             | Major    | Cleared     | AP [E03  | N/A             | System     | 2020/04/01 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 06:16:58 | AP failed to connect to LS  | Major    | Outstanding | AP [E03  | N/A             | N/A        | N/A                 | N/A          |
| 2020/04/01 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 [Out  | 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          |
| 2020/04/01 20:13:29 | AP rebooted by system       | Major    | Outstanding | AP [E03  | N/A             | N/A        | N/A                 | N/A          |
| 2020/04/01 15:06:16 | Connect to data streamin... | Critical | Cleared     | Node [A  | N/A             | System     | 2020/04/01 15:11:41 | Auto Cleared |
| 2020/04/01 12:15:08 | No LS responses             | Major    | Outstanding | AP [Out  | 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 19:39:31 | AP rebooted by system       | Major    | Outstanding | AP [E08  | N/A             | N/A        | N/A                 | N/A          |
| 2020/04/01 19:28:13 | 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 [Out  | 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          |



## Audit Records

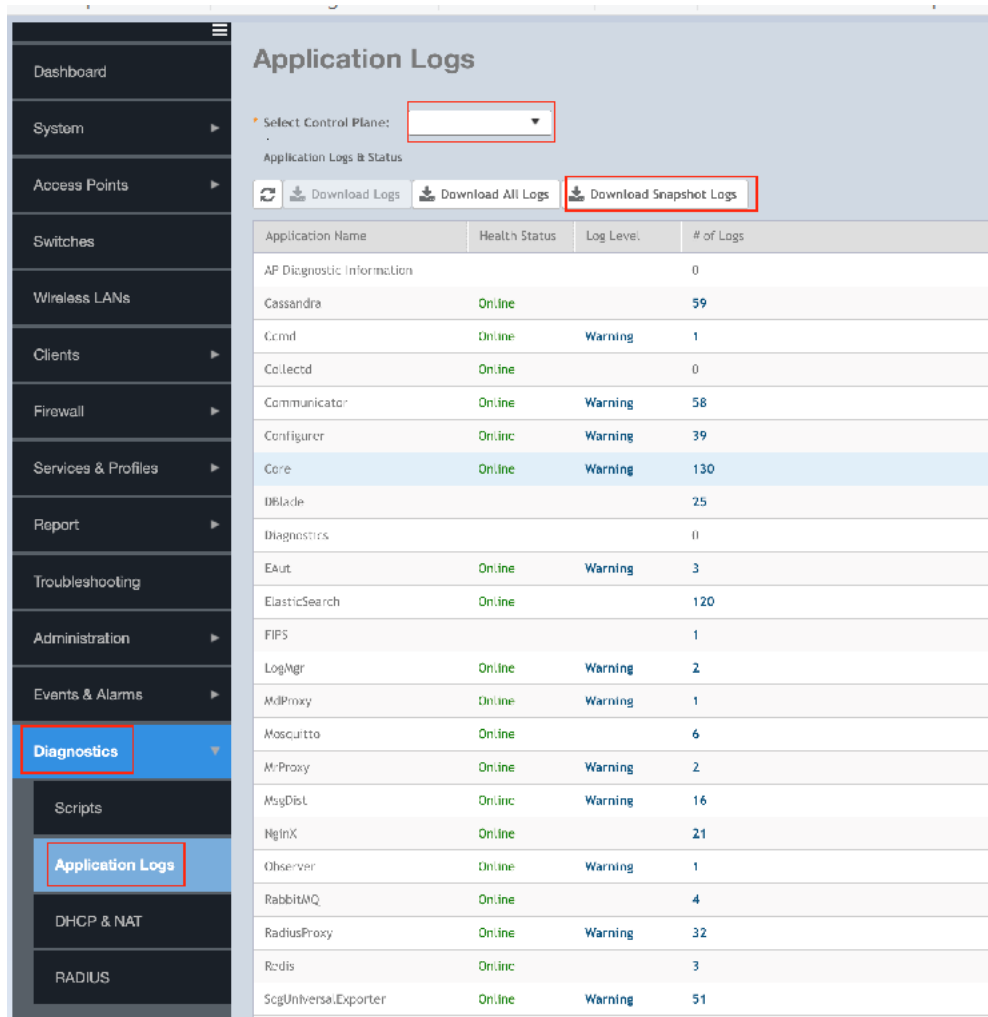
Downloading the Logs from the Controller

# 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 180** 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.



| Requirement       | Auditable Events                          | Additional Content | SZ100 (Physical)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | vSZ-H (Virtual)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | vSZ-D                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | AP                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|-------------------|-------------------------------------------|--------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| NDcPP21:FAU_GEN.1 | Start-up and shut-down of audit functions | None               | <p>The audit functions correspond with the startup and shutdown of the device</p> <p><b>Start Up</b><br/>Mar 30 18:03:43 SZ100<br/>Core:<br/>@@835,nodeBackToInService,"sourceBladeUID"="44743360-244d-4dcc-b722-8fdd45e30cf3","nodeMac"="B4:79:C8:25:82:30","clusterName"="SZ100Test","wsgMgmtIp"="172.16.16.244","nodeName"="SZ100"</p> <p><b>Shut Down</b><br/>Mar 31 22:09:18 SZ100<br/>Core:<br/>@@828,nodeShutdown,"clusterName"="SZ100Test","nodeMac"="B4:79:C8:25:82:30","sourceBladeUUID"="44743360-244d-4dcc-b722-8fdd45e30cf3","nodeName"="SZ100","wsgMgmtIp"="172.16.16.244"</p> | <p>The audit functions correspond with the startup and shutdown of the device</p> <p><b>Start Up</b><br/>Mar 31 22:29:27 vszh<br/>Core:<br/>@@835,nodeBackToInService,"nodeName"="vszh","clusterName"="High Scale","sourceBladeUID"="c8b436f2-eb54-495d-ab10-1212190c891a","wsgMgmtIp"="172.16.16.230","nodeMac"="00:0C:29:13:08:76"</p> <p><b>Shut Down</b><br/>Mar 30 17:32:31 vszh<br/>Core:<br/>@@828,nodeShutdown,"sourceBladeUUID"="c8b436f2-eb54-495d-ab10-1212190c891a","nodeName"="vszh","wsgMgmtIp"="172.16.16.230","nodeMac"="00:0C:29:13:08:76","clusterName"="High Scale"</p> | <p>The audit functions correspond with the startup and shutdown of the device</p> <p><b>Start Up</b><br/>Mar 30 16:13:09 vszh<br/>Core:<br/>@@515,dpPhyInterfaceUp,"dpKey"="97HM3WVA5234U0JPM34HJEUJ1XTA000C29B4693A000C29B46944","portID"="0"</p> <p><b>Shutdown</b><br/>Mar 30 16:12:33 vszh<br/>Core:<br/>@@513,dpDisconnected,"dpKey"="97HM3WVA5234U0JPM34HJEUJ1XTA000C29B4693A000C29B46944","timestamp"="1585584738918","cpName"="vszh","wsgIP"="172.16.8.230","reason"="1, NMI problem."</p> | <p>The audit functions correspond with the startup and shutdown of the device</p> <p><b>Start Up</b><br/>Mar 30 16:00:10 vszh<br/>Core:<br/>@@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>Shutdown</b><br/>Mar 30 16:00:10 vszh<br/>Core:<br/>@@301,apRebootByUser,"apMac"="94:BF:C4:22:75:00","reason"="AP rebooted by controller user","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"="39.232527,-76.8","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>NDcPP21:FCCPC_EXT.1</b>    | Enabling communications between a pair of components. Disabling communications between a pair of components. | Identities of the endpoints pairs enabled or disabled. | <p><b>Enabled</b><br/>Feb 24 15:37:36 SZ100<br/>Core: @@312,apConnected,"idealEventVersion"=3.5.1,"domainId"=8b2081d5-9662-40d9-a3db-2a3cf4dde3f7","zoneUID"="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><br/>Jan 28 16:23:03 SZ100<br/>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> | <p><b>Enabled</b><br/>Mar 29 16:07:14 vszh<br/>Core: @@312,apConnected,"idealEventVersion"=3.5.1,"domainId"=8b2081d5-9662-40d9-a3db-2a3cf4dde3f7","zoneUID"="7079e8e4-ac46-4086-803b-6b4bc3a46de2","zoneName"="TestZone","apGroupUID"="35f4aa9e-6b5c-4a05-8035-bdc2ac8674ea","apMac"="94:BF:C4:22:75:00","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><br/>Mar 29 15:44:32 vszh<br/>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> | <p><b>Enabled</b><br/>Mar 29 16:18:30 vszh<br/>Core: @@512,dpConnected,"dpKey"="97HM3WVA5234U0JPM34HJEUJ1XTA000C29B4693A000C29B46944","timestamp"="1585498710059","cpName"="vszh","wsgIP"="172.16.8.230"</p> <p><b>Disabled</b><br/>Mar 23 22:07:33 vszh<br/>Core: @@513,dpDisconnected,"dpKey"="97HM3WVA5234U0JPM34HJEUJ1XTA000C29B4693A000C29B46944","timestamp"="1585001239636","cpName"="vszh","wsgIP"="172.16.8.230","reason"="1, NMI problem."</p> | <p><b>Enabled</b><br/>Mar 18 16:05:01 vszh<br/>Core: @@99018,sshInitiation, "apMac"="94:BF:C4:22:75:00", "reason"="SSH Login successful with IP 172.16.8.254<br/>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","apGroupUID"="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><br/>Mar 29 16:07:27 vszh<br/>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","apGroupUID"="35f4aa9e-6b5c-4a05-8035-bdc2ac8674ea","domainId"="8b2081d5-9662-40d9-a3db-2a3cf4dde3f7","serialNumber"="521803001443","domainName"="Administration Domain","idealEventVersion"="3.5.1","apDescription"=""</p> |
| <b>NDcPP21:FCSHTTPS_EXT.1</b> | Failure to establish a HTTPS Session.                                                                        | Reason for failure.                                    | Mar 24 14:52:22 SZ100<br>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].]"                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | Mar 24 14:51:37 vszh<br>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].]"                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | N/A                                                                                                                                                                                                                                                                                                                                                                                                                                                      | N/A                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>NDcPP21:FCSIPSEC_EXT.1</b> | Failure to establish an IPsec SA.                                                                            | Reason for failure.                                    | <p><b>Invalid IKE Proposal</b><br/>Mar 11 21:30:48 SZ100<br/>strongswan: 16[IKE] received proposals unacceptable</p> <p><b>Invalid ESP Proposal</b><br/>Jan 3 13:17:22 SZ100<br/>strongswan: 05[IKE] no acceptable proposal found</p> <p><b>Invalid Cert Identifier</b><br/>Jan 27 18:32:54 SZ100<br/>strongswan: 10[CFG] no matching peer config found</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | <p><b>Invalid IKE Proposal</b><br/>Jan 31 14:15:52 vszh<br/>strongswan: 07[IKE] received proposals unacceptable</p> <p><b>Invalid ESP Proposal</b><br/>Jan 31 14:26:08 vszh<br/>strongswan: 12[IKE] no acceptable proposal found</p> <p><b>Invalid Cert Identifier</b><br/>Feb 4 15:47:44 vszh<br/>strongswan: 09[CFG] no matching peer config found</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | Mar 19 01:06:04 vszh<br>Core: @@99243,dpIPsecSaFailed,"dpKey"="97HM3WVA5234U0JPM34HJEUJ1XTA000C29B4693A000C29B46944","dstIP"="172.16.8.31","apIP"="172.16.8.248","reason"="spi 0x7a010000 SA not found"                                                                                                                                                                                                                                                  | Mar 18 15:12:31 vszh<br>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","apGroupUID"="35f4aa9e-6b5c-4a05-8035-bdc2ac8674ea","domainId"="8b2081d5-9662-40d9-a3db-2a3cf4dde3f7","serialNumber"="521803001443","domainName"="Administration Domain","idealEventVersion"="3.5.1","apDescription"=""                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |

|                                   |                                                                                                                  |                                                                                                  |                                                                                                                                                                                                                                                                                                                                                                                                  |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|-----------------------------------|------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>NDcPP21:FCS_NTP_EXT.1</b>      | Configuration of a new time server<br>Removal of configured time server                                          | Identity if new/removed time server                                                              | Feb 17 19:07:35 SZ100<br>Core:<br>@@99301,disContTime Change, "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"                                                                                                                                                                                                     | Feb 21 22:57:42 vszh<br>Core:<br>@@99301,disContTime Change, "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"                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | N/A                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | N/A                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>WLANASEP10:FCS_IPSEC_EXT.1</b> | Protocol failures. Establishment/Termination of an IPsec SA. Negotiation “down” from an IKEv2 to IKEv1 exchange. | Reason for failure. Non-TOE endpoint of connection (IP address) for both successes and failures. | <b>Protocol Failures</b><br>See NDcPP21:FCS_IPSEC_EXT.1<br><b>Establishment</b><br>Mar 24 15:16:04 SZ100 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]<br><br><b>Termination</b><br>Mar 24 15:57:24 SZ100 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] | <b>Protocol Failures</b><br>See NDcPP21:FCS_IPSEC_EXT.1<br><b>Establishment</b><br>Feb 4 17:05:51 vszh strongswan: 08[IKE] IKE_SA ipsec[1] established between 172.16.8.230[C=US, ST=MD, L=Catonsville, O=GSS, CN=SZ100.example.com , E=server-SZ100-IPsec-rsa@gossamersec.com]... 172.16.8.254[C=US, ST=MD, L=Catonsville, O=GSS, CN=tl4-16x.example.com, E=server-rsa@gossamersec.com]<br><b>Termination</b><br>Feb 4 17:06:20 vszh strongswan: 15[IKE] deleting IKE_SA ipsec[2] between 172.16.8.230[C=US, ST=MD, L=Catonsville, O=GSS, CN=SZ100.example.com , E=server-SZ100-IPsec-rsa@gossamersec.com]... 172.16.8.254[C=US, ST=MD, L=Catonsville, O=GSS, CN=tl4-16x.example.com, E=server-rsa@gossamersec.com] | <b>Protocol Failures</b><br>See NDcPP21:FCS_IPSEC_EXT.1<br><br><b>Establishment</b><br>Mar 18 15:04:27 vszh<br>Core:<br>@@99244,dpIPsecSaUpdated,"dpKey"="97HM3WVA5234U0JPM34HJEUJ1XTA000C29B4693A000C29B46944","dstIP"="172.16.8.248","apIP"="172.16.8.248","action"="spi 0xc52b4656 insert SA"<br><br><b>Termination</b><br>Mar 18 14:57:19 vszh<br>Core:<br>@@99242,dpIPsecTunnTerminated,"dpKey"="97HM3WVA5234U0JPM34HJEUJ1XTA000C29B4693A000C29B46944","apIP"="172.16.8.248" | <b>Protocol Failures</b><br>See NDcPP21:FCS_IPSEC_EXT.1<br><br><b>Establishment</b><br>Mar 18 15:04:27 vszh<br>Core:<br>@@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,M11.0/02:00","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"=""<br><br><b>Termination</b><br>Mar 18 15:04:19 vszh<br>Core:<br>@@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,M11.0/02:00","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>NDcPP21:FCS_SSHC_EXT.1</b>     | Failure to establish an SSH session.                                                                             | Reason for failure.                                                                              | N/A                                                                                                                                                                                                                                                                                                                                                                                              | N/A                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | 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:<br><br>Mar 31 22:32:07 esxidp dpm[3987]: @@99230,dpSshTunnFailed, "dpKey"="97HM3WVA5234U0JPM34HJEUJ1XTA000C29B4693A000C29B46944","scgIP"="172.16.8.230"                                                                                                                                                                                                | The AP wont log to the SZ controller if the ITT connection fails. A local log can be pulled from the AP if required:<br><br>Apr 2 00:39:20 T710 daemon.err rsmd_func[13975]: SShTunnel start Failed ServerIP=172.16.8.230                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |

|                               |                                      |                     |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |     |     |
|-------------------------------|--------------------------------------|---------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----|-----|
| <b>NDcPP21:FCS_SSHS_EXT.1</b> | Failure to establish an SSH session. | Reason for failure. | <p><b>Failed Password</b><br/>Mar 31 14:58:10 SZ100 sshd[16052]: Failed password for admin from 172.16.16.254 port 33578 ssh2</p> <p><b>Invalid Public Key Algorithm</b><br/>Mar 31 15:02:46 SZ100 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><br/>Mar 31 15:08:56 SZ100 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><br/>Mar 31 15:17:47 SZ100 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>                                                                                                                                                                                                                                                                                                                                                                                                                                                        | <p><b>Failed Password</b><br/>Mar 29 16:40:38 vszh sshd[10124]: Failed password for admin from 172.16.16.154 port 60940 ssh2</p> <p><b>Invalid Public Key Algorithm</b><br/>Mar 30 10:52:23 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><br/>Mar 30 10:56:07 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><br/>Mar 30 10:58:57 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>                                                                                                                                                                                                                                                                                                                                                                                                                                                   | N/A | N/A |
| <b>NDcPP21:FCS_TLSC_EXT.1</b> | Failure to establish a TLS Session.  | Reason for failure. | <p>Jan 30 13:19:47 SZ100 error: 14090086:SSL routines:SSL3_GET_SE RVER_CERTIFICATE:c ertificate verify failed (60)</p> <p>Apr 1 21:51:11 SZ100 tls: TLS_connect: Error in SSLv3 read server key exchange B</p> <p>Apr 1 21:53:15 SZ100 tls: error:1408D07B:SSL routines:SSL3_GET_KEY_EXCHANGE:bad signature</p> <p>Apr 1 21:55:56 SZ100 tls: Failed in __FUNCTION__ (SSL_connect): error:1408C095:SSL routines:SSL3_GET_FINAL_SHED:digest check failed</p> <p>Apr 1 21:59:19 SZ100 tls: Failed in __FUNCTION__ (SSL_connect): error:1408F081:SSL routines:SSL3_GET_RECORD:block cipher pad is wrong</p> <p>Apr 1 22:00:52 SZ100 tls: error:10067066:elliptic curve routines:ec_GFp_simple_oct2point:invalid encoding</p> <p>Apr 1 21:22:44 SZ100 tls: Failed in __FUNCTION__ (SSL_connect): error:140920F8:SSL routines:SSL3_GET_SERVER_HELLO:unknown cipher returned</p> <p>Apr 1 21:25:43 SZ100 tls: Failed in __FUNCTION__ (SSL_connect): error:1409210A:SSL routines:SSL3_GET_SERVER_HELLO:wrong ssl version</p> <p>Feb 18 22:06:20 SZ100 Certificate CN (Completely Random Common Name (Bad CN identifier)) does not match specified value (tl4-16x.example.com)!</p> | <p>Apr 1 22:14:39 vszh error: 14090086:SSL routines:SSL3_GET_SE RVER_CERTIFICATE:c ertificate verify failed (60)</p> <p>Apr 1 22:18:26 vszh tls: TLS_connect: Error in SSLv3 read server key exchange B</p> <p>Apr 1 22:21:08 vszh tls: error:1408D07B:SSL routines:SSL3_GET_KEY_EXCHANGE:bad signature</p> <p>Apr 1 22:24:09 vszh tls: Failed in __FUNCTION__ (SSL_connect): error:1408C095:SSL routines:SSL3_GET_FINAL_SHED:digest check failed</p> <p>Apr 1 22:27:45 vszh tls: Failed in __FUNCTION__ (SSL_connect): error:1408F081:SSL routines:SSL3_GET_RECORD:block cipher pad is wrong</p> <p>Apr 1 22:31:58 vszh tls: error:10067066:elliptic curve routines:ec_GFp_simple_oct2point:invalid encoding</p> <p>Apr 1 22:35:39 vszh tls: Failed in __FUNCTION__ (SSL_connect): error:140920F8:SSL routines:SSL3_GET_SERVER_HELLO:unknown cipher returned</p> <p>Apr 1 22:38:03 vszh tls: Failed in __FUNCTION__ (SSL_connect): error:1409210A:SSL routines:SSL3_GET_SERVER_HELLO:wrong ssl version</p> <p>Apr 1 22:41:42 vszh Certificate CN (Completely Random Common Name (Bad CN identifier)) does not match specified value (tl4-16x.example.com)!</p> | N/A | N/A |

|                            |                                                                                                              |                                         |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |     |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|----------------------------|--------------------------------------------------------------------------------------------------------------|-----------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| NDcPP21:FCS_TLSS_EXT.1     | Failure to establish a TLS Session.                                                                          | Reason for failure.                     | <p>2020/04/02 20:20:07 [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>2020/04/02 20:20:18 [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>2020/04/02 20:20:29 [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>2020/04/02 20:20:40 [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>2020/04/02 20:21:00 [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>2020/04/02 20:21:17 [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> | <p>2020/04/02 20:46:18 [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>2020/04/02 20:46:29 [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>2020/04/02 20:46:39 [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>2020/04/02 20:46:49 [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>2020/04/02 20:47:16 [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>2020/04/02 20:47:32 [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> | N/A | N/A                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| WLANASEP10:FIA_8021X_EXT.1 | Attempts to access the 802.1X controlled port prior to successful completion of the authentication exchange. | Provided client identity (MAC address). | N/A                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | N/A                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | N/A | Mar 13 19:35:29 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","tenantUID"="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>NDcPP21:FIA_AFL.1</b>          | Unsuccessful login attempt limit is met or exceeded.                                                                                                                                                                                    | Origin of the attempt (e.g., IP address).                                                                                                          | Feb 25 20:45:32 SZ100<br>Core:<br>@@8011,adminAccount<br>Logout,"userName"="admin",<br>"ip"="172.16.16.153",<br>"lockoutDuration"="5"                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | Feb 26 17:02:43 vszh<br>Core:<br>@@8011,adminAccount<br>Logout,"userName"="admin",<br>"ip"="172.16.16.153",<br>"lockoutDuration"="5"                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | N/A                                                                                                    | N/A                                                                                                   |
| <b>WLANASEP10:FIA_AFL.1</b>       | 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). |                                                                                                                                                    | See<br>NDcPP21:FIA_AFL.1                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | See<br>NDcPP21:FIA_AFL.1                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | N/A                                                                                                    | N/A                                                                                                   |
| <b>WLANASEP10:FIA_UAU.6</b>       | Attempts to re-authenticate.                                                                                                                                                                                                            | Origin of the attempt (e.g., IP address).                                                                                                          | Mar 31 17:29:19 SZ100<br>Web Activity:<br>"User:[admin],Browser<br>IP:[172.16.16.253],Action:[Re-authenticate],Resource:[Administrator],Description:[The re-authentication is successful.]"                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | Mar 30 12:48:22 vszh<br>Web Activity:<br>"User:[admin],Browser<br>IP:[172.16.16.253],Action:[Re-authenticate],Resource:[Administrator],Description:[The re-authentication is successful.]"                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | N/A                                                                                                    | N/A                                                                                                   |
| <b>NDcPP21:FIA_UAU_EXT.2</b>      | All use of identification and authentication mechanism.                                                                                                                                                                                 | Origin of the attempt (e.g., IP address).                                                                                                          | <b>Logon success</b><br><br><b>Web UI</b><br>Mar 25 17:29:19 SZ100<br>Web Activity:<br>"User:[admin],Browser<br>IP:[172.16.16.253],Action:[Logon],Resource:[Administrator],Description:[Administrator [admin] logged on from [172.16.16.253].]"<br><br><b>CLI</b><br>Mar 20 18:36:15 SZ100<br>Web Activity:<br>"User:[admin],Browser<br>IP:[127.0.0.1],Action:[Logon],Resource:[Administrator],Description:[Administrator [admin] logged on from CLI.]"<br><br><b>SSH</b><br>Mar 26 21:33:53 SZ100<br>Core:<br>@@8008,szLogin,"userName"="admin",<br>"ip"="172.16.16.254"<br><br><b>Logon Failure</b><br><br><b>WebUi</b><br>See<br>NDcPP21:FCS_HTTPS_EXT.1<br><br><b>CLI</b><br>Mar 26 22:13:53 SZ100<br>login: FAILED LOGIN 2 FROM (null) FOR admin, Authentication failure<br><br><b>SSH</b><br>Mar 26 22:04:59 SZ100<br>Core:<br>@@8007,szLoginFail,"userName"="admin",<br>"ip"="172.16.16.254" | <b>Logon success</b><br><br><b>Web UI</b><br>Mar 2 11:59:11 vszh<br>Web Activity:<br>"User:[admin],Browser<br>IP:[172.16.16.153],Action:[Logon],Resource:[Administrator],Description:[Administrator [admin] logged on from [172.16.16.153].]"<br><br><b>CLI</b><br>Mar 4 15:33:36 vszh<br>Web Activity:<br>"User:[admin],Browser<br>IP:[172.16.16.254],Action:[Logon],Resource:[Administrator],Description:[Administrator [admin] logged on from CLI.]"<br><br><b>SSH</b><br>Mar 4 15:33:28 vszh<br>Core:<br>@@8008,szLogin,"userName"="admin",<br>"ip"="172.16.16.254"<br><br><b>Logon Failure</b><br><br><b>WebUi</b><br>See<br>NDcPP21:FCS_HTTPS_EXT.1<br><br><b>CLI</b><br>Feb 26 20:10:59 vszh<br>login: FAILED LOGIN 3 FROM (null) FOR admin, Authentication failure<br><br><b>SSH</b><br>Feb 28 19:30:15 vszh<br>Core:<br>@@8007,szLoginFail,"userName"="admin",<br>"ip"="172.16.16.254" | N/A                                                                                                    | N/A                                                                                                   |
| <b>NDcPP21:FIA_UIA_EXT.1</b>      | All use of identification and authentication mechanism.                                                                                                                                                                                 | Origin of the attempt (e.g., IP address).                                                                                                          | See<br>NDcPP21:FIA_UAU_EXT.2                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | See<br>NDcPP21:FIA_UAU_EXT.2                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | N/A                                                                                                    | N/A                                                                                                   |
| <b>NDcPP21:FIA_X509_EXT.1/ITT</b> | Unsuccessful attempt to validate a certificate. Any addition, replacement or removal of trust anchors in the TOE's trust store                                                                                                          | Reason for failure of certificate validation<br>Identification of certificates added, replaced or removed as trust anchor in the TOE's trust store | See<br>FIA_X509_EXT.1/Rev                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | See<br>FIA_X509_EXT.1/Rev                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | <b>IPsec</b><br>See failure audit in<br>NDcPP21:FCS_IPSEC_EXT.1<br><b>Updates to TrustStore</b><br>N/A | <b>IPsec</b><br>See failure audit in<br>NDcPP21:FCS_IPSEC_EXT.1<br><b>Updates to TrusStore</b><br>N/A |

|                            |                                                                                                                                |                                                                                                                                                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |     |     |
|----------------------------|--------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----|-----|
| NDcPP21:FIA_X509_EXT.1/Rev | Unsuccessful attempt to validate a certificate. Any addition, replacement or removal of trust anchors in the TOE's trust store | Reason for failure of certificate validation<br>Identification of certificates added, replaced or removed as trust anchor in the TOE's trust store | <p><b>IPsec</b></p> <p>Jan 30 19:19:08 SZ100 strongswan: 13[CFG] no issuer certificate found for "C=US, ST=MD, L=Catonsville, O=GSS, CN=subca-rsa, E=subca-rsa@gossamersec.com"</p> <p>Dec 31 12:37:51 SZ100 strongswan: 05[CFG] subject certificate invalid (valid from Dec 23 13:07:29 2019 to Dec 23 13:12:00 2019)</p> <p>Dec 31 14:47:47 SZ100 strongswan: 08[CFG] certificate was revoked on Dec 23 13:08:41 UTC 2019, reason: unspecified</p> <p>Mar 17 01:09:45 SZ100 strongswan: 07[CFG] ocsdp response verification failed, no signer certificate 'C=US, ST=MD, L=Catonsville, O=GSS, CN=server-ocsp-subca-ecdsa, E=server-ocsp-subca-ecdsa@gossamersec.com' found</p> <p>Dec 31 12:53:19 SZ100 strongswan: 09[LIB] OpenSSL X.509 parsing failed</p> <p>Dec 19 19:02:25 SZ100 strongswan: 12[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>Jan 27 19:28:43 SZ100 strongswan: 08[CFG] ocsdp request to http://172.16.161.1:7777 failed</p> <p><b>RadSec</b></p> <p>Mar 4 16:16:02 SZ100 ocsdp: Certificate has been expired/revoked</p> <p>Mar 3 15:57:43 SZ100 tls: error:0D0680A8:asn1 encoding routines:ASN1_CHECK_TLEN:wrong tag</p> <p>Mar 3 15:59:27 SZ100 tls: error:0407006A:rsa routines:RSA_padding_check_PKCS1_type_1:block type is not 01</p> <p>Mar 3 16:00:10 SZ100 tls: error:04091068:rsa routines:INT_RSA_VERIFY:bad signature</p> <p>Mar 13 18:14:36 SZ100 Extension Key usage(OCSP SIGNING) is not present, Terminating TLS connect..</p> <p>Mar 17 15:07:41 SZ100 tls: 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></p> <p>Mar 17 00:33:49 SZ100 Web Activity: "User:[admin],Browser IP:[172.16.16.253],Action:[Create],Resource:[Trusted CA Chain],Description:[Trusted CA Chain [ECDSA_New] created.]"</p> <p><b>Update Chain in Trust store</b></p> <p>Mar 17 15:31:58 SZ100 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></p> <p>Mar 31 23:37:03 SZ100 Web Activity: "User:[admin],Browser IP:[172.16.16.153],Action:[Delete],Resource:[Trusted CA Chain],Description:[Trust</p> <p><b>IPsec</b></p> <p>Feb 3 14:40:48 vszh strongswan: 08[CFG] no issuer certificate found for "C=US, ST=MD, L=Catonsville, O=GSS, CN=tl4-16x.example.com, E=server-ecdsa@gossamersec.com"</p> <p>Feb 3 13:50:34 vszh strongswan: 13[CFG] subject certificate invalid (valid from Jan 22 13:07:31 2020 to Jan 22 13:12:00 2020)</p> <p>Feb 4 16:02:19 vszh strongswan: 05[CFG] certificate was revoked on Jan 22 13:08:38 UTC 2020, reason: unspecified</p> <p>Feb 4 17:06:14 vszh strongswan: 05[CFG] ocsdp 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>Feb 3 14:31:20 vszh strongswan: 08[LIB] OpenSSL X.509 parsing failed</p> <p>Feb 3 12:02:00 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>Feb 3 14:56:02 vszh strongswan: 16[CFG] ocsdp request to http://172.16.16.1:7778 failed</p> <p><b>RadSec</b></p> <p>Mar 4 15:32:11 vszh ocsdp: Certificate has been expired/revoked</p> <p>Mar 3 15:44:56 vszh tls: error:0D0680A8:asn1 encoding routines:ASN1_CHECK_TLEN:wrong tag</p> <p>Mar 3 15:35:17 vszh tls: error:0407006A:rsa routines:RSA_padding_check_PKCS1_type_1:block type is not 01</p> <p>Mar 3 16:08:19 vszh tls: error:04091068:rsa routines:INT_RSA_VERIFY:bad signature</p> <p>Mar 13 19:35:29 vszh Extension Key usage(OCSP SIGNING) is not present, Terminating TLS connect..</p> <p>Mar 13 19:34:47 vszh tls: 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></p> <p>Mar 23 17:04:52 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></p> <p>Mar 13 19:16:35 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></p> <p>Mar 31 23:45:27 vszh Web Activity: "User:[admin],Browser IP:[172.16.16.153],Action:[Delete],Resource:[Tru</p> <td>N/A</td> <td>N/A</td> | N/A | N/A |
|----------------------------|--------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----|-----|

|                                |                                          |      |                                                                                                                                                                                                                                                                                                                                                                                                                |                                                                                                                                                                                                                                                                                                                                                                                                   |                                                                                                                                                                                                                                                                                                                         |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|--------------------------------|------------------------------------------|------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                |                                          |      | ed CA Chain [ECDSA_New] deleted.]"                                                                                                                                                                                                                                                                                                                                                                             | sted CA Chain],Description:[Trust ed CA Chain [ECDSA] deleted.]"                                                                                                                                                                                                                                                                                                                                  |                                                                                                                                                                                                                                                                                                                         |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| NDcPP21:FMT_MOF.1/ManualUpdate | Any attempt to initiate a manual update. | None | Mar 23 19:39:36 SZ100 Configurer: c.r.w.c.o.ClusterUpgrade OperationService - <OPT> [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] | Jan 27 13:05:28 vszh Configurer: c.r.w.c.o.ClusterUpgrade OperationService - <OPT> [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] | Mar 29 16:11:24 vszh Configurer: c.r.w.c.o.ClusterUploadVdpOperationService - <OPT> [UploadVDPFirmware] => patch info : fileName=vdv-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/ | Mar 4 15:32:21 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","zoneUID"="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"="" |



|                   |                                        |      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |     |     |
|-------------------|----------------------------------------|------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----|-----|
| NDcPP21:FMT_SMF.1 | All management activities of TSF data. | None | <p><b>Ability to administer the TOE locally and remotely</b><br/>See NDcPP21: FIA_UAU_EXT.2</p> <p><b>Configure the access banner</b><br/>Mar 31 18:38:40 SZ100<br/>Web Activity:<br/>"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><br/>Mar 31 19:15:36 SZ100<br/>Web Activity:<br/>"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><br/>See NDcPP21:FMT_MOF.1/ManualUpdate</p> <p><b>Configure Audit Behavior</b><br/>Mar 31 17:47:07 SZ100<br/>Configurer:<br/>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><br/>Mar 31 17:54:07 SZ100<br/>Web Activity:<br/>"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><br/>See NDcPP21:FCO_CPC_EXT.1</p> <p><b>Ability to set the time which is used for time-stamps</b><br/>See NDcPP21:FPT_STM_EXT.1</p> <p><b>Configure RadSec (reference identifier)</b><br/>Mar 31 18:12:24 SZ100<br/>Web Activity:<br/>"User:[admin],Browser IP:[172.16.16.153],Action:[Update],Resource:[Authentication Service],Description:[Authentication service [Radsec] updated.]"</p> <p><b>Resetting Passwords</b><br/>Feb 28 22:06:21 SZ100<br/>Web Activity:<br/>"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><b>Ability to administer the TOE locally and remotely</b><br/>See NDcPP21: FIA_UAU_EXT.2</p> <p><b>Configure the access banner</b><br/>Mar 30 14:08:34 vszh<br/>Web Activity:<br/>"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><br/>Mar 30 14:30:09 vszh<br/>Web Activity:<br/>"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><br/>See NDcPP21:FMT_MOF.1/ManualUpdate</p> <p><b>Configure Audit Behavior</b><br/>Mar 30 13:05:23 vszh<br/>Configurer:<br/>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><br/>Mar 29 16:09:16 vszh<br/>Web Activity:<br/>"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><br/>See NDcPP21:FCO_CPC_EXT.1</p> <p><b>Ability to set the time which is used for time-stamps</b><br/>See NDcPP21:FPT_STM_EXT.1</p> <p><b>Configure RadSec (reference identifier)</b><br/>Mar 13 19:17:08 vszh<br/>Web Activity:<br/>"User:[admin],Browser IP:[172.16.16.253],Action:[Update],Resource:[Authentication Service],Description:[Authentication service [Radsec] updated.]"</p> <p><b>Resetting Passwords</b><br/>Mar 30 12:48:22 vszh<br/>Web Activity:<br/>"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> | N/A | N/A |
|-------------------|----------------------------------------|------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----|-----|

|                             |                                                                                                                        |                                                                                              |                                                                                                                                                                                                                                                                                                                                                                                                                                                               |                                                                                                                                                                                                                                                                                                                                                                                               |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|-----------------------------|------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                             |                                                                                                                        |                                                                                              | <p>Mar 17 00:43:04 SZ100 Web Activity:<br/>"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><br/>Mar 31 21:22:53 SZ100 Web Activity:<br/>"User:[admin],Browser IP:[172.16.16.153],Action:[Delete],Resource:[Client Cert],Description:[Client Cert [Client] deleted.]"</p>                                                                      | <p>Mar 23 16:36:55 vszh Web Activity:<br/>"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><br/>Mar 30 16:54:30 vszh Web Activity:<br/>"User:[admin],Browser IP:[172.16.16.153],Action:[Delete],Resource:[Client Cert],Description:[Client Cert [ECDSA_Client] deleted.]"</p>   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>WLANASEP10:FPT_FLS.1</b> | Failure of the TSF.                                                                                                    | Indication that the TSF has failed with the type of failure that occurred.                   | The logging service is not initiated in a fail state. An error will be presented at the detection of the fail state.                                                                                                                                                                                                                                                                                                                                          | The logging service is not initiated in a fail state. An error will be presented at the detection of the fail state.                                                                                                                                                                                                                                                                          | The logging service is not initiated in a fail state. An error will be presented at the detection of the fail state.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | The logging service is not initiated in a fail state. An error will be presented at the detection of the fail state.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>NDcPP21:FPT_ITT.1</b>    | Initiation of the trusted channel.<br>Termination of the trusted channel.<br>Failure of the trusted channel functions. | Identification of the initiator and target of failed trusted channels establishment attempt. | <p><b>IPsec</b><br/>See<br/>WLANASEP10:FCS_IPSEC_EXT.1</p> <p><b>SSH</b></p> <p><b>Failure</b><br/>See<br/>NDcPP21:FCS_SSHS_EXT.1</p> <p><b>Establishment</b><br/>Mar 26 13:04:22 SZ100 sshd[27340]: Accepted publickey for sshunnel from 172.16.16.249 port 37194 ssh2: RSA SHA256:Rf7WBKnCLNV0R1D4R5paZQQTWInl7cwoQheehcoGRMY</p> <p><b>Termination</b><br/>Mar 26 20:24:31 SZ100 sshd[27340]: pam_unix(sshd:session): session closed for user sshunnel</p> | <p><b>SSH</b></p> <p><b>Failure</b><br/>See<br/>NDcPP21:FCS_SSHS_EXT.1</p> <p><b>Establishment</b><br/>Mar 4 14:22:38 vszh sshd[30619]: Accepted publickey for sshunnel from 172.16.8.248 port 50644 ssh2: RSA SHA256:ioKMgn7kIMOybSZQWANl43f04L1KHio/Zalq82n0qRM</p> <p><b>Termination</b><br/>Mar 4 14:54:45 vszh sshd[30619]: pam_unix(sshd:session): session closed for user sshunnel</p> | <p><b>IPsec</b><br/>See<br/>WLANASEP10:FCS_IPSEC_EXT.1</p> <p><b>SSH</b></p> <p><b>Failure</b><br/>See<br/>NDcPP21:FCS_SSHC_EXT.1</p> <p><b>Establishment</b><br/>Mar 29 16:18:30 vszh Core:<br/>@@@512,dpConnected,"dpKey"="97HM3WVA5234U0JPM34HJEUJ1XTA000C29B4693A000C29B46944","timestamp"="1585498710059","cpName"="vszh","wsgIP"="172.16.8.230"</p> <p><b>Termination</b><br/>Mar 23 22:07:33 vszh Core:<br/>@@@513,dpDisconnected,"dpKey"="97HM3WVA5234U0JPM34HJEUJ1XTA000C29B4693A000C29B46944","timestamp"="1585001239636","cpName"="vszh","wsgIP"="172.16.8.230","reason"="1, NMI problem."</p> | <p><b>IPsec</b><br/>See<br/>WLANASEP10:FCS_IPSEC_EXT.1</p> <p><b>SSH</b></p> <p><b>Failure</b><br/>See<br/>NDcPP21:FCS_SSHC_EXT.1</p> <p><b>Establishment</b><br/>Mar 18 16:05:01 vszh Core:<br/>@@@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><br/>Mar 29 16:07:27 vszh Core:<br/>@@@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>NDcPP21:FPT_STM_EXT.1</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) | 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). | Feb 17 19:07:35 SZ100 Core: @@99301,disContTime Change, "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"                                                                                                                                                                                                                                                                                                                                                               | Feb 21 22:57:42 vszh Core: @@99301,disContTime Change, "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"                                                                                                                                                                                                                                                                                                                                                   | Feb 21 22:58:45 vszh Core: @@99211,dpDiscontinuousTimeChangeNTPServerdpNtpTimeSync,"dpKey"="97HM3WVA5234U0JPM34HJEUJ1XTA000C29B4693A000C29B46944", "before"="02/21/2020-04:59:01 PM", "after"="02/21/2020-10:58:45 PM", "source"="10.254.1.1"                                                                                                                                                              | Mar 4 15:32:20 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>WLANASEP10:FPT_TST_EXT.1</b> | Execution of this set of TSF self-tests. Detected integrity violations.                                                                                                                                    | For integrity violations, the TSF code file that caused the integrity violation.                                                                         | The logging service is not initiated in a fail state. An error will be presented at the detection of the fail state.                                                                                                                                                                                                                                                                                                                                                                                                                                 | The logging service is not initiated in a fail state. An error will be presented at the detection of the fail state.                                                                                                                                                                                                                                                                                                                                                                                                                    | The logging service is not initiated in a fail state. An error will be presented at the detection of the fail state.                                                                                                                                                                                                                                                                                       | The logging service is not initiated in a fail state. An error will be presented at the detection of the fail state.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>NDcPP21:FPT_TUD_EXT.1</b>    | Initiation of update; result of the update attempt (success or failure).                                                                                                                                   | None                                                                                                                                                     | <b>Initiation</b><br>See FMT_MOF.1 / ManualUpdate<br><br><b>Update Result</b><br>Mar 23 20:14:54 SZ100 Core: c.r.w.s.c.MainChannelDirectiveListener - receieved 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>Initiation</b><br>See FMT_MOF.1 / ManualUpdate<br><br><b>Update Result</b><br>Jan 27 13:33:41 vszh Core: c.r.w.s.c.MainChannelDirectiveListener - receieved 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>Initiation</b><br>See FMT_MOF.1 / ManualUpdate<br><br><b>Update Result</b><br>Mar 29 16:11:24 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>Initiation</b><br>See FMT_MOF.1 / ManualUpdate<br><br><b>Update Result</b><br>Mar 27 15:27:37 SZ100 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>NDcPP21:FTA_SSL.3</b>        | The termination of a remote session by the session locking mechanism.                                                                                                                                      | None                                                                                                                                                     | <b>WebUi</b><br>Mar 27 15:11:16 SZ100 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].]"<br><br><b>SSH</b><br>Mar 27 19:20:04 SZ100 sshd[21178]: pam_unix(sshd:session): session closed for user admin                                                                                                                                                                                                        | <b>WebUi</b><br>Mar 4 08:59:16 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].]"<br><br><b>SSH</b><br>Mar 27 19:20:04 SZ100 sshd[21178]: pam_unix(sshd:session): session closed for user admin                                                                                                                                                                                             | N/A                                                                                                                                                                                                                                                                                                                                                                                                        | N/A                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |

|                              |                                                                                                                  |                                                                                              |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |     |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|------------------------------|------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>NDcPP21:FTA_SSL.4</b>     | The termination of an interactive session.                                                                       | None                                                                                         | <b>WebUI</b><br>Mar 27 19:11:55 SZ100<br>Web Activity:<br>"User:[admin],Browser IP:[172.16.16.253],Action:[Log off],Resource:[Administrator],Description:[Administrator [admin] logged off from [172.16.16.253].]"<br><br><b>SSH</b><br>Mar 27 19:39:22 SZ100<br>Web Activity:<br>"User:[admin],Browser IP:[172.16.16.253],Action:[Log off],Resource:[Administrator],Description:[Administrator [admin] logged off from CLI.]"<br><br><b>CLI</b><br>Mar 27 19:47:31 SZ100<br>Web Activity:<br>"User:[admin],Browser IP:[127.0.0.1],Action:[Log off],Resource:[Administrator],Description:[Administrator [admin] logged off from CLI.]" | <b>WebUI</b><br>Feb 28 20:06:32 vszh<br>Web Activity:<br>"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].]"<br><br><b>SSH</b><br>Feb 28 19:12:05 vszh<br>Web Activity:<br>"User:[admin],Browser IP:[172.16.16.253],Action:[Log off],Resource:[Administrator],Description:[Administrator [admin] session timeout to logged off from CLI.]"<br><br><b>CLI</b><br>Mar 2 11:15:53 vszh<br>Web Activity:<br>"User:[admin],Browser IP:[127.0.0.1],Action:[Log off],Resource:[Administrator],Description:[Administrator [admin] logged off from CLI.]" | N/A | N/A                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>NDcPP21:FTA_SSL_EXT.1</b> | The termination of a local session by the session locking mechanism.                                             | None                                                                                         | Mar 27 20:06:53 SZ100<br>Web Activity:<br>"User:[admin],Browser IP:[127.0.0.1],Action:[Log off],Resource:[Administrator],Description:[Administrator [admin] logged off from CLI.]"                                                                                                                                                                                                                                                                                                                                                                                                                                                     | Mar 26 13:52:36 vszh<br>Web Activity:<br>"User:[admin],Browser IP:[172.16.16.153],Action:[Log off],Resource:[Administrator],Description:[Administrator [admin] logged off from CLI.]"                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | N/A | N/A                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>WLANASEP10:FTA_TSE.1</b>  | Denial of a session establishment due to the session establishment mechanism.                                    | Reason for denial, origin of establishment attempt.                                          | N/A                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | N/A                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | N/A | 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:<br>Apr 22 15:22:03 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>NDcPP21:FTP_ITC.1</b>     | Initiation of the trusted channel. Termination of the trusted channel. Failure of the trusted channel functions. | Identification of the initiator and target of failed trusted channels establishment attempt. | <b>IPsec</b><br>See WLANASEP10:FCS_IP SEC_EXT.1                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | <b>IPsec</b><br>See WLANASEP10:FCS_IP SEC_EXT.1                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | N/A | N/A                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |

|                                |                                                                                                                    |                                                        |                                                                                                                                                                                                                                                                                                                                                                              |                                                                                                                                                                                                                                                                                                                                                                              |                                                                                                                                                                                                                                                                                                                                                                                                                   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|--------------------------------|--------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>WLANASEP10:FTP_ITC.1</b>    | Failed attempts to establish a trusted channel (including IEEE 802.11). Detection of modification of channel data. | Identification of the initiator and target of channel. | <p><b>IPsec</b><br/>See<br/>WLANASEP10:FCS_IP_SEC_EXT.1</p> <p><b>RadSec</b><br/>See<br/>NDcPP21:FCS_TLSC_EXT.1</p>                                                                                                                                                                                                                                                          | <p><b>IPsec</b><br/>See<br/>WLANASEP10:FCS_IP_SEC_EXT.1</p> <p><b>RadSec</b><br/>See<br/>NDcPP21:FCS_TLSC_EXT.1</p>                                                                                                                                                                                                                                                          | <p><b>IPsec</b><br/>See<br/>WLANASEP10:FCS_IP_SEC_EXT.1</p>                                                                                                                                                                                                                                                                                                                                                       | <p><b>IEEE 802.11-2012 (WPA2) / IEEE 802.1X</b><br/>Mar 13 19:35:29 vszh Core:<br/>@@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","tenantUID"="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"=""</p> |
| <b>NDcPP21:FTP_TRP.1/Admin</b> | Initiation of the trusted path. Termination of the trusted path. Failure of the trusted path functions.            | None                                                   | <p><b>Initiation</b><br/>See<br/>NDcPP21:FIA_UAU_EXT.2</p> <p><b>Termination</b><br/>See<br/>NDcPP21:FTA_SSL.4</p> <p><b>Failure</b></p> <p><b>Web UI</b><br/>See<br/>NDcPP21:FCS_TLSS_EXT.1 and<br/>NDcPP21:FCS_HTTPS_EXT.1</p> <p><b>SSH</b><br/>See<br/>NDcPP21:FCS_SSHS_EXT.1</p>                                                                                        | <p><b>Initiation</b><br/>See<br/>NDcPP21:FIA_UAU_EXT.2</p> <p><b>Termination</b><br/>See<br/>NDcPP21:FTA_SSL.4</p> <p><b>Failure</b></p> <p><b>Web UI</b><br/>See<br/>NDcPP21:FCS_TLSS_EXT.1 and<br/>NDcPP21:FCS_HTTPS_EXT.1</p> <p><b>SSH</b><br/>See<br/>NDcPP21:FCS_SSHS_EXT.1</p>                                                                                        | N/A                                                                                                                                                                                                                                                                                                                                                                                                               | N/A                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>NDcPP21:FTP_TRP.1/Join</b>  | Initiation of the trusted path. Termination of the trusted path. Failure of the trusted path functions.            | None                                                   | <p><b>Initiation &amp; Termination</b><br/>See<br/>NDcPP21:FCO_CPC_EXT.1</p> <p><b>Failure</b><br/>As the join requests are initiated by the AP and vSZ-D, all failures are generated by the AP and vSZ-D at the time of the join attempt. If the join request is delivered successfully than there is no case where a failure would be registered by the SZ controller.</p> | <p><b>Initiation &amp; Termination</b><br/>See<br/>NDcPP21:FCO_CPC_EXT.1</p> <p><b>Failure</b><br/>As the join requests are initiated by the AP and vSZ-D, all failures are generated by the AP and vSZ-D at the time of the join attempt. If the join request is delivered successfully than there is no case where a failure would be registered by the SZ controller.</p> | <p><b>Initiation &amp; Termination</b><br/>See<br/>NDcPP21:FCO_CPC_EXT.1</p> <p><b>Failure</b><br/>The vSZ-D wont log to the SZ controller if the SSH connection is broken. A local log can be pulled from the vSZ-D if required:</p> <p>2020-04-02T00:44:42+00:00<br/>esxidp dpm[3942]:<br/>@@99231,dpHttpsConn Failed,"dpKey"="97HM3WVA5234U0JPM34HJEUJ1XTA000C29B4693A000C29B46944","scgIP"="172.16.8.230"</p> | <p><b>Initiation &amp; Termination</b><br/>See<br/>NDcPP21:FCO_CPC_EXT.1</p> <p><b>Failure</b><br/>The AP wont log to the SZ controller if the SSH connection is broken. A local log can be pulled from the AP if required:</p> <p>Apr 2 00:39:45 T710 local0.err<br/>remotelid[1210]:<br/>connect failed, reason: Connection refused<br/>Apr 2 00:39:45 T710 local0.info<br/>remotelid[1210]: fail to connect to SCG...</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |



© 2019 CommScope, Inc. All rights reserved.  
Ruckus Wireless, Inc., a wholly owned subsidiary of CommScope, Inc.  
350 West Java Dr., Sunnyvale, CA 94089 USA  
[www.ruckuswireless.com](http://www.ruckuswireless.com)