

# Ruckus FIPS and Common Criteria Configuration Guide for SmartZone and AP, 5.1.2

Supporting SmartZone Release 5.1.2

# Copyright, Trademark and Proprietary Rights Information

© 2019 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, Ruckus Networks, Ruckus logo, the Big Dog design, BeamFlex, ChannelFly, Edgelron, FastIron, HyperEdge, ICX, IronPoint, OPENG, SmartCell, Unleashed, Xclaim, and ZoneFlex 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

---

<b>Preface.....</b>	<b>7</b>
Document Conventions.....	7
Notes, Cautions, and Warnings.....	7
Command Syntax Conventions.....	8
Document Feedback.....	8
Ruckus Product Documentation Resources.....	8
Online Training Resources.....	9
Contacting Ruckus Customer Services and Support.....	9
What Support Do I Need?.....	9
Open a Case.....	9
Self-Service Resources.....	9
<b>About This Guide.....</b>	<b>11</b>
What's New in This Document.....	11
<b>Federal Information Processing Standards.....</b>	<b>13</b>
FIPS Overview.....	13
Crypto Officer Roles and Responsibilities.....	13
Zeroization Process.....	14
Quarantine State.....	14
<b>vSZ Installation with FIPS Image.....</b>	<b>17</b>
vSZ Installation Prerequisites for FIPS.....	17
Creating and Registering the Virtual Machine.....	17
Using FIPS-Related CLI Commands (vSZ).....	21
Viewing and Downloading FIPS Logs.....	26
Uploading Certificates to SmartZone OS.....	28
Enabling Other Secured Communication Services.....	31
Entity MIB Groups.....	33
Secured Client Authentication Services.....	40
Configuring Proxy Active Directory (AD).....	41
Configuring an LDAP Server.....	44
RadSec (RADIUS over TLS).....	46
Configuring RadSec.....	46
Mapping the Authentication Profile for the WLAN.....	58
Viewing the WLAN Configurations List.....	60
Authentication Using Common Access Card or Personal Identity Verification.....	62
Two-Factor Authentication.....	62
Three-Factor Authentication.....	64
Configuring AAA Servers.....	66
Enabling Common Access Card or Personal Identity Verification Authentication.....	71
Wireless Intrusion Detection and Prevention Services.....	72
Classifying a Rogue Policy.....	73
Creating a Monitoring AP Group.....	74
Rogue Devices.....	77
Creating an AP MAC OUI Address.....	79
<b>vSZ-D FIPS Installation with FIPS Image.....</b>	<b>81</b>

vSZ-D FIPS Installation Prerequisites for FIPS.....	81
Creating and Registering the Virtual Machine (vSZ-D).....	81
Joining vSZ-D to the vSZ Controller.....	87
Using FIPS CLI Commands (vSZ-D).....	90
Downloading vSZ-D FIPS Logs.....	93
<b>AP Configuration in FIPS Mode.....</b>	<b>95</b>
AP Models that Support FIPS Mode.....	95
FIPS AP Behavior.....	95
Crypto Officer Roles and Responsibilities for AP.....	96
Quarantine State for AP.....	96
AP Features Not Supported in FIPS Mode.....	97
Recovery SSID Not Supported.....	98
FTP, TFTP, and Web Not Supported.....	99
HTTP and Telnet Management Access Not Supported.....	99
Web Interface Access Through HTTPS Not Supported.....	100
SNMPv1 and SNMPv2c Not Supported.....	101
WLAN Interface Up or Down from AP CLI Not Supported.....	102
<b>X.509 Certificates.....</b>	<b>103</b>
Validating Certificates.....	103
Configuring X.509 Server Certificates on the Controller.....	105
Uploading X.509 Certificates on vSZ-D.....	108
<b>Password Management.....</b>	<b>111</b>
<b>Session Management.....</b>	<b>113</b>
<b>Configuring the WLAN Scheduler.....</b>	<b>115</b>
Setting the WLAN Scheduler from the CLI.....	116
<b>Configuring Global and Account Security Settings.....</b>	<b>119</b>
<b>Terminating Sessions.....</b>	<b>123</b>
Terminating Sessions for Non-Admin Users.....	124
Terminating Administrator Sessions.....	125
<b>Locking an Administrator Account .....</b>	<b>127</b>
Locking Non-Administrator Accounts.....	128
<b>Setting Up the Login Banner.....</b>	<b>133</b>
<b>IPsec Tunnel Setup.....</b>	<b>135</b>
<b>Configuring System IPsec using Preshared Key.....</b>	<b>137</b>
<b>Configuring System IPsec using Certificates.....</b>	<b>141</b>
<b>Configuring System Time.....</b>	<b>145</b>
<b>Configuring SoftGRE and IPsec in the WLAN.....</b>	<b>147</b>
<b>Configuring Ruckus GRE and IPsec in the WLAN.....</b>	<b>149</b>
<b>Auditable Events in AP and DP for Common Criteria.....</b>	<b>151</b>
<b>Tamper-Evident Seals.....</b>	<b>153</b>
General Information about Tamper-Evident Seals.....	153
Tamper-Evident Seals on SmartZone 100 Devices.....	153



Tamper-Evident Seals on SmartZone 300 Devices.....	157
Tamper-Evident Seals on T610 AP Devices.....	159
Tamper-Evident Seals on T710 AP Devices.....	159
Tamper-Evident Seals on R610 AP Devices.....	161
Tamper-Evident Seals on R710 AP Devices.....	162
Tamper-Evident Seals on R720 AP Devices.....	164
Tamper-Evident Seals on E510 AP Devices.....	165
<b>Trusted Channels Through TSF.....</b>	<b>169</b>
Trusted Communication Channels.....	169
Enabling Trusted Channel Using IEEE 802.11-2012 (WPA2) Standards .....	169
Enabling Trusted Channel Using IEEE 802.1X and IPsec.....	170
<b>FIPS-Compliant Products.....</b>	<b>171</b>
AP Controller Matrix.....	171
FIPS-Compliant Product SKUs and Descriptions.....	171



# Preface

- Document Conventions..... 7
- Command Syntax Conventions..... 8
- Document Feedback..... 8
- Ruckus Product Documentation Resources..... 8
- Online Training Resources..... 9
- Contacting Ruckus Customer Services and Support..... 9

## Document Conventions

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

**TABLE 1** Text Conventions

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

## Notes, Cautions, and Warnings

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

### NOTE

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

### ATTENTION

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



### CAUTION

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



### DANGER

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

# Command Syntax Conventions

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

Convention	Description
<b>bold text</b>	Identifies command names, keywords, and command options.
<i>italic text</i>	Identifies a variable.
[ ]	Syntax components displayed within square brackets are optional. Default responses to system prompts are enclosed in square brackets.
{ <b>x</b>   <b>y</b>   <b>z</b> }	A choice of required parameters is enclosed in curly brackets separated by vertical bars. You must select one of the options.
<b>x</b>   <b>y</b>	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 Ruckus 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.
- 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>

## Preface

### Contacting Ruckus Customer Services and Support

- 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](https://support.ruckuswireless.com/#products_grid)
- Security Bulletins—<https://support.ruckuswireless.com/security>

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

# About This Guide

- [What's New in This Document](#)..... 11

## What's New in This Document

**TABLE 2** Summary of Enhancements in FIPS Release 5.1.2

Feature	Description	Location
Wireless Intrusion Prevention Services (WIPS)	WIPS is a security system that monitors a WLAN for any threats from rogue devices through a monitoring AP.	Refer to <a href="#">Wireless Intrusion Detection and Prevention Services</a> on page 72 for more information.
Common Access Card/Personal Identity Verification (CAC/PIV) two-factor authentication	Testing the AAA server if the existing user name is associated with any user group.	Refer to <a href="#">Testing AAA Server (Auth)</a> for more information.
Certification Authority (CA)/Subject Alternate Name (SAN) Identity	The certificates use the CA/SAN to validate the configured identity.	Refer to <a href="#">Configuring AAA Servers</a> on page 66 for more information.
Password Management	Changing the administrator password and configuring the account lockout option.	Refer to <a href="#">Password Management</a> on page 111 for more information.
Session Management	Configuring the global and account security settings.	Refer to <a href="#">Configuring Global and Account Security Settings</a> on page 119 for more information.
Account Management	Display of consent banner and account activities pages.	Refer to <a href="#">Session Management</a> on page 113.
Spare NTP	NTP authentication for primary and backup servers is introduced.	Refer to <a href="#">Configuring System Time</a> for more information.
SNMP	Entity MIB groups supported only in the SZ300 and SZ100 platforms are introduced.	Refer to <a href="#">Entity MIB Groups</a> on page 33 for more information.
Change Default Switch Group behavior on SZ-100 and rename the group on SZ300	Minor updates made in the SmartZone Switch Management section.	Refer to the SmartZone Switch Management section for more information.
Show port details when user hovers mouse over a port icon		





# Federal Information Processing Standards

---

- FIPS Overview..... 13
- Crypto Officer Roles and Responsibilities..... 13
- Zeroization Process..... 14
- Quarantine State..... 14

## FIPS Overview

A device in Federal Information Processing Standards (FIPS) mode is compliant with the standards established by the United States government 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.

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:

- The device software is placed in FIPS mode with the FIPS security policy applied.
- Tamper-evident security seals labels are applied to the device according to the instructions included in [Tamper-Evident Seals](#) on page 153. The accessory kit must be purchased separately.
- The device software is placed in FIPS mode with the FIPS security policy 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.

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.

### NOTE

You can change the FIPS mode to trigger zeroization. On SmartZone controllers, you can change the FIPS mode by using the **fips enable** or **fips disable** commands. On vSZ-D, you can use the **fips zeroization** command.

For the vSZ-D or the AP, SmartZone pushes the configuration information and the CO (admin) does not need to configure the vSZ-D or the AP separately.

## 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) 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

- vSZ Installation Prerequisites for FIPS..... 17
- Creating and Registering the Virtual Machine..... 17
- Using FIPS-Related CLI Commands (vSZ)..... 21
- Viewing and Downloading FIPS Logs..... 26
- Uploading Certificates to SmartZone OS..... 28
- Enabling Other Secured Communication Services..... 31
- Secured Client Authentication Services..... 40
- RadSec (RADIUS over TLS)..... 46
- Authentication Using Common Access Card or Personal Identity Verification..... 62
- Wireless Intrusion Detection and Prevention Services..... 72

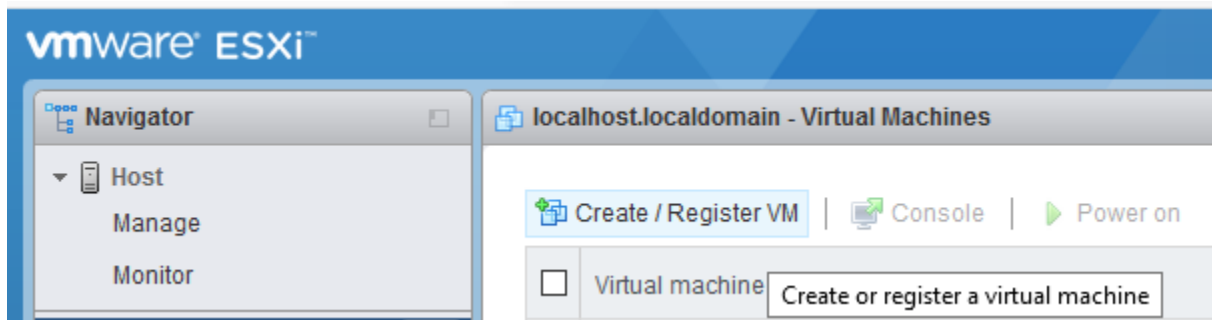
## vSZ Installation Prerequisites for FIPS

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

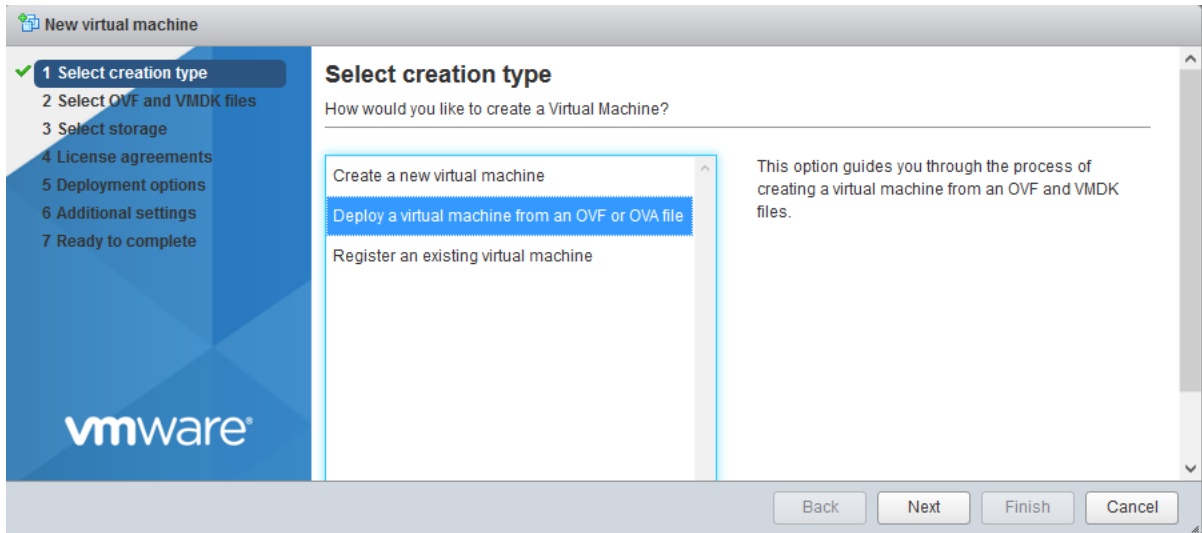
1. Install and deploy the .ova file on VMware ESXi using the **Create/Register VM** option, as shown in the following figure.

**FIGURE 3** Create and register VM



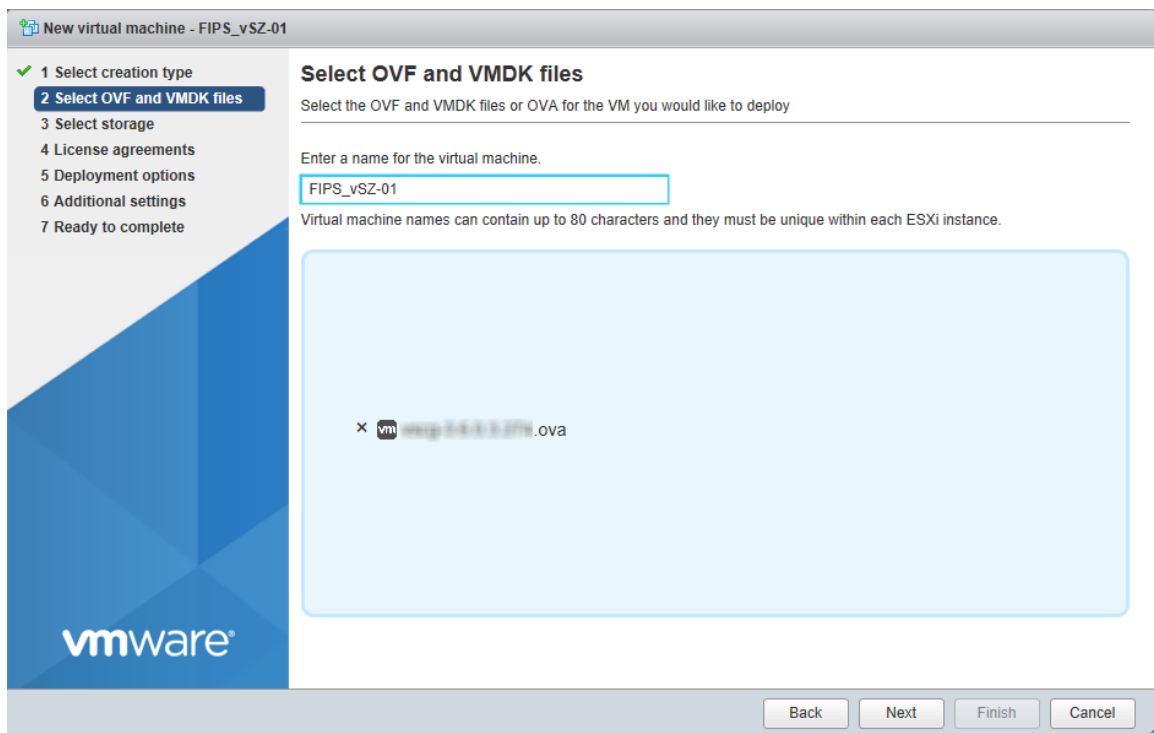
2. Select **Deploy a virtual machine from an OVF or OVA file**.

**FIGURE 4** Selecting the Creation Type



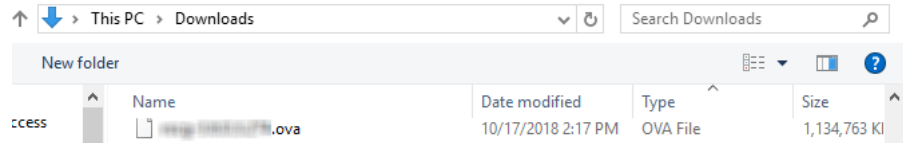
3. Click **Next** to select the OVF and VMDK files.
4. Enter the name of the VM and click the name of the OVF and VDMK file, as shown in the following figure.

**FIGURE 5** Selecting OVF and VMDK Files

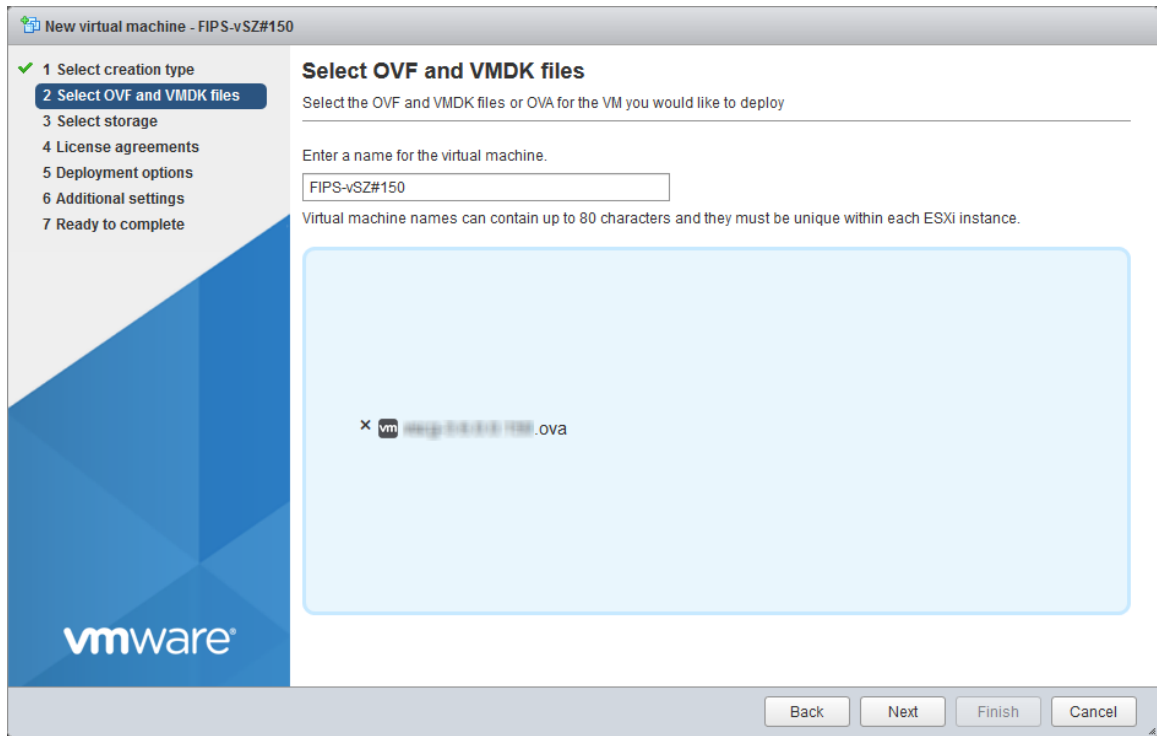


5. Select the .ova file from the browse window. The selected file is displayed in **Select OVF and VMDK** files screen

**FIGURE 6** Selecting the .ova File



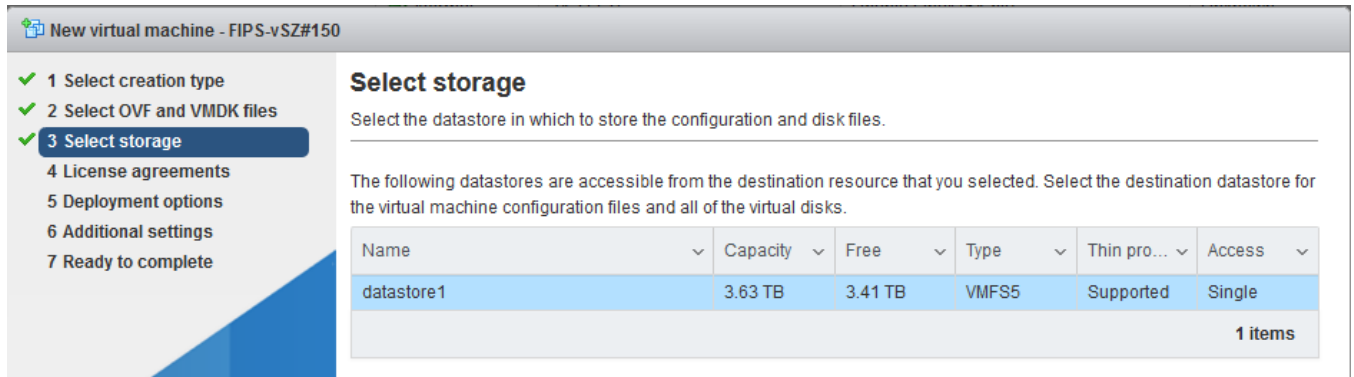
**FIGURE 7** Selected .ova File



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

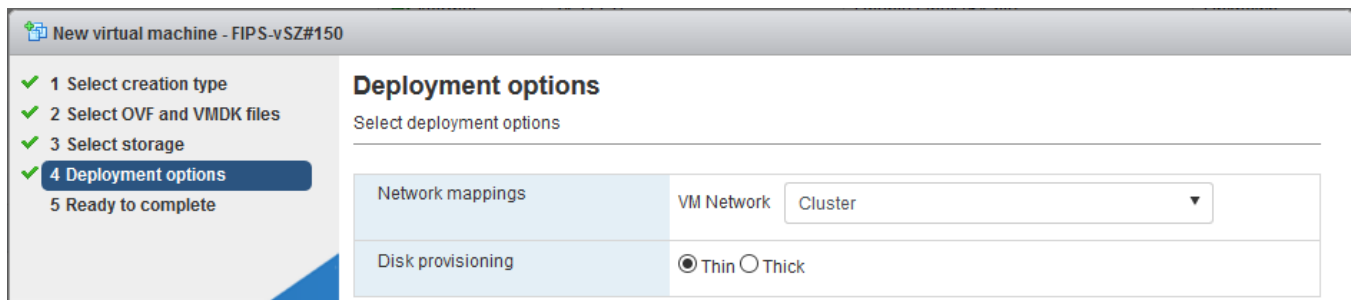
7. Select the required datastore.

**FIGURE 8** Selecting the Datastore



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

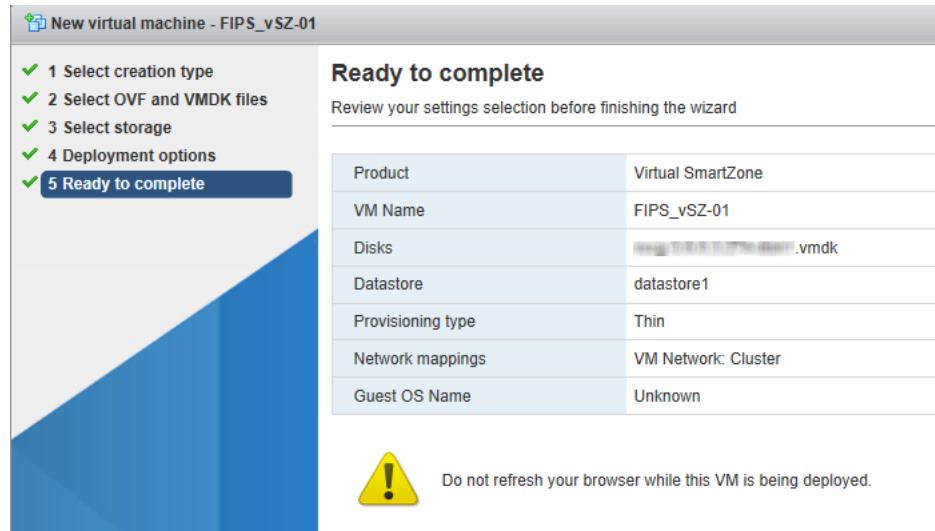
**FIGURE 9** Selecting Deployment Options





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

**FIGURE 10** Ready to complete installation



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

**FIGURE 11** Successful installation

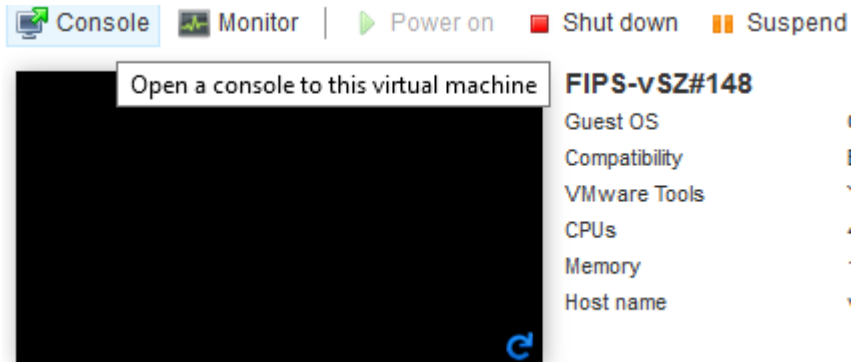
Recent tasks							
Task	Target	Initiator	Queued	Started	Result	Completed	
Power On VM	FIPS_vSZ-01	root	12/09/2018 07:22:20	12/09/2018 07:22:20	Completed successfully	12/09/2018 07:22:23	
Import VApp	Resources	root	12/09/2018 07:17:49	12/09/2018 07:17:49	Completed successfully	12/09/2018 07:22:19	

## Using FIPS-Related CLI Commands (vSZ)

- 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



- 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: 3.4.4.3.209

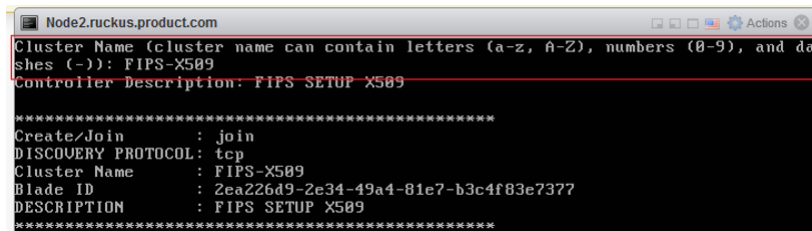
FIPS-12> en
Password: *****

FIPS-12# █
```

**NOTE**

The cluster name must be more than eight characters long to comply with FIPS and NIST requirements.

**FIGURE 16** Sample Cluster Name



```
Node2.ruckus.product.com
Cluster Name (cluster name can contain letters (a-z, A-Z), numbers (0-9), and dashes (-)): FIPS-X509
Controller Description: FIPS_SETUP X509

*****
Create/Join      : join
DISCOVERY PROTOCOL: tcp
Cluster Name    : FIPS-X509
Blade ID       : 2ea226d9-2e34-49a4-81e7-b3c4f83e7377
DESCRIPTION    : FIPS_SETUP X509
*****
```

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

**FIGURE 17** 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 _
```

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

**FIGURE 18** 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.

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

**FIGURE 19** 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 20** 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 21** 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

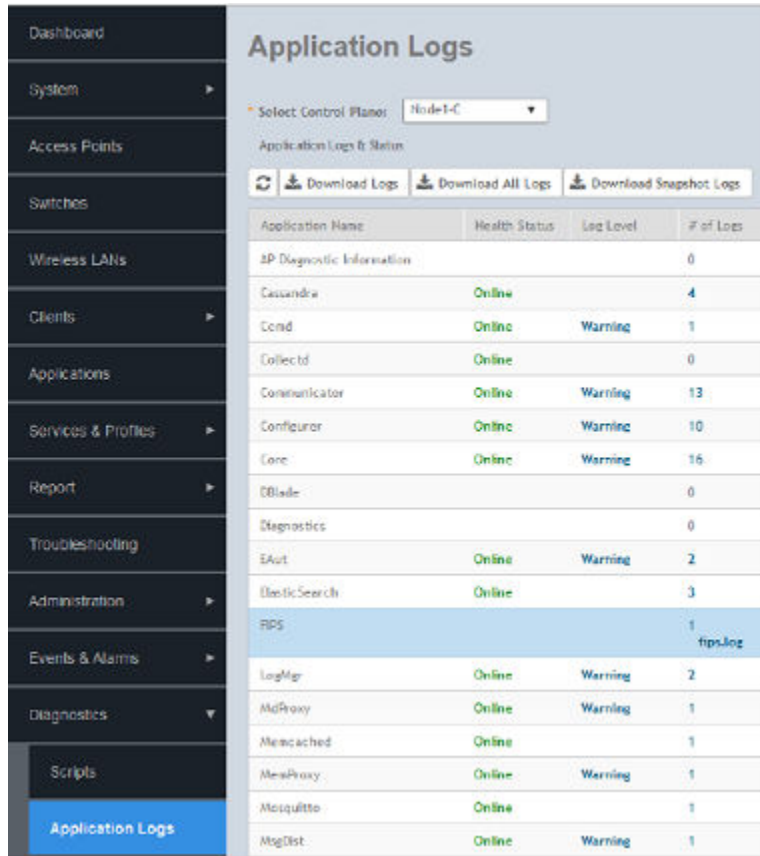
Node1# █
```

## Viewing and Downloading FIPS Logs

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

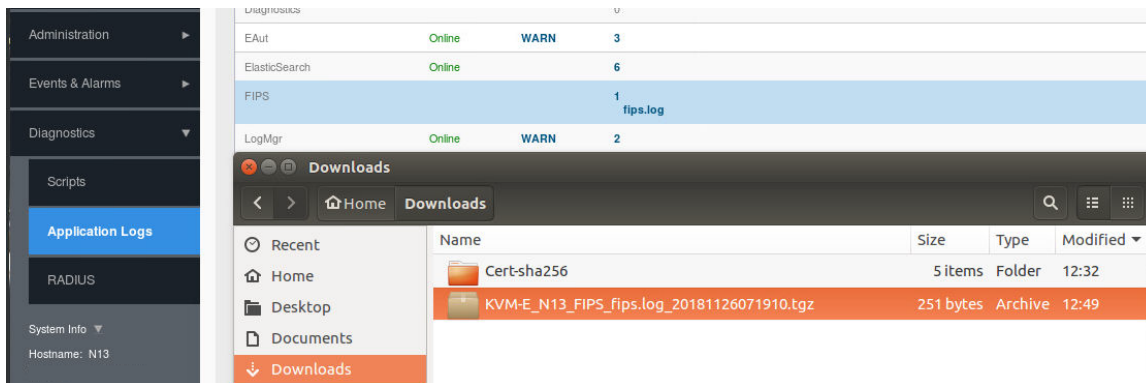
In the web interface, navigate to **Diagnostics > Application Logs > FIPS** to download the logs to the local machine.

**FIGURE 22** Using the Web Interface to Download FIPS Logs



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

**FIGURE 23** Downloaded FIPS Logs

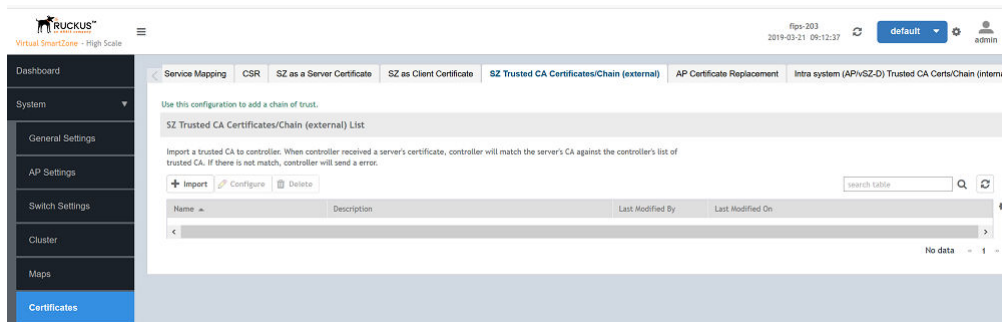


# Uploading Certificates to SmartZone OS

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 24** 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 25** Name and Description of the Certificate

## Import CA Certs (Chain)

\* Name:

Description:

Intermediate CA Certificates:

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

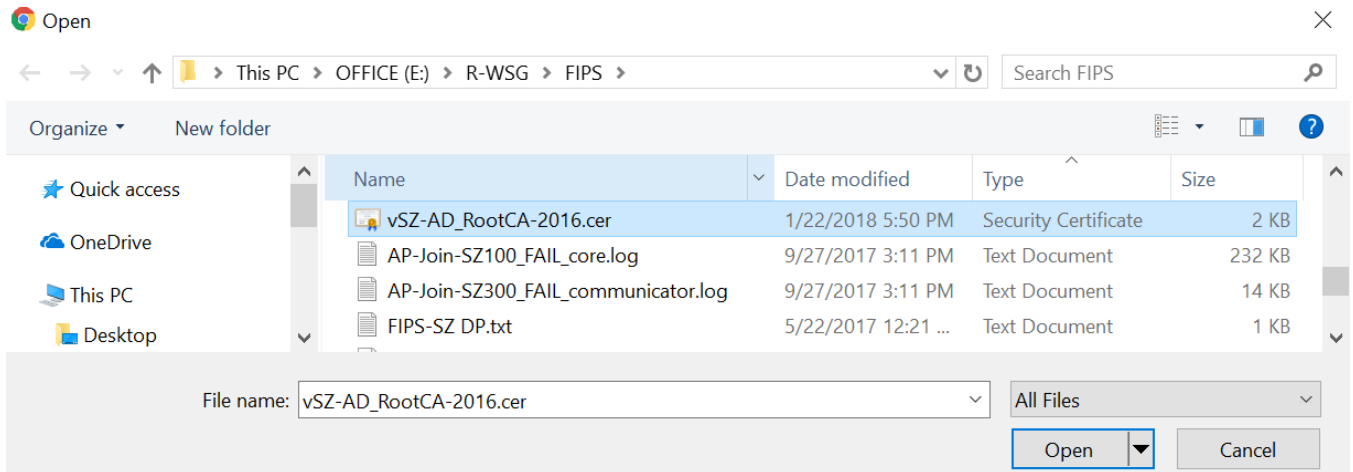
\* Root CA Certificate:

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 26** Selecting the Certificate



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

**FIGURE 27** Successful Certificate Import

## Import CA Certs (Chain)

The screenshot shows the "Import CA Certs (Chain)" dialog box. It has a close button in the top right corner. The fields are as follows:

- Name:** RadSec\_subCA-chain#1
- Description:** (empty text box)
- Intermediate CA Certificates:** A list with four rows. The first row has a checked checkbox and the text "ca-chain.cert.pem". Each row has "Browse" and "Clear" buttons.
- Root CA Certificate:** A checked checkbox and the text "ca.cert.pem". It has "Browse" and "Clear" buttons.

# Enabling Other Secured Communication Services

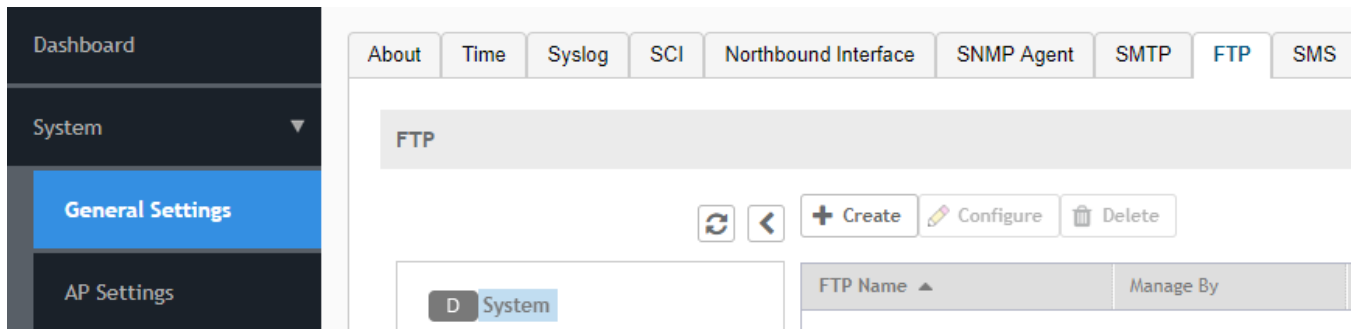
The following secured communication services are available in FIPS:

- SFTP
- SNMP
- SMTP
- Syslog

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 28** Selecting FTP

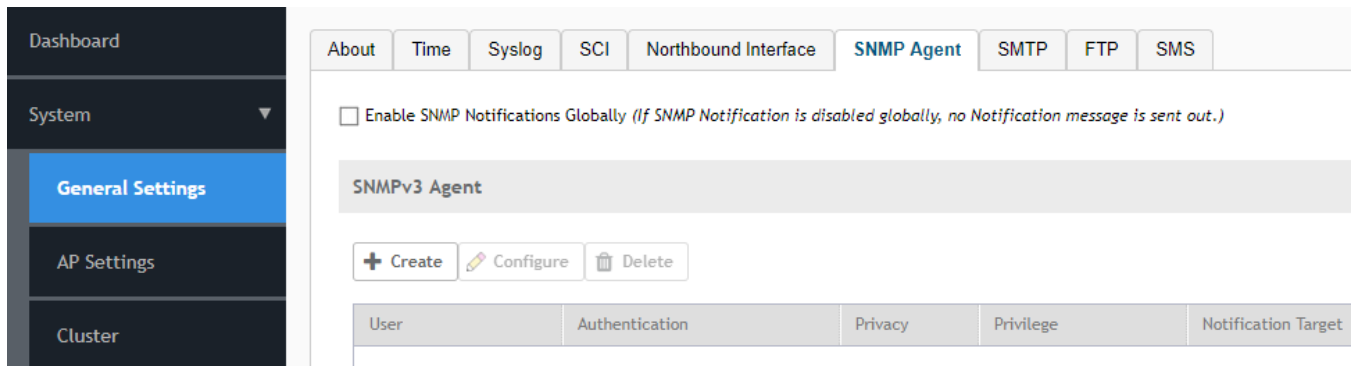


2. To enable the SNMP agent, in the web interface, navigate to **System > General Settings > SNMP Agent**. Enable the option for SNMP notifications.

**NOTE**

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

**FIGURE 29** Selecting the SNMP Agent



3. Click **Create** to create the SNMPv3 agent and configure the following options:
  - Enter a user name.
  - Select **Authentication**.
  - For **Auth Pass Phrase**, enter an authentication pass phrase.
  - Select **Privacy**.
  - Select **Privilege**.

**NOTE**

Only SHA is supported as the authentication method. Only AES is supported for privacy.

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

**FIGURE 30** Selecting the SMTP Server

Dashboard

System

General Settings

AP Settings

Cluster

Maps

Certificates

Templates

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

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

Enable SMTP Server

Logon Name:

Password:

\* SMTP Server Host:

\* SMTP Server Port:

\* Mail From:

From Display Name: Ruckus Support

\* Mail To:

Encryption Options:  TLS

Refresh OK Cancel Test

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

**FIGURE 31** Selecting the Syslog Server

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

Enable logging to remote syslog server

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

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

\* Application Logs Facility:  \* Filter Severity:

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

\* Other Logs Filter Severity:

\* Event Facility:

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

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

## Entity MIB Groups

The Entity MIB module represents multiple logical entities supported by a single SNMP agent. The following tables are the Entity MIB groups supported only in the SZ300 and SZ100 platforms.

### entityPhysical

The collection of objects that are used to represent physical system components where a single agent provides management information.

**TABLE 3** entPhysicalTable

OID	Name	Syntax	Description	Note
.1.3.6.1.2.1.47.1.1.1.1.1	entPhysicalIndex	PhysicalIndex Range is from 1 through 2147483647	The index for this entry	The index for this entry.
.1.3.6.1.2.1.47.1.1.1.1.2	entPhysicalDescr	SnmpAdminString	A textual description of the physical entity. This object must contain a string that identifies the manufacturer's name for the physical entity, and must be set to a	

**TABLE 3 entPhysicalTable (continued)**

OID	Name	Syntax	Description	Note
			distinct value for each version or model of the physical entity.	
.1.3.6.1.2.1.47.1.1.1.1.3	entPhysicalVendorType	AutonomousType	<p>An indication of the vendor-specific hardware type of the physical entity. Note that this is different from the definition of MIB-II's sysObjectID.</p> <p>An agent must set this object to a enterprise-specific registration identifier value, indicating the specific equipment type in detail. The associated instance of entPhysicalClass is used to indicate the general type of hardware device.</p> <p>If no vendor-specific registration identifier exists for this physical entity or the value is unknown by this agent, then the value { 0 0 } is returned.</p>	
.1.3.6.1.2.1.47.1.1.1.1.4	entPhysicalContainedIn	INTEGER Range is from 1 through 2147483647	<p>The value of entPhysicalIndex for the physical entity which contains this physical entity. A value of zero indicates this physical entity is not contained in any other physical entity. Note that the set of containment relationships define a strict hierarchy and recursion is not allowed.</p> <p>In the event a physical entity is contained by more than one physical entity (for example, double-wide modules), this object should identify the containing entity with the lowest value of entPhysicalIndex.</p>	
.1.3.6.1.2.1.47.1.1.1.1.5	entPhysicalClass	PhysicalClass Other(1), unknown(2), chassis(3), backplane(4), container(5) (for example, chassis slot or daughter-card holder), power supply(6), fan(7), sensor(8), module(9) (for example, plug-in card or daughter-card), port(10), stack(11) (for example, stack of multiple chassis entities).	<p>An indication of the general hardware type of the physical entity.</p> <p>An agent should set this object to the standard enumeration value that accurately indicates the general class of the physical entity, or the primary class if there is more than one. If no appropriate standard registration identifier exists for this physical entity, then the value other(1) is returned. If the value is unknown by this agent, then the value unknown(2) is returned.</p>	
.1.3.6.1.2.1.47.1.1.1.1.6	entPhysicalParentRelPos	entPhysicalParentRelPos Range is from 1 through 2147483647	<p>An indication of the relative position of this "child" component among all its "sibling" components.</p> <p>Sibling components are defined as entPhysicalEntries that share the same instance values of each of the entPhysicalContainedIn and entPhysicalClass objects.</p>	

**TABLE 3 entPhysicalTable (continued)**

OID	Name	Syntax	Description	Note
			<p>A Networking Management System (NMS) can use this object to identify the relative ordering for all sibling components of a particular parent (identified by the entPhysicalContainedIn instance in each sibling entry).</p> <p>This value should match any external labeling of the physical component if possible.</p> <p>If the physical position of this component does not match any external numbering or clearly visible ordering, then user documentation or other external reference material should be used to determine the parent-relative position. If this is not possible, then the the agent should assign a consistent (but possibly arbitrary) ordering to a given set of "sibling" components, perhaps based on internal representation of the components.</p> <p>If the agent cannot determine the parent-relative position for some reason, or if the associated value of entPhysicalContainedIn is <b>0</b>, then the value <b>-1</b> is returned. Otherwise, a non-negative integer is returned, indicating the parent-relative position of this physical entity.</p> <p>Parent-relative ordering normally starts from <b>1</b> and continues to <b>N</b>, where N represents the highest-positioned child entity. However, if the physical entities are labeled from a starting position of zero, then the first sibling should be associated with an entPhysicalParentRelPos value of <b>0</b>. Note that this ordering may be sparse or dense, depending on agent implementation.</p> <p>The actual values returned are not globally meaningful, as each "parent" component may use different numbering algorithms. The ordering is only meaningful among siblings of the same parent component.</p> <p>The agent should retain parent-relative position values across reboots, either through algorithmic assignment or use of non-volatile storage.</p>	

**TABLE 3 entPhysicalTable (continued)**

OID	Name	Syntax	Description	Note
.1.3.6.1.2.1.47.1.1.1.1.7	entPhysicalName	SnmpAdminString	<p>The textual name of the physical entity. The value of this object should be the name of the component as assigned by the local device and should be suitable for use in commands entered at the device's "console".</p> <p>Note that the value of entPhysicalName for two physical entities will be the same in the event that the console interface does not distinguish between them, for example, slot-1 and the card in slot-1.</p>	
.1.3.6.1.2.1.47.1.1.1.1.8	entPhysicalHardwareRev	SnmpAdminString	<p>The vendor-specific hardware revision string for the physical entity. The preferred value is the hardware revision identifier printed on the component itself (if present).</p> <p>Note that if revision information is stored internally in a non-printable (for example, binary) format, then the agent must convert such information to a printable format, in an implementation-specific manner.</p> <p>If no specific hardware revision string is associated with the physical component or this information is unknown to the agent, then this object will contain a zero-length string.</p>	
.1.3.6.1.2.1.47.1.1.1.1.9, .1.3.6.1.2.1.47.1.1.1.1.10	entPhysicalFirmwareRev, entPhysicalSoftwareRev	SnmpAdminString	<p>The vendor-specific firmware revision string for the physical entity.</p> <p>Note that if revision information is stored internally in a non-printable (for example, binary) format, then the agent must convert such information to a printable format and in an implementation-specific manner.</p> <p>If no specific firmware revision string is associated with the physical component, or this information is unknown to the agent, then this object will contain a zero-length string.</p>	
.1.3.6.1.2.1.47.1.1.1.1.11	entPhysicalSerialNum	SnmpAdminString String length is from 0 through 32.	<p>The vendor-specific serial number string for the physical entity. The preferred value is the serial number string actually printed on the component itself (if present).</p> <p>On the first instantiation of a physical entity, the value of entPhysicalSerialNum associated with that entity is set to the correct vendor-assigned serial number, if</p>	



**TABLE 3 entPhysicalTable (continued)**

OID	Name	Syntax	Description	Note
			<p>this information is available to the agent. If a serial number is unknown or non-existent, the entPhysicalSerialNum is set to a zero-length string.</p> <p>Note that the implementations that can correctly identify the serial numbers of all installed physical entities do not need to provide write access to the entPhysicalSerialNum object. Agents that cannot provide non-volatile storage for the entPhysicalSerialNum strings are not required to implement write access for this object.</p> <p>Not every physical component will have a serial number. Physical entities for which the associated value of the entPhysicalIsFRU object is equal to <b>false(2)</b> do not need their own unique serial numbers. An agent does not have to provide write access for such entities, and may return a zero-length string.</p> <p>If write access is implemented for an instance of entPhysicalSerialNum, and a value is written into the instance, the agent must retain the supplied value in the entPhysicalSerialNum instance associated with the same physical entity for as long as that entity remains instantiated. This includes instantiations across all re-initializations or reboots of the network management system, including those which result in a change of the physical entity's entPhysicalIndex value.</p>	
.1.3.6.1.2.1.47.1.1.1.1.12	entPhysicalMfgName	SnmpAdminString	<p>The name of the manufacturer of this physical component. The preferred value is the manufacturer name string printed on the component itself (if present).</p> <p>Note that the comparisons between instances of the entPhysicalModelName, entPhysicalFirmwareRev, entPhysicalSoftwareRev, and the entPhysicalSerialNum objects, are only meaningful amongst entPhysicalEntries with the same value of entPhysicalMfgName.</p> <p>If the manufacturer name string associated with the physical component is unknown to the agent,</p>	

**TABLE 3 entPhysicalTable (continued)**

OID	Name	Syntax	Description	Note
			then this object will contain a zero-length string.	
.1.3.6.1.2.1.47.1.1.1.1.13	entPhysicalModelName	SnmpAdminString	<p>The vendor-specific model name identifier string associated with this physical component. The preferred value is the customer-visible part number, which may be printed on the component itself.</p> <p>If the model name string associated with the physical component is unknown to the agent, then this object will contain a zero-length string.</p>	
.1.3.6.1.2.1.47.1.1.1.1.14	entPhysicalAlias	SnmpAdminString	<p>This object is an "alias" name for the physical entity as specified by a network manager, and provides a non-volatile "handle" for the physical entity.</p> <p>On the first instantiation of a physical entity, the value of entPhysicalAlias associated with that entity is set to the zero-length string. However, the agent may set the value to a locally unique default value, instead of a zero-length string.</p> <p>If write access is implemented for an instance of entPhysicalAlias, and a value is written into the instance, the agent must retain the supplied value in the entPhysicalAlias instance associated with the same physical entity for as long as that entity remains instantiated. This includes instantiations across all re-initializations or reboots of the network management system, including those which result in a change of the physical entity's entPhysicalIndex value.</p>	
.1.3.6.1.2.1.47.1.1.1.1.15	entPhysicalAssetID	SnmpAdminString	<p>This object is a user-assigned asset tracking identifier for the physical entity as specified by a network manager, and provides non-volatile storage of this information.</p> <p>On the first instantiation of a physical entity, the value of entPhysicalAssetID associated with that entity is set to the zero-length string.</p> <p>Not every physical component will have an asset tracking identifier. Physical entities for which the associated value of the entPhysicalIsFRU object is equal to <b>false(2)</b> do not need their own</p>	

**TABLE 3 entPhysicalTable (continued)**

OID	Name	Syntax	Description	Note
			<p>unique asset tracking identifiers. An agent does not have to provide write access for such entities, and may instead return a zero-length string.</p> <p>If write access is implemented for an instance of entPhysicalAssetID, and a value is written into the instance, the agent must retain the supplied value in the entPhysicalAssetID instance associated with the same physical entity for as long as that entity remains instantiated. This includes instantiations across all re-initializations or reboots of the network management system, including those which result in a change of the physical entity's entPhysicalIndex value.</p> <p>If no asset tracking information is associated with the physical component, then this object will contain a zero-length string.</p>	
.1.3.6.1.2.1.47.1.1.1.1.16	entPhysicalIsFRU	TruthValue Values are true(1), false(2)	<p>This object indicates whether or not this physical entity is considered a "field replaceable unit" by the vendor.</p> <p>If this object contains the value <b>true(1)</b>, then this entPhysicalEntry identifies a field-replaceable unit.</p> <p>For all entPhysicalEntries that represent components that are permanently contained within a field-replaceable unit, the value <b>false(2)</b> must be returned for this object.</p>	

### entPhysicalContainsTable

The table showcases the container or containee relationships between physical entities and provides all the information found by constructing the virtual containment tree for a given entPhysicalTable.

In the event a physical entity is contained by more than one physical entity, the table must include these additional mappings that cannot be represented in the entPhysicalTable virtual containment tree.

**TABLE 4 entPhysicalContainsTable**

OID	Name	Syntax	Description	Note
.1.3.6.1.2.1.47.1.1.1.1.1	entPhysicalIndex	PhysicalIndex	Refer to entPhysicalTable	Index of entPhysicalContainsTable
.1.3.6.1.2.1.47.1.3.3.1.1	entPhysicalChildIndex	PhysicalIndex	The value of entPhysicalIndex for the contained physical entity	Index of entPhysicalContainsTable

## entityGeneral

The collection of objects that are used to represent general entity information for which a single agent provides management information.

**TABLE 5 entGeneralTable (Single OID)**

OID	Name	Syntax	Description	Note
.1.3.6.1.2.1.47.1.4.1	entLastChangeTime	TimeStamp	The value of sysUpTime at the time a conceptual row is created, modified, or deleted.	Last change time stamp for the whole MIB

## entityMIBTraps

The collection of notifications used to indicate Entity MIB data consistency and general status information.

**TABLE 6 entityMIBTrapsTable (Single OID)**

OID	Name	Syntax	Description	Note
.1.3.6.1.2.1.47.2.0.1	entConfigChange	NOTIFICATION-TYPE	<p>An entConfigChange notification is generated when the value of entLastChangeTime changes. It can be utilized by an NMS to trigger logical or physical entity table maintenance polls.</p> <p>An agent should not generate more than one entConfigChange notification-event in a given time interval (suggested default is five seconds). A notification-event is the transmission of a single trap or inform PDU to a list of notification destinations.</p> <p>If additional configuration changes occur within the throttling period, then notification-events for these changes must be suppressed by the agent until the current throttling period expires. At the end of a throttling period, one notification-event must be generated if any configuration changes occurred since the start of the throttling period. In such a case, another throttling period is started immediately.</p> <p>An NMS should periodically check the value of entLastChangeTime to detect any missed entConfigChange notification-events, for example, due to throttling or transmission loss.</p>	

# Secured Client Authentication Services

SmartZone allows an encrypted channel between the SZ and the LDAP or AD server. During TLS tunnel establishment, the LDAP or AD server may send its server certificate to SZ for validation. SZ verifies the server certificate using the root CA uploaded by the operator and then attempts to establish the connection.

You can configure Proxy AD or configure the LDAP server to secure client authentication services.

## Configuring Proxy Active Directory (AD)

Perform the following steps to configure the proxy AD server.

1. In the web interface, select **Services & Profiles > Authentication**.

2. On the **Create Authentication Service** page, configure the following items:
  - Enter the authentication service name.
  - For **Service Protocol**, select **Active Directory**.
  - For **Global Catalog**, click **ON** for **Enable Global Catalog support**.
  - For **TLS Encryption**, click **ON**.
  - Enter the IP address.
  - For **Port**, enter **636**.
  - Enter the Windows domain name.
  - Enter the admin domain name.
  - Enter the admin password.
  - For **Confirm New Password**, re-enter the password.

FIGURE 32 AD Server Configuration

## Create Authentication Service

\* Name:

Friendly Name:

Description:

\* Service Protocol:  RADIUS  Active Directory  LDAP

Active Directory Service Options

**Primary Server**

Global Catalog:  ON Enable Global Catalog support  
For SCG as Proxy, this must be checked

TLS Encryption:  ON

\* IP Address:

\* Port:

\* Windows Domain Name:  example: dc=domain,dc=ruckuswireless,dc=com

\* Admin Domain Name:  example: admin@domain.ruckuswireless.com

\* Admin Password:

\* Confirm New Password:

**User Role Mapping**

3. Click **OK** to complete the AD authentication service.

## Configuring an LDAP Server

Perform the following steps to configure an LDAP server for FIPS.

1. In the interface, select navigate to **Services & Profiles > Authentication**.



2. On the **Create Authentication Service** page that is displayed, configure the following items:

- Enter the authentication service name.
- For **Service Protocol**, select **LDAP**.
- Enable **TLS Encryption**.
- Enter the IP address.
- For **Port**, enter **636**.
- Enter the base domain name.
- Enter the admin domain name.
- Enter the admin password.
- For **Confirm New Password**, re-enter the password.
- For **Key Attribute**, enter **UID**.
- For **Search Filter**, enter **objectClass**

**FIGURE 33** LDAP Server Configuration

**Create Authentication Service** ✕

\* Name:

Friendly Name:

Description:

\* Service Protocol:  RADIUS  Active Directory  LDAP

LDAP Service Options

Primary Server ▼

TLS Encryption:  ON

\* IP Address:

\* Port:

\* Base Domain Name:  example: dc=ldap,dc=com

\* Admin Domain Name:  example: cn=admin,dc=ldap,dc=com

\* Admin Password:

\* Confirm New Password:

\* Key Attribute:  example: uid

\* Search Filter:  example: (objectClass=Person, show more...)

User Role Mapping ▼

Group Attribute Value ▲	User Role	User Traffic Profile

3. Click **OK** to complete the LDAP authentication service.

## 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.

### 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 34** 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 \* 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**.

- 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 7 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

- 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 8 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

- 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 OSCP validation.

- 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.

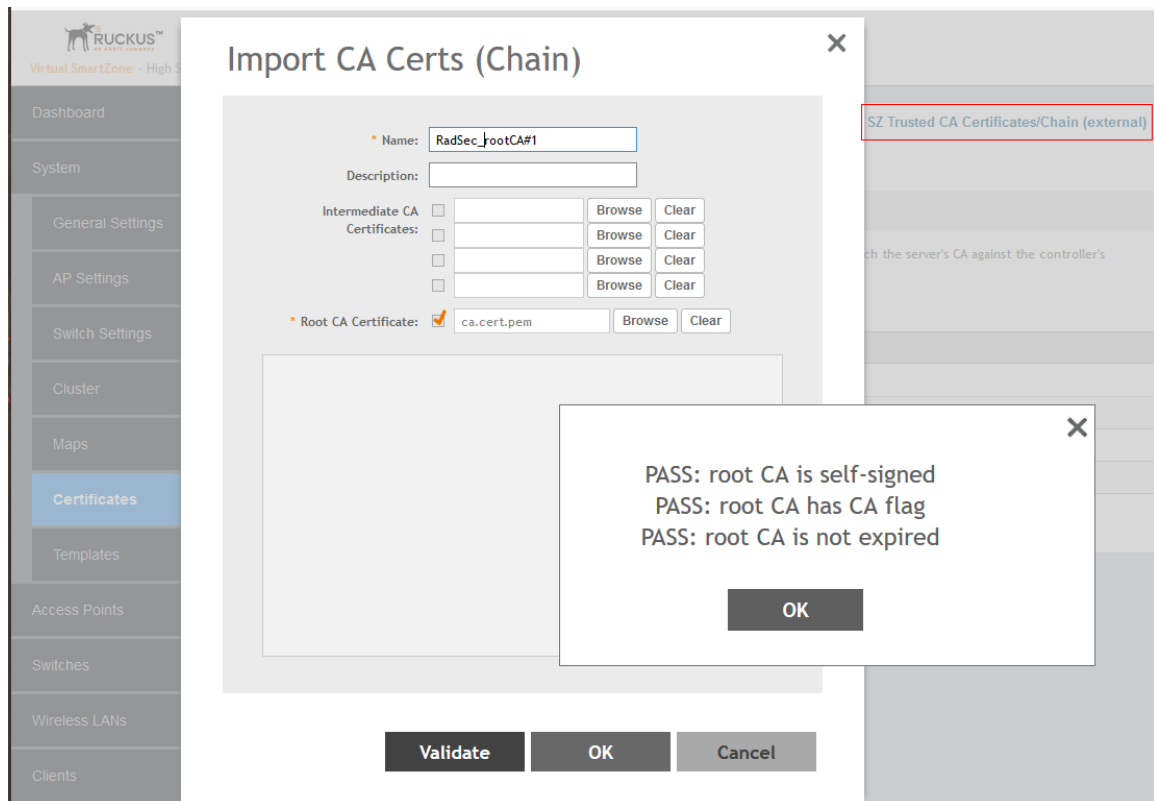
**NOTE**

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.

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

**FIGURE 35** 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.

13. 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 36** Configuring the Client Certificate

-----BEGIN CERTIFICATE-----  
Version: V3  
Subject: EMAILADDRESS=radsecClient@commscope.com, CH=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:  
2968816468379698624151593607456469162886462018858989002299767140370846988  
26638332793469582455289337620149806937469779525876683764905622192393261092  
06414723534710242903535954575092588749528110351296755111911370231225850409  
4701992383242172313501523680813490214313125373471018908084567277549580715  
9995975165254152264953037713178071331739270349875233246448227897814631284  
335949190668257666467235843079389548311686902977454765916076397635638835  
11884835953457088988535133939662329501186151161520323197699121873844367073  
865284457613853743644315085090368545219630730591667639078695943562706257  
0452250909455466533383337

- 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 37 Configuring RadSec Accounting Service

## Edit Accounting Service: radsec\_10.1.200.197

\* Name:

Description:

Service Protocol:  RADIUS Accounting

RADIUS Service Options

Encryption:  ON TLS

\* CN/SAN Identity:

OCSP Validation:  ON \* OSCP URL:

Client Certificate:  ▼

Primary Server

\* IP Address:

\* Port:

\* Shared Secret:

\* Confirm Secret:

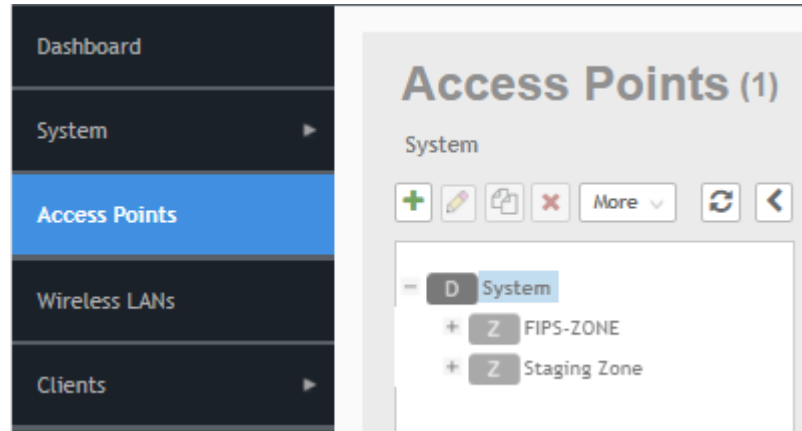
Reload...  
Disable  
client\_cert

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 38** 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 39** Configuring an AP Group

The screenshot shows the 'Configure Group' web interface. At the top, there is a 'Name' field with 'FIPS-Zone' entered and a 'Description' field. Below this, the 'Type' is set to 'Zone' (selected with a radio button), and the 'Parent Group' is 'System'. The 'Configuration' section is expanded to show 'General Options'. Key fields include: 'AP Firmware' set to '5.1.1.3.1023', 'Country Code' set to 'United States', 'Location' set to 'Ruckus HQ', and 'Location Additional Information' set to '350 W Java Dr, Sunnyvale, CA, USA'. 'AP Admin Logon' is configured with 'Logon ID' 'mahan' and a masked password. Other options include 'AP Time Zone' set to '(GMT+0:00) GMT' and 'AP IP Mode' set to 'IPv4 only'. At the bottom right, there are 'OK' and 'Cancel' buttons.

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 40** Creating a WLAN with Open Method

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

- Name:** A text input field.
- SSID:** A text input field.
- Description:** A text input field.
- Zone:** A dropdown menu with 'FIPS-Zone' selected.
- WLAN Group:** A dropdown menu with 'default' selected, and a '+ Create' button next to it.
- Authentication Options:**
  - Authentication Type:** Radio buttons for 'Standard usage (for most regular wireless networks)' (selected), 'Hotspot (WSP) v2', 'Hotspot 2.0 Access', and 'Hotspot 2.0 Onboarding'.
  - Method:** Radio buttons for 'Open' (selected), '802.1X EAP', and '802.1X EAP & MAC'.
- Encryption Options:**
  - Method:** Radio buttons for 'WPA2' (selected) and 'WPA3'.
  - Algorithm:** Radio buttons for 'AES' (selected) and 'TKIP'.
  - Passphrases:** A text input field with a 'Show' checkbox to its right.

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

**FIGURE 41** Creating a WLAN with 802.1X EAP & MAC Method

The screenshot displays the 'Create WLAN Configuration' web interface. At the top, the 'Zones' dropdown is set to 'FIPS-Zone' and the 'WLAN Group' is 'default'. A 'Create' button is visible. The 'Authentication Options' section includes: 'Authentication Type' with radio buttons for 'Standard usage (For most regular wireless networks)', 'Hotspot (WISPr)', 'Hotspot 2.0 Access', and 'Hotspot 2.0 Onboarding'; 'Method' with radio buttons for 'Open', '802.1X EAP', and '802.1X EAP & MAC'; and a checkbox for 'MAC Authentication' with a text input field. The 'MAC Address Format' dropdown is open, showing options: 'aabbccddeeff', 'aa-bb-cc-dd-ee-ff', 'AA-BB-CC-DD-EE-FF', 'AABBCCDDEEFF', and 'aa-bb-cc-dd-ee-ff'. The 'Encryption Options' section includes: 'Method' with radio buttons for 'Open', '802.1X EAP', and '802.1X EAP & MAC'; 'Algorithm' with radio buttons for 'TKIP', 'AES-CCMP', and 'AES-CCMP-128'; '802.11r Fast Roaming' with a checkbox for 'Enable 802.11r Fast BSS Transition'; and '802.11w WFP' with radio buttons for 'Disabled', 'Capable', and '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 42** Creating a WLAN with Hotspot WISPr in 802.1X EAP Method

The screenshot shows the 'Create WLAN Configuration' form. The 'Name' field is empty. The 'SSID' field is empty. The 'Description' field is empty. The 'Zone' dropdown menu is set to 'FIPSS-Zone'. The 'WLAN Group' dropdown menu is set to 'default'. In the 'Authentication Options' section, 'Authentication Type' is set to 'Hotspot (WISPr)' and 'Method' is set to '802.1X EAP'. In the 'Encryption Options' section, '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 43** Creating a WLAN with Hotspot WISPr in Open Method

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

## Mapping the Authentication Profile for the WLAN

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

### NOTE

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

**FIGURE 44** Mapping to the Hotspot Porta

Hotspot Portal

Hotspot (WISPr) Portal: H5-Profile + Create

Bypass CNA:  Enable

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

RadSec Auth Service + Create  Enable RFC 5580 Location Delivery Support

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

RadSec Account Service + Create Send interim update every 10 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 45** Configuring Realm-based Authentication Service

Name: RadSec Auth Profile

Description:

Enable Hosted AAA Support  Configure PLMN identifier

Realm Based Authentication Service

+ Create Configure Delete

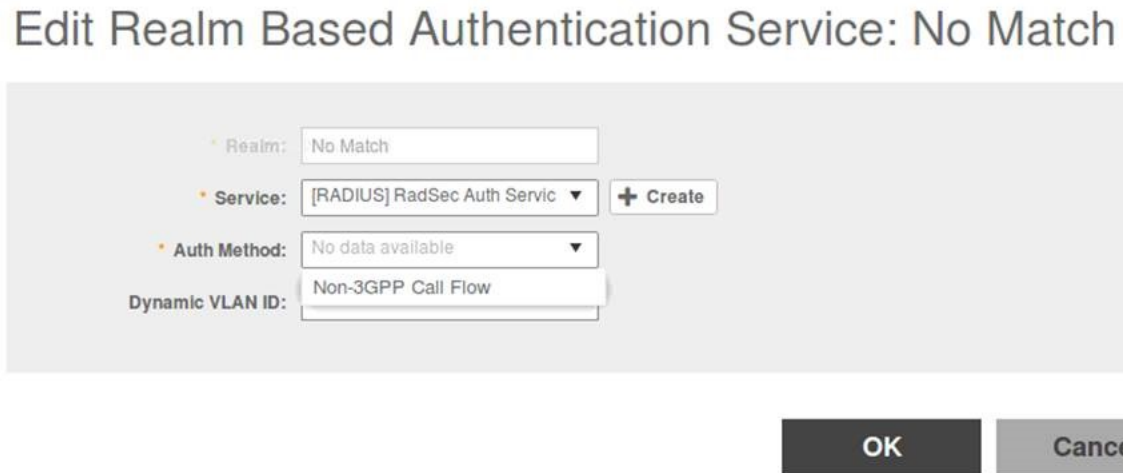
Realm	Protocol	Auth Service	Auth Method	Dynamic VLAN ID
No Match	RADIUS	RadSec Auth Service	NonGPPCallFlow	N/A
Unspecified	RADIUS	RadSec Auth Service	NonGPPCallFlow	N/A

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**.

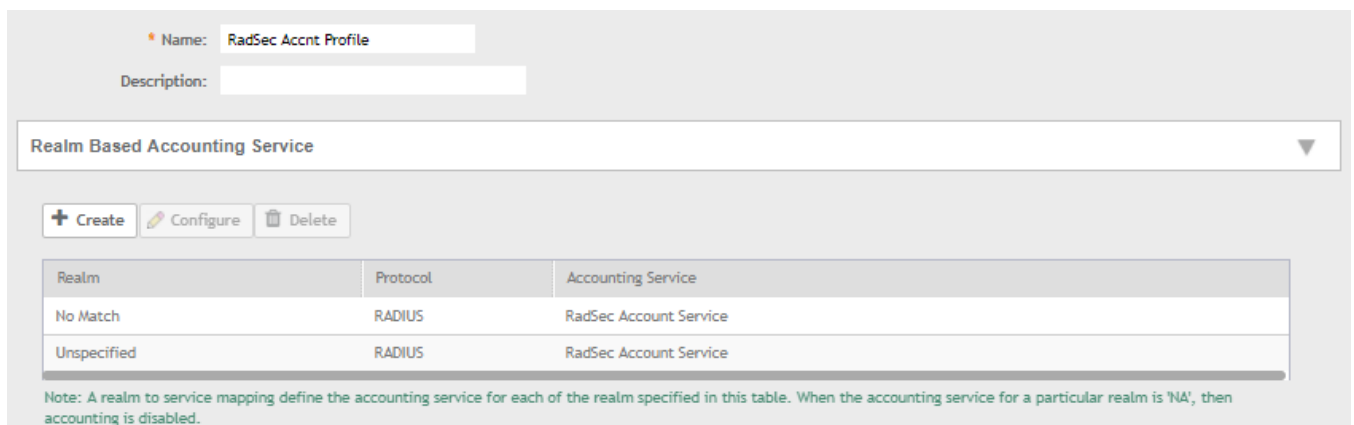
4. Click **Configure**, and configure the following items:
  - For **Service**, select **RadSec Auth Service**.
  - For **Auth Method**, select **No data available**.
  - For **Dynamic VLAN ID**, select **Non-3GPP Call Flow**.
  - Click **OK** to save the configuration.

**FIGURE 46** Editing Realm-based Authentication Service



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.

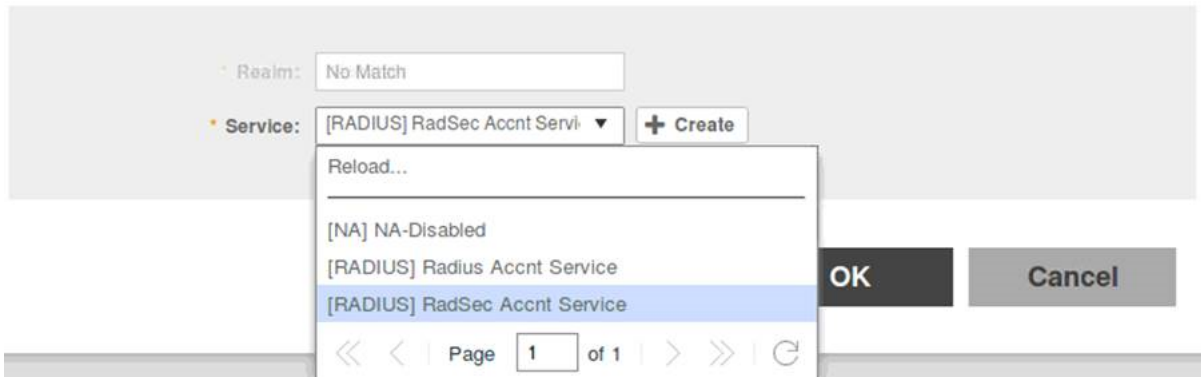
**FIGURE 47** Configuring Realm-based Accounting Service



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

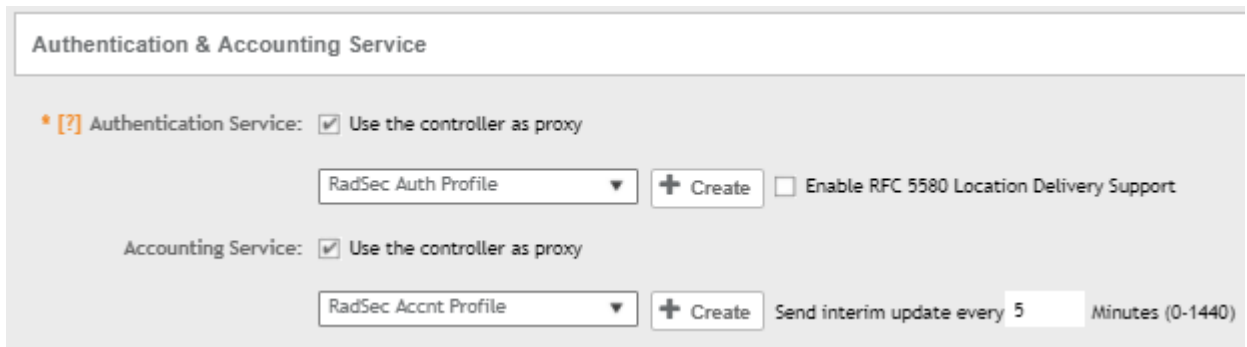
- Click **Configure**, and configure the following items:
  - For **Service**, select **RadSec Acct Service**.
  - Click **OK** to save the configuration.

## Edit Realm Based Accounting Service: No Match



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

**FIGURE 48** 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 49** Viewing FIPS zone WLANs

Wireless LANs

System > FIPS-ZONE

+ Create Configure Clone Delete More

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

# Authentication Using Common Access Card or Personal Identity Verification

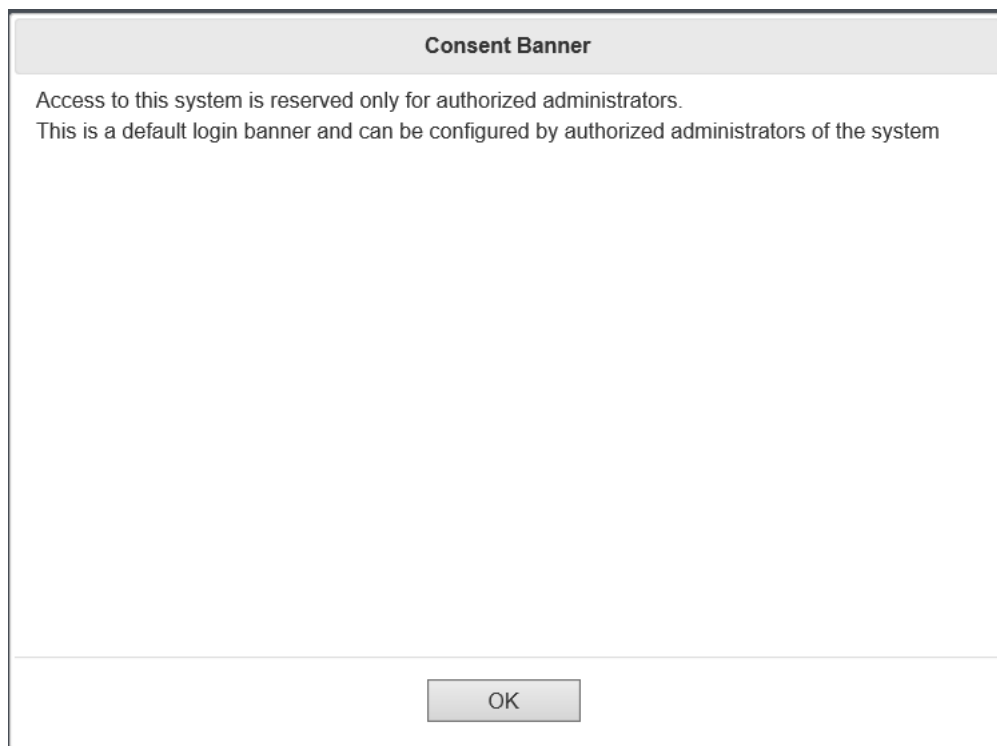
If TACACS+, Active Directory, or LDAP is selected as the authentication server, the user is taken through two-factor authentication. If RADIUS or RadSec is selected as the authentication server, the user is taken through three-factor authentication.

## Two-Factor Authentication

Perform the following procedure to log in to the controller.

1. Enter the server URL in the browser window.  
The **Consent Banner** page is displayed.

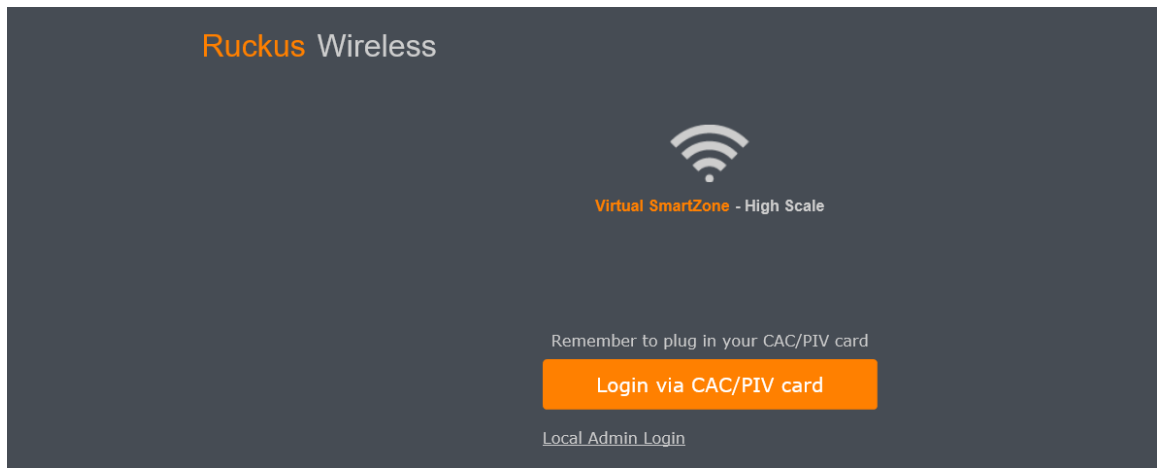
**FIGURE 50** Consent Banner



2. Click **OK** to proceed.

The first-level authentication login page to log in using a CAC or PIV card is displayed.

**FIGURE 51** Logging in to the Controller with the CAC or PIV Card



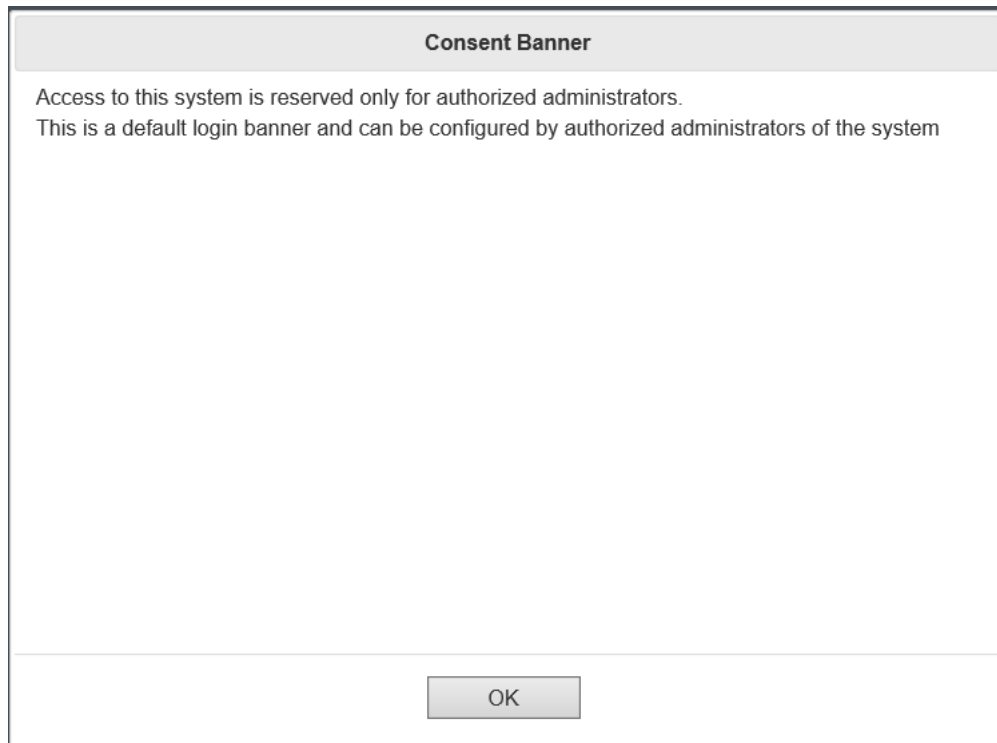
3. Click **Login via CAC/PIV card** and enter the personal identification number (PIN).  
For the protocol PEAP,  
You must also configure the Trusted CA certificate to support PEAP connection.

## Three-Factor Authentication

Perform the following procedure to log in to the controller.

1. Enter the server URL in the browser window.  
The **Consent Banner** page is displayed.

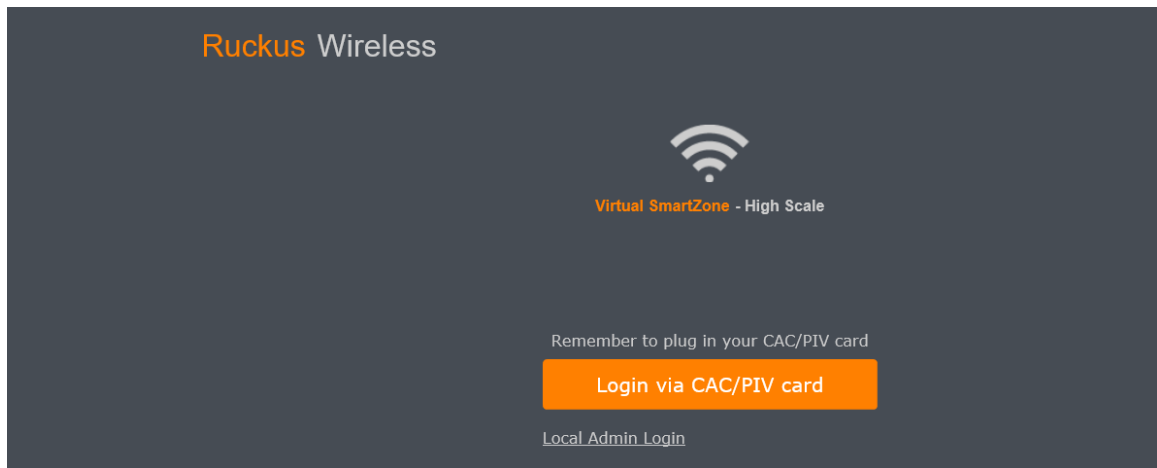
**FIGURE 52** Consent Banner



2. Click **OK** to proceed.

The first-level authentication login page to log in using a CAC or PIV card is displayed.

**FIGURE 53** Logging in to the Controller with the CAC or PIV Card



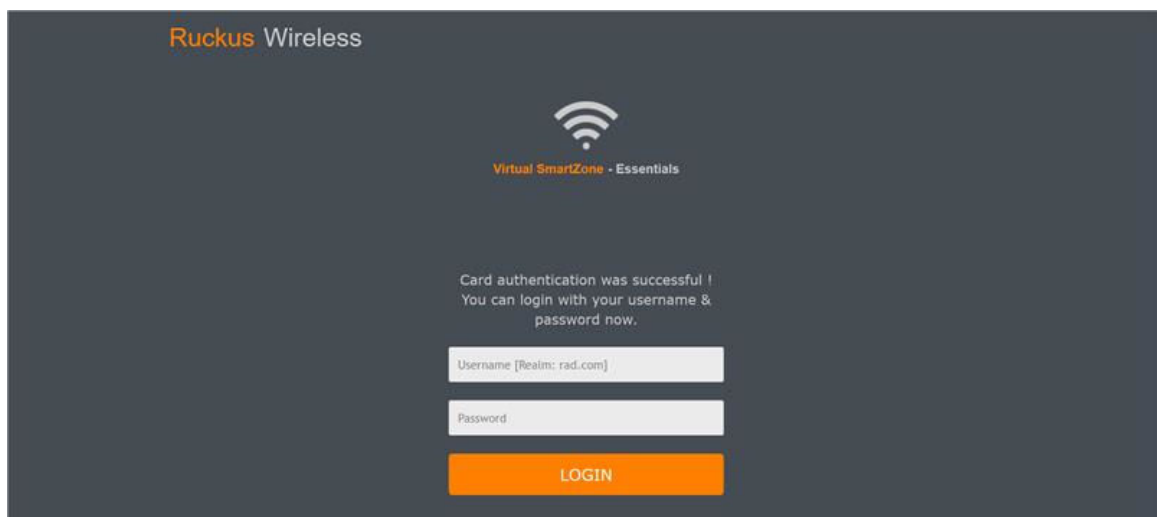
3. Click **Login via CAC/PIV card** and enter the personal identification number (PIN).
4. Enter the username and password.

The second-level authentication login page to enter username and password is displayed.

**NOTE**

This login page is displayed only if you select the RADIUS or RadSec as the authentication server.

**FIGURE 54** Logging into the Controller with the Username and Password



5. Click **Login**

## Configuring AAA Servers

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

Perform the following procedure to add and configure AAA servers.

1. Select **Administration > Admins and Roles > AAA** and click **Create** to add an external AAA server.
2. Enter the AAA server name.
3. For **Realm**, enter the realm or service.

4. For **Type**, select one of the external AAA server.
  - a) If **RADIUS** is selected as the external AAA server, then complete the following steps:
    - Enable the **TLS Encryption** check box if you want to use the Transport Layer Security (TLS) protocol to secure communication with the server.

**NOTE**

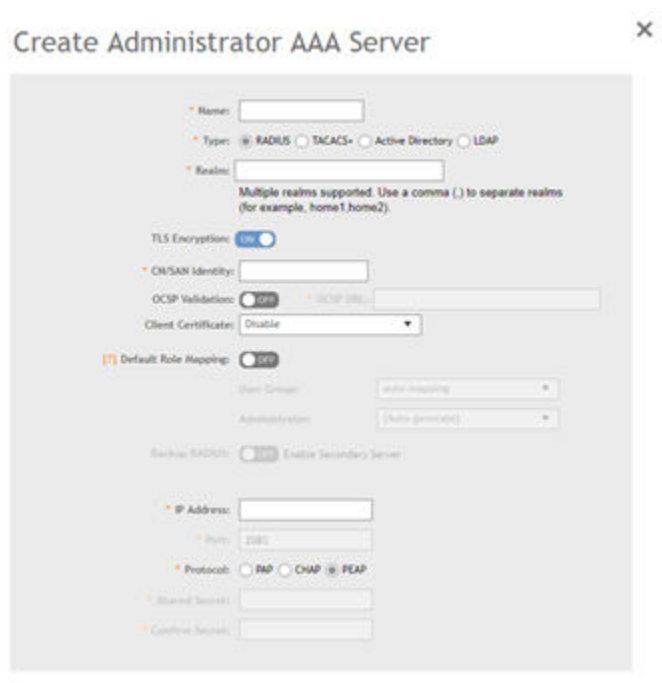
You must also configure the Trusted CA certificates to support TLS encryption

- For **CN/SAN Identity**, enter an address (for example, **bdc.commscope.com**. The maximum length is 1024 characters. For more information, refer to the section [Configuring RadSec](#) on page 46.
- Enable **OCSP Validation** and enter the **OCSP URL**.
- Select the client certificate from the list.
- Enter the IP address.
- Select the **PAP** or **CHAP** or **PEAP** protocol.

**NOTE**

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

**FIGURE 55** Creating a RADIUS Authentication Server



- b) If **TACACS+** is selected as the external AAA server, then complete the following steps:
  - Enter the IP address.
  - Enter the port number.
  - Enter the shared secret.
  - Re-enter the shared secret to confirm.

**FIGURE 56** Creating a TACACS+ Authentication Server

**Create Administrator AAA Server**

\* Name:

\* Type:  RADIUS  TACACS+  Active Directory  LDAP

\* Service:   
Multiple services supported. Use a comma (,) to separate services (for example, home1,home2).

[?] Default Role Mapping:  ON

User Group:

Administrator:

\* IP Address:

\* Port:

\* Shared Secret:

\* Confirm Secret:

OK Cancel

**NOTE**

TLS encryption is not supported in TACACS+ authentication.

- c) If **Active Directory** is selected as the external AAA server, then complete the following steps:
- Enable the **TLS Encryption** check box if you want to use the Transport Layer Security (TLS) protocol to secure communication with the server.

**NOTE**

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

- Enter the IP address.
- Enter the port number.
- Enter the Windows domain name.
- Enable **Proxy Agent** and enter the principal name as Windows domain Administrator name, Administrator password, and re-enter the Administrator password to confirm.



**FIGURE 57** Creating an Active Directory Authentication Server

**Create Administrator AAA Server**

\* Type:  RADIUS  TACACS+  Active Directory  LDAP

\* Realm:   
Multiple realms supported. Use a comma (,) to separate realms (for example, home1,home2).

TLS Encryption:  ON

[?] Default Role Mapping:  ON

User Group:

Administrator:

\* IP Address:

\* Port:

\* Windows Domain Name:  example: dc=domain,dc=ruckuswireless,dc=com

[?] Proxy Agent:  ON

\* User Principal Name:

\* Password:

\* Confirm Password:

**OK** **Cancel**

- d) If **LDAP** is selected as the external AAA server, then complete the following steps:
- Enable the **TLS Encryption** check box if you want to use the Transport Layer Security (TLS) protocol to secure communication with the server.

**NOTE**

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

- Enter the IP address.
- Enter the port number as **636**.
- Enter the base domain name.
- Enter the Windows domain name.
- Enter the admin password.
- Re-enter the admin password to confirm the new password.
- Enter the key attribute as **UID**.
- Enter the search filter as **objectClass**.

FIGURE 58 Creating an LDAP Service

**Create Administrator AAA Server**

\* Type:  RADIUS  TACACS+  Active Directory  LDAP

\* Realm:   
Multiple realms supported. Use a comma (,) to separate realms (for example, home1,home2).

TLS Encryption:  ON

[?] Default Role Mapping:  ON

User Group:

Administrator:

\* IP Address:

\* Port:

\* Base Domain Name:  example: dc=ldap,dc=com

\* Admin Domain Name:  example: cn=admin,dc=ldap,dc=com

\* Admin Password:

\* Confirm New Password:

\* Key Attribute:  example: uid

**OK** **Cancel**

5. Enable **Default Role Mapping**.
6. For **User Group**, select **auto-mapping** to map between the AAA and SZ accounts automatically.
7. Click **OK** to create and configure the selected external AAA server.

### Testing SZ Admin AAA Servers

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

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

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

2. Select the created AAA server and click **Test AAA**.  
An example for testing a RADIUS server is shown.

**FIGURE 59** Testing an AAA Server: RADIUS

The screenshot shows a dialog box titled "Test AAA Servers" with a close button (X) in the top right corner. The dialog contains the following fields and options:

- Name:** A dropdown menu with "peapIPv6" selected.
- Protocol:** A text field containing "PEAP".
- User Name:** A text box containing "ramu". Below it is the text "(Test with username ONLY.)".
- Password:** A masked text box with "\*\*\*\*\*". Below it is a checkbox labeled "Show password".

Below the fields, a green message reads: "AAA testing : Success! Associated with Auto Mapping [CACDEV]". At the bottom of the dialog are two buttons: "Test" (dark grey) and "Cancel" (light grey).

The **Protocol** field is displayed only for RADIUS server that depends on the SZ AAA server configuration.

3. In the **Name** field, select the AAA server that you created.
4. In the **User Name** field, enter an existing user name that is associated to a user group.

**NOTE**

For TACACS+ server, test with username and realm.

5. In the **Password** field, enter password for the user name you specified.
6. Click **Test**.

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

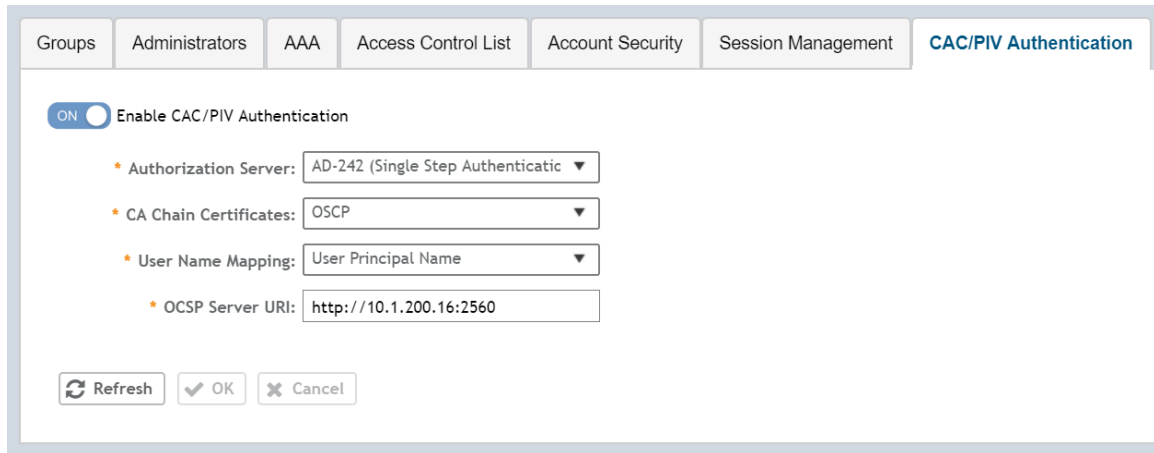
## Enabling Common Access Card or Personal Identity Verification Authentication

Perform the following procedure to enable CAC/PIV authentication.

1. Select **Administration > Admins and Roles > CAC/PIV Authentication**.

2. Select **Enable CAC/PIV Authentication**.

**FIGURE 60** Enabling CAC/PIV Authentication



3. Select the AAA authorization server from the list.

**NOTE**

For RADIUS, the login flow changes to three-factor authentication.

The CAC/PIV login prompts the user to insert the CAC/PIV smart card. The operating system and browser in conjunction with card reader drive support verifies the client certification using a personal identification number (PIN). Only after the PIN is verified as correct, the client certificate is sent to SZ for verification.

**NOTE**

Only Windows 7 and 10 are supported. Google Chrome (version - 72.0.3626.121), Internet Explorer (version 10 or 11), and Firefox (version - 68.0) browsers are supported.

4. Select the CA chain certificate from the list.

**NOTE**

To upload the certificates refer [Uploading Certificates to SmartZone OS](#) on page 28

5. For **User Name Mapping**, select the **User Principal Name** or **RFC822 Name** from the drop-down list.
6. Enter the OCSP server URL.
7. Click **OK**.

## Wireless Intrusion Detection and Prevention Services

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

## Classifying a Rogue Policy

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

Complete the following steps to create a rogue classification policy.

1. Select **Services & Profiles > WIPS**.
2. Under **Policy**, select the zone for which you want to create the policy and click **Create**.

**FIGURE 61** Creating a Rogue Classification Policy

**Create Rogue Classification Policy** X

Name:

Description:

Rogue Classification Rules ▼

+ Create Configure Delete Up Down  Q

Priority ▲	Name	Type and Criteria	Classification	⚙

OK Cancel

3. Enter the policy name and description.

4. Under **Rogue Classification Rules**, click **Create** and complete the following steps to create a rogue classification rule.
  - a) In the **Name** field, enter the rule name.
  - b) Under **Rule Type**, select one from the following rule type for classification:
    - **Ad Hoc**: The monitoring AP is able to detect the ad hoc network as a rogue.
    - **Clear to Send (CTS) Abuse**: Reported when the number of CTS frames per second to a specific receiver MAC address exceeds the specific threshold. The default number of frames per second is 50.
    - **Deauth Flood**: Reported when the number of deauthentication frames per second exceeds the specific threshold from a specific transmitter. The default number of frames per second is 50.
    - **Disassoc Flood**: Reported when the number of disassociation frames per second exceeds the specific threshold from specific transmitter. The default number of frames per second is 50.
    - **Excessive Power**
    - **Low RSSI**: In the **Signal Threshold** field, enter the RSSI threshold in dBm.
    - **MAC OUI**: In the **MAC OUI** field, enter the first three octets of the MAC address. For example, for a MAC address 11:22:33:44:55:66, the MAC OUI is 11:22:33.
    - **MAC (BSSID) Spoofing**
    - **Request to Send (RTS) Abuse**: Reported when the number of RTS frames per second to a specific receiver MAC address exceeds the specific threshold. The default number of frames per second is 50.
    - **Same Network**
    - **SSID**: Enter the partial or complete SSID string regardless of the zone being configured with the specific SSID.
    - **NULL SSID**
    - **SSID Spoofing**: Enter the SSID that is configured in a specific zone from a non-managed AP.
  - c) Under **Classification**, select one of the following actions to be taken for the selected rule type:
    - **Ignore**
    - **Know**
    - **Malicious**
    - **Rogue**
  - d) Click **OK** to save the changes.
5. Click **OK**.

#### NOTE

Click **Configure** or **Delete** to edit or delete a rogue classification policy respectively. To prioritize a classification rule, select the rule from the list and click **Up** or **Down** to position the rule.

## Creating a Monitoring AP Group

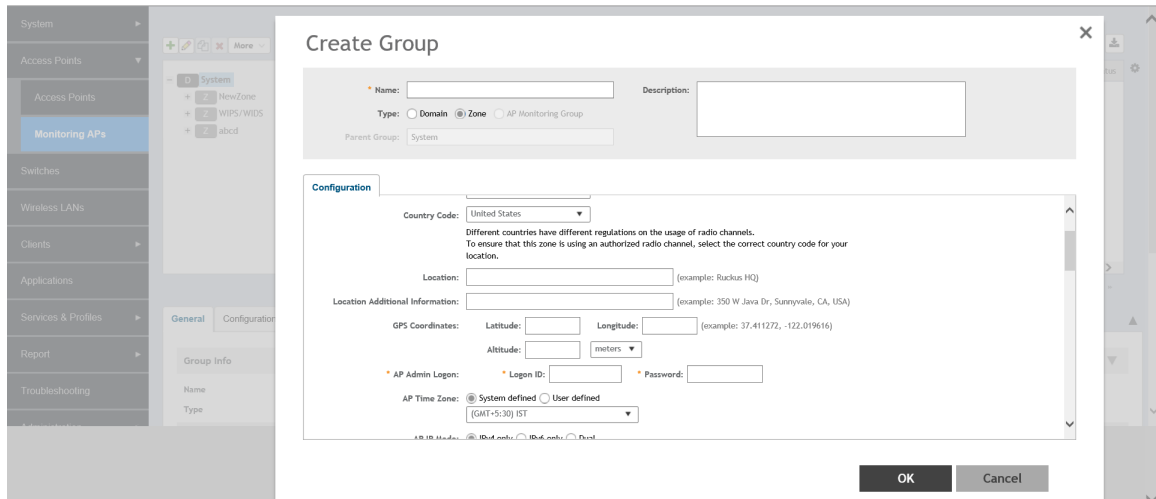
As a prerequisite, the monitoring AP must be connected to SZ.

Perform the following procedure to create a monitoring AP group.

1. From the left pane, select **Access Points > Monitoring APs** to create a zone.

2. Select **System** and click **+** to create a zone.

**FIGURE 62** Creating a Zone



3. For **Type**, select **Zone**.
4. Select **General Options > AP Admin Logon**, enter the user name and password, and click **OK**.
5. Under **Advanced Options**, enable **Rogue Detection**.
6. For **Rogue Classification Policy**, configure the following options:
  - a) In the **Report RSSI Threshold** field, enter the threshold (the threshold ranges from 0 through 100).
  - b) Enable **Protect the network from malicious rogue access points** and select one of the following options:
    - **Aggressive**
    - **Auto**
    - **Conservative**

**NOTE**

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

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

7. On the **Access Points** page, select the created zone and click **+** to create the AP monitoring group.

**FIGURE 63** Creating an AP Monitoring Group

**Create Group** [Close]

Name:  Description:

Type:  Domain  Zone  AP Monitoring Group

Parent Group: WIPS/WIDS

**Configuration**

**Model Specific Options**

**Advanced Options**

Location Based Service:  OFF Override  OFF Select an LBS server

AP Management VLAN:  OFF Override  Keep AP's settings  VLAN ID

Venue Code:  OFF Override

Rogue Classification Policy:  ON Override

ON Override Report RSSI Threshold:  (0-100)

ON Override Jamming Threshold:  %

Please choose the frequency for scanning

Low  Medium  High

8. Enter the group name.
9. Under **Advanced Options**, configure the following options:
  - a) Enable **Rogue Classification Policy** and select a rogue classification policy from the list.

**NOTE**

You can click **+** to create a rogue classification policy. Refer to [Classifying a Rogue Policy](#) on page 73.

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

**NOTE**

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



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

#### **Viewing Associated Events**

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

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

## **Rogue Devices**

Rogue (or unauthorized) APs and rogue clients pose problems for a wireless network in terms of airtime contention and security. Usually, a rogue AP or a rogue client appears when an employee obtains another manufacturer's AP and connects it to the LAN to gain wireless access to other LAN resources. This connection potentially allows more unauthorized users to access the corporate LAN, posing a security risk. Rogue APs and rogue clients also interfere with nearby Ruckus APs, thus degrading overall wireless network coverage and performance.

The SZ controller's rogue AP detection options include identifying the presence of a rogue AP or rogue client, and categorizing it as either a known neighbor AP or as a malicious rogue.

### **Viewing Rogue Devices**

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

If you enabled rogue AP or rogue client detection when you configured the common AP settings (refer to Configuring APs), click **Report > Rogue Devices**. Under **Device Type**, select **Access Point** or **Client**. The **Rogue Devices** page displays all the rogue APs or rogue clients that the controller has detected on the network, including the following information:

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

## Filtering Rogue Devices

From the list of rogue APs or rogue clients, you can filter the required rogue AP or rogue client based on rogue MAC address, type, or SSID.

Perform the following procedure to filter the rogue devices.

1. Select **Report > Rogue Devices**.
2. In the **Rogue Devices** page, select **Access Point** from the **Device Type** list and click **Settings** (⚙️).
3. In the **Apply Filters** page, enter the rogue MAC address for **Rogue MAC**.
4. Select **Type** from the list.

If **Device Type** is **Access Point**, select **Ignore, Known, Rogue, or Malicious**.

If **Device Type** is client, select **Active Probing, CTS Abuse, Data Encrypted, Deauth Flood, Disassoc Flood, Excessive Power, Known, Rogue Client, and RTS Abuse**.

5. Enter **SSID**.
6. Click **OK**.

### NOTE

You can click **Filter On** or **Filter Off** to add or remove the filters.

## Marking Rogue Access Points

You can mark a rogue (or unauthorized) AP as known.

To mark a rogue AP as known:

1. From the left pane, click **Report > Rogue Devices**. The **Rogue Devices** page is displayed.
2. Select the rogue AP from the list and click **Mark as Known**. The classification **Type** of the rogue AP changes to **Known**. You can also select the rogue AP from the list and click **Unmark** to change the classification.

## Locating a Rogue Device

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

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

1. From the left pane, select **Report > Rogue Devices**.
2. In the **Rogue Devices** page, select **Rogue AP** or **Client** from the **Device** list.

3. Click **Locate Rogue**.

The **Rogue AP Location** page appears locating the rogue AP or rogue client. You can select from the following options:

- **Map:** View the location in street view.
- **Satellite:** View the location as satellite imagery.
- **+**: Zoom in on the location.
- **-**: Zoom out of the location.

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

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

4. Click **OK**.

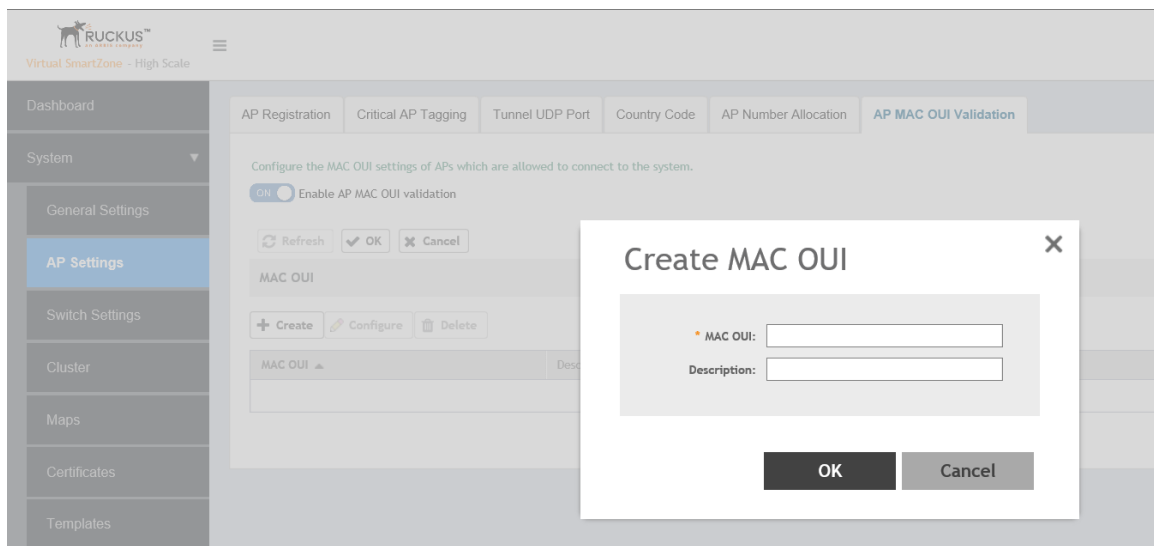
## Creating an AP MAC OUI Address

You must enable the AP MAC OUI validation for an AP with a specific organizationally unique identifier (OUI) to be allowed to connect to SZ. If the AP that is not in the OUI list connects to the SZ, then the AP is rejected and event code 186 is generated.

Perform the following procedure to create the MAC OUI address for an AP.

1. Select **System > AP Settings > AP MAC OUI Validation**.
2. Select **Enable AP MAC OUI Validation**.
3. Click **Create** to create the MAC OUI settings for an AP.

**FIGURE 64** Creating an AP MAC OUI Address



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



# vSZ-D FIPS Installation with FIPS Image

- vSZ-D FIPS Installation Prerequisites for FIPS..... 81
- Creating and Registering the Virtual Machine (vSZ-D)..... 81
- Joining vSZ-D to the vSZ Controller..... 87
- Using FIPS CLI Commands (vSZ-D)..... 90
- Downloading vSZ-D FIPS Logs..... 93

## vSZ-D FIPS Installation Prerequisites for FIPS

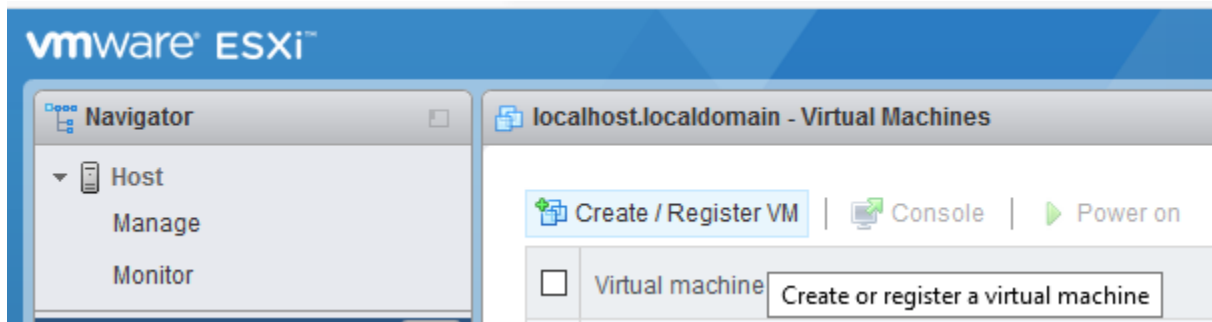
To comply with FIPS, you must have a new installation of SmartZone 5.1.1.3 and a corresponding AP. The installation will not work on a system upgraded to SmartZone 5.1.1.3. The system validates the image before it is loaded.

The Dell server must have VMware ESXi 6.5 installed to host the guest virtual machine.

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

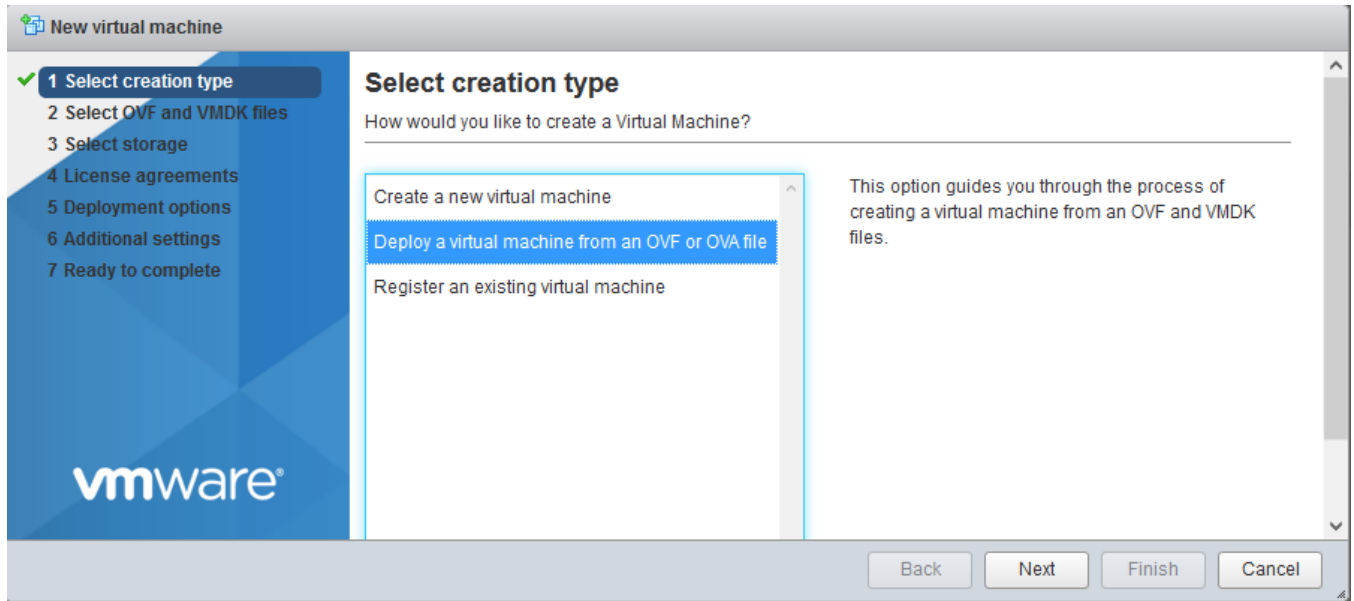
1. Install and deploy the .ova file on VMware ESXi using the **Create / Register VM** option, as shown in the following figure.

**FIGURE 65** Creating and register VM



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

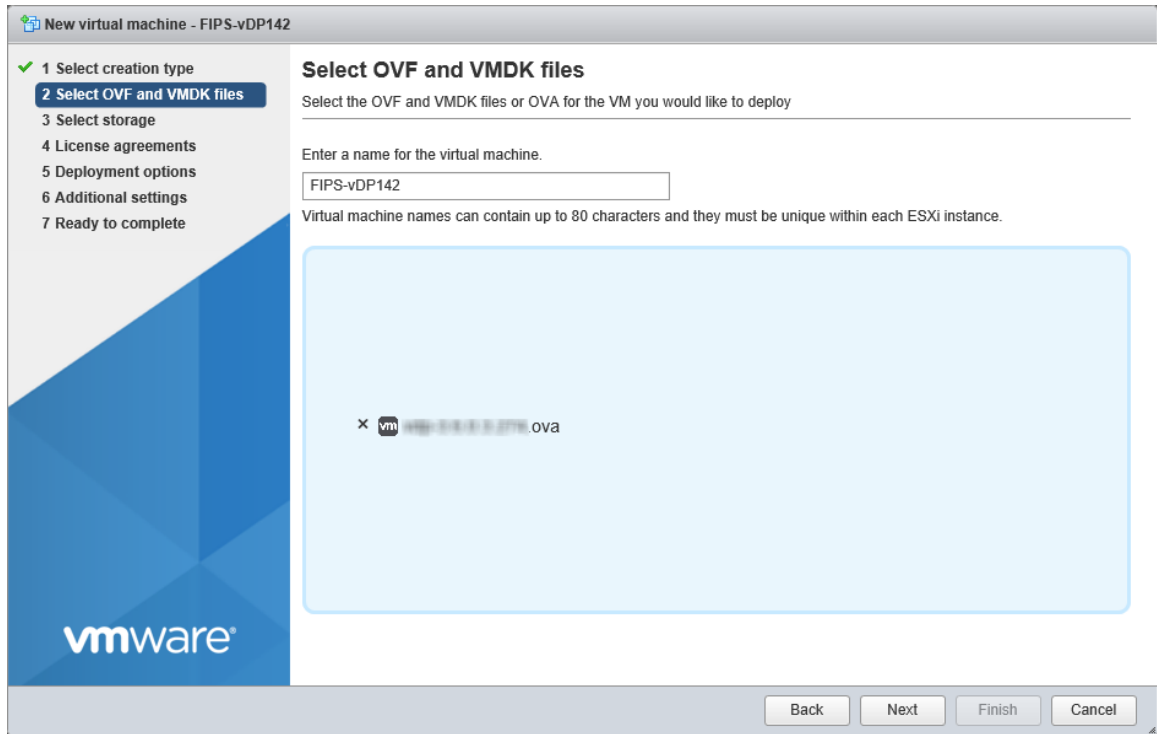
**FIGURE 66** Selecting the Creation Type



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 67** Selecting OVF and VMDK Files

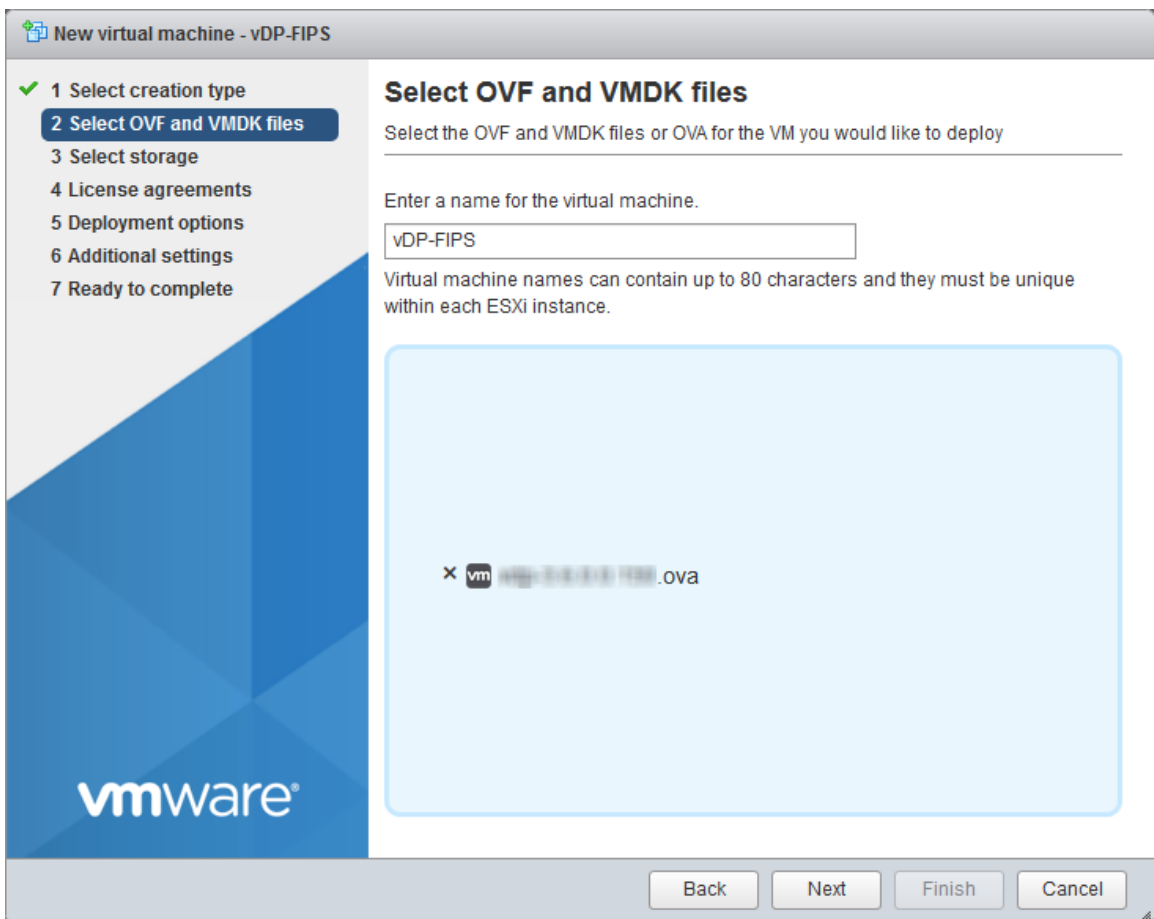


5. Select the .ova file from the browse window. The selected file is displayed in Select OVF and VMDK files screen

**FIGURE 68** Selecting the .ova File



**FIGURE 69** Selected file appears on screen

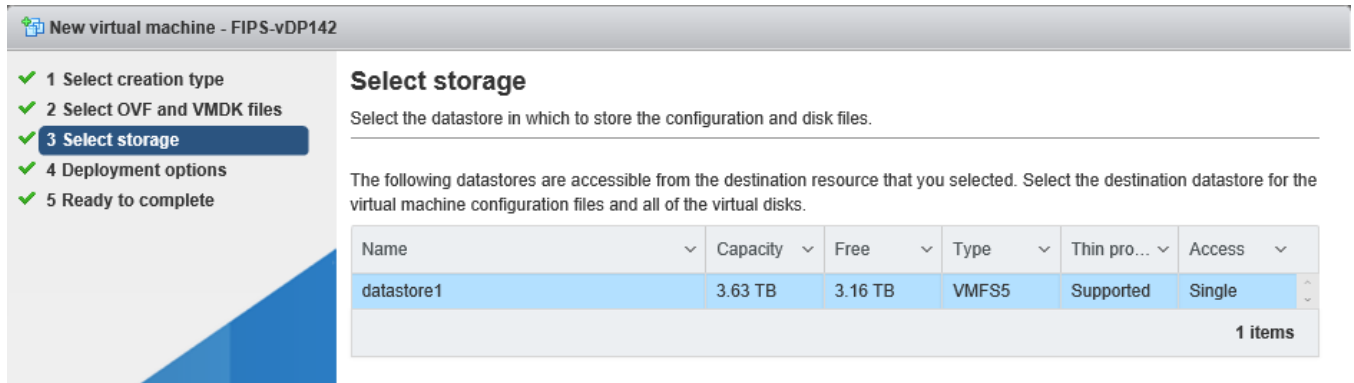


6. Click **Next** to select storage.



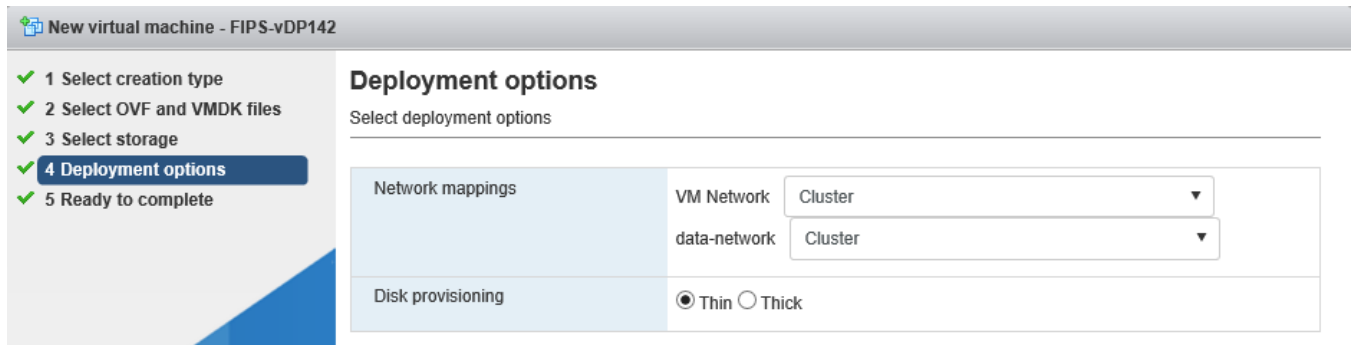
7. Select the required datastore.

**FIGURE 70** Selecting the Datastore



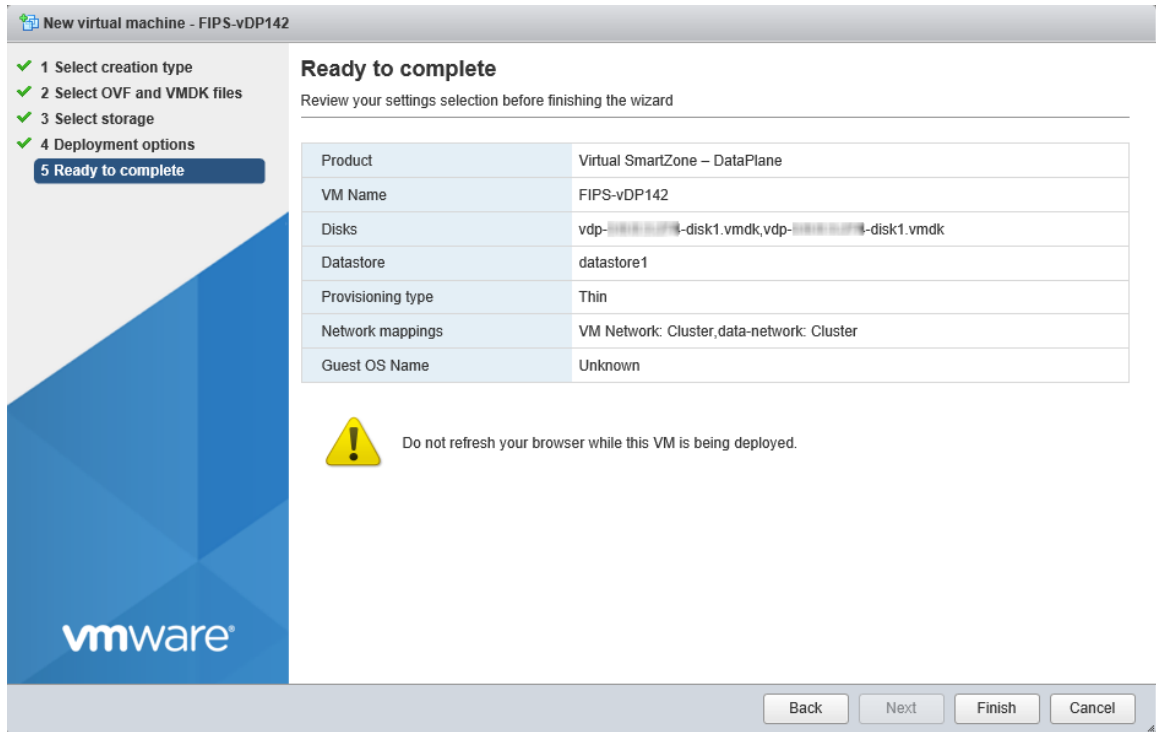
8. Click **Next** to select deployment options.

**FIGURE 71** Selecting Deployment options



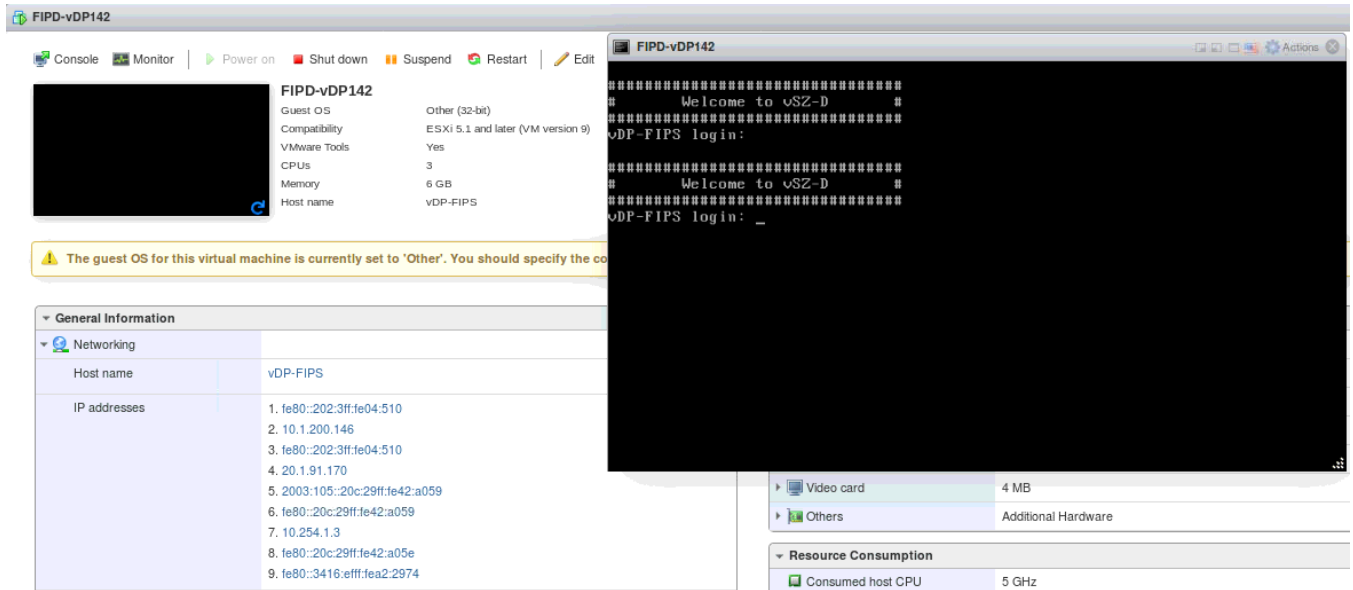
9. Click **Next** to review settings .

**FIGURE 72** Ready to Complete Installation



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

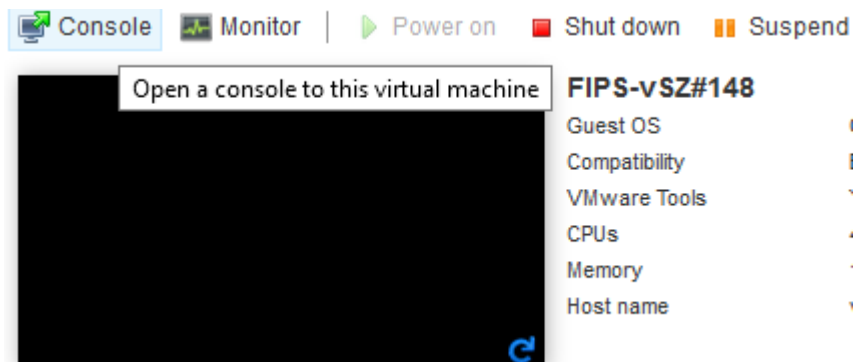
**FIGURE 73 Successful Installation**



## Joining vSZ-D to the vSZ Controller

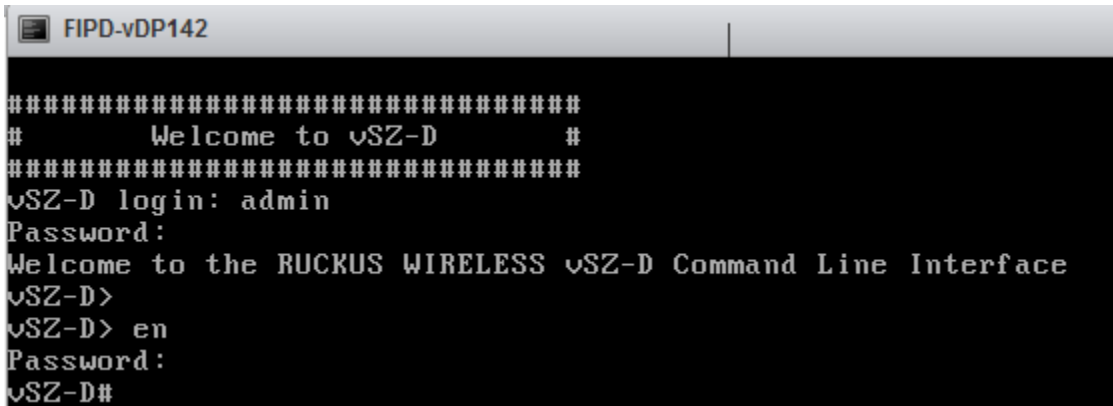
- Once the VM has been deployed, click **Power On** to start the vSZ-D.
- Open a console window to log in to the vSZ-D CLI.

**FIGURE 74 vSZ CLI Console**



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

**FIGURE 75** Logging In to Privileged EXEC Mode



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

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

**NOTE**

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

**FIGURE 76** 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_
```

- 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 77 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):
```

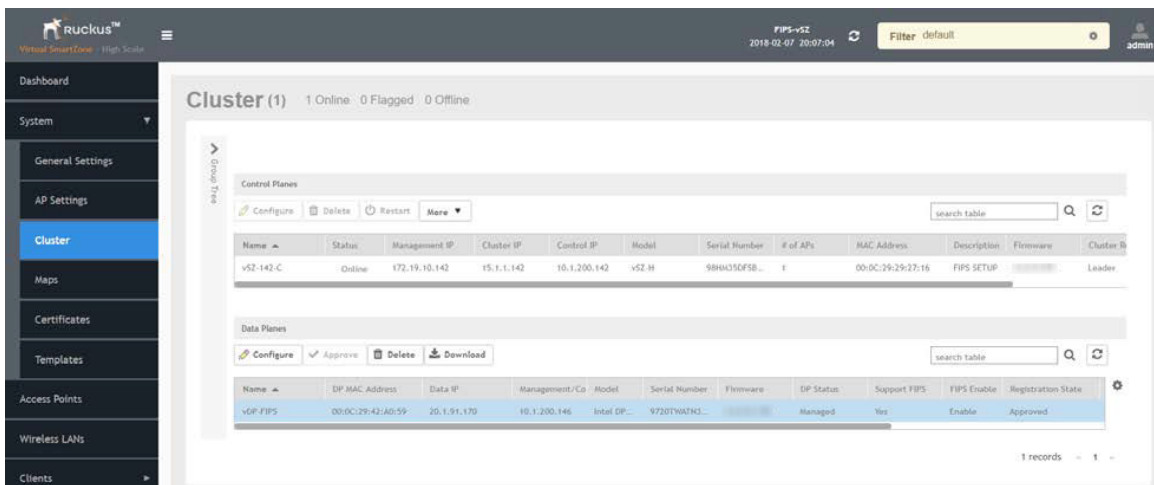
- Follow the sequence of steps shown in the following figure to join vSZ-D to the vSZ controller. The process changes the FIPS mode for vSZ-D according to the FIPS mode state of vSZ.

FIGURE 78 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 79 vSZ-D FIPS image approved



## Using FIPS CLI Commands (vSZ-D)

- 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 80** List of vSZ-D FIPS Commands

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

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

**FIGURE 81** Output of **fips selftest** Command

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

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

**FIGURE 82** 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 83** Using the fips zeroization Command

```
vSDP-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.

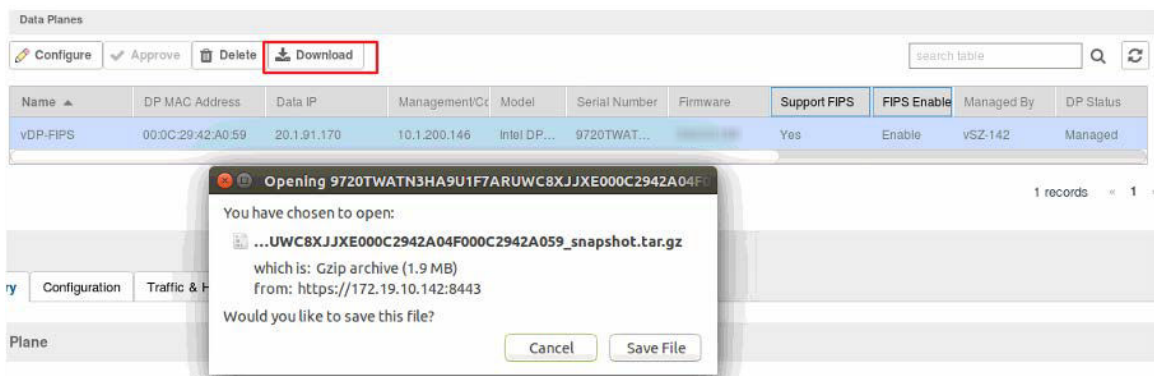
Perform the following steps to download vSZ-D FIPS logs.

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 84** 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..... 95
- FIPS AP Behavior..... 95
- Crypto Officer Roles and Responsibilities for AP..... 96
- Quarantine State for AP..... 96
- AP Features Not Supported in FIPS Mode..... 97

## AP Models that Support FIPS Mode

The following AP models support FIPS mode:

- E510
- R610
- R710
- R720
- T610
- T610s
- T710
- T710s

**NOTE**

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

The following ECDSA curves are supported by the AP:

- Elliptic curve: secp256r1
- Elliptic curve: secp384r1
- Elliptic curve: secp521r1

**NOTE**

When DP acts as a TLS client, it supports these three elliptic curves.

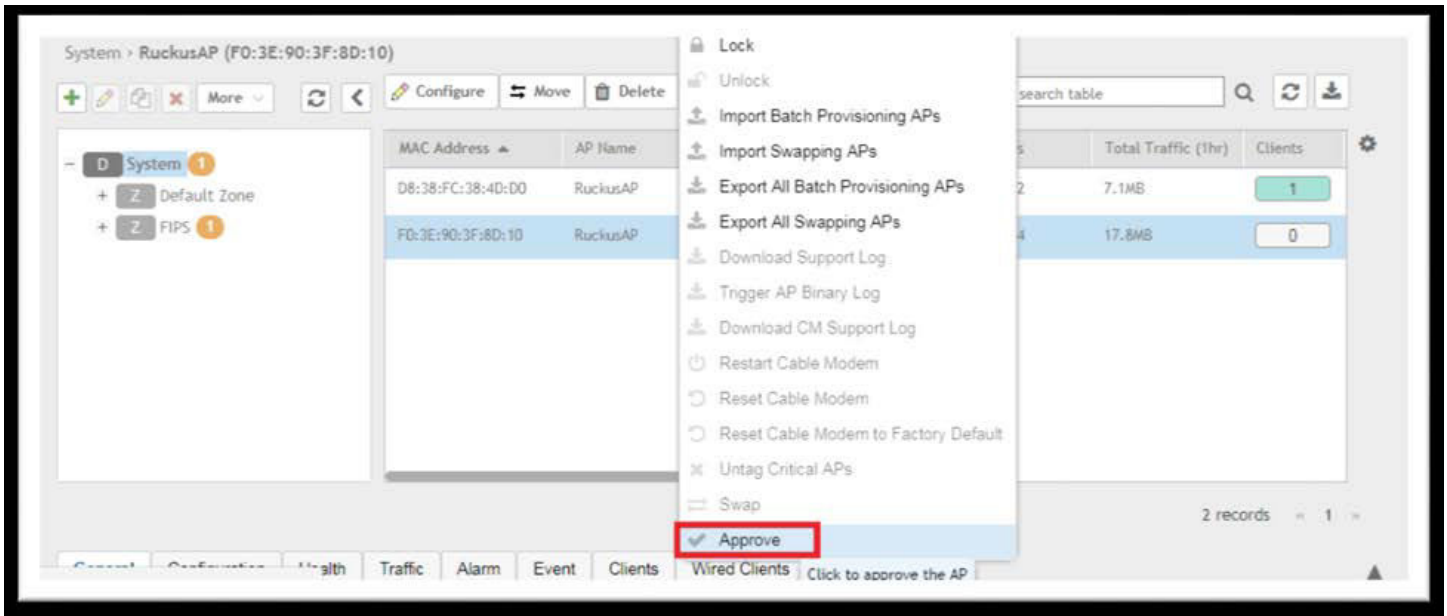
## FIPS AP Behavior

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

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

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

FIGURE 85 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: **set ap2ap\_dormant 1** on the AP or **rclient -d <ap-mac> -c "set ap2ap\_dormant 1"** on the controller.

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

## Crypto Officer Roles and Responsibilities for AP

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

## Quarantine State for AP

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

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

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

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

The following LEDs on the AP (R720, 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.)
- WLAN interface state cannot be set to Up or Down from AP CLI
- Not recommended to enable URL filtering in Common Criteria deployments since it is not CC certified

### **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 86 Output to get wlanlist Command

```
rkscli: 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 87 Unavailable Upgrade Methods in FIPS Mode

The screenshot shows the web interface for a Ruckus R720 Multimedia Hotzone Wireless AP. The page title is "Maintenance :: Upgrade". On the left, there is a navigation menu with sections: Status (Device, Internet, Local Subnets, Radio 2.4G, Radio 5G), Configuration (Device, Internet, Ethernet Ports), Maintenance (Upgrade, Reboot / Reset, Support Info), and Administration (Management, Diagnostics, Log). The main content area has the following elements:

- Upgrade Method:** Radio buttons for TFTP, FTP, Web, and Local. The Local button is selected. A red box highlights the TFTP, FTP, and Web options, indicating they are unavailable.
- Target Selection:** Radio buttons for Firmware and Device Certificate. Firmware is selected.
- Local Options:** A "Local File Name:" field with a "Choose File" button and the text "No file chosen".
- Warning:** A red-bordered box containing the text: "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."
- Perform Upgrade:** A button to execute the upgrade.

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

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

- Network Profile: 4bss
- SSH Access?:  Enabled  Disabled
- SSH Port: 22
- No Telnet & HTTP** (Red text)
- HTTPS Access?:  Enabled  Disabled
- HTTPS Port: 443
- Certificate Verification: PASSED (Green text), Request to reissue a new Ruckus PKI certificate
- PoE Operating Mode: AUTO (Dropdown menu)
- Auto-provisioning?:  Enabled  Disabled
- SmartCellGateway Agent?:  Enabled  Disabled
- Cloud Discovery Agent (FQDN):  Enabled  Disabled
- Set Controller Address (Reboot to take effect):  Enabled  Disabled

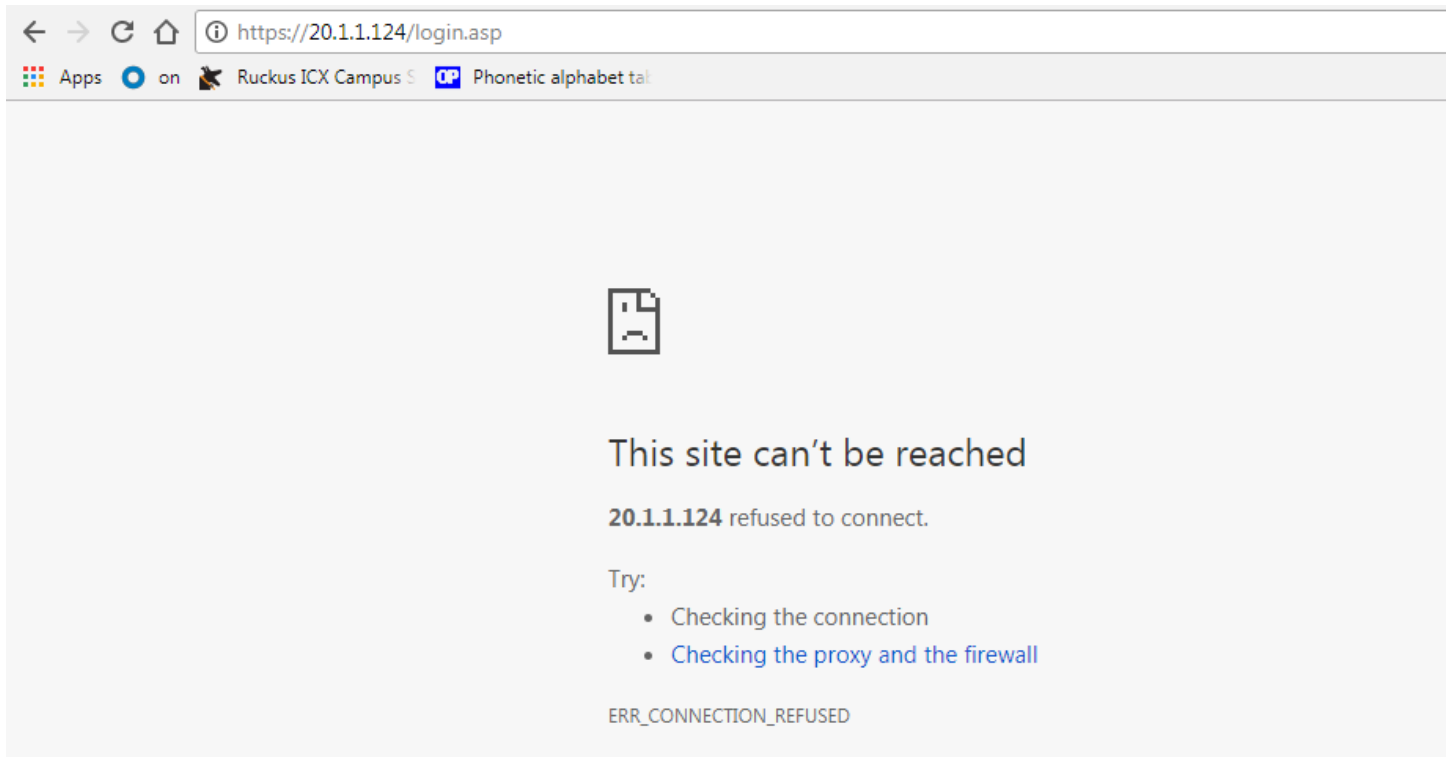
At the bottom, there are buttons for 'Update Settings' and a link for 'Restore previous settings'.

## 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 89** 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 90 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 91 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

- Validating Certificates..... 103
- Configuring X.509 Server Certificates on the Controller..... 105
- Uploading X.509 Certificates on vSZ-D..... 108

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.

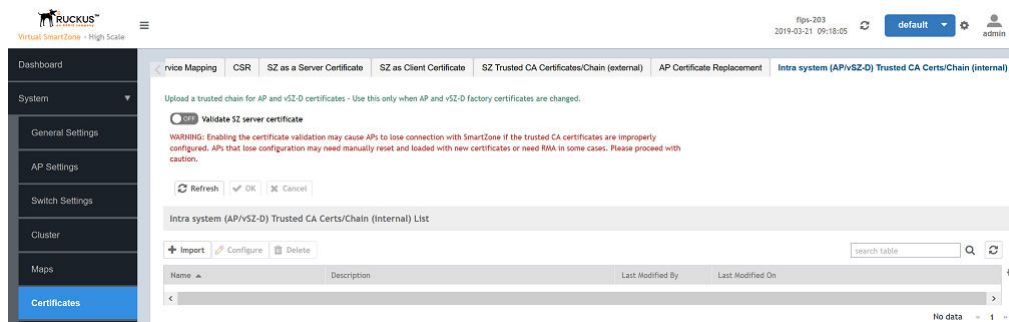
## Validating Certificates

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.

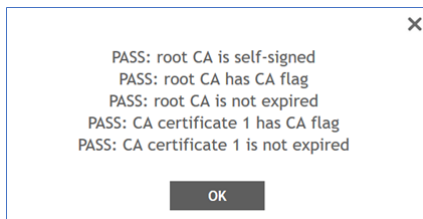
### NOTE

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

3. Click **Validate**.

The results of the validation are displayed.

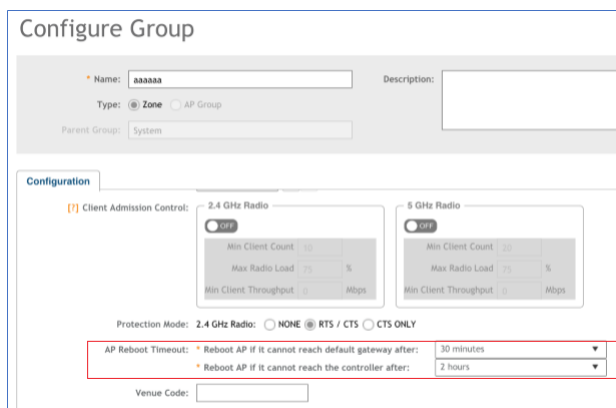
**FIGURE 93** Validation Message



4. Click **OK**.

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.

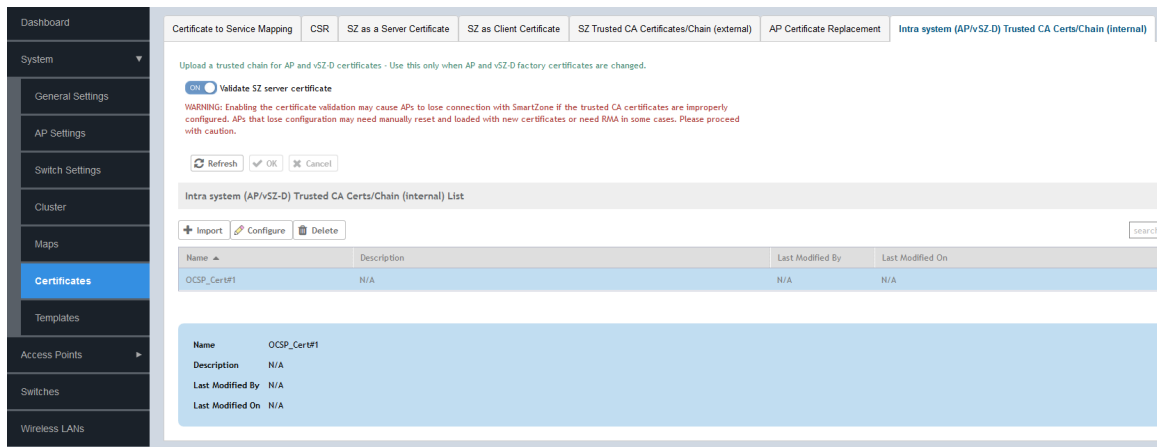
**FIGURE 94** Configuring AP Discovery Time



# Configuring X.509 Server Certificates on the Controller

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

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



## X.509 Certificates

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

#### 2. Under **Intra system (AP/vSZ-D) Trusted CA Certs/Chain (Internal) List,,**

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

- 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 or click **Using CSR** and select a key from the list.
- Key Passphrase: Enter the pass phrase.

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

#### Edit Certificate: OCSP\_SrvCert#1

Name:

Description:

Server Certificate

```
-----BEGIN CERTIFICATE-----
MIIEBTCCAeGgAwIBAgIBATAKBgkqhkiG9w0BBQwwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCQgE
Version: V3
Subject: EMAILADDRESS=ocspcsr@commscope.com, CN=ocspCSR.pem, OU=OCSP
validation, O=Commscope India Ltd, L=Vijayanagar, ST=Bagalkot, C=IN
Signature Algorithm: SHA256withRSA, OID = 1.2.840.113549.1.1.11
Key: Sun RSA public key, 2048 bits
modulus:
205811770012528435089202554786335359400199022665101870213768191871262835456034
981685401930891018917401808598191769257266165463806235260245316169650258681681
09395563614878896831333840035720884749824278471505163029427908323435953875389
436889033271138242783151900715292182908726193718167280850397874807583281960606
115546979095430454143919176892586048182180206776938632763597992132721178498488
762164553576903639989549687504984534514299855067037772708735718602494737789411
139974510631601550874880067850459818058895221926754442020360284945290121666888
43293345187204171849517516152563848741097251078616325042562192853732983
public exponent: 65537
```

Server Certificate:

Intermediate CA certificate:

Root CA certificate:

Private Key:  Upload

Using CSR

Key Passphrase:

## Edit CA Chain Certificates: OCSP\_Cert#1

\* Name:

Description:

Intermediate CA Certificates:

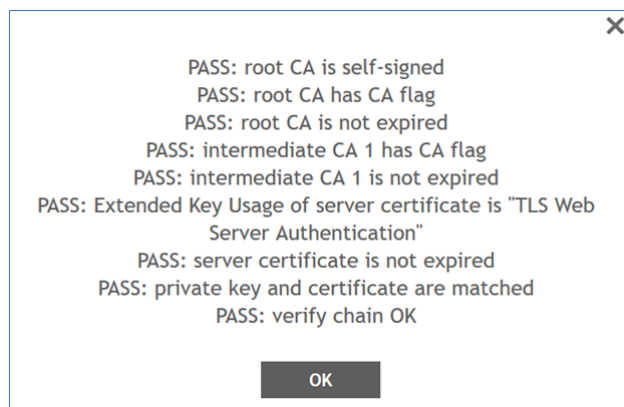
<input checked="" type="checkbox"/>	<input type="text" value="ca-chain.cert.pem"/>	<input type="button" value="Browse"/>	<input type="button" value="Clear"/>
<input type="checkbox"/>	<input type="text"/>	<input type="button" value="Browse"/>	<input type="button" value="Clear"/>
<input type="checkbox"/>	<input type="text"/>	<input type="button" value="Browse"/>	<input type="button" value="Clear"/>
<input type="checkbox"/>	<input type="text"/>	<input type="button" value="Browse"/>	<input type="button" value="Clear"/>

\* Root CA Certificate:

3. Click **Validate**.

The results of the validation are displayed

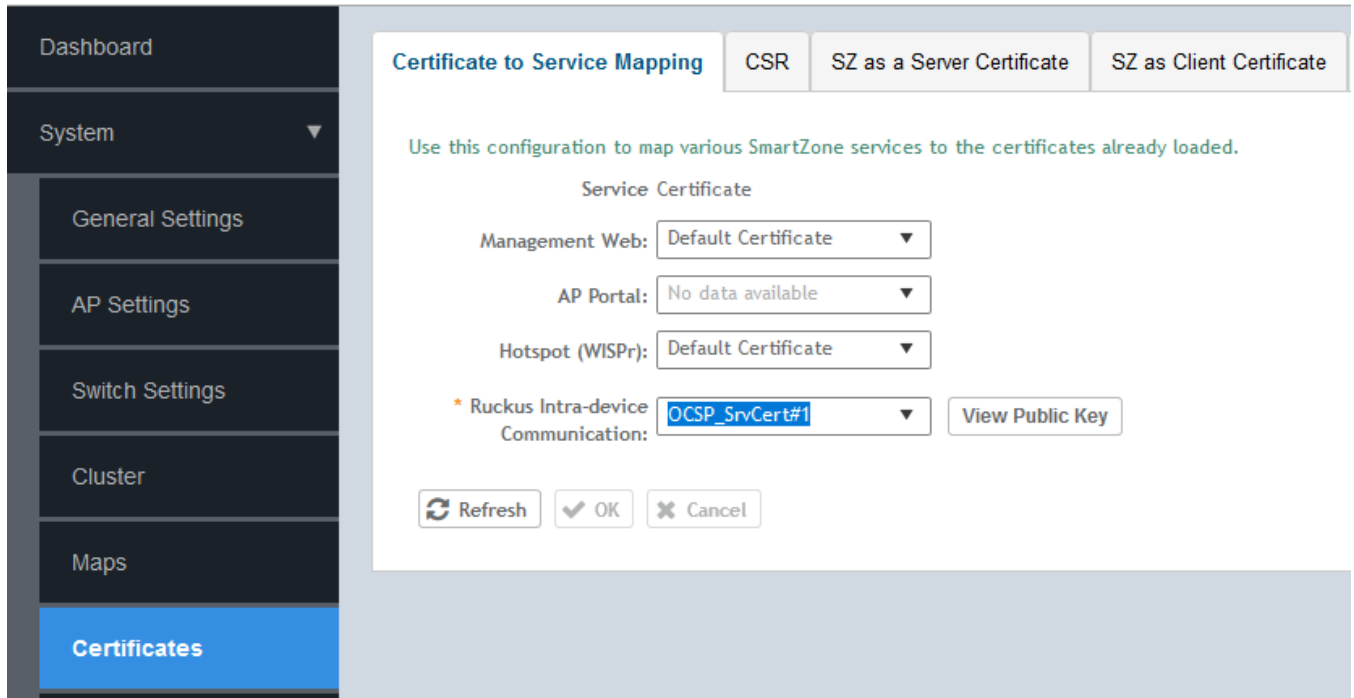
**FIGURE 95** Validation Message



4. Click **OK**.

5. 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 96** Mapping Service Certificates



6. Click **OK**.

## 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.
3. The following message is displayed: \*\*\*\*\* Paste your certificate sentence including BEGIN/END CERTIFICATE:  
\*\*\*\*\* Example: -----BEGIN CERTIFICATE-----  
xx -----END CERTIFICATE-----  
\*\*\*\*\* . Paste the contents of the *ca.pem* file.
4. Press **Enter** to finish.  
The certificate format is verified. Once verification is completed, the following message is displayed: Verify certificate format done please type " end " 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**.



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----
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
-----END CERTIFICATE-----
*****

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

----BEGIN CERTIFICATE----
MIIEtzCCA5+gAwIBAgIJAP38SkXhlwnzMA0GCSqGSIb3DQEBCwUAMIGYMQswCQYD
VQQGEwJVUzELMAkGA1UECBMCQ0ExEjAQBgNVBAcTCVN1bm55dmFsZEdMBsGA1UE
ChMUUnVja3VzIFdpdmVsZXNzIEluYy4xKTAnBgkqhkiG9w0BCQEWGnNlcnZpY2VA
cnVja3VzdzIyZWxlcnM3Y29tMR4wHAYDVQQDExVDXJ0aWZpY2F0ZSBBdXR0b3Jp
dHkwHhcNMTgwOTE3MDMzNjQ1WzYwOTUzMDMzNjQ1WjCBMDELMAkGA1UEBHMCM
VVMxZmZlbnRlbnRlbnRlbnRlbnRlbnRlbnRlbnRlbnRlbnRlbnRlbnRlbnRlbnRl
Y2t1cyBxXjIyZWxlcnM3Y29tMR4wHAYDVQQDExVDXJ0aWZpY2F0ZSBBdXR0b3Jp
c3dpdmVsZXNzLmNvbTEeMBwGA1UEAxMVV2VudGlnaWNhdGUGXV0aG9yaXR5MIIB
IjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAp3BM7P3ZEUWwuFT8+ejJ+UP0
kODr+RDMl6u9kBJqsURYpw+hRZnpN56LfeNp+GBBTBlJgKJ3RdTmK22zs9gj2JeD
AZZ72K72GEiYMikfoXXY5Nrl6Dat2MrZmxOtpqZkKtwG6SyTywtpxUnlpgzQcHx4
rXvr4ikoxKaNWYXAxJcGXmWrPhQ91Bm3XjgB/6W8Zch+aXh1jL5kPnhWLzuzLqLV
Q9+EmVE6eyc2TzMZBu0qlyciN9KgMipGluIDJzWw7PUwnPjU12CpT4rFtWbl6W5
AyrXqAAbP0W+vLobVYqkaytkSldr9qhaC398WljHmM5mz90Cb+i4yTOcbINi8QID
AQABO4IBADCB/TAdBgNVHQ4EFgQUdJcnbgqRcK2B/mDGYy6w12gSvkgwgc0GA1Ud
IwSbXTCBwoAUDjcnbgqRcK2B/mDGYy6w12gSvkgwgc0GA1UdIwYwODUwR0wGwYD
VQKExRSdWNRdXMGV2lyZWxlcnM3Y29tMR4wHAYDVQQDExVDXJ0aWZpY2F0ZSBBd
dXN3aXJlbGVzcy5jb20xHjAcBgNVBAMTFUNlcnRpZmljYXRIIEF1dGhvcml0eYUJ
AP38SkXhlwnzMAwGA1UdEwQFMAMBAf8wDQYJKoZIhvcNAQELBQADggEBAEUv3Kns
GJ5uNLoXWDlr2Mrt8Doh50cxXrBOPhtWaxyrQyNKzPY+i08p9ET1hjd+/+7e6ES
YgtiwleWR8iZHsn1GdXgFVhz55d8pJZ2NztbADdvhR1AJGkj5Hclw+oX1eeKql
wrkoYjGF/+O5O24+sWfftZb1HJDrEoGeQGSOIR+iBOB0yhHQHdvr9dozcZk37aD7
Hix74KlqDRh25xDiRYEGSg/joXGjh9tW4Bhe3sPgX195IHCKZycs+rknuy3SfLX

Verify your certificate format now, wait a moment.

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

## X.509 Certificates

Uploading X.509 Certificates on vSZ-D

### 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

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

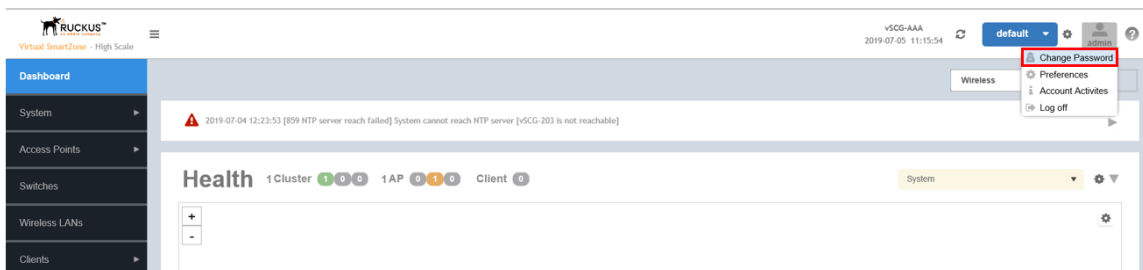
Passwords can be composed of any combination of uppercase and lowercase letters, numbers, and the following special characters: !, @, #, \$, %, ^, &, \*, (, and ). (No other special characters are allowed.) The password length ranges from 8 to 64 characters.

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

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

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

**FIGURE 97** Changing the Administrator Password



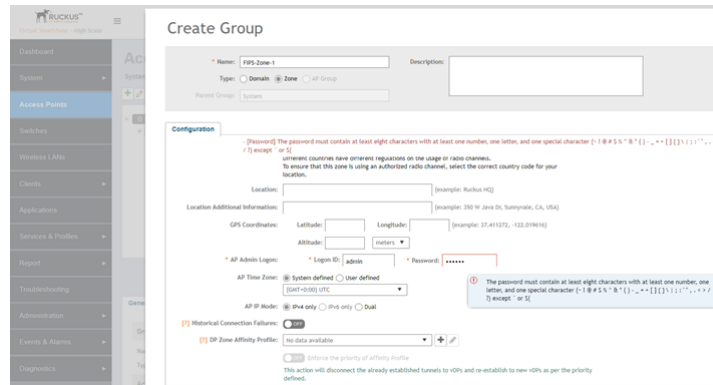
After the password is successfully changed, select **Administration > Admin Activities** to view the activity log. The account activity can be verified in the controller CLI by using the `/opt/ruckuswireless/wsg/log/web/activity.log` command.

**FIGURE 98** Sample Verification Message

```
2019-02-05 05:04:39,504 Activity User:[admin],Resource:[10.32.139.173],Action:[Log On],Resource:[Administrator],Description:[Administrator [admin] logged on from 10.32.139.173.]
2019-02-05 05:04:39,652 Activity User:[admin],Resource:[10.32.139.173],Action:[Re-authenticate],Resource:[Administrator],Description:[The re-authentication is successful.]
2019-02-05 05:04:39,658 Activity User:[admin],Resource:[10.32.139.173],Action:[Update],Resource:[Administrator],Description:[Administrator [admin] password changed.]
2019-02-05 05:04:39,836 Activity User:[admin],Resource:[10.32.139.173],Action:[Update],Resource:[Administrator],Description:[Administrator [admin] updated.]
```

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

**FIGURE 99** Modifying AP Admin Login



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

**FIGURE 100** Dataplane Password Change Event Log

Name	DP Type	DP MAC Address	Data IP	Management/Co	Model	Serial Number	Firmware	Managed By	DP Status	Registration Stat
Fps-vDP	External-Virtual	00:0C:29:3D:F5:90	25.1.91.203	10.1.200.41	v5Z-0	972032R09...	5.1.1.0.222	fips-203	Managed	Approved

Date and Time	Code	Type	Severity	Activity
2019/01/04 15:13:41	504	Data plane configuration up...	Informational	Data plane [fips-vDP@972032R0996A9V0P2L4NHQ4BRV000C296DF56000C296DF590] has been updated to dpcizer configuration [475e610-0e81-11e9-82f4-00000028689]
2019/01/04 15:13:41	99203	Password Management	Informational	Data plane [972032R0996A9V0P2L4NHQ4BRV000C296DF56000C296DF590] min password length changed, source: [DnsGUA], account: [admin].
2019/01/04 15:08:53	99214	Password Management	Informational	User logout to data plane [972032R0996A9V0P2L4NHQ4BRV000C296DF56000C296DF590], source: [10.1.200.203], account: [admin].
2019/01/04 15:06:49	99205	Password Management	Informational	Data plane [972032R0996A9V0P2L4NHQ4BRV000C296DF56000C296DF590] enable password changed, source: [10.1.200.203], account: [admin].
2019/01/04 15:06:50	99212	Password Management	Informational	User login into data plane [972032R0996A9V0P2L4NHQ4BRV000C296DF56000C296DF590], source: [10.1.200.203], account: [admin].
2019/01/04 15:05:42	99214	Password Management	Informational	User logout to data plane [972032R0996A9V0P2L4NHQ4BRV000C296DF56000C296DF590], source: [10.1.200.203], account: [admin].
2019/01/04 15:05:40	99205	Password Management	Informational	Data plane [972032R0996A9V0P2L4NHQ4BRV000C296DF56000C296DF590] enable password changed, source: [10.1.200.203], account: [admin].
2019/01/04 15:05:04	99205	Password Management	Informational	Data plane [972032R0996A9V0P2L4NHQ4BRV000C296DF56000C296DF590] enable password changed, source: [10.1.200.203], account: [admin].

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

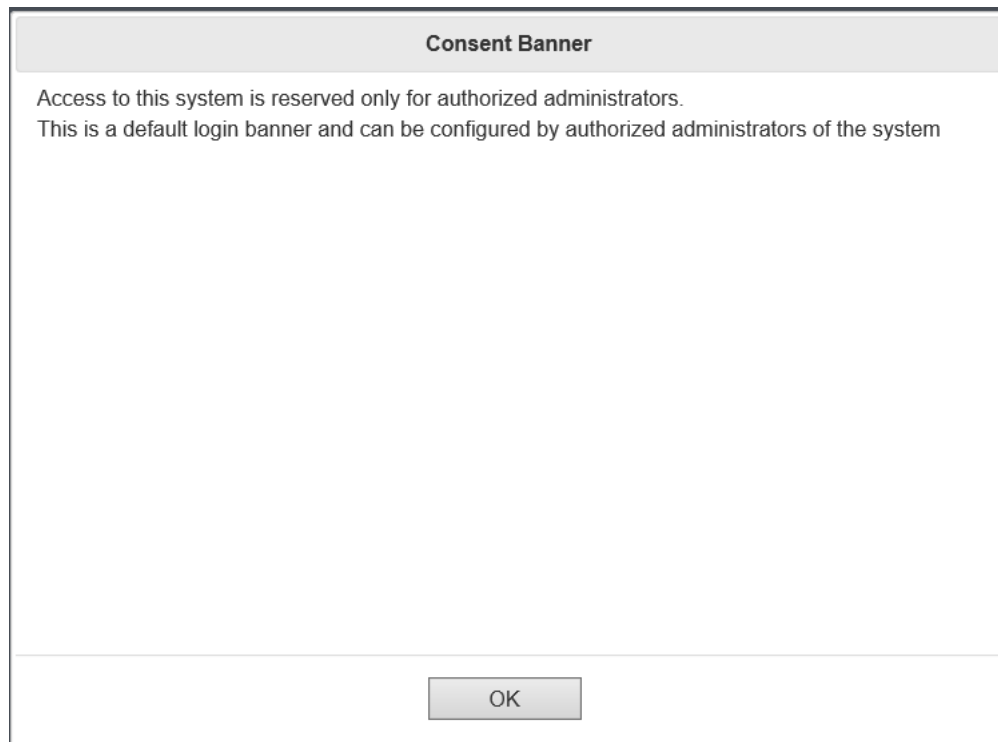
# Session Management

---

Complete the following steps to log in to the controller.

1. Enter the server URL in the browser window.  
The **Consent Banner** page is displayed.

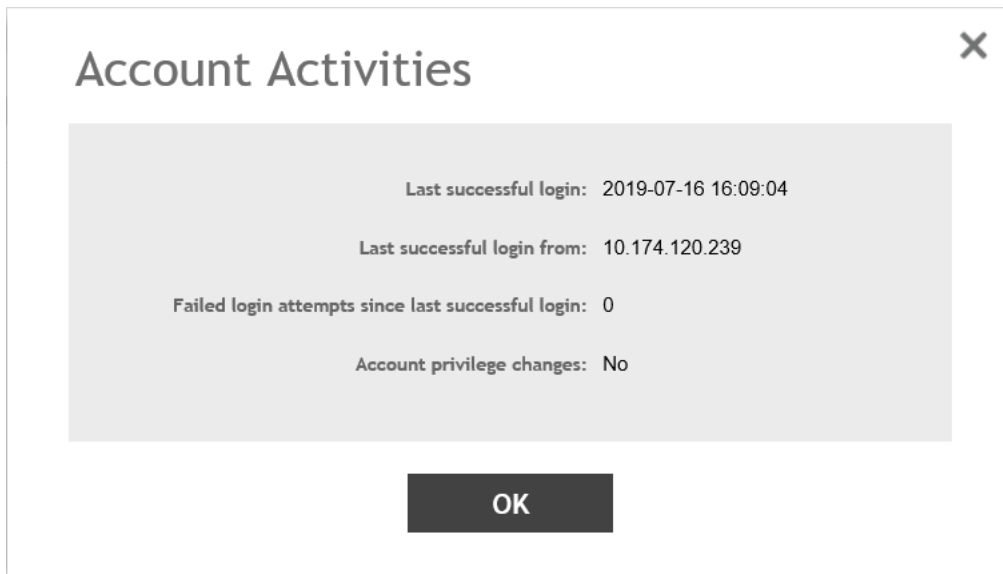
**FIGURE 101** Consent Banner



2. Click **OK** to proceed.

3. Enter the user name and password and click **Login**.  
The **Account Activities** page is displayed.

**FIGURE 102** Account Activities Page

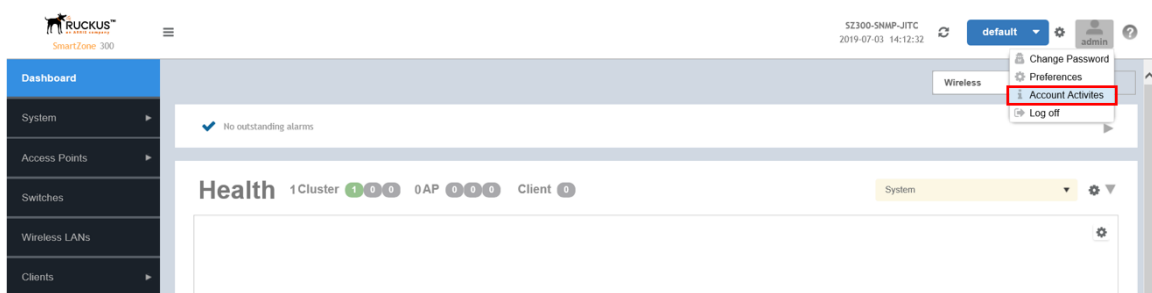


The **Account Activities** page notifies the administrator of the data and time of the last login, the IP address from where the last login was successful, the number of failed login attempts since the last successful login, and the account privilege changes of the administrator account since the last login.

4. Click **OK**.

Account activities can also be viewed from **Admin > Account Activities**.

**FIGURE 103** Viewing Account Activities



# Configuring the WLAN Scheduler

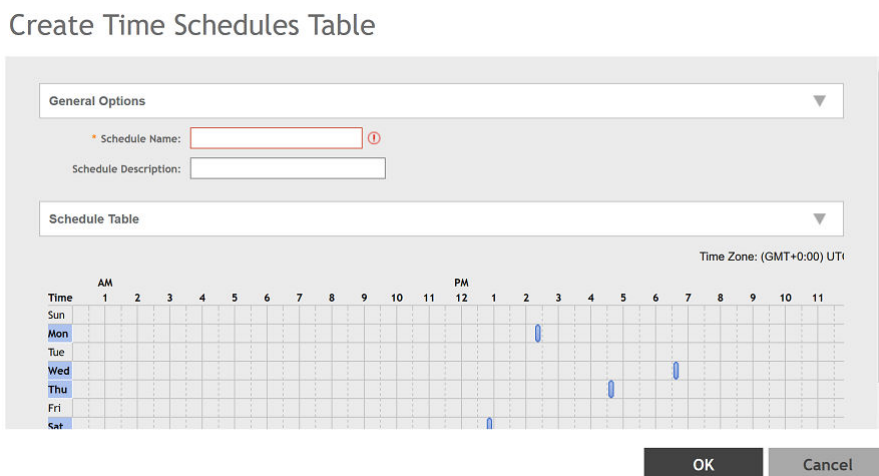
- [Setting the WLAN Scheduler from the CLI..... 116](#)

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 Schedules Table** page displays.

**FIGURE 104** Creating Time Schedules Table

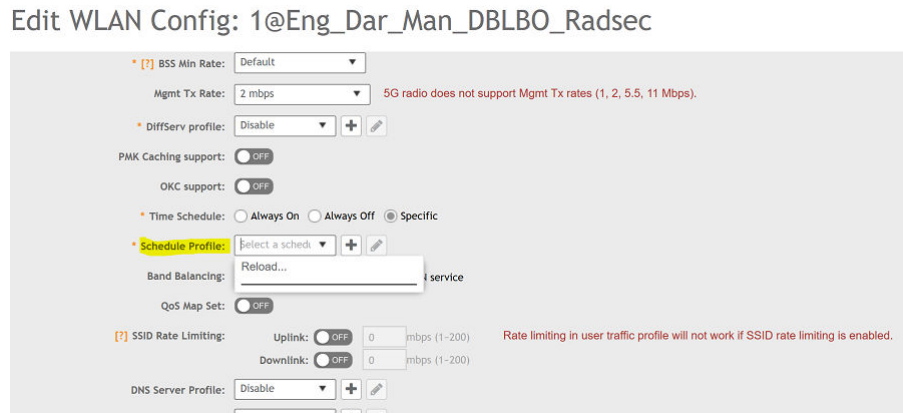


5. Click **OK**.

The time schedule is configured.

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

**FIGURE 105** Selecting the Scheduler Profile



## Setting the WLAN Scheduler from the CLI

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

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

**FIGURE 106** Sample Commands to Configure WLAN Scheduler from CLI

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

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



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

FIGURE 107 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|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|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|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|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|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|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|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 108 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|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|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|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|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|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|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|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
```



# Configuring Global and Account Security Settings

Complete the following steps to configure the global and account security settings for administrator accounts.

1. Select **Administration > Admins and Roles > Account Security**.

**FIGURE 112** Account Security Page

The screenshot shows the 'Account Security' configuration page. The 'Global Security' section has the following settings:

- Captcha for Login:
- Concurrent Session(s):  Maximum allowed interactive concurrent session per account: 3 (3 - 10) sessions
- Maximum allowed API concurrent session per account: 64 (64 - 2048) sessions
- Absolute Timeout Settings:  30 (1-1440) minutes

The 'Account Security' section contains a table with the following data:

Name	Idle Timeout	Account Lockout	Lockout Duration	Password Expiration	Password Reuse	Two-Factor Auth	Disable Inactive Accou	Minimum Password Len	Description
Arris-group	30 Minutes	Disabled	Disabled	90 Days	1	Disabled	90 Days	8	N/A
Default	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	N/A
test	15 Minutes	6 Failures	30 Minutes	90 Days	4	Disabled	90 Days	8	N/A
test1	15 Minutes	6 Failures	30 Minutes	90 Days	4	Disabled	90 Days	8	N/A

2. Under **Global Security**, you can configure the following options:
  - **Captha for Login:** Enable the option to provide additional security to ensure that a human is signing into the account.
  - **Concurrent Session(s):** Enable the option and enter the number of sessions:
    - Maximum allowed interactive concurrent sessions per account
    - Maximum allowed API concurrent sessions per account
  - **Absolute Timeout Settings:** Enable the option and enter the timeout in minutes. After the absolute timeout, the active web and public API sessions are closed.
3. Click **OK** to save the global security settings.

- Under **Account Security**, select an account security profile and click **Configure** to configure the profile. The **Edit Account Security** page is displayed.

**FIGURE 113** Editing an Account Security Profile

**Edit Account Security [Default]** ✕

Name:

Description:

Session Idle Timeout:  OFF  (1-1440) minutes

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

ON Lock account after  failed attempts during  minute time period.  
*This option does not apply to AAA Admin Users.*

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

Password Reuse:  OFF Passwords cannot be the same as the last  (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

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

Minimum Password Length:  OFF Password must be at least  (8-64) characters  
*When minimum password length is changed, admin should change passwords for all users manually as well. Minimum password length changes apply for all future passwords only*

Password Complexity:  OFF Password must be fulfilled as below:  
*When the password complexity is turned from off to on, admin should change all users' passwords manually. The password complexity rule will only be applied to the upcoming password changes.*

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

5. Enable and configure the following options:
    - **Session Idle Timeout:** Enter the timeout duration in minutes.
    - **Account Lockout:** Enter the account lockout time and number of failed authentication attempts.
    - **Password Expiration:** Enter the number of days the account password will be valid.
    - **Password Reuse:** Enter the number of times the last passwords must not be reused. By default, last four passwords cannot be reused.
    - **Two-Factor Authentication:** Provides username/password and SMS authentication. For SMS authentication, the SMS gateway must be configured.
    - **Disable Inactive Accounts:** Enter the number of days after which the administrator user IDs are locked due to inactivity.
    - **Minimum Password Length:** Enter the minimum number of characters required for a password. If there is a change in the minimum password length, then the administrator must change the passwords for all users manually.
    - **Password Complexity:** The password entered must adhere to the following rules:
      - At least one uppercase character
      - At least one lowercase character
      - At least one numeric character
      - At least one special character
      - At least eight characters from the previous password is changed
    - **Minimum Password Lifetime:** Ensures that the password is not changed twice within a period of 24 hours.
- For more details, refer to the section *Creating Account Security* in the *SmartZone Administrator Guide* for this release.
6. Click **OK** to save the account security profile.



# Terminating Sessions

- Terminating Sessions for Non-Admin Users..... 124
- Terminating Administrator Sessions..... 125

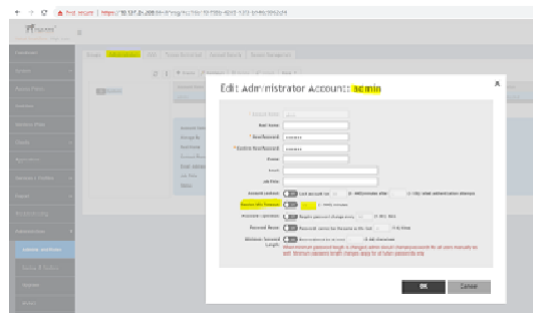
The SmartZone controller can terminate a remote interactive session after it has exceeded the session timeout value configured by the security administrator.

## Terminating Sessions for Admin Users

The session idle timeout configuration applies to managed AP's and vSZ-D.

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

**FIGURE 114** Session Idle Timeout Configuration



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

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

**FIGURE 115** 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 the CLI sessions of the AP and vSZ-D, the session idle timeout value configured from the administrator profile is applicable.

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

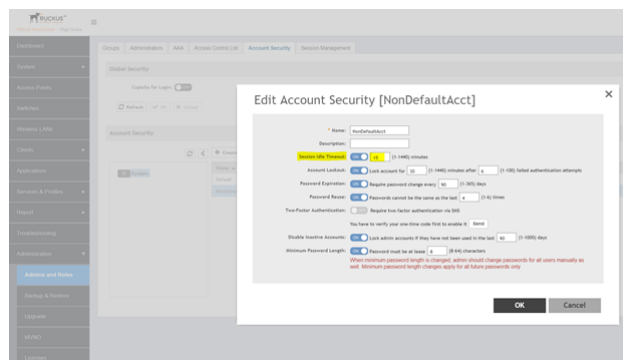
For a GUI session, the default session idle timeout is 15 minutes.

# 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.

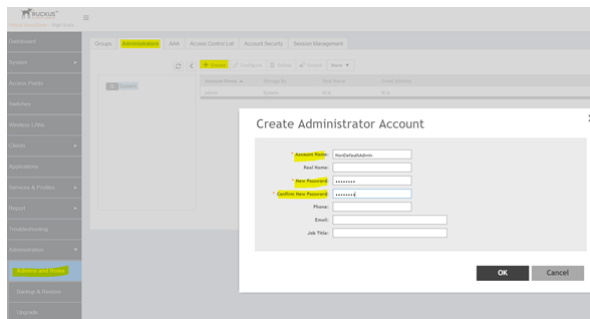
**FIGURE 116** Session Timeout Configuration from the Security Profile



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.

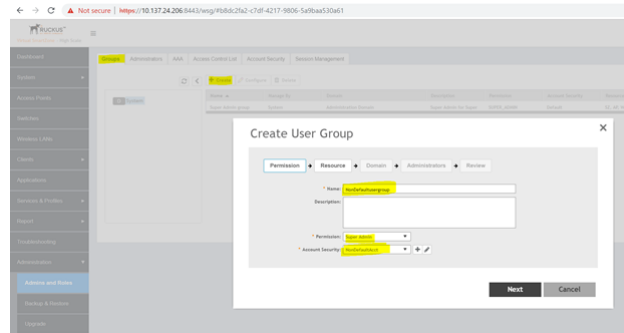
**FIGURE 117** Creating a Non-Admin Account





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

**FIGURE 118** 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.

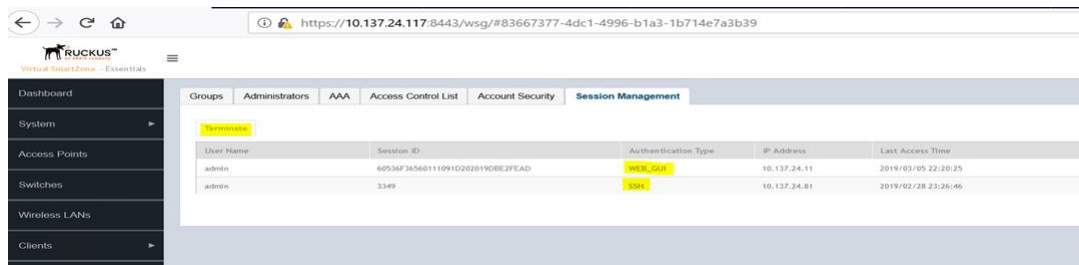
1. From the controller web interface, select **Administration > Admin and Roles > Session Management**
2. Select the administrator session you want to discontinue and click **Terminate**.

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 119** Sample Session Termination for Web Interface Session.



**FIGURE 120** Sample Session Termination for CLI Session.

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

en
Please wait. CLI initializing...

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

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

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

# Locking an Administrator Account

- [Locking Non-Administrator Accounts..... 128](#)

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

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

The **Edit Administrator Account** page appears.

**FIGURE 121** Configuring the Account Lock

## Edit Administrator Account: admin

Account Name: admin

Real Name:

New Password: .....

Confirm New Password: .....

Phone: 68687886687

Email:

Job Title: Admin

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

Session Idle Timeout:  ON 60 (1-1440) minutes

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

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

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

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

Password Complexity:  OFF Password must be fulfilled as below:

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

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

OK Cancel

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

### NOTE

The administrator must wait until the lockout period expires.

4. Click **OK**. The **Password Confirmation** screen appears.
5. Click **OK**.  
You can modify the account lock settings from the security profile also. Select **Administration > Admins and Roles > Account Security**, and click **Configure** to edit the value from within the selected profile.

## Locking Non-Administrator Accounts

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

1. From the controller web interface, select **Administration > Admin and Roles > Account Security**.
2. Click **Configure**.
3. Enable **Account Lockout** and configure one of the following options:
  - Enter the account lockout time and the number of failed authentication attempts.
  - Enter the number of failed attempts after which the account is locked and the corresponding time period. For example, after three unsuccessful login attempts in a time interval of 15 minutes, the account is locked and must be released by an administrator.

**FIGURE 122** Account Lockout Configuration from the Security Profile

**Edit Account Security [Default]** ✕

Name:

Description:

Session Idle Timeout:  OFF  (1-1440) minutes

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

ON Lock account after  failed attempts during  minute time period.  
*This option does not apply to AAA Admin Users.*

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

Password Reuse:  OFF Passwords cannot be the same as the last  (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

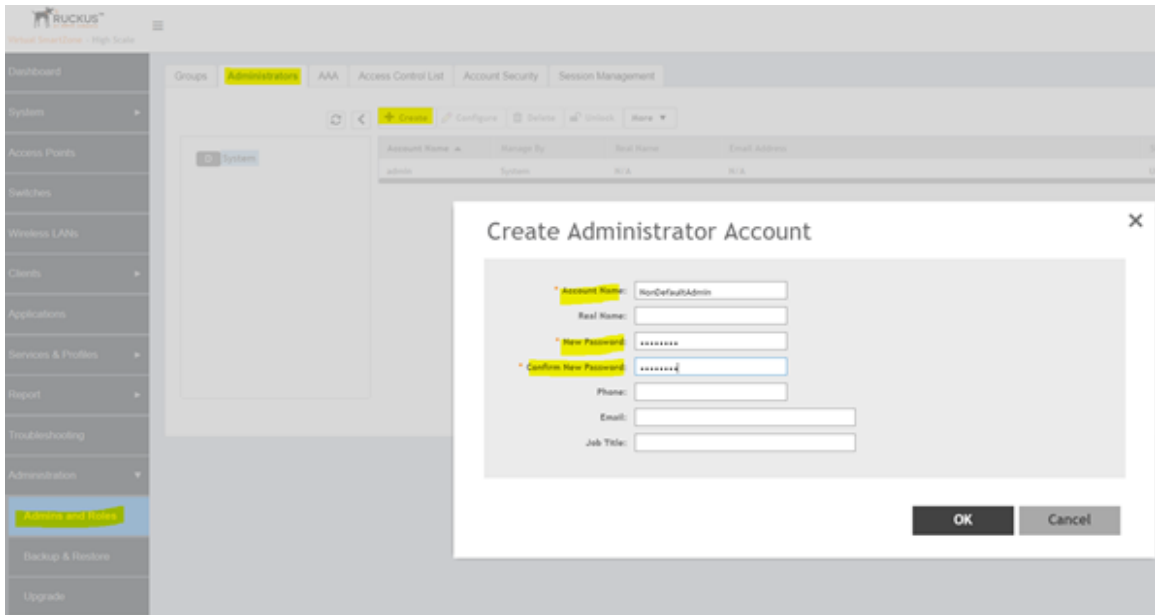
Disable Inactive Accounts:  OFF Lock admin accounts if they have not been used in the last  (1-1000) days

Minimum Password Length:  OFF Password must be at least  (8-64) characters  
*When minimum password length is changed, admin should change passwords for all users manually as well. Minimum password length changes apply for all future passwords only*

Password Complexity:  OFF Password must be fulfilled as below:  
*When the password complexity is turned from off to on, admin should change all users' passwords manually. The password complexity rule will only be applied to the upcoming password changes.*  
· At least one upper-case character  
· At least one lower-case character

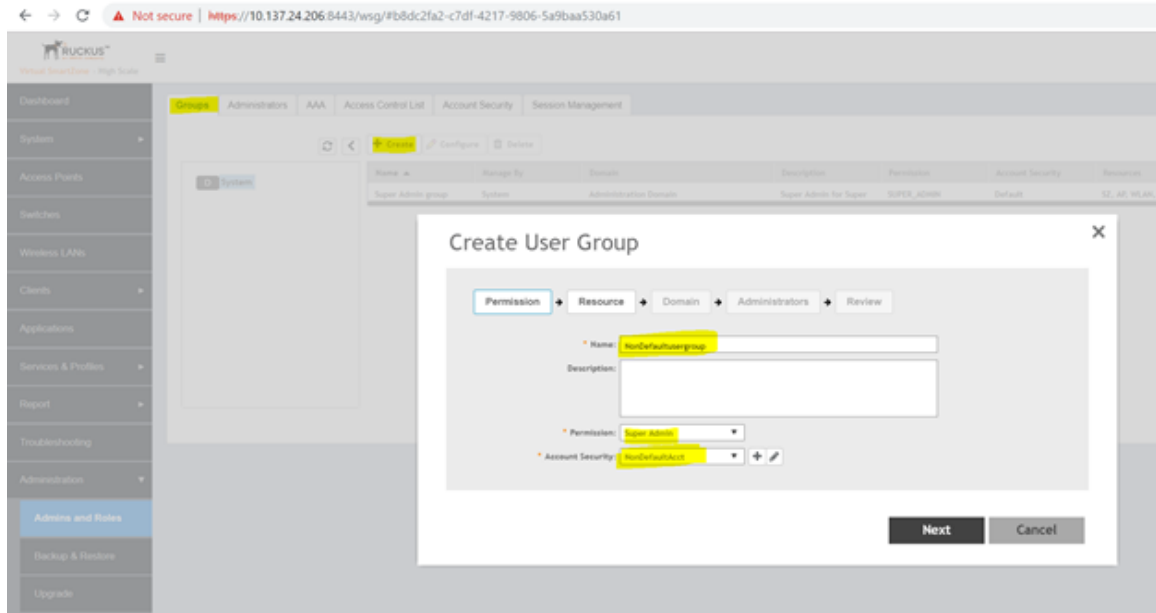
4. To create a non-administrator user account, select **Administration > Admin and Roles > Administrators**.

**FIGURE 123** 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 124** Creating User Groups



For detailed configuration information, refer to the section *Creating User Groups* in the *SmartZone Administrator Guide* for this release.

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

**FIGURE 125** Locked User Account

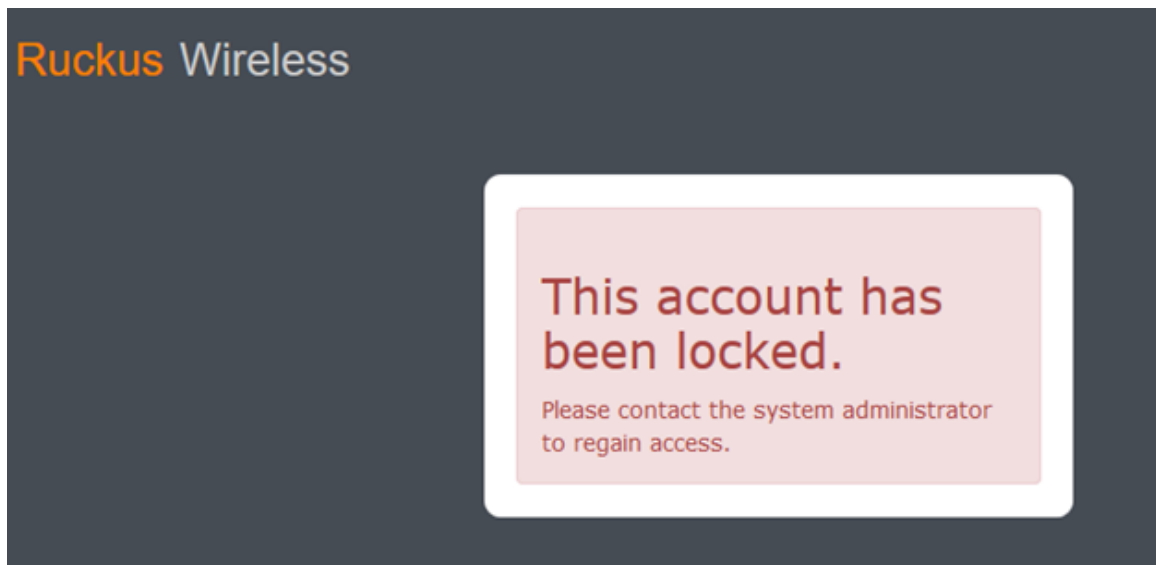


FIGURE 126 AP User Locked: Verification from CLI

```
[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 :

arkscli : Login failureConnection to 192.168.11.67 closed.
[root@IRAWAT ~]#
```

FIGURE 127 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. For detailed configuration information, refer to the *Managing Events and Alarms* section in the *SmartZone Administrator Guide* for this release.



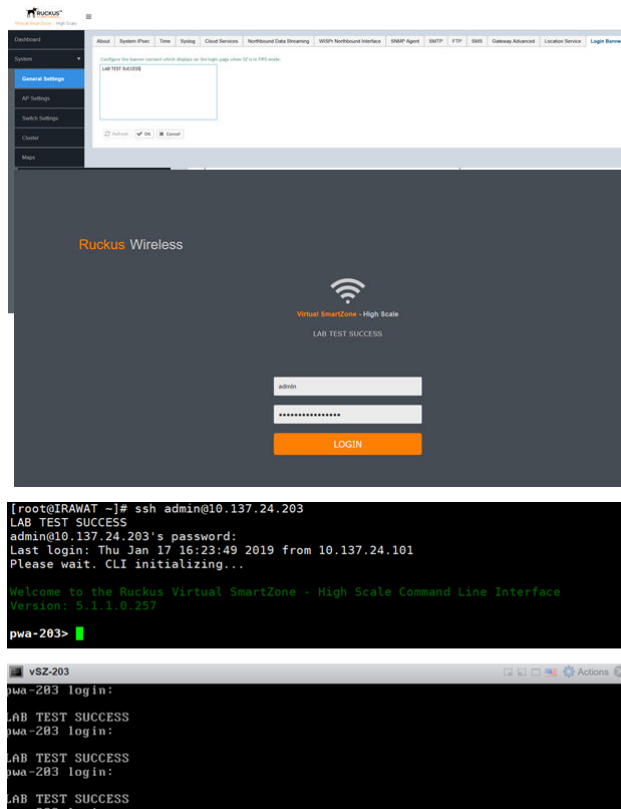


# Setting Up the Login Banner

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

1. From the controller web interface, Select **System** > **General Settings** > **Login Banner**.
2. Configure the content of the login banner as required.

**FIGURE 128** Login Banner: Web Interface and CLI

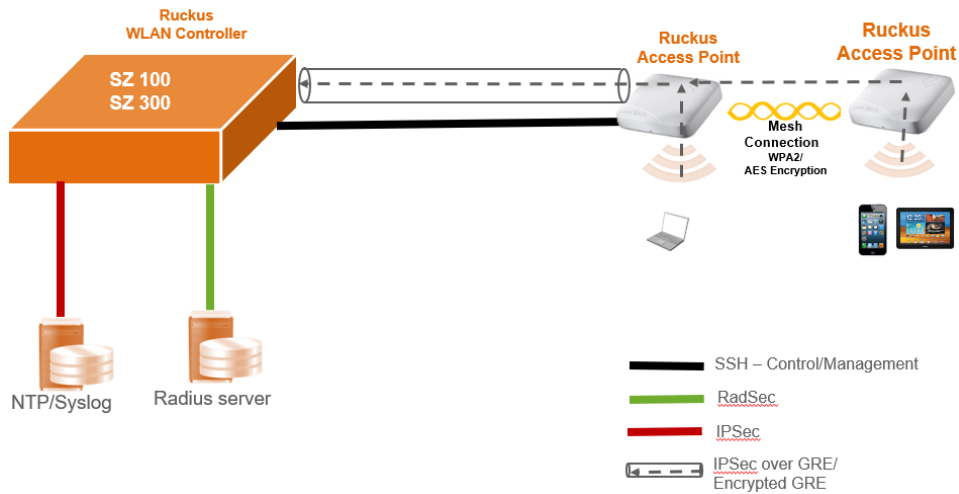




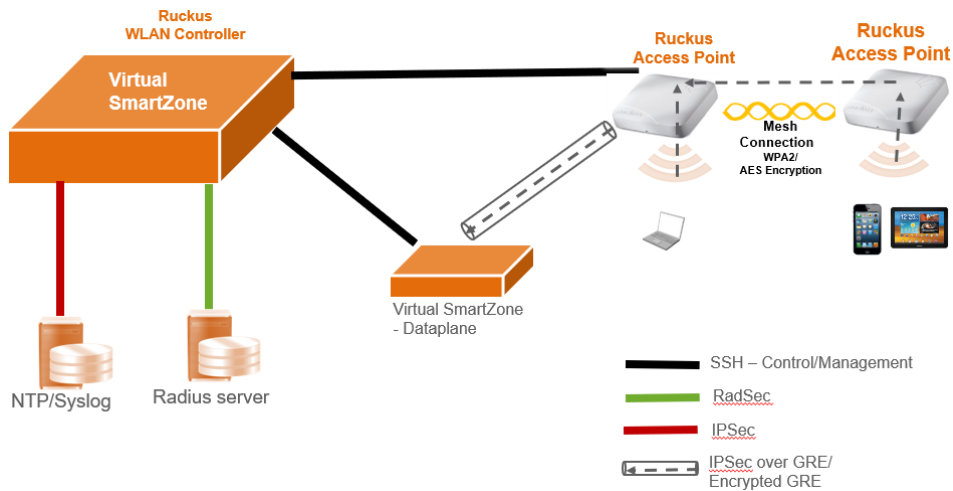
# IPsec Tunnel Setup

SZ and vSZ maintain different centralized deployment models for IPsec tunnel setup..

**FIGURE 129** IPsec Tunnel Setup: SZ and External Server



**FIGURE 130** IPsec Tunnel Setup - vSZ and External Server



**NOTE**

The SSH encryption algorithm, the SSH integrity MAC algorithm, the SSH client and server parameters, and the rekey limitation are not user-configurable. The rekey limitation is 1 hour or 1 GB of data traffic when the DP or AP connects to the SZ SSH server as an SSH client. The SSH client or server discards the data packets if the incoming packet size exceeds the packet size limitation; the maximum packet size is 256 KB.



# Configuring 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**

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

**NOTE**

The preshared key text ranges from 8 through 64 ASCII characters or 44 through 128 bit-based characters.

- 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**

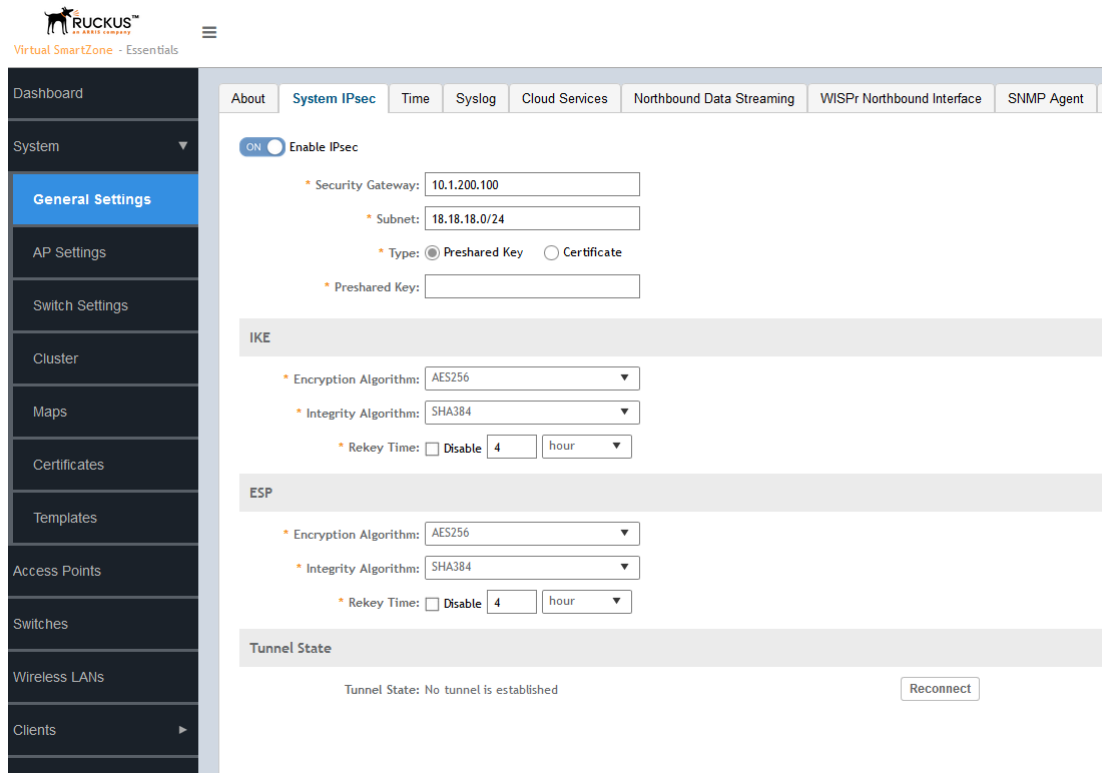
The supported encryption algorithms are AES128, AES192, and AES256. The supported integrity algorithms are SHA1, SHA256, SHA384, and SHA512. By default, DH group is DH-20 [ECP-384], which cannot be changed.

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

**NOTE**

System IPsec supports tunnel mode only.

FIGURE 131 System IPsec Settings



2. Click **OK**.





# 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**
- Remote ID: Enter the remote ID for certificate authentication.
- **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 132 System IPsec Settings

ON  Enable IPsec

\* Security Gateway: 10.1.200.100

\* Subnet: 18.18.18.0/24

\* Type:  Preshared Key  Certificate

\* Remote ID: =aaa, L=aaa, O=aaa, OU=aaa, CN=aaa

\* Certificate: ocsPCA18

\* OSCP:  OFF

IKE

\* Encryption Algorithm: AES128

\* Integrity Algorithm: SHA1

\* Rekey Time:  Disable 4 hour

ESP

\* Encryption Algorithm: AES128

\* Integrity Algorithm: SHA1

\* Rekey Time:  Disable 4 hour

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 133 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 System Time

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

The NTP server, which is accessible through the IPsec tunnel, securely synchronizes its time with that of the controller. The NTP server is also reachable through the IP address.

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

**FIGURE 134** Setting System Time

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

- System Time:** 2019-07-04 20:01:35 IST
- System UTC Time:** 2019-07-04 14:31:35 UTC
- NTP Primary Server:** 10.1.200.100 (with a 'Sync Server' button)
- NTP Backup Server:** (empty field)
- System Time Zone:** (GMT+5:30) IST (dropdown menu)

Below these are two sections for authentication:

- NTP Primary Server Authentication:**
  - Key Type: SHA1 (dropdown)
  - Key ID: 1 - 65534
  - Key: (empty field)
- NTP Backup Server Authentication:**
  - Key Type: SHA1 (dropdown)
  - Key ID: 1 - 65534
  - Key: (empty field)

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

2. For **NTP Primary Server**, enter the NTP primary server address that you want to use.

**NOTE**

Provide the IP address that is part of the IPsec subnet configured in the System IPsec configuration.

3. For **System Time Zone**, select the time zone from the list that you want the controller to use.

**NOTE**

The default time zone is (GMT +0:00) UTC.

4. Click **Sync Server**.

**NOTE**

First, the SZ time is synced with the configured NTP server and then the cluster follower AP's and vDP's time is synced to the SZ time.

5. Under **NTP Primary Server Authentication**, provide the NTP primary server authentication which includes the **Key Type, Key ID, and Key**.  
Only the SHA1 key type is supported. The key ID ranges from 1 through 65534.
6. Under **NTP Primary Backup Authentication**, provide the NTP backup server authentication information which includes the **Key Type, Key ID, and Key**.  
Only the SHA1 key type is supported. The key ID ranges from 1 through 65534.
7. Click **OK**.

The syslog server is reachable by the way of an IPSec tunnel and it will receive the logs in a secured way from the controller, provided System IPSec is enabled.

In order to configure the NTP subnet accessible by way of IPSec, refer to [Configuring System IPsec using Preshared Key](#) on page 137 and [Configuring System IPsec using Certificates](#) on page 141.

# Configuring SoftGRE and IPsec in the WLAN

You can configure the Soft GRE tunnel profile and IPsec profile in the WLAN to manage AP traffic.

1. Follow the steps listed in "Creating a SoftGRE Profile" of the *SmartZone Administrator Guide* for this release to create a SoftGRE profile.

## NOTE

Only IPv4 addressing format is supported for FIPS devices.

2. Follow the steps listed in "Creating an IPsec Profile" of the *SmartZone Administrator Guide* for this release to create a IPsec profile.

## NOTE

For **Tunnel mode**, select SoftGRE. Only IPv4 addressing format is supported. SoftGRE over IPsec supports tunnel mode only.

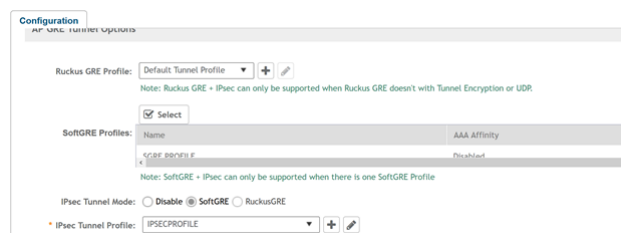
Refer to the topology diagrams in the section *Configuring System IPsec using Preshared Key* to setup IPsec tunnel for SZ and vSZ.

The following Security Association options are supported for FIPS devices:

- Encryption Algorithm: Options include AES128, AES192, and AES256.
- Integrity Algorithm: Options include SHA1, SHA256, SHA384, and SHA512.
- Pseudo-Random Function: Options include Use integrity ALG, PRF-SHA1, PRF-SHA256, PRF-SHA384, and PRF-SHA512.
- DH Group: Options for Diffie-Hellman groups for IKE include modp768, modp1024, modp1536, modp2048, modp3072, modp4096, modp6144, modp8192, ECP384.

3. Create an AP zone with the appropriate SoftGRE and IPsec profiles. Go to **Access Points**.
4. Select the FIPS zone and click the + icon to configure the AP GRE Tunnel Options from the **Configuration** tab. Refer to "Creating an AP Zone" of the *SmartZone Administrator Guide* for this release.

**FIGURE 135** AP GRE Tunnel Configurations



5. Go to **Wireless LAN**.
6. Select the zone. The **Creating WLAN Configuration** page displays.
7. Go to **Data Plan Options** and select the SoftGRE tunnel profile. By default, SoftGRE and IPsec are enabled and attached at the zone level to the WLAN.





# 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.

1. Follow the steps listed in the "Creating an IPsec Profile" of the *SmartZone Administrator Guide* for this release to create a IPsec profile.

## NOTE

The following IKE and ESP proposals are supported:

- AES128-SHA1-MODP2048
- AES256-SHA384-ECP384

IKE encryption proposals should be greater than or equal to ESP encryption proposal. RuckusGRE over IPsec supports IKEv2 authentication by X.509 certificate only.

2. Follow the steps listed in "Creating a Ruckus GRE Profile" of the *SmartZone Administrator Guide* for this release to create a Ruckus GRE profile.

## NOTE

For **Tunnel mode**, select RGRE.

Set **Tunnel Encryption** to Disable.

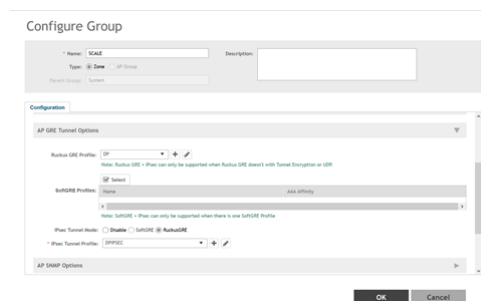
3. Create an AP zone with the appropriate Ruckus GRE and IPsec profiles. Go to **Access Points**.

## NOTE

RuckusGRE over IPsec is supported in transport mode only.

4. Select the FIPS zone and click the + icon to configure the AP GRE Tunnel Options from the **Configuration** tab. Refer to "Creating an AP Zone" of the *SmartZone Administrator Guide* for this release.

**FIGURE 136** AP GRE Tunnel Configurations



5. Go to **Wireless LAN**.
6. Select the zone. The **Creating WLAN Configuration** page displays.
7. 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.



# 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	authReauth	This event occurs once the user is blocked and waits for specified amount of time before getting login prompt
99008	auth8021xClient	This event occurs when receiving data frame before client is authorized
99009	fwManualInitiation	This event occurs when there is manual firmware update
99010	apMGMNTTSFData	This event occurs when there is all management activities of TSF data initiated/started/executed
99012	apSelfTests	This event occurs when all self-tests are passed for fips_sku builds
99013	fwInitiationUpdate	This event occurs when there is firmware update
99014	disContiChan	This event occurs when AP syncs its time with SZ
99015	apLocalSessionTimeout	This event occurs when local AP session terminates due to session timeout
99016	apRemoteSessionTimeout	This event occurs when remote AP session terminates due to session timeout
99017	apSessionExit	This event occurs on user-initiated termination of an interactive AP session
99018	sshInitiation	This event occurs when the SSH session started with successful authentication
99019	sshTermination	This event occurs when there is exit from an established SSH session
99020	sshFailure	This event occurs when there is SSH session initiation with failed authentication
99021	tlsInitiation	This event occurs when there is a successful login through AP web-GUI or AP establishes a trusted TLS connection
99022	tlsTermination	This event occurs when there is logout from AP web-GUI session or AP gracefully terminates a trusted TLS connection
99023	tlsFailure	This event occurs whenever there is a failed login through AP web-GUI or AP fails to establish a trusted TLS connection
99024	ipsecInitiation	This event occurs when there is an IPsec session initiation
99025	ipsecTermination	This event occurs when there is an IPsec session terminated or exited
99026	ipsecFailure	This event occurs when there is IPsec session attempt failure

The following table lists the auditable events in the data plane (DP) for Common Criteria (CC).

**TABLE 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>vdp_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
99213	dpUserLogin	This event occurs whenever an administrator login is successful
99214	dpUserLoginFailed	This event occurs whenever an administrator login fails
	dpUserLogout	This event occurs whenever there is a termination of an interactive session
99215	dpAccountLocked	This event occurs whenever the maximum number of unsuccessful user authentications has been exceeded with subsequent actions taken and restoration of the account
99220	dpSessionIdleUpdated	This event occurs whenever a remote session is terminated by the session locking mechanism
99221	dpSessionIdleTerminated	This event occurs whenever a remote session is terminated by the session locking mechanism
99230	dpSshTunnFailed	This event occurs whenever there is initiation and termination of trusted path and subsequent failure of the trusted path functions
99231	dpHttpsConnFailed	This event occurs whenever there is initiation and termination of trusted path and subsequent failure of the trusted path functions
99240	dpIPsecTunnCreateFailed	This event occurs whenever attempts to establish a trusted channel (including IEEE 802.11) fails
99241	dpIPsecTunnInitiate	This event occurs whenever attempts to establish a trusted channel (including IEEE 802.11) fails
99242	dpIPsecTunnTerminated	This event occurs whenever attempts to establish a trusted channel (including IEEE 802.11) fails
99243	dpIPsecSaFailed	This event occurs whenever there is an establishment or termination of an IPsec SA connection
99244	dpIPsecSaUpdated	This event occurs whenever cryptographic keys are generated, imported, changed, or deleted

# Tamper-Evident Seals

- General Information about Tamper-Evident Seals..... 153
- Tamper-Evident Seals on SmartZone 100 Devices..... 153
- Tamper-Evident Seals on SmartZone 300 Devices..... 157
- Tamper-Evident Seals on T610 AP Devices..... 159
- Tamper-Evident Seals on T710 AP Devices..... 159
- Tamper-Evident Seals on R610 AP Devices..... 161
- Tamper-Evident Seals on R710 AP Devices..... 162
- Tamper-Evident Seals on R720 AP Devices..... 164
- Tamper-Evident Seals on E510 AP Devices..... 165

## 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:

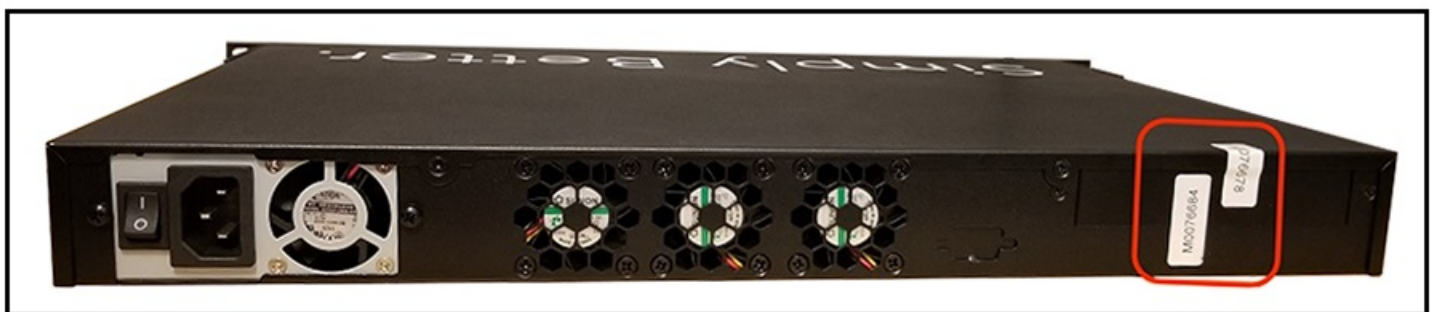
- All surfaces to which the seals will be applied must be clean and dry. Use alcohol to clean the surfaces. Do not use other solvents.
- Do not cut, trim, punch, or otherwise alter the tamper-evident seal.
- Do not use bare fingers to handle the labels. Slowly peel the packing from each seal, taking 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 137** SmartZone 100 Rear Seals



**FIGURE 138** SmartZone 100 Rear Seals (vertical)



**FIGURE 139** SmartZone 100 Side Seal (Horizontal View)



**FIGURE 140** SmartZone 100 Side Seal (Vertical View)



**FIGURE 141** SmartZone 100 Bottom Seals





**FIGURE 142** SmartZone 100 Top View



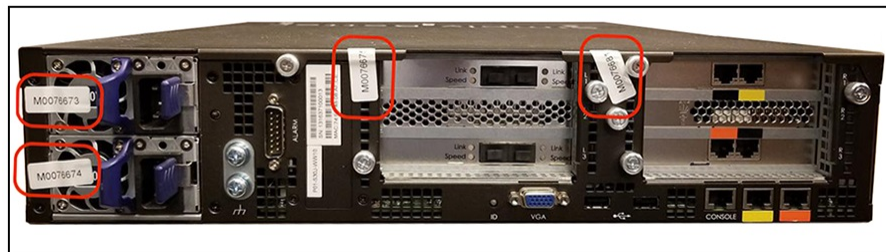
## Tamper-Evident Seals on SmartZone 300 Devices

The following images show locations where FIPS tamper-evident seals must be placed on SmartZone 300 devices.

**FIGURE 143** SmartZone 300 Top Seals



**FIGURE 144** SmartZone 300 Rear Seals



**FIGURE 145** 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 146 T610 AP Side Seals



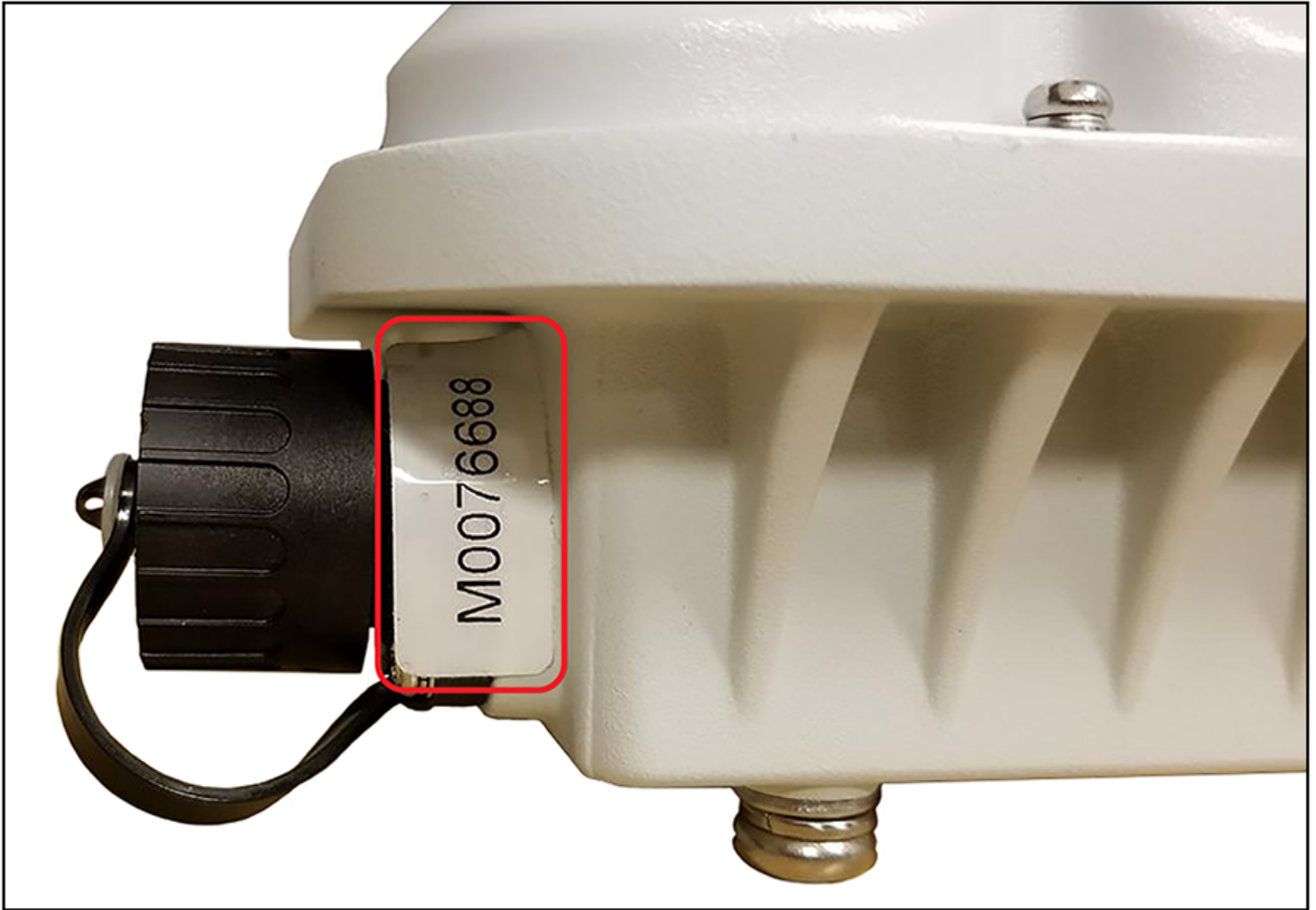
FIGURE 147 T610 AP Side Seal Detail



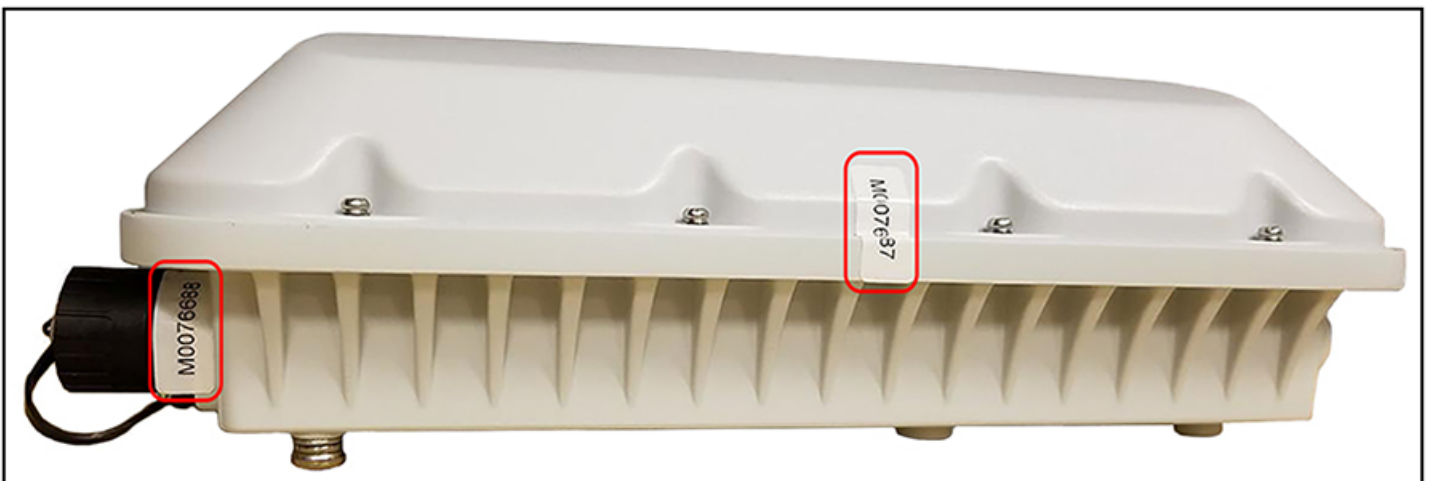
# Tamper-Evident Seals on T710 AP Devices

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

**FIGURE 148** T710 AP Collar Seal



**FIGURE 149** T710 AP Side Seals



**FIGURE 150** 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 151** R610 AP Side Seal





**FIGURE 152 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 153 R710 AP Side Seal**



**FIGURE 154** R710 AP Side Seal (Opposite Side)



**FIGURE 155** R710 AP Seals (Bottom View)



## Tamper-Evident Seals on R720 AP Devices

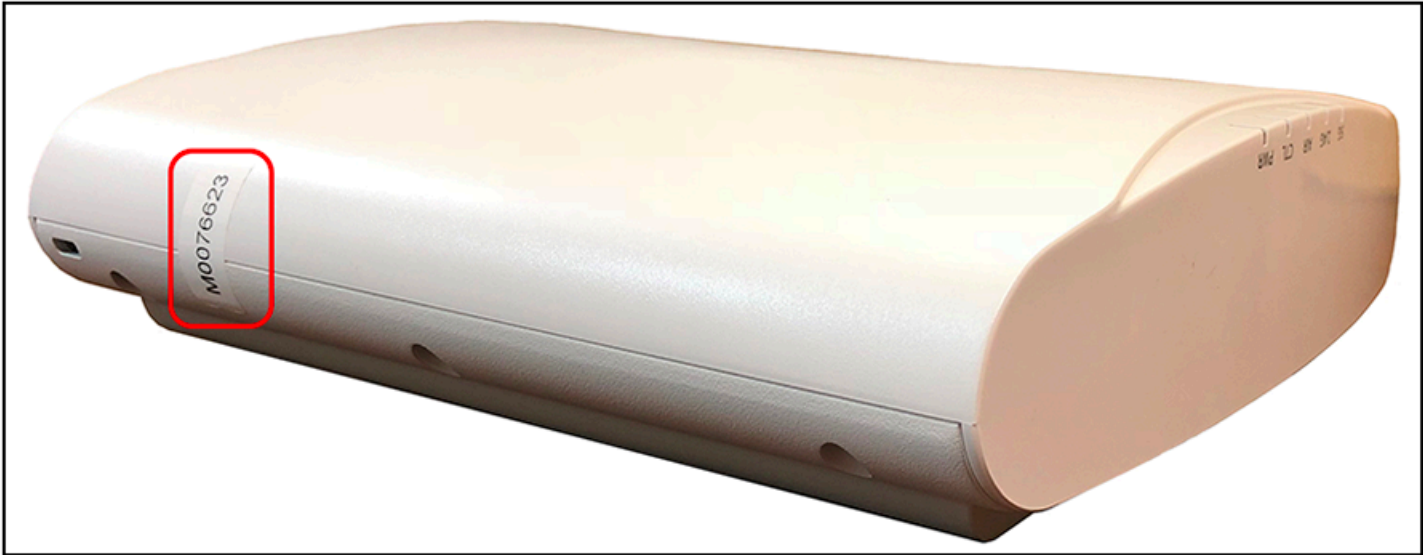
The following images show locations where FIPS tamper-evident seals must be placed on R720 AP devices.



**FIGURE 156 R720 AP Right Side Seal**



**FIGURE 157 R720 AP Left Side Seal**



## Tamper-Evident Seals on E510 AP Devices

The following images show locations where FIPS tamper-evident seals must be placed on E510 AP devices.

**FIGURE 158** E510 AP Seals (Top View)

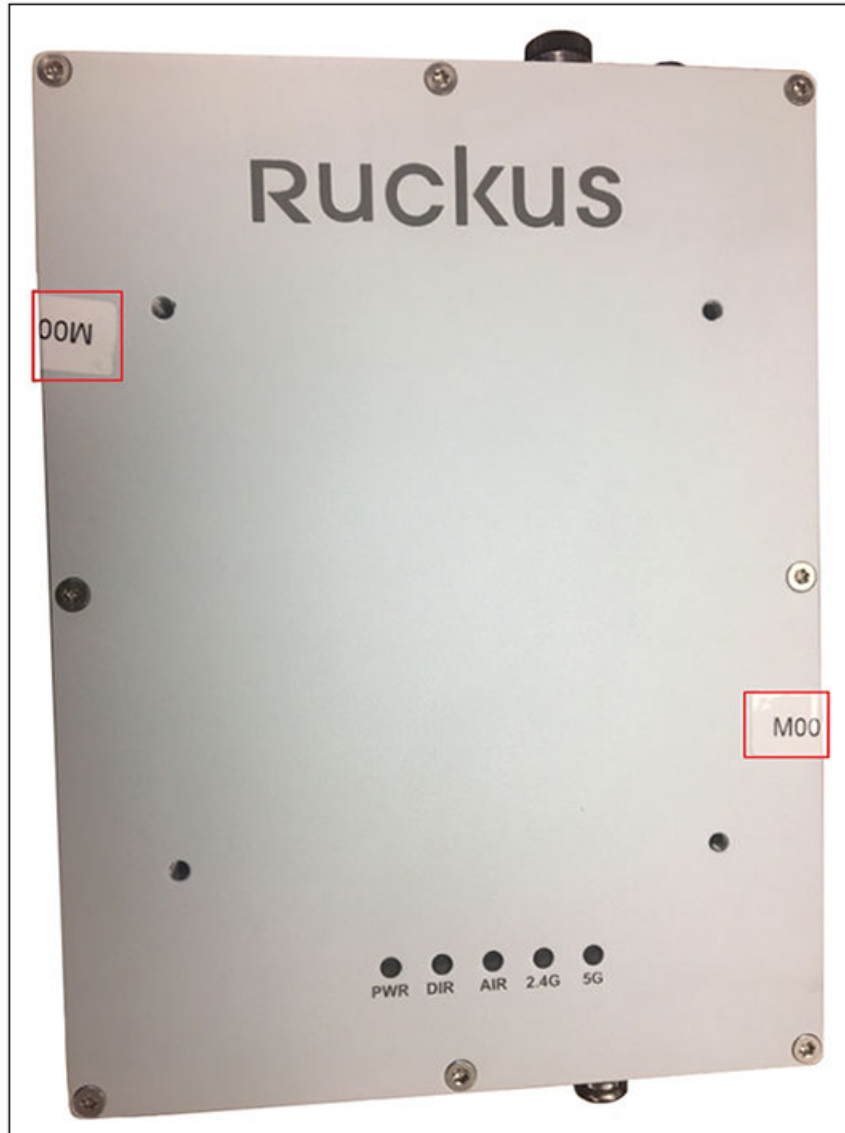


FIGURE 159 E510 AP Seal (Top-Right View)

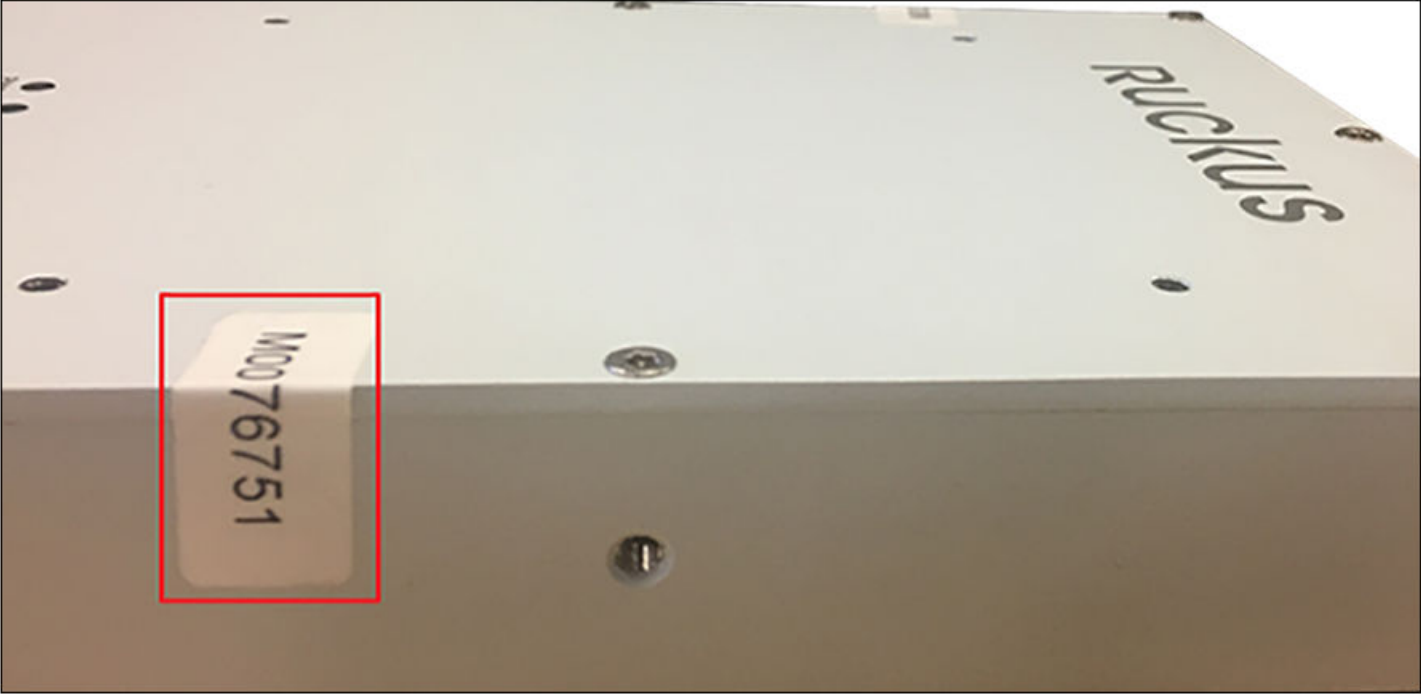


FIGURE 160 E510 AP Seal (Top-Left View)





# Trusted Channels Through TSF

- Trusted Communication Channels..... 169
- Enabling Trusted Channel Using IEEE 802.11-2012 (WPA2) Standards ..... 169
- Enabling Trusted Channel Using IEEE 802.1X and IPsec..... 170

## 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

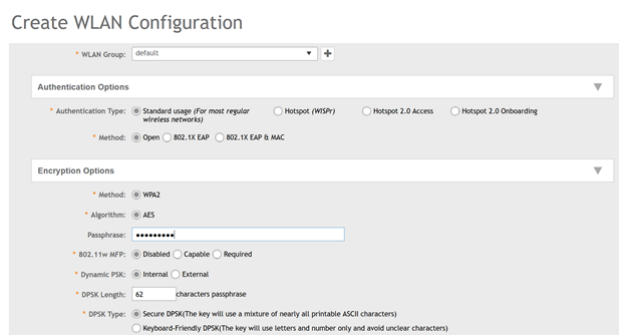
You can enable a secure and trusted channel for communication by using IEEE 802.11-2012 (WPA2) standards.

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. For more information, refer to the *SmartZone Administrator Guide* for this release.

Under Authentication Options, for Method, select Open. Under Encryption Options, for Method, select WPA2.

**FIGURE 161** Configuring the WLAN



## 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 46 to configure a RadSec profile.
2. Follow the steps listed in [Configuring Ruckus GRE and IPsec in the WLAN](#) on page 149 to configure Ruckus GRE and IPsec for a WLAN.

# FIPS-Compliant Products

- AP Controller Matrix.....171
- FIPS-Compliant Product SKUs and Descriptions..... 171

## 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 11 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, controller, and Cloudpath products by SKU.

**TABLE 12 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	TAA T710s XX 11ac dual outdoor AP 4x4:4

## FIPS-Compliant Products

### FIPS-Compliant Product SKUs and Descriptions

**TABLE 12 FIPS-Compliant AP Products (continued)**

SKU	Long Description	Short Description
	Temperature. Includes standard 1-year warranty. For box contents, see Shipping Container Contents.	
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 13 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

**TABLE 14 FIPS-Compliant Cloudpath Products**

SKU	Long description	Short description
LF9-vCLP-WW00	TAA/FIPS - compliant Cloudpath base on-site MSP server software as a virtual appliance, one (1) instance license. No user licenses included. No support required. Server license is valid as long as user subscription licenses are attached to it. Each server supports 20K users. Must use perpetual user license to use this.	TAA Cloudpath MSP server virtual license





© 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)