Cisco Catalyst 9300/9300L/9400/9500/9600 Series Switches

CC Configuration Guide

Version: 0.4
Date: July 17, 2023

Table of Contents

Prepared By:
Cisco Systems, Inc.
170 West Tasman Dr.
San Jose, CA 95134

This document provides Guidance to IT personnel for the TOE, Cisco Catalyst 9300/9300L/9400/9500/9600 Series Switches running IOS-XE 17.9. This Guidance document includes instructions to successfully install the TOE in the Operational Environment, instructions to manage the security of the TSF, and instructions to provide a protected administrative capability.

Revision History

Version	Date	Change
0.1	October 5, 2022	Initial Version
0.2	June 16, 2023	Updates from testing
0.3	June 29, 2023	Updates for check out
0.4	July 17, 2023	Final Updates

1. Introduction

This Operational User Guidance with Preparative Procedures documents the administration of the Cisco Catalyst 9300/9300L/9400/9500/9600 Series Switches running IOS-XE 17.9 TOE, as it was certified under Common Criteria. The TOE may be referenced below as the Cat 9K Switches, TOE, or Switch.

1.1. Audience

This document is written for administrators installing and configuring the TOE. This document assumes that you are familiar with the basic concepts and terminologies used in internetworking, and understand your network topology and the protocols that the devices in your network can use, that you are a trusted individual, and that you are trained to use the operating systems on which you are running your network.

1.2. Purpose

This document is the Operational User Guidance with Preparative Procedures for the Common Criteria evaluation. It was written to highlight the specific TOE configuration and administrator functions and interfaces that are necessary to configure and maintain the TOE in the evaluated configuration. This document is not meant to detail specific actions performed by the administrator but rather is a road map for identifying the appropriate locations within Cisco documentation to get the specific details for configuring and maintaining switch operations. All security relevant commands to manage the TSF data are provided within this documentation within each functional section.

1.3. Document References

This section lists the Cisco Systems documentation that is also a portion of the Common Criteria Configuration Item (CI) List. The documents used are shown below in Table 1. Throughout this document, the guides will be referred to by the "#", such as [1].

Table 1 Cisco Documentation

#	Title	Link
1	Cisco Catalyst 9300 Switches Hardware Installation Guide	https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9300/hardware/install/b_c9300_hig.html
2	Cisco Catalyst 9400 Switches Hardware Installation Guide	https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9400/hardware/install/b_c9400_hig.html
3	Cisco Catalyst 9500 Switches Hardware Installation Guide	https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9500/hardware/install/b_catalyst_9500_hig.html
4	Cisco Catalyst 9600 Switches Hardware Installation Guide	https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9600/hardware/install/b_9600_hig.html
5	Release Notes for Cisco Catalyst 9300 Series Switches	https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9300/software/release/17-2/release_notes/ol-17-2-9300.html
6	Release Notes for Cisco Catalyst 9400 Series Switches	https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9400/software/release/17-8/release_notes/ol-17-8-9400.html
7	Release Notes for Cisco Catalyst 9500 Series Switches	https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9500/software/release/17-9/release_notes/ol-17-9-9500.html

#	Title	Link
8	Release Notes for Cisco Catalyst 9600 Series Switches	https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9600/software/release/17-6/release_notes/ol-17-6-9600.html
9	Software Configuration Guide, Cisco IOS-XE Cupertino 17.9.x (Catalyst 9300 Switches)	https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9300/software/release/17-9/configuration_guide/b-179-9300-cg.html
10	Software Configuration Guide, Cisco IOS-XE Cupertino 17.9.x (Catalyst 9400 Switches)	https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9400/software/release/17-9/configuration_guide/b-179-9400-cg.html
11	Software Configuration Guide, Cisco IOS-XE Cupertino 17.9.x (Catalyst 9500 Switches)	https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9500/software/release/17-9/configuration_guide/b-179-9500-cg.html
12	Software Configuration Guide, Cisco IOS-XE Cupertino 17.9.x (Catalyst 9600 Switches)	https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9600/software/release/17-9/configuration_guide/b-179-9600-cg.html
13	Security Configuration Guide, Cisco IOS XE Cupertino 17.9.x (Catalyst 9300 Switches)	https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9300/software/release/17-9/configuration_guide/sec/b_179_sec_9300_cg.html
14	Security Configuration Guide, Cisco IOS XE Cupertino 17.9.x (Catalyst 9400 Switches)	https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9400/software/release/17-9/configuration_guide/sec/b_179_sec_9400_cg/troubleshooting_for_security.html
15	Security Configuration Guide, Cisco IOS XE Cupertino 17.9.x (Catalyst 9500 Switches)	https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9500/software/release/17-9/configuration_guide/sec/b_179_sec_9500_cg/troubleshooting_for_security.html
16	Security Configuration Guide, Cisco IOS XE Cupertino 17.9.x (Catalyst 9600 Switches)	https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9600/software/release/17-9/configuration_guide/sec/b_179_sec_9600_cg.html
17	Command Reference, Cisco IOS XE Cupertino 17.9.x (Catalyst 9300 Switches)	https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9300/software/release/17-9/command_reference/b_179_9300_cr.html
18	Command Reference, Cisco IOS XE Cupertino 17.9.x (Catalyst 9400 Switches)	https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9400/software/release/17-9/command_reference/b_179_9400_cr.html
19	Command Reference, Cisco IOS XE Cupertino 17.9.x (Catalyst 9500 Switches)	https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9500/software/release/17-9/command_reference/b_179_9500_cr.html
20	Cisco IOS Configuration Fundamentals Command Reference	https://www.cisco.com/c/en/us/td/docs/ios/fundamentals/command/reference/cf_book.html
21	System Message Guide for Cisco IOS XE Cupertino 17.9.x	https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/17_xe/syslogs/17-9-x/b-system-message-guide-17-9-x.html

#	Title	Link
22	Troubleshoot MACSEC on Catalyst 9000	https://www.cisco.com/c/en/us/support/docs/switches/catalyst-9300-series-switches/216849-troubleshoot-macsec-on-catalyst-9000.html

1.4. TOE Overview

The TOE is the Cisco Catalyst 9300/9300L/9400/9500/9600 Series Switches running IOS-XE 17.9. The TOE is a purpose-built, switching and routing platform with Open System Interconnection (OSI) Layer2 and Layer3 traffic filtering capabilities. The TOE also supports Media Access Control Security (MACsec) encryption for switch-to-switch (inter-network device) security.

1.5. Operational Environment

The TOE requires the following IT Environment Components when the TOE is configured in its evaluated configuration:

Table 2. Operational Environment Components

Component	Usage/Purpose Description
Audit (syslog) Server	This includes any syslog server to which the TOE transmits syslog messages over a secure Internet Protocol security (IPsec) trusted channel.
Local Console	This includes any IT Environment Console that is directly connected to the TOE via the Serial Console Port and is used by the TOE administrator to support TOE administration. This interface is accessible and available locally even if the network were to go down and is not subject to administrator lockout.
Management Workstation with Secure Shell v2 (SSHv2) client	This includes any IT Environment Management workstation that is used by the TOE administrator to support TOE administration using SSHv2 protected channels. Any SSH client that supports SSHv2 may be used.
Remote Authentication Dial-In User Service (RADIUS) Authentication, Authorization, and Accounting (AAA) Server	This includes any IT environment RADIUS AAA server that provides authentication services to TOE administrators over a secure IPsec trusted channel either directly or connected to a TOE Peer that also supports a secure IPsec trusted channel.
Media Access Control security (MACsec) Peer	This includes any MACsec peer with which the TOE participates in MACsec communications. MACsec Peer may be any device that supports MACsec communications.
Certification Authority (CA)	This includes any IT Environment CA on the TOE network. The CA can be used to provide the TOE with a valid certificate during certificate enrolment as well as validating a certificate.

1.6. Excluded Functionality

The functionality listed below is not included in the evaluated configuration.

Table 3. Excluded Functionality and Rationale

Function Excluded	Rationale
Non-FIPS 140-2 mode of operation	The TOE includes FIPS mode of operation. The FIPS modes allows the TOE to use only approved cryptography. FIPS mode of operation must be enabled in order for the TOE to be operating in its evaluated configuration.

Additionally, the TOE includes a number of functions where there are no Security Functional Requirements that apply from the collaborative Protection Profile for Network Devices v2.2 or the MACsec Ethernet Encryption Extended Package v1.2. The excluded functionality does not affect the TOE's conformance to the claimed Protection Profiles.

Warning: Use of other cryptographic engines beyond what is required for the TOE was not evaluated nor tested during the CC evaluation.

2. TOE Acceptance

The administrator should perform the following actions to ensure the TOE is correct and that it has not been tampered with during delivery.

1. Before unpacking the TOE, inspect the physical packaging the equipment was delivered in. Verify that the external cardboard packing is printed with the Cisco Systems logo and motifs. If it is not, contact the supplier of the equipment (Cisco Systems or an authorized Cisco distributor/partner).

2. Verify that the packaging has not obviously been opened and resealed by examining the tape that seals the package. If the package appears to have been resealed, contact the supplier of the equipment (Cisco Systems or an authorized Cisco distributor/partner).

3. Verify that the box has a white tamper-resistant, tamper-evident Cisco Systems bar coded label applied to the external cardboard box. If it does not, contact the supplier of the equipment (Cisco Systems or an authorized Cisco distributor/partner). This label will include the Cisco product number, serial number, and other information regarding the contents of the box.

4. Note the serial number of the TOE on the shipping documentation. The serial number displayed on the white label affixed to the outer box will be that of the device. Verify the serial number on the shipping documentation matches the serial number on the separately mailed invoice for the equipment. If it does not, contact the supplier of the equipment (Cisco Systems or an authorized Cisco distributor/partner).

5. Verify that the box was indeed shipped from the expected supplier of the equipment (Cisco Systems or an authorized Cisco distributor/partner). This can be done by verifying with the supplier that they shipped the box with the courier company that delivered the box and that the consignment note number for the shipment matches that used on the delivery. Also verify that the serial numbers of the items shipped match the serial numbers of the items delivered. This verification should be performed by some mechanism that was not involved in the actual equipment delivery, for example, phone/FAX or other online tracking service.

6. Once the TOE is unpacked, inspect the unit. Verify that the serial number displayed on the unit itself matches the serial number on the shipping documentation and the invoice. If it does not, contact the supplier of the equipment (Cisco Systems or an authorized Cisco distributor/partner).

3. Procedures and Operational Guidance for IT Environment

To operate in its evaluated configuration, the TOE requires the operational components listed in Table 2. Below are additional details needed to configure the Syslog and RADIUS Servers:

- Syslog Server. Any syslog server that can be accessed over IPsec may be used. Install the syslog server per installation instructions provided with the syslog server software. Configure the host operating system to restrict access to syslog data to authorized personnel only. Configure the system to accept inbound syslog over IPsec from the TOE.
- RADIUS Server. A RADIUS server that can be accessed over IPsec may be used. Install the RADIUS server per installation instructions provided with the RADIUS server software. Configure the host operating system to restrict access to RADIUS data to authorized personnel only. Configure the system to accept inbound RADIUS over IPsec from the TOE.

4. Preparative Procedures and Operational Guidance for the TOE

4.1.Switch — Power Up

Warning: IMPORTANT SAFETY INSTRUCTIONS

Blank faceplates and cover panels serve three important functions: they prevent exposure to hazardous voltages and currents inside the chassis; they contain electromagnetic interference (EMI) that might disrupt other equipment; and they direct the flow of cooling air through the chassis. Do not operate the system unless all cards, faceplates, front covers, and rear covers are in place.

1. If you are powering up the switch, move the power switch to the ON position. Listen for the fans; you should immediately hear them operating. Ensure that the power supply LED OK is green and the FAIL LED is not illuminated. The front-panel indicator LEDs provide power, activity, and status information useful during bootup. For more detailed information about the LEDs, see the LEDs section in the Hardware Installation Guide.
2. Observe the initialization process. When the system boot is complete (the process takes a few seconds), the Switch begins to initialize.

```
Loading from ROMMON with a System Image in Bootflash
```

3. When initialization has completed, the following will be displayed:

```
Press RETURN to get started!
```

4.2. Switch — Initial Configuration

1. The administrator will be prompted to enter the initial configuration dialog. Enter no and confirm you would like to terminate autoinstall. The CC Configuration will use manual steps to provide the initial configuration.

```
Would you like to enter the initial configuration dialog? [yes/no]: no

Would you like to terminate autoinstall? [yes]:yes

Press RETURN to get started!
```

2. Enter privilege EXEC mode

```
SWITCH> enable
```

3. Enter configure terminal

```
SWITCH# configure terminal
```

4. Configure a hostname

```
SWITCH(config)# hostname mySWITCH
```

5. Configure the Enable Secret Password using Type 9

```
SWITCH(config)# enable algorithm-type scrypt secret <the unencrypted (cleartext)
'enable' secret>
```

Note: Compose a password with a length between 8 and 16 using any combination of upper and lower case letters, numbers, and the following special characters: "!", "@", "#", "$", "%", "^", "&", "*", "(", ")

6. Provide an initial configuration for an Out-of-Band Management Interface. For example:

```
SWITCH(config)# interface GigabitEthernet0/0

SWITCH(config-if)# vrf forwarding Mgmt-vrf

SWITCH(config-if)# ip address <IP address> <mask>

SWITCH(config-if)# no shutdown

SWITCH(config-if)# exit
```

7. Configure a default route to reach the Switch.

```
SWITCH(config)# ip route <prefix> <mask> <ip-address>
```

8. Configure the console to require username and password authentication

```
SWITCH(config)#line console 0

SWITCH(config-line)# login authentication default
```

9. Save the initial configuration to nvram by executing "wr mem" or "copy system:running-config nvram:startup-config" command.

Note: Instructions for adding additional administrative users are specified in 4.2.14 below.

4.2.1. Configure Time and Date

Perform the following to configure time and date.

1. Enter enable and then enter configuration mode.

```
SWITCH> enable

SWITCH# configure terminal
```

2. Configure the time zone. The zone argument is the name of the time zone (typically a standard acronym). The hours-offset argument is the number of hours the time zone is different from UTC. The minutes-offset argument is the number of minutes the time zone is different from UTC. For example clock timezone EST -5

```
SWITCH(config)# clock timezone zone-hours-offset [minutes-offset]
```

3. [Optional] Configure daylight savings time in areas where it starts and ends on a particular day of the week each year. The offset argument is used to indicate the number of minutes to add to the clock during summer time. For example clock summer-time PST recurring 1 monday january 12:12 4 Tuesday december 12:12 120

```
SWITCH(config)# clock summer-time zone recurring [week day month hh : mm week day
month hh : mm [offset]]
```

4. [Optional] Configure a specific summer time start and end date. The offset argument is used to indicate the number of minutes to add to the clock during summer time. For example clock summer-time PST date 1 january 1999 12:12 4 december 2001 12:12 120

```
SWITCH(config)# clock summer-time zone date month year hh:mm date month year hh :
mm [offset]1:5
```

5. Configure Calendar time as authoritative.

```
SWITCH(config)# clock calendar-valid
```

6. Return to privileged EXEC mode.

```
SWITCH(config)# end
```

7. Set the clock using the clock set command. For example clock set 12:12:12 1 january 2011

```
SWITCH# clock set hh : mm : ss date month year
```

4.2.2. Enable Configuration Change Notification and Logging

The Configuration Change Notification and Logging feature tracks changes made to the Cisco software running configuration. Perform the following steps to ensure all required audit events are logged.

1. Ensure logging is enabled

```
SWITCH(config)#logging on
```

2. Enter archive config mode

```
SWITCH(config)# archive
```

3. Enter logging config sub-mode

```
SWITCH(config-archive)# log config
```

4. Enable the config logger

```
SWITCH(config-archive-log-cfg)# logging enable
```

5. Suppress password when displaying logged commands

```
SWITCH(config-archive-log-cfg)# hidekeys
```

6. Enter the number of entries to be retained. The range is from 1 to 1000; the default is 100

```
SWITCH(config-archive-log-cfg)# logging size <1-1000>
```

7. Enable sending of logged commands to remote syslog server

```
SWITCH(config-archive-log-cfg)# notify syslog
```

8. Exit configuration mode and return to privileged EXEC mode

```
SWITCH(config-archive-log-cfg)# end
```

4.2.3. Configure Embedded Event Manager (EEM)

To capture audit events for Common Criteria the following Cisco Embedded Event Manager script should be used. Enter it at the CLI as follows:

```
SWITCH# config t
```

```
SWITCH#(config)# event manager applet cli_log

SWITCH#(config-applet)# event cli pattern "." mode exec enter

SWITCH#(config-applet)# action 0010 info type routername

SWITCH#(config-applet)# action 0020 syslog msg "User:$_cli_username via Port:$_cli_tty
Executed[$_cli_msg]"

SWITCH#(config-applet)# action 0030 set _exit_status "1"

SWITCH#(config)#end
```

4.2.4. Configure Local Logging Buffer Size

Configure the size of the local logging buffer. The local logging buffer size can be configured in a range of <4096-2147483647> bytes. **Note:** It is recommended to not make the buffer size too large because the TOE could run out of memory for other tasks. It is recommended to set it to at least 150000000

```
SWITCH(config)# logging buffer 150000000
```

If the local storage space for audit data is full the TOE will overwrite the oldest audit record to make room for the new audit record.

4.2.5. Generate Logs on Failed Login Attempts

To generate logs for failed login attempts enter

```
SWITCH(config)# login on-failure log
```

4.2.6. Include Date on Audit Records

To include the year with the time stamp on all audit records in the message log enter:

```
SWITCH(config)# service timestamps log datetime year
```

4.2.7. Generate Logs on Successful Login Attempts

To generate logs for successful login attempts enter

```
SWITCH(config)# login on-success log
```

4.2.8. Set Syslog Server Logging Level

Set syslog server logging level to debug

```
SWITCH(config)# logging trap debugging
```

4.2.9. Enable Debug Logging

To generate all required audit events, the following debug commands must be entered each time the TOE is restarted:

```
SWITCH# debug crypto pki validation

SWITCH# debug crypto pki transaction

SWITCH# debug crypto pki api
```

```
SWITCH# debug crypto pki messages

SWITCH# debug crypto isakmp

SWITCH# debug crypto ipsec

SWITCH# debug crypto ikev2

SWITCH# debug crypto engine
```

Warning: **If the Administrator restarts the TOE the debug commands above must be re-entered.**

4.2.10. Configure Required Logging

To generate additional required audit events, the following commands must be configured:

```
SWITCH(config)# ip ssh logging events

SWITCH(config)# crypto logging session

SWITCH(config)# crypto logging ikev2
```

4.2.11. Configure Local Authentication

1. To enable the authentication, authorization, and accounting (AAA) access control model, issue the aaa new-model command in global configuration mode.

```
SWITCH(config)# aaa new-model
```

2. To set the default authentication at login to use local authentication use the aaa authentication login command

```
SWITCH(config)# aaa authentication login default local
```

3. To set the default authorization method to use local credentials use the aaa authorization exec command

```
SWITCH(config)# aaa authorization exec default local
```

4.2.12. Configure Authentication Failure

To block brute-force attack attempts, the Controller needs to be configured for authentication failure. The administrator needs to define the maximum number of failed login attempts within a time period. In addition, the administrator needs to define the time period to ban an offending account.

1. Specify the value for maximum number of failed attempts within a time period (seconds), and the time period (seconds) to ban an offending account.

```
SWITCH(config)# aaa authentication rejected <1-25> in <1-65535> ban <1-65535>
```

For example, to block accounts for 10 minutes after 5 failed login attempts within one 1 hour, enter:

```
aaa authentication rejected 5 in 3600 ban 600
```

2. Exit configuration mode and return to privileged EXEC mode

```
SWITCH(config)# end
```

4.2.13. Define Password Policy

Administrators must define a "aaa common-criteria policy" and apply the policy to each local account. This ensures password changes will prompt for your old password before allowing a new password and will also ensure passwords contain a minimum of 8 characters.

1. Create the AAA security password policy and enter common criteria configuration policy mode.

```
SWITCH(config)# aaa common-criteria policy <policy name>
```

2. Set the minimum length for passwords. The TOE supports a minimum length from 1 to 127 characters. It's recommended to configure a minimum length between 8 and 16 characters:

```
SWITCH(config-cc-policy)# min-length <8-16>
```

3. Set a password lifetime appropriate for your organization. For example, to set a password lifetime of 90 days enter:

```
SWITCH(config-cc-policy)# lifetime day 90
```

   When the password expires the user will prompted to perform a password change.

4. Type exit to return to the main configuration mode.

```
SWITCH(config-cc-policy)# exit
```

5. To verify the Common Criteria password policy enter

```
SWITCH(config)# do show aaa common-criteria policy <policy name>
```

4.2.14. Add Administrator Account

The administrator should create and use a new account that has the Common Criteria Password Policy applied. To add an administrative account use the username command in configuration mode. You will need to specify the Common Criteria Password Policy.

```
SWITCH(config)# username <user> privilege 15 common-criteria-policy <policy name> algorithm-type scrypt secret password <the unencrypted (cleartext) password for the user>
```

Passwords may be composed of any combination of upper- and lower-case letters, numbers, and the following special characters:

Table 4. Password Special Characters

Special Character	Name
!	Exclamation
@	At sign
#	Number sign (hash)
$	Dollar sign
%	Percent
^	Caret
&	Ampersand
*	Asterisk

(	Left parenthesis
)	Right parenthesis
	Space
;	Semicolon
:	Colon
"	Double Quote
‘	Single Quote
|	Vertical Bar
+	Plus
-	Minus
=	Equal Sign
.	Period
,	Comma
/	Slash
\	Backslash
<	Less Than
>	Greater Than
_	Underscore
`	Grave accent (backtick)
~	Tilde
{	Left Brace
}	Right Brace

4.2.15. Session Termination

All sessions at the local console port must terminate after an Administrator specified time interval of session inactivity has elapsed. Use the steps below to configure the time interval.

1. Enter the line configuration mode for console.

```
SWITCH(config)# line console 0
```

2. Specify the timeout value in minutes. The range is from 0 to 35791.

```
SWITCH(config-line)# exec-timeout <time in minutes>
```

4.2.16. Access Banner

The administrator should configure an initial banner that describes restrictions of use, legal agreements, or any other appropriate information to which users consent by accessing the Switch. The banner will display on the CLI and SSH interface prior to allowing any administrative access.

To configure an access banner, follow the steps below

1. In privilege EXEC mode, enter configure terminal

   ```
   SWITCH# config terminal
   ```

2. Enter the banner text using 'banner login delimiter message delimiter' format. Do not use " or % as a delimiting character. White space characters will not work.

   ```
   SWITCH(config)# banner login z <message text> z
   ```

   Message text. The text is alphanumeric, case sensitive, and can contain special characters. It cannot contain the delimiter character you have chosen. The text has a maximum length of 80 characters and a maximum of 40 lines.

   To clear a login banner use "no login banner"

4.2.17. Verify TOE Software

The TOE ships with the correct software image pre-installed however this may not be the CC validated version. Follow the steps below to verify if you have the CC validated version.

1. Enter show version and verify the version is 17.09

   ```
   SWITCH# show version | include Software
   ```

2. If the version is not 17.09 you will need to obtain the 17.09 software image. Navigate to Cisco Software Central at https://software.cisco.com/. Use your Cisco Care Online (CCO) or SMART account and download the 17.09 image.

Table 5. Evaluated Software Images

Platform	Image
Cisco Catalyst 9300/9300L,9400, 9500, 9600	cat9k_iosxe.17.09.02.SPA

3. To update the software, refer to section 5.8 of the this document.

4.2.18. SSH Remote Administration Protocol

The TOE provides remote administration using SSH. The steps below provide instructions to configure SSH Server for the CC evaluated configuration. For additional information on SSH refer to the "Configuring Secure Shell" Chapter of [**13, 14, 15, or 16**] depending on your TOE model.

1. In privileged EXEC mode, enter configure terminal

   ```
   SWITCH# configure terminal
   ```

2. Specify the host domain name applicable to the Switch

   ```
   SWITCH(config)# ip domain name cisco.com
   ```

3. Generate a crypto key for SSH. Assign a label such as SSH-KEY

```
SWITCH(config)# crypto key generate rsa label SSH-KEY modulus [2048 | 3072]
```

4. Assign the key pair to SSH

```
SWITCH(config)# ip ssh rsa keypair-name SSH-KEY
```

5. Enable SSHv2. This will also deny use of SSHv1

```
SWITCH(config)# ip ssh version 2
```

6. Configure the SSH Server Key Exchange

```
SWITCH(config)# ip ssh server algorithm kex diffie-hellman-group14-sha1
```

7. Specify the allowed encryption algorithms and the order they are to be supported

```
SWITCH(config)# ip ssh server algorithm encryption aes256-cbc aes128-cbc
```

8. Specify the allowed Message Authentication Code (MAC) algorithms and the order they are to be supported

```
SWITCH(config)# ip ssh server algorithm mac hmac-sha2-512 hmac-sha2-256
```

9. The administrator needs to configure the Switch for SSH public key authentication. This is necessary to avoid a potential situation where password failures by remote Administrators lead to no Administrator access for a temporary period of time. During the defined lockout period, the Switch provides the ability for the Administrator account to login remotely using SSH public key authentication.

   Before proceeding, please have the SSH public key ready for use. The public key is generated from your SSH client on the Management workstation.

   a. Configure Public Key Algorithms for SSH public-key based authentication

```
SWITCH(config)# ip ssh server algorithm publickey ssh-rsa
```

   b. Configure Host Key Algorithms for SSH public-key based authentication

```
SWITCH(config)# ip ssh server algorithm hostkey rsa-sha2-256 rsa-sha2-512
```

   c. Enter public-key configuration mode

```
SWITCH(config)# ip ssh pubkey-chain
```

   d. Specify the admin user account to configure for SSH public key authentication

```
SWITCH(conf-ssh-pubkey-user)# username admin
```

   e. Enter public-key data configuration mode

```
SWITCH(conf-ssh-pubkey-user)# key-string
```

   f. Paste the data portion of the public key generated from the SSH client. **Note:** If necessary you may split the key into multiple lines.

```
SWITCH(conf-ssh-pubkey-data)# <paste your public key>
```

   g. Return to configuration mode by entering exit 3 times:

```
SWITCH(conf-ssh-pubkey-data)# exit

SWITCH(conf-ssh-pubkey-user)# exit

SWITCH(conf-ssh-pubkey)# exit
```

10. SSH connections with the same session keys cannot be used longer than one hour, and with no more than one gigabyte of transmitted data. In the steps below configure a time-based and volume-based (in kilobytes) rekey values. **Note:** Values can be configured to be lower if desired. The minimum time value is 10 minutes. The minimum volume value is 100 kilobytes.

    Note: To ensure rekeying is performed before one hour expires, the Administrator should specify a rekey time of 59 minutes:

    ```
    SWITCH(config)# ip ssh rekey time 59

    SWITCH(config)# ip ssh rekey volume 1000000
    ```

11. Display SSH configuration information

    ```
    SWITCH(config)# do show ip ssh
    ```

12. Confirm the SSH configuration includes the following settings. Your choice for encryption and MAC algorithms may be a subset of this list.

    - SSH Enabled - version 2.0
    - Authentication methods: publickey or password
    - Authentication Publickey Algorithms: ssh-rsa
    - Hostkey Algorithms: rsa-sha2-256, rsa-sha2-512
    - Encryption Algorithms: aes128-cbc, aes256-cbc
    - MAC Algorithms: hmac-sha2-512, hmac-sha2-256
    - KEX Algorithms: diffie-hellman-group14-sha1

13. Enter line configuration mode to configure the virtual terminal line settings 0 4

    ```
    SWITCH(config)# line vty 0 4
    ```

14. Specify vty lines 0-4 to use only SSH

    ```
    SWITCH(config-line)# transport input ssh
    ```

15. Specify a timeout value for vty lines 0-4

    ```
    SWITCH(config-line)# exec-timeout <time in minutes>
    ```

16. Type Exit

    ```
    SWITCH(config-line)# exit
    ```

17. Enter line configuration mode to configure the virtual terminal lines 5-15

    ```
    SWITCH(config)# line vty 5 15
    ```

18. Specify the vty lines to use only SSH

    ```
    SWITCH(config-line)# transport input ssh
    ```

19. Specify a timeout value for vty lines 5-15

    ```
    SWITCH(config-line)# exec-timeout <time in minutes>
    ```

20. Exit configuration mode and return to privileged EXEC mode

```
SWITCH(config)# end
```

21. Enter “show running-config” and verify all vty lines include “transport input SSH” and have a configured timeout value

```
SWITCH# show running-config
```

Additional information on SSH is located in the “Configuring Secure Shell” Chapter of [**13, 14, 15, or 16**] depending on your TOE model.

Before proceeding to the next section, logout out of your local console CLI session by entering either “exit or “logout”

The remaining preparative procedures can be performed using the local console or remotely over SSH.

4.2.19. Disable Unused Protocols

The following remote management protocols (HTTP, HTTPS, SNMP) were not tested in the evaluated configuration and must be disabled:

```
SWITCH(config)# no ip http server

SWITCH(config)# no ip http secure-server

SWITCH(config)# no snmp-server
```

4.2.20. IPsec

IPsec is a framework of open standards developed by the IETF. It provides security for the transmission of sensitive information over unprotected networks such as the Internet. IPsec acts at the network layer, protecting and authenticating IP packets between participating IPsec device(s). In the CC evaluated configuration IPsec is required to provide protected transmission of audit events to remote syslog server. This protection can be provided in one of two methods:

1. With a syslog and RADIUS server operating as an IPsec peer of the TOE and the records tunneled over that connection.
2. With a syslog and RADIUS server is not directly co-located with the TOE but is adjacent to an IPsec peer within a trusted facility, and the records are tunneled over the public network.

The Administrator defines which packets are considered sensitive and should be sent through these secure tunnels and specifies the parameters that should be used to protect these sensitive packets by specifying the characteristics of these tunnels. When the IPsec recognizes a sensitive packet, the Switch sets up the appropriate secure tunnel and sends the packet through the tunnel to the remote peer.

More accurately, these tunnels are sets of security associations (SAs) that are established between two IPsec peers. The SAs define the protocols and algorithms to be applied to sensitive packets and specify the keying material to be used by the two peers. SAs are unidirectional and are established per the ESP security protocol.

The administrator defines the traffic that needs to be protected between two IPsec peers by configuring access lists and applying these access lists to interfaces using crypto map sets. Therefore, traffic may be selected on the basis of the source and destination address, and optionally the Layer 4 protocol and port. (The access lists used for IPsec are only used to determine the traffic that needs to be protected by IPsec, not the traffic that should be blocked or permitted through the interface. Separate access lists define blocking and permitting at the interface.)

A crypto map set can contain multiple entries, each with a different access list. The crypto map entries are searched in a sequence and the Switch attempts to match the packet to the access list specified in that entry. When a packet matches a permit entry in a particular access list, and the corresponding crypto map entry is tagged, IPsec is triggered. If there is no SA that IPsec can use to protect this traffic to the peer, IPsec uses IKE to negotiate with the remote peer to set up the necessary IPsec SAs on behalf of the data flow. The negotiation uses information specified in the crypto map entry as well as the data flow information from the specific access list entry.

Once established, the set of SAs (outbound to the peer) is then applied to the triggering packet and to subsequent applicable packets as those packets exit the Switch. "Applicable" packets are packets that match the same access list criteria that the original packet

matched. For example, all applicable packets could be encrypted before being forwarded to the remote peer. The corresponding inbound SAs are used when processing the incoming traffic from that peer.

Access lists associated with IPsec crypto map entries also represent the traffic that the Switch needs protected by IPsec. Inbound traffic is processed against crypto map entries. if an unprotected packet matches a permit entry in a particular access list associated with an IPsec crypto map entry, that packet is dropped because it was not sent as an IPsec-protected packet.

Crypto map entries also include transform sets. A transform set is an acceptable combination of security protocols, algorithms, and other settings that can be applied to IPsec-protected traffic. During the IPsec SA negotiation, the peers agree to use a particular transform set when protecting a particular data flow.

Note: The evaluated configuration allows authentication of the peer using pre-shared key or X.509 certificates. If you are only using pre-shared keys and not X.509 certificates you can skip the next two sections and proceed directly to the IKE section.

4.2.20.1. Generating a Crypto Key Pair for IPsec

1. In privileged EXEC mode, enter configure terminal

```
SWITCH# configure terminal
```

2. The Administrator can choose to generate an elliptic curve or RSA key. Assign a label such as IPSEC-KEY

```
SWITCH(config)# crypto key generate rsa general modulus 2048 label IPSEC-KEY
```

4.2.20.2. Create Trustpoints for IPsec

IPsec must be configured to use X.509v3 certificates supporting a minimum path length of three (root CA -> intermediate CA -> end-entity). Therefore, you will need to create two trustpoints. The section below provides steps to create a root CA and a subordinate CA using CA certificates from your organization's PKI. Before proceeding, please have the root CA and subordinate CA certificates ready for import from your CA administrator.

Note: You will set up the CRL certificate revocation mechanism used to ensure that the certificate of the IPsec peer has not been revoked. If the TOE is unable to obtain a CRL, the TOE will reject the peer's certificate and a "CRL fetch for trustpoint <trustpoint name> failed" message will appear in the message log (refer to section 6 for details on audit). The Administrator will need to enable the remote syslog server and/or remote login authentication as described below in sections 4.2.21.10 and 4.2.21.11, respectively, once the revocation server is back online.

1. Create, configure, and authenticate a root trustpoint for IPsec

```
SWITCH(config)# crypto pki trustpoint <root trustpoint name>

SWITCH(ca-trustpoint)# enrollment terminal pem

SWITCH(ca-trustpoint)# revocation-check none

SWITCH(ca-trustpoint)# chain-validation stop

SWITCH(ca-trustpoint)# crypto pki authenticate <root trustpoint name>
```

   Enter your base 64 encoded root CA certificate. End with a blank line or the word "quit" on a line by itself. When prompted enter yes to accept the CA certificate. The Switch should respond with:

   "Trustpoint CA certificate accepted."

   "% Certificate successfully imported"

2. Create, configure, and authenticate the subordinate trustpoint:

```
SWITCH(config)# crypto pki trustpoint <subordinate trustpoint name>
```

```
SWITCH(ca-trustpoint)# enrollment terminal pem

SWITCH(ca-trustpoint)# revocation-check none

SWITCH(ca-trustpoint)# chain-validation continue <root trustpoint name>

SWITCH(ca-trustpoint)# subject-name C=<two letter country code>, ST=<two letter state
code>, L=<locality>, O=<organization>, OU=<organizational unit>, CN=Switch
```

In the next step you will need to provide the key pair selected and the label

```
SWITCH(ca-trustpoint)# rsakeypair IPSEC-KEY
```

Authenticate the trustpoint

```
SWITCH(ca-trustpoint)# crypto pki authenticate <subordinate trustpoint name>
```

Enter your base 64 encoded subordinate CA certificate. End with a blank line or the word "quit" on a line by itself. When prompted enter yes to accept the CA certificate. The Switch should respond with:

"Trustpoint CA certificate accepted."

"% Certificate successfully imported"

3. Generate a certificate signing request for the Switch

```
SWITCH(config)# crypto pki enroll <subordinate trustpoint name>
```

When prompted to include the router serial number and IP address in the subject name, enter no. When prompted to Display the Certificate Request to terminal, enter yes.

4. Copy the contents of the Certificate Request. Be sure to include:

-----BEGIN CERTIFICATE REQUEST-----

-----END CERTIFICATE REQUEST-----

5. Save the contents in a file and securely distribute it to your PKI administrator for signing by the subordinate CA. Once signed, your PKI administrator will need to provide the certificate in PEM format.

6. Import the signed certificate to the subordinate trustpoint

```
SWITCH(config)# crypto pki import <subordinate trustpoint name> certificate
```

7. When prompted enter the base 64 encoded device certificate. End with a blank line or the word "quit" on a line by itself. The Switch should respond with:

"% Router Certificate successfully imported"

8. Configure the trustpoints to perform revocation checking using CRL

```
SWITCH(config)# crypto pki trustpoint <root trustpoint name>

SWITCH(ca-trustpoint)# revocation-check CRL

SWITCH(ca-trustpoint)# crl cache none

SWITCH(ca-trustpoint)# match key-usage cRLSign

SWITCH(ca-trustpoint)# exit

SWITCH(config)# crypto pki trustpoint <subordinate trustpoint name>

SWITCH(ca-trustpoint)# revocation-check CRL
```

```
SWITCH(ca-trustpoint)# crl cache none

SWITCH(ca-trustpoint)# match key-usage cRLSign

SWITCH(ca-trustpoint)# exit
```

Additional information on PKI with IPsec can be found in the "Configuring IPsec" Chapter of [**13, 14, 15, or 16**] depending on your TOE model.

4.2.20.3.IKEv2

This section discusses IKEv2 which requires configuring an IKEv2 Proposal, Policy, Keyring, and Profile.

1. Configure the IKEv2 Proposal. An IKEv2 proposal is regarded as complete only when it has at least an encryption algorithm, an integrity algorithm, and a Diffie-Hellman (DH) group configured. If no proposal is configured and attached to an IKEv2 policy, then the default proposal is used in the negotiation, and it contains selections that are not valid for the TOE. Thus the following settings must be set in configuring the IPsec with IKEv2 functionality for the TOE:

    a. In privileged EXEC mode, enter configure terminal.

    ```
    SWITCH# configure terminal
    ```

    b. Specify the IKEv2 proposal. The IKEv2 proposal MUST have a set of an encryption algorithms, a set of integrity algorithms, and a DH group configured.

    ```
    SWITCH(config)# crypto ikev2 proposal <name>
    ```

    c. Set the encryption algorithm(s) for the proposal.

    ```
    SWITCH(config-ikev2-proposal)# encryption < aes-cbc-128 | aes-cbc-256>
    ```

    Note: If the IKEv2 proposal is set to aes-cbc-128, then the IPsec transform set must also be set to esp-aes 128. If the IKEV2 proposal is set to aes-cbc-256, then the IPsec transform set can be set to either esp-aes 128 or esp-aes 256.

    d. Set the integrity algorithm(s) for the proposal.

    ```
    SWITCH(config-ikev2-proposal)# integrity <sha1 | sha256 | sha512>
    ```

    e. Set the Diffie-Hellman group(s)

    ```
    SWITCH(config-ikev2-proposal)# group 14
    ```

    f. Enter exit to return to the main configuration mode.

    ```
    SWITCH(config-ikev2-proposal)# exit
    ```

2. Configure the IKEv2 Policy

    a. Define the IKEv2 policy name.

    ```
    SWITCH(config)# crypto ikev2 policy <Name of IKEv2 policy>
    ```

    b. Specify the proposal created in the previous section

    ```
    SWITCH(config-ikev2-policy)# proposal <name>
    ```

    c. Enter exit to return to the main configuration mode

    ```
    SWITCH(config-ikev2-policy)# exit
    ```

3. Configure the IKEv2 Keyring. If you chose pre-shared key as the authentication method you must complete these steps.

   a. Define the IKEv2 keyring.

   ```
   SWITCH(config)# crypto ikev2 keyring <Name of IKEv2 Keyring>
   ```

   b. Define the peer block

   ```
   SWITCH(config-ikev2-keyring)# peer <Name of the peer block>
   ```

   c. In peer sub mode specify the IPv4 address of peer

   ```
   SWITCH(config-ikev2-keyring-peer)# address <IPv4 Address>
   ```

   d. Specify the IKEv2 peer through an identity address

   ```
   SWITCH(config-ikev2-keyring-peer)# identity address <IPv4 Address>
   ```

   e. Specify a pre-shared key.

   To specify a text-based pre-shared key:

   ```
   SWITCH(config-ikev2-keyring-peer)# pre-shared-key 0 <pre-shared key>
   ```

   Note: By default it is possible to configure pre-shared keys of length 1-127 characters. The recommendation for a strong pre-shared key is a minimum of length of 22 characters composed of any combination of upper and lower case letters, numbers, and special characters (that include: "!", "@", "#", "$", "%", "^", "&", "*", "(", and ")").

   To specify a bit-based pre-shared key:

   ```
   SWITCH(config-ikev2-keyring-peer)# pre-shared-key hex <pre-shared key in hex>
   ```

   Note: By default, it is possible to configure bit-based pre-shared keys of length 2-228 characters. The recommendation for a strong pre-shared key is a minimum of length of 22 characters composed of letters (case insensitive), numbers, and special characters (that include: "!", "@", "#", "$", "%", "^", "&", "*", "(", and ")").

   d. Enter exit twice to return to the main configuration mode

   ```
   SWITCH(config-ikev2-keyring-peer)# exit

   SWITCH(config-ikev2-keyring)# exit
   ```

4. Configure the IKEv2 Profile. An IKEv2 profile is a repository of nonnegotiable parameters of the IKE SA (such as local/remote identities and authentication methods) and the services available to the authenticated peers that match the profile. An IKEv2 profile must be configured and must be attached to either a crypto map or an IPsec profile on both the IKEv2 initiator and responder.

   a. Define the IKEv2 Profile.

   ```
   SWITCH(config)# crypto ikev2 profile <name of IKEv2 profile>
   ```

   b. Set the local authentication method.

   ```
   SWITCH(config-ikev2-profile)# authentication local <rsa-sig> <pre-share>
   ```

   c. Set the remote authentication method.

   ```
   SWITCH(config-ikev2-profile)# authentication remote <rsa-sig> <pre-share>
   ```

   d. Specify the local IKE FQDN identity to use.

```
SWITCH(config-ikev2-profile)# identity local fqdn <fully qualified domain name
string>
```

e. If you are using pre-shared keys specify the key ring created in the previous section

```
SWITCH(config-ikev2-profile)# keyring local <key ring name>
```

f. Set the IKE SA lifetime in seconds.

```
SWITCH(config-ikev2-profile)# lifetime <120-86400>
```

g. Enter exit to return to the main configuration mode

```
SWITCH(config-ikev2-profile)# exit
```

4.2.20.4. IPsec Transform Sets and SA Lifetimes

The Switch must be configured with the proper transform for IPsec ESP encryption and integrity as well as IPsec lifetimes. During the IPsec SA negotiation, the peers agree to use a particular transform set for protecting a particular data flow.

The Administrator can specify multiple transform sets and then specify one or more of these transform sets in a crypto map entry. The transform set defined in the crypto map entry is used in the IPsec SA negotiation to protect the data flows specified by that crypto map entry's access list.

During IPsec security association negotiations with IKE, peers search for a transform set that is the same at both peers. When such a transform set is found, it is selected and applied to the protected traffic as part of both peers' IPsec SAs. (With manually established SAs, there is no negotiation with the peer, so both sides must specify the same transform set.)

1. Define the allowed transform sets. The evaluated configuration supports the following:

```
SWITCH(config)# crypto ipsec transform-set <transform set tag> esp-aes 128 esp-sha-hmac

SWITCH(config)# crypto ipsec transform-set <transform set tag> esp-aes 128 esp-sha256-
hmac

SWITCH(config)# crypto ipsec transform-set <transform set tag> esp-aes 128 esp-sha512-
hmac

SWITCH(config)# crypto ipsec transform-set <transform set tag> esp-aes 256 esp-sha-hmac

SWITCH(config)# crypto ipsec transform-set <transform set tag> esp-aes 256 esp-sha256-
hmac

SWITCH(config)# crypto ipsec transform-set <transform set tag> esp-aes 256 esp-sha512-
hmac
```

Note: If the IKEv2 proposal is set to aes-cbc-128, then the ipsec transform set must also be set to esp-aes 128. If the IKEV2 proposal is set to aes-ccb-256, then the ipsec transform set can be set to either esp-aes 128 or esp-aes 256.

2. Define the IPsec mode which is either tunnel mode or transport mode.

```
SWITCH(cfg-crypto-trans)# mode <transport | tunnel>
```

3. Type exit to return to the main configuration mode.

```
SWITCH(cfg-crypto-trans)# exit
```

4. Define the IPsec security association lifetime. The lifetime can be chosen based on time (hours) or can be volume based. A time-based lifetime must be entered in seconds where 1 hour=3600 seconds and 8 hours=28800 seconds.

```
SWITCH(config)# crypto ipsec security-association lifetime <seconds < 120-28800>> |
<kilobytes  <2560-4294967295>>
```

4.2.20.5. IPsec Crypto Map and Access Control List

The administrator can define the traffic that needs to be protected between two IPsec peers by configuring access lists and applying these access lists to interfaces using crypto map sets. Therefore, traffic may be selected on the basis of the source and destination address, and optionally the Layer 4 protocol and port. (The access lists used for IPsec are only used to determine the traffic that needs to be protected by IPsec, not the traffic that should be blocked or permitted through the interface. Separate access lists define blocking and permitting at the interface).

```
SWITCH(config)# access-list <IP access-list number> permit ip 192.168.3.0 0.0.0.255
10.3.2.0 0.0.0.255
```

For example, if your syslog or RADIUS host is 10.83.84.76 you could define an access list 102 as:

```
SWITCH(config)# access-list 102 permit ip any host 10.83.84.76
```

When a packet matches a permit entry in a particular access list, the method of security in the corresponding crypto map is applied. If the crypto map entry is tagged as ipsec-isakmp, IPsec is triggered. For example:

```
SWITCH(config)# crypto map <crypto map tag> <sequence number> ipsec-isakmp
```

The match address command specifies to use access list number order to determine which traffic is relevant.

```
SWITCH(config-crypto-map)# match address <IP access-list number>
```

Crypto map entries also include transform sets. A transform set is an acceptable combination of security protocols, algorithms, and other settings that can be applied to IPsec-protected traffic. During the IPsec SA negotiation, the peers agree to use a particular transform set when protecting a particular data flow. Use the set transform-set command specifies the transform set tag.

```
SWITCH(config-crypto-map)# set transform-set <proposal tag>
```

The set peer command specifies the ip address of the peer

```
SWITCH(config-crypto-map)# set peer <IP address of peer>
```

If using IKEv2 the set ikev2-profile command specifies the profile to use

```
SWITCH(config-crypto-map)# set ikev2-profile <name of the ikev2 profile>
```

You will need to apply the crypto map to an interface. The GigabitEthernet1 interface configured earlier may be used.

```
SWITCH(config)# int GigabitEthernet1

SWITCH(config-if)# crypto map <crypto map tag>

SWITCH(config-if)# end
```

A crypto map set can contain multiple entries, each with a different access list. The crypto map entries are searched in a se-quence--the router attempts to match the packet to the access list specified in that entry.

When a packet matches a permit entry in a particular access list, and the corresponding crypto map entry is tagged connections are established, if necessary. If the crypto map entry is tagged as ipsec-isakmp, IPsec is triggered.

If there is no SA that the IPsec can use to protect this traffic to the peer, IPsec uses IKE to negotiate with the remote peer to set up the necessary IPsec SAs on behalf of the data flow. The negotiation uses information specified in the crypto map entry as well as the data flow information from the specific access list entry.

Once established, the set of SAs (outbound to the peer) is then applied to the triggering packet and to subsequent applicable packets as those packets exit the Switch. "Applicable" packets are packets that match the same access list criteria that the original packet matched. For example, all applicable packets could be encrypted before being forwarded to the remote peer. The corresponding inbound SAs are used when processing the incoming traffic from that peer.

Access lists associated with IPsec crypto map entries also represent the traffic that the Switch needs protected by IPsec. Inbound traffic is processed against crypto map entries. if an unprotected packet matches a permit entry in a particular access list associated with an IPsec crypto map entry, that packet is dropped because it was not sent as an IPsec-protected packet.

Traffic that does not match a permit crypto map ACL and does not match a non-crypto permit ACL on the interface would be DISCARDED. For example:

```
SWITCH(config)# access-list 102 permit ip 192.168.3.0 0.0.0.255

SWITCH(config)# access-list 103 permit ip 192.168.4.0 0.0.0.255
```

In the example above host 10.83.84.76 does not match either access-list.

Traffic that does not match a permit ACL in the crypto map, but does match a non-crypto permit ACL would be allowed to BYPASS the tunnel. For example, a non-crypto permit ACL for ICMP would allow ping traffic to flow unencrypted if a permit crypto map was not configured that matches the ping traffic. For example:

```
SWITCH(config)# access-list 102 permit ip 192.168.3.0 0.0.0.255

SWITCH(config)# access-list 103 permit ip any host 10.83.84.76
```

In the example above host 10.83.84.76 matches access-list 103 and will bypass the tunnel.

For additional information on Access Control Lists and how rule processing impacts the processing of an IP packet refer to the "ACLs" Chapter of [**13, 14, 15, or 16**] depending on your TOE model.

4.2.20.6. Security Policy Database (SPD)

RFC 4301 calls for an IPsec implementation to protect IP traffic through the use of a Security Policy Database (SPD). The SPD is used to define how IP packets are to be handled: PROTECT the packet (e.g., encrypt the packet), BYPASS the IPsec services (e.g., no encryption), or DISCARD the packet (e.g., drop the packet).

The traffic matching permit ACL would then flow through the IPsec tunnel and be classified as "PROTECTED".

Traffic that does not match a permit crypto map ACL and does not match a non-crypto permit ACL on the interface would be DISCARDED.

Traffic that does not match a permit ACL in the crypto map, but does match a non-crypto permit ACL would be allowed to BYPASS the tunnel. For example, a non-crypto permit ACL for ICMP would allow ping traffic to flow unencrypted if a permit crypto map was not configured that matches the ping traffic.

4.2.20.7. Configure Reference Identifier

If you are using X.509 certificates for IKE peer authentication this section describes configuration of the peer reference identifier through use of a certificate map. Certificate maps provide the ability for a certificate to be matched with a given set of criteria. You can specify which fields within a certificate should be checked and which values those fields may or may not have. There are six logical tests for comparing the field with the value: equal, not equal, contains, does not contain, less than, and greater than or equal. The subordinate trustpoint can bind themselves to certificate maps, and the Switch will determine if they are valid during IKE authentication.

1. Start certificate-map mode

```
SWITCH(config)# crypto pki certificate map <attribute map tag> | <sequence-number>
```

2. Specify one or more certificate fields together with their matching criteria and the value to match. In the evaluated configuration, the field name must specify the SAN (alt-subject-name) field of the peer's certificate. Match criteria should be "eq" for equal.

   For example:

   ```
   SWITCH(ca-certificate-map)# alt-subject-name eq <FQDN of Peer SAN field>

   SWITCH(ca-certificate-map)# alt-subject-name eq < IP Address of Peer in SAN field>
   ```

3. Type exit to return to the main configuration mode.

   ```
   SWITCH(ca-certificate-map)# exit
   ```

4. Associate the certificate map to the IPsec trustpoint created in section 4.2.21.2

   ```
   SWITCH(config)# crypto pki trustpoint < subordinate trustpoint name>

   SWITCH(ca-trustpoint)# match certificate <attribute map tag>
   ```

4.2.20.8. Match Identity

If you are not using X.509 certificates and are using pre-shared key for IKE peer authentication, add a match identity statement to your IKE profile created earlier. Enter:

```
SWITCH(config)# crypto ikev2 profile <profile name>

SWITCH(config-ikev2-profile)# match identity remote address <IP address of peer>
```

4.2.20.9. IKEv2 Fragmentation

Enable support for both the Cisco proprietary IKEv2 fragmentation methodology and the IETF fragmentation methodology specified in RFC 7383.

```
SWITCH#(config)# crypto ikev2 fragmentation
```

The IETF method encrypts packets after fragmentation whereas the Cisco proprietary method performs fragmentation on the encrypted packet. This command expands interoperability between a Cisco device and a non-Cisco host.

4.2.20.10. Enable Remote Syslog Server

Once IPsec has been setup and configured to protect the transmission of audit events to the remote syslog server, use the logging host command below to enable the TOE to transmit audit data. When an audit event is generated, is it simultaneously sent to the external server and the local store.

To configure a remote syslog server enter the following command:

```
SWITCH(config)# logging host <ip address>
```

4.2.20.11. Configure Remote Login Authentication

Once IPsec has been setup and configured to protect the transmission of audit events to the remote RADIUS server, follow the steps below to configure a RADIUS server.

1. Specify the RADIUS Server Name

   ```
   SWITCH(config)# radius server <name for the radius server configuration>
   ```

2. Specify the RADIUS Server Address

```
SWITCH(config-radius-server)# address ipv4 | ipv6 <IPv4 Address> <IPv6 Address>
auth-port 1612
```

3. Specify the RADIUS shared secret

```
SWITCH(config-radius-server)# key <0 | 6> <key>
```

4. Type exit to return to the main configuration mode.

```
SWITCH(config-radius-server)# exit
```

5. Configure AAA for RADIUS

   a. Configure Group Server Name

   ```
   SWITCH(config)# aaa group server radius <radius server-group name>
   ```

   b. Specify RADIUS Server Name

   ```
   SWITCH(config-sg-radius)# server name <radius server name>
   ```

   c. Type exit to return to the main configuration mode

   ```
   SWITCH(config-sg-radius)# exit
   ```

For additional information refer to the "Configuring RADIUS" Chapter of [**13, 14, 15, or 16**].

4.2.20.12. Enable Remote Login Authentication

Use the aaa authentication command below to enable the remote authentication.

```
SWITCH(config)# aaa authentication login default group <radius server-group name> local
```

The local parameter at the end means if the RADIUS server is offline or otherwise unavailable, the TOE will fall back and use local authentication. **Warning: If the RADIUS server is available and the account is not properly configured, the Administrator login will not be successful.**

For additional information refer to the "Configuring RADIUS" Chapter of [**13, 14, 15, or 16**] depending on your TOE model.

4.2.20.13. IPsec References

For additional information on IPsec refer to the "Configuring IPsec" Chapter of [**13, 14, 15, or 16**] depending on your TOE model.

Note: The TOE uses X.509v3 certificates to support authentication for IPsec connections. The TSF determines the validity of certificates by ensuring that the certificate and the certificate path are valid in accordance with RFC 5280. The certificate path is validated by ensuring that all the CA certificates have the basicConstraints extension and the CA flag is set to TRUE and the certificate path must terminate with a trusted CA certificate. OCSP is not supported; therefore the OCSP Signing purpose (id-kp 9 with OID 1.3.6.1.5.5.7.3.9) is trivially satisfied by the TOE. Revocation checking is performed on the leaf and intermediate certificate(s) when authenticating a certificate chain provided by the remote peer.

4.2.21. MACSEC and MKA Configuration

The TOE authenticates and encrypts packets between itself and a MACsec peer. The MACsec Key Agreement (MKA) Protocol provides the required session keys and manages the required encryption keys to protect data exchanged by the peers. By default, MACsec is disabled and there are no MKA policies configured on the TOE.

The following is an example of an MKA policy:

```
SWITCH(config)# mka policy <policy-name>

SWITCH(config-mka-policy)# key-server priority 200

SWITCH(config-mka-policy)# macsec-cipher-suite gcm-aes-128

SWITCH(config-mka-policy)# confidentiality-offset 30

SWITCH(config-mka-policy)# end
```

The following is an example of configuring MACsec PSK

```
SWITCH(config)# key chain keychain1 macsec

SWITCH(config-key-chain)# key 1000

SWITCH(config-key-chain)# cryptographic-algorithm aes-128-cmac

SWITCH(config-key-chain)# key-string 12345678901234567890123456789012

SWITCH(config-key-chain)# lifetime local 12:12:00 October 2 2022 12:19:00 October 2
203

SWITCH(config-mka-policy)# end
```

Note: When specifying the value of the key identifier, the Administrator must ensure the length does not exceed 64 hex digits (32 bytes). An example of the maximum length would be:

key abcdef0123456789abcdef0123456789abcdef0123456789abcdef0123456789

The following is an example of configuring MACsec MKA on an Interface using PSK

```
SWITCH(config) interface GigabitEthernet 1/0/1

SWITCH(config-if)# macsec network-link

SWITCH(config-if)# mka policy my_policy

SWITCH(config-if)# mka pre-shared-key key-chain mykeychain1

SWITCH(config-if) # macsec replay-protection window-size 10

SWITCH(config-if) # end
```

Detailed steps to configure MACsec and an MKA policy on the TOE can be found in the “Configuring MACsec Encryption” Chapter of [**13, 14, 15, or 16**] depending on your TOE model.

Configuration Examples for MACsec Encryption can be found in the "Configuration Examples for MACsec Encryption" section of the "Configuring MACsec Encryption" Chapter of [**13, 14, 15, or 16**] depending on your TOE model.

To verify MACsec is enabled, refer to the “show" commands listed under **Step 2** of Scenario 2 in [**22**].

4.2.22. FIPS Mode

The administrator needs to configure the Switch for FIPS mode of operation.

1. In privilege EXEC mode, enter configure terminal

```
SWITCH# config terminal
```

2. Enter a FIPS authorization key. **Note:** The key length should be 32 characters. If you have High Availability enabled ensure both active and standby Switches have the same FIPS authorization key.

```
SWITCH(config)# fips authorization-key 12345678901234567890123456789012
```

3. Exit configuration mode and return to privileged EXEC mode

```
SWITCH(config)# end
```

4. You must now reboot the switch to enable FIPS mode.

4.2.23. Verify FIPS Mode

To verify FIPS mode enter the following

```
SWITCH# show fips status
```

The status of FIPS mode on the device will be displayed

For additional information, refer to the "Secure Operation in FIPS Mode" chapter of **[13, 14, 15, or 16]** depending on your TOE model.

5. Operational Guidance for the TOE

5.1. Access CLI Over SSH

From your remote management workstation, initiate a connect using SSH and supply either your public key or password credentials. Upon successful login you will be presented with privilege administrator access denoted by the 'hashtag' symbol:

```
SWITCH#
```

5.2. View Audit Events

Audit events may be viewed at the CLI by entering:

```
SWITCH# show logging
```

5.3. Unblock Locked-Out Account

To unblock an account that has been prevented from logging in due to successive login failures enter the following:

```
SWITCH# clear aaa local user blocked username <username>
```

5.4. Cryptographic Self-Tests

The TOE runs a suite of self-tests during initial start-up to verify correct operation of cryptographic modules. If any component reports failure for the POST, the system crashes and appropriate information is displayed on the local console. All ports are blocked from moving to forwarding state during the POST. If all components of all modules pass the POST, the system is placed in FIPS PASS state and ports are allowed to forward data traffic. If any of the tests fail, a message is displayed to the local console and the TOE component will automatically reboot. If the Administrator observes a cryptographic self-test failure, they must contact Cisco Technical Support. Refer to the Contact Cisco section of this document.

If the Administrator needs to execute cryptographic self-tests for the Switch after the image is loaded enter the following command:

```
SWITCH# test crypto self-test
```

5.5.Zeroize Private Key

Should the Administrator need to zeroize a private key generated as instructed in the SSH or IPsec sections of this document and stored in NVRAM, the following command may be used in configuration mode:

```
SWITCH(config)# crypto key zeroize rsa <key pair label>
```

The keys are zeroized immediately after use.

Other keys stored in SDRAM are zeroized when no longer in use, zeroized with a new value of the key, or zeroized on power-cycle.

5.6.IPsec Session Interruption and Recovery

If an IPsec session with a peer is unexpectedly interrupted, the connection will be broken and the Administrator will find a connection time out error message in the audit log. The administrator can use the show command below to confirm the connection is broken:

```
SWITCH# show crypto ipsec sa
```

When a connection is broken no administrative interaction is required. The IPsec session will be reestablished (a new SA set up) once the peer is back online.

5.7.MACsec Session Interruption and Recovery

If a MACsec session with a peer is unexpectedly interrupted, the connection will be broken and the Administrator will find a connection time out error message in the audit log. The administrator can use the show command below to confirm the connection is broken:

```
SWITCH# show mka statistics

SWITCH# show mka sessions

SWITCH# show mka statistics
```

When a connection is broken no administrative interaction is required. The MACsec session will be reestablished once the peer is back online.

5.8. Update TOE Software

5.8.1. One-Shot Upgrade

Using the CLI, the Administrator may install new image files in one stage (all at once) or may choose to perform a multi-stage upgrade.

1. Follow the steps below to update the TOE Software in one stage (all at once) using the CLI.

   a. You will need to obtain an updated 17.9 software image. Navigate to Cisco Software Central at https://software.cisco.com/software/csws/ws/platform/home?locale=en_US#. Use your Cisco Care Online (CCO) or SMART account and download the image for your Switch platform.

   b. Place the image on a TFTP, FTP, or SFTP server that is reachable by the SWITCH.

c. At the SWITCH console enter: `install add file [tftp | ftp | sftp://<IP Address of TFTP/FTP/SFTP server>] <image name.bin> activate commit`

   The image installation process will begin.

d. The SWITCH console will respond with "`This operation may require a reload of the system. Do you want to proceed? [y/n]`"

e. Using a separate remote session, the Administrator can query the currently installed but not yet active SWITCH software version by entering the following command at the CLI:

   `SWITCH# show active install`

f. To Activate the new image, return to the SWITCH console and respond "y" to the prompt "`This operation may require a reload of the system. Do you want to proceed? [y/n]`"

g. The SWITCH will commit the new image, save the configuration, and reload.

The TOE will automatically verify the integrity of the stored image when loaded for execution.

The SWITCH uses a Cisco public key to validate the digital signature to obtain an embedded SHA512 hash that was generated prior to the image being distributed from Cisco. The SWITCH then computes its own hash of the image using the same SHA512 algorithm. The SWITCH verifies the computed hash against the embedded hash. If they match the image is authenticated and has not been modified or tampered. If they do not match the image will not boot or execute.

After boot, the authorized administrator can also manually verify the digital signature by executing on the SWITCH:

`verify bootflash:<image or package name>`

5.8.2. Multi-Stage Upgrade

1. Follow the steps below to update the TOE Software in separate stages:

   a. You will need to obtain an updated 17.9 software image. Navigate to Cisco Software Central at https://software.cisco.com/software/csws/ws/platform/home?locale=en_US#

      Use your Cisco Care Online (CCO) or SMART account and download the image for your Switch platform.

   b. Place the image on a TFTP, FTP, or SFTP server that is reachable by the SWITCH.

   c. At the SWITCH console enter: `SWITCH# copy tftp bootflash:`

      The SWITCH will prompt for address or name of remote host. Enter the IP address of your TFTP Sever. Once the image has successfully downloaded, the Predownload Status will change to "Complete"

      The SWITCH will prompt for Source filename. Enter the name of the image file.

      The SWITCH will begin loading the image via TFTP to bootflash:

   d. At the SWITCH console enter: `install add file bootflash:cat9k_iosxe.17.09.02.SPA.bin`

      The SWITCH will begin installing the image file. It should respond that the image was successfully added and will display the version.

   e. If you are ready to perform the upgrade, enter: `install activate`

      The SWITCH should respond with "`System configuration has been modified`"

      Press Yes(y) to save the configuration and proceed.

f. The SWITCH console will respond with "`This operation may require a reload of the system. Do you want to proceed? [y/n]`"

h. Using a separate remote session, the Administrator can query the currently installed but not yet active SWITCH software version by entering the following command at the CLI:

```
SWITCH# show active install
```

g. To Activate the new image, return to the SWITCH console and respond "y" to the prompt "`This operation may require a reload of the system. Do you want to proceed? [y/n]`"

The SWITCH will begin activating the image package and should respond with a list of the packages that it activated. The SWITCH console will then respond with a message stating the Activate stage finished and that it will now reload.

h. After the SWITCH has reloaded, access the CLI console and enter the following to commit the image:

```
SWITCH# install commit
```

The SWITCH should respond that it successful committed the package.

2. The administrator can verify the image is install and activated on the SWITCH by entering:

```
SWITCH# show install summary
```

The image Filename/Version should say "C" for activated and committed.

Note: At installation, the SWITCH extracts sub-packages from the image file that was installed (.bin) and the SWITCH boots using a package provisioning file, packages.conf. This provisioning file manages the bootup of each individual sub-package.

If desired, the authorized administrator can manually verify the digital signature on each individual sub-package by executing verify bootflash:<package name> on the SWITCH. For example:

```
SWITCH# verify bootflash:cat9k-rpboot.17.09.02.SPA.pkg

SWITCH# verify bootflash:cat9k-rbase.17.09.02.SPA.pkg
```

The TOE will automatically verify the integrity of the stored image when loaded for execution.

The TOE uses a Cisco public key to validate the digital signature to obtain an embedded SHA512 hash that was generated prior to the image being distributed from Cisco. The TOE then computes its own hash of the image using the same SHA512 algorithm and verifies the computed hash against the embedded hash. If they match the image is authenticated and has not been modified or tampered. If they do not match the image will not boot or execute.

After boot, the authorized administrator can also manually verify the digital signature by executing on the TOE:

```
verify bootflash:<image or package name>
```

6. Auditing

Auditing allows Security Administrators to discover intentional and unintentional issues with the TOE's configuration and/or operation. Auditing of administrative activities provides information that may be used to hasten corrective action should the system be configured incorrectly. Security audit data can also provide an indication of failure of critical portions of the TOE (e.g. a communication channel failure or anomalous activity (e.g. establishment of an administrative session at a suspicious time, repeated failures to establish sessions or authenticate to the TOE) of a suspicious nature.

The TOE generates an audit record whenever an audited event occurs. The types of events that cause audit records to be generated include, cryptography related events, identification and authentication related events, and administrative events (the specific events and the contents of each audit record are listed in the table below). Each of the events is specified in enough detail to identify the user for which the event is associated, when the event occurred, where the event occurred, the outcome of the event, and the type of event that occurred.

The SWITCH, which is the component that stores audit data locally, will also transmit all audit messages in real-time to a specified external syslog server.

Table 6. Sample Audit Events

SFR	Auditable Event	Sample Audit Event Data
FAU_GEN.1.1	Startup and Shutdown of Audit Function	<45>554: C9300-24T: Apr 18 2023 04:10:24: %SYS-5-RESTART: System restarted -- <46>564: C9300-24T: Apr 18 2023 04:10:24: %SYS-6-LOGGINGHOST_STARTSTOP: Logging to host 172.16.16.239 port 514 (Mgmt-vrf) started - CLI initiated <46>2905: C9300-24T: Apr 18 2023 04:06:41: %HA_EM-6-LOG: cli_log: User:admin via Port:0 Executed[reload]

FCS_IPSEC_EXT.1	Failure to establish an IPsec SA with reason for failure.	**Failed to find matching policy (General)** <47>12048: C9300-24T: *Nov 16 2022 14:43:24: IKEv2:Received Packet [From 192.168.144.254:500/To 192.168.144.50:500/VRF i0:f0] <43>12092: C9300-24T: *Nov 16 2022 14:43:24: %IKEV2-3-NEG_ABORT: Negotiation aborted due to ERROR: Failed to find a matching policy **Invalid transform proposal received (bad ESP cipher)** <47>5309: C9300-24T: *Nov 16 2022 13:27:45: IKEv2:Received Packet [From 192.168.144.254:500/To 192.168.144.50:500/VRF i0:f0] <47>5492: C9300-24T: *Nov 16 2022 13:27:45: IPSEC(ipsec_process_proposal): invalid transform proposal received: <47>5493: C9300-24T: {esp-gcm } <47>5496: C9300-24T: *Nov 16 2022 13:27:45: IKEv2-ERROR:(SESSION ID = 7,SA ID = 1):Received Policies: : Failed to find a matching policyESP: Proposal 1: AES-GCM-128 Don't use ESN **Failed to find matching proposal (bad IKE cipher)** <47>7471: C9300-24T: *Nov 16 2022 13:53:20: IKEv2:Received Packet [From 192.168.144.254:500/To 192.168.144.50:500/VRF i0:f0] <47>7501: C9300-24T: *Nov 16 2022 13:53:20: IKEv2-ERROR:(SESSION ID = 14,SA ID = 1):Received Policies: : Failed to find a matching policyProposal 1: AES-GCM-128 SHA256 SHA256 DH_GROUP_2048_MODP/Group 14 <47>7502: C9300-24T: *Nov 16 2022 13:53:20: IKEv2-ERROR:(SESSION ID = 14,SA ID = 1):Expected Policies: : Failed to find a matching policyProposal 1: AES-CBC-128 AES-CBC-256 SHA256 SHA96 SHA256 SHA512 DH_GROUP_2048_MODP/Group 14 <47>7504: C9300-24T: *Nov 16 2022 13:53:20: IKEv2:(SESSION ID = 14,SA ID = 1):Sending no proposal chosen notify **Failed to validate certificate (Bad Reference Identifier)** <47>11334: C9300-24T: Feb 22 2023 16:12:18: IKEv2:Received Packet [From 192.168.144.254:500/To 192.168.144.50:500/VRF i0:f0] <47>11728: C9300-24T: Feb 22 2023 16:12:18: CRYPTO_PKI: Checking cert map authorization <43>11732: C9300-24T: Feb 22 2023 16:12:18: %PKI-3-CERTIFICATE_INVALID_UNAUTHORIZED: Certificate chain validation has failed. Unauthorized

FCS_SSHS_EXT.1	Failure to establish an SSH session; Reason for failure	**No matching cipher** <43>3591: C9300-24T: Apr 13 2023 03:28:47: %SSH-3-NO_MATCH: No matching cipher found: client aes128-ctr server aes256-cbc,aes128-cbc <45>3592: C9300-24T: Apr 13 2023 03:28:47: %SSH-5-SSH2_SESSION: SSH2 Session request from 172.16.16.254 (tty = 0) using crypto cipher '', hmac '' Failed <45>3593: C9300-24T: Apr 13 2023 03:28:47: %SSH-5-SSH2_CLOSE: SSH2 Session from 172.16.16.254 (tty = 0) for user '' using crypto cipher '', hmac '' closed **No matching host key type** <43>3595: C9300-24T: Apr 13 2023 03:42:33: %SSH-3-NO_MATCH: No matching hostkey algorithm found: client ssh-rsa server rsa-sha2-256,rsa-sha2-512 <45>3596: C9300-24T: Apr 13 2023 03:42:33: %SSH-5-SSH2_SESSION: SSH2 Session request from 172.16.16.254 (tty = 0) using crypto cipher '', hmac '' Failed <45>3597: C9300-24T: Apr 13 2023 03:42:33: %SSH-5-SSH2_CLOSE: SSH2 Session from 172.16.16.254 (tty = 0) for user '' using crypto cipher '', hmac '' closed **No matching MAC** <43>3598: C9300-24T: Apr 13 2023 04:03:38: %SSH-3-NO_MATCH: No matching mac found: client hmac-sha1 server hmac-sha2-512,hmac-sha2-256 <45>3599: C9300-24T: Apr 13 2023 04:03:38: %SSH-5-SSH2_SESSION: SSH2 Session request from 172.16.16.254 (tty = 0) using crypto cipher '', hmac '' Failed <45>3600: C9300-24T: Apr 13 2023 04:03:38: %SSH-5-SSH2_CLOSE: SSH2 Session from 172.16.16.254 (tty = 0) for user '' using crypto cipher '', hmac '' closed **No matching key exchange method** <43>3601: C9300-24T: Apr 13 2023 04:14:40: %SSH-3-NO_MATCH: No matching kex algorithm found: client ecdh-sha2-nistp256,ext-info-c server diffie-hellman-group14-sha1 <45>3602: C9300-24T: Apr 13 2023 04:14:40: %SSH-5-SSH2_SESSION: SSH2 Session request from 172.16.16.254 (tty = 0) using crypto cipher '', hmac '' Failed <45>3603: C9300-24T: Apr 13 2023 04:14:40: %SSH-5-SSH2_CLOSE: SSH2 Session from 172.16.16.254 (tty = 0) for user '' using crypto cipher '', hmac '' closed **Oversized Packet** <43>3577: C9300-24T: Apr 13 2023 03:14:56: %SSH-3-BAD_PACK_LEN: Bad packet length 33068 <46>3578: C9300-24T: Apr 13 2023 03:14:56: %SYS-6-LOGOUT: User admin has exited tty session 1(172.16.16.254)

FIA_AFL.1	Failed Login due to Exceeding limit	<45>58605: C9300-24T: Mar 28 2023 06:11:09: %AAA-5-LOCAL_USER_BLOCKED: User TestUser17674 blocked for login till 01:14:09 EST Mar 28 2023 <44>58606: C9300-24T: Mar 28 2023 06:11:11: %SEC_LOGIN-4-LOGIN_FAILED: Login failed [user: TestUser17674] [Source: 172.16.16.254] [localport: 22] [Reason: Login Authentication Failed] at 01:11:11 EST Tue Mar 28 2023

FIA_UIA_EXT.1 FIA_UAU_EXT.2	All use of the authentication mechanism.	**SSH Authentication Success – Password** <45>3552: C9300-24T: Apr 13 2023 01:46:38: %SEC_LOGIN-5-LOGIN_SUCCESS: Login Success [user: admin] [Source: 172.16.16.254] [localport: 22] at 20:46:38 EST Wed Apr 12 2023 <45>3553: C9300-24T: Apr 13 2023 01:46:38: %SSH-5-SSH2_USERAUTH: User 'admin' authentication for SSH2 Session from 172.16.16.254 (tty = 0) using crypto cipher 'aes128-cbc', hmac 'hmac-sha2-256' Succeeded **SSH Authentication Failure – Password** <44>3566: C9300-24T: Apr 13 2023 02:59:27: %SEC_LOGIN-4-LOGIN_FAILED: Login failed [user: admin] [Source: 172.16.16.254] [localport: 22] [Reason: Login Authentication Failed] at 21:59:27 EST Wed Apr 12 2023 <45>3567: C9300-24T: Apr 13 2023 02:59:27: %SSH-5-SSH2_USERAUTH: User '' authentication for SSH2 Session from 172.16.16.254 (tty = 0) using crypto cipher 'aes128-cbc', hmac 'hmac-sha2-256' Failed **SSH Authentication Success – Public Key** <45>69666: C9300-24T: Apr 7 2023 03:40:31: %SEC_LOGIN-5-LOGIN_SUCCESS: Login Success [user: testadmin] [Source: 172.16.16.254] [localport: 22] at 22:40:31 EST Thu Apr 6 2023 <45>69667: C9300-24T: Apr 7 2023 03:40:31: %SSH-5-SSH2_USERAUTH: User 'testadmin' authentication for SSH2 Session from 172.16.16.254 (tty = 0) using crypto cipher 'aes256-cbc', hmac 'hmac-sha2-256' Succeeded **SSH Authentication Failure – Public Key** <44>69676: C9300-24T: Apr 7 2023 03:45:59: %SEC_LOGIN-4-LOGIN_FAILED: Login failed [user: testadmin] [Source: 172.16.16.254] [localport: 22] [Reason: Login Authentication Failed] at 22:45:59 EST Thu Apr 6 2023 <45>69677: C9300-24T: Apr 7 2023 03:47:11: %SSH-5-SSH2_USERAUTH: User '' authentication for SSH2 Session from 172.16.16.254 (tty = 0) using crypto cipher 'aes256-cbc', hmac 'hmac-sha2-256' Failed **Console Authentication Success** <45>69547: C9300-24T: Apr 7 2023 03:24:54: %SEC_LOGIN-5-LOGIN_SUCCESS: Login Success [user: admin] [Source: LOCAL] [localport: 0] at 22:24:54 EST Thu Apr 6 2023 **Console Authentication Failure** <44>2814: C9300-24T: Apr 12 2023 05:25:52: %SEC_LOGIN-4-LOGIN_FAILED: Login failed [user: admin] [Source: LOCAL] [localport: 0] [Reason: Login Authentication Failed] at 00:25:52 EST Wed Apr 12 2023
FIA_X509_EXT.1/Rev	Unsuccessful attempt to validate a certificate	**Expired Server Cert** <47>4151: C9300-24T: Feb 2 2023 08:35:30: IKEv2:Received Packet [From 192.168.144.254:500/To 192.168.144.50:500/VRF i0:f0]

		<47>4219: C9300-24T: Feb 2 2023 08:35:30: IKEv2-ERROR:Current time is more than cert validity time **Expired SubCA Cert** <47>4263: C9300-24T: Feb 2 2023 08:36:25: IKEv2:Received Packet [From 192.168.144.254:500/To 192.168.144.50:500/VRF i0:f0] <43>4426: C9300-24T: Feb 2 2023 08:36:25: %PKI-3-CERTIFICATE_INVALID_EXPIRED: Certificate chain validation has failed. The certificate (SN: 13) has expired. Validity period ended on 2022-11-29T00:45:00Z **Absent or invalid basicConstraint flag** <47>9890: C9300-24T: Feb 2 2023 18:42:27: IKEv2:Received Packet [From 192.168.144.254:500/To 192.168.144.50:500/VRF i0:f0] <47>10038: C9300-24T: Feb 2 2023 18:42:27: IKEv2:(SESSION ID = 18,SA ID = 1):Verify cert failed <47>10036: C9300-24T: Feb 2 2023 18:42:27: IKEv2:(SA ID = 1):[PKI -> IKEv2] Validation of certificate chain FAILED **Revoked Certificate** <47>5136: C9300-24T: Feb 2 2023 08:38:09: IKEv2:Received Packet [From 192.168.144.254:500/To 192.168.144.50:500/VRF i0:f0] <43>5571: C9300-24T: Feb 2 2023 08:38:10: %PKI-3-CERTIFICATE_REVOKED: Certificate chain validation has failed. The certificate (SN: 00D1) is revoked **Corrupt Cert ASN1** <47>8123: C9300-24T: Feb 2 2023 08:44:45: IKEv2:Received Packet [From 192.168.144.254:500/To 192.168.144.50:500/VRF i0:f0] <47>8257: C9300-24T: Feb 2 2023 08:44:45: CRYPTO_PKI: status = 0x705(E_INPUT_DATA : invalid encoding format for input data): BER/DER decoding of certificate has failed **Corrupt Cert Signature** <47>8307: C9300-24T: Feb 2 2023 08:45:41: IKEv2:Received Packet [From 192.168.144.254:500/To 192.168.144.50:500/VRF i0:f0] <47>8657: C9300-24T: Feb 2 2023 08:45:41: ../cert-c/source/vericert.c(145) : E_INVALID_SIGNATURE : error verifying digitial signature **Corrupt Public Key** <47>8720: C9300-24T: Feb 2 2023 09:03:26: IKEv2:Received Packet [From 192.168.144.254:500/To 192.168.144.50:500/VRF i0:f0] <47>9069: C9300-24T: Feb 2 2023 09:03:26: ../cert-c/source/vericert.c(145) : E_INVALID_SIGNATURE : error verifying digitial signature **CRL Incorrectly Signed**

		<47>6582: C9300-24T: Feb 2 2023 08:41:05: IKEv2:Received Packet [From 192.168.144.254:500/To 192.168.144.50:500/VRF i0:f0] <47>6991: C9300-24T: Feb 2 2023 08:41:05: Key-usage mismatch. Cert does not have cRLSign bit set. <47>6992: C9300-24T: Feb 2 2023 08:41:05: CRYPTO_PKI: CRL verify has failed **Invalid Certificate Chain** <47>9314: C9300-24T: Feb 2 2023 17:38:45: IKEv2:Received Packet [From 192.168.144.254:500/To 192.168.144.50:500/VRF i0:f0] <47>9461: C9300-24T: Feb 2 2023 17:38:45: IKEv2:(SA ID = 1):[PKI -> IKEv2] Validation of certificate chain FAILED **Unreachable Revocation Server** <47>10926: C9300-24T: Feb 2 2023 19:02:37: IKEv2:Received Packet [From 192.168.144.254:500/To 192.168.144.50:500/VRF i0:f0] <43>11311: C9300-24T: Feb 2 2023 19:02:45: %PKI-3-CRL_FETCH_FAIL: CRL fetch for trustpoint rootca-rsa failed **Add Trust Anchor** See FMT_SMF.1 **Remove Trust Anchor** See FMT_SMF.1
FMT_MOF.1/ ManualUpdate	Any attempt to initiate a manual update	See FPT_TUD_EXT.1

FMT_SMF.1	All management activities of TSF data.	**Ability to administer the TOE locally and remotely** See FIA_UIA_EXT.1 **Ability to configure the access banner** <45>228: C9300-24T: Oct 13 2022 17:22:30: %PARSER-5-CFGLOG_LOGGEDCMD: User:admin logged command:banner login z This is the CC Login Banner z <45>229: C9300-24T: Oct 13 2022 17:22:32: %SYS-5-CONFIG_I: Configured from console by admin on console **Ability to configure the session inactivity time before session termination or locking** Console: <45>68998: C9300-24T: Mar 28 2023 19:51:15: %PARSER-5-CFGLOG_LOGGEDCMD: User:admin logged command:line con 0 <45>68999: C9300-24T: Mar 28 2023 19:51:15: %PARSER-5-CFGLOG_LOGGEDCMD: User:admin logged command:exec-timeout 1 SSH: <45>51340: C9300-24T: Mar 28 2023 00:22:02: %PARSER-5-CFGLOG_LOGGEDCMD: User:admin logged command:line vty 0 15 <45>51341: C9300-24T: Mar 28 2023 00:22:02: %PARSER-5-CFGLOG_LOGGEDCMD: User:admin logged command:exec-timeout 1 **Ability to update the TOE, and to verify the updates using [digital signature] capability prior to installing those updates** See FPT_TUD_EXT.1 **Ability to configure the authentication failure parameters for FIA AFL.1** <45>58533: C9300-24T: Mar 28 2023 06:10:30: %PARSER-5-CFGLOG_LOGGEDCMD: User:admin logged command:aaa authentication rejected 5 in 3600 ban 180 **Ability to modify the behavior of the transmission of audit data to an external IT entity** <45>199: C9300-24T: *Oct 13 2022 06:19:55: %PARSER-5-CFGLOG_LOGGEDCMD: User:admin logged command:logging host 172.16.16.239 vrf Mgmt-vrf transport udp port 514 **Ability to manage the cryptographic keys** Generate Crypto Key for SSH: <45>337: C9300L-48T-4G: Oct 18 2022 23:25:56: %PARSER-5-CFGLOG_LOGGEDCMD: User:admin logged command:crypto key generate rsa label * modulus 2048 <45>336: C9300L-48T-4G: Oct 18 2022 23:25:56: %CRYPTO_ENGINE-5-KEY_ADDITION: A key named SSH-KEY has been generated or imported by crypto-engine Generate Crypto Key for IPsec: <45>2660: C9300-24T: Feb 2 2023 07:56:48: %PARSER-5-CFGLOG_LOGGEDCMD: User:admin logged command:crypto key generate rsa general-keys modulus 2048 label *

		<45>2659: C9300-24T: Feb 2 2023 07:56:48: %CRYPTO_ENGINE-5-KEY_ADDITION: A key named IPSEC-KEY has been generated or imported by crypto-engine Delete Crypto Key: <46>514: C9300L-48T-4G: Apr 21 2023 01:32:43: %HA_EM-6-LOG: cli_log: User:admin via Port:0 Executed[crypto key zeroize rsa *] <45>515: C9300L-48T-4G: Apr 21 2023 01:32:45: %CRYPTO_ENGINE-5-KEY_DELETED: A key named SSH-KEY has been removed from key storage **See also audits below for ability to manage the TOE's trust store and the trusted public keys database.** **Ability to configure the cryptographic functionality** Configure SSH: <45>385: C9300-24T: Oct 18 2022 23:32:27: %PARSER-5-CFGLOG_LOGGEDCMD: User:admin logged command:ip ssh version 2 <45>386: C9300-24T: Oct 18 2022 23:32:42: %PARSER-5-CFGLOG_LOGGEDCMD: User:admin logged command:ip ssh server algorithm kex diffie-hellman-group14-sha1 <45>387: C9300-24T: Oct 18 2022 23:32:49: %PARSER-5-CFGLOG_LOGGEDCMD: User:admin logged command:ip ssh server algorithm encryption aes256-cbc aes128-cbc <45>388: C9300-24T: Oct 18 2022 23:32:57: %PARSER-5-CFGLOG_LOGGEDCMD: User:admin logged command:ip ssh server algorithm mac hmac-sha2-512 hmac-sha2-256 <45>389: C9300-24T: Oct 18 2022 23:33:04: %PARSER-5-CFGLOG_LOGGEDCMD: User:admin logged command:ip ssh server algorithm hostkey rsa-sha2-256 rsa-sha2-512 <45>390: C9300-24T: Oct 18 2022 23:33:13: %PARSER-5-CFGLOG_LOGGEDCMD: User:admin logged command:ip ssh server algorithm publickey rsa-sha2-256 rsa-sha2-512 Configure IPSec: <45>2717: C9300-24T: *Nov 16 2022 04:21:22: %PARSER-5-CFGLOG_LOGGEDCMD: User:admin logged command:crypto ikev2 proposal syslogipsec <45>2718: C9300-24T: *Nov 16 2022 04:21:38: %PARSER-5-CFGLOG_LOGGEDCMD: User:admin logged command:encryption aes-cbc-128 aes-cbc-256 <45>2719: C9300-24T: *Nov 16 2022 04:21:47: %PARSER-5-CFGLOG_LOGGEDCMD: User:admin logged command:prf sha256 <45>2720: C9300-24T: *Nov 16 2022 04:22:03: %PARSER-5-CFGLOG_LOGGEDCMD: User:admin logged command:integrity sha1 sha256 sha512 <45>2721: C9300-24T: *Nov 16 2022 04:22:09: %PARSER-5-CFGLOG_LOGGEDCMD: User:admin logged command:group 14 <45>2771: C9300-24T: *Nov 16 2022 07:25:24: %PARSER-5-CFGLOG_LOGGEDCMD: User:admin logged command:crypto ipsec security-association lifetime kilobytes 2560 <45>2772: C9300-24T: *Nov 16 2022 07:25:35: %PARSER-5-CFGLOG_LOGGEDCMD: User:admin logged command:crypto ipsec security-association lifetime seconds 28800 <45>2773: C9300-24T: *Nov 16 2022 07:26:05: %PARSER-5-CFGLOG_LOGGEDCMD: User:admin logged command:crypto

		ipsec transform-set SyslogTransform esp-aes 256 esp-sha256-hmac **Ability to configure the thresholds for SSH rekeying** <45>405: C9300-24T: Oct 18 2022 23:34:38: %PARSER-5-CFGLOG_LOGGEDCMD: User:admin logged command:ip ssh rekey time 10 <45>406: C9300-24T: Oct 18 2022 23:34:43: %PARSER-5-CFGLOG_LOGGEDCMD: User:admin logged command:ip ssh rekey volume 100 **Ability to set the time which is used for timestamps** See FPT_STM_EXT.1 **Reset Passwords** <45>69400: C9300-24T: Apr 6 2023 05:32:08: %PARSER-5-CFGLOG_LOGGEDCMD: User:TestUser5775 logged command:username TestUser5775 secret * **Ability to configure the reference identifier for the peer** <45>3133: C9300-24T: Feb 13 2023 23:42:06: %PARSER-5-CFGLOG_LOGGEDCMD: User:admin logged command:crypto pki certificate map sanmap 1 <45>3134: C9300-24T: Feb 13 2023 23:42:25: %PARSER-5-CFGLOG_LOGGEDCMD: User:admin logged command:alt-subject-name eq tl16-16x.example.com **Ability to manage the TOE's trust store and designate X509.v3 certificates as trust anchors** Create Trustpoint: <45>3075: C9300-24T: Apr 21 2023 04:06:10: %PARSER-5-CFGLOG_LOGGEDCMD: User:admin logged command:crypto pki trustpoint rootca-rsa <46>3074: C9300-24T: Apr 21 2023 04:06:10: %PKI-6-TRUSTPOINT_CREATE: Trustpoint: rootca-rsa created succesfully Import CA Cert: <45>3113: C9300-24T: Apr 21 2023 04:10:02: %PARSER-5-CFGLOG_LOGGEDCMD: User:admin logged command:crypto pki authenticate rootca-rsa <47>3103: C9300-24T: Apr 21 2023 04:10:00: CRYPTO_PKI: trustpoint rootca-rsa authentication status = 0 <47>3104: C9300-24T: rootca-rsa:A CA certificate has been installed <47>3105: C9300-24T: #011#011#011Issuer-name : cn=rootca-rsa,e=rootca-rsa@gossamersec.com,o=GSS,l=Catonsville,st=MD,c=US <47>3106: C9300-24T: #011#011#011Subject-name : cn=rootca-rsa,e=rootca-rsa@gossamersec.com,o=GSS,l=Catonsville,st=MD,c=US <47>3107: C9300-24T: #011#011#011Serial-number: 010001 <47>3108: C9300-24T: #011#011#011End-date : 2024-11-28T00:40:43Z **Generate Certificate Request**

		<45>2917: C9300-24T: Feb 2 2023 08:02:35: %PARSER-5-CFGLOG_LOGGEDCMD: User:admin logged command:crypto pki enroll rootca-rsa **Remove Trustpoint & Certs** <45>2650: C9300-24T: Feb 2 2023 07:54:01: %PARSER-5-CFGLOG_LOGGEDCMD: User:admin logged command:no crypto pki trustpoint rootca-rsa <46>2645: C9300-24T: Feb 2 2023 07:54:01: %PKI-6-TRUSTPOINT_DELETE: Trustpoint: rootca-rsa deleted succesfully **Ability to manage the trusted public keys database** Configure public key authentication: <45>69681: C9300-24T: Apr 7 2023 03:47:48: %PARSER-5-CFGLOG_LOGGEDCMD: User:admin logged command:ip ssh server algorithm authentication publickey <45>69598: C9300-24T: Apr 7 2023 03:30:30: %PARSER-5-CFGLOG_LOGGEDCMD: User:admin logged command:ip ssh server algorithm publickey ssh-rsa Configure User with public key: <45>69615: C9300-24T: Apr 7 2023 03:30:54: %PARSER-5-CFGLOG_LOGGEDCMD: User:admin logged command:ip ssh pubkey-chain <45>69616: C9300-24T: Apr 7 2023 03:31:09: %PARSER-5-CFGLOG_LOGGEDCMD: User:admin logged command:username testadmin <45>69617: C9300-24T: Apr 7 2023 03:33:32: %PARSER-5-CFGLOG_LOGGEDCMD: User:admin logged command:key-string <45>69618: C9300-24T: Apr 7 2023 03:34:39: %PARSER-5-CFGLOG_LOGGEDCMD: User:admin logged command:ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDWO7sikGOBE0wbiSiqDO/niFb0BaceZzExysqqpID+kmhpnIi53nw/o5U4bvZ7wZVkogM31hKimnYKe1irm8uci4W7cVccn4gzVOxZgdfAU6k7fG3H7YWiHiMd8X6WQCyATvb91jhDlC8XnUtyTNhzuiYh30kYMpeCh4tD4NlTMLylagLZyiV/N7qe51TvnjbExC/M/xY/kl+ISTGyaWP/B <45>69619: C9300-24T: Apr 7 2023 03:34:43: %PARSER-5-CFGLOG_LOGGEDCMD: User:admin logged command:tb97nclRDv85p3sFN9uJ8PSfUi9SAZx5kNe0ujrPhv2mYawsbZCYPjRV7ltphpGiPHMCxLZSg5WHlfTGaWlPMWet6g7rAppW8LrXBn+WQyzzICWAv8qxDOCNhmRGMsT root@tl16-16x Remove public key and association with user: <45>69568: C9300-24T: Apr 7 2023 03:26:21: %PARSER-5-CFGLOG_LOGGEDCMD: User:admin logged command:ip ssh pubkey-chain <45>69569: C9300-24T: Apr 7 2023 03:26:47: %PARSER-5-CFGLOG_LOGGEDCMD: User:admin logged command:no username testadmin **Ability to import X509v3 certificates to the TOE's trust store** Import CSR Generated Cert: <45>3170: C9300-24T: Apr 21 2023 04:14:31: %PARSER-5-CFGLOG_LOGGEDCMD: User:admin logged command:crypto pki import rootca-rsa certificate

		<47>3165: C9300-24T: Apr 21 2023 04:14:31: CRYPTO_PKI: pubkey_name : 0~1#0130#011#006#003U#004#006#023#002US1#0130#011#006#003U#004#010#014#002MD1#0240#022#006#003U#004#007#014#013Catonsville1#0140 <47>3166: C9300-24T: #006#003U#004 <47>3167: C9300-24T: #014#003GSS1)0'#006#011*<86>H<86>÷#015#001#011#001#026#032rootca-rsa@gossamersec.com1#0230#021#006#003U#004#003#014 <47>3168: C9300-24T: rootca-rsa <47>3175: C9300-24T: Apr 21 2023 04:14:43: crypto_ca_certificate: saved cert to nvram:rootca-rsa#197.cer [OK] <47>3176: C9300-24T: Apr 21 2023 04:14:43: crypto_ca_certificate: saved cert to nvram:rootca-rsa#1CA.cer [OK]rootca-rsa:unlocked trustpoint rootca-rsa, refcount is 0 **Generate a PSK based CAK and install it in the device** <189>3090: Jun 26 2023 20:03:02: %PARSER-5-CFGLOG_LOGGEDCMD: User:admin logged command:key-string * **Manage the Key Server to create, delete, and activate MKA participants [as specified in 802.1X, sections 9.13 and 9.16 (cf. MIB object ieee8021XKayMkaParticipantEntry) and section. 12.2 (cf. function createMKA())];** Create/Activate: <191>3158: Jun 26 2023 20:03:13: MKA-EVENT: Created New CA 0x80007F603BC25BA8 Participant on interface GigabitEthernet1/0/3 with SCI A0F8.4915.CD83/000B for Peer MAC a0f8.4915.cd83. Delete: <191>4266: Jun 26 2023 20:48:28: MKA-EVENT: Deleting MKA Session on interface GigabitEthernet1/0/3 & Bring-Down-Dot1x is TRUE. **Specify a lifetime of a CAK** <189>5564: Jun 5 2023 17:04:17: %PARSER-5-CFGLOG_LOGGEDCMD: User:admin logged command:lifetime local 13:04:16 Jun 05 2023 duration 600 **Enable, disable, or delete a PSK based CAK using [CLI management commands]** Enable: <189>3090: Jun 26 2023 20:03:02: %PARSER-5-CFGLOG_LOGGEDCMD: User:admin logged command:key-string * Disable/Delete: <189>10019: Jun 29 2023 21:50:45: %PARSER-5-CFGLOG_LOGGEDCMD: User:admin logged command:no key-string

FPT_RPL.1	Detected replay attempt	**Detected replay attempt** <191>6844: Jun 2 2023 19:36:09: MKA-ERR 0015.5d90.160e/0001 B200000D: MKPDU Validation FAIL - Live Peer MN 5 is NOT greater than last received MN 6 and so could be an old/replayed MKPDU.
FPT_STM_EXT.1	Discontinuous changes to time - either Administrator actuated or changed via an automated process.	<46>70061: C9300-24T: Apr 11 2023 05:12:22: %HA_EM-6-LOG: cli_log: User:admin via Port:0 Executed[clock set 10:25:20 15 April 2023] <46>70062: C9300-24T: Apr 15 2023 15:25:20: %SYS-6-CLOCKUPDATE: System clock has been updated from 00:12:22 EST Tue Apr 11 2023 to 10:25:20 EST Sat Apr 15 2023, configured from console by admin on console.
FPT_TUD_EXT.1	Initiation of update. result of the update attempt (success or failure)	**Success:** <46>2883: C9300-24T: May 19 2023 03:18:34: %HA_EM-6-LOG: cli_log: User:admin via Port:0 Executed[install add file activate commit] <45>2884: C9300-24T: May 19 2023 03:18:34: %INSTALL-5-INSTALL_START_INFO: Switch 1 R0/0: install_mgr: Started install add_activate_commit flash:cat9k_iosxe.17.09.02.SPA.bin <45>2888: C9300-24T: May 19 2023 03:21:36: %INSTALL-5-INSTALL_COMPLETED_INFO: Switch 1 R0/0: install_mgr: Completed install add_activate_commit **Failure:** <46>2910: C9300-24T: May 10 2023 05:08:01: %HA_EM-6-LOG: cli_log: User:admin via Port:0 Executed[install add file tftp://172.16.16.250/cat9k_iosxe.17.09.02.SPA-modified_sig.bin activate commit] <45>2911: C9300-24T: May 10 2023 05:08:01: %INSTALL-5-INSTALL_START_INFO: Switch 1 R0/0: install_mgr: Started install add_activate_commit cat9k_iosxe.17.09.02.SPA-modified_sig.bin <43>2912: C9300-24T: May 10 2023 05:08:51: %INSTALL-3-OPERATION_ERROR_MESSAGE: Switch 1 R0/0: install_mgr: Failed to install add_activate_commit package tftp://****/cat9k_iosxe.17.09.02.SPA-modified_sig.bin, Error:
FTA_SSL_EXT.1	The termination of a local session by the session locking mechanism.	<46>69014: C9300-24T: Mar 28 2023 19:56:54: %SYS-6-TTY_EXPIRE_TIMER: (exec timer expired, tty 0 (0.0.0.0)), user admin <46>69015: C9300-24T: Mar 28 2023 19:56:54: %SYS-6-LOGOUT: User admin has exited tty session 0()

FTA_SSL.3	The termination of a remote session by the session locking mechanism.	<46>51528: C9300-24T: Mar 28 2023 00:27:10: %SYS-6-TTY_EXPIRE_TIMER: (exec timer expired, tty 2 (172.16.16.254)), user admin <46>51529: C9300-24T: Mar 28 2023 00:27:10: %SYS-6-LOGOUT: User admin has exited tty session 2(172.16.16.254) <45>51530: C9300-24T: Mar 28 2023 00:27:10: %SSH-5-SSH2_CLOSE: SSH2 Session from 172.16.16.254 (tty = 1) for user 'admin' using crypto cipher 'aes256-cbc', hmac 'hmac-sha2-256' closed
FTA_SSL.4	The termination of an interactive session.	**SSH** <46>2919: C9300-24T: Apr 25 2023 04:25:24: %HA_EM-6-LOG: cli_log: User:admin via Port:1 Executed[exit] <46>2920: C9300-24T: Apr 25 2023 04:25:24: %SYS-6-LOGOUT: User admin has exited tty session 1(172.16.16.254) <45>2921: C9300-24T: Apr 25 2023 04:25:24: %SSH-5-SSH2_CLOSE: SSH2 Session from 172.16.16.254 (tty = 0) for user 'admin' using crypto cipher 'aes256-cbc', hmac 'hmac-sha2-256' closed **Local Console** <46>10916: C9300-24T: Nov 2 2022 03:04:58: %HA_EM-6-LOG: cli_log: User:admin via Port:0 Executed[exit] <46>10917: C9300-24T: Nov 2 2022 03:04:58: %SYS-6-LOGOUT: User admin has exited tty session 0()
FTP_ITC.1	Initiation of the IPsec trusted channel. Termination of the IPsec trusted channel. Failure of the IPsec trusted channel functions	<45>3074: C9300-24T: *Nov 16 2022 12:10:28: %IKEV2-5-SA_UP: SA UP <45>3075: C9300-24T: *Nov 16 2022 12:10:28: %CRYPTO-5-IKEV2_SESSION_STATUS: Crypto tunnel v2 is UP. Peer 192.168.144.254:4500 Id: 192.168.144.254 <47>3160: C9300-24T: *Nov 16 2022 12:10:28: IKEv2:(SESSION ID = 1,SA ID = 1):(SA ID = 1):[IPsec -> IKEv2] Creation of IPsec SA into IPsec database PASSED <47>3185: C9300-24T: *Nov 16 2022 12:10:33: IKEv2:(SESSION ID = 1,SA ID = 1):Deleting SA <45>3186: C9300-24T: *Nov 16 2022 12:10:33: %IKEV2-5-SA_DOWN: SA DOWN <45>3187: C9300-24T: *Nov 16 2022 12:10:33: %CRYPTO-5-IKEV2_SESSION_STATUS: Crypto tunnel v2 is DOWN. Peer 192.168.144.254:4500 Id: 192.168.144.254 See FCS_IPSEC_EXT.1 for Audits associated with failures of IPsec Sessions.

	Initiation of the MACsec trusted channel. Termination of the MACsec trusted channel. Failure of the MACsec trusted channel functions	<191>7188: Jun 5 2023 17:51:13: MKA-EVENT a0f8.4915.cd81/0000 CC00000D: >> FSM - Initializing MKA Session for PSK keychain on interface GigabitEthernet1/0/1 with SCI A0F8.4915.CD81/0009. <189>4199: Jun 26 2023 20:48:18: %MKA-5-SESSION_STOP: (Gi1/0/1 : 9) MKA Session stopped by MKA for RxSCI 0015.5d90.160e/0001, AuditSessionID , CKN 1000 <187>3148: Jun 5 2023 14:43:40: %MKA-3-MKPDU_VALIDATE_FAILURE: (Gi1/0/1 : 9) Validation of a MKPDU failed for RxSCI 0015.5d90.160e/0001, AuditSessionID , CKN 1000
FTP_TRP.1/Admin	Initiation of the SSH trusted path. Termination of the SSH trusted path. Failure of the SSH trusted path functions.	See FIA_UIA_EXT.1 for Audits of successful establishment of SSH sessions. See FTA_SSL.3 and FTA_SSL.4. See FCS_SSHS_EXT.1 for Audits associated with failures of SSH Sessions
FCS_MACSEC_EXT.1	Session establishment; Secure Channel Identifier (SCI)	**Session Establishment** <45>6840: C9300-24T: Jun 1 2023 21:10:54: %MKA-5-SESSION_SECURED: (Gi1/0/1 : 9) MKA Session was secured for RxSCI 0015.5d90.160e/0001, AuditSessionID , CKN 1000
FCS_MACSEC_EXT.3.1	Creation and update of Secure Association Key; Creation and update times	**SAK (Security Association Key) creation** <47>6861: C9300-24T: Jun 1 2023 21:11:09: MKA-EVENT 0015.5d90.160e/0001 1200000D: Generation of new Latest SAK suc-ceeded (Latest AN=1, KN=2)… **SAK (Security Association Key) update** <190>4155: Jun 26 2023 20:47:05: %MKA-6-SAK_REKEY_SUC-CESS: (Gi1/0/1 : 9) MKA Session successfully completed a SAK Rekey (new Latest AN/KN 0/9, Old AN/KN 3/8) for RxSCI 0015.5d90.160e/0001, AuditSessionID , CKN 1000
FCS_MACSEC_EXT.4.4	Creation of Connectivity Association; Connectivity Association Key Names	**Creation of Connectivity Association** <189>3235: Jun 2 2023 12:43:05: %MKA-5-SESSION_SECURED: (Gi1/0/1 : 9) MKA Session was secured for RxSCI 5cb1.2e12.ca01/0008, AuditSessionID , CKN 1000

7. Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see *What's New in Cisco Product Documentation*.

To receive new and revised Cisco technical content directly to your desktop, you can subscribe to the What's New in Cisco Product Documentation RSS feed. The RSS feeds are a free service.

8. Contacting Cisco

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco website at www.cisco.com/go/offices.