Cisco Catalyst 9200CX/9300X/9300LM/9500X Series Switches

CC Configuration Guide

Version: 0.5
Date: November 16, 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 9200CX/9300X/9300LM/9500X 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	January 19, 2023	Initial Version
0.2	July 27, 2023	Updates
0.3	August 25, 2023	Updates
0.4	October 27, 2023	Updates for Checkout Package
0.5	November 16, 2023	Updates to address checkout comments

1. Introduction

This Operational User Guidance with Preparative Procedures documents the administration of the Cisco Catalyst 9200CX/9300X/9300LM/9500X Series Switches 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 9200 Switches Hardware Installation Guide)	https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9200/hardware/install/b-c9200-hig.html
2	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
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	Release Notes for Cisco Catalyst 9200 Series Switches, Cisco IOS-XE Cupertino 17.9.x	https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9200/software/release/17-9/release_notes/ol-17-9-9200.html
5	Release Notes for Cisco Catalyst 9300 Series Switches	https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9300/software/release/17-9/release_notes/ol-17-9-9300.html
6	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
7	Software Configuration Guide, Cisco IOS-XE Cupertino 17.9.x (Catalyst 9200 Switches)	https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9200/software/release/17-9/configuration_guide/b-179-9200-cg.html

8	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
9	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
10	Security Configuration Guide, Cisco IOS XE Cupertino 17.9.x (Catalyst 9200 Switches)	https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9200/software/release/17-9/configuration_guide/sec/b_179_sec_9200_cg.html
11	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
12	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
13	Command Reference, Cisco IOS-XE Cupertino 17.9.x (Catalyst 9200 Switches)	https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9200/software/release/17-9/command_reference/b_179_9200_cr.html
14	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
15	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
16	Cisco IOS Configuration Fundamentals Command Reference	https://www.cisco.com/c/en/us/td/docs/ios/fundamentals/command/reference/cf_book.html
17	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
18	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 9200CX/9300X/9300LM/9500X Series Switches all running Internetworking Operating System (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 TLS.
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.
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.
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.

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.
Telnet	Telnet sends authentication data in plain text. This feature must remain disabled in the evaluated configuration. SSHv2 must be used to secure the trusted path for remote administration for all SSHv2 sessions.
Hypertext Transfer Protocol (HTTP)	HTTP Is not associated with Security Functional Requirements claimed in [NDcPP].

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 server:

- Syslog Server. Any syslog server that can be accessed over TLS 1.2 may be used. Install the syslog server per installation instructions provided with the syslog server software. Preparative Procedures and Operational Guidance for the TOE

3.1.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!
```

3.2. 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. Configure Gigabit Ethernet Management Interface VRF

   Enter: `SWITCH(config)# do show running-config vrf`

   If there was not a Mgmt-vrf automatically created follow the steps below to create one:

```
SWITCH(config)# vrf definition Mgmt-vrf
SWITCH(config-vrf)# address-family ipv4
SWITCH(config-vrf)# exit-address-family
SWITCH(config-vrf)# address-family ipv6
SWITCH(config-vrf)# exit-address-family
SWITCH(config-vrf)# exit
```

7. Provide an initial configuration for the Management Interface. For example:

```
SWITCH(config)# interface GigabitEthernet0/0
SWITCH(config-if)# ip address <IP address> <mask>
SWITCH(config-if)# vrf forwarding Mgmt-vrf
SWITCH(config-if)# no shutdown
SWITCH(config-if)# exit
```

8. Configure a default route to reach the Switch and a default route for the Mgmt-vrf

```
SWITCH(config)# ip route <prefix> <mask> <default gateway/next hop>
SWITCH(config)# ip route vrf Mgmt-vrf <prefix> <mask> <default gateway/next hop>
```

9. Configure the console to require username and password authentication

```
SWITCH(config)# line console 0
SWITCH(config-line)# login authentication default
```

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

3.2.1. 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
```

3.2.2. 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
```

3.2.3. 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.

3.2.4. Generate Logs on Failed Login Attempts

To generate logs for failed login attempts enter

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

3.2.5. 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
```

3.2.6. Generate Logs on Successful Login Attempts

To generate logs for successful login attempts enter

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

3.2.7. Set Syslog Server Logging Level

Set syslog server logging level to debug

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

3.2.8. 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 engine
SWITCH# debug ssl openssl errors
```

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

3.2.9. 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
```

3.2.10. 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
```

3.2.11. 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
```

3.2.12. 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>
```

3.2.13. 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

3.2.14. Session Termination

All sessions at the local console and auxiliary 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>
```

3. Enter the line configuration mode for aux port:

```
SWITCH(config-line)# line aux 0
```

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

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

3.2.15. 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"

3.2.16. 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/software/csws/ws/platform/home?locale=en_US#. Use your Cisco Care Online (CCO) or SMART account and download the 17.09 image.

Table 5. Evaluated Software Images

Platform	Image
Cisco Catalyst 9200CX	cat9k_lite_iosxe.17.09.02.SPA.bin
Cisco Catalyst 9300X/9300LM/9500X	cat9k_iosxe.17.09.02.SPA.bin

3. To update the software, refer to section 4.8 of the this document.

3.2.17. 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 [**10**], [**11**], or [**12**] depending on your TOE model. If you downloaded the entire contents of [**10**] in PDF format the "Configuring Secure Shell" is in Chapter 13. If you downloaded the entire contents of [**11**] or [**12**] in PDF format the "Configuring Secure Shell" is in Chapter 16.

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
```

Note: RSA signature services using 2048 or 3072 key sizes are automatically configured when SSH is configured as instructed in the steps above.

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.

3.2.18. 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
```

3.2.19. TLS – Syslog

TLS is used by the TOE to securely transmit generated audit data to an external syslog server. As described in section 1.5, the TOE requires an Audit (syslog) Server in the IT Environment to which the TOE transmits syslog messages over TLS. The TOE will validate the X.509 certificate presented by the remote syslog server but does not require a X.509 certificate for the TOE itself. The Administrator will need to ensure the remote syslog server is properly configured with a valid X.509 certificate and the CDP (Certificate Distribution Point) for CRL revocation checking is available on the network. If the CDP for CRL revocation checking is unavailable or the remote syslog server is not properly configured with a valid X.509 certificate, the TOE will not establish the connection to the Syslog server. In this case, the Administrator should troubleshoot and resolve the issue before proceeding.

The steps below provide instructions to configure TLS on the TOE.

Note: Before proceeding, the Administrator should determine the TLS 1.2 ciphersuites the TOE should use. The table below lists the configuration option and its associated TLS cipherSuite support:

Table 6. TLS ciphersuites

Configuration Option	Ciphersuite Support
ecdhe-rsa-aes-cbc-sha2	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
ecdhe-rsa-aes-gcm-sha2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
dhe-aes-cbc-sha2	TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
dhe-aes-gcm-sha2	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 TLS_DHE_RSA_WITH_AES_256_GCM_SHA384

3.2.19.1. Create and Configure a Certificate Map

1. Create a certificate-map mode. In step 2 you will configure the reference identifier of the peer syslog server.

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

2. Specify the SAN (alt-subject-name) field together with the matching criteria of 'equal' and the value to match for the remote syslog server. The examples below values to match for peer.cisco.com and the IP address of the peer:

```
SWITCH(ca-certificate-map)# alt-subject-name eq <peer.cisco.com>

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

3. Enter exit to return to main config mode.

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

3.2.19.2. Create, Configure, and Authenticate the Root Trustpoint

4. Create, configure, and authenticate the root trustpoint

   Note: Use a root trustpoint name specific to syslog. For example myrootca-syslog

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

SWITCH(ca-trustpoint)# enrollment terminal pem

SWITCH(ca-trustpoint)# revocation-check none

SWITCH(ca-trustpoint)# match eku server-auth

SWITCH(ca-trustpoint)# exit

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

Enter the 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 TOE should respond with:

"Trustpoint CA certificate accepted."

"% Certificate successfully imported"

3.2.19.3. Create, Configure, and Authenticate the Intermediate Trustpoint

5. Create, configure, and authenticate the intermediate trustpoint:

Note: Use an intermediate trustpoint name specific to syslog. For example mysubca-syslog

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

SWITCH(ca-trustpoint)# match eku server-auth

SWITCH(ca-trustpoint)# exit
```

6. Authenticate the trustpoint

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

Enter the base 64 encoded intermediate 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 Controller should respond with:

"Trustpoint CA certificate accepted."

"% Certificate successfully imported"

7. 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
```

3.2.19.4. Configure a TLS Profile

1. Create a TLS Profile for Syslog

```
SWITCH(config)# logging tls-profile <profile name>
```

2. Configure version of TLS to be 1.2

```
SWITCH(config-tls-profile)# tls-version TLSv1.2
```

3. Configure a ciphersuite using the configuration options column from Table 6

```
SWITCH(config-tls-profile)# ciphersuite <list of ciphersuites>
```

8. Enter exit to return to main config mode.

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

3.2.19.5. Configure DNS Name Server

Note: Using the Management Ethernet interface VRF, ensure your DNS name server contains an entry for the FQDN of the Syslog Server.

```
SWITCH(config)# ip name-server vrf Mgmt-vrf <IP Address of DNS Server>
```

3.2.19.6. Enable Remote Syslog Server

Once TLS 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 using the TLS profile. When an audit event is generated, is it simultaneously sent to the external server and the local store.

If using the reference identifier per RFC 6125 section 6

```
SWITCH(config)# logging host <FQDN of Syslog Server> vrf Mgmt-vrf transport tls profile <TLS Profile>
```

If using IPv4 address in SAN

```
SWITCH(config)# logging host <IP of Syslog Server> vrf Mgmt-vrf transport tls profile <TLS Profile>
```

Note: RSA signature services using 2048 or 3072 key sizes are automatically configured when TLS is configured as instructed in the steps above.

Note: The supported cryptographic algorithms and key strengths are configured implicitly by defining the supported TLS ciphersuites. The TOE presents the Supported Elliptic Curves Extension with NIST curves secp256r1,secp384r1, and secp521r1 in the Client Hello. This behavior is performed by default and there is no security management function to disable it.

Note: The TOE uses X.509v3 certificates to support authentication for TLS connections to a Syslog audit server. The TOE 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. The TOE will also verify the extendedKeyUsage field of the TLS peer certificate contains the

Server Authentication purpose. 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.

3.2.20. 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 GigabitEthernet1

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 **[10], [11], or [12**] depending on your TOE model. If you downloaded the entire contents of [**7**] in PDF format the “Configuring MACsec Encryption” is in Chapter 13. If you downloaded the entire contents of [**8**] in PDF format the “Configuring MACsec Encryption” is in Chapter 14.

Configuration Examples for MACsec Encryption can be found in the "Configuration Examples for MACsec Encryption" section of the "Configuring MACsec Encryption" Chapter of **[10], [11], or [12**] depending on your TOE model. If you downloaded the entire contents of [**10**] in PDF format the “Configuring MACsec Encryption” is in Chapter 12. If you downloaded the entire contents of [**11**] in PDF format the “Configuring MACsec Encryption” is in Chapter 13. If you downloaded the entire contents of [**11**] in PDF format the “Configuring MACsec Encryption” is in Chapter 14.

To verify MACsec is enabled, refer to the “show" commands listed under **Step 2** of Scenario 2 in [**18**].

3.2.21. 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. **Note:** 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.

3.2.22. 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 **[10], [11], or [12**] depending on your TOE model. If you downloaded the entire contents of [**10**] in PDF format the “Secure Operation in FIPS Mode” is in Chapter 33. If you downloaded the entire contents of [**11**] in PDF format the “Secure Operation in FIPS Mode” is in Chapter 36. If you downloaded the entire contents of [**12**] in PDF format the “Secure Operation in FIPS Mode” is in Chapter 40.

4. Operational Guidance for the TOE

4.1. 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#
```

4.2. View Audit Events

Audit events may be viewed at the CLI by entering:

```
SWITCH# show logging
```

4.3. 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>
```

4.4. 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
```

4.5. Zeroize Private Key

Should the Administrator need to zeroize a private key generated as instructed in the SSH 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.

4.6. 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.

4.7. TLS Syslog Server Interruption and Recovery

If the TLS connection to the Syslog Server is unexpectedly interrupted, the TLS client connection will be broken. When the connection is broken no administrative interaction is required. The TLS session will be reestablished once communication to the Syslog Server is available again.

4.8. Update TOE Software

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.

4.8.1. One-Shot 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. To query the currently active software version at the SWITCH console enter:

   ```
   SWITCH# show version
   ```

   d. 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.

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

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

   ```
   SWITCH# show install summary
   ```

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

   Note: Since the update process involves rebooting before an upgrade can be completed, the TOE will cease to pass traffic during the update.

   Note: If you respond with a 'n' the SWITCH software will not be upgraded.

2. 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>
   ```

4.8.2. 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. To query the currently active software version at the SWITCH console enter:

   ```
   SWITCH# show version
   ```

   d. 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 bin image file.

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

e. At the SWITCH console enter: `install add file bootflash: cat9k_lite_iosxe.17.09.02.SPA.bin`

For the 9200CX: `install add file bootflash: cat9k_lite_iosxe.17.09.02.SPA.bin`

For the 9300X/9300LM/9500X: `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.

f. At the SWITCH console enter: `install activate`

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

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

g. 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 running software version as well as the installed but not yet active SWITCH software version by entering the following command at the CLI:

```
SWITCH# show install summary
```

i. To Activate the new image, return to the SWITCH console and respond with a '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.

Note: Since the update process involves rebooting before an upgrade can be completed, the TOE will cease to pass traffic during the update

Note: If you respond with a 'n' the SWITCH software will not be upgraded.

j. 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 on the 9200CX:

```
SWITCH# verify bootflash:cat9k_lite-rpboot.17.09.02.SPA.pkg

SWITCH# verify bootflash:cat9k_lite-rbase.17.09.02.SPA.pkg
```

For example on the 9300X/9300LM/9500X:

```
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>
```

5. 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 7. Sample Audit Events

SFR	Auditable Event and Additional Audit Record Content	Sample Audit Event Data
FAU_GEN.1.1	Startup and Shutdown of Audit Function	<190>2561: C9200CX: *Aug 8 2023 09:13:32: %SYS-6-LOGGINGHOST_STARTSTOP: Logging to host 192.168.144.25 port 6514 started - reconnection <190>2564: C9200CX: *Aug 8 2023 09:14:21: %SYS-6-LOGGINGHOST_STARTSTOP: Logging to host 192.168.144.25 port 6514 stopped - disconnection

FCS_SSHS_EXT.1	Failure to establish an SSH session; Reason for failure	**No matching cipher** <187>351: C9200CX: *Oct 19 2023 16:02:56: %SSH-3-NO_MATCH: No matching cipher found: client aes128-ctr server aes128-cbc,aes256-cbc <189>352: C9200CX: *Oct 19 2023 16:02:56: %SSH-5-SSH2_SESSION: SSH2 Session request from 192.168.144.25 (tty = 0) using crypto cipher '', hmac '' Failed <189>353: C9200CX: *Oct 19 2023 16:02:56: %SSH-5-SSH2_CLOSE: SSH2 Session from 192.168.144.25 (tty = 0) for user '' using crypto cipher '', hmac '' closed **No matching host key type** <187>381: C9200CX: *Oct 19 2023 16:09:01: %SSH-3-NO_MATCH: No matching hostkey algorithm found: client ecdsa-sha2-nistp384 server rsa-sha2-256,rsa-sha2-512 <189>382: C9200CX: *Oct 19 2023 16:09:01: %SSH-5-SSH2_SESSION: SSH2 Session request from 192.168.144.25 (tty = 0) using crypto cipher '', hmac '' Failed <189>383: C9200CX: *Oct 19 2023 16:09:01: %SSH-5-SSH2_CLOSE: SSH2 Session from 192.168.144.25 (tty = 0) for user '' using crypto cipher '', hmac '' closed **No matching MAC** <187>411: C9200CX: *Oct 19 2023 16:13:07: %SSH-3-NO_MATCH: No matching mac found: client hmac-md5 server hmac-sha2-256,hmac-sha2-512 <189>412: C9200CX: *Oct 19 2023 16:13:07: %SSH-5-SSH2_SESSION: SSH2 Session request from 192.168.144.25 (tty = 0) using crypto cipher '', hmac '' Failed <189>413: C9200CX: *Oct 19 2023 16:13:07: %SSH-5-SSH2_CLOSE: SSH2 Session from 192.168.144.25 (tty = 0) for user '' using crypto cipher '', hmac '' closed **No matching key exchange method** <187>423: C9200CX: *Oct 19 2023 16:14:18: %SSH-3-NO_MATCH: No matching kex algorithm found: client ecdh-sha2-nistp384,ext-info-c server diffie-hellman-group14-sha1 <189>424: C9200CX: *Oct 19 2023 16:14:18: %SSH-5-SSH2_SESSION: SSH2 Session request from 192.168.144.25 (tty = 0) using crypto cipher '', hmac '' Failed <189>425: C9200CX: *Oct 19 2023 16:14:18: %SSH-5-SSH2_CLOSE: SSH2 Session from 192.168.144.25 (tty = 0) for user '' using crypto cipher '', hmac '' closed **Oversized Packet** <187>336: C9200CX: *Oct 19 2023 16:02:02: %SSH-3-BAD_PACK_LEN: Bad packet length 65836

FCS_TLSC_EXT.1	Failure to establish an TLS session; Reason for failure	**Invalid Cipher** <191>570: C9200CX: *Oct 20 2023 15:13:35: 0:error:14094410:SSL routines:ssl3_read_bytes:sslv3 alert handshake failure:../VIEW_ROOT/cisco.comp/openssl/src/dist/ssl/record/rec_layer_s3.c:1536:SSL alert number 40 **Invalid EKU** <191>2165: C9200CX: *Oct 20 2023 15:26:56: CRYPTO_OPSSL: EKU check failed for certificate <191>2166: C9200CX: *Oct 20 2023 15:26:56: 0:error:1416F086:SSL routines:tls_process_server_certificate:certificate verify failed:../VIEW_ROOT/cisco.comp/openssl/src/dist/ssl/statem/statem_clnt.c:1921: **Wrong Certificate** <191>2253: C9200CX: *Oct 20 2023 15:27:29: 0:error:1416F17F:SSL routines:tls_process_server_certificate:wrong certificate type:../VIEW_ROOT/cisco.comp/openssl/src/dist/ssl/statem/statem_clnt.c:1965: **Null Ciphersuite** **Server selects different ciphersuite** <191>2337: C9200CX: *Oct 20 2023 15:28:01: 0:error:1421C0F8:SSL routines:set_client_ciphersuite:unknown cipher returned:../VIEW_ROOT/cisco.comp/openssl/src/dist/ssl/statem/statem_clnt.c:1340: **Bad ECDHE Curve** <191>2490: C9200CX: *Oct 20 2023 15:29:06: 0:error:141A417A:SSL routines:tls_process_ske_ecdhe:wrong curve:../VIEW_ROOT/cisco.comp/openssl/src/dist/ssl/statem/statem_clnt.c:2224: **Wrong TLS Version** <191>2574: C9200CX: *Oct 20 2023 15:29:38: 0:error:1425F102:SSL routines:ssl_choose_client_version:unsupported protocol:../VIEW_ROOT/cisco.comp/openssl/src/dist/ssl/statem/statem_lib.c:2087: **Corrupt KEX Message** <191>2654: C9200CX: *Oct 20 2023 15:30:11: 0:error:1416D07B:SSL routines:tls_process_key_exchange:bad signature:../VIEW_ROOT/cisco.comp/openssl/src/dist/ssl/statem/statem_clnt.c:2435: **Modified Finished Message** <191>2745: C9200CX: *Oct 20 2023 15:30:43: 0:error:1416C095:SSL routines:tls_process_finished:digest check

		failed:../VIEW_ROOT/cisco.comp/openssl/src/dist/ssl/statem/statem_lib.c:865: **Plaintext Finished Message** <191>2831: C9200CX: *Oct 20 2023 15:31:16: 0:error:1408F119:SSL routines:ssl3_get_record:decryption failed or bad record mac:../VIEW_ROOT/cisco.comp/openssl/src/dist/ssl/record/ssl3_record.c:677: **Modified Server Hello Nonce** <191>2918: C9200CX: *Oct 20 2023 15:31:48: 0:error:1416D07B:SSL routines:tls_process_key_exchange:bad signature:../VIEW_ROOT/cisco.comp/openssl/src/dist/ssl/statem/statem_clnt.c:2435: **Invalid Identifier** <191>3477: C9200CX: *Oct 20 2023 15:47:37: 0:error:1416F086:SSL routines:tls_process_server_certificate:certificate verify failed:../VIEW_ROOT/cisco.comp/openssl/src/dist/ssl/statem/statem_clnt.c:1921:
FIA_AFL.1	Unsuccessful login attempts limit is met or exceeded; Origin of the attempt (e.g., IP address) Administrator lockout due to excessive authentication failures.	<189>301: C9200CX: Jul 31 2023 20:28:02: %AAA-5-LOCAL_USER_BLOCKED: User admin blocked for login till 16:30:02 EDT Jul 31 2023 <188>302: C9200CX: Jul 31 2023 20:28:04: %SEC_LOGIN-4-LOGIN_FAILED: Login failed [user: admin] [Source: 172.16.16.25] [localport: 22] [Reason: Login Authentication Failed] at 16:28:04 EDT Mon Jul 31 2023

FIA_UIA_EXT.1 FIA_UAU_EXT.2	All use of the authentication mechanism; Origin of the attempt (e.g. IP address).	**SSH Authentication Success – Password** <189>789: C9200CX: *Oct 18 2023 19:37:32: %SEC_LOGIN-5-LOGIN_SUCCESS: Login Success [user: admin] [Source: 172.16.16.25] [localport: 22] at 15:37:32 EDT Wed Oct 18 2023 **SSH Authentication Failure – Password** <188>875: C9200CX: *Oct 18 2023 15:37:09: %SEC_LOGIN-4-LOGIN_FAILED: Login failed [user: pubkeyuser] [Source: 172.16.16.25] [localport: 22] [Reason: Login Authentication Failed] at 11:37:09 EDT Wed Oct 18 2023 **SSH Authentication Success – Public Key** <189>1906: C9200CX: *Oct 18 2023 18:05:46: %SEC_LOGIN-5-LOGIN_SUCCESS: Login Success [user: pubkeyuse] [Source: 172.16.16.25] [localport: 22] at 14:05:46 EDT Wed Oct 18 2023 **SSH Authentication Failure – Public Key** <188>875: C9200CX: *Oct 18 2023 15:37:09: %SEC_LOGIN-4-LOGIN_FAILED: Login failed [user: pubkeyuser] [Source: 172.16.16.25] [localport: 22] [Reason: Login Authentication Failed] at 11:37:09 EDT Wed Oct 18 2023 **Console Authentication Success** <189>290: C9200CX: *Oct 19 2023 12:04:22: %SEC_LOGIN-5-LOGIN_SUCCESS: Login Success [user: admin] [Source: LOCAL] [localport: 0] at 08:04:22 EDT Thu Oct 19 2023 **Console Authentication Failure** <188>875: C9200CX: *Oct 18 2023 15:37:09: %SEC_LOGIN-4-LOGIN_FAILED: Login failed [user: pubkeyuser] [Source: 172.16.16.25] [localport: 22] [Reason: Login Authentication Failed] at 11:37:09 EDT Wed Oct 18 2023
FIA_X509_EXT.1/Rev	Unsuccessful attempt to validate a certificate; Reason for failure Any addition, replacement or removal of trust anchors in the TOE's trust store; Identification of certificates added, replaced or removed as trust anchor in the TOE's trust store	**Absent or invalid basicConstraint flag** <191>8915: C9200CX: Oct 20 2023 17:21:30: CRYPTO_PKI: Remove session revocation service providersgss_rootca-rsa:validation status - CRYPTO_INVALID_CERT <191>8928: C9200CX: Oct 20 2023 17:21:30: 0:error:1416F086:SSL routines:tls_process_server_certificate:certificate verify failed:../VIEW_ROOT/cisco.comp/openssl/src/dist/ssl/statem/statem_clnt.c:1921:

		Revoked Certificate <187>12560: C9200CX: Oct 20 2023 17:31:15: %PKI-3-CERTIFICATE_REVOKED: Certificate chain validation has failed. The certificate (SN: 00D1) is revoked **Corrupt Cert ASN1** <191>20226: C9200CX: Oct 20 2023 17:36:09: 0:error:1416F00D:SSL routines:tls_process_server_certificate:ASN1 lib:../VIEW_ROOT/cisco.comp/openssl/src/dist/ssl/statem/statem_clnt.c:1861: **Corrupt Cert Signature** <191>21612: C9200CX: Oct 20 2023 17:37:13: ../cert-c/source/vericert.c(145) : E_INVALID_SIGNATURE : error verifying digitial signature **Corrupt Public Key** <191>21620: C9200CX: Oct 20 2023 17:37:13: CRYPTO_PKI: (A02BD)chain cert was anchored to trustpoint gss_rootca-rsa, and chain validation result was: CRYPTO_INVALID_CERT **Invalid Certificate Chain** <191>22923: C9200CX: Oct 20 2023 18:06:43: 0:error:1416F086:SSL routines:tls_process_server_certificate:certificate verify failed:../VIEW_ROOT/cisco.comp/openssl/src/dist/ssl/statem/statem_clnt.c:1921: **No cRLSign** <191>17857: C9200CX: Oct 20 2023 17:34:34: CRYPTO_PKI: (A029B) Requesting CRL at http://172.16.8.25/subsubca-no-crl-key-usage-rsa.crl: <191>17679: C9200CX: Oct 20 2023 17:34:29: Key-usage mismatch. Cert does not have cRLSign bit set. **Unreachable Revocation Server** <187>6661: C9200CX: Oct 20 2023 17:04:27: %PKI-3-CRL_FETCH_FAIL: CRL fetch for trustpoint gss_rootca-rsa failed **Certificate expired** <187>10685: C9200CX: Oct 20 2023 17:29:38: %PKI-3-CERTIFICATE_INVALID_EXPIRED: Certificate chain validation has failed. The certificate (SN: 0087) has expired. Validity period ended on 2023-09-05T15:21:00Z **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** <189>360: C9407RSUP2: *Aug 15 2023 15:09:51: %PARSER-5-CFGLOG_LOGGEDCMD: User:admin logged command:banner login c "Warning, this device is for Gossamer use only "c **Ability to configure the session inactivity time before session termination or locking** Console: <189>369: C9200CX: Aug 24 2023 03:31:44: %PARSER-5-CFGLOG_LOGGEDCMD: User:admin logged command:line console 0 <189>371: C9200CX: Aug 24 2023 03:31:47: %PARSER-5-CFGLOG_LOGGEDCMD: User:admin logged command:exec-timeout 0 SSH: <189>852: C9200CX: *Oct 18 2023 19:45:19: %PARSER-5-CFGLOG_LOGGEDCMD: User:admin logged command:line vty 0 15 **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** <189>280: C9200CX: Jul 31 2023 20:24:41: %PARSER-5-CFGLOG_LOGGEDCMD: User:admin logged command:aaa authentication rejected 5 in 120 ban 120 **Ability to modify the behavior of the transmission of audit data to an external IT entity** <189>3913: C9200CX: *Aug 8 2023 12:52:36: %PARSER-5-CFGLOG_LOGGEDCMD: User:admin logged command:no logging host 192.168.144.25 transport tls profile gsstls **Ability to manage the cryptographic keys** Generate Crypto Key for SSH: <189>317: C9200CX: *Oct 15 2023 07:48:24: %PARSER-5-CFGLOG_LOGGEDCMD: User:admin logged command:crypto key generate rsa modulus 2048 label * Delete Crypto Key: <189>1462: C9200CX: *Oct 19 2023 14:34:27: %CRYPTO_ENGINE-5-KEY_DELETED: A key named testkey5 has been removed from key storage <189>1463: C9200CX: *Oct 19 2023 14:34:27: %PARSER-5-CFGLOG_LOGGEDCMD: User:admin logged command:crypto key zeroize rsa * **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: <189>429: C9200CX: *Oct 18 2023 14:43:45: %PARSER-5-CFGLOG_LOGGEDCMD: User:admin logged command:ip ssh server algorithm encryption aes128-cbc aes256-cbc <189>430: C9200CX: *Oct 18 2023 14:43:47: %PARSER-5-CFGLOG_LOGGEDCMD: User:admin logged command:ip ssh server algorithm kex diffie-hellman-group14-sha1 <189>431: C9200CX: *Oct 18 2023 14:43:48: %PARSER-5-CFGLOG_LOGGEDCMD: User:admin logged command:ip ssh server algorithm mac hmac-sha2-256 hmac-sha2-512 <189>432: C9200CX: *Oct 18 2023 14:43:49: %PARSER-5-CFGLOG_LOGGEDCMD: User:admin logged command:ip ssh server algorithm hostkey rsa-sha2-256 rsa-sha2-512 <189>433: C9200CX: *Oct 18 2023 14:43:50: %PARSER-5-CFGLOG_LOGGEDCMD: User:admin logged command:ip ssh server algorithm publickey ssh-rsa Configure TLS: <189>873: C9200CX: *Aug 7 2023 18:04:41: %PARSER-5-CFGLOG_LOGGEDCMD: User:admin logged command:logging tls-profile gsstls <189>874: C9200CX: *Aug 7 2023 18:04:42: %PARSER-5-CFGLOG_LOGGEDCMD: User:admin logged command:ciphersuite ecdhe-rsa-aes-cbc-sha2 ecdhe-rsa-aes-gcm-sha2 dhe-aes-cbc-sha2 dhe-aes-gcm-sha2 **Ability to configure the thresholds for SSH rekeying** <189>328: C9200CX: Aug 24 2023 03:20:50: %PARSER-5-CFGLOG_LOGGEDCMD: User:admin logged command:ip ssh rekey time 10 <189>375: C9200CX: Aug 24 2023 03:32:03: %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** <189>590: C9200CX: *Aug 3 2023 19:35:38: %PARSER-5-CFGLOG_LOGGEDCMD: User:TestUser8240 logged command:username TestUser8240 password * **Ability to configure the reference identifier for the peer** <189>1280: C9200CX: *Oct 19 2023 14:10:46: %PARSER-5-CFGLOG_LOGGEDCMD: User:admin logged command:crypto pki certificate map gsscertmap_dns 1 <189>1283: C9200CX: *Oct 19 2023 14:10:48: %PARSER-5-CFGLOG_LOGGEDCMD: User:admin logged command:alt-subject-name eq tl25-16x.example.com **Ability to manage the TOE's trust store and designate X509.v3 certificates as trust anchors** Create Trustpoint: <190>1110: C9200CX: *Oct 19 2023 13:51:52: %PKI-6-TRUSTPOINT_CREATE: Trustpoint: test2 created succesfully

		<189>1111: C9200CX: *Oct 19 2023 13:51:52: %PARSER-5-CFGLOG_LOGGEDCMD: User:admin logged command:crypto pki trustpoint test2 Import CA Cert: <189>1170: C9200CX: *Oct 19 2023 13:57:31: %PARSER-5-CFGLOG_LOGGEDCMD: User:admin logged command:crypto pki authenticate gss_rootca-rsa **Remove Trustpoint & Certs** <190>1112: C9200CX: *Oct 19 2023 13:52:01: %PKI-6-TRUSTPOINT_DELETE: Trustpoint: test2 deleted succesfully <189>1113: C9200CX: *Oct 19 2023 13:52:01: %PARSER-5-CFGLOG_LOGGEDCMD: User:admin logged command:no crypto pki trustpoint test2 **Ability to manage the trusted public keys database** Configure public key authentication: <189>433: C9200CX: *Oct 18 2023 14:43:50: %PARSER-5-CFGLOG_LOGGEDCMD: User:admin logged command:ip ssh server algorithm publickey ssh-rsa Configure User with public key: <189>837: C9200CX: *Oct 18 2023 15:33:11: %PARSER-5-CFGLOG_LOGGEDCMD: User:admin logged command:ip ssh pubkey-chain <189>840: C9200CX: *Oct 18 2023 15:33:29: %PARSER-5-CFGLOG_LOGGEDCMD: User:admin logged command:username pubkeyuser <189>844: C9200CX: *Oct 18 2023 15:33:35: %PARSER-5-CFGLOG_LOGGEDCMD: User:admin logged command:key-string <189>850: C9200CX: *Oct 18 2023 15:34:29: %PARSER-5-CFGLOG_LOGGEDCMD: User:admin logged command:ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQC2sEMNrw0/bE1RMTDp7LqVyjplqTz657RGOefvoIcOI7XXNVgUonPnfthLBUW2nDSQ4ZxElh2wlwCQhVy1gnAPzUrMhcIxe5GC1UoubmWMv41wH4K7fq/ <189>852: C9200CX: *Oct 18 2023 15:34:37: %PARSER-5-CFGLOG_LOGGEDCMD: User:admin logged command:qSJjsOF3MEJIc4kGg4+CvxGyyulL2FnwCEMUpJikfE+/ycD7zXM9Gzy3XoWlyEbAyj39/putSLS35ErOcMC21BqCybhismyqGOEIVkKIbqhvm2lUbCzmWJzgFna2hzRjTgV1hSiNowqeOT+dEBIu+llM1QjwO6edBaJ28MqUQi/0bVKvgYQiRHl1DZQ1OZVdVUQCK5H+uX8xg+RDo4qFfYxHc87nz268j root@tl25-16x Remove public key and association with user: <189>1083: C9200CX: *Oct 19 2023 13:48:14: %PARSER-5-CFGLOG_LOGGEDCMD: User:admin logged command:ip ssh pubkey-chain <189>1084: C9200CX: *Oct 19 2023 13:48:20: %PARSER-5-CFGLOG_LOGGEDCMD: User:admin logged command:no username pubkeyuser **Generate a PSK based CAK and install it in the device** <189>21831: C9300-24T: Jun 30 2023 00:11:03: %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>28030: C9300-24T: Jun 29 2023 23:43:40: MKA-EVENT: Created New CA 0x80007F81AE53C5D0 Participant on interface GigabitEthernet1/0/3 with SCI A0F8.4915.CD83/000B for Peer MAC a0f8.4915.cd83. Delete: <191>28161: C9300-24T: Jun 29 2023 23:44:57: MKA-EVENT: Deleting MKA Session on interface GigabitEthernet1/0/3 & Bring-Down-Dot1x is TRUE. **Specify a lifetime of a CAK** <189>27268: C9300-24T: Jun 29 2023 23:31:58: %PARSER-5-CFGLOG_LOGGEDCMD: User:admin logged command:lifetime local 19:31:47 Jun 29 2023 duration 600 **Enable, disable, or delete a PSK based CAK using [CLI management commands]** Enable: <189>21831: C9300-24T: Jun 30 2023 00:11:03: %PARSER-5-CFGLOG_LOGGEDCMD: User:admin logged command:key-string * Disable/Delete: <189>21833: C9300-24T: Jun 30 2023 00:11:04: %PARSER-5-CFGLOG_LOGGEDCMD: User:admin logged command:no key-string:
FPT_RPL.1	Detected replay attempt	**Detected replay attempt** <191>25886: C9300-24T: Jun 30 2023 00:32:43: MKA-ERR 0015.5d90.160e/0001 5B00000D: MKPDU Validation FAIL - Live Peer MN 8 is NOT greater than last received MN 15 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.	<190>377: C9200CX: *Oct 13 2023 15:32:28: %HA_EM-6-LOG: cli_log: User:admin via Port:2 Executed[clock set 11:23:18 Oct 13 2023] <190>378: C9200CX: *Oct 13 2023 15:23:18: %SYS-6-CLOCKUPDATE: System clock has been updated from 11:32:28 EDT Fri Oct 13 2023 to 11:23:18 EDT Fri Oct 13 2023, configured from console by admin on vty0 (172.16.16.25).

FPT_TUD_EXT.1	Initiation of update. result of the update attempt (success or failure)	**Success:** <190>1568: C9200CX: *Oct 19 2023 14:58:40: %HA_EM-6-LOG: cli_log: User:admin via Port:0 Executed[install add file ftp://gssftpuser@172.16.16.26/images/cat9k_lite_iosxe.17.09.02.SPA.bin activate commit] <189>1569: C9200CX: *Oct 19 2023 14:58:40: %INSTALL-5-INSTALL_START_INFO: Switch 1 R0/0: install_mgr: Started install add_activate_commit cat9k_lite_iosxe.17.09.02.SPA.bin <189>1572: C9200CX: *Oct 19 2023 15:13:55: %INSTALL-5-INSTALL_COMPLETED_INFO: Switch 1 R0/0: install_mgr: Completed install add_activate_commit **Failure:** <190>703: C9200CX: *Oct 15 2023 03:15:46: %HA_EM-6-LOG: cli_log: User:admin via Port:0 Executed[install add file tftp://172.16.16.26/cat9k_lite_iosxe.17.09.02.SPA-no_sig.bin activate commit] <189>704: C9200CX: *Oct 15 2023 03:15:46: %INSTALL-5-INSTALL_START_INFO: Switch 1 R0/0: install_mgr: Started install add_activate_commit cat9k_lite_iosxe.17.09.02.SPA-no_sig.bin <187>820: C9200CX: *Oct 15 2023 03:31:13: %INSTALL-3-OPERATION_ERROR_MESSAGE: Switch 1 R0/0: install_mgr: Failed to install add_activate_commit package flash:/cat9k_lite_iosxe.17.09.02.SPA-no_sig.bin, Error:
FTA_SSL_EXT.1	The termination of a local session by the session locking mechanism.	<190>361: C9200CX: Aug 24 2023 03:30:51: %SYS-6-TTY_EXPIRE_TIMER: (exec timer expired, tty 0 (0.0.0.0)), user admin <190>362: C9200CX: Aug 24 2023 03:30:51: %SYS-6-LOGOUT: User admin has exited tty session 0()
FTA_SSL.3	The termination of a remote session by the session locking mechanism.	C9200CX: *Oct 18 2023 19:46:35: %SYS-6-TTY_EXPIRE_TIMER: (exec timer expired, tty 2 (192.168.144.25)), user admin <190>866: C9200CX: *Oct 18 2023 19:46:35: %SYS-6-LOGOUT: User admin has exited tty session 2(192.168.144.25) <189>867: C9200CX: *Oct 18 2023 19:46:35: %SSH-5-SSH2_CLOSE: SSH2 Session from 192.168.144.25 (tty = 0) for user 'admin' using crypto cipher 'aes128-cbc', hmac 'hmac-sha2-256' closed
FTA_SSL.4	The termination of an interactive session.	**SSH** <190>792: C9200CX: *Oct 18 2023 19:37:34: %HA_EM-6-LOG: cli_log: User:admin via Port:2 Executed[exit] <190>793: C9200CX: *Oct 18 2023 19:37:34: %SYS-6-LOGOUT: User admin has exited tty session 2(172.16.16.25) <189>794: C9200CX: *Oct 18 2023 19:37:34: %SSH-5-SSH2_CLOSE: SSH2 Session from 172.16.16.25 (tty = 0) for user 'admin' using crypto cipher 'aes128-cbc', hmac 'hmac-sha2-256' closed **Local Console** <190>728: C9200CX: *Oct 18 2023 19:29:00: %HA_EM-6-LOG: cli_log: User:admin via Port:0 Executed[exit] <190>729: C9200CX: *Oct 18 2023 19:29:00: %SYS-6-LOGOUT: User admin has exited tty session 0()

FTP_ITC.1	Initiation of the TLS trusted channel. Termination of the TLS trusted channel. Failure of the TLS trusted channel functions Identification of the initiator and target of failed trusted channels establishment attempt.	<190>913: C9200CX: *Aug 7 2023 18:11:46: %SYS-6-LOGGINGHOST_STARTSTOP: Logging to host 192.168.144.25 port 6514 started - CLI initiated <190>3912: C9200CX: *Aug 8 2023 12:52:36: %SYS-6-LOGGINGHOST_STARTSTOP: Logging to host 192.168.144.25 port 6514 stopped - CLI initiated <187>3914: C9200CX: *Aug 8 2023 12:52:36: %SYS-3-LOGGINGHOST_FAIL: Logging to host 192.168.144.25 port 6514 failed
	Initiation of the MACsec trusted channel. Termination of the MACsec trusted channel. Failure of the MACsec trusted channel functions	Initiation: <191>28035: C9300-24T: Jun 29 2023 23:43:40: MKA-EVENT a0f8.4915.cd83/0000 8300000E: >> FSM - Initializing MKA Session for PSK keychain on interface GigabitEthernet1/0/3 with SCI A0F8.4915.CD83/000B. Termination: <189>27852: C9300-24T: Jun 29 2023 23:41:47: %MKA-5-SESSION_STOP: (Gi1/0/1 : 9) MKA Session stopped by MKA for RxSCI 0015.5d90.160e/0001, AuditSessionID , CKN 1111 Failure: <187>25888: C9300-24T: Jun 30 2023 00:32:43: %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** <188>28082: C9300-24T: Jun 29 2023 23:44:47: %MKA-4-SESSION_UNSECURED: (Gi1/0/1 : 9) MKA Session was stopped by MKA and not secured for RxSCI a0f8.4915.cd81/0000, AuditSessionID , CKN 1000
FCS_MACSEC_EXT.3.1	Creation and update of Secure Association Key; Creation and update times	**SAK (Security Association Key) creation** <190>26053: C9300-24T: Jun 30 2023 00:33:08: %MKA-6-SAK_REKEY: (Gi1/0/3 : 11) MKA Session is beginning a SAK Rekey (current Latest AN/KN 1/6, Old AN/KN 0/5) for RxSCI 0015.5d90.160f/0001, AuditSessionID , CKN 5000 **SAK (Security Association Key) update** <190>26092: C9300-24T: Jun 30 2023 00:33:09: %MKA-6-SAK_REKEY_SUCCESS: (Gi1/0/3 : 11) MKA Session successfully completed a SAK Rekey (new Latest AN/KN 2/7, Old AN/KN 1/6) for RxSCI 0015.5d90.160f/0001, AuditSessionID , CKN 5000
FCS_MACSEC_EXT.4.4	Creation of Connectivity Association; Connectivity Association Key Names	**Creation of Connectivity Association** <188>28082: C9300-24T: Jun 29 2023 23:44:47: %MKA-4-SESSION_UNSECURED: (Gi1/0/1 : 9) MKA Session was stopped by MKA and not secured for RxSCI a0f8.4915.cd81/0000, AuditSessionID , CKN 1000

6. 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.

7. 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.