d

Cisco Catalyst Industrial Ethernet 3200, 3300, 3400, 3400H (IE3x00) Rugged Series Switches running IOS-XE 17.12

CC Configuration Guide

Version: 0.8
Date: May 15, 2024

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 Industrial Ethernet 3200, 3300, 3400, 3400H (IE3x00) Rugged Series Switches running IOS-XE 17.12. 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	06 July 2023	Initial Version
0.2	31 August 2023	Updated IOS-XE version, added IE3K PIDs, added IPsec VTI configurations
0.3	12 December 2023	Update Command Guidance
0.4	6 February 2024	Addressed Lab Comments
0.5	12 March 2024	Addressed Lab Comments
0.6	28 March 2024	Address Lab Comments
0.7	05 April 2024	Updates for Checkout Package
0.8	15 May 2024	Updates to address checkout comments

1. Introduction

This Operational User Guidance with Preparative Procedures documents the administration of the Cisco Catalyst Industrial Ethernet 3200, 3300, 3400, 3400H (IE3x00) Rugged Series Switches running IOS-XE 17.12TOE, as it was certified under Common Criteria. The TOE may be referenced below as the CAT IE3K 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, see **Table 1 Cisco Documentation**. All security relevant commands to manage the TSF data are provided within this documentation within each functional section.

1.3. Supported Hardware and Software

Only the following hardware and software listed below is compliant with the IE3x00 Series Switches running IOS-XE 17.12 NDcPPv2.2e evaluation. Using hardware not specified invalidates the secure configuration. Likewise, using any software version other than the evaluated software listed below will invalidate the secure configuration.

3200 Series

- IE-3200-8T2S,
- IE-3200-8P2S

3300 Series

- IE-3300-8T2S
- IE-3300-8P2S
- IE-3300- 8T2X
- IE-3300- 8U2X

3400 Series

- IE-3400-8T2S
- IE-3400-8P2S

3400H Series

- IE-3400H-8FT
- IE-3400H-8T
- IE-3400H-16FT
- IE-3400H-16T
- IE-3400H-24FT
- IE-3400H-24T

1.4. Supported Configurations

The TOE is comprised of both software and hardware. The hardware is comprised of the following: IE3x00 Series Switches. The software is comprised of the Universal Cisco Internet Operating System (IOS) software image Release IOS-XE 17.12. The IE3x00 Series Switches running IOS-XE 17.12 that comprise the TOE have common hardware characteristics. These characteristics affect only non-TSF relevant functions of the switches (such as throughput and amount of storage) and therefore support security equivalency of the switches in terms of hardware.

The IE3x00 Series Switches primary features include the following:

- Central processor that supports all system operations;
- Dynamic memory, used by the central processor for all system operation;
- x86 CPU complex with minimum, based on model of 2 GB memory;
- Flash memory (EEPROM), used to store the Cisco IOS-XE image (binary program);
- Non-volatile read-only memory (ROM) is used to store the bootstrap program and power-on diagnostic programs and
- Non-volatile random-access memory (NVRAM) is used to store switch configuration parameters that are used to initialize the system at start-up.
- Physical network interfaces (minimally two) (e.g., RJ45 serial and standard 10/100/1000 Ethernet ports). Some models have a fixed number and/or type of interfaces; some models have slots that accept additional network interfaces;
- Dedicated management port on the switch, RJ-45 console port and a USB mini-Type B console connection;
- Built for harsh environments and temperature ranges, fanless, convection-cooled with no moving parts for extended durability and hardened for vibration, shock and surge, and electrical noise immunity.

Cisco IOS-XE is a Cisco-developed highly configurable proprietary operating system that provides for efficient and effective routing and switching. Although IOS-XE performs many networking functions, this TOE only addresses the functions that provide for the security of the TOE itself as described in this document.

1.5. 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 IE3x00 Rugged Series Switches Hardware Installation Guide --- Product Overview	https://www.cisco.com/c/en/us/td/docs/switches/lan/cisco_ie3X00/Hardware/installation/guide/b_ie3x00_hig/b_ie2k-ip67-hig_chapter_01.html
2	Cisco Catalyst IE3x00 Rugged Series Switches Hardware Installation Guide --- Switch Installation	https://www.cisco.com/c/en/us/td/docs/switches/lan/cisco_ie3X00/Hardware/installation/guide/b_ie3x00_hig/b_ie2k-ip67-hig_chapter_010.html
3	Cisco Catalyst IE3x00 Rugged Series Switches Hardware Installation Guide --- Technical Specifications	https://www.cisco.com/c/en/us/td/docs/switches/lan/cisco_ie3X00/Hardware/installation/guide/b_ie3x00_hig/b_ie2k-ip67-hig_chapter_0110.html
4	Cisco Catalyst IE3x00 Rugged Series Switches Hardware Installation Guide --- Express Setup	https://www.cisco.com/c/en/us/td/docs/switches/lan/cisco_ie3X00/Hardware/installation/guide/b_ie3x00_hig/m_HIGEXPRESS_ie3x00.html
5	Cisco Catalyst IE3x00 Rugged Series Switches Hardware Installation Guide --- Configuring the Switch with the CLI Setup Program	https://www.cisco.com/c/en/us/td/docs/switches/lan/cisco_ie3X00/Hardware/installation/guide/b_ie3x00_hig/m_HGCLISET.html
6	Cisco Catalyst IE3x00 Rugged Series Switches Hardware Installation Guide --- Cable and Connectors	https://www.cisco.com/c/en/us/td/docs/switches/lan/cisco_ie3X00/Hardware/installation/guide/b_ie3x00_hig/HIGCABLE.html
7	Command Reference, Cisco IOS XE Dublin 17.12.x (Catalyst 9300 Switches)	https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9300/software/release/17-12/command_reference/b_1712_9300_cr.html

#	Title	Link
8	Security Configuration Guide, Cisco Catalyst IE3x00 and IE3100 Rugged, IE3400 Heavy Duty, and ESS3300 Series Switches	https://www.cisco.com/c/en/us/td/docs/switches/lan/cisco_ie3X00/software/17_3/b_security_17-3_iot_switch_cg.html
9	Programmability Command Reference, Cisco IOS XE Dublin 17.12.x	https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/prog/command/1712/b_1712_programmability_cr.html
10	System Message Guide for Cisco IOS XE Dublin 17.12.x	https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/17_xe/syslogs/17-12-x/b-system-message-guide-17-12-x.html

1.6. TOE Overview

The Cisco Catalyst Industrial Ethernet 3200, 3300, 3400, 3400H (IE3x00) Rugged Series Switches running IOS-XE 17.12TOE provides a rugged secure switching infrastructure for use in industrial environments.

1.7. 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 IPsec. The syslog audit server is used for remote storage of audit records that have been generated by and transmitted from the TOE. The syslog server will need to act as an IPsec peer or as an IPsec endpoint.
Certification Authority (CA)	This includes any IT Environment Certification Authority on the TOE network. This can be used to provide the TOE with a valid certificate during certificate enrollment.
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.
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.

1.8. Excluded Functionality

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

Table 3. Excluded Functionality and Rationale

Function Excluded	Rationale
HTTP/HTTPS	Remote Management is performed using SSH
SNMP	Remote Management is performed using SSH
Other cryptographic engines	The TOE leverages the IOS Common Cryptographic Module (IC2M) Rel5a to provide cryptography in support of other TOE security functionality. No other cryptographic engine or module has been evaluated or tested in the CC evaluation.

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 v2.2e. The excluded functionality does not affect the TOE's conformance to the claimed Protection Profile.

Warning: As noted in Table 3, 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 IPsec may be used. Install the syslog server per installation instructions provided with the syslog server software.

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 is prompted to enter the initial configuration dialog. Enter `no` and confirm you would like to terminate autoinstall, `yes`. The CC Configuration uses 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 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: “!”, “@”, “#”, “$”, “%”, “^”, “&”, “*”, “(“, “)

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)# no shutdown

SWITCH(config-if)# exit
```

6. Configure a default route to reach the Switch

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

   Configure the console to require username and password authentication

   ```
   SWITCH(config)# line console 0

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

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

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. 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
```

4.2.3. 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. To set the logging ID to the hostname, run:

   ```
   SWITCH(config)#logging origin-id hostname
   ```

3. Enter archive config mode

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

4. Enter logging config sub-mode

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

5. Enable the config logger

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

6. Suppress password when displaying logged commands

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

7. 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>
   ```

8. Enable sending of logged commands to remote syslog server

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

9. Exit configuration mode and return to privileged EXEC mode

   ```
   SWITCH(config-archive-log-cfg)# 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- 67108864> 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 15000000

```
    SWITCH(config)# logging buffer 15000000
```

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 Switch 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 is 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 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>
```

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:

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 pre-installed image shipped with the TOE may not be the CC validated version of **ie31xx-universalk9.17.12.02.SPA.bin**. Follow the steps below to verify if you have the CC validated version.

1. Enter show version and verify the version is 17.12

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

2. If the version is not 17.12 you will need to obtain the 17.12 software image. Navigate to Cisco Software Central at https://software.cisco.com. Use your Cisco Care Online (CCO) or SMART account and download the 17.12 image.

3. To update the software, refer to section 5.7 of 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.

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 an RSA crypto key for SSH. Assign a label such as `SSH-KEY`:

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

Note: Only one set of keys can be configured using the **crypto key generate** command at a time. Repeating the command overwrites the old keys. If the configuration is not saved to NVRAM with a "**copy run start**", the generated keys are lost on the next reload of the switch.

4. Assign the key pair to SSH:

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

5. Enable SSHv2. This denies use of SSHv1:

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

SSH must be configured to require use of as a minimum, Diffie-Hellmann group 14, ECDH-sha2-nistp256, ECDH-sha2-nistp384. IOS allows the required DH groups to be specified by their modulus size. The default is modulus 1024 (DH Group 1). To require use of DH Group 14, specify a minimum modulus size of 2048 using the following command:

```
ip ssh dh min size 2048
```

In addition, configure your ssh client for dh-group-14, ECDH-sha2-nistp256 and ECDH-sha2-nistp384, in Putty, configure the SSH client to support only diffie-hellman-group14-sha1 key exchange. To configure Putty, do the following:

- Go into Putty Configuration Select > Connection > SSH > Kex;
- Under Algorithm selection policy: move Diffie-Hellman group 14 to the top of the list;
- Move the "warn below here" option to right below DH group14

When SSHv2 is enabled, the TOE can be configured to limit the algorithms and ciphers that can be used for the secure SSH connection

6. Configure the SSH Server Key Exchange:

```
SWITCH(config)# ip ssh server algorithm kex diffie-hellman-group14-sha1 ecdh-sha2-nistp256
ecdh-sha2-nistp384
```

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 as the authentication method:

   ```
   SWITCH(config)# ip ssh server algorithm authentication publickey
   ```

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

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

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

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

   d. Enter public-key configuration mode:

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

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

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

   f. Enter public-key data configuration mode:

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

   g. 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>
   ```

   h. 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. To configure Password as the authentication method for SSH:

```
SWITCH(config)# ip ssh server algorithm authentication password
```

13. 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: aes256-cbc, aes128-cbc
    - MAC Algorithms: hmac-sha2-512, hmac-sha2-256
    - KEX Algorithms: diffie-hellman-group14-sha1, ecdh-sha2-nistp256, ecdh-sha2-nistp384

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

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

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

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

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

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

17. Type Exit

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

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

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

19. Specify the vty lines to use only SSH

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

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

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

21. Exit configuration mode and return to privileged EXEC mode

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

22. 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.

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 Overview

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 is provided with a syslog server operating as an IPsec peer of the TOE and the records tunneled over that connection.

The TOE allows all privileged administrators to configure Internet Key Exchange (IKE) and IPsec policies. IPsec provides the following network security services:

- Data confidentiality--The IPsec sender can encrypt packets before transmitting them across a network.
- Data integrity--The IPsec receiver can authenticate packets sent by the IPsec sender to ensure that the data has not been altered during transmission.
- Data origin authentication--The IPsec receiver can authenticate the source of the sent IPsec packets. This service is dependent upon the data integrity service.
- Anti-replay--The IPsec receiver can detect and reject replayed packets.

IPsec provides secure tunnels between two peers, such as two switches. The privileged 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 peer recognizes a sensitive packet, the peer sets up the appropriate secure tunnel and sends the packet through the tunnel to the remote peer.

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.

With IPsec, privileged administrators can define the traffic that needs to be protected between two IPsec peers by configuring an IPsec VTI and IP route entries. The IP route command is used to determine the traffic that needs to be protected by IPsec, not the traffic that should be blocked or permitted through the interface. Multiple IP route commands can be used for different subnets.

The IP route entries are searched in a sequence--the switch attempts to match the packet to the subnet specified in that entry, for example:

- Traffic matching an ip route entry in the VTI configuration would flow through the IPsec tunnel and be classified as PROTECTED.
- Traffic that does not match an ip route entry and does not match a non-crypto permit ACL on the interface or a non-crypto permit ACL on another interface not specified in the VTI configuration would be DISCARDED.
- Traffic that traverses an interface not specified in the VTI configuration and matches a non-crypto permit ACL on that interface would be allowed to BYPASS the tunnel. For example, management plane traffic.

When a packet matches a permit entry in a particular IP route entry, and the corresponding IPSec Policy, connections are established, if necessary. If the IP route entry is tagged in the IPSec Policy, 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 IPSec Policy as well as the data flow information from the specific IP route 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 IP route entry 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.

IP route entries associated with the IPsec Policy also represent the traffic that the switch needs protected by IPsec. Inbound traffic is processed against an ip route entry --if an unprotected packet matches a permit entry in a particular subnet associated with the IPsec Policy, that packet is dropped because it was not sent as an IPsec-protected packet.

The IPsec Policy also includes 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.

4.2.21. Configuration of IPsec

SSH must be used for remote administration, IPsec tunnels are used for the transmission of audit records to the syslog server. To ensure the IPsec tunnels will be consistent with the evaluated configuration, use parameters as described in this section. Configuring IPsec tunnels requires configuration of the following elements:

- **Layer-3 Interfaces:** IP-enabled interfaces that can be local tunnel endpoints.
- **Route Entries:** Route entries list the routes to particular network destination.
- **IKEv2 Transforms:** Administratively-specified parameters to be permitted during IKE SA negotiation (see tables below for permitted parameters).
- **IKEv2 Transform Sets:** Administratively named sets of IKEv2 Transforms that can be applied within the IPsec Policy.
- **IPsec Transforms:** Administratively-specified parameters to be permitted during IPsec SA negotiation (see tables below for permitted parameters).

Sample IPsec VTI Configuration:

1. Enable privileged EXEC mode:

```
SWITCH> enable
```

2. Enter global configuration mode:

```
SWITCH# configure terminal
```

3. Configure transform set:

```
SWITCH(config)# crypto ipsec transform-set TSET esp-aes 256 esp-sha256-hmac
```

```
    mode tunnel
```

4. Configure IPsec profile:

```
SWITCH(config)# crypto ikev2 profile PROF
    match identity remote address 192.0.2.2 255.255.255.255
    authentication remote rsa-sig
    authentication local rsa-sig
    lifetime 86400
      !

SWITCH(config)# crypto ipsec profile PROF
    set transform-set TSET
    set ikev2-profile PROF
```

5. Configure interface:

```
SWITCH(config)# interface GigabitEthernet0/0/0
    ip address 192.0.2.1 255.255.255.
```

6. Configure IPsec VTI:

```
SWITCH(config)# interface Tunnel0
   ip address 100.0.2.1 255.255.255.252
   tunnel source GigabitEthernet0/0/0
   tunnel mode ipsec ipv4
   tunnel destination 192.0.2.2
   tunnel protection ipsec profile PROF
```

7. Configure logging with the syslog server IP address and subnet mask:

```
SWITCH(config)# logging host 192.3.3.3
SWITCH(config)# logging source-interface Tunnel0
```

8. Configure route to the Syslog server:

```
SWITCH(config)# ip route 192.0.2.0 255.255.255.0 Tunnel0
```

9. Verify IPsec VTI with these commands:

```
SWITCH# show crypto session
SWITCH# show interface tunnel0
SWITCH# show ip route
```

4.2.22. Security Policy Database (SPD)

RFC 4301 calls for an IPsec implementation to protect IP traffic using 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).

- Traffic matching an ip route entry in the VTI configuration would flow through the IPsec tunnel and be classified as PROTECTED.
- Traffic that does not match an ip route entry and does not match a non-crypto permit ACL on the interface or a non-crypto permit ACL on another interface not specified in the VTI configuration would be DISCARDED.
- Traffic that traverses an interface not specified in the VTI configuration and matches a non-crypto permit ACL on that interface would be allowed to BYPASS the tunnel. For example, management plane traffic.

4.2.23. IKEv2 and Transform Sets

This section discusses IKEv2 and transform sets which requires configuring an IKEv2 Proposal, Transform Set, 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 or PRF algorithms, and a DH group configured.

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

   c. Set the encryption algorithm(s) for the proposal. Choose one or both of the following:

   ```
   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.

   IPsec transform sets are configured in the next section.

   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 Transform Set for IPsec ESP encryption and integrity. Also ensure only tunnel mode is configured. The choices for encryption are **esp-aes 128 or esp-aes-256**. The choices for intergrity are **HMAC-SHA-1, HMAC-SHA-256, HMAC-SHA-512.** Below are two examples:

   a. To configure IPsec ESP to use AES-CBC-128 with HMAC-SHA-1 use the following command:

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

   b. To configure IPsec ESP to use AES-CBC-256 with HMAC-SHA-256 use the following command:

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

   Replace <tag> with a name for the defined transform set.

   c. Tunnel mode is the default mode for all IKE connections. While in the configuration mode for transform sets, ensure only tunnel mode is configured with the following:

   ```
   SWITCH(cfg-crypto-trans) mode tunnel
   ```

3. Configure the IKEv2 Policy

d. Define the IKEv2 policy name.

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

e. Specify the proposal created in the previous section

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

f. Enter exit to return to the main configuration mode

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

4. 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>
```

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

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

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

h. 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 “)”).

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

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

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

5. 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 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- 2592000>
    ```

    g. Enter exit to return to the main configuration mode

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

6. Configure the IPsec Profile which will be used to specify the transform set(s) and IKEv2 profile.

    a. Create the IPsec Profile

    ```
    SWITCH(config)# crypto ipsec <profile>
    ```

    b. Specify the Transform Set(s) created in Step 2

    ```
    SWITCH(ipsec-profile)# set transform-set < list of transform sets in priority order>
    ```

    c. Specify the IKEv2 Profile created in Step 5

    ```
    SWITCH(ipsec-profile)# set ikev2-profile <profile name>
    ```

4.2.24. IPsec SA Lifetimes

To change the time value to 8 hours as claimed in the Security Target, the “crypto ipsec security-association lifetime” command can be used as specified below:

```
SWITCH(config)# crypto ipsec security-association lifetime seconds <120-2592000>
```

To specify the IPsec SA lifetime in kilobytes encrypted use the command below specifying a value from the allowable range:

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

This functionality is available to the Privileged Administrator. Configuration of VPN settings is restricted to the privileged administrator.

4.2.25. Generating a Crypto Key Pair for IPsec

1. In privileged EXEC mode, enter configure terminal:

```
SWITCH# configure terminal
```

2. The Administrator will need to generate a RSA key. Assign a label such as IPSEC-KEY

```
SWITCH(config)# crypto key generate rsa general modulus <2048 | 3072> label IPSEC-KEY
```

4.2.26. 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 as described below in sections 4.2.30, once the revocation server is back online.

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.

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

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
```

4.2.27. 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. PKI trustpoints can be associated with certificate maps, and the TOE will determine if they are valid during IKE authentication.

Table 5 Reference Identifier Configuration

Sequence	Command	Action
Step 1	(config)# **crypto pki certificate map** *label sequence-number*	Starts certificate-map mode
Step 2	*(ca-certificate-map)#* **alt-subject-name eq** < peer.FQDN> eg alt-subject-name eq <peer.cisco.com>	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.
Step 3	(ca-certificate-map)# **exit**	Exits ca-certificate-map mode.
Step 4	For IKEv2: (config)# crypto pki trustpoint < subordinate trustpoint name> (config-ikev2-profile)# match certificate *<attribute map tag>* (config ikev2-profile)#end	Associate the certificate map to the IPsec trustpoint

4.2.28. 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>
```

4.2.29. 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.

4.2.30. 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, it is simultaneously sent to the external server and the local store.

To ensure that the TOE will initiate the IPsec connection to the remote syslog server:

```
SWITCH(config)# logging source-interface <interface-name and number>
```

To configure a remote syslog server enter the following command:

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

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

A locked user account may be unblocked by a privileged administrator by using this command:

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

You can enter a single username, or you can enter `all` to specify all locked users are to be unblocked.

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 and 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. 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.

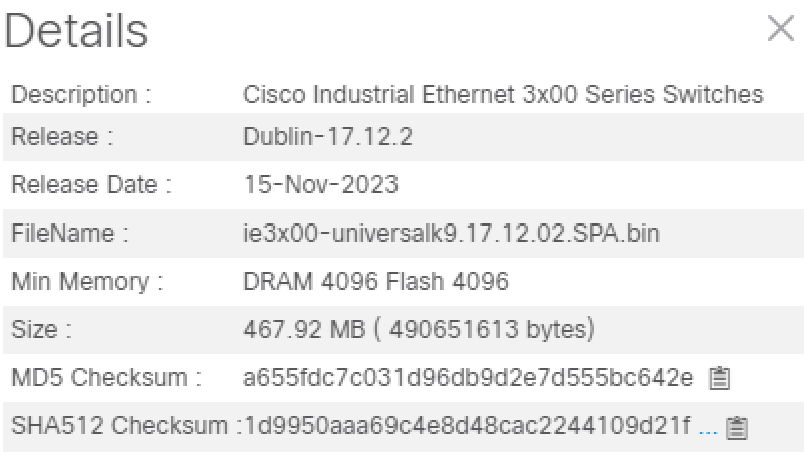
5.7.1. One-Shot Upgrade

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 17.12 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. Use a hash utility to verify that the software image has not been tampered by calculating the hash of the image then compare it with the image at Cisco Software Central. For the TOE image and every TOE update image available for download at Cisco Software Central, there is an associated SHA-512 hash that has been computed at the time of image creation. This hash can be viewed by hovering over the image name. A "Details" pane appears, and the last item listed is the SHA-512 checksum. Below is an example of the "Details" pane:



Details

Description :	Cisco Industrial Ethernet 3x00 Series Switches
Release :	Dublin-17.12.2
Release Date :	15-Nov-2023
FileName :	ie3x00-universalk9.17.12.02.SPA.bin
Min Memory :	DRAM 4096 Flash 4096
Size :	467.92 MB (490651613 bytes)
MD5 Checksum :	a655fdc7c031d96db9d2e7d555bc642e
SHA512 Checksum :	1d9950aaa69c4e8d48cac2244109d21f ...

a. Use a hash utility to calculate the hash of the image.

b. Compare the result with the SHA-512 hash associated with the image at Cisco Software Central.

c. If the hash values match, proceed with installing the image. If the hash values do not match do not install the image and contact Cisco Technical Support. Refer to the Contact Cisco section of this document.

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

```
SWITCH# show version
```

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 begins.

e. The SWITCH console responds

```
This operation may require a reload of the system. Do you want to proceed? [y/n]”
```

f. Respond with a `y` to the prompt. The SWITCH commits the new image, saves the configuration, and reloads.

Note: Since the update process involves rebooting before an upgrade can be completed, the TOE does not pass traffic during the update.

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

5.7.2. Multi-Stage Upgrade

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

a. You will need to obtain an updated 17.12 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. Copy the image to the bootflash partition. (Note this will copy the image but not install it). At the SWITCH console enter:

```
SWITCH# copy tftp bootflash:
```

The SWITCH prompts for address or name of remote host.

d. Enter the IP address of your TFTP Sever.

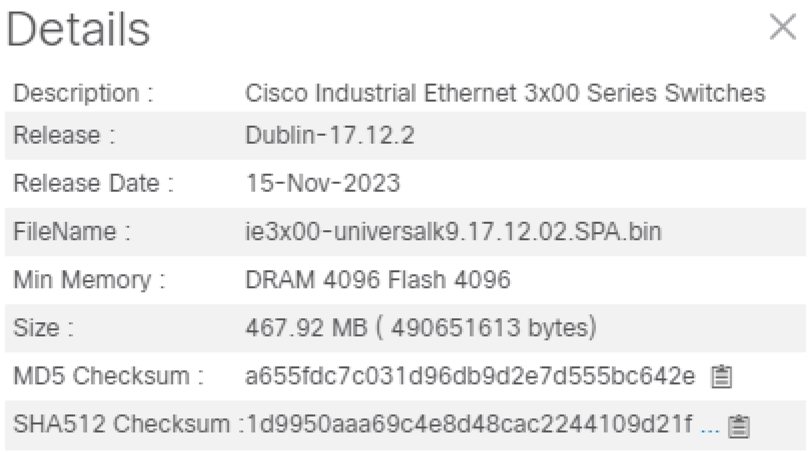
Once the image has successfully downloaded, the Predownload Status will change to “Complete.”
The SWITCH prompts for Source filename.

e. Enter the name of the bin image file.

The SWITCH begins loading the image via TFTP to bootflash

f. Verify that the software image has not been tampered. For the TOE image and every TOE update image available for download at Cisco Software Central, there is an associated SHA-512 hash that has been computed at the time of image creation. This hash can be viewed by hovering over the image name. A “Details” pane appears, and the last item listed is the SHA-512 checksum.

Below is an example of the “Details” pane:



Details

Description :	Cisco Industrial Ethernet 3x00 Series Switches
Release :	Dublin-17.12.2
Release Date :	15-Nov-2023
FileName :	ie3x00-universalk9.17.12.02.SPA.bin
Min Memory :	DRAM 4096 Flash 4096
Size :	467.92 MB (490651613 bytes)
MD5 Checksum :	a655fdc7c031d96db9d2e7d555bc642e
SHA512 Checksum :	1d9950aaa69c4e8d48cac2244109d21f ...

a. Use the **verify /sha512** command to verify the hash on the image

i. For example: verify /sha512 ie3x00-universalk9.17.12.02.SPA.bin

b. Compare the result with the SHA-512 hash associated with the image at Cisco Software Central.

c. If the hash values match, proceed with installing the image. If the hash values do not match do not install the image and contact Cisco Technical Support. Refer to the Contact Cisco section of this document.

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

```
SWITCH# show version
```

h. At the SWITCH console enter:

```
install add file bootflash:ie3x00-universalk9.17.12.02.SPA.bin
```

The SWITCH begins installing the image file, and responds the image was successfully added and displays the version.

i. At the SWITCH console enter:

```
install activate
```

The SWITCH responds

```
System configuration has been modified.

Press Yes(y) to save the configuration and proceed? [y/n]
```

j. Respond `y` to the prompt.

Note: Since the update process involves rebooting before an upgrade can be completed, the TOE does not pass traffic during the update.

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

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

k. After the SWITCH has reloaded, access the CLI console and enter:

```
SWITCH# install commit
```

The SWITCH responds that it has successfully committed the package.

l. 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.

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 and Additional Audit Record Content	Sample Audit Event Data
FAU_GEN.1.1	Startup and Shutdown of Audit Function	**Startup of Audit** Jan 25 2024 20:01:50: %SYS-5-RESTART: System restarted -- Cisco IOS Software [Dublin], IE3x00 Switch Software (IE3x00-UNIVERSALK9-M), Version 17.12.2, RELEASE SOFTWARE (fc2) Technical Support: http://www.cisco.com/techsupport Copyright (c) 1986-2023 by Cisco Systems, Inc. Compiled Tue 14-Nov-23 05:57 by mcpre <46>438: IE3200: *Jan 25 2024 20:02:03: %SYS-6-LOGGINGHOST_STARTSTOP: Logging to host 192.168.145.46 port 514 started - reconnection **Shutdown of Audit** <46>1923: IE3200: Jan 18 2024 03:59:06: %HA_EM-6-LOG: cli_log: User:admin via Port:0 Executed[reload] <45>1924: IE3200: Jan 18 2024 03:59:09: %SYS-5-RELOAD: Reload requested by admin on console. Reload Reason: Reload Command.

FCS_IPSEC_EXT.1	Failure to establish an IPsec SA with reason for failure.	**Failed to find matching policy (General)**
		`<47>3536: IE3200: Jan 18 2024 06:28:04: IKEv2:(SESSION ID = 22,SA ID = 1):Received Packet [From 192.168.144.46:500/To 192.168.144.168:500/VRF i0:f0]`
		`<43>3685: IE3200: Jan 18 2024 06:28:10: %IKEV2-3-NEG_ABORT: Negotiation aborted due to ERROR: Failed to find a matching policy`
		
		Invalid transform proposal received (bad ESP cipher)
		`<47>2213: IE3200: Jan 18 2024 06:22:15: IKEv2:(SESSION ID = 22,SA ID = 1):Received Packet [From 192.168.144.46:500/To 192.168.144.168:500/VRF i0:f0]`
		`<47>2420: IE3200: Jan 18 2024 06:22:20: IPSEC(ipsec_process_proposal): invalid transform proposal received:`
		`<47>2421: IE3200:     {esp-aes 192 esp-sha-hmac }`
		`<47>2424: IE3200: Jan 18 2024 06:22:20: IKEv2-ERROR:(SESSION ID = 23,SA ID = 1):Received Policies: : Failed to find a matching policyESP: Proposal 1:  AES-CBC-192 SHA96 Don't use ESN`
		
		Failed to find matching proposal (bad IKE cipher)
		`<47>3139: IE3200: Jan 18 2024 06:24:31: IKEv2:Received Packet [From 192.168.144.46:500/To 192.168.144.168:500/VRF i0:f0]`
		`<47>3154: IE3200: Jan 18 2024 06:24:31: IKEv2-ERROR:(SESSION ID = 24,SA ID = 1):Received Policies: : Failed to find a matching policyProposal 1:  AES-CBC-192 SHA1 SHA96 DH_GROUP_2048_MODP/Group 14`
		`<47>3155: IE3200: Jan 18 2024 06:24:31: IKEv2-ERROR:(SESSION ID = 24,SA ID = 1):Expected Policies: : Failed to find a matching policyProposal 1:`
		`<47>3156: IE3200:  AES-CBC-128 AES-CBC-256 SHA1 SHA256 SHA512 SHA96 SHA256 SHA512 DH_GROUP_2048_MODP/Group 14`
		`<47>3157: IE3200: Jan 18 2024 06:24:31: IKEv2-ERROR:(SESSION ID = 24,SA ID = 1):: Failed to find a matching policy`
		`<47>3158: IE3200: Jan 18 2024 06:24:31: IKEv2:(SESSION ID = 24,SA ID = 1):Sending no proposal chosen notify`
		
		Failed to validate certificate (Bad Reference Identifier)
		`<47>8084: IE3200: Jan 18 2024 06:50:15: IKEv2:Received Packet [From 192.168.144.46:500/To 192.168.144.168:500/VRF i0:f0]`
		`<43>8299: IE3200: Jan 18 2024 06:50:16: %PKI-3-CERTIFICATE_INVALID_UNAUTHORIZED: Certificate chain validation has failed. Unauthorized`
		`<47>8303: IE3200: Jan 18 2024 06:50:16: IKEv2:(SESSION ID = 32,SA ID = 1):Verification of peer's authentication data FAILED`

FCS_SSHS_EXT.1	Failure to establish an SSH session;
	Reason for failure
		No matching cipher
		`<43>24440: IE3200: Dec 13 2023 02:51:05: %SSH-3-NO_MATCH: No matching cipher found: client aes128-gcm@openssh.com server aes128-cbc,aes256-cbc`
		`<45>24441: IE3200: Dec 13 2023 02:51:05: %SSH-5-SSH2_SESSION: SSH2 Session request from 172.16.16.46 (tty = 0) using crypto cipher '', hmac '' Failed`
		`<45>24442: IE3200: Dec 13 2023 02:51:05: %SSH-5-SSH2_CLOSE: SSH2 Session from 172.16.16.46 (tty = 0) for user '' using crypto cipher '', hmac '' closed`
		
		No matching host key type
		`<43>24461: IE3200: Dec 13 2023 02:55:56: %SSH-3-NO_MATCH: No matching hostkey algorithm found: client x509v3-ssh-rsa server rsa-sha2-256,rsa-sha2-512`
		`<45>24462: IE3200: Dec 13 2023 02:55:56: %SSH-5-SSH2_SESSION: SSH2 Session request from 172.16.16.46 (tty = 0) using crypto cipher '', hmac '' Failed`
		`<45>24463: IE3200: Dec 13 2023 02:55:56: %SSH-5-SSH2_CLOSE: SSH2 Session from 172.16.16.46 (tty = 0) for user '' using crypto cipher '', hmac '' closed`
		
		No matching MAC
		`<43>24579: IE3200: Dec 13 2023 03:19:10: %SSH-3-NO_MATCH: No matching mac found: client hmac-md5 server hmac-sha2-256,hmac-sha2-512`
		`<45>24580: IE3200: Dec 13 2023 03:19:10: %SSH-5-SSH2_SESSION: SSH2 Session request from 172.16.16.46 (tty = 0) using crypto cipher '', hmac '' Failed`
		`<45>24581: IE3200: Dec 13 2023 03:19:10: %SSH-5-SSH2_CLOSE: SSH2 Session from 172.16.16.46 (tty = 0) for user '' using crypto cipher '', hmac '' closed`
		
		No matching key exchange method
		`<43>24603: IE3200: Dec 13 2023 03:23:47: %SSH-3-NO_MATCH: No matching kex algorithm found: client diffie-hellman-group1-sha1,ext-info-c server diffie-hellman-group14-sha1,ecdh-sha2-nistp256,ecdh-sha2-nistp384`
		`<45>24604: IE3200: Dec 13 2023 03:23:47: %SSH-5-SSH2_SESSION: SSH2 Session request from 172.16.16.46 (tty = 0) using crypto cipher '', hmac '' Failed`
		`<45>24605: IE3200: Dec 13 2023 03:23:47: %SSH-5-SSH2_CLOSE: SSH2 Session from 172.16.16.46 (tty = 0) for user '' using crypto cipher '', hmac '' closed`
		
		Oversized packet
		`<43>24419: IE3200: Dec 13 2023 02:48:53: %SSH-3-BAD_PACK_LEN: Bad packet length 33068`
		`<46>24420: IE3200: Dec 13 2023 02:48:53: %SYS-6-LOGOUT: User admin has exited tty session 2(172.16.16.46)`

FIA_AFL.1	Failed Login due to Exceeding limit	`<45>24001: IE3200: Dec 11 2023 22:09:29: %AAA-5-LOCAL_USER_BLOCKED: User TestUser17085 blocked for login till 22:10:29 UTC Dec 11 2023`
		`<44>24002: IE3200: Dec 11 2023 22:09:31: %SEC_LOGIN-4-LOGIN_FAILED: Login failed [user: TestUser17085] [Source: 172.16.16.46] [localport: 22] [Reason: Login Authentication Failed] at 22:09:31 UTC Mon Dec 11 2023`

FIA_UIA_EXT.1
FIA_UAU_EXT.2
	All use of the authentication mechanism.	**SSH Authentication Success – Password**
		`<45>26095: IE3200: Dec 15 2023 07:03:34: %SEC_LOGIN-5-LOGIN_SUCCESS: Login Success [user: admin] [Source: 172.16.16.46] [localport: 22] at 07:03:34 UTC Fri Dec 15 2023`
		`<45>26096: IE3200: Dec 15 2023 07:03:34: %SSH-5-SSH2_USERAUTH: User 'admin' authentication for SSH2 Session from 172.16.16.46 (tty = 0) using crypto cipher 'aes256-cbc', hmac 'hmac-sha2-256' Succeeded`
		
		SSH Authentication Failure – Password
		`<44>24413: IE3200: Dec 13 2023 02:45:32: %SEC_LOGIN-4-LOGIN_FAILED: Login failed [user: admin] [Source: 172.16.16.46] [localport: 22] [Reason: Login Authentication Failed] at 02:45:32 UTC Wed Dec 13 2023`
		`<45>24414: IE3200: Dec 13 2023 02:45:32: %SSH-5-SSH2_USERAUTH: User '' authentication for SSH2 Session from 172.16.16.46 (tty = 0) using crypto cipher 'aes128-cbc', hmac 'hmac-sha2-256' Failed`
		
		SSH Authentication Success – Public Key
		`<45>26095: IE3200: Dec 15 2023 07:03:34: %SEC_LOGIN-5-LOGIN_SUCCESS: Login Success [user: admin] [Source: 172.16.16.46] [localport: 22] at 07:03:34 UTC Fri Dec 15 2023`
		`<45>26096: IE3200: Dec 15 2023 07:03:34: %SSH-5-SSH2_USERAUTH: User 'admin' authentication for SSH2 Session from 172.16.16.46 (tty = 0) using crypto cipher 'aes256-cbc', hmac 'hmac-sha2-256' Succeeded`
		
		SSH Authentication Failure – Public Key
		`<44>24413: IE3200: Dec 13 2023 02:45:32: %SEC_LOGIN-4-LOGIN_FAILED: Login failed [user: admin] [Source: 172.16.16.46] [localport: 22] [Reason: Login Authentication Failed] at 02:45:32 UTC Wed Dec 13 2023`
		`<45>24414: IE3200: Dec 13 2023 02:45:32: %SSH-5-SSH2_USERAUTH: User '' authentication for SSH2 Session from 172.16.16.46 (tty = 0) using crypto cipher 'aes128-cbc', hmac 'hmac-sha2-256' Failed`
		
		Console Authentication Success
		`<45>26186: IE3200: Dec 15 2023 08:07:29: %SEC_LOGIN-5-LOGIN_SUCCESS: Login Success [user: admin] [Source: LOCAL] [localport: 0] at 08:07:29 UTC Fri Dec 15 2023`
		
		Console Authentication Failure
		`<44>26185: IE3200: Dec 15 2023 08:07:29: %SEC_LOGIN-4-LOGIN_FAILED: Login failed [user: admin] [Source: LOCAL] [localport: 0] [Reason: Login Authentication Failed] at 08:07:29 UTC Fri Dec 15 2023`

FIA_X509_EXT.1/Rev	Unsuccessful attempt to validate a certificate	**Add Trust Anchor**
		`See FMT_SMF.1`
		
		Remove Trust Anchor
		`See FMT_SMF.1`
		
		Missing Basic Constraints
		`<47>8085: IE3200: Dec 21 2023 22:07:25: IKEv2:(SESSION ID = 0,SA ID = 0):Received Packet [From 192.168.144.46:500/To 192.168.144.168:500/VRF i0:f0]`
		`<47>8223: IE3200: Dec 21 2023 22:07:31: IKEv2:(SESSION ID = 20,SA ID = 1):Verify cert failed`
		`<47>8221: IE3200: Dec 21 2023 22:07:31: IKEv2:(SA ID = 1):[PKI -> IKEv2] Validation of certificate chain FAILED`
		
		Basic constraints false for CA
		`<47>8884: IE3200: Dec 21 2023 22:09:35: IKEv2:(SESSION ID = 0,SA ID = 0):Received Packet [From 192.168.144.46:500/To 192.168.144.168:500/VRF i0:f0]`
		`<47>9022: IE3200: Dec 21 2023 22:09:40: IKEv2:(SESSION ID = 21,SA ID = 1):Verify cert failed`
		`<47>9020: IE3200: Dec 21 2023 22:09:40: IKEv2:(SA ID = 1):[PKI -> IKEv2] Validation of certificate chain FAILED`
		
		Certificate revoked
		`<47>9455: IE3200: Jan 18 2024 07:10:23: IKEv2:Received Packet [From 192.168.144.46:500/To 192.168.144.168:500/VRF i0:f0]`
		`<43>9600: IE3200: Jan 18 2024 07:10:23: %PKI-3-CERTIFICATE_REVOKED: Certificate chain validation has failed. The certificate (SN: 00D1) is revoked`
		
		Corrupt Cert ASN1
		`<47>124307: IE3200: Jan 18 2024 23:36:58: IKEv2:(SESSION ID = 46,SA ID = 1):Received Packet [From 192.168.144.46:500/To 192.168.144.168:500/VRF i0:f0]`
		`<47>124477: IE3200: Jan 18 2024 23:37:04: CRYPTO_PKI: status = 0x705(E_INPUT_DATA : invalid encoding format for input data): BER/DER decoding of certificate has failed`
		`<43>124573: IE3200: Jan 18 2024 23:37:04: %IKEV2-3-NEG_ABORT: Negotiation aborted due to ERROR: Failed to enqueue an item to a list`
		
		Corrupt Cert Signature
		`<47>125705: IE3200: Jan 18 2024 23:39:31: IKEv2:(SESSION ID = 46,SA ID = 1):Received Packet [From 192.168.144.46:500/To 192.168.144.168:500/VRF i0:f0]`
		`<47>126158: IE3200: Jan 18 2024 23:39:36: crypto_engine: Decrypt with public RSA key, got error signature verification failure`
		`<47>126160: IE3200: Jan 18 2024 23:39:36: ../cert-c/source/vericert.c(145) : E_INVALID_SIGNATURE : error verifying digitial signature`

		Corrupt Public Key
		`<47>126220: IE3200: Jan 18 2024 23:40:09: IKEv2:Received Packet [From 192.168.144.46:500/To 192.168.144.168:500/VRF i0:f0]`
		`<47>127395: IE3200: Jan 18 2024 23:40:43: ../cert-c/source/vericert.c(145) : E_INVALID_SIGNATURE : error verifying digitial signature`
		
		Invalid Chain
		`<47>3490: IE3200: Dec 21 2023 21:53:07: IKEv2:(SESSION ID = 8,SA ID = 3):Received Packet [From 192.168.144.46:500/To 192.168.144.168:500/VRF i0:f0]`
		`<47>3702: IE3200: Dec 21 2023 21:53:13: IKEv2:(SA ID = 1):[PKI -> IKEv2] Validation of certificate chain FAILED`
		
		No cRLSign
		`<47>122159: IE3200: Jan 18 2024 23:35:47: IKEv2:(SESSION ID = 46,SA ID = 1):Received Packet [From 192.168.144.46:500/To 192.168.144.168:500/VRF i0:f0]`
		`<47>122719: IE3200: Jan 18 2024 23:35:52: Key-usage mismatch. Cert does not have cRLSign bit set.`
		`<47>122720: IE3200: Jan 18 2024 23:35:52: CRYPTO_PKI: CRL verify has failed`
		
		Unreachable Revocation Server
		`<47>13382: IE3200: Dec 21 2023 22:36:23: IKEv2:(SESSION ID = 22,SA ID = 4):Received Packet [From 192.168.144.46:500/To 192.168.144.168:500/VRF i0:f0]`
		`<43>13612: IE3200: Dec 21 2023 22:36:33: %PKI-3-CRL_FETCH_FAIL: CRL fetch for trustpoint rootca-rsa failed`
		
		Certificate expired
		`Expired Server Cert:`
		`<47>8808: IE3200: Jan 18 2024 07:06:34: IKEv2:Received Packet [From 192.168.144.46:500/To 192.168.144.168:500/VRF i0:f0]`
		`<47>8899: IE3200: Jan 18 2024 07:06:34: IKEv2-ERROR:Current time is more than cert validity time`
		
		`Expired SubCA Cert:`
		`<47>8938: IE3200: Jan 18 2024 07:08:28: IKEv2:Received Packet [From 192.168.144.46:500/To 192.168.144.168:500/VRF i0:f0]`
		`<43>9071: IE3200: Jan 18 2024 07:08:28: %PKI-3-CERTIFICATE_INVALID_EXPIRED: Certificate chain validation has failed.  The certificate (SN: 13) has expired.    Validity period ended on 2023-07-20T14:47:00Z`

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>26061: IE3200: Dec 15 2023 07:02:23: %PARSER-5-CFGLOG_LOGGEDCMD: User:admin  logged command:banner login c This is the CC Login Banner. CC Testing in Progress. c`
		`<45>26063: IE3200: Dec 15 2023 07:02:27: %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>24105: IE3200: Dec 13 2023 01:47:35: %PARSER-5-CFGLOG_LOGGEDCMD: User:admin  logged command:line con 0`
		`<45>24107: IE3200: Dec 13 2023 01:47:36: %PARSER-5-CFGLOG_LOGGEDCMD: User:admin  logged command:exec-timeout 1`
		
		SSH:
		`<45>23767: IE3200: *Dec 11 2023 21:41:55: %PARSER-5-CFGLOG_LOGGEDCMD: User:admin  logged command:line vty 0 15`
		`<45>23768: IE3200: *Dec 11 2023 21:41:55: %PARSER-5-CFGLOG_LOGGEDCMD: User:admin  logged command:exec-timeout 1`
		
		Ability to update the TOE, and to verify the updates using [published hash] capability prior to installing those updates
		`See FPT_TUD_EXT.1`
		
		Ability to configure the authentication failure parameters for FIA AFL.1
		`<45>23887: IE3200: Dec 11 2023 21:53:31: %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>1446: IE3200: Dec 20 2023 04:03:21: %PARSER-5-CFGLOG_LOGGEDCMD: User:admin  logged command:logging host 192.168.144.46`
		
		Ability to manage the cryptographic keys
		
		Generate Crypto Key for SSH:
		`<45>26195: IE3200: Dec 15 2023 08:26:52: %CRYPTO_ENGINE-5-KEY_ADDITION: A key named SSH-KEY has been generated or imported by crypto-engine`
		`<45>26197: IE3200: Dec 15 2023 08:26:53: %PARSER-5-CFGLOG_LOGGEDCMD: User:admin  logged command:crypto key generate rsa label * modulus 2048`
		
		Generate Crypto Key for IPsec:

		<46>128094: IE3200: Jan 19 2024 00:23:14: %HA_EM-6-LOG: cli_log: User:admin via Port:0 Executed[crypto key generate rsa general-keys modulus 2048 label *] <47>128095: IE3200: Jan 19 2024 00:23:14: crypto_engine: Generate public/private keypair <45>128096: IE3200: Jan 19 2024 00:23:17: %CRYPTO_ENGINE-5-KEY_ADDITION: A key named IPSEC-KEY has been generated or imported by crypto-engine **Delete Crypto Key:** <46>128127: IE3200: Jan 19 2024 00:30:24: %HA_EM-6-LOG: cli_log: User:admin via Port:0 Executed[crypto key zeroize rsa *] <47>128133: IE3200: Jan 19 2024 00:30:41: CRYPTO_ENGINE: keypair IPSEC-KEY deleted by Exec <45>128134: IE3200: Jan 19 2024 00:30:41: %CRYPTO_ENGINE-5-KEY_DELETED: A key named IPSEC-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. **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>26203: IE3200: Dec 15 2023 08:29:44: %PARSER-5-CFGLOG_LOGGEDCMD: User:admin logged command:ip ssh version 2 <45>118466: IE3200: Jan 18 2024 23:02:02: %PARSER-5-CFGLOG_LOGGEDCMD: User:admin logged command:ip ssh server algorithm authentication publickey <189>5989: *Nov 29 2023 02:41:08: %PARSER-5-CFGLOG_LOGGEDCMD: User:admin logged command:ip ssh server algorithm publickey ssh-rsa <189>5991: *Nov 29 2023 02:41:37: %PARSER-5-CFGLOG_LOGGEDCMD: User:admin logged command:ip ssh server algorithm hostkey rsa-sha2-256 rsa-sha2-512 <45>128157: IE3200: Jan 19 2024 01:40:19: %PARSER-5-CFGLOG_LOGGEDCMD: User:admin logged command:ip ssh server algorithm mac hmac-sha2-256 hmac-sha2-512 <45>128159: IE3200: Jan 19 2024 01:40:34: %PARSER-5-CFGLOG_LOGGEDCMD: User:admin logged command:ip ssh server algorithm encryption aes128-cbc aes256-cbc <45>128161: IE3200: Jan 19 2024 01:41:02: %PARSER-5-CFGLOG_LOGGEDCMD: User:admin logged command:ip ssh server algorithm kex diffie-hellman-group14-sha1 ecdh-sha2-nistp256 ecdh-sha2-nistp384 **Configure IPsec:** <45>128180: IE3200: Jan 19 2024 01:44:00: %PARSER-5-CFGLOG_LOGGEDCMD: User:admin logged command:crypto ikev2 proposal syslogipsec <45>128184: IE3200: Jan 19 2024 01:44:14: %PARSER-5-CFGLOG_LOGGEDCMD: User:admin logged command:encryption aes-cbc-128 aes-cbc-256

		<45>128186: IE3200: Jan 19 2024 01:44:25: %PARSER-5-CFGLOG_LOGGEDCMD: User:admin logged command:integrity sha1 sha256 sha512 <45>128189: IE3200: Jan 19 2024 01:44:31: %PARSER-5-CFGLOG_LOGGEDCMD: User:admin logged command:group 14 <45>128197: IE3200: Jan 19 2024 01:44:45: %PARSER-5-CFGLOG_LOGGEDCMD: User:admin logged command:crypto ikev2 policy Syslog <45>128199: IE3200: Jan 19 2024 01:44:55: %PARSER-5-CFGLOG_LOGGEDCMD: User:admin logged command:match address local 192.168.144.168 <45>128201: IE3200: Jan 19 2024 01:45:05: %PARSER-5-CFGLOG_LOGGEDCMD: User:admin logged command:proposal syslogipsec <45>128205: IE3200: Jan 19 2024 01:45:26: %PARSER-5-CFGLOG_LOGGEDCMD: User:admin logged command:crypto ikev2 keyring * <45>128207: IE3200: Jan 19 2024 01:45:32: %PARSER-5-CFGLOG_LOGGEDCMD: User:admin logged command:peer syslogpeer <45>128209: IE3200: Jan 19 2024 01:45:44: %PARSER-5-CFGLOG_LOGGEDCMD: User:admin logged command:address 192.168.144.46 255.255.255.0 <45>128211: IE3200: Jan 19 2024 01:45:52: %PARSER-5-CFGLOG_LOGGEDCMD: User:admin logged command:identity address 192.168.144.46 <45>128222: IE3200: Jan 19 2024 01:47:08: %PARSER-5-CFGLOG_LOGGEDCMD: User:admin logged command:pre-shared-key local hex 07080912345A6B2C3D3E3F1A1B2C3D4E5F <45>128224: IE3200: Jan 19 2024 01:47:17: %PARSER-5-CFGLOG_LOGGEDCMD: User:admin logged command:pre-shared-key remote hex 07080912345A6B2C3D3E3F1A1B2C3D4E5F <45>128247: IE3200: Jan 19 2024 01:47:47: %PARSER-5-CFGLOG_LOGGEDCMD: User:admin logged command:crypto ikev2 profile SyslogProfile <45>128249: IE3200: Jan 19 2024 01:48:01: %PARSER-5-CFGLOG_LOGGEDCMD: User:admin logged command:match identity remote address 192.168.144.46 255.255.255.255 <45>128251: IE3200: Jan 19 2024 01:48:08: %PARSER-5-CFGLOG_LOGGEDCMD: User:admin logged command:authentication remote rsa-sig <45>128253: IE3200: Jan 19 2024 01:48:14: %PARSER-5-CFGLOG_LOGGEDCMD: User:admin logged command:authentication local rsa-sig <45>128255: IE3200: Jan 19 2024 01:48:23: %PARSER-5-CFGLOG_LOGGEDCMD: User:admin logged command:keyring local * <45>128257: IE3200: Jan 19 2024 01:48:31: %PARSER-5-CFGLOG_LOGGEDCMD: User:admin logged command:pki trustpoint rootca-rsa <45>128774: IE3200: Jan 19 2024 01:50:47: %PARSER-5-CFGLOG_LOGGEDCMD: User:admin logged command:crypto ipsec transform-set SyslogTransform esp-aes esp-sha-hmac

		<45>128776: IE3200: Jan 19 2024 01:50:51: %PARSER-5-CFGLOG_LOGGEDCMD: User:admin logged command:mode tunnel <45>26246: IE3200: Dec 18 2023 21:42:28: %PARSER-5-CFGLOG_LOGGEDCMD: User:admin logged command:interface Tunnel0 <45>26249: IE3200: Dec 18 2023 21:42:46: %PARSER-5-CFGLOG_LOGGEDCMD: User:admin logged command:ip address 100.100.100.100 255.255.255.0 <45>26251: IE3200: Dec 18 2023 21:42:54: %PARSER-5-CFGLOG_LOGGEDCMD: User:admin logged command:tunnel source Vlan2 <45>26253: IE3200: Dec 18 2023 21:42:59: %PARSER-5-CFGLOG_LOGGEDCMD: User:admin logged command:tunnel mode ipsec ipv4 <45>26255: IE3200: Dec 18 2023 21:43:18: %PARSER-5-CFGLOG_LOGGEDCMD: User:admin logged command:tunnel destination 192.168.144.46 <45>26257: IE3200: Dec 18 2023 21:43:30: %PARSER-5-CFGLOG_LOGGEDCMD: User:admin logged command:tunnel protection ipsec profile SylogProfile **Ability to configure the thresholds for SSH rekeying** <189>229: *Nov 30 2023 21:29:28: %PARSER-5-CFGLOG_LOGGEDCMD: User:admin logged command:ip ssh rekey time 10 <189>230: *Nov 30 2023 21:29:36: %PARSER-5-CFGLOG_LOGGEDCMD: User:admin logged command:ip ssh rekey volume 100 <189>231: *Nov 30 2023 21:29:39: %SYS-5-CONFIG_I: Configured from console by admin on console **Ability to set the time which is used for timestamps** See FPT_STM_EXT.1 **Reset Passwords** <45>23725: IE3200: *Dec 11 2023 21:23:39: %PARSER-5-CFGLOG_LOGGEDCMD: User:TestUser16028 logged command:username TestUser16028 secret * **Ability to configure the reference identifier for the peer** <45>139117: IE3200: Jan 19 2024 02:19:20: %PARSER-5-CFGLOG_LOGGEDCMD: User:admin logged command:crypto pki certificate map est 1 <45>139121: IE3200: Jan 19 2024 02:19:41: %PARSER-5-CFGLOG_LOGGEDCMD: User:admin logged command:alt-subject-name eq tl15-16x.example.com <45>139357: IE3200: Jan 19 2024 02:20:47: %PARSER-5-CFGLOG_LOGGEDCMD: User:admin logged command:crypto pki trustpoint rootca-rsa <45>139571: IE3200: Jan 19 2024 02:20:54: %PARSER-5-CFGLOG_LOGGEDCMD: User:admin logged command:match certificate est **Ability to manage the TOE's trust store and designate X509.v3 certificates as trust anchors**

		Create Trustpoint: <45>158895: IE3200: Jan 25 2024 03:12:03: %PARSER-5-CFGLOG_LOGGEDCMD: User:admin logged command:crypto pki trustpoint rootca-rsa <46>158894: IE3200: Jan 25 2024 03:12:03: %PKI-6-TRUSTPOINT_CREATE: Trustpoint: rootca-rsa created succesfully **Import CA Cert:** <45>312189: IE3200: Jan 25 2024 21:50:20: %PARSER-5-CFGLOG_LOGGEDCMD: User:admin logged command:crypto pki authenticate rootca-rsa <47>323361: IE3200: Jan 25 2024 21:51:00: crypto_ca_certificate: saved cert to nvram:rootca-rsa#1CA.cer [OK] <47>335327: IE3200: Jan 25 2024 21:54:52: CRYPTO_PKI: subject="cn=rootca-rsa,o=GSS,l=Catonsville,st=MD,c=US" serial number= 01 00 01 **Generate Certificate Request** Generate Certificate Request: <46>158811: IE3200: Jan 25 2024 02:17:15: %HA_EM-6-LOG: cli_log: User:admin via Port:0 Executed[crypto pki enroll rootca-rsa] **Remove Trustpoint & Certs** <45>158872: IE3200: Jan 25 2024 03:11:16: %PARSER-5-CFGLOG_LOGGEDCMD: User:admin logged command:no crypto pki trustpoint rootca-rsa <46>158869: IE3200: Jan 25 2024 03:11:16: %PKI-6-TRUSTPOINT_DELETE: Trustpoint: rootca-rsa deleted successfully **Ability to manage the trusted public keys database** Configure public key authentication: <189>5989: *Nov 29 2023 02:41:08: %PARSER-5-CFGLOG_LOGGEDCMD: User:admin logged command:ip ssh server algorithm publickey ssh-rsa <45>118466: IE3200: Jan 18 2024 23:02:02: %PARSER-5-CFGLOG_LOGGEDCMD: User:admin logged command:ip ssh server algorithm authentication publickey **Configure User with public key:** <45>118429: IE3200: Jan 18 2024 22:59:41: %PARSER-5-CFGLOG_LOGGEDCMD: User:admin logged command:ip ssh pubkey-chain <45>118431: IE3200: Jan 18 2024 22:59:45: %PARSER-5-CFGLOG_LOGGEDCMD: User:admin logged command:username testadmin <45>118433: IE3200: Jan 18 2024 22:59:58: %PARSER-5-CFGLOG_LOGGEDCMD: User:admin logged command:key-string <45>118439: IE3200: Jan 18 2024 23:00:54: %PARSER-5-CFGLOG_LOGGEDCMD: User:admin logged command:Ltzx9zuDefExfmVGWnpko2wckbA093hvsoabD15Dq2vt **Remove public key and association with user:**

		<45>118400: IE3200: Jan 18 2024 22:58:37: %PARSER-5-CFGLOG_LOGGEDCMD: User:admin logged command:ip ssh pubkey-chain <45>118402: IE3200: Jan 18 2024 22:58:41: %PARSER-5-CFGLOG_LOGGEDCMD: User:admin logged command:no username admin **Ability to import X509v3 certificates to the TOE's trust store** Import CSR Generated Certificate: <46>158837: IE3200: Jan 25 2024 02:46:09: %HA_EM-6-LOG: cli_log: User:admin via Port:0 Executed[crypto pki import rootca-rsa certificate] <47>158840: IE3200: Jan 25 2024 02:46:44: CRYPTO_PKI: make trustedCerts list for rootca-rsa <47>158841: IE3200: Jan 25 2024 02:46:44: CRYPTO_PKI: subject="cn=rootca-rsa,o=GSS,l=Catonsville,st=MD,c=US" serial number= 01 00 01 <47>158844: IE3200: Jan 25 2024 02:46:44: CRYPTO_PKI: Attempting to insert the peer's public key into cache <47>158845: IE3200: Jan 25 2024 02:46:44: CRYPTO_PKI:Peer's public inserted successfully with key id 276 <47>158850: IE3200: Jan 25 2024 02:46:44: CRYPTO_PKI: pubkey name : 0S1#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>158851: IE3200: #006#003U#004 <47>158852: IE3200: #014#003GSS1#0230#021#006#003U#004#003#014 <47>158853: IE3200: rootca-rsa
FPT_STM_EXT.1	Discontinuous changes to time - either Administrator actuated or changed via an automated process.	<46>25350: IE3200: Dec 14 2023 02:56:53: %HA_EM-6-LOG: cli_log: User:admin via Port:0 Executed[clock set 10:25:20 15 April 2023] <46>25351: IE3200: .Apr 15 2023 10:25:20: %SYS-6-CLOCKUPDATE: System clock has been updated from 02:56:53 UTC Thu Dec 14 2023 to 10:25:20 UTC 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>159976: IE3200: Jan 25 2024 19:23:56: %HA_EM-6-LOG: cli_log: User:admin via Port:0 Executed[install add file tftp://172.16.16.47/ie3x00-universalk9.17.12.02.SPA.bin activate commit] <45>159977: IE3200: Jan 25 2024 19:24:04: %INSTALL-5-INSTALL_START_INFO: R0/0: install_engine: Started install one-shot tftp://172.16.16.47/ie3x00-universalk9.17.12.02.SPA.bin <45>160041: IE3200: Jan 25 2024 20:00:08: %INSTALL-5-INSTALL_COMPLETED_INFO: R0/0: install_engine: Completed install one-shot PACKAGE flash:ie3x00-universalk9.17.12.02.SPA.bin **Failure:** Corrupt Image (Valid Signature): <46>159530: IE3200: Jan 25 2024 05:54:55: %HA_EM-6-LOG: cli_log: User:admin via Port:0 Executed[install add file activate commit] <45>159531: IE3200: Jan 25 2024 05:55:04: %INSTALL-5-INSTALL_START_INFO: R0/0: install_engine: Started install one-shot flash:ie3x00-universalk9.17.12.02.SPA_CORRUPT.bin <43>159533: IE3200: Jan 25 2024 05:55:24: %INSTALL-3-OPERATION_ERROR_MESSAGE: R0/0: install_engine: Failed to install_add_activate_commit package flash:ie3x00-universalk9.17.12.02.SPA_CORRUPT.bin, Error: File flash:ie3x00-universalk9.17.12.02.SPA_CORRUPT.bin is corrupt or is not a valid package. **No Signature:** <46>159547: IE3200: Jan 25 2024 06:10:40: %HA_EM-6-LOG: cli_log: User:admin via Port:0 Executed[install add file tftp://172.16.16.47/ie3x00-universalk9.17.12.02_NOSIG.SPA.bin activate commit] <45>159548: IE3200: Jan 25 2024 06:10:49: %INSTALL-5-INSTALL_START_INFO: R0/0: install_engine: Started install one-shot tftp://172.16.16.47/ie3x00-universalk9.17.12.02_NOSIG.SPA.bin <43>159549: IE3200: Jan 25 2024 06:23:57: %INSTALL-3-OPERATION_ERROR_MESSAGE: R0/0: install_engine: Failed to install_add_activate_commit package flash:ie3x00-universalk9.17.12.02_NOSIG.SPA.bin, Error: File flash:ie3x00-universalk9.17.12.02_NOSIG.SPA.bin is corrupt or is not a valid package. **Modified Signature:** <46>159572: IE3200: Jan 25 2024 06:30:25: %HA_EM-6-LOG: cli_log: User:admin via Port:0 Executed[install add file tftp://172.16.16.47/ie3x00-universalk9.17.12.02.SPA_MODSIG.bin activate commit] <45>159573: IE3200: Jan 25 2024 06:30:34: %INSTALL-5-INSTALL_START_INFO: R0/0: install_engine: Started install one-shot tftp://172.16.16.47/ie3x00-universalk9.17.12.02.SPA_MODSIG.bin <43>159574: IE3200: Jan 25 2024 06:43:34: %INSTALL-3-OPERATION_ERROR_MESSAGE: R0/0: install_engine: Failed to install_add_activate_commit package flash:ie3x00-

		universalk9.17.12.02.SPA_MODSIG.bin, Error: File flash:ie3x00-universalk9.17.12.02.SPA_MODSIG.bin is corrupt or is not a valid package.
FTA_SSL_EXT.1	The termination of a local session by the session locking mechanism.	<46>24113: IE3200: Dec 13 2023 01:49:12: %SYS-6-TTY_EXPIRE_TIMER: (exec timer expired, tty 0 (0.0.0.0)), user admin <46>24114: IE3200: Dec 13 2023 01:49:12: %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>23839: IE3200: Dec 11 2023 21:37:26: %SYS-6-TTY_EXPIRE_TIMER: (exec timer expired, tty 2 (172.16.16.46)), user admin <46>23840: IE3200: Dec 11 2023 21:37:26: %SYS-6-LOGOUT: User admin has exited tty session 2(172.16.16.46) <45>23842: IE3200: Dec 11 2023 21:37:26: %SSH-5-SSH2_CLOSE: SSH2 Session from 172.16.16.46 (tty = 0) for user 'admin' using crypto cipher 'aes256-cbc', hmac 'hmac-sha2-256' closed
FTA_SSL.4	The termination of an interactive session.	**SSH:** <46>26106: IE3200: Dec 15 2023 07:03:36: %HA_EM-6-LOG: cli_log: User:admin via Port:2 Executed[exit] <46>26107: IE3200: Dec 15 2023 07:03:36: %SYS-6-LOGOUT: User admin has exited tty session 2(172.16.16.46) <45>26108: IE3200: Dec 15 2023 07:03:36: %SSH-5-SSH2_CLOSE: SSH2 Session from 172.16.16.46 (tty = 0) for user 'admin' using crypto cipher 'aes256-cbc', hmac 'hmac-sha2-256' closed **Local Console:** <46>26189: IE3200: Dec 15 2023 08:07:32: %HA_EM-6-LOG: cli_log: User:admin via Port:0 Executed[exit] <46>26190: IE3200: Dec 15 2023 08:07:32: %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
		Establish IPSec Session
		`<45>8674: IE3200: Jan 18 2024 06:50:48: %IKEV2-5-SA_UP: SA UP`
		`<45>8675: IE3200: Jan 18 2024 06:50:48: %CRYPTO-5-IKEV2_SESSION_STATUS: Crypto tunnel v2 is UP.  Peer 192.168.144.46:4500       Id: 192.168.144.46`
		`<47>8718: IE3200: Jan 18 2024 06:50:48: IKEv2:(SESSION ID = 33,SA ID = 1):(SA ID = 1):[IPsec -> IKEv2] Creation of IPsec SA into IPsec database PASSED`
		`<45>8719: IE3200: Jan 18 2024 06:50:48: %LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel0, changed state to up`
		
		Terminate IPsec Session
		`<47>1093: IE3200: Jan 18 2024 06:19:25: IKEv2:(SESSION ID = 17,SA ID = 1):Deleting SA`
		`<45>1094: IE3200: Jan 18 2024 06:19:25: %IKEV2-5-SA_DOWN: SA DOWN`
		`<45>1095: IE3200: Jan 18 2024 06:19:25: %CRYPTO-5-IKEV2_SESSION_STATUS: Crypto tunnel v2 is DOWN.  Peer 192.168.144.46:500       Id: 192.168.144.46`
		
		Failures of IPsec Session
		See FCS_IPSEC_EXT.1 for Audits associated with failures of IPsec Sessions.

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

7. Obtaining Technical Assistance and Submitting a Service Request

Cisco provides Cisco.com as a starting point for all technical assistance. Customers and partners can obtain troubleshooting tips, and sample configurations from online tools. For Cisco.com registered users, additional troubleshooting tools are available from the TAC website.

8. Contact 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.