Cisco Catalyst Industrial Ethernet 9300 Rugged Series Switches running IOS-XE 17.9

CC Configuration Guide

Version: 0.5
Date: November 6, 2023

Table of Contents

List of Tables

Document Introduction

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

This document provides the basis for an evaluation of a specific Target of Evaluation (TOE), Cisco Catalyst Industrial Ethernet 9300 Rugged Series (IE9300). This Security Target (ST) defines a set of assumptions about the aspects of the environment, a list of threats that the product intends to counter, a set of security objectives, a set of security requirements, and the IT security functions provided by the TOE which meet the set of requirements.

1 Introduction

This Operational User Guidance with Preparative Procedures documents the administration of the Cisco Catalyst Industrial Ethernet 9300 Rugged Series Switch (IE9300), the TOE, as it is certified under Common Criteria. The Cisco Catalyst Industrial Ethernet 9300 Rugged Series Switch may be referenced below as IE9300, TOE, or simply switch.

2 Audience

This document is written for administrators 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. The administrator configuring the TOE must review this Configuration Guide and the documents identified in Table 1 below. In this document, users of the TOE are referred to as "users" or "administrators".

A user with privilege level 15, access to all TOE commands, is referred to as an Authorized Administrator or privileged administrator.

2.1 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 IE9300 operations. All security relevant commands to manage the TSF data are provided within this documentation within each functional section.

2.2 Document References

This document refers to several Cisco Systems documents. The documents used are shown below in Table 2. Throughout this document, the guides will be referred to by the "#", such as **[1]**.

Table 1 Cisco Documentation

#	Title	Link
[1]	Release Notes for Cisco Catalyst IE9300 Rugged Series Switches, and Cisco Catalyst IE9300 Embedded Series Switch, Cisco IOS XE Cupertino 17.9.x	https://www.cisco.com/c/en/us/td/docs/switches/lan/cisco_ie9300/software/17_9/17-9-x-ie93xx-rn.html

[2]	Cisco Catalyst IE9300 Rugged Series Switches Hardware Installation Guide	https://www.cisco.com/c/en/us/td/docs/switches/lan/cisco_ie9300/hardware/installation/ie93xx-hig.html
[3]	Configuration Guides (IE300)	https://www.cisco.com/c/en/us/support/switches/catalyst-ie9300-rugged-series/products-installation-and-configuration-guides-list.html
[4]	Software Configuration Guide, Cisco Catalyst IE9300 Rugged Series Switches	https://www.cisco.com/c/en/us/td/docs/switches/lan/cisco_ie9300/software/17_8/security-config-guide-ie93xx.html
[5]	Secure Shell Configuration Guide, Cisco IOS XE 17	https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_usr_ssh/configuration/xe-17/sec-usr-ssh-xe-17-book.html
[6]	Security for VPNs with IPsec Configuration Guide, Cisco IOS XE 17	https://www.cisco.com/c/en/us/td/docs/routers/ios/config/17-x/sec-vpn/b-security-vpn.html

[7]	Cisco IOS Security Command Reference	A to C: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/security/a1/sec-a1-cr-book.html D to L: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/security/d1/sec-d1-cr-book.html M to R: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/security/m1/sec-m1-cr-book.html S to Z: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/security/s1/sec-s1-cr-book.html
[8]	Public Key Infrastructure Configuration Guide	https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_conn_pki/configuration/xe-17/sec-pki-xe-17-book.html?dtid=osscdc000283
[9]	Command Reference, Cisco IOS XE Cupertino 17.9.x	https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9300/software/release/17-9/command_reference/b_179_9300_cr.html
[10]	Cisco IOS Configuration Fundamentals Command Reference	https://www.cisco.com/c/en/us/td/docs/ios/fundamentals/command/reference/cf_book.html
[11]	IP Routing Configuration Guide, Cisco Catalyst IE3x00, IE3400 Heavy Duty, and ESS3300	https://www.cisco.com/c/en/us/td/docs/switches/lan/cisco_ie3X00/software/17_3/b_ip_routing_17-3_iot_switch_cg.html
[12]	Cisco Errors and System Messages, Cisco IOS-XE 17.9	https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/17_xe/syslogs/17-9-x/b-system-message-guide-17-9-x.html
[13]	IP Addressing: NAT Configuration Guide	https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_conn_vpnips/configuration/xe-17/sec-sec-for-vpns-w-ipsec-xe-17-book-cat8000.html
[14]	Loading and Managing System Images Configuration Guide	https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sys-image-mgmt/configuration/xe-17-1/sysimgmgmt-xe-17-1-book.html

[15]	MACSEC and MKA Configuration	https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/macsec/configuration/xe-17/macsec-xe-17-book.html
[16]	Access Control List Configuration Guide	https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_data_acl/configuration/xe-3s/asr903/17-1-1/b-sec-data-acl-xe-17-1-asr900.html
[17]	IPsec Configuration Guide	https://www.cisco.com/c/en/us/td/docs/routers/ios/config/17-x/sec-vpn/b-security-vpn.html
[18]	FlexVPN and Internet Key Exchange Version 2 Configuration Guide	https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_conn_ike2vpn/configuration/xe-17/sec-flex-vpn-xe-17-book-cat8000/sec-cfg-ikev2-flex.html
[19]	Troubleshoot MACSEC on Catalyst 9000	https://www.cisco.com/c/en/us/support/docs/switches/catalyst-9300-series-switches/216849-troubleshoot-macsec-on-catalyst-9000.html

2.3 Supported Hardware and Software

Only the hardware and software listed in section 1.5 of the Security Target (ST) is compliant with the Common Criteria evaluation. Using hardware not specified in the ST invalidates the secure configuration. Likewise, using any software version other than the evaluated software listed in the ST will invalidate the secure configuration. The TOE is a hardware and software solution that makes up the IE9300. The network, on which they reside, is considered part of the environment. The software is pre-installed and is comprised of the Cisco IOS-XE software image Release 17.9. In addition, the software image is also downloadable from the Cisco web site.

2.4 Operational Environment

2.4.1 Supported non-TOE Hardware/ Software/ Firmware

The TOE supports (in some cases optionally) the following hardware, software, and firmware in its environment:

Table 2 IT Environment Components

Component	Required	Usage/Purpose Description for TOE performance
RADIUS AAA Server	Yes	This includes any IT environment RADIUS AAA server that provides authentication services to TOE Administrators over a secure IPsec trusted channel either directly or connected to a TOE Peer that also supports a secure IPsec trusted channel
Management Workstation with SSH Client	Yes	This includes any IT Environment Management workstation with a SSH client installed that is used by the TOE administrator to support TOE administration through SSH protected channels. Any SSH client that supports SSHv2 may be used.
Local Console	Yes	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.
Certification Authority (CA)	Yes	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.

Component	Required	Usage/Purpose Description for TOE performance
MACsec peer	Yes	This includes any MACsec peer with which the TOE participates in MACsec communications. It may be any device that supports MACsec communications.
Audit (syslog) Server	Yes	This includes any syslog server to which the TOE transmits syslog messages over a secure Internet Protocol security (IPsec) trusted channel either directly or connected to a TOE Peer that also supports a secure IPsec trusted channel
TOE Peer	Conditional	The TOE Peer is required if the remote syslog server and/or the remote authentication is attached for the TOE’s use. If the remote syslog server and/or the remote authentication is directly connected to the TOE for the TOE’s use, then the TOE Peer is not required.

2.4.2 Excluded Functionality

The following functionality is excluded from the evaluation:

Table 3 Excluded Functionality

Excluded Functionality	Exclusion Rationale
Non-FIPS 140-2 mode of operation	This mode of operation includes non-FIPS allowed operations.

These services will be disabled by configuration. The exclusion of this functionality does not affect compliance to the U.S. Government Protection Profile for Security Requirements for Network Devices

2.5 Secure Acceptance of the TOE

In order to ensure the correct TOE is received, the TOE should be examined to ensure that that is has not been tampered with during delivery.

Verify that the TOE software and hardware were not tampered with during delivery by performing the following actions:

Step 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. Ifit is not, contact the supplier of the equipment (Cisco Systems or an authorized Cisco distributor/partner).

Step 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).

Step 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.

Step 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).

Step 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.

Step 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).

Step 7 Approved methods for obtaining a Common Criteria evaluated software images:

- Download the Common Criteria evaluated software image file from Cisco.com onto a trusted computer system.
- Software images are available from Cisco.com at the following: http://www.cisco.com/cisco/software/navigator.html.
- The TOE ships with the correct software images installed, however this may not be the evaluated version.

Step 8 Once the file is downloaded, verify that it was not tampered with by using a SHA-512 utility to compute a SHA-512 hash for the downloaded file and comparing this with the SHA-512 hash for the image listed in Table 5 below. If the SHA-512 hashes do not match, contact Cisco Technical Assistance Center (TAC), https://tools.cisco.com/ServiceRequestTool/create/launch.do.

Once the file has been copied, it is recommended that you read and familiarize yourself with the Installation and Boot **[3]**. You may also want to familiarize yourself with **[7]** basic commands, **[1]** release notes and **[10]** Cisco IOS Fundamentals before proceeding with the installation and configuration of the TOE.

Step 9 To verify the digital signature prior to installation, the show software authenticity file command allows you to display software authentication related information that includes image credential information, key type used for verification, signing information, and other attributes in the signature envelope, for a specific image file. The TOE will verify the image signature after rebooting as described in **[14]** Installation and Boot. The **show software authenticity file** command allows you to display software authentication related information that includes image credential information, key type used for verification, signing information, and other attributes in the signature envelope, for a specific image file. The command handler will extract the signature envelope and its fields from the image file and dump the required information. To display the software public keys that are in the storage with the key types, use the **show software authenticity keys** command in privileged EXEC mode.

```
SWITCH# show software authenticity file {bootflash0:filename | bootflash1:filename | bootflash:filename |
nvram:filename | usbflash0:filename | usbflash1:filename}
```

To display information related to software authentication for the current ROM monitor (ROMMON), monitor library (monlib), and Cisco IOS image used for booting, use the **show software authenticity running** command in privileged EXEC mode.

If the output from the **show software authenticity file** command does not provide expected output as described in **[1]**, contact Cisco Technical Assistance Center (TAC) https://tools.cisco.com/ServiceRequestTool/create/launch.do.

After verifying the digital signature with the **show software authenticity file** command, an upgrade and reboot should be configured on the switch as described in **[1]**. The switch will not boot if the digital signature is not valid and an error will be displayed on the console:

```
autoboot: boot failed, restarting...
```

Step 10 To install and configure the IE9300 follow the instructions as described in **[3]** Administering the Device.

Start your IE9300 as described in [**3**] and executing associated commands. Confirm that the TOE loads the image correctly, completes internal self-checks and displays the cryptographic export warning on the console.

Step 11 The end-user must confirm once the TOE has booted that they are indeed running the evaluated version. Use the "**show version**" command **[3]** to display the currently running system image filename and the system software release version. It is also recommended the license level be verified and activated as described in **[3]**. It is assumed the end-user has acquired a permanent license is valid for the lifetime of the system on which it is installed.

Table 4 Evaluated Software Images

Platform	**Image Name**	**Hash**
IE-9310-26S2C IE-9320-26S2C	ie9k_iosxe.17.09.01.SPA.bin	IE9300: MD5 checksum: cc90f9999ded798a17d7afd7308076bd SHA512 checksum: afb63b657186b2cc2e9c71241aefe0a92606c100a6c9d1c25ad85910f4094691a9eed52d873112332eb107bc205af30aae8ceca5384da06438f1323ade9c5cd6

When updates, including PSIRTS (bug fixes) to the evaluated image are posted, customers are notified that updates are available (if they have purchased continuing support), information provided how to download updates and how to verify the updates. This information is the same as described above for installing the software image.

3 Secure Installation and Configuration

3.1 Physical Installation

Follow the Cisco Hardware Installation Guide for the IE9300 **[2]** for hardware installation instructions.

4 Preparative Procedures and Operational Guidance for the TOE

4.1 Switch — Power Up

1. 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
   ```

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

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

4.2 Switch — Initial Configuration

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

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

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

   Press RETURN to get started!
   ```

2. Enter privilege EXEC mode

   ```
   SWITCH> enable
   ```

3. Enter configure terminal

   ```
   SWITCH# configure terminal
   ```

4. Configure a hostname

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

5. Configure the Enable Secret Password using Type 8 or Type 9

   a. Configure the Enable Secret Password Using Type 8:

      ```
      enable algorithm-type sha256 secret <the unencrypted (cleartext) 'enable' secret>
      ```

   b. Configure the Enable Secret Password Using Type 9:

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

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

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

   ```
   SWITCH(config)# interface GigabitEthernet1

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

   SWITCH(config-if)# no shutdown

   SWITCH(config-if)# exit
   ```

7. Configure a default route to reach the Switch.

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

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

4.3 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**

4.4 Enable Configuration Change Notification and Logging

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

1. Ensure logging is enabled

   SWITCH(config)# **logging on**

2. Enter archive config mode

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

3. Enter logging config sub-mode

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

4. Enable the config logger

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

5. Suppress password when displaying logged commands

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

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

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

7. Enable sending of logged commands to remote syslog server

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

8. Exit configuration mode and return to privileged EXEC mode

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

4.5 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
```

4.6 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 (default) to 2,148,483,647bytes. **Note:** It is recommended to not make the buffer size too large because the TOE could run out of memory for other tasks. It is recommended to set it to at least 150000000

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

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

4.7 Generate Logs on Failed Login Attempts

To generate logs for failed login attempts enter

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

4.8 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
```

4.9 Generate Logs on Successful Login Attempts

To generate logs for successful login attempts enter

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

4.10 Set Syslog Server Logging Level

Set syslog server logging level to debug

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

4.11 Generate PKI Validation Logs

1. To generate logs for PKI validation enter

   ```
   SWITCH# debug crypto pki validation
   ```

2. To generate logs for PKI transactions enter

   ```
   SWITCH# debug crypto pki transactions
   ```

4.12 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
   ```

4.13 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 before locking the offending account.

```
SWITCH(config)# aaa local authentication attempts max-fail <number of failures>
```

4.14 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

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

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

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

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

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

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

5. To verify the Common Criteria password policy enter

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

4.15 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 <sha256 | 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 5 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

4.16 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>
```

4.17 Access Banner

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

To configure an access banner, follow the steps below

1. In privilege EXEC mode, enter configure terminal

   ```
   SWITCH# config terminal
   ```

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

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

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

   To clear a login banner use "no login banner"

4.18 Verify TOE Software

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

1. Enter show version and verify the version is 17.09

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

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

Table 6. Evaluated Software Images

Platform	Image
Cisco Catalyst Industrial Ethernet 9300	ie9k_iosxe.17.09.01.SPA.bin

4.19 Upgrade TOE Software

1. Place the downloaded image on a TFTP, FTP, or SFTP server that is reachable by the SWITCH.
2. At the SWITCH console enter: install add file [tftp | ftp | sftp://<IP Address of TFTP/FTP/SFTP server>] <image name.bin> activate commit

Note: Upon 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.

4.20 SSH Remote Administration Protocol

The TOE provides remote administration using SSH. The steps below provide instructions to configure SSH Server for the CC evaluated configuration. For additional information on SSH refer to the "Configuring Secure Shell" Chapter of [**4**].

1. In privileged EXEC mode, enter configure terminal

   ```
   SWITCH# configure terminal
   ```

2. Specify the host domain name applicable to the Switch

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

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

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

4. Assign the key pair to SSH

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

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

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

6. Configure the SSH Server Key Exchange

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

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

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

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

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

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

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

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

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

   b. Enter public-key configuration mode

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

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

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

d. Enter public-key data configuration mode

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

e. 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>
```

f. 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. Disable keyboard-interactive based authentication

```
SWITCH(config)# no ip ssh server authenticate user keyboard
```

11. 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.

```
SWITCH(config)# ip ssh rekey time 60

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

12. Display SSH configuration information

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

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
- Hostkey Algorithms: ssh-rsa (rsa-sha2-256, rsa-sha2-512)
- Encryption Algorithms: aes128-cbc, aes256-cbc
- MAC Algorithms: hmac-sha2-512, hmac-sha2-256
- KEX Algorithms: diffie-hellman-group14-sha1

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
    ```

Additional Information on SSH can be found in the Secure Shell Configuration Guide, Cisco IOS XE 17 [**5**].

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.

4.21 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
```

4.22 IPsec

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

1. With a syslog and RADIUS server operating as an IPsec peer of the TOE and the records tunneled over that connection.

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

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

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

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

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

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

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

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

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

4.23 Generating a Crypto Key Pair for IPsec

1. In privileged EXEC mode, enter configure terminal

   ```
   SWITCH# configure terminal
   ```

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

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

4.24 Create Trustpoints for IPsec

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

Note: You will set up the CRL certificate revocation mechanism used to ensure that the certificate of the IPsec peer has not been revoked. If the TOE is unable to obtain a CRL, the TOE will reject the peer's certificate and a "CRL fetch for trustpoint <trustpoint name> failed" message will appear in the message log (refer to section 6 for details on audit). The Administrator will need to enable the remote syslog server and/or remote login authentication as described below in sections 4.33 and 4.34, respectively, 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)# **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)# **chain-validation continue <root trustpoint name>**

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

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

a. If you generated a rsa key enter

```
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)# 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)# match key-usage cRLSign

SWITCH(ca-trustpoint)# exit
```

Additional Information on PKI can be found in the Public Key Infrastructure Configuration Guide, Cisco IOS-XE 17 [**8**].

4.25 IKEv2

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

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

   a. In privileged EXEC mode, enter configure terminal.

   ```
   SWITCH# configure terminal
   ```

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

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

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

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

   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-isakmp)# exit
   ```

2. Configure the IKEv2 Policy

   a. Define the IKEv2 policy name.

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

   b. Specify the proposal created in the previous section

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

   c. Enter exit to return to the main configuration mode

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

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

   a. Define the IKEv2 keyring.

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

b. Define the peer block

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

c. In peer sub mode specify the IPv4/IPv6 address of peer

SWITCH(config-ikev2-keyring-peer**)# address <IPv4 Address | IPv6 Address/prefix>**

d. Specify the IKEv2 peer through an identity address

SWITCH(config-ikev2-keyring-peer)# **identity address <IPv4 Address | IPv6 Address/prefix>**

e. Specify a pre-shared key.

To specify a text-based pre-shared key:

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

Note: Pre-shared keys on the TOE must be at least 22 characters in length and can be composed of any combination of upper and lower case letters, numbers, and special characters (that include: "!", "@", "#", "$", "%", "^", "&", "*", "(", and ")") and the characters found in table 5.

To specify a bit-based pre-shared key:

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

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

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

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

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

a. Define the IKEv2 Profile.

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

b. Set the local authentication method.

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

c. Set the remote authentication method.

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

d. Specify the local IKE FQDN identity to use.

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

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

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

f. Set the IKE SA lifetime in seconds.

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

g. Enter exit to return to the main configuration mode

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

4.26 IPsec Transform Sets and SA Lifetimes

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

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

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

1. Define the allowed transform sets.

   SWITCH(config)# **crypto ipsec transform-set <transform set tag> <esp-aes 128 | esp-aes 256> <esp-sha-hmac | esp-sha256-hmac | esp-sha512-hmac>**

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

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

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

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

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

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

4.27 IPsec Crypto Map and Access Control List

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

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

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

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

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

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

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

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

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

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

The set peer command specifies the ip address of the peer

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

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

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

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

```
SWITCH(config)# int GigabitEthernet1
```

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

```
SWITCH(config-if)# end
```

A crypto map set can contain multiple entries, each with a different access list. The crypto map entries are searched in a sequence--the router attempts to match the packet to the access list specified in that entry. When a packet matches a permit entry in a particular access list, and the corresponding crypto map entry is tagged connections are established, if necessary. If the crypto map entry is tagged as ipsec-isakmp, IPsec is triggered.

If there is no SA that the IPsec can use to protect this traffic to the peer, IPsec uses IKE to negotiate with the remote peer to set up the necessary IPsec SAs on behalf of the data flow. The negotiation uses information specified in the crypto map entry as well as the data flow information from the specific access list entry. Once established, the set of SAs (outbound to the peer) is then applied to the triggering packet and to subsequent applicable packets as those packets exit the Switch. "Applicable" packets are packets that match the same access list criteria that the original packet matched. For example, all applicable packets could be encrypted before being forwarded to the remote peer. The corresponding inbound SAs are used when processing the incoming traffic from that peer.

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

4.28 Security Policy Database (SPD)

RFC 4301 calls for an IPsec implementation to protect IP traffic through the use of a Security Policy Database (SPD). The SPD is used to define how IP packets are to be handled: PROTECT the packet (e.g., encrypt the packet), BYPASS the IPsec services (e.g., no encryption), or DISCARD the packet (e.g., drop the packet).
The traffic matching permit ACL would then flow through the IPsec tunnel and be classified as "PROTECTED".
Traffic that does not match a permit crypto map ACL and does not match a non-crypto permit ACL on the interface would be DISCARDED.
Traffic that does not match a permit ACL in the crypto map, but does match a non-crypto permit ACL would be allowed to BYPASS the tunnel. For example, a non-crypto permit ACL for ICMP would allow ping traffic to flow unencrypted if a permit crypto map was not configured that matches the ping traffic.

4.29 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. IKEv2 profiles can bind themselves to certificate maps, and the Switch will determine if they are valid during IKE authentication.

1. Start certificate-map mode

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

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

   For example:

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

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

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

4. Associate the certificate map to the IPsec trustpoint created in section 4.24

   ```
   SWITCH(config)# crypto pki trustpoint < subordinate trustpoint name>
   SWITCH(ca-trustpoint)# match certificate <attribute map tag>
   SWITCH(config-ikev2-profile)# end
   ```

4.30 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>
```

4.31 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.

4.32 Enable IKE and IPsec Logging

To generate the required audit events for IKE and IPsec perform the following steps

```
SWITCH# debug crypto ipsec
```

```
SWITCH# debug crypto ikev2
```

```
SWITCH# crypto logging ikev2
```

```
SWITCH# debug crypto isakmp
```

```
SWITCH# debug crypto engine
```

4.33 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 configure a remote syslog server enter the following command:

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

4.34 Configure Remote Login Authentication

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

1. Specify the RADIUS Server Name

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

2. Specify the RADIUS Server Address

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

3. Specify the RADIUS shared secret

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

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

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

5. Configure AAA for RADIUS

   a. Configure Group Server Name

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

b. Specify RADIUS Server Name

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

c. Type exit to return to the main configuration mode

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

For more information see the "Configuring RADIUS" section of [**4**].

4.35 Enable Remote Login Authentication

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

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

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

For more information see the "Configuring Authentication" section of [**4**].

4.36 IPsec References

For Cisco IPsec documentation references, see "Security for VPNs with IPsec Configuration Guide, Cisco IOS XE 17" [**6**] .

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

4.37 MACSEC and MKA Configuration

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

The following is an example of an MKA policy:

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

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

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

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

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

The following is an example of configuring MACsec PSK

```
SWITCH(config)# key chain keychain1 macsec
SWITCH(config-key-chain)# key 1000
SWITCH(config-key-chain)# cryptographic-algorithm aes-128-cmac
SWITCH(config-key-chain)# key-string 12345678901234567890123456789012
SWITCH(config-key-chain)# lifetime local 12:12:00 October 2 2022 12:19:00 October 2 203
SWITCH(config-mka-policy)# end
```

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

```
SWITCH(confing) interface GigabitEthernet1
SWITCH(config-if)# macsec network-link
SWITCH(config-if)# mka policy my_policy
SWITCH(config-if)# mka pre-shared-key key-chain mykeychain1
SWITCH(config-if) # macsec replay-protection window-size 10
SWITCH(config-if) # end
```

Detailed steps to configure MACsec and an MKA policy on the TOE can be found in the MACsec Encryption chapter of [**4**].

Configuration Examples for MACsec Encryption can be found in the "Configuring Examples for MACsec Encryption" section of [**4**].

To verify MACsec is enabled, refer to the "show" commands listed under **Step 2** of Scenario 2 in [**17**].

4.38 FIPS Mode

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

1. In privilege EXEC mode, enter configure terminal

```
SWITCH# config terminal
```

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

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

3. Exit configuration mode and return to privileged EXEC mode

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

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

4.39 Verify FIPS Mode

To verify FIPS mode enter the following

```
SWITCH# show fips status
```

The status of FIPS mode on the device will be displayed

For additional information, refer to the Secure Operation in FIPS Mode chapter of [**4**].

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 Unlock Locked-Out Account

Display a list of all locked out accounts:

```
SWITCH# show aaa local user lockout
```

Clear unsuccessful login attempts:

```
SWITCH# clear aaa local user fail-attempts
```

Unlock the account**:**

```
SWITCH# clear aaa local user lockout username
```

5.4 Cryptographic Self-Tests

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

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

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

5.5 Zeroize Private Key

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

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

The keys are zeroized immediately after use.

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

5.6 IPsec Session Interruption and Recovery

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

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

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

5.7 Update TOE Software

5.8 One-Shot Upgrade

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

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

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

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

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

       The image installation process will begin.

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

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

       ```
       SWITCH# show active install
       ```

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

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

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

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

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

All hardware SWITCH appliances will display at bootup a message that the image was successfully validated:

"RSA Signed RELEASE Image Signature Verification Successful."

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

verify bootflash:<image or package name>

5.9 Multi-Stage Upgrade

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

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

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

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

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

      The SWITCH will prompt for Source filename. Enter the name of the IE9300 bin image file.

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

   d. At the SWITCH console enter: install add file bootflash:<IE9300 bin file>

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

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

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

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

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

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

      SWITCH# **show active install**

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

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

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

      SWITCH# **install commit**

The SWITCH should respond that it successful committed the package.

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

   SWITCH# **show install summary**

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

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

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

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

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

All hardware SWITCH appliances will display at bootup a message that the image was successfully validated:

"RSA Signed RELEASE Image Signature Verification Successful."

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

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

6 Secure Management

6.1 User Roles

The IE9300 switches have both privileged and semi-privileged administrator roles as well as non-administrative access. Non-administrative access is granted to authenticated neighbor switches for the ability to receive updated routing tables per the information flow rules. There is no other access or functions associated with non-administrative access. These privileged and semi- privileged roles are configured in the Access Control and Session Termination section above. The TOE also allows for customization of other levels. Privileged access is defined by any privilege level entering an 'enable secret 5' after their individual login. ***Note:*** The command 'enable secret' is a replacement for the 'enable password' command since the 'enable secret' creates the password and stores it in encrypted. Privilege levels are number 0-15 that specifies the various levels for the user. The privilege levels are not necessarily hierarchical. Privilege level 15 has access to all commands on the TOE. Privilege levels 0 and 1 are defined by default, while levels 2-14 are undefined by default. Levels 0-14 can be set to include any of the commands available to the level
15 administrator and are considered the semi-privileged administrator for purposes of this evaluation. The privilege level determines the functions the user can perform, hence the authorized administrator with the appropriate privileges.

To establish a username-based authentication system, use the username command in global configuration mode.

```
SWITCH(config)# username name [privilege level]
```

When a user no longer requires access to the TOE, the user account can be removed. To remove an established username-based authentication account, use the "no" form of the command.

```
SWITCH(config)# no username name
```

Refer to the IOS Command Reference Guide for available commands and associated roles and privilege levels.

6.2 Passwords

The password complexity is not enforced by the switch by default, and must be administratively set in the configuration. The Authorized Administrator must configure the password policy using the authentication, authorization and accounting (AAA) CC policy. The Authorized Administrator must perform the following steps to set the AAA CC policy **[7]**:

1. Enable the new AAA CC policy:

```
SWITCH> enable
SWITCH# configure terminal
SWITCH(config)# aaa new-model
SWITCH(config)# aaa common-criteria policy <policy name>
SWITCH(config)# end
```

To prevent administrators from choosing insecure passwords, each password must be:

1. At least 8 characters long. Use the following command to set the minimum length to 8 or greater.

```
SWITCH (config)#security passwords min-length length
```

Example: SWITCH (config)# **security passwords min-length 8**

Note: Details for the **security passwords min-length** command can be found in the: **[7]** Under Reference Guides Cisco IOS Security Command Reference: Commands S to Z.

2. Composed of any combination of characters that includes characters for at least 3 of these four character sets: upper case letters, lower case letters, numerals, and the following special characters: "!", "@", "#", "$", "%", "^", "&", "*", "(", ")". Configure the switch to enforce that complexity requirement by using enabling "**aaa password restriction**".

   Example: SWITCH (config)# **aaa password restriction**

Enabling **aaa password restriction** will also enforce the following restrictions:

2. The new password cannot have any character repeated more than three times consecutively.
3. The new password cannot be the same as the associated username.
4. The password obtained by capitalization of the username or username reversed is not accepted.
5. The new password cannot be "cisco", "ocsic", or any variant obtained by changing the capitalization of letters therein, or by substituting "1", "|", or "!" for i, or by substituting "0" for "o", or substituting "$" for "s".

Note: The **aaa password restriction** command can only be used after the **aaa new-model** command is configured. **[7]** Under Reference Guides Cisco IOS Security Command Reference: *Commands A to C*.

The following configuration steps are optional but recommended for good password complexity. The below items are recommended but are not enforced by the TOE:

1. Does not contain more than three sequential characters, such as abcd
2. Does not contain dictionary words
3. Does not contain common proper names

Administrative passwords, including any "enable" password that may be set for any privilege level, must be stored in non-plaintext form. To have passwords stored as a SHA-256 hash, use the "**service password-encryption**" command in config mode.

SWITCH (config)#**service password-encryption**

Once that service has been enabled, passwords can be entered in plaintext, or has SHA-256 hash values, and will be stored as SHA-256 hash values in the configuration file when using the "username" command.

SWITCH (config)#**username** *name* {**password** *password* | **password** *encryption- type encrypted-password*}

Whether or not "service password-encryption" has been enabled, a password for an individual username can be entered in either plaintext or as a SHA-256 hash value, and be stored as a SHA- 256 hash value by using the following command:

SWITCH(config)#**username** *name* **secret** {**0** *password* | **4** *secret-string | 5 SHA256 secret-string*}

To store the enable password in non-plaintext form, use the '**enable secret'** command when setting the enable password. The enable password can be entered as plaintext, or as an MD5 hash value. Example:

SWITCH(config)#**enable secret** [**level** *level*] {*password* | **0** | **4** | **5** [*encryption-type*]
encrypted-password }

level - (Optional) Specifies the level for which the password applies. You can specify up to sixteen privilege levels, using the numerals 0 through 15.

password – password that will be entered

0 - Specifies an unencrypted clear-text password. The password is converted to a SHA256 secret and gets stored in the switch.

4 - Specifies an SHA256 encrypted secret string. The SHA256 secret string is copied from the switch configuration.

5 - Specifies a message digest alogrithm5 (MD5) encrypted secret.

encryption-type - (Optional) Cisco-proprietary algorithm used to encrypt the password. The encryption types available for this command are 4 and 5. If you specify a value for *encryption- type* argument, the next argument you supply must be an encrypted password (a password encrypted by a Cisco switch).

encrypted-password - Encrypted password that is copied from another switch configuration.

Use of enable passwords are not necessary, so all administrative passwords can be stored as SHA- 256 if enable passwords are not used.

Note: *Cisco no longer recommends that the 'enable password' command be used to configure a password for privileged EXEC mode. The password that is entered with the 'enable password' command is stored as plain text in the configuration file of the networking device. If passwords were created with the 'enable password' command, it can be hashed by using the 'service password-encryption' command. Instead of using the 'enable password' command, Cisco recommends using the 'enable secret' command because it stores a SHA-256 hash value of the password.*

To have IKE preshared keys stored in encrypted form, use the **password encryption aes** command to enable the functionality and the **key config-key password-encrypt** command to set the master password to be used to encrypt the preshared keys. The preshared keys will be stored encrypted with symmetric cipher Advanced Encryption Standard [AES].

SWITCH (config)# **password encryption aes**

SWITCH (config)# **key config-key password-encryption** [***text***]

Note: Details for the **password encryption aes** command can be found in the: **[7]** See manual *Cisco IOS Security Command Reference: Commands M to R*.

6.3 Clock Management

Clock management is restricted to the privileged administrator. Use the commands below to configuring the time and date:

```
SWITCH(config)# clock timezone [zone] hours-offset [minutes-offset]
SWITCH(config)# clock summer-time zone recurring [week day month hh:mm week day month hh:mm
[offset]]
SWITCH(config)# clock summer-time zone date date month year hh:mm:ss date month year hh:mm:ss
[offset]
SWITCH(config)# exit
SWITCH# clock set hh:mm:ss date month year
```

6.4 Identification and Authentication

Configuration of Identification and Authentication settings is restricted to the privileged administrator.

The IE9300 can be configured to use any of the following authentication methods:

6.4.1 Remote authentication (RADIUS)

Refer to "Authentication Server Protocols" elsewhere in Section 3.3.2 in this document.

6.4.2 Local authentication (password or SSH public key authentication);

Note: this should only be configured for local fallback if the remote authentication server is not available.

6.4.3 X.509v3 certificates

Refer to "Create Trustpoints for IPsec" in Section 4.24 above for more details and **[8].**

6.4.4 Login Banners

The TOE may be configured by the privileged administrators with banners using the **banner login** command. This banner is displayed before the username and password prompts. To create a banner of text "This is a banner" use the command

```
banner login c This is a banner c
```

where c is the delimiting character. The delimiting character may be any character except '?', and it must not be part of the banner message.

6.5 Configure Reference Identifier

When certificates are used for authentication, the distinguished name (DN) is verified to ensure the certificate is valid and is from a valid entity. The DN naming attributes in the certificate is compared with the expected DN naming attributes and deemed valid if the attribute types are the same and the values are the same and as expected. The fully qualified domain name (FQDN) can also be used as verification where the attributes in the certificate are compared with the expected CN: FQDN, CN: user FQDN and CN: IP Address.

This section describes configuration of the peer reference identifier which is achieved through configuring the DN attributes with 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. ISAKMP and ikev2 profiles can bind themselves to certificate maps, and the TOE will determine if they are valid during IKE authentication.

Note: *SAN is not supported for reference identifiers.*

Table 7 Reference Identifier Configuration

Step1	(config)# **crypto pki certificate map** *label sequence-number*	Starts certificate-map mode

Step2	*(ca-certificate-map)# field-name match-criteria match-value*	In ca-certificate-map mode, you specify one or more certificate fields together with their matching criteria and the value to match. • *field-name*—Specifies one of the following case-insensitive name strings or a date: –subject-name –issuer-name –unstructured-subject-name –alt-subject-name –name –valid-start –expires-on Note Date field format is dd mm yyyy hh:mm:ss or mm dd yyyy hh:mm:ss. • *match-criteria*—Specifies one of the following logical operators: –eq—Equal (valid for name and date fields) –ne—Not equal (valid for name and date fields) –co—Contains (valid only for name fields) –nc—Does not contain (valid only for name fields) –lt —Less than (valid only for date fields) –ge —Greater than or equal (valid only for date fields) • *match-value*—Specifies the name or date to test with the logical operator assigned by match-criteria.
Step3	(ca-certificate-map)# **exit**	Exits ca-certificate-map mode.
Step4	For IKEv1: crypto isakmp profile ikev1-profile1 match certificate *label* For IKEv2: crypto ikev2 profile ikev2-profile1 match certificate *label*	Associates the certificate-based ACL defined with the crypto pki certificate map command to the profile.

For example: To create a certificate map for IKEv1 to match four subject-name values of the peer enter:

```
# conf t
(config)# crypto pki certificate map cert-map-match-all 99 (ca-certificate-map)# subject-name co
cn=CC_PEER
(ca-certificate-map)# subject-name co o=ACME
(ca-certificate-map)# subject-name co ou=North America (ca-certificate-map)# subject-name co c=US
```

```
(ca-certificate-map)#exit
(config)# crypto isakmp profile ike1-profile-match-cert match certificate cert-map-match-all
```

FQDN attributes include the hostname, domain name and IP address:

Configure a hostname:

```
SWITCH# hostname SWITCH
```

Configure a domain name:

```
SWITCH# ip domain-name cisco.com
```

Configure an IP address:

```
SWITCH(config)#interface g0/0
SWITCH(config-if)#ip address 10.10.10.110 255.255.255.0
```

7 Security Relevant Events

Authorized Administrators must review audit records on a regular basis. Audit records can be viewed locally or from the remote syslog server. Audit records contain up to 80 characters and a percent sign (%), which follows the optional sequence number or time-stamp information. Audit records include the following information:

- sequence number – unique number assigned to an audit record
- timestamp - date and time of the message or event (format mm/dd hh:mm:ss or hh:mm:ss (short uptime or d h)
- facility - the facility to which the message refers (for example, SNMP, SYS, and so forth)
- severity - single-digit code indicating the severity of the event, range from 0 - 7
- MNEMONIC - text string that uniquely describes the message
- description - text string containing detailed information about the event
- hostname-n - hostname of a stack member and its switch number in the stack. Though the stack master is a stack member, it does not append its hostname to system messages

The Authorized Administrator can view audit records by entering the “show logging” CLI command [6].

Table 8 below provides sample audit records for the required auditable events; these records are a sample and not meant as an exact record for the event. In addition, for some cryptographic failures producing an audit record would require extensive manipulation and therefore snippets of source code are provided to illustrate what would be displayed in an audit record. The indication that the TSF self-test was completed successful is indicated by reaching a log-in prompt. If TSF self-test did not complete successfully, a system failure error message would be displayed

Table 8 General Auditable Events

Requirement	Auditable Events	Additional Audit Record Contents	Sample Record
FCS_MACSEC_EXT.1	Session establishment	Secure Channel Identifier (SCI)	**Session Establishment** Mar 15 2016 12:49:11.891 IST: %MKA-5-SESSION_START: (Te1/2 : 22) MKA Session started for RxSCI 188b.9d3c.c83f/0000, AuditSessionID 092B033C0000000E000C08B8, AuthMgr-Handle 45000002 Mar 15 2016 12:49:11.891 IST: MKA-EVENT: Started a new MKA Session on interface TenGigabitEthernet1/2 for Peer MAC 188b.9d3c.c83f with SCI80E0.1DC6.3E7F/0016 successfully
FCS_MACSEC_EXT.3.1	Creation and update of Secure Association Key	Creation and update times	**For SAK (Security Association Key) creation-** Mar 15 2016 12:54:49.937 IST: MKA-EVENT 80e0.1dc6.3e7f/0016 C7000003: Generation of new Latest SAK succeeded (Latest AN=0, KN=1)... **For SAK (Security Association Key) update –** Mar 15 2016 <tel:2016> 14:38:53.326 IST: %MKA-6-SAK_REKEY: (Gi0/1/0 : 10) MKA Session is beginning a SAK Rekey (current Latest AN/KN 0/1, Old AN/KN 0/1) for RxSCI f4cf.e298.ccb8/000a, AuditSessionID CKN 1000000000000000000000000000000000000000000000000000000000000000
FCS_MACSEC_EXT.4.4	Creation of Connectivity Association	Connectivity Association Key Names	**Creation of Connectivity Association** Mar 15 2016 <Gi1/0/2 : 9> 14:38:53.326 IST: %MKA-5-SESSION_SECURED: (Gi1/0/2 : 9) MKA Session was secured for RxSCI 90e2.ba12.a00d/0000, AuditSessionID 000000000000000D001C2D92, CKN 24AA15376050334AE1EA9BE8A1D0894B00000000000000000000000000000000
FCS_IPSEC_EXT.1	Failure to establish an IPsec SA.	Reason for failure.	**Failed to find matching policy (General)** <47>12048: IE9300: *Nov 16 2022 14:43:24: IKEv2:Received Packet [From 192.168.144.254:500/To 192.168.144.50:500/VRF i0:f0] <43>12092: IE9300: *Nov 16 2022 14:43:24: %IKEV2-3-NEG_ABORT: Negotiation aborted due to ERROR: Failed to find a matching policy **Invalid transform proposal received (bad ESP cipher)**

Requirement	Auditable Events	Additional Audit Record Contents	Sample Record
			<47>5309: IE9300: *Nov 16 2022 13:27:45: IKEv2:Received Packet [From 192.168.144.254:500/To 192.168.144.50:500/VRF i0:f0] <47>5492: IE9300: *Nov 16 2022 13:27:45: IPSEC(ipsec_process_proposal): invalid transform proposal received: <47>5493: IE9300: {esp-gcm } <47>5496: IE9300: *Nov 16 2022 13:27:45: IKEv2-ERROR:(SESSION ID = 7,SA ID = 1):Received Policies: : Failed to find a matching policyESP: Proposal 1: AES-GCM-128 Don't use ESN **Failed to find matching proposal (bad IKE cipher)** <47>7471: IE9300: *Nov 16 2022 13:53:20: IKEv2:Received Packet [From 192.168.144.254:500/To 192.168.144.50:500/VRF i0:f0] <47>7501: IE9300: *Nov 16 2022 13:53:20: IKEv2-ERROR:(SESSION ID = 14,SA ID = 1):Received Policies: : Failed to find a matching policyProposal 1: AES-GCM-128 SHA256 SHA256 DH_GROUP_2048_MODP/Group 14 <47>7502: IE9300: *Nov 16 2022 13:53:20: IKEv2-ERROR:(SESSION ID = 14,SA ID = 1):Expected Policies: : Failed to find a matching policyProposal 1: AES-CBC-128 AES-CBC-256 SHA256 SHA96 SHA256 SHA512 DH_GROUP_2048_MODP/Group 14 <47>7504: IE9300: *Nov 16 2022 13:53:20: IKEv2:(SESSION ID = 14,SA ID = 1):Sending no proposal chosen notify **Failed to validate certificate (Bad Reference Identifier)** <47>11334: IE9300: Feb 22 2023 16:12:18: IKEv2:Received Packet [From 192.168.144.254:500/To 192.168.144.50:500/VRF i0:f0] <47>11728: IE9300: Feb 22 2023 16:12:18: CRYPTO_PKI: Checking cert map authorization <43>11732: IE9300: Feb 22 2023 16:12:18: %PKI-3-CERTIFICATE_INVALID_UNAUTHORIZED: Certificate chain validation has failed. Unauthorized
FCS_SSHS_EXT.1	Failure to establish an SSH session	Reason for failure.	**No matching cipher** <43>3591: IE9300: Apr 13 2023 03:28:47: %SSH-3-NO_MATCH: No matching cipher found: client aes128-ctr server aes256-cbc,aes128-cbc <45>3592: IE9300: Apr 13 2023 03:28:47: %SSH-5-SSH2_SESSION: SSH2 Session request from 172.16.16.254 (tty = 0) using crypto cipher '', hmac '' Failed <45>3593: IE9300: Apr 13 2023 03:28:47: %SSH-5-SSH2_CLOSE: SSH2 Session from 172.16.16.254 (tty = 0) for user '' using crypto cipher '', hmac '' closed

Requirement	Auditable Events	Additional Audit Record Contents	Sample Record
			No matching host key type <43>3595: IE9300: Apr 13 2023 03:42:33: %SSH-3-NO_MATCH: No matching hostkey algorithm found: client ssh-rsa server rsa-sha2-256,rsa-sha2-512 <45>3596: IE9300: Apr 13 2023 03:42:33: %SSH-5-SSH2_SESSION: SSH2 Session request from 172.16.16.254 (tty = 0) using crypto cipher '', hmac '' Failed <45>3597: IE9300: Apr 13 2023 03:42:33: %SSH-5-SSH2_CLOSE: SSH2 Session from 172.16.16.254 (tty = 0) for user '' using crypto cipher '', hmac '' closed **No matching MAC** <43>3598: IE9300: Apr 13 2023 04:03:38: %SSH-3-NO_MATCH: No matching mac found: client hmac-sha1 server hmac-sha2-512,hmac-sha2-256 <45>3599: IE9300: Apr 13 2023 04:03:38: %SSH-5-SSH2_SESSION: SSH2 Session request from 172.16.16.254 (tty = 0) using crypto cipher '', hmac '' Failed <45>3600: IE9300: Apr 13 2023 04:03:38: %SSH-5-SSH2_CLOSE: SSH2 Session from 172.16.16.254 (tty = 0) for user '' using crypto cipher '', hmac '' closed **No matching key exchange method** <43>3601: IE9300: Apr 13 2023 04:14:40: %SSH-3-NO_MATCH: No matching kex algorithm found: client ecdh-sha2-nistp256,ext-info-c server diffie-hellman-group14-sha1 <45>3602: IE9300: Apr 13 2023 04:14:40: %SSH-5-SSH2_SESSION: SSH2 Session request from 172.16.16.254 (tty = 0) using crypto cipher '', hmac '' Failed <45>3603: IE9300: Apr 13 2023 04:14:40: %SSH-5-SSH2_CLOSE: SSH2 Session from 172.16.16.254 (tty = 0) for user '' using crypto cipher '', hmac '' closed **Oversized Packet** <43>3577: IE9300: Apr 13 2023 03:14:56: %SSH-3-BAD_PACK_LEN: Bad packet length 33068 <46>3578: IE9300: Apr 13 2023 03:14:56: %SYS-6-LOGOUT: User admin has exited tty session 1(172.16.16.254)
FIA_AFL.1	Unsuccessful login attempts limit is met or exceeded.	Origin of the attempt (e.g., IP address).	<189>61076: IE9320: *Sep 27 2023 08:13:40: %AAA-5-USER_LOCKED: User user1 locked out on authentication failure

Requirement	Auditable Events	Additional Audit Record Contents	Sample Record
	Administrator lockout due to excessive authentication failures		<44>58606: IE9300: Mar 28 2023 06:11:11: %SEC_LOGIN-4-LOGIN_FAILED: Login failed [user: TestUser17674] [Source: 172.16.16.254] [localport: 22] [Reason: Login Authentication Failed] at 01:11:11 EST Tue Mar 28 2023
FIA_UIA_EXT.1	All use of the identification and authentication mechanism.	Origin of the attempt (e.g., IP address).	See Audit events in FIA_UAU_EXT.2
FIA_UAU_EXT.2	All use of the authentication mechanism.	Origin of the attempt (e.g., IP address).	**Console** **Success** <189>61076: IE9320: *Sep 27 2023 08:13:40: %AAA-5-USER_LOCKED: User user1 locked out on authentication failure **Failure** <188>359: IE9320: *Aug 31 2023 13:31:51: %SEC_LOGIN-4-LOGIN_FAILED: Login failed [user: admin] [Source: LOCAL] [localport: 0] [Reason: Login Authentication Failed] at 09:31:51 EDT Thu Aug 31 2023 **SSH Authentication Success – Password** <45>3552: IE9300: Apr 13 2023 01:46:38: %SEC_LOGIN-5-LOGIN_SUCCESS: Login Success [user: admin] [Source: 172.16.16.254] [localport: 22] at 20:46:38 EST Wed Apr 12 2023 <45>3553: IE9300: Apr 13 2023 01:46:38: %SSH-5-SSH2_USERAUTH: User 'admin' authentication for SSH2 Session from 172.16.16.254 (tty = 0) using crypto cipher 'aes128-cbc', hmac 'hmac-sha2-256' Succeeded **SSH Authentication Failure – Password** <44>3566: IE9300: Apr 13 2023 02:59:27: %SEC_LOGIN-4-LOGIN_FAILED: Login failed [user: admin] [Source: 172.16.16.254] [localport: 22] [Reason: Login Authentication Failed] at 21:59:27 EST Wed Apr 12 2023 <45>3567: IE9300: Apr 13 2023 02:59:27: %SSH-5-SSH2_USERAUTH: User '' authentication for SSH2 Session from 172.16.16.254 (tty = 0) using crypto cipher 'aes128-cbc', hmac 'hmac-sha2-256' Failed

Requirement	Auditable Events	Additional Audit Record Contents	Sample Record
			SSH Authentication Success – Public Key <45>69666: IE9300: Apr 7 2023 03:40:31: %SEC_LOGIN-5-LOGIN_SUCCESS: Login Success [user: testadmin] [Source: 172.16.16.254] [localport: 22] at 22:40:31 EST Thu Apr 6 2023 <45>69667: IE9300: Apr 7 2023 03:40:31: %SSH-5-SSH2_USERAUTH: User 'testadmin' authentication for SSH2 Session from 172.16.16.254 (tty = 0) using crypto cipher 'aes256-cbc', hmac 'hmac-sha2-256' Succeeded **SSH Authentication Failure – Public Key** <191>3787: IE9320: *Sep 22 18:41:25.440: SSH2 1: failed: Pubkey Authentication ssh2_authenticate_pubkey for user 'admin2'<191>3785: IE9320: *Sep 22 18:41:25.440: SSH2 1: ssh2_validate_pubkey: Verifying pubkey blob is acceptable for 'admin2' in SSH2_MSG_USERAUTH_REQUEST <191>3786: IE9320: *Sep 22 18:41:25.440: SSH2 1: ssh2_validate_pubkey: Publickey for 'admin2' not found <191>3787: IE9320: *Sep 22 18:41:25.440: SSH2 1: failed: Pubkey Authentication ssh2_authenticate_pubkey for user 'admin2'
FIA_X509_EXT.1	Unsuccessful attempt to validate a certificate Any addition, replacement or removal of trust anchors in the TOE's trust store	Reason for failure Identification of certificates added, replaced or removed as trust anchor in the TOE's trust store	**Expired Server Cert** <47>4151: IE9300: Feb 2 2023 08:35:30: IKEv2:Received Packet [From 192.168.144.254:500/To 192.168.144.50:500/VRF i0:f0] <47>4219: IE9300: Feb 2 2023 08:35:30: IKEv2-ERROR:Current time is more than cert validity time **Expired SubCA Cert** <47>4263: IE9300: Feb 2 2023 08:36:25: IKEv2:Received Packet [From 192.168.144.254:500/To 192.168.144.50:500/VRF i0:f0] <43>4426: IE9300: Feb 2 2023 08:36:25: %PKI-3-CERTIFICATE_INVALID_EXPIRED: Certificate chain validation has failed. The certificate (SN: 13) has expired. Validity period ended on 2022-11-29T00:45:00Z **Absent or invalid basicConstraint flag** <47>9890: IE9300: Feb 2 2023 18:42:27: IKEv2:Received Packet [From 192.168.144.254:500/To 192.168.144.50:500/VRF i0:f0] <47>10038: IE9300: Feb 2 2023 18:42:27: IKEv2:(SESSION ID = 18,SA ID = 1):Verify cert failed

Requirement	Auditable Events	Additional Audit Record Contents	Sample Record
			<47>10036: IE9300: Feb 2 2023 18:42:27: IKEv2:(SA ID = 1):[PKI -> IKEv2] Validation of certificate chain FAILED **Revoked Certificate** <47>5136: IE9300: Feb 2 2023 08:38:09: IKEv2:Received Packet [From 192.168.144.254:500/To 192.168.144.50:500/VRF i0:f0] <43>5571: IE9300: Feb 2 2023 08:38:10: %PKI-3-CERTIFICATE_REVOKED: Certificate chain validation has failed. The certificate (SN: 00D1) is revoked **Corrupt Cert ASN1** <47>8123: IE9300: Feb 2 2023 08:44:45: IKEv2:Received Packet [From 192.168.144.254:500/To 192.168.144.50:500/VRF i0:f0] <47>8257: IE9300: Feb 2 2023 08:44:45: CRYPTO_PKI: status = 0x705(E_INPUT_DATA : invalid encoding format for input data): BER/DER decoding of certificate has failed **Corrupt Cert Signature** <47>8307: IE9300: Feb 2 2023 08:45:41: IKEv2:Received Packet [From 192.168.144.254:500/To 192.168.144.50:500/VRF i0:f0] <47>8657: IE9300: Feb 2 2023 08:45:41: ../cert-c/source/vericert.c(145) : E_INVALID_SIGNATURE : error verifying digitial signature **Corrupt Public Key** <47>8720: IE9300: Feb 2 2023 09:03:26: IKEv2:Received Packet [From 192.168.144.254:500/To 192.168.144.50:500/VRF i0:f0] <47>9069: IE9300: Feb 2 2023 09:03:26: ../cert-c/source/vericert.c(145) : E_INVALID_SIGNATURE : error verifying digitial signature **CRL Incorrectly Signed** 187>20144: IE9320: Sep 5 2023 18:25:30: %PKI-3-CRL_INSERT_FAIL: CRL download for trustpoint "gss_rootca-rsa" has been discarded. <187>20145: IE9320: Reason : failed to verify CRL signature <47>6992: IE9300: Feb 2 2023 08:41:05: CRYPTO_PKI: CRL verify has failed **Invalid Certificate Chain** <47>9314: IE9300: Feb 2 2023 17:38:45: IKEv2:Received Packet [From 192.168.144.254:500/To 192.168.144.50:500/VRF i0:f0]

Requirement	Auditable Events	Additional Audit Record Contents	Sample Record
			<47>9461: IE9300: Feb 2 2023 17:38:45: IKEv2:(SA ID = 1):[PKI -> IKEv2] Validation of certificate chain FAILED **Unreachable Revocation Server** <47>10926: IE9300: Feb 2 2023 19:02:37: IKEv2:Received Packet [From 192.168.144.254:500/To 192.168.144.50:500/VRF i0:f0] <43>11311: IE9300: Feb 2 2023 19:02:45: %PKI-3-CRL_FETCH_FAIL: CRL fetch for trustpoint rootca-rsa failed **Add Trust Anchor** See FMT_SMF.1 **Remove Trust Anchor** See FMT_SMF.1
FMT_MOF.1/ManualUpdate	Any attempt to initiate a manual update	None.	<189>465: IE9320: *Sep 27 2023 01:50:34: %INSTALL-5-INSTALL_COMPLETED_INFO: Switch 1 R0/0: install_mgr: Completed install add_activate_commit
FMT_MOF.1/Services	Starting and stopping of Services	None.	Jul 19 12:10:00 toe-loopback 289: *Jul 19 2018 12:10:00.678: \%SYS-6-LOGGINGHOST_STARTSTOP: Logging to host 10.24.0.1 port 514 started - CLI initiated Jul 19 12:09:51 toe-loopback 282: *Jul 19 2018 12:09:51.963: \%SYS-6-LOGGINGHOST_STARTSTOP: Logging to host 10.24.0.1 port 514 stopped - CLI initiated
FMT_MTD.1/CryptoKeys	Management of Cryptographic keys	None.	**Crypto keys (generating and deleting):** Feb 17 2013 16:14:47: %PARSER-5-CFGLOG_LOGGEDCMD: User:test_admin logged command: crypto key generate Feb 17 2013 16:37:27: %PARSER-5-CFGLOG_LOGGEDCMD: User:test_admin logged command:crypto key zeroize See all other records in Table 8 “Auditable Administrative Events”.
FMT_SMF.1	All management activities of TSF data	None.	**Resetting of passwords:** Nov 21 2017 15:06:53.679: \%PARSER-5-CFGLOG_LOGGEDCMD: User:admin logged command:no enable password

Requirement	Auditable Events	Additional Audit Record Contents	Sample Record
			Nov 21 2017 15:06:53.724: \%PARSER-5-CFGLOG_LOGGEDCMD: User:admin logged command:no username script privilege 15 password 0 password Nov 21 2017 15:08:54.042: \%PARSER-5-CFGLOG_LOGGEDCMD: User:admin logged command:username script privilege 15 password 0 secret Nov 21 2017 15:08:54.070: \%PARSER-5-CFGLOG_LOGGEDCMD: User:admin logged command:enable password secret See all other records in Table 8 "Auditable Administrative Events".
FPT_STM_EXT.1	Discontinuous changes to time - either Administrator actuated or changed via an automated process.	For discontinuous changes to time: The old and new values for the time. Origin of the attempt to change time for success and failure (e.g., IP address).	**Administrator Actions:** **Manual changes to the system time:** Feb 5 2013 06:28:00.000: %SYS-6-CLOCKUPDATE: System clock has been updated from 11:27:52 UTC Tue Feb 5 2013 to 06:28:00 UTC Tue Feb 5 2013, configured from console by admin on console.
FPT_RPL.1	Detected replay attempt	None.	*Jul 7 18:43:14.595: %MKA-3-MKPDU_VALIDATE_FAILURE: (Gi0/0/1 : 11) Validation of a MKPDU failed for RxSCI 6412.25a1.a409/0009, AuditSessionID , CKN 1234000000000000000000000000000000000000000000000000000000000000
FPT_TUD_EXT.1	Initiation of update. result of the update attempt (success or failure)	None.	**Success:** <46>2883: IE9300: May 19 2023 03:18:34: %HA_EM-6-LOG: cli_log: User:admin via Port:0 Executed[install add file activate commit] <45>2884: IE9300: May 19 2023 03:18:34: %INSTALL-5-INSTALL_START_INFO: Switch 1 R0/0: install_mgr: Started install add_activate_commit flash: ie9k-universalk9.17.09.03.SPA.bin <45>2888: IE9300: May 19 2023 03:21:36: %INSTALL-5-INSTALL_COMPLETED_INFO: Switch 1 R0/0: install_mgr: Completed install add_activate_commit **Failure:**

Requirement	Auditable Events	Additional Audit Record Contents	Sample Record
			<46>2910: IE9300: May 10 2023 05:08:01: %HA_EM-6-LOG: cli_log: User:admin via Port:0 Executed[install add file tftp://172.16.16.250/ ess3x00-universalk9.17.09.03-modified.SPA.bin activate commit] <45>2911: IE9300: May 10 2023 05:08:01: %INSTALL-5-INSTALL_START_INFO: Switch 1 R0/0: install_mgr: Started install add_activate_commit ess3x00-universalk9.17.09.03-modified.SPA.bin <43>2912: IE9300: May 10 2023 05:08:51: %INSTALL-3-OPERATION_ERROR_MESSAGE: Switch 1 R0/0: install_mgr: Failed to install add_activate_commit package tftp://****/ess3x00-universalk9.17.09.03-modified.SPA.bin, Error:
FTA_SSL_EXT.1	The termination of a local session by the session locking mechanism.	None.	**In the TOE this is represented by login attempts that occur after the timeout of a local administrative user.** <190>61125: IE9320: *Sep 27 2023 08:27:30: %SYS-6-TTY_EXPIRE_TIMER: (exec timer expired, tty 0 (0.0.0.0)), user testuser1 <190>61126: IE9320: *Sep 27 2023 08:27:30: %SYS-6-LOGOUT: User testuser1 has exited tty session 0()
FTA_SSL.3	The termination of a *remote* session by the session locking mechanism.	None.	**Audit record generated when SSH session is terminated because of idle timeout:** May 29 2012 15:18:00 UTC: %SYS-6-TTY_EXPIRE_TIMER: (exec timer expired, tty 0 (0.0.0.0)), user admin
FTA_SSL.4	The termination of an interactive session.	None.	**SSH** <46>2919: IE9300: Apr 25 2023 04:25:24: %HA_EM-6-LOG: cli_log: User:admin via Port:1 Executed[exit] <46>2920: IE9300: Apr 25 2023 04:25:24: %SYS-6-LOGOUT: User admin has exited tty session 1(172.16.16.254) <45>2921: IE9300: Apr 25 2023 04:25:24: %SSH-5-SSH2_CLOSE: SSH2 Session from 172.16.16.254 (tty = 0) for user 'admin' using crypto cipher 'aes256-cbc', hmac 'hmac-sha2-256' closed **Local Console** <46>10916: IE9300: Nov 2 2022 03:04:58: %HA_EM-6-LOG: cli_log: User:admin via Port:0 Executed[exit] <46>10917: IE9300: Nov 2 2022 03:04:58: %SYS-6-LOGOUT: User admin has exited tty session 0()
FTP_ITC.1	Initiation of the trusted channel. Termination of the trusted channel.	Identification of the initiator and target of failed trusted	**IPsec** <45>3074: IE9300: *Nov 16 2022 12:10:28: %IKEV2-5-SA_UP: SA UP <45>3075: IE9300: *Nov 16 2022 12:10:28: %CRYPTO-5-IKEV2_SESSION_STATUS: Crypto tunnel v2 is UP. Peer 192.168.144.254:4500 Id: 192.168.144.254

Requirement	Auditable Events	Additional Audit Record Contents	Sample Record
	Failure of the trusted channel functions.	channels establishment attempt.	<47>3160: IE9300: *Nov 16 2022 12:10:28: IKEv2:(SESSION ID = 1,SA ID = 1):(SA ID = 1):[IPsec -> IKEv2] Creation of IPsec SA into IPsec database PASSED <47>3185: IE9300: *Nov 16 2022 12:10:33: IKEv2:(SESSION ID = 1,SA ID = 1):Deleting SA <45>3186: IE9300: *Nov 16 2022 12:10:33: %IKEV2-5-SA_DOWN: SA DOWN <45>3187: IE9300: *Nov 16 2022 12:10:33: %CRYPTO-5-IKEV2_SESSION_STATUS: Crypto tunnel v2 is DOWN. Peer 192.168.144.254:4500 Id: 192.168.144.254 **MACsec** <191>7188: Jun 5 2023 17:51:13: MKA-EVENT a0f8.4915.cd81/0000 CC00000D: >> FSM - Initializing MKA Session for PSK keychain on interface GigabitEthernet1/0/1 with SCI A0F8.4915.CD81/0009. <189>4199: Jun 26 2023 20:48:18: %MKA-5-SESSION_STOP: (Gi1/0/1 : 9) MKA Session stopped by MKA for RxSCI 0015.5d90.160e/0001, AuditSessionID , CKN 1000 <187>3148: Jun 5 2023 14:43:40: %MKA-3-MKPDU_VALIDATE_FAILURE: (Gi1/0/1 : 9) Validation of a MKPDU failed for RxSCI 0015.5d90.160e/0001, AuditSessionID , CKN 1000
FTP_TRP.1	Initiation of the trusted channel. Termination of the trusted channel. Failures of the trusted path functions.	None.	See FIA_UIA_EXT.2 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

Table 9 Auditable Administrative Events

Requirement	Management Action to Log	Sample Log
FAU_GEN.1: Audit data generation	Startup and Shutdown of Audit Function Clear logs	**Startup and shutdown of Audit function:** *Sep 27 15:12:00.726: %SYS-5-RESTART: System restarted – **Clear logs:** *Sep 27 15:46:15.399: %HA_EM-6-LOG: cli_log: host[IE9310] user[lab] port[2] exec_lvl[15] command[clear logging] Executed
FAU_GEN.2: User identity association	None	N/A
FAU_STG_EXT.1: External audit trail storage	Configuration of syslog export settings	Feb 17 2013 17:05:16: %PARSER-5-CFGLOG_LOGGEDCMD: User:test_admin logged command:logging host
FCS_CKM.1: Cryptographic key generation (for asymmetric keys)	Manual key generation	Feb 17 2013 16:14:47: %PARSER-5-CFGLOG_LOGGEDCMD: User:test_admin logged command: crypto key generate rsa modulus 2048 label Feb 17 2013 16:37:27: %PARSER-5-CFGLOG_LOGGEDCMD: User:test_admin logged command:crypto key zeroize rsa
FCS_CKM_EXT.4: Cryptographic key zeroization	Manual key zeroization	Feb 17 2013 16:37:27: %PARSER-5-CFGLOG_LOGGEDCMD: User:test_admin logged command:crypto key zeroize
FCS_COP.1/DataEncryption: Cryptographic operation (for data encryption/decryption)	None	N/A
FCS_COP.1/SigGen: Cryptographic operation (for cryptographic signature)	None	N/A
FCS_COP.1/Hash: Cryptographic operation (for cryptographic hashing)	None	N/A

Requirement	Management Action to Log	Sample Log
FCS_COP.1/KeyedHash: Cryptographic operation (for keyed-hash message authentication)	None	N/A
FCS_RBG_EXT.1: Cryptographic operation (random bit generation)	None	N/A
FCS_IPSEC_EXT.1	Configuration of IPsec settings: including mode, security policy, IKE version, algorithms, lifetimes, DH group, and certificates.	Feb 17 2013 16:14:47: %PARSER-5-CFGLOG_LOGGEDCMD: User:test_admin logged command: crypto isakmp policy 1
FCS_MACSEC_EXT.1		**Generate a PSK based CAK and install it in the device** <189>3090: Jun 26 2023 20:03:02: %PARSER-5-CFGLOG_LOGGEDCMD: User:admin logged command:key-string * **Manage the Key Server to create, delete, and activate MKA participants [as specified in 802.1X, sections 9.13 and 9.16 (cf. MIB object ieee8021XKayMkaParticipantEntry) and section. 12.2 (cf. function createMKA())];** Create/Activate: <191>3158: Jun 26 2023 20:03:13: MKA-EVENT: Created New CA 0x80007F603BC25BA8 Participant on interface GigabitEthernet1/0/3 with SCI A0F8.4915.CD83/000B for Peer MAC a0f8.4915.cd83. Delete: <191>4266: Jun 26 2023 20:48:28: MKA-EVENT: Deleting MKA Session on interface GigabitEthernet1/0/3 & Bring-Down-Dot1x is TRUE. **Specify a lifetime of a CAK**

Requirement	Management Action to Log	Sample Log
		<189>5564: Jun 5 2023 17:04:17: %PARSER-5-CFGLOG_LOGGEDCMD: User:admin logged command:lifetime local 13:04:16 Jun 05 2023 duration 600 **Enable, disable, or delete a PSK based CAK using [CLI management commands]** Enable: <189>3090: Jun 26 2023 20:03:02: %PARSER-5-CFGLOG_LOGGEDCMD: User:admin logged command:key-string * Disable/Delete: <189>10019: Jun 29 2023 21:50:45: %PARSER-5-CFGLOG_LOGGEDCMD: User:admin logged command:no key-string
FCS_SSH_EXT.1	Configuration of SSH settings: including certificates or passwords, algorithms, host names, users.	Feb 17 2013 16:14:47: %PARSER-5-CFGLOG_LOGGEDCMD: User:test_admin logged command: ip ssh version 2
FIA_AFL.1	Configuring number of failures. Unlocking the user.	Feb 17 2013 16:14:47: %PARSER-5-CFGLOG_LOGGEDCMD: User:test_admin logged command: aaa local authentication attempts max-fail [number of failures] Feb 7 2013 02:05:41.953: %AAA-5-USER_UNLOCKED: User user unlocked by admin on vty0 (21.0.0.1)
FIA_PMG_EXT.1: Password management	Setting length requirement for passwords.	Feb 15 2013 13:12:25.055: %PARSER-5-CFGLOG_LOGGEDCMD: User:cisco logged command: security passwords min-length 15
FIA_PSK_EXT.1: Pre-Shared Key Composition	Creation of a pre-shared key.	<189>516: IE9320: *Oct 2 2023 13:59:52: %PARSER-5-CFGLOG_LOGGEDCMD:

Requirement	Management Action to Log	Sample Log
		User:admin logged command:pre-shared-key 0 password
FIA_UIA_EXT.1: User identification and authentication	Logging into TOE.	Jan 17 2013 05:05:49.460: %SEC_LOGIN-5-LOGIN_SUCCESS: Login Success [user: ranger] [Source: 21.0.0.3] [localport: 22] at 00:05:49 EST Thu Jan 17 2013
FIA_UAU_EXT.2: Password-based authentication mechanism	None	N/A
FIA_UAU.7: Protected authentication feedback	None	N/A
FIA_X509_EXT.1/Rev: X.509 Certificates	Generating a certificate.	<189>520: IE9320: *Oct 2 2023 14:10:39: %PARSER-5-CFGLOG_LOGGEDCMD: User:admin logged command:crypto key generate rsa modulus 2048 label *
FIA_X509_EXT.2	None.	None.
FIA_X509_EXT.3	None.	None.
FMT_MOF.1/ManualUpdate: Management of Security Functions Behavior	See all other rows in table.	N/A
FMT_MTD.1/CoreData: Management of TSF data (for general TSF data)	See all other rows in table.	N/A
FMT_SMF.1: Specification of management functions	See all other rows in table.	N/A
FMT_SMR.2: Restrictions on Security roles	Configuring administrative users with specified roles.	Feb 15 2013 13:12:25.055: %PARSER-5-CFGLOG_LOGGEDCMD: User:cisco logged command: username admin 15

Requirement	Management Action to Log	Sample Log
FPT_SKP_EXT.1: Protection of TSF Data (for reading of all symmetric keys)	None	N/A
FPT_APW_EXT.1: Protection of Administrator Passwords	None	N/A
FPT_STM_EXT.1: Reliable time stamps	Manual changes to the system time.	Feb 5 2013 06:28:00.000: %SYS-6-CLOCKUPDATE: System clock has been updated from 11:27:52 UTC Tue Feb 5 2013 to 06:28:00 UTC Tue Feb 5 2013, configured from console by admin on console.
FPT_TUD_EXT.1: Trusted update	Software updates	<46>2883: IE9300: May 19 2023 03:18:34: %HA_EM-6-LOG: cli_log: User:admin via Port:0 Executed[install add file activate commit]
FPT_TST_EXT.1: TSF testing	None	N/A
FTA_SSL_EXT.1: TSF-initiated session locking	Specifying the inactivity time period.	Feb 15 2013 13:12:25.055: %PARSER-5-CFGLOG_LOGGEDCMD: User:cisco logged command: exec-timeout 60
FTA_SSL.3: TSF-initiated termination	Specifying the inactivity time period.	Feb 15 2013 13:12:25.055: %PARSER-5-CFGLOG_LOGGEDCMD: User:cisco logged command: exec-timeout 60
FTA_SSL.4: User-initiated termination	Logging out of TOE.	**SSH** <190>11096: IE9320: Apr 6 2023 04:14:13: %HA_EM-6-LOG: cli_log: User:TestUser5142 via Port:2 Executed[exit]

Requirement	Management Action to Log	Sample Log
		<190>11097: IE9320: Apr 6 2023 04:14:13: %SYS-6-LOGOUT: User TestUser5142 has exited tty session2(172.16.16.254) <189>11098: IE9320: Apr 6 2023 04:14:13: %SSH-5-SSH2_CLOSE: SSH2 Session from 172.16.16.254 (tty = 0) for user 'TestUser5142' using crypto cipher 'aes256-cbc', hmac 'hmac-sha2-256' closed **Local Console** <190>1156: IE9320: Apr 13 2023 05:05:19: %HA_EM-6-LOG: cli_log: User:admin via Port:0 Executed[exit] <190>1157: IE9320: Apr 13 2023 05:05:19: %SYS-6- LOGOUT: User admin has exited tty session 0()
FTA_TAB.1: Default TOE access banners	Configuring the banner displayed prior to authentication.	Feb 15 2013 13:12:25.055: %PARSER-5-CFGLOG_LOGGEDCMD: User:cisco logged command: banner login d This is a banner d
FTP_ITC.1: Inter-TSF trusted channel	None	N/A
FTP_TRP.1: Trusted path	Connecting to the TOE with SSH.	Jan 17 05:05:49.460: %SEC_LOGIN-5-LOGIN_SUCCESS: Login Success [user: Cisco] [Source: 21.0.0.3] [localport: 22] at 00:05:49 EST Thu Jan 17 2013

7.1 Managing Audit Records

The TOE provides the privileged Administrator the ability to manage local audit records stored within the TOE. Audit logging is enabled by default on the TOE.

Configuring the audit log severity level is done with the **logging buffered** command.

Switch(config)# **logging buffered <0-7>**

Severity levels:

1 – Alerts

2 – Critical

3 – Errors
4 – Warnings
5 – Notifications
6 – Informational
7 – Debugging

Viewing the audit log is done with the **show logging** command.

```
Switch# show logging
```

Clearing the audit log is done with the **clear logging** command.

```
Switch# clear logging
```

8 Network Services and Protocols

The table below lists the network services/protocols available on the TOE as a client (initiated outbound) and/or server (listening for inbound connections), all of which run as system-level processes. The table indicates whether each service or protocol is allowed to be used in the certified configuration.

For more detail about each service, including whether the service is limited by firewall mode (routed or transparent), or by context (single, multiple, system), refer to the ***Command Reference*** guides listed in Table 2.

Table 10 Protocols and Services

Service or Protocol	Description	Client (initiating)	Allowed	Server (terminating)	Allowed	Allowed use in the certified configuration
AH	Authentication Header (part of IPsec)	Yes	No	Yes	No	No, ESP must be used in all IPsec connections. Protocol is not considered part of the evaluation.
DHCP	Dynamic Host Configuration Protocol	Yes	Yes	Yes	Yes	No restrictions. Protocol is not considered part of the evaluation.
DNS	Domain Name Service	Yes	Yes	No	n/a	No restrictions. Protocol is not considered part of the evaluation.
ESP	Encapsulating Security Payload (part of IPsec)	Yes	Yes	Yes	Yes	Configure ESP as described in the section 5.1 of this document.
FTP	File Transfer Protocol	Yes	No	No	n/a	Use tunneling through IPsec
ICMP	Internet Control Message Protocol	Yes	Yes	Yes	Yes	No restrictions. Protocol is not considered part of the evaluation.
IKE	Internet Key Exchange	Yes	Yes	Yes	Yes	As described in section 5.1 of this document.
IPsec	Internet Protocol Security (suite of protocols including IKE, ESP and AH)	Yes	Yes	Yes	Yes	Only to be used for securing traffic that originates from or terminates at the TOE, not for “VPN Gateway” functionality to secure traffic through the TOE. See IKE and ESP for other usage restrictions.
Kerberos	A ticket-based authentication protocol	Yes	Over IPsec	No	n/a	If used for authentication of TOE administrators, tunnel this authentication protocol secure with IPsec.

Service or Protocol	Description	Client (initiating)	Allowed	Server (terminating)	Allowed	Allowed use in the certified configuration
LDAP	Lightweight Directory Access Protocol	Yes	No, use RADIUS	No	n/a	Use RADIUS instead
NTP	Network Time Protocol	Yes	Yes	No	n/a	Any configuration. Use of key-based authentication is recommended
RADIUS	Remote Authentication Dial In User Service	Yes	Yes	No	n/a	If used for authentication of TOE administrators, secure through IPsec.
SNMP	Simple Network Management Protocol	Yes (snmp-trap)	Yes	Yes	No	Outbound (traps) only. Recommended to tunnel through IPsec.
SSH	Secure Shell	Yes	Yes	Yes	Yes	As described in the section 3.3.1 of this document.
Telnet	A protocol used for terminal emulation	Yes	No	Yes	No	Use of SSH is recommended.
TFTP	Trivial File Transfer Protocol	Yes	Yes	No	n/a	Recommend using SCP instead or tunneling through IPsec. Protocol is not considered part of the evaluation.

Note: The table above does not include the types of protocols and services listed here:

- OSI Layer 2 protocols such as CDP, VLAN protocols like 802.11q, Ethernet encapsulation protocols like PPPoE, etc. The certified configuration places no restrictions on the use of these protocols; however evaluation of these protocols was beyond the scope of the Common Criteria product evaluation. Follow best practices for the secure usage of these services.
- Routing protocols such as EIGRP, OSPF, and RIP. The certified configuration places no restrictions on the use of these protocols, however evaluation of these protocols was beyond the scope of the Common Criteria product evaluation, so follow best practices for the secure usage of these protocols.
- Protocol inspection engines, used for filtering traffic, can be enabled with “inspect” commands. These engines are not used for initiating or terminating sessions, so they are not considered network “services” or “processes’ as defined in Table 10 above. The evaluated configuration places no restrictions on the use of the protocol inspection engines; however, evaluation of this functionality was beyond the scope of the CC evaluation. Follow best practices for the secure usage of these services.
- Network protocols that can be proxied through/by the TOE. Proxying of services by the TOE does not result in running said service on the TOE in any way that would allow the TOE itself to be accessible via that service, nor does it allow the TOE to initiate a connection to a remote server independent of the remote client that has initiated the connection. The evaluated configuration places no restrictions on enabling of proxy functionality; however, evaluation of this functionality was beyond the scope of the CC evaluation. Follow best practices for the secure usage of these services.

9 Modes of Operation

An IOS switch has several modes of operation, these modes are as follows:

Booting – while booting, the switches drop all network traffic until the switch image and configuration has loaded. This mode of operation automatically progresses to the Normal mode of operation. During booting, an administrator may press the **break** key on a console connection within the first 60 seconds of startup to enter the ROM Monitor mode of operation. This Booting mode is referred to in the IOS guidance documentation as "ROM Monitor Initialization". Additionally, if the Switch does not find a valid operating system image it will enter ROM Monitor mode and not normal mode therefore protecting the switch from booting into an insecure state.

Normal (EXEC) - The IOS-XE image and configuration is loaded, and the TOE is operating as configured. All levels of administrative access occur in this mode and all TOE security functions are available. In Normal mode there is little interaction between the TOE and the administrator. However, the configuration of the TOE can have a detrimental effect on security; therefore, guidance in this document must be followed. Misconfiguration of the switch could result in the unprotected network having access to the internal/protected network.

ROM Monitor – This mode of operation is a maintenance, debugging, and disaster recovery mode. While the switch is in this mode, no network traffic is routed between the network interfaces. In this state the switch may be configured to upload a new boot image from a specified TFTP server, perform configuration tasks and run various debugging commands. It should be noted that while no administrator password is required to enter ROM monitor mode, physical access to the switch is required; therefore, the switch should be stored in a physically secure location to avoid unauthorized access which may lead to the switch being placed in an insecure state.

9.1 Power-on Self-Tests Run During Bootup and Normal Operation

Following operational error, the TOE reboots (once power supply is available) and enters booting mode. The only exception to this is if there is an error during the Power on Startup Test (POST) during bootup, then the TOE will shut down. If any component reports failure for the POST, the system crashes and appropriate information is displayed on the screen and saved in the crashinfo file. Within the POST, self-tests for the cryptographic operations are performed. The same cryptographic POSTs can also be run on-demand as described in section **Error! Reference source not found.**, and when the tests are run on-demand after system startup has completed (and the syslog daemon has started), error messages will be written to the log.

All ports are blocked from moving to forwarding state during the POST. Only when all components of all modules pass the POST is the system placed in FIPS PASS state and ports are allowed to forward data traffic.

POST tests include:

- AES Known Answer Test –

For the encrypt test, a known key is used to encrypt a known plain text value resulting in an encrypted value. This encrypted value is compared to a known encrypted value to ensure that the encrypt operation is working correctly. The decrypt test is just the opposite. In this test a known key is used to decrypt a known encrypted value. The resulting plaintext value is compared to a known plaintext value to ensure that the decrypt operation is working correctly.

- RSA Signature Known Answer Test (both signature/verification) –

This test takes a known plaintext value and Private/Public key pair and used the public key to encrypt the data. This value is compared to a known encrypted value to verify that encrypt operation is working properly. The encrypted data is then decrypted using the private key. This value is compared to the original plaintext value to ensure the decrypt operation is working properly.

- RNG/DRBG Known Answer Test –

For this test, known seed values are provided to the DRBG implementation. The DRBG uses these values to generate random bits. These random bits are compared to known random bits to ensure that the DRBG is operating correctly.

- HMAC Known Answer Test –

For each of the hash values listed, the HMAC implementation is fed known plaintext data and a known key. These values are used to generate a MAC. This MAC is compared to a known MAC to verify that the HMAC and hash operations are operating correctly.

- SHA-1/256/512 Known Answer Test –

For each of the values listed, the SHA implementation is fed known data and key. These values are used to generate a hash. This hash is compared to a known value to verify they match and the hash operations are operating correctly.

- ECDSA self-test –

This test takes a known plaintext value and Private/Public key pair and used the public key to encrypt the data. This value is compared to a known encrypted value to verify that encrypt operation is working properly. The encrypted data is then decrypted using the private key. This value is compared to the original plaintext value to ensure the decrypt operation is working properly.

- Software Integrity Test –

The Software Integrity Test is run automatically whenever the IOS system images is loaded and confirms that the image file that's about to be loaded has maintained its integrity.

If any of the POST fails, the following actions should be taken:

- If possible, review the crashinfo file. This will provide additional information on the cause of the crash.
- Restart the TOE to perform POST and determine if normal operation can be resumed.
- If the problem persists, contact Cisco Technical Assistance via http://www.cisco.com/techsupport or 1 800 553-2447.
- If necessary, return the TOE to Cisco under guidance of Cisco Technical Assistance.

10 Security Measures for the Operational Environment

Proper operation of the TOE requires functionality from the environment. It is the responsibility of the authorized administrator of the TOE to ensure that the Operational Environment provides the necessary functions, and adheres to the environment security objectives listed below. The environment security objective identifiers map to the environment security objectives as defined in the Security Target.

Table 11 Operational Environment Security Measures

Security Objective for the Operational Environment	Definition of the Security Objective	Responsibility of the Administrators
OE.PHYSICAL	Physical security, commensurate with the value of the TOE and the data it contains, is provided by the environment.	The TOE must be installed in a physically secured location that only allows physical access to authorized personnel.
OE.NO_GENERAL_PURPOSE	There are no general-purpose computing capabilities (e.g., compilers or user applications) available on the TOE, other than those services necessary for the operation, administration and support of the TOE.	None. IOS-XE is a purpose-built operating system that does not allow installation of additional software.
~~OE.NO_THRU_TRAFFIC_PROTECTION~~	~~The TOE does not provide any protection of traffic that traverses it. It is assumed that protection of this traffic will be covered by other security and assurance measures in the operational environment.~~	~~Administrators will ensure protection of any critical network traffic (administration traffic, authentication traffic, audit traffic, etc.) and ensure appropriate operational environment measures and policies are in place for all other types of traffic.~~
OE.TRUSTED_ADMIN	TOE Administrators are trusted to follow and apply all administrator guidance in a trusted manner.	Administrators must read, understand, and follow the guidance in this document to securely install and operate the TOE and maintain secure communications with components of the operational environment.

OE.UPDATES	The TOE firmware and software is updated by an administrator on a regular basis in response to the release of product updates due to known vulnerabilities.	Administrators must download updates, including psirts (bug fixes) to the evaluated image, to ensure that the security functionality of the TOE is maintained
OE.ADMIN_CREDENTIALS_SECURE	The administrator's credentials (private key) used to access the TOE must be protected on any other platform on which they reside.	Administrators must securely store and appropriately restrict access to credentials that are used to access the TOE (i.e., private keys and passwords)
OE.RESIDUAL_INFORMATION	The Security Administrator ensures that there is no unauthorized access possible for sensitive residual information (e.g. cryptographic keys, keying material, PINs, passwords etc.) on networking equipment when the equipment is discarded or removed from its operational environment.	Administrators must securely wipe the TOE of all sensitive information prior to removing from the operational environment.

11 Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation at:

With CCO login: http://www.cisco.com/en/US/partner/docs/general/whatsnew/whatsnew.html

Without CCO login: http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS version 2.0.

You can access the most current Cisco documentation on the World Wide Web at the following sites:

- http://www.cisco.com
- http://www-china.cisco.com
- http://www-europe.cisco.com

11.1 Documentation Feedback

If you are reading Cisco product documentation on the World Wide Web, you can submit technical comments electronically. Click Feedback in the toolbar and select Documentation. After you complete the form, click Submit to send it to Cisco.

You can e-mail your comments to bug-doc@cisco.com.

To submit your comments by mail, for your convenience many documents contain a response card behind the front cover. Otherwise, you can mail your comments to the following address:

Cisco Systems, Inc., Document Resource Connection 170 West
Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

11.2 Obtaining Technical Assistance

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

Cisco.com is the foundation of a suite of interactive, networked services that provides immediate, open access to Cisco information and resources at anytime, from anywhere in the world. This highly integrated Internet application is a powerful, easy-to-use tool for doing business with Cisco.

Cisco.com provides a broad range of features and services to help customers and partners streamline business processes and improve productivity. Through Cisco.com, you can find information about Cisco and our networking solutions, services, and programs. In addition, you can resolve technical issues with online technical support, download and test software packages, and order Cisco learning materials and merchandise. Valuable online skill assessment, training, and certification programs are also available.

Customers and partners can self-register on Cisco.com to obtain additional personalized information and services. Registered users can order products, check on the status of an order, access technical support, and view benefits specific to their relationships with Cisco.

To access Cisco.com, go to the following website:

http://www.cisco.com

12 List of Acronyms

The following acronyms and abbreviations are used in this document:

Table 12 Acronyms

Acronyms/Abbreviations	Definition
AAA	Administration, Authorization, and Accounting
ACL	Access Control List
AES	Advanced Encryption Standard
AGD	Guidance Document
BRI	Basic Rate Interface
CAK	Connectivity Association Key
CAVP	Cryptographic Algorithm Validation Program
CBC	Cipher Block Chaining
CC	Common Criteria for Information Technology Security Evaluation
CDP	CRL Distribution Point
CEM	Common Evaluation Methodology for Information Technology Security
CKN	Secure Connectivity Association Key Name
CLI	Command Line Interface
CM	Configuration Management
CRL	Certificate Revocation List
CSR	Certificate Signing Request
CSU	Channel Service Unit
CTR	Counter
CVL	Component Validation List
DH	Diffie-Hellman
DHCP	Dynamic Host Configuration Protocol
DSU	Data Service Unit
EAP	Extensible Authentication Protocol
ESP	Encapsulating Security Payload
ESS	Embedded Switch Series
GE	Gigabit Ethernet port
HTTPS	Hyper-Text Transport Protocol Secure
IC2M	IOS Common Cryptographic Module
ICK	Integrity Check Key
ICMP	Internet Control Message Protocol

ICV	Integrity Check Value
IEEE	Institute of Electrical and Electronics Engineers
IKE	Internet Key Exchange
IT	Information Technology
IP	Internet Protocol
IPsec	IP Security
ISAKMP	Internet Security Association and Key Management Protocol
ISDN	Integrated Services Digital Network
ISO	International Organization of Standardization
IT	Information Technology
KDF	Key Derivation Function
KEK	Key Encryption Key
KAS	Key Agreement Scheme
KAS-SSC	KAS Shared Secret Computation
KW	Key Wrap
MAC	Media Access Control
MACsec	Media Access Control security
MKA	MACsec Key Agreement Protocol
MKPDU	MACsec Key Agreement Protocol Data Unit
MN	Member Number
MPDU	MAC Protocol Data Unit
NDcPP	collaborative Protection Profile for Network Devices
NIST	National Institute of Standards and Technology
NVRAM	Non-Volatile Random-Access Memory
OCSP	Online Certificate Status Protocol
OS	Operating System
OSI	Open Systems Interconnection
OSP	Organizational Security Policies
PAE	Physical Address Extension
PC	Personal Computer
PKCS	Public Key Cryptographic Standard
PoE	Power over Ethernet
PP	Protection Profile
PRNG	Pseudo Random Number Generator
PSK	Pre-Shared Key

PUB	Publication
RA	Registration Authority
RADIUS	Remote Authentication Dial-In User Service
RFC	Request For Comment
RNG	Random Number Generator
RSA	Rivest, Shamir and Adleman
SA	Security Association
SAK	Security Association Key
SAR	Security Assurance Requirement
SCEP	Simple Certificate Enrollment Protocol
SCI	Secure Channel Identifier
SecTAG	MAC Security TAG
SecY	MAC Security Entity
SFP	Small–form-factor pluggable port
SFR	Security Functional Requirement
SHA	Secure Hash Algorithm
SHS	Secure Hash Standard
SNMP	Simple Network Management Protocol
SPD	Security Policy Definition
SSH	Secure Shell
ST	Security Target
TCP	Transport Control Protocol
TSC	TSF Scope of Control
TSF	TOE Security Function
TSP	TOE Security Policy
VPN	Virtual Private Network
WAN	Wide Area Network
WIC	WAN Interface Card