Cisco Embedded Services 3300 Series and 9300 Series Switches (ESS3300 & ESS9300)

CC Configuration Guide

Version: 0.7
Date: September 29, 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 supporting evidence for an evaluation of a specific Target of Evaluation (TOE), the Cisco Embedded Service 9300 Series (ESS9300) and the Cisco Embedded Services 3300 Series (ESS3300). This Operational User Guidance with Preparative Procedures addresses the administration of the TOE software and hardware and describes how to install, configure, and maintain the TOE in the Common Criteria evaluated configuration. Administrators of the TOE will be referred to as administrators, authorized administrators, TOE administrators, semi-privileged administrators, and privileged administrators in this document.

1 Introduction

This Operational User Guidance with Preparative Procedures documents the administration of the Cisco Embedded Service 9300 Series (ESS9300) and the Cisco Embedded Services 3300 Series (ESS3300), the TOE, as they were certified under Common Criteria. The Cisco Embedded Service 9300 Series and Cisco Embedded Services 3300 Series (ESS3300) may be referenced below as ESS9300 and ESS3300, 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 ESS9300 and ESS3300 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 1. 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 IE3x00 Rugged, IE3400 Heavy Duty, and ESS3300 Series Switches, Cisco IOS XE Cupertino 17.9.x Release Notes for Cisco Catalyst 9300 Series Switches, Cisco IOSXE Bengaluru 17.9.x	https://www.cisco.com/c/en/us/td/docs/switches/lan/cisco_ie3X00/software/17_9/17-9-x-release-notes-iot-switch.html https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9300/software/release/17-9/release_notes/ol-17-9-9300.html
[2]	Cisco Embedded Service 3300 Series Switches Hardware Technical Guide Cisco Catalyst ESS-9300-10X Embedded Switch Hardware Technical Guide	https://www.cisco.com/c/en/us/td/docs/switches/lan/embedded/ess3300/hardware/ESS3300-tech-guide.html https://www.cisco.com/c/en/us/td/docs/switches/lan/embedded/ess9300/hardware/tech-guide/b-cisco-catalyst-ess-9300-10x-embedded-switch-hardware-technical-guide.html

[3]	Configuration Fundamentals Configuration Guide (ESS3300) Configuration Fundamentals Configuration Guide (ESS9300)	https://www.cisco.com/c/en/us/td/docs/switches/lan/embedded/ess3300/software_config/b-cisco-embedded-services-3300-series-configuration.html https://www.cisco.com/c/en/us/td/docs/switches/lan/embedded/ess9300/config/b-cisco-embedded-service-9300-series-switches-configuration-guide.html
[4]	Software Configuration Guide, Cisco IOS XE Cupertino 17.9.x	https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9300/software/release/17-9/configuration_guide/b-179-9300-cg.html
[5]	Security Configuration Guide	https://www.cisco.com/c/en/us/td/docs/switches/lan/cisco_ie3X00/software/17_3/b_security_17-3_iot_switch_cg.html
[6]	Network Management Configuration Guide, Cisco Catalyst IE3x00 Rugged, IE3400 Heavy Duty, and ESS3300 Series Switches	https://www.cisco.com/c/en/us/td/docs/switches/lan/cisco_ie3X00/software/17_3/b_network_mgmt_17-3_iot_switch_cg.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]	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
[10]	Cisco IOS Configuration Fundamentals Command Reference	https://www.cisco.com/c/en/us/td/docs/ios/fundamentals/command/reference/cf_book.html

[11]	Cisco Embedded Service 3300 Series Switches Software Configuration Overview Cisco Embedded Service 9300 Series Switches Configuration Guide Overview	https://www.cisco.com/c/en/us/td/docs/switches/lan/embedded/ess3300/software_config/b_Software_Configuration_Overview/b_Software_Configuration_Overview_chapter_00.html https://www.cisco.com/c/en/us/td/docs/switches/lan/embedded/ess9300/config/b-cisco-embedded-service-9300-series-switches-configuration-guide/m-ESS9300-overview.html
[12]	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
[13]	Secure Shell Configuration Guide	https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_usr_ssh/configuration/xe-17/sec-usr-ssh-xe-17-book/sec-secure-shell-v2.html
[14]	Security Configuration Guide for the ESS3300 Switches, MACsec Encryption	https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/macsec/configuration/xe-17/macsec-xe-17-book.html
[15]	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 https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_data_acl/configuration/xe-17/sec-data-acl-xe-17-book.html
[16]	IPsec Configuration Guide	https://www.cisco.com/c/en/us/td/docs/routers/ios/config/17-x/sec-vpn/b-security-vpn.html
[17]	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

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 ESS9300 and the ESS3300. 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.

Component	Required	Usage/Purpose Description for TOE performance
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.
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.
ESS9300 & ESS3300 Enclosure	Yes	The end user can opt to use an enclosure that accommodates the TOE's size (ESS3300: 3.0 x 3.775 in., ESS9300: 4.3x3.3 in.) and provides no compute capabilities. The TOE functionality is implemented inside the ESS 3300 and 9300 physical chassis, as the chassis includes the underlying board (with or without a cooling plate) and all electronic components attached to it; therefore, no computational capabilities outside of the TOE boundary are required to secure the TOE. During testing, the TOE was enclosed within a Cisco developed hardened enclosure. It is a specially designed enclosure used for Cisco internal testing purposes only. It has no compute capabilities and is not a commercially available product. The enclosure passes network connections directly to the TOE interfaces and does not change or modify TSF functionality. In the evaluated configuration, the enclosures used for testing contain the ESS boards including the integrated multi-pin BTB interface connector with pins dedicated for power input, ethernet ports, and console ports (two combo Gigabit Ethernet WAN ports, four Gigabit Ethernet LAN ports, and one UART RS232 RJ-45 console port). Refer to the ST Section 1.7 for hardware technical guidance on the ESS boards layout and dimensions and Multi-pin BTB Interface Connector description that includes pinout mapping descriptions for network interfaces and power inputs.

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.
USB console access	USB console access was not tested. The RS-232 RJ45 console port was used during testing.
USB Host interface for USB Flash Memory Device	USB Host interface for USB Flash Memory Device was not tested and is not required.

Transport Layer Security (TLS)	TLS is not associated with Security Functional Requirements claimed in [NDcPP]. Use tunnelling through IPsec.

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 4 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 **[2]** fundamental Cisco ESS9300 & ESS3300 and IOS concepts 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 **[1]** 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 ESS9300 & ESS3300 follow the instructions as described in **[3]** Administering the Device.

Start your ESS9330/ESS3300 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

ESS-3300-NCP ESS-3300-CON ESS-3300-24T-NCP ESS-3300-24T-CON	ess3x00-universalk9.17.09.03.SPA.bin	ESS3300: MD5 checksum: f201b4eb064b05e520ea16143194673d SHA512 checksum: d8770ddec91661ab393af1a65511baa8b5b3ba9d02e8997fbf39ec3d96f04d57bdcfff560cd999ad051ba192f5171853f9431150f4b56dc3db188fd7ec4dc9fb
ESS-9300-10X	ie9k_iosxe.17.09.03.SPA.bin	ESS9300: MD5 checksum: 17866b5b99607281d8af3f762a80fba0 SHA512 checksum: 0fe26c3831655f9ec8b9e5c4c1d661688ee34e9f761920e4949635b8d5ccc89cab628be6791c0d458b64f062da9553c0d538e3b5f998557fb8d38524c13c4e51

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 ESS9300 and ESS3300 **[2]** for hardware installation instructions.

3.2 Initial Setup via Direct Console Connection

The ESS9300/ESS3300 must be given basic configuration via console connection prior to being connected to any network.

3.2.1 Options to be chosen during the initial setup of the ESS9300 and ESS3300

The setup starts automatically when a device has no configuration file in NVRAM. When setup completes, it presents the System Configuration Dialog. This dialog guides the administrator through the initial configuration with prompts for basic information about the TOE and network and then creates an initial configuration file. After the file is created, an authorized administrator can use the CLI to perform additional configuration. *Performing Basic System Management* in **[3]** describes how to use Setup to build a basic configuration and to make configuration changes. The following items must be noted during setup:

It should be noted that the account created during the initial installation of the TOE is considered the privileged administrator and has been granted access to all commands on the TOE.

The term "authorized administrator" is used in this document to refer to any administrator that has successfully authenticated to the switch and has access to the appropriate privileges to perform the requested functions.

Refer to the IOS Command Reference Guide for available commands, associated roles and privilege levels as used in the example above **[3] [7]**.

1. **Enter host name** - the hostname is the name given to the device. The hostname should comply with the organization's device naming policies
2. **Enable Secret** – The password must adhere to the password complexity requirements as described in the relevant section below in this document. This command ensures that the enable password is stored encrypted. To configure, use the **enable secret 5** as described in Cisco IOS Security Command Reference **[7]**: Commands D to L -> E -> enable secret. Note that this setting can be confirmed after initial configuration is complete by examining the configuration file and looking for "enable secret 5"**.**
3. **Virtual Terminal Password** - Must adhere to the password complexity requirements. Note that securing the virtual terminal (or vty) lines with a password in the evaluated configuration is suggested, though not a requirement for the evaluated configuration. This password allows access to the device through only the console port. Later in this guide, steps will be given to allow ssh into the vty lines. Reference password (line configuration) in Cisco IOS Security Command Reference **[7]**: Commands M to R -> pac key through port-misuse -> password (line configuration)
4. **Configure SNMP Network Management** – No (this is the default). Note that this setting can be confirmed after configuration is complete by examining the configuration file to ensure that there is no "snmp-server" entry. To ensure there is no snmp server agent running, use the "**no snmp- server**' command as described in Configuring SNMP -> Disabling the SNMP Agent **[3]** Note, in the evaluated configuration, SNMP should remain disabled.

5. **Enter interface name used to connect to the management network from the above interface summary** – a list of current interfaces is displayed. Select the interface to be used to connect to the network. Following the organization's networking policies, provide the following information:
    - Configure IP on this interface: **Yes**
    - IP address for this interface
    - Subnet mask for this interface

3.2.2 Saving Configuration

IOS-XE uses both a running configuration and a starting configuration. Configuration changes affect the running configuration. In order to save that configuration, the running configuration (held in memory) must be copied to the startup configuration. This may be achieved by either using the **write memory** command or the **copy system:running-config nvram:startup-config** command. These commands should be used frequently when making changes to the configuration of the Switch. If the Switch reboots and resumes operation when uncommitted changes have been made, these changes will be lost, and the Switch will revert to the last configuration saved.

3.2.3 Enabling FIPS Mode

The TOE must be run in the FIPS mode of operation. The use of the cryptographic engine in any other mode was not evaluated nor tested during the CC evaluation of the TOE. This is done by setting the following in the configuration:

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

1. In privilege EXEC mode, enter configure terminal

SWITCH# config terminal

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

SWITCH(config)# fips authorization-key <key>

3. Exit configuration mode and return to privileged EXEC mode

SWITCH(config)# end

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

To verify FIPS mode, enter the following command:

SWITCH(config)# show fips status

3.2.4 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 Section 10 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**

3.2.5 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.

3.2.6 Administrator Configuration and Credentials

The ESS9300/ESS3300 must be configured to use a username and password for each administrator and one password for the enable command. Ensure all passwords are stored encrypted by using the following command:

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

Configures local AAA authentication:

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

SWITCH(config)# **aaa authorization exec default local**
When creating administrator accounts, all individual accounts are to be set to a privilege level of one. This is done by using the following commands:

SWITCH(config)# **username <name> password <password>**

to create a new username and password combination, and

SWITCH(config)# **username <name> privilege 1**

to set the privilege level of <name> to 1.

To login to the switch, connect via SSH or local console. Enter the username and password when prompted.

User Access Verification

Username: <enter configured username>

Password: <enter configured password>

3.2.7 Session Termination

Inactivity settings must trigger termination of the administrator session. These settings are configurable by setting:

SWITCH(config)# **line vty <first> <last>**

The first and last are the range of vty lines on the box (i.e. “0 15”).

SWITCH(config-line)# **exec-timeout <time>**

SWITCH(config-line)# **line console**

SWITCH(config)# **exec-timeout <time>**

The time is the period of inactivity after which the session should be terminated. Configuration of these settings is limited to the privileged administrator (see Section 4.1).

To save these configuration settings to the startup configuration:

copy run start

The line console setting is not immediately activated for the current session. The current console session must be exited. When the user logs back in, the inactivity timer will be activated for the new session.

3.2.8 User Lockout

User accounts must be configured to lockout after a specified number of authentication failures:

SWITCH(config)# **aaa local authentication attempts max-fail [*number of failures*]**

The number of failures is the number of consecutive failures that will trigger locking of the account. The minimum value is 1 and maximum value is 65535. Configuration of these settings is limited to the privileged administrator (see Section 4.1).

Related commands:

clear aaa local user fail-attempts [username *username* | all]	Clears the unsuccessful login attempts of the user.
clear aaa local user lockout username [username]	Unlocks the locked-out user.
show aaa local user lockout	Displays a list of all locked-out users.

Note: *this lockout only applies to privilege 14 users and below.*

Note: Administrator lockouts are not applicable to the local console. Local administrators cannot be locked out and have the ability to unlock other users by using the local console.

3.3 Network Protocols and Cryptographic Settings

Telnet for management purposes is enabled by default and must be disabled in the evaluated configuration. To only allow ssh for remote administrator sessions, use the **transport input ssh** command on a specific line vty (as shown below in 3.3.1.1). This command disables telnet by only allowing ssh connections for remote administrator access.

3.3.1 Remote Administration Protocols

3.3.1.1 Steps to configure SSH on switch

1. Configure a hostname:
   SWITCH(config)# **hostname SWITCH**

2. Configure a domain name:
   SWITCH(config)# **ip domain name <e.g. cisco.com>**

3. Generate RSA – choose a longer modulus length for the evaluated configuration (2048 / 3072):
   SWITCH(config)# **crypto key generate rsa**
   How many bits in the modulus [512]: **3072**

RSA keys are generated in pairs—one public key and one private key. This command is not saved in the switch configuration; however, the keys generated by this command are saved in the private configuration in NVRAM (which is never displayed to the user or backed up to another device) the next time the configuration is written to NVRAM.

Note: *Only one set of keys can be configured using the* ***crypto key generate*** *command at a time. Repeating the command overwrites the old keys.*

Note: *If the configuration is not saved to NVRAM with a "****copy running-config startup-config****", the generated keys are lost on the next reload of the switch.*

4. Assign the key pair to SSH

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

5. Enable SSH v2:
   SWITCH(config)# **ip ssh version 2**

6. Configure –SSH timeout:
   SWITCH(config)# **ip ssh time-out 60**

7. Configure SSH retries:
   SWITCH(config)# **ip ssh authentication-retries 3**

8. Ensure that the product is configured to support diffie-hellman-group14-sha1 key exchange using the following command 'ip ssh dh min size 2048':
   SWITCH(config)# **ip ssh dh min size 2048**

9. Configure vty lines to accept 'ssh' login services:
   SWITCH(config)# **line vty <0-19>**
   SWITCH(config-line)# **transport input ssh**

10. To secure and control SSH sessions, the evaluated configuration requires SSHv2 session to only use AES-CBC-128 and AES-CBC-256 encryption key algorithms. To set, use the following command:

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

11. The TOE also needs to be configured to only support HMAC-SHA2-256 and HMAC-SHA2-512 MAC algorithms using the following:

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

12. The TOE needs to be configured to only support Diffie-Hellman Group 14 SHA 1 key exchange algorithms using the following:

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

13. Configure the SSH rekey time-based rekey (in minutes) and volume-based rekey values (in kilobytes) (values can be configured to be lower than the default values if a shorter interval is desired):
    a. **ip ssh rekey time 60**
    b. **ip ssh rekey volume 1000000**

    Note: *When configuring an SSH rekey time or volume interval, the TOE will begin re-key based upon the first threshold reached*

14. To verify the proper encryption algorithms are used for established SSHv2 connections; use the "**show ssh**" command. To disconnect SSH sessions, use the **disconnect ssh** command.

15. To terminate a remote or local session to the switch, use the "**exit**" or "**logout**" command at the User or Privilege EXEC prompt to terminate the session.

    Switch# **exit**
    or
    Switch# **logout**

16. The TOE acting as the SSH server supports three types of user authentication methods and sends these authentication methods to the SSH client in the following predefined order:
    - Keyboard-interactive authentication method (this method is not included nor allowed in the evaluated configuration and must be disabled using the following command **no ip ssh server authenticate user keyboard**
    - Password authentication method
    - Public-key authentication method:

1) Configure Host Key Algorithms for SSH public-key based authentication

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

2) Enter public-key configuration mode

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

3) Specify the admin user account to configure for SSH public key authentication

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

4) Enter public-key data configuration mode

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

5) 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>**

Note: The SSH public key algorithm is ssh-rsa for both rsa-sha2-256 and rsa-sha2-512 hostkeys.

By default, all the user authentication methods are enabled. Use the **no ip ssh server authenticate user {publickey | keyboard | password}** command to disable any specific user authentication method so that the disabled method is not negotiated in the SSH user authentication protocol. This feature helps the SSH server offer any preferred user authentication method in an order different from the predefined order. The disabled user authentication method can be enabled using the **ip ssh server authenticate user {publickey | keyboard | password }** command in **[7]**.

1) HTTP and HTTPS servers were not evaluated and must be disabled:
SWITCH(config)# **no ip http server**
SWITCH(config)# **no ip http secure-server**

2) SNMP server was not evaluated and must be disabled:

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

Recovery from an event where the connection is unintentionally broken is to follow the steps to establish a connection as listed above.

3.3.2 Authentication Server Protocols

RADIUS (outbound) for authentication of TOE administrators to remote authentication servers are disabled by default but should be enabled by administrators in the evaluated configuration.

To configure RADIUS refer to **[5].** Use best practices for the selection and protection of a key to ensure that the key is not easily guessable and is not shared with unauthorized users.

These protocols are to be tunneled over an IPsec connection in the evaluated configuration. The instructions for setting up this communication are the same as those for protecting communications with a syslog server, detailed in Section 3.3.5 below.

3.3.3 Logging Configuration

1. Logging of command execution must be enabled:

- Disable all logging:

SWITCH(config)#**no logging console**

- Enable logging:

SWITCH(config)# **logging on**
SWITCH(config)# **archive**
SWITCH(config-archive)# **log config**
SWITCH(config-archive-log-cfg)# **logging enable**
SWITCH(config-archive-log-cfg)# **logging size <1-1000>**
SWITCH(config-archive-log-cfg)# **notify syslog**

- Suppress keys and password output:

SWITCH(config-archive-log-cfg)#**hidekeys**
SWITCH(config-archive-log-cfg)#**exit**
SWITCH(config-archive)#**exit**

2. Add year to the timestamp:
   SWITCH(config)# **service timestamps log datetime year**
3. Enable any required debugging. Debugging is needed for radius (if used), ipsec, and ikev2 (if using ikev2) to generate the events required in the Security Target, however administrators should use discretion when enabling a large number of debugs on an on-going basis:

   SWITCH# **debug radius authentication**
   SWITCH# **debug crypto isakmp**
   SWITCH# **debug crypto ipsec**
   SWITCH# **debug crypto ikev2**
   SWITCH# **debug crypto pki server**

4. Set the size of the logging buffer. It is recommended to set it to at least 150000000:

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

5. To generate logging messages for failed and successful login attempts in the evaluated configuration, issue the login on-failure and login on-success commands:

SWITCH(config)# **login on-failure log**
SWITCH(config)# **login on-success log**

6. To configure the logs to be sent to a syslog server:

   SWITCH(config)# **logging host<ip address of syslog server>**

   Ex. SWITCH(config)# **logging host 192.168.202.57**

7. To specify the severity level for logging to the syslog host, use the **logging trap** command. Level 7 will send all logs required in the evaluation up to the debug level logs (as enabled in step 3 above) to the syslog server:

   SWITCH(config)# **logging trap 7**

   WARNING: this setting has the ability to generate a large number of events that could affect the performance of your device, network, and syslog host.

8. To configure the syslog history table use the **logging history** command. The severity level are numbered 0 through 7, with 0 being the highest severity level and 7 being the lowest severity level (that is, the lower the number, the more critical the message). Specifying a level causes messages at that severity level and numerically lower levels to be stored in the switch's history table. To change the number of syslog messages stored in the switch's history table, use the logging history size global configuration command. The range of messages that can be stored is 1-500. When the history table is full (that is, it contains the maximum number of message entries specified with the logging history size command), the oldest message entry is deleted from the table to allow the new message entry to be stored.

   SWITCH(config)# **logging history <level>**

   SWITCH(config)# **logging history size <number>**

3.3.4 Usage of Embedded Event Manager

In order to ensure that all commands executed by a level 15 user are captured in a syslog record, the following Cisco Embedded Event Manager script can 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 1.0 info type routername**

SWITCH#(config-applet)# **action 2.0 syslog msg "User:$_cli_username via Port:$_cli_tty Executed[$_cli_msg]"**

SWITCH#(config-applet)# **action 3.0 set _exit_status "1"**

SWITCH#(config)# **end**

For more information on EEM scripting see: https://www.cisco.com/c/en/us/products/ios-nx-os-software/ios-embedded-event-manager-eem/index.html.

3.3.5 Logging Protection

If an authorized administrator wants to backup the logs to a syslog server, then protection must be provided for the syslog server communications as configured in Section 3.3.6 below. This can be provided in one of two ways:

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

When a Syslog server is configured on the TOE, generated audit events are simultaneously sent to the external server and the local logging buffer.

3.3.6 Syslog Server Running on an IPsec Endpoint

For deployments where the syslog server is able to operate as an IPsec peer of the TOE, the IPsec tunnel will protect events as they are sent to the server. Examples of products that can be installed on a syslog server to allow it to be an IPsec peer include the Racoon tool that is part of the IPsec Tools on many Linux systems, strongSwan, Openswan, and FreeS/WAN.

Following are sample instructions to configure the TOE to support an IPsec tunnel with aes encryption, with 10.10.10.101 as the IPsec peer IP on the syslog server, 10.10.10.110 and 30.0.0.1 as the local TOE IPs, and the syslog server running on 40.0.0.1 (a separate interface on the syslog server).

SWITCH# **configure terminal**
SWITCH(config)#**crypto isakmp policy 1**
SWITCH(config-isakmp)#**encryption aes**
SWITCH(config-isakmp)#**authentication pre-share**
SWITCH(config-isakmp)#**group 14**
SWITCH(config-isakmp)#**lifetime 28800**
SWITCH(config-isakmp)#**exit**
SWITCH(config)#**crypto isakmp key [insert 22 character preshared key] address 10.10.10.101**
SWITCH(config)#**crypto isakmp key [insert 22 character preshared key] address 40.0.0.1**
SWITCH(config)#**crypto ipsec transform-set sampleset esp-aes esp-sha-hmac**
SWITCH(cfg-crypto-trans)#**mode tunnel**

SWITCH(config)#**crypto map sample 19 ipsec-isakmp**
SWITCH(config-crypto-map)#**set peer 10.10.10.101**
SWITCH(config-crypto-map)#**set transform-set sampleset**
SWITCH(config-crypto-map)#**set pfs group14**
SWITCH(config-crypto-map)#**match address 170**
SWITCH(config-crypto-map)#**exit**
SWITCH(config)#**interface g0/0**
SWITCH(config-if)#**ip address 10.10.10.110 255.255.255.0**
SWITCH(config-if)#**crypto map sample**
SWITCH(config-if)#**interface Loopback 1**
SWITCH(config-if)#**ip address 30.0.0.1 255.0.0.0**
SWITCH(config-if)#**exit**
SWITCH(config)# **ip route 40.0.0.0 255.0.0.0 10.10.10.101**
SWITCH(config)# **access-list extended 170**
SWITCH (config-ext-nacl)# **permit ip 30.0.0.0 0.255.255.255 40.0.0.0 0.255.255.255**
SWITCH (config-ext-nacl)# **exit**
SWITCH(config)#**logging source-interface Loopback 1**
SWITCH(config)#**logging host 40.0.0.1**

3.3.7 Syslog Server Adjacent to an IPsec Peer

If the syslog server is not directly co-located with the TOE, then the syslog server must be located in a physically protected facility and connected to a switch capable of establishing an IPsec tunnel with the TOE. This will protect the syslog records as they traverse the public network.

Following are sample instructions to configure the TOE to support an IPsec tunnel with aes encryption, with 11.1.1.4 as the IPsec peer, 10.1.1.7 and 11.1.1.6 as the local IPs, and the syslog server on the 12.1.1.0 /28 subnet:

SWITCH#**configure terminal**
SWITCH(config)#**crypto isakmp policy 1**
SWITCH(config-isakmp)#**encryption aes**
SWITCH(config-isakmp)#**authentication pre-share**
SWITCH(config-isakmp)#**group 14**
SWITCH(config-isakmp)#**lifetime 28800**
SWITCH (config- isakmp)# **exit**
SWITCH(config)#**crypto isakmp key [insert 22 character preshared key] address 11.1.1.4**

SWITCH(config)#**crypto isakmp key [insert 22 character preshared key] address 12.1.1.1**
SWITCH(config)#**crypto ipsec transform-set sampleset esp-aes esp-sha-hmac**
SWITCH(cfg-crypto-trans)#**mode tunnel**
SWITCH(config)#**crypto map sample 1 ipsec-isakmp**
SWITCH(config-crypto-map)#**set peer 11.1.1.4**
SWITCH(config-crypto-map)#**set transform-set sampleset**
SWITCH(config-crypto-map)#**match address 115**
SWITCH(config-crypto-map)#**exit**
SWITCH(config)#**interface g0/1**
SWITCH(config-if)#**ip address 10.1.1.7 255.255.255.0**
SWITCH(config-if)#**no ip route-cache**
SWITCH(config-if)#**crypto map sample**
SWITCH(config-if)#**interface g0/0**
SWITCH(config-if)#**ip address 11.1.1.6 255.255.255.0**
SWITCH(config-if)#**crypto map sample**
SWITCH(config-if)#**exit**
SWITCH(config)#**ip route 12.1.1.0 255.255.255.0 11.1.1.4**
SWITCH(config)#**access-list extended 115**
SWITCH (config-ext-nacl)**# permit ip 10.1.1.0 0.0.0.255 12.1.1.0 0.0.0.255 log**
SWITCH (config-ext-nacl)# **exit**
SWITCH(config)#**logging host 12.1.1.1**

Recovery from an event where the connection is unintentionally broken is to follow the steps to establish a connection as listed above.

3.3.8 Routing Protocols

The routing protocols are used to maintain routing tables. The routing tables can also be configured and maintained manually. Refer to the applicable sections in **[9]** *IP Routing Configuration Guide* for configuration of the routing protocols.

3.3.9 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 2023
SWITCH(config-mka-policy)# end
```

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

```
key abcdef0123456789abcdef0123456789abcdef0123456789abcdef0123456789
```

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

```
SWITCH(config) interface GigabitEthernet 1/0/1
SWITCH(config-if)# macsec network-link
SWITCH(config-if)# mka policy my_policy
SWITCH(config-if)# mka pre-shared-key key-chain mykeychain1
SWITCH(config-if) # macsec replay-protection window-size 10
```

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

The detailed steps to configure MKA, configure MACsec and MKA on interfaces are listed in **[14]**.

Note: MACsec using EAP-TLS is outside the scope of the TOE.
Note: During the setup and configuration of the TOE and the MACsec functionality, the Authorized Administrator issues the command – "service password-encryption". This prevents the CAK value from being shown in clear text to the administrators on the CLI when the "show run" output is displayed.

Note: If using AES 128-bit CMAC mode encryption, the key string will be 32-bit hexadecimal in length. If using 256-bit encryption, the key string will be 64-bit hexadecimal in length."

4 Secure Management

4.1 User Roles

The ESS9300 and ESS3300 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 Section 3.2 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.

4.2 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, the following special characters: "!", "@", "#", "$", "%", "^", "&", "*", "(", ")" and the characters found in table 5 below. Configure the switch to enforce that complexity requirement by using enabling "**aaa password restriction**".

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

Table 5 - Additional Password Special Characters

Special Character	Name
	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

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*.

4.3 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**

4.4 Identification and Authentication

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

The ESS9300 and ESS3300 can be configured to use any of the following authentication methods:

4.4.1 Remote authentication (RADIUS)

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**

4.4.2 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.

4.4.3 X.509v3 certificates

Refer to "X.509 Certificates" in Section 5.1.3 below for more details.

4.4.4 Login Banners

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**

The message 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"

5 Virtual Private Networks (VPN)

5.1 IPsec Overview

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

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

IPsec provides secure *tunnels* between two peers, such as two switches. The privileged administrator defines which packets are considered sensitive and should be sent through these secure tunnels and specifies the parameters that should be used to protect these sensitive packets by specifying the characteristics of these tunnels. When the IPsec peer recognizes a sensitive packet, the peer sets up the appropriate secure tunnel and sends the packet through the tunnel to the remote peer.

More accurately, these *tunnels* are sets of security associations (SAs) that are establishedbetween 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 security protocol (AH or ESP).

With IPsec, privileged administrators 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 based on 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--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 as cisco, 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.

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.

5.1.1 IKEv2 Transform Sets

An Internet Key Exchange version 2 (IKEv2) proposal is a set of transforms used in the negotiation of IKEv2 SA as part of the IKE_SA_INIT exchange. 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:**

SWITCH # **conf t**

SWITCH (config)#**crypto ikev2 proposal sample**

SWITCH (config-ikev2-proposal)# **integrity sha1**

This configures IPsec IKEv2 to use SHA-1 cryptographic hashing. SHA 256 and SHA-512 can be configured with the integrity command, **integrity <sha256 | sha512>**.

SWITCH (config-ikev2-proposal)# **encryption aes-cbc-128**

This configures IPsec IKEv2 to use AES-CBC-128 for payload encryption. AES-CBC-256 can be selected with the encryption command, **encryption <aes-cbc-256>**.

Note: *the authorized administrator must ensure that the keysize for this setting is greater than or equal to the keysize selected for ESP in Section 5.1.3 below. If AES 128 is selected here, then the highest keysize that can be selected on the TOE for ESP is AES 128 (either CBC or GCM).*

Note: *Both confidentiality and integrity are configured with the hash and encryption commands respectively. As a result, confidentiality-only mode is disabled.*

SWITCH (config-ikev2-proposal)# **authentication local pre-share**

This configures IPsec to use pre-shared keys. X.509 v3 certificates are also supported for authentication of IPsec peers. See Section 5.1.4 below for additional information.

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

This selects DH Group 14 (2048-bit MODP) for IKE.

SWITCH (config-ikev2-proposal)# **lifetime 86400**

The default time value for Phase 1 SAs is 24 hours (86400 seconds), but this setting can be changed using the command above with different values.

SWITCH (config)#**crypto ikev2 keyring keyring-1**

SWITCH (config-ikev2-keyring)# **peer peer1**

SWITCH (config-ikev2-keyring-peer)# **address 0.0.0.0 0.0.0.0**

SWITCH (config-ikev2-keyring-peer)# **pre-shared-key cisco123!cisco123!CISC**

This section creates a keyring to hold the pre-shared keys referenced in the steps above. In IKEv2 these pre-shared keys are specific to the peer.

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 ")").*

The TOE supports pre-shared keys up to 128 bytes in length. While longer keys increase the difficulty of brute-force attacks, but longer keys increase processing time.

*HEX keys generated off system can also be input for IKEv2 using the following instead of the pre-shared-key command above: '***pre-shared-key hex [hex key]**'.

For example: **pre-shared-key hex 0x6A6B6C**. *See 'pre-shared-key (IKEv2 keyring)' in* ***[17]*** *for more information on this command.*

This configures IPsec to use pre-shared keys. X.509 v3 certificates are also supported for authentication of IPsec peers. See Section 5.1.4 below foradditional information.

SWITCH (config)#**crypto logging ikev2**

This setting enables IKEv2 syslog messages.

Note: *The configuration above is not a complete IKE v2 configuration, and that additional settings will be needed. See* ***[17]*** *Configuring Internet Key Exchange Version 2 (IKEv2) for additional information on IKE v2 configuration.*

5.1.2 IPsec Transforms and Lifetimes

Regardless of the IKE version selected, the TOE must be configured with the proper transform for IPsec ESP encryption and integrity as well as IPsec lifetimes.

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

Example command:

SWITCH(config)# **crypto ipsec transform-set EXAMPLE esp-aes 128 esp- sha-hmac**

Note: The size of the key selected here must be less than or equal to the key size selected for the IKE encryption setting in 5.1.1 and 5.1.2 above. If AES-CBC- 128 was selected there for use with IKE encryption, then only AES-CBC-128 may be selected here.

SWITCH(config-crypto)#**mode tunnel**

This configures tunnel mode for IPsec. Tunnel is the default, but by explicitly specifying tunnel mode, the switch will request tunnel mode and will accept only tunnel mode.

SWITCH(config-crypto)#**mode transport**

This configures transport mode for IPsec.

SWITCH (config)#**crypto ipsec security-association lifetime seconds 28800**

The default time value for Phase 1 SAs is 24 hours. The default time value for Phase 2 SAs is 1 hour. There is no configuration required for these since the defaults are acceptable. However, to change the setting to 8 hours as claimed in the Security Target the crypto ipsec security-association lifetime command can be used as specified above.

SWITCH (config)#**crypto ipsec security-association lifetime kilobytes 100000**

This configures a lifetime of 100 MB of traffic for Phase 2 SAs. The default amount for this setting is 2560KB, which is the minimum configurable value for this command. The maximum configurable value for this command is 4GB.

Additional information regarding configuration of IPsec can be found in the **[16]**. The IPSEC commands are dispersed within the Security Command References.

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

5.1.3 X.509 Certificates

The TOE may be configured by the privileged administrators to use X.509v3 certificates to authenticate IPsec peers. RSA certificates are supported.

Creation of these certificates and loading them on the TOE is covered in **[8]**, and a portion of the TOE configuration for use of these certificates follows below.

5.1.4 Generate a Key Pair

RSA keys are generated in pairs—one public key and one private key:

SWITCH(config)# **crypto key generate rsa modulus 2048/3072**

The keys generated by this command are saved in the private configuration in NVRAM (which is never displayed to the user or backed up to another device) the next time the configuration is written to NVRAM.

Note: Only one set of keys can be configured using the crypto key generate command at a time. Repeating the command overwrites the old keys.

Note: If the configuration is not saved to NVRAM with a "copy run start", the generated keys are lost on the next reload of the switch.

Note: If the error "% Please define a domain-name first" is received, enter the command 'ip domain-name [domain name].

5.1.5 Creation of the Certificate Signing Request

The certificate signing request for the TOE will be created using the RSA key pair and the domain name configured in Section 3.3 above.

In order for a certificate signing request to be generated, the TOE must be configured with a hostname, trustpoint, enrollment method and revocation checking. This is done by using the following commands **[7]**:

- To specify the hostname for the peer in the IKE keyring exchange, use the **hostname** *name* in configuration mode

  Hostname <**name**>
  Where the <**name**> is the name of the peer (**hostname SWITCH**)

- To declare the trustpoint that the TOE should use, use the **crypto pki trustpoint** *name* command in configuration mode

  crypto pki trustpoint <**name**>
  Where the <**name**> creates the name of the trustpoint (**crypto pki trustpoint ciscotest**)

- To specify the enrollment parameters of a certification authority (CA), use the enrollment [terminal or url] command in ca-trustpoint configuration mode

  enrollment url <**url**>
  Where the <**url**> specifies the URL of the file system where the TOE should send certificate requests (**enrollment url http://192.168.2.137:80**)

- To specify the subject name settings in the certificate request, use the subject-name command in ca-trustpoint configuration mode.

  subject-name <**x.500-name**>
  Where the <**x.500-name**> specifies the subject name used in the certificate request. If the <**x.500-name**> argument is not specified, the fully qualified domain name (FQDN), which is the default subject name, will be used (**subject-name CN=catTOE.cisco.com,OU=TAC**)

- All of the certificates include at least the following information:

  public key and (Common Name, Organization, Organizational Unit, Country) <**subject-name**> **CN=catTOE.cisco.com,O=cisco,OU=TAC,C=U**

- To specify the revocation check method, use the revocation-check command in ca-trustpool configuration mode.

(ca-trustpoint)**#revocation-check crl**

This will set up the certificate revocation mechanism to CRL, which is to be used to ensure that the certificate of a peer has not been revoked. If the TOE is unable to obtain a CRL or if the OCSP server returns an error, the TOE will reject the peer's certificate. The signing CA is required to have the cRLSign Key Usage or the TOE will consider the CRL invalid and reject the peer certificate.

- To create the certificate signing request, use the crypto pki enroll command in global configuration mode.

crypto pki enroll <name>

Where **<name>** is the CA that was set above using the **crypto pki trustpoint** command (**crypto pki enroll ciscotest**)

5.1.6 Securely Connecting to a Certificate Authority for Certificate Signing

The TOE must communicate with the CA for Certificate Signing over IPSEC. This authentication will use pre-shared keys.

Following are sample instructions to configure the TOE to support an IPsec tunnel with aes encryption, with 10.10.10.102 as the IPsec peer IP on the CA, 10.10.10.110 as the local TOE IP.

SWITCH# **configure terminal**
SWITCH(config)# **crypto isakmp policy 1**
SWITCH(config-isakmp)# **encryption aes**
SWITCH(config-isakmp)# **authentication pre-share**
SWITCH(config-isakmp)# **group 14**
SWITCH(config-isakmp)# **lifetime 86400**
SWITCH(config)# **crypto isakmp key [insert 22 character preshared key] address 10.10.10.101**
SWITCH(config)# **crypto ipsec transform-set sampleset esp-aes esp-sha- hmac**
SWITCH(cfg-crypto-trans)# **mode tunnel**
SWITCH(config)# **crypto map sample 19 ipsec-isakmp**
SWITCH(config-crypto-map)# **set peer 10.10.10.102**
SWITCH(config-crypto-map)# **set transform-set sampleset**

SWITCH(config-crypto-map)# **set pfs group14**

SWITCH(config-crypto-map)# **match address 170** SWITCH(config-crypto-map)# **exit**
SWITCH(config)# **interface g0/0**
SWITCH(config-if)# **ip address 10.10.10.110 255.255.255.0**

SWITCH(config-if)# **crypto map sample**
SWITCH(config-if)# **exit**
SWITCH(config)# **access-list 170 permit ip 10.10.10.0 0.255.255.255 10.10.10.0 0.255.255.255**

5.1.7 Authenticating the Certificate Authority

The TOE must authenticate the CA by acknowledging its attributes match the publicly posted fingerprint. The TOE administrator must verify that the output of the command below matches the fingerprint of the CA on its public site.

1. Authenticate the CA: **crypto ca authenticate *trustpoint-name***
   Device (config)#**crypto ca authenticate ciscotest**
   Certificate has the following attributes:
   Fingerprint MD5: 8DE88FE5 78FF27DF 97BA7CCA 57DC1217
   Fingerprint SHA1: 271E80EC 30304CC1 624EEE32 99F43AF8 DB9D0280

   % Do you accept this certificate? [yes/no]: **yes**
   Trustpoint CA certificate accepted.

5.1.8 Storing Certificates to a Local Storage Location

Certificates are stored to NVRAM by default; however, some switches do not have the required amount of NVRAM to successfully store certificates. All Cisco platforms support NVRAM and flash local storage. Depending on the platform, an authorized administrator may have other supported local storage options including bootflash, slot, disk, USB flash, or USB token. During run time, an authorized administrator can specify what active local storage device will be used to store certificates. For more detailed information see **[8]**.

How to Specify a Local Storage Location for Certificates -

The summary steps for storing certificates locally to the TOE are as follows:

1. Enter configure terminal mode:
2. SWITCH# **configure terminal**
3. Specify the local storage location for certificates: **crypto pki certificate storage <location-name>**
   SWITCH# (config)# **crypto pki certificate storage flash:/certs**
4. Exit:
   SWITCH# (config)# **exit**
5. Save the changes made to the device
   SWITCH# **copy system:running-config nvram:startup-config**
6. Display the current setting for the PKI certificate storage location:

SWITCH# show crypto pki certificates storage

The following is sample output from the show crypto pki certificates storage command, which shows that the certificates are stored in the certs subdirectory of

disk0:

```
Device# show crypto pki certificates storage Certificates will be stored in
                                    disk0:/certs/
```

5.1.9 Configuring a Revocation Mechanism for PKI Certificate Status Checking

Perform this task to set up the CRL certificate revocation mechanism that is used to check the status of certificates in a PKI.

Use the **revocation-check** command to specify at least one method (CRL or skip the revocation check) that is to be used to ensure that the certificate of a peer has not been revoked.

(ca-trustpoint)#**revocation-check crl**

If the signing CA does not have the cRLSign Key Usage, the TOE will consider the CRL as invalid and the TOE will reject the peer's certificate.

5.1.10 Configuring Certificate Chain Validation

Perform this task to configure the processing level for the certificate chain path of peer certificates. Prerequisites:

- The device must be enrolled in your PKI hierarchy.
- The appropriate key pair must be associated with the certificate.

1. Enter configure terminal mode:
   SWITCH# **configure terminal**
2. Set the crypto pki trustpoint name:
   SWITCH(config)# **crypto pki trustpoint ca-sub1**
3. Configure the level to which a certificate chain is processed on all certificates including subordinate CA certificates using **the chain-validation [{stop | continue} [parent- trustpoint]] command**:
   SWITCH(ca-trustpoint)# **chain-validation continue ca-sub1**
   - Use the stop keyword to specify that the certificate is already trusted. This is the default setting.
   - Use the continue keyword to specify that the subordinate CA certificate associated with the trustpoint must be validated.
   - The parent-trustpoint argument specifies the name of the parent trustpoint the certificate must be validated against.

   ***Note**: A trustpoint associated with the root CA cannot be configured to be validated to the next level. The **chain-validation** command is configured with the continue keyword for the trust point associated with the root CA, an error message will be displayed and the chain validation will revert to the default **chain-validation** command setting.*

4. Exit:

SWITCH(ca-trustpoint)# **exit**

5.1.11 Setting X.509 for use with IKE

Once X.509v3 keys are installed on the TOE, they can be set for use with IKEv2 with the commands:

SWITCH (config)#**crypto ikev2 proposal sample**

SWITCH(config-ikev2-profile)#**authentication [remote | local] rsa-sig**

If an invalid certificate is loaded, authentication will not succeed.

5.1.12 Deleting Certificates

If the need arises, certificates that are saved on the switch can be deleted. The switch saves its own certificates and the certificate of the CA.

To delete the switch's certificate from the switch's configuration, the following commands can be used in global configuration mode:

Switch# **show crypto ca certificates** [*Displays the certificates stored on switch*] Switch(config)# **crypto ca certificate chain** *name* [*Enters certificate chain configuration mode*

Switch(config-cert-cha)# **no certificate** *certificate-serial-number* [*deletes the certificate*]

To delete the CA's certificate, the entire CA identity must be removed, which also removes all certificates associated with the CA—switch's certificate and the CA certificate. To remove a CA identity, the following command in global configuration mode can be used:

Switch(config)# **no crypto ca identity** *name* [*Deletes all identity information and certificates associated with the CA*]

5.1.13 Information Flow Policies

The TOE may be configured by the privileged administrators for information flow control/ firewall rules as well as VPN capabilities using the access control functionality. Configuration of information flow policies is restricted to the privileged administrator.

On the TOE, an authorized administrator can define the traffic rules on the box by configuring access lists (with permit, deny, and/or log actions) and applying these access lists to interfaces using access and crypto map sets:

- The 'discard' option is accomplished using access lists with deny entries, which are applied to interfaces within access-groups.
- The 'bypassing' option is accomplished using access lists, which are applied to interfaces within crypto maps for IPsec and the 'filter tunnel' command for SSL VPN.
- The 'protecting' option is accomplished using access lists with permit entries, which are applied to interfaces within crypto maps for IPsec and the 'filter tunnel' command for SSL VPN.

The criteria used in matching traffic in all of these access lists includes the source and destination address, and optionally the Layer 4 protocol and port.

The TOE enforces information flow policies on network packets that are receive by TOE interfaces and leave the TOE through other TOE interfaces. When network packets are received on a TOE interface, the TOE verifies whether the network traffic is allowed or not and performs one of the following actions, pass/not pass information, as well as optional logging.

Create an ACL:
Switch(config)# access-list 100 < deny | permit> ip <source address> <source wildcard bits> <destination address> <destination wildcard bits>

Create crypto map:
Switch(config)# crypto map <MAP_NAME> isakmp-profile
Switch(config-crypto-map)# set peer 10.0.0.1
Switch(config-crypto-map)# set transform-set SAMPLE_SET
Switch(config-crypto-map)# match address 100

Apply the crypto map to an interface:
Switch(config)# interface GigabitEthernet0/0
Switch(config-if)# crypto map <MAP_NAME>

Please refer to the "Cisco IOS Security Command Reference: Commands A to C" for additional information on configuring crypto maps, https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/security/a1/sec-a1-cr-book.html.

5.1.14 IPsec Session Interruption/Recovery

If an IPsec session with a peer is unexpectedly interrupted, the connection will be broken. In these cases, no administrative interaction is required. The IPsec session will be reestablished (a new SA set up) once the peer is back online.

5.2 Product Updates

Verification of authenticity of updated software is done in the same manner as ensuring that the TOE is running a valid image. See Section 2.5, steps 7 and 9 above for the method to download and verify an image prior to running it on the TOE.

5.3 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 SAN: FQDN, SAN: 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.

1. Start certificate-map mode

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

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

   For example:

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

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

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

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

4. Associate the certificate map to the IPsec trustpoint created in section 5.1.10

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

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

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

6 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 5 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 6 General Auditable Events

Requirement	Auditable Events	Additional Audit Record Contents	Sample Record
FCS_MACSEC_EXT.1	Session establishment	Secure Channel Identifier (SCI)	**Session Establishment** <45>6840: ESS3300: Jun 1 2023 21:10:54: %MKA-5-SESSION_SECURED: (Gi1/0/1 : 9) MKA Session was secured for RxSCI 0015.5d90.160e/0001, AuditSessionID , CKN 1000
FCS_MACSEC_EXT.4.4	Creation of Connectivity Association	Connectivity Association Key Names	**Creation of Connectivity Association** <189>3235: Jun 2 2023 12:43:05: %MKA-5-SESSION_SECURED: (Gi1/0/1 : 9) MKA Session was secured for RxSCI 5cb1.2e12.ca01/0008, AuditSessionID , CKN 1000
FCS_MACSEC_EXT.3.1	Creation and update of Secure Association Key	Creation and update times	**For SAK (Security Association Key) creation-**

Requirement	Auditable Events	Additional Audit Record Contents	Sample Record
			<47>6861: ESS3300: Jun 1 2023 21:11:09: MKA-EVENT 0015.5d90.160e/0001 1200000D: Generation of new Latest SAK suc-ceeded (Latest AN=1, KN=2)… **For SAK (Security Association Key) update –** <190>4155: Jun 26 2023 20:47:05: %MKA-6-SAK_REKEY_SUCCESS: (Gi1/0/1 : 9) MKA Session successfully completed a SAK Rekey (new Latest AN/KN 0/9, Old AN/KN 3/8) for RxSCI 0015.5d90.160e/0001, AuditSessionID , CKN 1000
FCS_IPSEC_EXT.1	Failure to establish an IPsec SA.	Reason for failure.	**Failed to find matching policy (General)** <47>12048: ESS3300: *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: ESS3300: *Nov 16 2022 14:43:24: %IKEV2-3-NEG_ABORT: Negotiation aborted due to ERROR: Failed to find a matching policy **Invalid transform proposal received (bad ESP cipher)** <47>5309: ESS3300: *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: ESS3300: *Nov 16 2022 13:27:45: IPSEC(ipsec_process_proposal): invalid transform proposal received: <47>5493: ESS3300: {esp-gcm } <47>5496: ESS3300: *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: ESS3300: *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: ESS3300: *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: ESS3300: *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: ESS3300: *Nov 16 2022 13:53:20: IKEv2:(SESSION ID = 14,SA ID = 1):Sending no proposal chosen notify

Requirement	Auditable Events	Additional Audit Record Contents	Sample Record
			Failed to validate certificate (Bad Reference Identifier) <47>11334: ESS3300: 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: ESS3300: Feb 22 2023 16:12:18: CRYPTO_PKI: Checking cert map authorization <43>11732: ESS3300: 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: ESS3300: Apr 13 2023 03:28:47: %SSH-3-NO_MATCH: No matching cipher found: client aes128-ctr server aes256-cbc,aes128-cbc <45>3592: ESS3300: 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: ESS3300: Apr 13 2023 03:28:47: %SSH-5-SSH2_CLOSE: SSH2 Session from 172.16.16.254 (tty = 0) for user '' using crypto cipher '', hmac '' closed **No matching host key type** <43>3595: ESS3300: 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: ESS3300: 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: ESS3300: 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: ESS3300: 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: ESS3300: 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: ESS3300: 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**

Requirement	Auditable Events	Additional Audit Record Contents	Sample Record
			<43>3601: ESS3300: 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: ESS3300: 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: ESS3300: 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: ESS3300: Apr 13 2023 03:14:56: %SSH-3-BAD_PACK_LEN: Bad packet length 33068 <46>3578: ESS3300: 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. Administrator lockout due to excessive authentication failures	Origin of the attempt (e.g., IP address).	<45>58605: ESS3300: Mar 28 2023 06:11:09: %AAA-5-LOCAL_USER_BLOCKED: User TestUser17674 blocked for login till 01:14:09 EST Mar 28 2023 <44>58606: ESS3300: 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).	**SSH Authentication Success – Password** <45>3552: ESS3300: 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: ESS3300: 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

Requirement	Auditable Events	Additional Audit Record Contents	Sample Record
			SSH Authentication Failure – Password <44>3566: ESS3300: 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: ESS3300: Apr 13 2023 02:59:27: %SSH-5-SSH2_USERAUTH: User '' authentication for SSH2 Session from 172.16.16.254 (tty = 0) using crypto cipher 'aes128-cbc', hmac 'hmac-sha2-256' Failed **SSH Authentication Success – Public Key** <45>69666: ESS3300: 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: ESS3300: Apr 7 2023 03:40:31: %SSH-5-SSH2_USERAUTH: User 'testadmin' authentication for SSH2 Session from 172.16.16.254 (tty = 0) using crypto cipher 'aes256-cbc', hmac 'hmac-sha2-256' Succeeded **SSH Authentication Failure – Public Key** <44>69676: ESS3300: Apr 7 2023 03:45:59: %SEC_LOGIN-4-LOGIN_FAILED: Login failed [user: testadmin] [Source: 172.16.16.254] [localport: 22] [Reason: Login Authentication Failed] at 22:45:59 EST Thu Apr 6 2023 <45>69677: ESS3300: Apr 7 2023 03:47:11: %SSH-5-SSH2_USERAUTH: User '' authentication for SSH2 Session from 172.16.16.254 (tty = 0) using crypto cipher 'aes256-cbc', hmac 'hmac-sha2-256' Failed **Console Authentication Success** <45>69547: ESS3300: Apr 7 2023 03:24:54: %SEC_LOGIN-5-LOGIN_SUCCESS: Login Success [user: admin] [Source: LOCAL] [localport: 0] at 22:24:54 EST Thu Apr 6 2023 **Console Authentication Failure** <44>2814: ESS3300: Apr 12 2023 05:25:52: %SEC_LOGIN-4-LOGIN_FAILED: Login failed [user: admin] [Source: LOCAL] [localport: 0] [Reason: Login Authentication Failed] at 00:25:52 EST Wed Apr 12 2023.
FIA_X509_EXT.1	Unsuccessful	Reason for	**Expired Server Cert**

Requirement	Auditable Events	Additional Audit Record Contents	Sample Record
	attempt to validate a certificate Any addition, replacement or removal of trust anchors in the TOE's trust store	failure Identification of certificates added, replaced or removed as trust anchor in the TOE's trust store	<47>4151: ESS3300: 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: ESS3300: Feb 2 2023 08:35:30: IKEv2-ERROR:Current time is more than cert validity time **Expired SubCA Cert** <47>4263: ESS3300: 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: ESS3300: 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: ESS3300: 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: ESS3300: Feb 2 2023 18:42:27: IKEv2:(SESSION ID = 18,SA ID = 1):Verify cert failed <47>10036: ESS3300: Feb 2 2023 18:42:27: IKEv2:(SA ID = 1):[PKI -> IKEv2] Validation of certificate chain FAILED **Revoked Certificate** <47>5136: ESS3300: 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: ESS3300: 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: ESS3300: 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: ESS3300: 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: ESS3300: Feb 2 2023 08:45:41: 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>8657: ESS3300: Feb 2 2023 08:45:41: ../cert-c/source/vericert.c(145) : E_INVALID_SIGNATURE : error verifying digitial signature **Corrupt Public Key** <47>8720: ESS3300: 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: ESS3300: Feb 2 2023 09:03:26: ../cert-c/source/vericert.c(145) : E_INVALID_SIGNATURE : error verifying digitial signature **CRL Incorrectly Signed** <47>6582: ESS3300: Feb 2 2023 08:41:05: IKEv2:Received Packet [From 192.168.144.254:500/To 192.168.144.50:500/VRF i0:f0] <47>6991: ESS3300: Feb 2 2023 08:41:05: Key-usage mismatch. Cert does not have cRLSign bit set. <47>6992: ESS3300: Feb 2 2023 08:41:05: CRYPTO_PKI: CRL verify has failed **Invalid Certificate Chain** <47>9314: ESS3300: Feb 2 2023 17:38:45: IKEv2:Received Packet [From 192.168.144.254:500/To 192.168.144.50:500/VRF i0:f0] <47>9461: ESS3300: Feb 2 2023 17:38:45: IKEv2:(SA ID = 1):[PKI -> IKEv2] Validation of certificate chain FAILED **Unreachable Revocation Server** <47>10926: ESS3300: 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: ESS3300: 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.	Jul 10 11:04:09.179: %PARSER-5-CFGLOG_LOGGEDCMD: User:cisco logged command:upgrade

Requirement	Auditable Events	Additional Audit Record Contents	Sample Record
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 6 “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 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 6 “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.	<191>6844: Jun 2 2023 19:36:09: MKA-ERR 0015.5d90.160e/0001 B200000D: MKPDU Validation FAIL - Live Peer MN 5 is NOT greater than last received MN 6 and so could be an old/replayed MKPDU.

Requirement	Auditable Events	Additional Audit Record Contents	Sample Record
FPT_TUD_EXT.1	Initiation of update. result of the update attempt (success or failure)	None.	**Success:** <46>2883: ESS3300: 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: ESS3300: May 19 2023 03:18:34: %INSTALL-5-INSTALL_START_INFO: Switch 1 R0/0: install_mgr: Started install add_activate_commit flash: ess3x00-universalk9.17.09.03.SPA.bin <45>2888: ESS3300: May 19 2023 03:21:36: %INSTALL-5-INSTALL_COMPLETED_INFO: Switch 1 R0/0: install_mgr: Completed install add_activate_commit **Failure:** <46>2910: ESS3300: 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: ESS3300: 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: ESS3300: 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.** 001383: May 10 18:06:34.091: %SYS-6-EXEC_EXPIRE_TIMER: (tty 0 (0.0.0.0)) exec-timeout timer expired for user securityperson 001384: May 10 18:06:34.091: %SYS-6-EXIT_CONFIG: User securityperson has exited tty session 0(0.0.0.0)
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: ESS3300: Apr 25 2023 04:25:24: %HA_EM-6-LOG: cli_log: User:admin via Port:1 Executed[exit] <46>2920: ESS3300: Apr 25 2023 04:25:24: %SYS-6-LOGOUT: User admin has exited tty session 1(172.16.16.254)

Requirement	Auditable Events	Additional Audit Record Contents	Sample Record
			<45>2921: ESS3300: 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: ESS3300: Nov 2 2022 03:04:58: %HA_EM-6-LOG: cli_log: User:admin via Port:0 Executed[exit] <46>10917: ESS3300: 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. Failure of the trusted channel functions.	Identification of the initiator and target of failed trusted channels establishment attempt.	**IPsec** <45>3074: ESS3300: *Nov 16 2022 12:10:28: %IKEV2-5-SA_UP: SA UP <45>3075: ESS3300: *Nov 16 2022 12:10:28: %CRYPTO-5-IKEV2_SESSION_STATUS: Crypto tunnel v2 is UP. Peer 192.168.144.254:4500 Id: 192.168.144.254 <47>3160: ESS3300: *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: ESS3300: *Nov 16 2022 12:10:33: IKEv2:(SESSION ID = 1,SA ID = 1):Deleting SA <45>3186: ESS3300: *Nov 16 2022 12:10:33: %IKEV2-5-SA_DOWN: SA DOWN <45>3187: ESS3300: *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

Requirement	Auditable Events	Additional Audit Record Contents	Sample Record
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 7 Auditable Administrative Events

Requirement	Management Action to Log	Sample Log
FAU_GEN.1: Audit data generation	Changing logging settings. Clearing logs.	Feb 17 2013 16:29:07: %PARSER-5-CFGLOG_LOGGEDCMD: User:test_admin logged command:logging enable Feb 17 2013 16:34:02: %PARSER-5-CFGLOG_LOGGEDCMD: User:test_admin logged command:logging informational Feb 17 2013 17:05:16: %PARSER-5-CFGLOG_LOGGEDCMD: User:test_admin logged command:clear logging
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 *****

Requirement	Management Action to Log	Sample Log
		Jan 24 2013 03:10:08.878: %GDOI-5-KS_REKEY_TRANS_2_UNI: Group getvpn transitioned to Unicast Rekey.ip
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
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**

Requirement	Management Action to Log	Sample Log
		<189>3090: Jun 26 2023 20:03:02: %PARSER-5-CFGLOG_LOGGEDCMD: User:admin logged command:key-string * **Manage the Key Server to create, delete, and activate MKA participants [as specified in 802.1X, sections 9.13 and 9.16 (cf. MIB object ieee8021XKayMkaParticipantEntry) and section. 12.2 (cf. function createMKA())];** Create/Activate: <191>3158: Jun 26 2023 20:03:13: MKA-EVENT: Created New CA 0x80007F603BC25BA8 Participant on interface GigabitEthernet1/0/3 with SCI A0F8.4915.CD83/000B for Peer MAC a0f8.4915.cd83. Delete: <191>4266: Jun 26 2023 20:48:28: MKA-EVENT: Deleting MKA Session on interface GigabitEthernet1/0/3 & Bring-Down-Dot1x is TRUE. **Specify a lifetime of a CAK** <189>5564: Jun 5 2023 17:04:17: %PARSER-5-CFGLOG_LOGGEDCMD: User:admin logged command:lifetime local 13:04:16 Jun 05 2023 duration 600 **Enable, disable, or delete a PSK based CAK using [CLI management commands]** Enable: <189>3090: Jun 26 2023 20:03:02: %PARSER-5-CFGLOG_LOGGEDCMD: User:admin logged command:key-string * Disable/Delete: <189>10019: Jun 29 2023 21:50:45: %PARSER-5-CFGLOG_LOGGEDCMD: User:admin logged command:no key-string

Requirement	Management Action to Log	Sample Log
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.	Feb 15 2013 13:12:25.055: %PARSER-5-CFGLOG_LOGGEDCMD: User:cisco logged command: crypto isakmp key *****
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

Requirement	Management Action to Log	Sample Log
FIA_X509_EXT.1/Rev: X.509 Certificates	Generating a certificate.	Feb 17 2013 16:14:47: %PARSER-5-CFGLOG_LOGGEDCMD: User:test_admin logged command: crypto key generate
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
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.

Requirement	Management Action to Log	Sample Log
FPT_TUD_EXT.1: Trusted update	Software updates	Jul 10 2013 11:04:09.179: %PARSER-5-CFGLOG_LOGGEDCMD: User:cisco logged command:upgrade
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.	Feb 15 2013 13:12:25.055: %PARSER-5-CFGLOG_LOGGEDCMD: User:cisco logged command: exit
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

6.1 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**

7 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 8 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.
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 instead
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 7 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.

8 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.

When a reload is needed, if NVRAM is empty, IOS-XE will try to boot automatically from an image that is in the flash directory, Images are loaded from top to bottom, so ensure a valid image is listed above all other images in flash by executing the following CLI command [3]:

#boot system flash: <image filename>

To return to Normal (EXEC) mode from ROM Monitor mode, use the following command:

continue

While no administrator password is required to enter ROM Monitor mode, physical access to the TOE is required; therefore, the TOE should be stored in a physically secure location to avoid unauthorized access which may lead to the TOE being placed in an insecure state.

8.1 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 3.2.4, 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.

- 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.

9 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 9 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.

10 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

10.1 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.

10.2 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

11 List of Acronyms

The following acronyms and abbreviations are used in this document:

Table 10 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