



# Cisco Catalyst 9400X/9600X Series Switches 17.12

## Security Target

**Version:** 0.6

**Date:** September 17, 2024

## Table of Contents

Document Introduction.....	6
1. Security Target Introduction.....	8
1.1. ST and TOE Reference.....	8
1.2. TOE Overview.....	8
1.3. TOE Product Type .....	9
1.4. Required non-TOE Hardware/Software/Firmware.....	9
1.5. TOE Description .....	9
1.6. TOE Evaluated Configuration.....	10
1.7. Physical Scope of the TOE .....	11
1.8. Logical Scope of the TOE.....	13
Security Audit .....	14
Cryptographic Support.....	14
Identification and Authentication.....	14
Security Management.....	14
Protection of the TSF .....	15
TOE Access .....	15
Trusted Path/Channels.....	15
1.9. Excluded Functionality.....	16
2. Conformance Claims.....	16
2.1. Common Criteria Conformance Claim .....	16
2.2. PP Configuration Conformance Claim.....	16
2.3. Protection Profile Conformance Claim Rationale .....	19
2.3.1. TOE Appropriateness.....	19
2.3.2. TOE Security Problem Definition Consistency .....	19
2.3.3. Statement of Security Requirements Consistency.....	19
3. Security Problem Definition .....	20
3.1. Assumptions.....	20
3.2. Threats.....	21
3.3. Organizational Security Policies.....	23
4. Security Objectives .....	25
4.1. Security Objectives for the TOE .....	25
4.2. Security Objectives for the Environment .....	26
5. Security Requirements.....	27
5.1. Conventions .....	27
5.2. Class: Security Audit (FAU) .....	30

5.2.1.	FAU_GEN.1 – Audit Data Generation .....	30
5.2.2.	FAU_GEN.1/MACSEC – Audit Data Generation (MACsec) .....	32
5.2.3.	FAU_GEN.2 – User Identity Association.....	33
5.2.4.	FAU_STG_EXT.1 – Protected Audit Event Storage.....	33
5.3.	Class: Cryptographic Support (FCS) .....	33
5.3.1.	FCS_CKM.1 – Cryptographic Key Generation (Refinement) .....	33
5.3.2.	FCS_CKM.2 – Cryptographic Key Establishment (Refinement).....	33
5.3.3.	FCS_CKM.4 – Cryptographic Key Destruction .....	34
5.3.4.	FCS_COP.1/DataEncryption – Cryptographic Operation (AES Data Encryption/Decryption) .....	34
5.3.5.	FCS_COP.1/MACSEC – Cryptographic Operation (MACsec AES Data Encryption/Decryption).....	34
5.3.6.	FCS_COP.1/SigGen – Cryptographic Operation (Signature Generation and Verification) .....	34
5.3.7.	FCS_COP.1/Hash – Cryptographic Operation (Hash Algorithm) .....	35
5.3.8.	FCS_COP.1/KeyedHash – Cryptographic Operation (Keyed Hash Algorithm) .....	35
5.3.9.	FCS_COP.1/CMAC – Cryptographic Operation (AES-CMAC Keyed Hash Algorithm).....	35
5.3.10.	FCS_RBG_EXT.1 – Random Bit Generation.....	35
5.3.11.	FCS_MACSEC_EXT.1 – MACsec.....	35
5.3.12.	FCS_MACSEC_EXT.2 – MACsec Integrity and Confidentiality .....	35
5.3.13.	FCS_MACSEC_EXT.3 – MACsec Randomness .....	36
5.3.14.	FCS_MACSEC_EXT.4 – MACsec Key Usage .....	36
5.3.15.	FCS_MKA_EXT.1 – MACsec Key Agreement.....	36
5.3.16.	FCS_SSHS_EXT.1 – SSH Server Protocol .....	37
5.3.17.	FCS_TLSC_EXT.1 TLS Client Protocol Without Mutual Authentication .....	37
5.4.	Class: Identification and Authentication (FIA) .....	38
5.4.1.	FIA_AFL.1 – Authentication Failure Management.....	38
5.4.2.	FIA_PMG_EXT.1 – Password Management.....	38
5.4.3.	FIA_PSK_EXT.1 – Pre-Shared Key Composition .....	39
5.4.4.	FIA_UIA_EXT.1 – User Identification and Authentication .....	39
5.4.5.	FIA_UAU_EXT.2 – Password-based Authentication Mechanism .....	39
5.4.6.	FIA_UAU.7 – Protected Authentication Feedback.....	39
5.4.7.	FIA_X509_EXT.1/Rev – X.509 Certificate Validation .....	39
5.4.8.	FIA_X509_EXT.2 – X.509 Certificate Authentication.....	40
5.5.	Class: Security Management (FMT) .....	40
5.5.1.	FMT_MOF.1/ManualUpdate – Management of Security Functions Behavior .....	40
5.5.2.	FMT_MTD.1/CoreData – Management of TSF Data .....	40
5.5.3.	FMT_MTD.1/CryptoKeys – Management of TSF Data .....	40
5.5.4.	FMT_SMF.1 – Specification of Management Functions.....	40

- 5.5.5. FMT\_SMF.1/MACSEC – Specification of Management Functions (MACsec) .....41
- 5.5.6. FMT\_SMR.2 – Restrictions on Security Roles .....41
- 5.6. Class: Protection of the TSF (FPT) .....41
  - 5.6.1. FPT\_CAK\_EXT.1 Protection of CAK Data .....41
  - 5.6.2. FPT\_FLS.1 Failure with Preservation of Secure State.....42
  - 5.6.3. FPT\_RPL.1 Replay Detection .....42
  - 5.6.4. FPT\_RPL\_EXT.1 Replay Protection for XPN .....42
  - 5.6.5. FPT\_APW\_EXT.1 – Protection of Administrator Passwords .....42
  - 5.6.6. FPT\_SKP\_EXT.1 – Protection of TSF Data (for reading of all pre-shared, symmetric and private keys) .....42
  - 5.6.7. FPT\_STM\_EXT.1 – Reliable Time Stamps .....42
  - 5.6.8. FPT\_TST\_EXT.1 – TSF Testing .....42
  - 5.6.9. FPT\_TUD\_EXT.1 – Trusted Update .....43
- 5.7. Class: TOE Access (FTA) .....43
  - 5.7.1. FTA\_SSL\_EXT.1 – TSF-initiated Session Locking.....43
  - 5.7.2. FTA\_SSL.3 – TSF-initiated Termination .....43
  - 5.7.3. FTA\_SSL.4 – User-initiated Termination .....43
  - 5.7.4. FTA\_TAB.1 – Default TOE Access Banners .....43
- 5.8. Class: Trusted Path/Channels (FTP).....43
  - 5.8.1. FTP\_ITC.1 – Inter-TSF Trusted Channel .....43
  - 5.8.2. FTP\_ITC.1/MACSEC – Inter-TSF Trusted Channel (MACsec Communications).....43
  - FTP\_TRP.1/Admin – Trusted Path .....44
- 5.9. TOE SFR Dependencies Rationale .....44
- 5.10. TOE SFR Dependencies Rationale .....44
- 5.11. TOE SFR Dependencies Rationale .....45
- 5.12. Security Assurance Requirements Rationale .....45
- 5.13. Assurance Measures .....45
- 6. TOE Summary Specification.....46
  - 6.1. Key Zeroization.....56
  - 6.2. CAVP Certificates .....57
- 7. References .....59
  - 7.1. Acronyms and Terms .....59
  - 7.2. Obtaining Documentation and Submitting a Service Request .....61
  - 7.3. Contacting Cisco .....61

## Table of Tables

- Table 1. ST and TOE Identification ..... 8

Table 2. Required IT Environment Components .....	9
Table 3. Hardware Models and Specifications .....	11
Table 4. Excluded Functionality and Rationale.....	16
Table 5. PP Configuration Conformance.....	16
Table 6. NIAP Technical Decisions.....	17
Table 7. TOE Assumptions .....	20
Table 8. Threats .....	21
Table 9. Organizational Security Policies .....	23
Table 10. Security Objectives for the TOE.....	25
Table 11. Security Objectives for the Environment.....	26
Table 12. Security Requirement Conventions.....	27
Table 13. Security Functional Requirements .....	28
Table 14. Auditable Events .....	31
Table 15. MACsec Auditable Events .....	32
Table 16. Additional Password Special Characters.....	38
Table 17. Assurance Requirements.....	44
Table 18. Assurance Measures .....	45
Table 19. TSS Rationale .....	46
Table 20. Key Zeroization .....	56
Table 21. CAVP Certificates .....	57
Table 22. References.....	59
Table 23. Acronyms and Terms.....	60

## Table of Figures

Figure 1. TOE and Environment.....	10
------------------------------------	----

## Document Introduction

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

This document provides the basis for an evaluation of a specific Target of Evaluation (TOE), Cisco Catalyst 9400X/9600X Series Switches 17.12. This Security Target (ST) defines a set of assumptions about the aspects of the environment, a list of threats that the product intends to counter, a set of security objectives, a set of security requirements, and the IT security functions provided by the TOE which meet the set of requirements. Administrators of the TOE will be referred to as administrators, Authorized Administrators, TOE administrators, semi-privileged, privileged administrators, and security administrators in this document.

### Revision History

Version	Date	Change
0.1	December 20, 2023	Initial Version
0.2	March 21, 2024	Updates to Address Check-In Comments
0.3	August 6, 2024	Updates for Check Out Package
0.4	August 19, 2024	Additional Updates for Check Out Package
0.5	September 11, 2024	Updates to Address Check Out Comments
0.6	September 17, 2024	Final Updates

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: [www.cisco.com/go/trademarks](http://www.cisco.com/go/trademarks). Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

© 2024 Cisco Systems, Inc. All rights reserved.

# 1. Security Target Introduction

This Security Target contains the following sections:

- Security Target Introduction
- Conformance Claims
- Security Problem Definition
- Security Objectives
- Security Requirements
- TOE Summary Specification
- References

The structure and content of this ST comply with the requirements specified in the Common Criteria (CC), Part 1, Annex A, and Part 2.

## 1.1. ST and TOE Reference

This section provides information needed to identify and control this ST and its TOE.

**Table 1. ST and TOE Identification**

Name	Description
ST Title	Cisco Catalyst 9400X/9600X Series Switches 17.12 Security Target
ST Version	0.6
Publication Date	September 17, 2024
Vendor and ST Author	Cisco Systems, Inc.
TOE Reference	Cisco Catalyst 9400X/9600X Series Switches 17.12
TOE Hardware Models	Catalyst 9400X/9600X Series Switches
TOE Software Version	IOS-XE 17.12.02
Keywords	Audit, Authentication, Encryption, MACsec, Network Device, Secure Administration

## 1.2. TOE Overview

The Cisco Catalyst 9400X/9600X Series Switches 17.12 TOE is an enterprise access and core/distribution switch for enterprise and campus deployments. Switches are used to connect multiple devices, such as computers, wireless access points, printers, and servers on the same network within a building or campus. A switch enables connected devices to share information and talk to each other and are key building blocks for any network.



### 1.3. TOE Product Type

The Cisco Catalyst 9400X/9600X Series Switches 17.12 TOE is a layer 2 and 3 network device comprised of both hardware and software. The hardware is the Catalyst 9400X and Catalyst 9600X switches as described below in Table 3 of section 1.7.

### 1.4. Required non-TOE Hardware/Software/Firmware

The TOE requires the following hardware/software/firmware in the IT environment when the TOE is configured in its evaluated configuration.

**Table 2. Required IT Environment Components**

Component	Usage/Purpose/Description
MACsec Peer	This includes any MACsec peer with which the TOE participates in MACsec communications. MACsec Peer may be any device that supports MACsec communications.
Syslog Server	This includes any syslog server to which the TOE would transmit syslog messages over a TLS 1.2 trusted channel.
Certificate Authority	The Certification Authority is used to provide the TOE with valid certificates. The CA also provides the TOE with a method to check the peer certificate revocation status of devices the TOE communicates with.
Management Workstation	This includes any IT Environment Management workstation with a SSH client installed that is used by the Security Administrator for remote administration over SSH trusted paths.
Local Console	This includes any IT Environment Console that is directly connected to the TOE component via the console port and is used by the Security Administrator for local TOE administration.

### 1.5. TOE Description

The Cisco Catalyst 9400X/9600X Series Switches 17.12 Target of Evaluation (TOE) is a purpose-built, switching and routing platform enabling connected devices to communicate over a network at layer 2 or 3. The TOE provides Administrative control and management of the network. For communicating with other network devices, the TOE provides AES-128 and 256 MACsec encryption. The TOE also provides Layer 3 capabilities, including OSPF, EIGRP, ISIS, RIP, and routed access.

Hardware models only vary in component characteristics. These characteristics affect non-security relevant functions, such as throughput and amount of storage. Since there is no security relevant impact due to differing components, equivalence between all switch models is claimed.

Primary features of the Catalyst 9400X/9600X Series Switches include the following:

- Central processor that supports all system operations
- Dynamic memory, used by the central processor for all system operations
- Central Processing Unit (CPU) complex with 8-GigaBytes (GB) memory, 16-GB of flash, and an external Universal Serial Bus (USB) 3.0 Solid State Drive (SSD) pluggable storage slot (delivering 120-GB of storage with an optional SSD drive)
- Serial Advanced Technology Attachment (SATA) SSD local storage
- Flash memory Electrically Erasable Programmable Read-Only Memory (EEPROM), used to store the Cisco IOS-XE image (binary program)
- Non-volatile Read Only Memory (ROM) is used to store the bootstrap program and power-on diagnostic programs
- Non-volatile Random-Access Memory (NVRAM) is used to store switch configuration parameters that are used to initialize the system at start-up.

- Physical network interfaces (minimally two) (e.g., Registered Jack (RJ-45) serial and standard 10/100/1000 Ethernet ports). The number of network interface ports varies by model
- Dedicated management port on the switch, RJ-45 console port, and a USB mini-Type B console connection
- Resiliency with Field Replaceable Units (FRU) and redundant power supply, fans, and modular uplinks

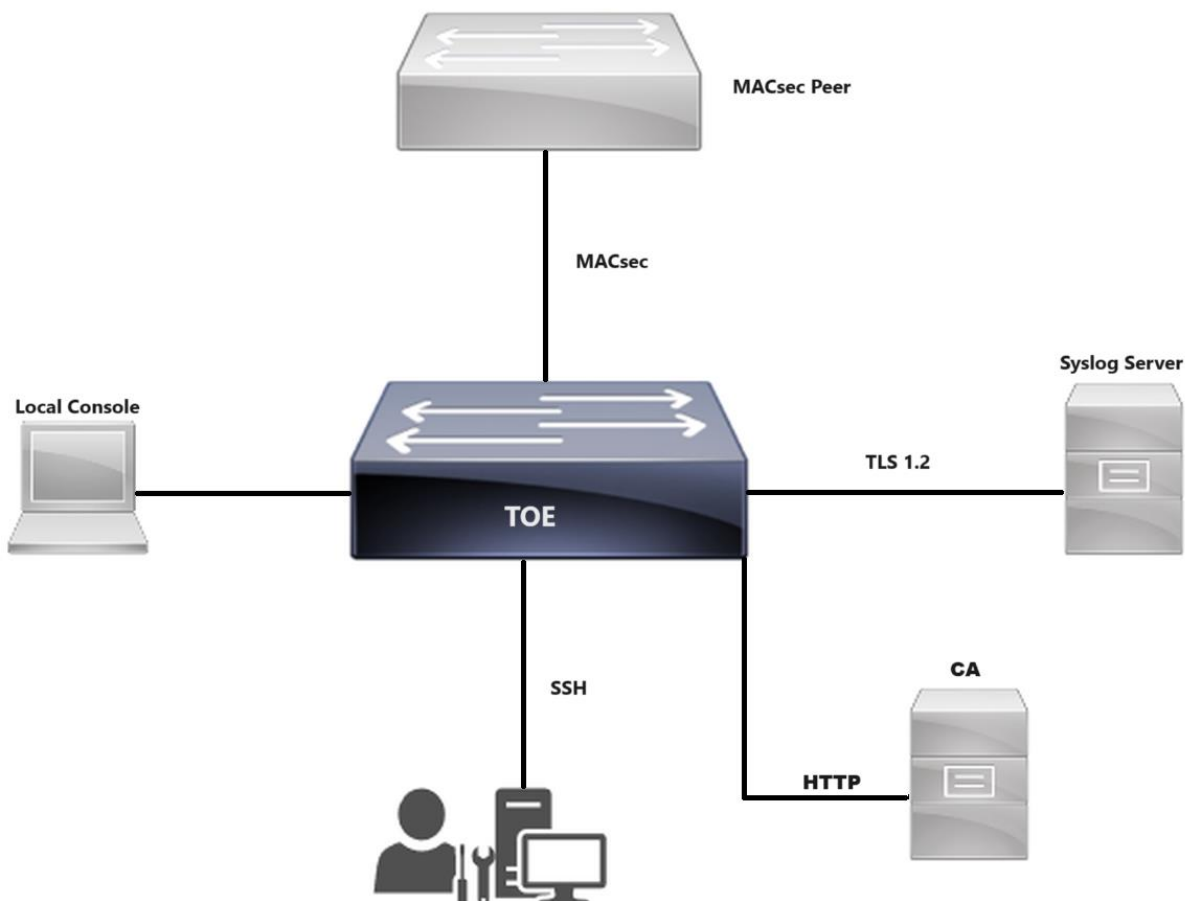
Cisco IOS-XE is a Cisco-developed highly configurable proprietary operating system that provides for efficient and effective routing and switching. Although IOS-XE performs many networking functions, this evaluation only addresses the functions that provide for the security of the TOE itself as described in section 1.8 below.

## 1.6. TOE Evaluated Configuration

Deployment of the TOE in its evaluated configuration consists of at least one TOE switch model following the Cisco Catalyst 9400X/9600X Series Switches 17.12 CC Configuration Guide (AGD). The TOE has two or more network interfaces and is connected to at least one internal and one external network. The Cisco IOS-XE configuration determines how packets are handled to and from the TOE's network interfaces. The switch configuration will determine how traffic flows received on an interface will be handled. Typically, packet flows are passed through the internet working device and forwarded to their configured destination.

A typical deployment with a single instance of the TOE is depicted in in figure 1 below.

Figure 1. TOE and Environment






The TOE can be administered interactively using a CLI over a local console connection or remotely over SSH.








The operational environment of the TOE will include at least one MACsec peer. The environment will also include an audit (syslog) server and a Management Workstation. The syslog server is used to store audit records, where the TOE uses TLS 1.2 to secure the transmission of the records. The Certification Authority is used to provide the TOE with valid certificates. The CA also provides the TOE with a method to check the peer certificate revocation status of devices the TOE communicates with.





### 1.7. Physical Scope of the TOE

The Cisco Catalyst 9400X/9600X Series Switches 17.12 TOE is composed of hardware and software with the following specifications:

**Table 3. Hardware Models and Specifications**

Hardware Component	Hardware Model and Picture	Specifications
<b>Chassis</b>	<p style="text-align: center;"><b>C9404R</b></p> 	<p><b>Slots:</b></p> <ul style="list-style-type: none"> <li>■ Line-card slots: 2</li> <li>■ Supervisor engine slots: 2</li> <li>■ Dedicated supervisor engine slot numbers: 2 and 3</li> </ul> <p><b>Power supply bays: 4</b>  <b>Fan-tray bays: 1</b></p>
	<p style="text-align: center;"><b>C9407R</b></p> 	<p><b>Slots:</b></p> <ul style="list-style-type: none"> <li>■ Line-card slots: 5</li> <li>■ Supervisor engine slots: 2</li> <li>■ Dedicated supervisor engine slot numbers: 3 and 4</li> </ul> <p><b>Power supply bays: 8</b>  <b>Fan-tray bays: 1</b></p>
	<p style="text-align: center;"><b>C9410R</b></p> 	<p><b>Slots:</b></p> <ul style="list-style-type: none"> <li>■ Line-card slots: 8</li> <li>■ Supervisor engine slots: 2</li> <li>■ Dedicated supervisor engine slot numbers: 5 and 6</li> </ul> <p><b>Power supply bays: 8</b>  <b>Fan-tray bays: 1</b></p>

Hardware Component	Hardware Model and Picture	Specifications
<b>Supervisor engines</b>	<p style="text-align: center;"><b>C9400X-SUP-2</b></p>  <p style="text-align: center;"><b>C9400X-SUP-2XL</b></p> 	<p><b>ASIC:</b> Cisco Unified Access Data Plane (UADP) 3.0; Encryption/decryption of MACsec traffic.</p> <p><b>Processor:</b> Intel Xeon D-1548 (Broadwell)</p> <p><b>Ports:</b></p> <ul style="list-style-type: none"> <li>■ Up to 4 non-blocking 25/10 Gigabit Ethernet uplinks</li> <li>■ 384 ports of non-blocking 1Gigabit Ethernet Fiber (SFP) ports</li> <li>■ 388 ports of non-blocking 10 Gigabit Ethernet SFP+ ports (4 uplinks plus 384 10G line cards ports)</li> </ul> <p><b>Management Ports:</b></p> <ul style="list-style-type: none"> <li>■ Ethernet management port: RJ-45 connectors, 4-pair Cat 5 UTP cabling</li> <li>■ Management console port: RJ-45-to-DB9 cable for PC connections,</li> <li>■ USB mini-Type B Console Port</li> </ul>
<b>Line Cards</b>	<p style="text-align: center;"><b>C9400-LC-48HX</b></p>  <p style="text-align: center;"><b>C9400-LC-48XS</b></p>  <p style="text-align: center;"><b>C9400X-LC-48HN</b></p>  <p style="text-align: center;"><b>C9400-LC-24XY</b></p>  <p style="text-align: center;"><b>C9400-LC-12QC</b></p> 	<p><b>Ports:</b> 48</p> <p><b>Speed:</b> 10GBASE-T, 5G/2.5G multigigabit, 1000M/100M</p> <p><b>Port Type:</b> RJ-45 UPOE+ IEEE 802.3bt, IEEE 802.3at, IEEE 802.3af, Cisco pre-standard</p> <p><b>Ports:</b> 48</p> <p><b>Speed:</b> 10 GE or 1 GE</p> <p><b>Port Type:</b> SFP+/SFP</p> <p><b>Ports:</b> 48</p> <p><b>Speed:</b> 5G/2.5G multigigabit, 1000M/100M</p> <p><b>Port Type:</b> RJ-45 UPOE+ IEEE 802.3bt, IEEE 802.3at, IEEE 802.3af, Cisco pre-standard</p> <p><b>Ports:</b> 24</p> <p><b>Speed:</b> 25G, 10G</p> <p><b>Port Type:</b> SFP28, SFP+</p> <p><b>Ports:</b> 12</p> <p><b>Speed:</b> 100G, 40G</p> <p><b>Port Type:</b> QSFP28, QSFP+</p>

Hardware Component	Hardware Model and Picture	Specifications
<b>Chassis</b>	<p><b>C9606R</b></p> 	<p><b>Slots:</b></p> <ul style="list-style-type: none"> <li>■ Line-card slots: 4</li> <li>■ Supervisor engine slots: 2</li> <li>■ Dedicated supervisor engine slot numbers: 3 and 4</li> </ul> <p><b>Power supply bays: 4</b> <b>Fan-tray bays: 1</b></p>
<b>Supervisor engines</b>	<p><b>C9600X-SUP2</b></p> 	<p><b>ASIC:</b> Cisco Silicon One Q200 <b>Processor:</b> Intel Xeon D-1573N (Broadwell) <b>Ports:</b></p> <ul style="list-style-type: none"> <li>■ Up to 8 non-blocking 400/200 Gigabit Ethernet QSFP-DD ports</li> <li>■ Up to 128 non-blocking 100 Gigabit Ethernet QSPF28 ports</li> <li>■ Up to 128 non-blocking 40 Gigabit Ethernet QSPF+ ports</li> <li>■ Up to 256 non-blocking 50G/25G/10G Gigabit Ethernet QSPF56 ports</li> <li>■ Up to 192 non-blocking 10 Gigabit Ethernet RJ45 copper port</li> </ul>
<b>Line Cards</b>	<p><b>C9600-LC-40YL4CD</b></p> 	<p><b>Ports</b></p> <ul style="list-style-type: none"> <li>■ 40 ports 50/25/10GE SFP56</li> <li>■ 2 ports 200/100/40QSFP56 uplinks</li> <li>■ 2 ports 400/200/100GE QSFP-DD uplink</li> </ul> <p><b>CDR5M PHY:</b> Encryption/decryption of MACsec traffic</p>
	<p><b>C9600X-LC-32CD</b></p> 	<p><b>Ports</b></p> <ul style="list-style-type: none"> <li>■ 30 ports 100/40G QSFP28</li> <li>■ 2 ports 400/200/100G QSFP-DD</li> </ul> <p><b>CDR5M PHY:</b> Encryption/decryption of MACsec traffic</p>

The TOE includes the **cat9k\_iosxe.17.12.02.SPA.bin** software image available for download on Cisco Software Central at <https://software.cisco.com/>. Customers can use their Cisco Care Online (CCO) or SMART account to download the software in a binary image format.

## 1.8. Logical Scope of the TOE

The TOE is comprised of several security features including:

- Security Audit
- Cryptographic Support
- Identification and Authentication
- Security Management
- Protection of the TSF
- TOE Access
- Trusted Path/Channels

These features are described in more detail in the following subsections.

## Security Audit

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

The TOE provides extensive capabilities to generate audit data targeted at detecting such activity. The TOE generates an audit record for each auditable event. Each security relevant audit event has the date, timestamp, event description, and subject identity. The TOE stores audit messages in a circular audit trail configurable by the Security Administrator. All audit logs are transmitted to an external audit server over a trusted channel protected with TLS 1.2. The TOE can determine when communication with the syslog server fails. If that should occur, the TOE will store all audit records locally and when the connection to the remote syslog server is restored, all stored audit records will be transmitted to the remote syslog server.

## Cryptographic Support

The TOE provides cryptographic functions to implement SSH, TLS, and MACsec protocols. The cryptographic algorithm implementation has been validated for CAVP conformance. This includes key generation and random bit generation, key establishment methods, key destruction, and the various types of cryptographic operations to provide AES encryption/decryption, signature verification, hash generation, and keyed hash generation.

The 9400X series supports MACsec using the proprietary Unified Access Data Plane (UADP) 2.0 Application-Specific Integrated Circuit (ASIC). The MACsec Controller (MSC) is embedded within the ASICs that are utilized within Cisco hardware platforms. The 9600X series support MACsec using the Marvell CDR5M PHY using the 400G MACsec Engine on Marvell Alaska C PHYs version X7121M C0.

SSH and TLS protocols are implemented using the IOS Common Cryptographic Module (IC2M) and CiscoSSL FOM cryptographic modules. Refer to Table 21 for identification of the relevant CAVP certificates.

## Identification and Authentication

The TOE implements three types of authentication to provide a trusted means for Security Administrators and remote servers/endpoints to securely communicate: X.509v3 certificate-based authentication for remote syslog servers, password-based authentication for Security Administrators on the local serial console or SSHv2 interfaces, and pre-shared keys for MACsec endpoints. The SSHv2 interface also supports authentication using SSH keys.

Security Administrators have the ability to compose strong passwords which are stored using a SHA-2 hash. Additionally, the TOE detects and tracks successive unsuccessful remote authentication attempts and will prevent the offending account from making further attempts until a Security Administrator defined time period has elapsed or until the Administrator manually unblocks the account.

## Security Management

The TOE provides secure remote administrative interface and local interface to perform the following security management functions:

- Local and remote administration of the TOE and the services provided by the TOE via the TOE CLI.
- The ability to manage the warning banner message and content which allows the Authorized Administrator the ability to define warning banner that is displayed prior to establishing a session (note this applies to the interactive (human) users, e.g., administrative users.
- The ability to set and modify the time limits of session inactivity.
- The ability to configure the number of failed Administrator logon attempts that will cause the account to be locked until a specified time period has elapsed.

- The ability to update the IOS-XE software. The validity of the image is provided using a digital signature prior to installing the update.
- The ability to modify the behavior of the transmission of audit data to an external IT entity.
- The ability to manage cryptographic keys.
- The ability to manage the cryptographic functionality which allows the Authorized Administrator the ability to identify and configure the algorithms used to provide protection of the data, such as generating the RSA keys to enable SSHv2.
- Ability to manage the TOE's trust store and designate X509.v3 certificates as trust anchor.
- Ability to configure thresholds for SSH rekeying.
- Ability to re-enable an Administrator account.
- The ability to manage the trusted public keys database.
- The ability to manage the Key Server and associated MKA participants.
- Manage a PSK-based CAK and install it in the device.
- The ability to specify the lifetime of a CAK and to enable, disable or delete a PSK in the CAK cache of a device.
- The ability to configure and set the time clock.
- The ability to configure the reference identifiers for peers, which can be IP address, FQDN identifier or can be the same as the peer's name.
- Ability to import X.509v3 certificates to the TOE's trust store.

The TOE provides a Security Administrator role and only the Security Administrator can perform the above security management functions.

## Protection of the TSF

The TOE protects critical security data including keys and passwords against tampering by untrusted subjects. The TOE provides reliable timestamps to support monitoring local and remote interactive administrative sessions for inactivity, validating X.509 certificates (to determine if a certificate has expired), and to support accurate audit records.

The TOE detects replay of MACsec traffic. If replay is detected, the MACsec packets are discarded.

The TOE provides self-tests to ensure it is operating correctly, including the ability to detect software integrity failures. Additionally, the TOE provides an ability to perform software updates and to verify those software updates are from Cisco Systems, Inc.

## TOE Access

The TOE monitors both local and remote admin sessions for inactivity and terminates when a threshold time period is reached. Once a session has been terminated the TOE requires the user to re-authenticate.

The TOE also displays a Security Administrator specified advisory notice and consent warning message prior to initiating identification and authentication for each administrative user.

## Trusted Path/Channels

The TOE provides encryption (protection from disclosure and detection of modification) for communication paths and channels between itself and remote endpoints.

In addition, the TOE provides two-way authentication of each endpoint in a cryptographically secure manner, meaning that even if there was a malicious attacker between the two endpoints, any attempt to represent themselves to either endpoint of the communications path as the other communicating party would be detected.

## 1.9. Excluded Functionality

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

**Table 4. Excluded Functionality and Rationale**

Function Excluded	Rationale
Non-FIPS 140-2 mode of operation	The TOE includes FIPS mode of operation. The FIPS modes allows the TOE to use only approved cryptography. FIPS mode of operation must be enabled in order for the TOE to be operating in its evaluated configuration.
HTTP/HTTPS (for remote management)	Remote Management is performed using SSH
SNMP	Remote Management is performed using SSH

These services can be disabled by using the configuration settings as described in section 4.2.18 of the Cisco Catalyst 9400X/9600X Series Switches 17.12 CC Configuration Guide (AGD).

Additionally, the TOE includes a number of functions where there are no Security Functional Requirements that apply from the collaborative Protection Profile for Network Devices v2.2e or the PP-Module for MACsec Ethernet Encryption v1.0. The excluded functionality does not affect the TOE's conformance to the claimed Protection Profiles.

## 2. Conformance Claims

### 2.1. Common Criteria Conformance Claim

The TOE and ST are compliant with the Common Criteria (CC) Version 3.1, Revision 5, dated: April 2017. The TOE and ST are CC Part 2 extended and CC Part 3 conformant.

### 2.2. PP Configuration Conformance Claim

The TOE and ST are conformant with the PP Configuration identified in the PP-Configuration column of Table 5.

**Table 5. PP Configuration Conformance**

PP-Configuration	Component	Version	Date
PP-Configuration for Network Devices and MACsec Ethernet Encryption, 2023-03-29, Version 1.0, (CFG_NDcPP-MACsec_V1.0), which includes the components in the next column	Base-PP: collaborative Protection Profile for Network Devices (CPP_ND_V2.2E)	2.2e	March 23, 2020
	PP-Module: PP-Module for MACsec Ethernet Encryption (MOD_MACsec_V1.0)	1.0	March 2, 2023

This ST applies the following NIAP Technical Decisions:



Table 6. NIAP Technical Decisions

Number	Title	PP	Applicable	Exclusion Rational
TD0800	Updated NIT Technical Decision for IPsec IKE/SA Lifetimes Tolerance	[NDcPP]	No	The TOE does not claim IPsec
TD0792	NIT Technical Decision: FIA_PMG_EXT.1 - TSS EA not in line with SFR	[NDcPP]	Yes	
TD0790	NIT Technical Decision: Clarification Required for testing IPv6	[NDcPP]	Yes	
TD0738	NIT Technical Decision for Link to Allowed-With List	[NDcPP]	Yes	
TD0670	NIT Technical Decision for Mutual and Non-Mutual Auth TLSC Testing	[NDcPP]	Yes	
TD0639	NIT Technical Decision for Clarification for NTP MAC Keys	[NDcPP]	No	The TOE does not claim FCS_NTP_EXT.1
TD0638	NIT Technical Decision for Key Pair Generation for Authentication	[NDcPP]	Yes	
TD0636	NIT Technical Decision for Clarification of Public Key User Authentication for SSH	[NDcPP]	No	The TOE does not claim FCS_SSHC_EXT.1
TD0635	NIT Technical Decision for TLS Server and Key Agreement Parameters	[NDcPP]	No	The TOE does not claim FCS_TLSS_EXT.1
TD0632	NIT Technical Decision for Consistency with Time Data for vNDs	[NDcPP]	Yes	
TD0631	NIT Technical Decision for Clarification of public key authentication for SSH Server	[NDcPP]	Yes	
TD0592	NIT Technical Decision for Local Storage of Audit Records	[NDcPP]	Yes	
TD0591	NIT Technical Decision for Virtual TOEs and hypervisors	[NDcPP]	Yes	
TD0581	NIT Technical Decision for Elliptic curve-based key establishment and NIST SP 800-56Arev3	[NDcPP]	Yes	
TD0580	NIT Technical Decision for clarification about use of DH14 in NDcPPv2.2e	[NDcPP]	Yes	
TD0572	NIT Technical Decision for Restricting FTP_ITC.1 to only IP address identifiers	[NDcPP]	Yes	
TD0571	NIT Technical Decision for Guidance on how to handle FIA_AFL.1	[NDcPP]	Yes	
TD0570	NIT Technical Decision for Clarification about FIA_AFL.1	[NDcPP]	Yes	
TD0569	NIT Technical Decision for Session ID Usage Conflict in FCS_DTLSS_EXT.1.7	[NDcPP]	No	FCS_TLSS_EXT.1 not claimed

Number	Title	PP	Applicable	Exclusion Rational
TD0564	NIT Technical Decision for Vulnerability Analysis Search Criteria	[NDcPP]	Yes	
TD0563	NIT Technical Decision for Clarification of audit date information	[NDcPP]	Yes	
TD0556	NIT Technical Decision for RFC 5077 question	[NDcPP]	No	FCS_TLSS_EXT.1 not claimed
TD0555	NIT Technical Decision for RFC Reference incorrect in TLSS Test	[NDcPP]	No	FCS_TLSS_EXT.1 not claimed
TD0547	NIT Technical Decision for Clarification on developer disclosure of AVA_VAN	[NDcPP]	Yes	
TD0546	NIT Technical Decision for DTLS - clarification of Application Note 63	[NDcPP]	No	FCS_DTLS_EXT.1 not claimed
TD0537	NIT Technical Decision for Incorrect reference to FCS_TLSC_EXT.2.3	[NDcPP]	Yes	
TD0536	NIT Technical Decision for Update Verification Inconsistency	[NDcPP]	Yes	
TD0528	NIT Technical Decision for Missing EAs for FCS_NTP_EXT.1.4	[NDcPP]	No	FCS_NTP_EXT.1 not claimed
TD0527	Updates to Certificate Revocation Testing (FIA_X509_EXT.1)	[NDcPP]	Yes	
TD0870	Security Objectives Rationale for MOD_MACSEC_V1.0	[MOD_MACSEC]	Yes	
TD0869	Correction to MN Usage for FPT_RPL.1 Test	[MOD_MACSEC]	Yes	
TD0841	Correction For Tests Incorrectly Requiring Group MACsec	[MOD_MACSEC]	Yes	
TD0840	Alignment of Test 22.1 to FMT_SMF.1/MACSEC	[MOD_MACSEC]	Yes	
TD0826	Aligning MOD_MACSEC_V1.0 with CPP_ND_V3.0E	[MOD_MACSEC]	No	CPP_ND_V3.0E not claimed
TD0817	MACsec Data Delay Protection, Key Agreement, and Conditional Support for Group CAK	[MOD_MACSEC]	Yes	
TD0816	Clarity for MACsec Self Test Failure Response	[MOD_MACSEC]	Yes	
TD0748	Correction to FMT_SMF.1/MACSEC Test 21	[MOD_MACSEC]	Yes	
TD0746	Correction to FPT_RPL.1 Test 25	[MOD_MACSEC]	Yes	
TD0728	Corrections to MACSec PP-Module SD	[MOD_MACSEC]	Yes	

## 2.3. Protection Profile Conformance Claim Rationale

### 2.3.1. TOE Appropriateness

The TOE provides all of the functionality at a level of security commensurate with that identified in the U.S. Government Protection Profiles.

### 2.3.2. TOE Security Problem Definition Consistency

The Assumptions, Threats, and Organization Security Policies included in the Security Target represent the Assumptions, Threats, and Organization Security Policies specified in [NDcPP] and [MOD\_MACSEC] for which conformance is claimed verbatim. All concepts covered in the Protection Profile Security Problem Definition are included in the Security Target Statement of Security Objectives Consistency.

The Security Objectives included in the Security Target represent the Security Objectives specified in [NDcPP] and [MOD\_MACSEC] for which conformance is claimed verbatim. All concepts covered in the Protection Profile's Statement of Security Objectives are included in the Security Target.

### 2.3.3. Statement of Security Requirements Consistency

The Security Functional Requirements included in the Security Target represent the Security Functional Requirements specified in [NDcPP] and [MOD\_MACSEC] for which conformance is claimed verbatim. All concepts covered the Protection Profile's Statement of Security Requirements are included in the Security Target. Additionally, the Security Assurance Requirements included in the Security Target are identical to the Security Assurance Requirements included in the claimed Protection Profiles.

### 3. Security Problem Definition

This section identifies the following:

- Assumptions about the TOE's operational environment. These assumptions include both practical realities in the development of the TOE security requirements and the essential environmental conditions on the use of the TOE.
- Threats addressed by the TOE and the IT Environment.
- Organizational Security Policies imposed by an organization on the TOE to address its security needs.

The security problem definition below has been drawn verbatim from [NDcPP] and [MOD\_MACSEC].

#### 3.1. Assumptions

**Table 7. TOE Assumptions**

Assumption	Assumption Definition
A.PHYSICAL_PROTECTION	The Network Device is assumed to be physically protected in its operational environment and not subject to physical attacks that compromise the security or interfere with the device's physical interconnections and correct operation. This protection is assumed to be sufficient to protect the device and the data it contains. As a result, the cPP does not include any requirements on physical tamper protection or other physical attack mitigations. The cPP does not expect the product to defend against physical access to the device that allows unauthorized entities to extract data, bypass other controls, or otherwise manipulate the device. For vNDs, this assumption applies to the physical platform on which the VM runs.
A.LIMITED_FUNCTIONALITY	The device is assumed to provide networking functionality as its core function and not provide functionality/ services that could be deemed as general purpose computing. For example the device should not provide computing platform for general purpose applications (unrelated to networking functionality).  If a virtual TOE evaluated as a pND, following Case 2 vNDs as specified in Section 1.2, the VS is considered part of the TOE with only one vND instance for each physical hardware platform. The exception being where components of a distributed TOE run inside more than one virtual machine (VM) on a single VS. In Case 2 vND, no non-TOE guest VMs are allowed on the platform.
A.NO_THRU_TRAFFIC_PROTECTION	A standard/generic Network Device does not provide any assurance regarding the protection of traffic that traverses it. The intent is for the Network Device to protect data that originates on or is destined to the device itself, to include administrative data and audit data. Traffic that is traversing the Network Device, destined for another network entity, is not covered by the ND cPP. It is assumed that this protection will be covered by cPPs for particular types of Network Devices (e.g., firewall).

A.TRUSTED_ADMINISTRATOR	<p>The Security Administrator(s) for the Network Device are assumed to be trusted and to act in the best interest of security for the organization. This includes appropriately trained, following policy, and adhering to guidance documentation. Administrators are trusted to ensure passwords/credentials have sufficient strength and entropy and to lack malicious intent when administering the device. The Network Device is not expected to be capable of defending against a malicious Administrator that actively works to bypass or compromise the security of the device.</p> <p>For TOEs supporting X.509v3 certificate-based authentication, the Security Administrator(s) are expected to fully validate (e.g. offline verification) any CA certificate (root CA certificate or intermediate CA certificate) loaded into the TOE's trust store (aka 'root store', 'trusted CA Key Store', or similar) as a trust anchor prior to use (e.g. offline verification).</p>
A.REGULAR_UPDATES	<p>The Network Device firmware and software is assumed to be updated by an Administrator on a regular basis in response to the release of product updates due to known vulnerabilities.</p>
A.ADMIN_CREDENTIALS_SECURE	<p>The Administrator's credentials (private key) used to access the Network Device are protected by the platform on which they reside.</p>
A.RESIDUAL_INFORMATION	<p>The Administrator must ensure 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.</p>

## 3.2. Threats

**Table 8. Threats**

Threat	Threat Definition
T.UNAUTHORIZED_ADMINISTRATOR_ACCESS	<p>Threat agents may attempt to gain Administrator access to the Network Device by nefarious means such as masquerading as an Administrator to the device, masquerading as the device to an Administrator, replaying an administrative session (in its entirety, or selected portions), or performing man-in-the-middle attacks, which would provide access to the administrative session, or sessions between Network Devices. Successfully gaining administrator access allows malicious actions that compromise the security functionality of the device and the network on which it resides.</p>

T.WEAK_CRYPTOGRAPHY	Threat agents may exploit weak cryptographic algorithms or perform a cryptographic exhaust against the key space. Poorly chosen encryption algorithms, modes, and key sizes will allow attackers to compromise the algorithms, or brute force exhaust the key space and give them unauthorized access allowing them to read, manipulate and/or control the traffic with minimal effort.
T.UNTRUSTED_COMMUNICATION_CHANNELS	Threat agents may attempt to target Network Devices that do not use standardized secure tunneling protocols to protect the critical network traffic. Attackers may take advantage of poorly designed protocols or poor key management to successfully perform man-in-the middle attacks, replay attacks, etc. Successful attacks will result in loss of confidentiality and integrity of the critical network traffic, and potentially could lead to a compromise of the Network Device itself.
T.WEAK_AUTHENTICATION_ENDPOINTS	Threat agents may take advantage of secure protocols that use weak methods to authenticate the endpoints – e.g., shared password that is guessable or transported as plaintext. The consequences are the same as a poorly designed protocol, the attacker could masquerade as the Administrator or another device, and the attacker could insert themselves into the network stream and perform a man-in-the-middle attack. The result is the critical network traffic is exposed and there could be a loss of confidentiality and integrity, and potentially the Network Device itself could be compromised.
T.UPDATE_COMPROMISE	Threat agents may attempt to provide a compromised update of the software or firmware which undermines the security functionality of the device. Non-validated updates or updates validated using non-secure or weak cryptography leave the update firmware vulnerable to surreptitious alteration.
T.UNDETECTED_ACTIVITY	Threat agents may attempt to access, change, and/or modify the security functionality of the Network Device without Administrator awareness. This could result in the attacker finding an avenue (e.g., misconfiguration, flaw in the product) to compromise the device and the Administrator would have no knowledge that the device has been compromised.
T.SECURITY_FUNCTIONALITY_COMPROMISE	Threat agents may compromise credentials and device data enabling continued access to the Network Device and its critical data. The compromise of credentials include replacing existing credentials with an attacker's credentials, modifying existing credentials, or obtaining the Administrator or device credentials for use by the attacker.
T.PASSWORD_CRACKING	Threat agents may be able to take advantage of weak administrative passwords to gain privileged access to the device. Having privileged access to the device provides the attacker unfettered access to the network traffic, and may allow them to take advantage of any trust relationships with other Network Devices.

T.SECURITY_FUNCTIONALITY_FAILURE	An external, unauthorized entity could make use of failed or compromised security functionality and might therefore subsequently use or abuse security functions without prior authentication to access, change or modify device data, critical network traffic or security functionality of the device.
T.DATA_INTEGRITY	<p>An attacker may modify data transmitted over the layer 2 link in a way that is not detected by the recipient.</p> <p>Devices on a network may be exposed to attacks that attempt to corrupt or modify data in transit without authorization. If malicious devices are able to modify and replay data that is transmitted over a layer 2 link, then the data contained within the communications may be susceptible to a loss of integrity.</p>
T.NETWORK_ACCESS	<p>An attacker may send traffic through the TOE that enables them to access devices in the TOE's operational environment without authorization.</p> <p>A MACsec device may sit on the periphery of a network, which means that it may have an externally-facing interface to a public network. Devices located in the public network may attempt to exercise services located on the internal network that are intended to be accessed only from within the internal network or externally accessible only from specifically authorized devices. If the MACsec device allows unauthorized external devices access to the internal network, these devices on the internal network may be subject to compromise. Similarly, if two MACsec devices are deployed to facilitate end-to-end encryption of traffic that is contained within a single network, an attacker could use an insecure MACsec device as a method to access devices on a specific segment of that network such as an individual LAN.</p>
T.UNTRUSTED_MACSEC_COMMUNICATION_CHANNELS	<p>An attacker may acquire sensitive TOE or user data that is transmitted to or from the TOE because an untrusted communication channel causes a disclosure of data in transit.</p> <p>A generic network device may be threatened by the use of insecure communications channels to transmit sensitive data. The attack surface of a MACsec device also includes the MACsec trusted channels. Inability to secure communications channels, or failure to do so correctly, would expose user data that is assumed to be secure to the threat of unauthorized disclosure.</p>

### 3.3. Organizational Security Policies

**Table 9. Organizational Security Policies**

Policy Name	Policy Definition
P.ACCESS_BANNER	The TOE shall display an initial banner describing restrictions of use, legal agreements, or any other appropriate information to which users consent by accessing the TOE.





## 4. Security Objectives

This section identifies the security objectives of the TOE and the IT Environment. The security objectives identify the responsibilities of the TOE and the TOE's IT environment in meeting the security needs.

### 4.1. Security Objectives for the TOE

The following table identifies the Security Objectives for the TOE. These security objectives reflect the stated intent to counter identified threats and/or comply with any security policies. The security objectives below have been drawn verbatim from [NDCPP] and [MOD\_MACSEC].

**Table 10. Security Objectives for the TOE**

Environment Security Objective	TOE Security Objective Definition
O.AUTHENTICATION_MACSEC	To further address the issues associated with unauthorized disclosure of information, a compliant TOE's authentication ability (MKA) will allow a MACsec peer to establish connectivity associations (CAs) with another MACsec peer. MACsec endpoints authenticate each other to ensure they are communicating with an authorized MAC Security Entity (SecY) entity. Addressed by: FCS_MACSEC_EXT.4, FCS_MKA_EXT.1, FIA_PSK_EXT.1, FCS_DEVID_EXT.1 (selection-based), FCS_EAP-TLS_EXT.1 (selection-based)
O.AUTHORIZED_ADMINISTRATION	All network devices are expected to provide services that allow the security functionality of the device to be managed. The MACsec device, as a specific type of network device, has a refined set of management functions to address its specialized behavior. In order to further mitigate the threat of a compromise of its security functionality, the MACsec device prescribes the ability to limit brute-force authentication attempts by enforcing lockout of accounts that experience excessive failures and by limiting access to security-relevant data that administrators do not need to view. Addressed by: FMT_SMF.1/MACSEC, FPT_CAK_EXT.1, FIA_AFL_EXT.1 (optional), FTP_TRP.1/MACSEC (optional), FMT_SNMP_EXT.1 (selection-based)
O.CRYPTOGRAPHIC_FUNCTIONS_MACSEC	To address the issues associated with unauthorized modification and disclosure of information, compliant TOEs will implement cryptographic capabilities. These capabilities are intended to maintain confidentiality and allow for detection and modification of data that is transmitted outside of the TOE. Addressed by: FCS_COP.1/CMAC, FCS_COP.1/MACSEC, FCS_MACSEC_EXT.2, FCS_MACSEC_EXT.3, FTP_ITC.1/MACSEC, FTP_TRP.1/MACSEC (optional), FCS_SNMP_EXT.1 (selection-based)
O.PORT_FILTERING_MACSEC	To further address the issues associated with unauthorized network access, a compliant TOE's port filtering capability will restrict the flow of network traffic through the TOE based on layer 2 frame characteristics and whether or not the traffic represents valid MACsec frames and MACsec Key Agreement Protocol Data Units (MKPDUs). Addressed by: FCS_MACSEC_EXT.1, FIA_PSK_EXT.1, FPT_DDP_EXT.1

O.REPLAY_DETECTION	A MACsec device is expected to help mitigate the threat of MACsec data integrity violations by providing a mechanism to detect and discard replayed traffic for MPDUs. Addressed by: FPT_RPL.1, FPT_RPL_EXT.1 (optional)
O.SYSTEM_MONITORING_MACSEC	To address the issues of administrators being able to monitor the operations of the MACsec device, compliant TOEs will implement the ability to log the flow of Ethernet traffic. Specifically, the TOE will provide the means for administrators to configure rules to 'log' when Ethernet traffic grants or restricts access. As a result, the 'log' will result in informative event logs whenever a match occurs. In addition, the establishment of security CAs is auditable, not only between MACsec devices, but also with MAC Security Key Agreement Entities (KaYs). Addressed by: FAU_GEN.1/MACSEC
O.TSF_INTEGRITY	To mitigate the security risk that the MACsec device may fail during startup, it is required to fail-secure if any self-test failures occur during startup. This ensures that the device will only operate when it is in a known state. Addressed by: FPT_FLS.1

## 4.2. Security Objectives for the Environment

The following table identifies the Security Objectives for the Environment. These security objectives reflect the stated intent to counter identified threats and/or comply with any security policies. The security objectives below have been drawn verbatim from [NDcPP] and [MOD\_MACSEC].

**Table 11. Security Objectives for the Environment**

Environment Security Objective	IT Environment Security Objective Definition
OE.PHYSICAL	Physical security, commensurate with the value of the TOE and the data it contains, is provided by the environment.
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. Note: For vNDs the TOE includes only the contents of the its own VM, and does not include other VMs or the VS.
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.

OE.TRUSTED_ADMIN	Security Administrators are trusted to follow and apply all guidance in a trusted manner. For vNDs, this includes the VS Administrator responsible for configuring the VMs that implement ND functionality.  For TOEs supporting X.509v3 certificate-based authentication, the Security Administrator(s) are assumed to monitor the revocation status of all certificates in the TOE's trust store and to remove any certificate from the TOE's trust store in case such certificate can no longer be trusted.
OE.UPDATE	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.
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.
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. For vNDs, this applies when the physical platform on which the VM runs is removed from its operational environment.

## 5. Security Requirements

This section identifies the Security Functional Requirements for the TOE. The Security Functional Requirements in this section are drawn from [CC\_PART2], [NDcPP], [MOD\_MACSEC], and NIAP Technical Decisions.

### 5.1. Conventions

[CC\_PART1] defines operations on Security Functional Requirements. This document uses the following conventions to identify the operations permitted by [NDcPP], [MOD\_MACSEC] and NIAP Technical Decisions.

**Table 12. Security Requirement Conventions**

Convention	Indication
Assignment	Indicated with <i>italicized text</i>
Refinement	Indicated with <b>bold text</b> and <del>strikethroughs</del>
Selection	Indicated with <u>underlined text</u>
Assignment within a Selection	Indicated with <i><u>italicized and underlined text</u></i>
Iteration	indicated by adding a string starting with '/' (e.g. 'FCS_COP.1/Hash')

Where operations were completed in the [NDcPP] itself, the formatting used in the [NDcPP] has been retained. Formatting used in [NDcPP] and [MOD\_MACSEC] that is inconsistent with the listed conventions has not been retained in the ST.

The TOE Security Functional Requirements are identified in the following table and are described in more detail in the following subsections.

**Table 13. Security Functional Requirements**

Class Name	Component Identification	Component Name	Drawn From
FAU: Security Audit	FAU_GEN.1	Audit data generation	[NDcPP]
	FAU_GEN.1/MACSEC	Audit Data Generation (MACsec)	[MOD_MACSEC]
	FAU_GEN.2	User Identity Association	[NDcPP]
	FAU_STG_EXT.1	Protected Audit Event Storage	[NDcPP]
FCS: Cryptographic Support	FCS_CKM.1	Cryptographic Key Generation (Refinement)	[NDcPP]
	FCS_CKM.2	Cryptographic Key Establishment	[NDcPP]
	FCS_CKM.4	Cryptographic Key Destruction	[NDcPP]
	FCS_COP.1/DataEncryption	Cryptographic Operation (AES Data Encryption/Decryption)	[NDcPP]
	FCS_COP.1/MACSEC	Cryptographic Operation (MACsec AES Data Encryption/Decryption)	[MOD_MACSEC]
	FCS_COP.1/SigGen	Cryptographic Operation (Signature Generation and Verification)	[NDcPP]
	FCS_COP.1/Hash	Cryptographic Operation (Hash Algorithm)	[NDcPP]
	FCS_COP.1/KeyedHash	Cryptographic Operation (Keyed Hash Algorithm)	[NDcPP]
	FCS_COP.1/CMAC	Cryptographic Operation (AES-CMAC Keyed Hash Algorithm)	[MOD_MACSEC]
	FCS_RBG_EXT.1	Random Bit Generation	[NDcPP]
	FCS_MACSEC_EXT.1	MACsec	[MOD_MACSEC]
	FCS_MACSEC_EXT.2	MACsec Integrity and Confidentiality	[MOD_MACSEC]
	FCS_MACSEC_EXT.3	MACsec Randomness	[MOD_MACSEC]
	FCS_MACSEC_EXT.4	MACsec Key Usage	[MOD_MACSEC]
	FCS_MKA_EXT.1	MACsec Key Agreement	[MOD_MACSEC]
	FCS_SSHS_EXT.1	SSH Server Protocol	[NDcPP]
FCS_TLSC_EXT.1	TLS Client Protocol Without Mutual Authentication	[NDcPP]	

Class Name	Component Identification	Component Name	Drawn From
FIA: Identification and authentication	FIA_AFL.1	Authentication Failure Management	[NDcPP]
	FIA_PMG_EXT.1	Password Management	[NDcPP]
	FIA_PSK_EXT.1	Extended: Pre-Shared Key Composition	[MOD_MACSEC]
	FIA_UIA_EXT.1	User Identification and Authentication	[NDcPP]
	FIA_UAU_EXT.2	Password-based Authentication Mechanism	[NDcPP]
	FIA_UAU.7	Protected Authentication Feedback	[NDcPP]
	FIA_X509_EXT.1/Rev	X.509 Certificate Validation	[NDcPP]
	FIA_X509_EXT.2	X.509 Certificate Authentication	[NDcPP]
FMT: Security Management	FMT_MOF.1/ManualUpdate	Management of security functions behaviour	[NDcPP]
	FMT_MTD.1/CoreData	Management of TSF Data	[NDcPP]
	FMT_MTD.1/CryptoKeys	Management of TSF Data	[NDcPP]
	FMT_SMF.1	Specification of Management Functions	[NDcPP]
	FMT_SMF.1/MACSEC	Specification of Management Functions (MACsec)	[MOD_MACSEC]
	FMT_SMR.2	Restrictions on Security Roles	[NDcPP]
FPT: Protection of the TSF	FPT_CAK_EXT.1	Protection of CAK Data	[MOD_MACSEC]
	FPT_FLS.1	Failure with Preservation of Secure State	[MOD_MACSEC]
	FPT_RPL.1	Replay Detection	[MOD_MACSEC]
	FPT_RPL_EXT.1	Replay Protection for XPN	[MOD_MACSEC]
	FPT_APW_EXT.1	Extended: Protection of Administrator Passwords	[NDcPP]
	FPT_SKP_EXT.1	Extended: Protection of TSF Data (for reading of all pre-shared, symmetric and private keys)	[NDcPP]
	FPT_STM_EXT.1	Reliable Time Stamps	[NDcPP]
	FPT_TST_EXT.1	TSF Testing (Extended)	[NDcPP]

Class Name	Component Identification	Component Name	Drawn From
	FPT_TUD_EXT.1	Trusted update	[NDcPP]
FTA: TOE Access	FTA_SSL_EXT.1	TSF-initiated Session Locking	[NDcPP]
	FTA_SSL.3	TSF-initiated Termination	[NDcPP]
	FTA_SSL.4	User-initiated Termination	[NDcPP]
	FTA_TAB.1	Default TOE Access Banners	[NDcPP]
FTP: Trusted path/channels	FTP_ITC.1	Inter-TSF trusted channel	[NDcPP]
	FTP_ITC.1/MACSEC	Inter-TSF Trusted Channel (MACsec Communications)	[MOD_MACSEC]
	FTP_TRP.1/Admin	Trusted Path	[NDcPP]

## 5.2. Class: Security Audit (FAU)

### 5.2.1. FAU\_GEN.1 – Audit Data Generation

**FAU\_GEN.1.1** The TSF shall be able to generate an audit record of the following auditable events:

- a) Start-up and shutdown of the audit functions;
- b) All auditable events for the not specified level of audit; and
- c) *All administrator actions comprising:*
  - *Administrative login and logout (name of user account shall be logged if individual user accounts are required for Administrators).*
  - *Changes to TSF data related to configuration changes (in addition to the information that a change occurred it shall be logged what has been changed).*
  - *Generating/import of, changing, or deleting of cryptographic keys (in addition to the action itself a unique key name or key reference shall be logged).*
  - *Resetting passwords (name of related user account shall be logged).*
  - *[Starting and stopping services];*
- d) *Specifically defined auditable events listed in Table 14.*

**FAU\_GEN.1.2** The TSF shall record within each audit record at least the following information:

- a) Date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event; and
- b) For each audit event type, based on the auditable event definitions of the functional components included in the cPP/ST, information specified in column three of Table 14.

Table 14. Auditable Events

SFR	Auditable Event	Additional Audit Record Contents
FAU_GEN.1	None.	None.
FAU_GEN.2	None.	None.
FAU_STG_EXT.1	None.	None.
FCS_CKM.1	None.	None.
FCS_CKM.2	None.	None.
FCS_CKM.4	None.	None.
FCS_COP.1/DataEncryption	None.	None.
FCS_COP.1/SigGen	None.	None.
FCS_COP.1/Hash	None.	None.
FCS_COP.1/KeyedHash	None.	None.
FCS_RBG_EXT.1	None.	None.
FCS_SSHS_EXT.1	Failure to establish an SSH session	Reason for failure.
FCS_TLSC_EXT.1	Failure to establish a TLS session	Reason for failure.
FIA_AFL.1	Unsuccessful login attempts limit is met or exceeded.	Origin of the attempt (e.g., IP address).
FIA_PMG_EXT.1	None.	None.
FIA_UIA_EXT.1	All use of the identification and authentication mechanism.	Origin of the attempt (e.g., IP address).
FIA_UAU_EXT.2	All use of the identification and authentication mechanism.	Origin of the attempt (e.g., IP address).
FIA_UAU.7	None.	None.
FIA_X509_EXT.1/Rev	Unsuccessful attempt to validate a certificate  Any addition, replacement or removal of trust anchors in the TOE's trust store.	Reason for failure of certificate validation  Identification of certificates added, replaced or removed as trust anchor in the TOE's trust store.
FIA_X509_EXT.2	None.	None.
FMT_MOF.1/ManualUpdate	Any attempt to initiate a manual update	None.
FMT_MTD.1/CoreData	None.	None.
FMT_MTD.1/CryptoKeys	None.	None.
FMT_SMF.1	All management activities of TSF data.	None.
FMT_SMR.2	None.	None.

SFR	Auditable Event	Additional Audit Record Contents
FPT_APW_EXT.1	None.	None.
FPT_SKP_EXT.1	None.	None.
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).
FPT_TST_EXT.1	None.	None.
FPT_TUD_EXT.1	Initiation of update. result of the update attempt (success or failure)	None.
FTA_SSL_EXT.1	The termination of a local session by the session locking mechanism.	None.
FTA_SSL.3	The termination of a remote session by the session locking mechanism.	None.
FTA_SSL.4	The termination of an interactive session.	None.
FTA_TAB.1	None.	None.
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.
FTP_TRP.1/Admin	Initiation of the trusted path. Termination of the trusted path. Failures of the trusted path functions.	None.

### 5.2.2. FAU\_GEN.1/MACSEC – Audit Data Generation (MACsec)

**FAU\_GEN.1.1/MACSEC** The TSF shall be able to generate an audit record of the following auditable events:

- a) Start-up and shutdown of the audit functions;
- b) All auditable events for the [*not specified*] level of audit;
- c) **All administrative actions;**
- d) [Specifically defined auditable events listed in the Auditable Events table (Table 15)]

**Table 15. MACsec Auditable Events**

SFR	Auditable Event	Additional Audit Record Contents
FCS_MACSEC_EXT.1	Session establishment	Secure Channel Identifier (SCI)



SFR	Auditable Event	Additional Audit Record Contents
FCS_MACSEC_EXT.3	Creation and update of SAK	Creation and update times
FCS_MACSEC_EXT.4	Creation of CA	Connectivity Association Key Names (CKNs)
FPT_RPL.1	Detected replay attempt	None.

**FAU\_GEN.1.2/MACSEC** The TSF shall record within each audit record at least the following information:

- Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and
- For each audit event type, based on the auditable event definitions of the functional components included in the PP-Module/ST, [information specified in column three of the Auditable Events table (Table 15)].

### 5.2.3. FAU\_GEN.2 – User Identity Association

**FAU\_GEN.2.1** For audit events resulting from actions of identified users, the TSF shall be able to associate each auditable event with the identity of the user that caused the event.

### 5.2.4. FAU\_STG\_EXT.1 – Protected Audit Event Storage

**FAU\_STG\_EXT.1.1** The TSF shall be able to transmit the generated audit data to an external IT entity using a trusted channel according to FTP\_ITC.1.

**FAU\_STG\_EXT.1.2** The TSF shall be able to store generated audit data on the TOE itself. In addition [

- The TOE shall consist of a single standalone component that stores audit data locally].

**FAU\_STG\_EXT.1.3** The TSF shall [overwrite previous audit records according to the following rule: [oldest audit records are overwritten]] when the local storage space for audit data is full.

## 5.3. Class: Cryptographic Support (FCS)

### 5.3.1. FCS\_CKM.1 – Cryptographic Key Generation (Refinement)

**FCS\_CKM.1.1** The TSF shall generate **asymmetric** cryptographic keys in accordance with a specified cryptographic key generation algorithm: [

- RSA schemes using cryptographic key sizes of 2048-bit or greater that meet the following: FIPS PUB 186-4, “Digital Signature Standard (DSS)”, Appendix B.3;
- ECC schemes using ‘NIST curves’ [P-256, P-384, P-521] that meet the following: FIPS PUB 186-4, “Digital Signature Standard (DSS)”, Appendix B.4

] and specified cryptographic key sizes [assignment: *cryptographic key sizes*] that meet the following: [assignment: *list of standards*].

### 5.3.2. FCS\_CKM.2 – Cryptographic Key Establishment (Refinement)

**FCS\_CKM.2.1** The TSF shall **perform** cryptographic **key establishment** in accordance with a specified cryptographic key **establishment** method: [

- Elliptic curve-based key establishment schemes that meet the following: NIST Special Publication 800-56A Revision 3, “Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography”

] that meets the following: ~~[assignment: list of standards]~~.

### 5.3.3. FCS\_CKM.4 – Cryptographic Key Destruction

**FCS\_CKM.4.1** The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method

- *For plaintext keys in volatile storage, the destruction shall be executed by a [single overwrite consisting of [zeroes, a new value of the key]];*
- *For plaintext keys in non-volatile storage, the destruction shall be executed by the invocation of an interface provided by a part of the TSF that [
 
  - logically addresses the storage location of the key and performs a [single-pass] overwrite consisting of [zeroes, a new value of the key]];*

that meets the following: *No Standard.*

### 5.3.4. FCS\_COP.1/DataEncryption – Cryptographic Operation (AES Data Encryption/Decryption)

**FCS\_COP.1.1/DataEncryption** The TSF shall perform *encryption/decryption* in accordance with a specified cryptographic algorithm *AES used in [CBC, GCM] mode* and cryptographic key sizes [128 bits, 256 bits] that meet the following: *AES as specified in ISO 18033-3, [CBC as specified in ISO 10116, GCM as specified in ISO 19772]*.

### 5.3.5. FCS\_COP.1/MACSEC – Cryptographic Operation (MACsec AES Data Encryption/Decryption)

**FCS\_COP.1.1/MACSEC** The TSF shall perform *[encryption and decryption]* in accordance with a specified cryptographic algorithm [*AES used in AES Key Wrap, GCM*] and cryptographic key sizes [128, 256] bits that meets the following: [*AES as specified in ISO 18033-3, AES Key Wrap as specified in NIST SP 800-38F, GCM as specified in ISO 19772*].

***Application Note:*** *The selection of 128 and 256 bit key sizes applies to AES-GCM. For AES Key Wrap, only the selection of 128-bit key size applies.*

### 5.3.6. FCS\_COP.1/SigGen – Cryptographic Operation (Signature Generation and Verification)

**FCS\_COP.1.1/SigGen** The TSF shall perform *cryptographic signature services (generation and verification)* in accordance with a specified cryptographic algorithm

[

- RSA Digital Signature Algorithm and cryptographic key sizes (modulus) [2048 bits, 3072 bits],

]

that meet the following:

[

- For RSA schemes: FIPS PUB 186-4, “Digital Signature Standard (DSS)”, Section 5.5, using PKCS #1 v2.1 Signature Schemes RSASSA-PSS and/or RSASSA-PKCS1v1\_5; ISO/IEC 9796-2, Digital signature scheme 2 or Digital Signature scheme 3,

].

### 5.3.7. FCS\_COP.1/Hash – Cryptographic Operation (Hash Algorithm)

**FCS\_COP.1.1/Hash** The TSF shall perform *cryptographic hashing services* in accordance with a specified cryptographic algorithm [SHA-256, SHA-384, SHA-512] and cryptographic key sizes [~~assignment: cryptographic key sizes~~] and **message digest sizes [256, 384, 512] bits** that meet the following: *ISO/IEC 10118-3:2004*.

### 5.3.8. FCS\_COP.1/KeyedHash – Cryptographic Operation (Keyed Hash Algorithm)

**FCS\_COP.1.1/KeyedHash** The TSF shall perform *keyed-hash message authentication* in accordance with a specified cryptographic algorithm [HMAC-SHA-256] and cryptographic key sizes [256] and **message digest sizes [256] bits** that meet the following: *ISO/IEC 9797-2:2011, Section 7 “MAC Algorithm 2”*.

### 5.3.9. FCS\_COP.1/CMAC – Cryptographic Operation (AES-CMAC Keyed Hash Algorithm)

**FCS\_COP.1.1/CMAC** The TSF shall perform [*keyed-hash message authentication*] in accordance with a specified cryptographic algorithm [AES-CMAC] and cryptographic key sizes [128, 256] **bits and message digest size of 128 bits** that meets the following: [*NIST SP 800-38B*].

### 5.3.10. FCS\_RBG\_EXT.1 – Random Bit Generation

**FCS\_RBG\_EXT.1.1** The TSF shall perform all deterministic random bit generation services in accordance with ISO/IEC 18031:2011 using [CTR\_DRBG (AES)].

**FCS\_RBG\_EXT.1.2** The deterministic RBG shall be seeded by at least one entropy source that accumulates entropy from [[1] platform-based noise source] with a minimum of [256 bits] of entropy at least equal to the greatest security strength, according to ISO/IEC 18031:2011 Table C.1 “Security Strength Table for Hash Functions”, of the keys and hashes that it will generate.

### 5.3.11. FCS\_MACSEC\_EXT.1 – MACsec

**FCS\_MACSEC\_EXT.1.1** The TSF shall implement MACsec in accordance with IEEE Standard 802.1AE-2018.

**FCS\_MACSEC\_EXT.1.2** The TSF shall derive a Secure Channel Identifier (SCI) from a peer’s MAC address and port to uniquely identify the originator of an MPDU.

**FCS\_MACSEC\_EXT.1.3** The TSF shall reject any MPDUs during a given session that contain an SCI other than the one used to establish that session.

**FCS\_MACSEC\_EXT.1.4** The TSF shall permit only EAPOL (Port Access Entity (PAE) EtherType 88-8E), MACsec frames (EtherType 88-E5), and MAC control frames (EtherType is 88-08) and shall discard others.

### 5.3.12. FCS\_MACSEC\_EXT.2 – MACsec Integrity and Confidentiality

**FCS\_MACSEC\_EXT.2.1** The TOE shall implement MACsec with support for integrity protection with a confidentiality offset of [0, 30, 50].

**FCS\_MACSEC\_EXT.2.2** The TSF shall provide assurance of the integrity of protocol data units (MPDUs) using an Integrity Check Value (ICV) derived with the SAK.

**FCS\_MACSEC\_EXT.2.3** The TSF shall provide the ability to derive an Integrity Check Value Key (ICK) from a Connectivity Association Key (CAK) using a KDF.

### 5.3.13. FCS\_MACSEC\_EXT.3 – MACsec Randomness

**FCS\_MACSEC\_EXT.3.1** The TSF shall generate unique Secure Association Keys (SAKs) using [key derivation from Connectivity Association Key (CAK) per section 9.8.1 of IEEE 802.1X-2010] such that the likelihood of a repeating SAK is no less than 1 in 2 to the power of the size of the generated key.

**FCS\_MACSEC\_EXT.3.2** The TSF shall generate unique nonces for the derivation of SAKs using the TOE's random bit generator as specified by FCS\_RBG\_EXT.1.

### 5.3.14. FCS\_MACSEC\_EXT.4 – MACsec Key Usage

**FCS\_MACSEC\_EXT.4.1** The TSF shall support peer authentication using pre-shared keys (PSKs) [no other method].

**FCS\_MACSEC\_EXT.4.2** The TSF shall distribute SAKs between MACsec peers using AES key wrap as specified in FCS\_COP.1/MACSEC.

**FCS\_MACSEC\_EXT.4.3** The TSF shall support specifying a lifetime for CAKs.

**FCS\_MACSEC\_EXT.4.4** The TSF shall associate Connectivity Association Key Names (CKNs) with SAKs that are defined by the KDF using the CAK as input data (per IEEE 802.1X-2010, Section 9.8.1).

**FCS\_MACSEC\_EXT.4.5** The TSF shall associate CKNs with CAKs. The length of the CKN shall be an integer number of octets, between 1 and 32 (inclusive).

### 5.3.15. FCS\_MKA\_EXT.1 – MACsec Key Agreement

**FCS\_MKA\_EXT.1.1** The TSF shall implement Key Agreement Protocol (MKA) in accordance with IEEE 802.1X-2010 and 802.1Xbx-2014.

**FCS\_MKA\_EXT.1.2** The TSF shall provide assurance of the integrity of MKA protocol data units (MKPDUs) using an Integrity Check Value (ICV) derived from an Integrity Check Value Key (ICK).

**FCS\_MKA\_EXT.1.3** The TSF shall provide the ability to derive an Integrity Check Value Key (ICK) from a CAK using a KDF.

**FCS\_MKA\_EXT.1.4** The TSF shall enforce an MKA Lifetime Timeout limit of 6.0 seconds and [MKA Bounded Hello Timeout limit of 0.5 seconds].

**FCS\_MKA\_EXT.1.5** The key server shall refresh a SAK when it expires. The key server shall distribute a SAK by [

- pairwise CAKS that are PSKs

].

**FCS\_MKA\_EXT.1.6** The key server shall distribute a fresh SAK whenever a member is added to or removed from the live membership of the CA.

**FCS\_MKA\_EXT.1.7** The TSF shall validate MKPDUs according to IEEE 802.1X-2010 Section 11.11.2. In particular, the TSF shall discard without further processing any MKPDUs to which any of the following conditions apply:

- a. The destination address of the MKPDU was an individual address
- b. The MKPDU is less than 32 octets long
- c. The MKPDU comprises fewer octets than indicated by the Basic Parameter Set body length, as encoded in bits 4 through 1 of octet 3 and bits 8 through 1 of octet 4, plus 16 octets of ICV
- d. The CAK Name is not recognized

If an MKPDU passes these tests, then the TSF will begin processing it as follows:

- a. If the Algorithm Agility parameter identifies an algorithm that has been implemented by the receiver, the ICV shall be verified as specified in IEEE 802.1X-2010 Section 9.4.1.
- b. If the Algorithm Agility parameter is unrecognized or not implemented by the receiver, its value can be recorded for diagnosis but the received MKPDU shall be discarded without further processing.

Each received MKPDU that is validated as specified in this clause and verified as specified in IEEE 802.1X-2010 Section 9.4.1 shall be decoded as specified in IEEE 802.1X-2010 Section 11.11.4.

### 5.3.16. FCS\_SSHS\_EXT.1 – SSH Server Protocol

**FCS\_SSHS\_EXT.1.1** The TSF shall implement the SSH protocol that complies with: RFCs 4251, 4252, 4253, 4254, [5656, 6668, 8308 section 3.1, 8332].

**FCS\_SSHS\_EXT.1.2** The TSF shall ensure that the SSH protocol implementation supports the following user authentication methods as described in RFC 4252: public key-based, [password-based].

**FCS\_SSHS\_EXT.1.3** The TSF shall ensure that, as described in RFC 4253, packets greater than [65,806] bytes in an SSH transport connection are dropped.

**FCS\_SSHS\_EXT.1.4** The TSF shall ensure that the SSH transport implementation uses the following encryption algorithms and rejects all other encryption algorithms: [aes128-cbc, aes256-cbc, aes128-gcm@openssh.com, aes256-gcm@openssh.com].

**FCS\_SSHS\_EXT.1.5** The TSF shall ensure that the SSH public-key based authentication implementation uses [rsa-sha2-256, rsa-sha2-512] as its public key algorithm(s) and rejects all other public key algorithms.

**FCS\_SSHS\_EXT.1.6** The TSF shall ensure that the SSH transport implementation uses hmac-sha2-256, implicit] as its MAC algorithm(s) and rejects all other MAC algorithm(s).

**FCS\_SSHS\_EXT.1.7** The TSF shall ensure that [ecdh-sha2-nistp256] and [ecdh-sha2-nistp384] are the only allowed key exchange methods used for the SSH protocol.

**FCS\_SSHS\_EXT.1.8** The TSF shall ensure that within SSH connections, the same session keys are used for a threshold of no longer than one hour, and each encryption key is used to protect no more than one gigabyte of data. After any of the thresholds are reached, a rekey needs to be performed.

### 5.3.17. FCS\_TLSC\_EXT.1 TLS Client Protocol Without Mutual Authentication

**FCS\_TLSC\_EXT.1.1** The TSF shall implement [TLS 1.2 (RFC 5246)] and reject all other TLS and SSL versions. The TLS implementation will support the following ciphersuites [

- TLS\_ECDHE\_RSA\_WITH\_AES\_256\_GCM\_SHA384 as defined in RFC 5289
- TLS\_ECDHE\_RSA\_WITH\_AES\_128\_GCM\_SHA256 as defined in RFC 5289

]

and no other ciphersuites.

**FCS\_TLSC\_EXT.1.2** The TSF shall verify that the presented identifier matches [the reference identifier per RFC 6125 section 6, IPv4 address in SAN] and no other attribute types.

**FCS\_TLSC\_EXT.1.3** When establishing a trusted channel, by default the TSF shall not establish a trusted channel if the server certificate is invalid. The TSF shall also [

- Not implement any administrator override mechanism

].

**FCS\_TLSC\_EXT.1.4** The TSF shall [present the Supported Elliptic Curves/Supported Groups Extension with the following curves/groups: [secp256r1, secp384r1, secp521r1] and no other curves/groups] in the Client Hello.

## 5.4. Class: Identification and Authentication (FIA)

### 5.4.1. FIA\_AFL.1 – Authentication Failure Management

**FIA\_AFL.1.1** The TSF shall detect when an Administrator configurable positive integer within [1-25] unsuccessful authentication attempts occur related to *Administrators attempting to authenticate remotely using a password*.

**FIA\_AFL.1.2** When the defined number of unsuccessful authentication attempts has been met, the TSF shall [prevent the offending Administrator from successfully establishing remote session using any authentication method that involves a password until [unblocking action] is taken by an Administrator; prevent the offending Administrator from successfully establishing remote session using any authentication method that involves a password until an Administrator defined time period has elapsed].

### 5.4.2. FIA\_PMG\_EXT.1 – Password Management

**FIA\_PMG\_EXT.1.1** The TSF shall provide the following password management capabilities for administrative passwords:

1. Passwords shall be able to be composed of any combination of upper and lower case letters, numbers, and the following special characters: ["!", "@", "#", "\$", "%", "^", "&", "\*", "(", ")"] *[Additional Special Characters listed in Table 16]*;

**Table 16. 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

- Minimum password length shall be configurable to between [1] and [127] characters.

### 5.4.3. FIA\_PSK\_EXT.1 – Pre-Shared Key Composition

**FIA\_PSK\_EXT.1.1** The TSF shall use PSKs for MKA as defined by IEEE 802.1X-2010, [no other protocols].

**FIA\_PSK\_EXT.1.2** The TSF shall be able to [accept] bit-based pre-shared keys.

### 5.4.4. FIA\_UIA\_EXT.1 – User Identification and Authentication

**FIA\_UIA\_EXT.1.1** The TSF shall allow the following actions prior to requiring the non-TOE entity to initiate the identification and authentication process:

- Display the warning banner in accordance with FTA\_TAB.1;
- [no other actions]

**FIA\_UIA\_EXT.1.2** The TSF shall require each administrative user to be successfully identified and authenticated before allowing any other TSF-mediated action on behalf of that administrative user.

### 5.4.5. FIA\_UAU\_EXT.2 – Password-based Authentication Mechanism

**FIA\_UAU\_EXT.2.1** The TSF shall provide a local [password-based, SSH public key-based] authentication mechanism to perform local administrative user authentication.

### 5.4.6. FIA\_UAU.7 – Protected Authentication Feedback

**FIA\_UAU.7.1** The TSF shall provide only *obscured feedback* to the administrative user while the authentication is in progress **at the local console**.

### 5.4.7. FIA\_X509\_EXT.1/Rev – X.509 Certificate Validation

**FIA\_X509\_EXT.1.1/Rev** The TSF shall validate certificates in accordance with the following rules:

- RFC 5280 certificate validation and certificate path validation **supporting a minimum path length of three certificates**.
- The certificate path must terminate with a trusted CA certificate designated as a trust anchor.
- The TSF shall validate a certification path by ensuring that all CA certificates in the certification path contain the basicConstraints extension with the CA flag set to TRUE.
- The TSF shall validate the revocation status of the certificate using [a Certificate Revocation List (CRL) as specified in RFC [5280 Section 6.3](#)].
- The TSF shall validate the extendedKeyUsage field according to the following rules:

- Certificates used for trusted updates and executable code integrity verification shall have the Code Signing purpose (id-kp 3 with OID 1.3.6.1.5.5.7.3.3) in the extendedKeyUsage field.
- Server certificates presented for TLS shall have the Server Authentication purpose (id-kp 1 with OID 1.3.6.1.5.5.7.3.1) in the extendedKeyUsage field.
- Client certificates presented for TLS shall have the Client Authentication purpose (id-kp 2 with OID 1.3.6.1.5.5.7.3.2) in the extendedKeyUsage field.
- OCSP certificates presented for OCSP responses shall have the OCSP Signing purpose (id-kp 9 with OID 1.3.6.1.5.5.7.3.9) in the extendedKeyUsage field.

**FIA\_X509\_EXT.1.2/Rev** The TSF shall only treat a certificate as a CA certificate if the basicConstraints extension is present and the CA flag is set to TRUE.

#### 5.4.8. FIA\_X509\_EXT.2 – X.509 Certificate Authentication

**FIA\_X509\_EXT.2.1** The TSF shall use X.509v3 certificates as defined by RFC 5280 to support authentication for [TLS], and [no additional uses].

**FIA\_X509\_EXT.2.2** When the TSF cannot establish a connection to determine the validity of a certificate, the TSF shall [not accept the certificate].

### 5.5. Class: Security Management (FMT)

#### 5.5.1. FMT\_MOF.1/ManualUpdate – Management of Security Functions Behavior

**FMT\_MOF.1.1/ManualUpdate** The TSF shall restrict the ability to enable the functions to perform manual update to Security Administrators.

#### 5.5.2. FMT\_MTD.1/CoreData – Management of TSF Data

**FMT\_MTD.1.1/CoreData** The TSF shall restrict the ability to manage the TSF data to Security Administrators.

#### 5.5.3. FMT\_MTD.1/CryptoKeys – Management of TSF Data

**FMT\_MTD.1.1/CryptoKeys** The TSF shall restrict the ability to manage the cryptographic keys to Security Administrators.

#### 5.5.4. FMT\_SMF.1 – Specification of Management Functions

**FMT\_SMF.1.1** The TSF shall be capable of performing the following management functions:

- *Ability to administer the TOE locally and remotely;*
- *Ability to configure the access banner;*
- *Ability to configure the session inactivity time before session termination or locking;*
- *Ability to update the TOE, and to verify the updates using [digital signature] capability prior to installing those updates;*
- *Ability to configure the authentication failure parameters for FIA\_AFL.1;*

[

- Ability to modify the behaviour of the transmission of audit data to an external IT entity;
- Ability to manage the cryptographic keys;



- Ability to configure the cryptographic functionality;
  - Ability to configure thresholds for SSH rekeying;
  - Ability to re-enable an Administrator account;
  - Ability to set the time which is used for time-stamps;
  - Ability to configure the reference identifier for the peer;
  - Ability to manage the TOE's trust store and designate X509.v3 certificates as trust anchors;
  - Ability to import X.509v3 certificates to the TOE's trust store;
  - Ability to manage the trusted public keys database
- ]

### 5.5.5. FMT\_SMF.1/MACSEC – Specification of Management Functions (MACsec)

**FMT\_SMF.1.1/MACSEC** The TSF shall be capable of performing the following management functions **related to MACsec functionality**: *[Ability of a Security Administrator to:*

- *Manage a PSK-based CAK and install it in the device*
- *Manage the key server to create, delete, and activate MKA participants [as specified in IEEE 802.1X-2020, Sections 9.13 and 9.16 (cf. MIB object ieee8021XKayMkaParticipant Entry) and section 12.2 (cf. function createMKA())]*
- *Specify the lifetime of a CAK*
- *Enable, disable, or delete a PSK-based CAK using [CLI management commands]*

[

- *No other MACsec management functions*

]].

### 5.5.6. FMT\_SMR.2 – Restrictions on Security Roles

**FMT\_SMR.2.1** The TSF shall maintain the roles:

- *Security Administrator.*

**FMT\_SMR.2.2** The TSF shall be able to associate users with roles.

**FMT\_SMR.2.3** The TSF shall ensure that the conditions

- *The Security Administrator role shall be able to administer the TOE locally;*
  - *The Security Administrator role shall be able to administer the TOE remotely*
- are satisfied.

## 5.6. Class: Protection of the TSF (FPT)

### 5.6.1. FPT\_CAK\_EXT.1 Protection of CAK Data

**FPT\_CAK\_EXT.1.1** The TSF shall prevent reading of CAK values by administrators.

### 5.6.2. FPT\_FLS.1 Failure with Preservation of Secure State

**FPT\_FLS.1.1** The TSF shall **fail-secure** when **any of** the following types of failures occur: [failure of the power-on self-tests, failure of integrity check of the TSF executable image, failure of noise source health tests].

### 5.6.3. FPT\_RPL.1 Replay Detection

**FPT\_RPL.1.1** The TSF shall detect replay for the following entities: [MPDUs, MKA frames].

**FPT\_RPL.1.2** The TSF shall perform [discarding of the replayed data, logging of the detected replay attempt] when replay is detected.

### 5.6.4. FPT\_RPL\_EXT.1 Replay Protection for XPN

**FPT\_RPL\_EXT.1.1** The TSF shall support extended packet numbering (XPN) as per IEEE 802.1AE-2018.

**FPT\_RPL\_EXT.1.2** The TSF shall support [GCM-AES-XPN-128, GCM-AES-XPN-256] as per IEEE 802.1AE-2018.

**Application Note:** *The FPT\_RPL\_EXT.1 requirement applies to the Catalyst 9600X series model. It does not apply to the 9400X series.*

### 5.6.5. FPT\_APW\_EXT.1 – Protection of Administrator Passwords

**FPT\_APW\_EXT.1.1** The TSF shall store administrative passwords in non-plaintext form.

**FPT\_APW\_EXT.1.2** The TSF shall prevent the reading of plaintext administrative passwords.

### 5.6.6. FPT\_SKP\_EXT.1 – Protection of TSF Data (for reading of all pre-shared, symmetric and private keys)

**FPT\_SKP\_EXT.1.1** The TSF shall prevent reading of all pre-shared keys, symmetric keys, and private keys.

### 5.6.7. FPT\_STM\_EXT.1 – Reliable Time Stamps

**FPT\_STM\_EXT.1.1** The TSF shall be able to provide reliable time stamps for its own use.

**FPT\_STM\_EXT.1.2** The TSF shall [allow the Security Administrator to set the time].

### 5.6.8. FPT\_TST\_EXT.1 – TSF Testing

**FPT\_TST\_EXT.1.1** The TSF shall run a suite of the following self-tests [during initial start-up (on power on), periodically during normal operation] to demonstrate the correct operation of the TSF: [

- *AES Known Answer Test*
- *HMAC Known Answer Test*
- *RNG/DRBG Known Answer Test*
- *SHA-256/384/512 Known Answer Test*
- *RSA Signature Known Answer Test (both signature/verification)*
- *Software Integrity Test*

].

### 5.6.9. FPT\_TUD\_EXT.1 – Trusted Update

**FPT\_TUD\_EXT.1.1** The TSF shall provide *Security Administrators* the ability to query the currently executing version of the TOE firmware/software and [the most recently installed version of the TOE firmware/software].

**FPT\_TUD\_EXT.1.2** The TSF shall provide *Security Administrators* the ability to manually initiate updates to TOE firmware/software and [no other update mechanism].

**FPT\_TUD\_EXT.1.3** The TSF shall provide means to authenticate firmware/software updates to the TOE using a [digital signature] prior to installing those updates.

## 5.7. Class: TOE Access (FTA)

### 5.7.1. FTA\_SSL\_EXT.1 – TSF-initiated Session Locking

**FTA\_SSL\_EXT.1.1** The TSF shall, for local interactive sessions, [terminate the session] after a Security Administrator-specified time period of inactivity.

### 5.7.2. FTA\_SSL.3 – TSF-initiated Termination

**FTA\_SSL.3.1** The TSF shall terminate a **remote** interactive session after a *Security Administrator-configurable time interval of session inactivity*.

### 5.7.3. FTA\_SSL.4 – User-initiated Termination

**FTA\_SSL.4.1** The TSF shall allow **Administrator**-initiated termination of the **Administrator**'s own interactive session.

### 5.7.4. FTA\_TAB.1 – Default TOE Access Banners

**FTA\_TAB.1.1** Before establishing an **administrative user** session the TSF shall display a **Security Administrator-specified advisory notice and consent** warning message regarding use of the TOE.

## 5.8. Class: Trusted Path/Channels (FTP)

### 5.8.1. FTP\_ITC.1 – Inter-TSF Trusted Channel

**FTP\_ITC.1.1** The TSF shall **be capable of using [TLS] to** provide a trusted communication channel between itself and **authorized IT entities supporting the following capabilities: audit server, [no other capabilities]** that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from **disclosure and detection of modification of the channel data**.

**FTP\_ITC.1.2** The TSF shall permit **the TSF or the authorized IT entities** to initiate communication via the trusted channel.

**FTP\_ITC.1.3** The TSF shall initiate communication via the trusted channel for [

- *Syslog server over TLS*

]

### 5.8.2. FTP\_ITC.1/MACSEC – Inter-TSF Trusted Channel (MACsec Communications)

**FTP\_ITC.1.1/MACSEC** The TSF shall provide a communication channel between itself and a MACsec peer that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.

**FTP\_ITC.1.2/MACSEC** The TSF shall permit [the TSF, another trusted IT product] to initiate communication via the trusted channel.

**FTP\_ITC.1.3/MACSEC** The TSF shall initiate communication via the trusted channel for *[communications with MACsec peers that require the use of MACsec]*.

### FTP\_TRP.1/Admin – Trusted Path

**FTP\_TRP.1.1/Admin** The TSF shall **be capable of using [SSH]** to provide a communication path between itself and **authorized remote Administrators** that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from **disclosure and provides detection of modification of the channel data**.

**FTP\_TRP.1.2/Admin** The TSF shall permit **remote Administrators** to initiate communication via the trusted path.

**FTP\_TRP.1.3/Admin** The TSF shall require the use of the trusted path for *initial Administrator authentication and all remote administration actions*.

## 5.9. TOE SFR Dependencies Rationale

The Security Functional Requirements included in the ST represent all mandatory, optional, and selection-based SFRs specified in [NDcPP] and [MOD\_MACSEC] against which exact compliance is claimed.

All dependency rationale in the ST are considered to be identical to those that are defined in the claimed PP.

## 5.10. TOE SFR Dependencies Rationale

The TOE assurance requirements for this ST are taken directly from the NDcPP which are derived from [CC\_PART3]. The assurance requirements are summarized in the table below.

**Table 17. Assurance Requirements**

Assurance Class	Components	Description
Security Target (ASE)	ASE_CCL.1	Conformance claims
	ASE_ECD.1	Extended components definition
	ASE_INT.1	ST introduction
	ASE_OBJ.1	Security objectives for the operational environment
	ASE_REQ.1	Stated security requirements
	ASE_SPD.1	Security Problem Definition
	ASE_TSS.1	TOE summary specification
Development (ADV)	ADV_FSP.1	Basic functional specification
Guidance Documents (AGD)	AGD_OPE.1	Operational user guidance
	AGD_PRE.1	Preparative procedures
Life Cycle Support (ALC)	ALC_CMC.1	Labeling of the TOE
	ALC_CMS.1	TOE CM coverage
Tests (ATE)	ATE_IND.1	Independent testing – conformance
Vulnerability Assessment (AVA)	AVA_VAN.1	Vulnerability survey

## 5.11. TOE SFR Dependencies Rationale

[NDcPP] and [MOD\_MACSEC] contain all the requirements claimed in this Security Target. As such the dependencies are not applicable since the PPs themselves have been approved.

## 5.12. Security Assurance Requirements Rationale

The Security Assurance Requirements (SARs) in this Security Target represent the SARs identified in the [NDcPP] and [MOD\_MACSEC]. As such, the [NDcPP] and [MOD\_MACSEC] SAR rationale is deemed acceptable since the PPs themselves have been approved.

## 5.13. Assurance Measures

The TOE satisfies the identified assurance requirements. The table below identifies the Assurance Measures applied by Cisco to satisfy the assurance requirements.

**Table 18. Assurance Measures**

Assurance Component	Rationale
ASE_INT.1 ASE_CCL.1 ASE_OBJ.1 ASE_ECD.1 ASE_REQ.1 ASE_SPD.1 ASE_TSS.1	Cisco provided this Security Target document.
ADV_FSP.1	No additional "functional specification" documentation was provided by Cisco to satisfy the Evaluation Activities.
AGD_OPE.1 AGD_PRE.1	Cisco will provide the guidance documents with the ST.
ALC_CMC.1 ALC_CMS.1	Cisco will identify the TOE such that it can be distinguished from other products or versions from the Cisco and can be easily specified when being procured by an end user.
ATE_IND.1	Cisco will provide the TOE for testing.
AVA_VAN.1	Cisco will provide the TOE for Vulnerability Analysis.

## 6. TOE Summary Specification

The table below identifies and describes how the Security Functional Requirements identified above are met by the TOE.

**Table 19. TSS Rationale**

TOE SFRs	How the SFR is Met													
FAU_GEN.1 FAU_GEN.1/MACSEC	<p>The TOE generates an audit record whenever an audited event occurs. The types of events that cause audit records to be generated include start-up and shut-down of the audit mechanism cryptography related events, identification and authentication related events, and administrative events (the specific events and the contents of each audit record are listed in Tables 14 and 15 above.</p> <p>Each of the events is specified in the audit record is in enough detail to identify the user for which the event is associated, when the event occurred, where the event occurred, the outcome of the event, and the type of event that occurred such as generating keys, including the key identifier. Additionally, the start-up and shut-down of the audit functionality is audited.</p> <p>The audit trail consists of the individual audit records; one audit record for each event that occurred. The audit record can contain up to 80 characters and a percent sign (%), which follows the time-stamp information. As noted above, the information includes at least all the required information. Additional information can be configured.</p>													
FAU_GEN.2	<p>The TOE shall ensure that each auditable event is associated with the user that triggered the event and as a result, they are traceable to a specific user. For example, a human user, user identity or related session ID would be included in the audit record. For an IT entity or device, the IP address, MAC address, host name, or other configured identification is presented.</p>													
FAU_STG_EXT.1	<p>The TOE is a standalone device configured to export syslog records to a specified, external syslog server in real-time. The TOE protects communications with an external syslog server using TLS. If the TLS connection fails, the TOE will store audit records on the TOE when it discovers it can no longer communicate with its configured syslog server. When the connection is restored, the TOE will transmit the buffer contents to the syslog server.</p> <p>For audit records stored internally to the TOE the audit records are stored in a circular log file where the TOE overwrites the oldest audit records when the audit trail becomes full. The size of the logging files on the TOE is configurable by the Administrator with the minimum value being 4096 (default) to 2,147,483,647 bytes of available disk space. Refer to the Cisco Catalyst 9400X/9600X Series Switches 17.12 CC Configuration Guide for command description and usage information.</p> <p>Only Authorized Administrators can clear the local logs, and local audit records are stored in a directory that does not allow Administrators to modify the contents.</p>													
FCS_CKM.1 FCS_CKM.2	<p>The following table describes the key generation algorithms the TOE implements to generate asymmetric keys used for <b>device authentication</b>:</p> <table border="1" data-bbox="436 1503 1273 1818"> <thead> <tr> <th data-bbox="436 1503 542 1562">Scheme</th> <th data-bbox="542 1503 732 1562">Standard</th> <th data-bbox="732 1503 867 1562">Key Size/ NIST Curve</th> <th data-bbox="867 1503 1094 1562">SFR</th> <th data-bbox="1094 1503 1273 1562">Service</th> </tr> </thead> <tbody> <tr> <td data-bbox="436 1562 542 1818" rowspan="2">RSA</td> <td data-bbox="542 1562 732 1818" rowspan="2">FIPS PUB 186-4</td> <td data-bbox="732 1562 867 1650">2048</td> <td data-bbox="867 1562 1094 1650">FCS_SSHS_EXT.1</td> <td data-bbox="1094 1562 1273 1650">SSH Remote Administration</td> </tr> <tr> <td data-bbox="732 1650 867 1818">3072</td> <td data-bbox="867 1650 1094 1818">FCS_TLSC_EXT.1</td> <td data-bbox="1094 1650 1273 1818">Transmit generated audit data to an external IT entity</td> </tr> </tbody> </table>	Scheme	Standard	Key Size/ NIST Curve	SFR	Service	RSA	FIPS PUB 186-4	2048	FCS_SSHS_EXT.1	SSH Remote Administration	3072	FCS_TLSC_EXT.1	Transmit generated audit data to an external IT entity
Scheme	Standard	Key Size/ NIST Curve	SFR	Service										
RSA	FIPS PUB 186-4	2048	FCS_SSHS_EXT.1	SSH Remote Administration										
		3072	FCS_TLSC_EXT.1	Transmit generated audit data to an external IT entity										

TOE SFRs	How the SFR is Met																									
	<p>The following table shows the key generation algorithms the TOE implements to generate asymmetric keys used for <b>key establishment</b>:</p> <table border="1" data-bbox="436 317 1265 758"> <thead> <tr> <th>Scheme</th> <th>Standard</th> <th>Key Size/ NIST Curve</th> <th>SFR</th> <th>Service</th> </tr> </thead> <tbody> <tr> <td>ECC</td> <td>FIPS PUB 186-4</td> <td>P-256 P-384 P-521</td> <td>FCS_TLSC_EXT.1</td> <td>Transmit generated audit data to an external IT entity</td> </tr> <tr> <td>ECC</td> <td>FIPS PUB 186-4</td> <td>P-256 P-384</td> <td>FCS_SSHS_EXT.1</td> <td>SSH Remote Administration</td> </tr> </tbody> </table> <p>The following table shows the methods the TOE implements for <b>key establishment</b>:</p> <table border="1" data-bbox="436 846 1265 1146"> <thead> <tr> <th>Scheme</th> <th>Standard</th> <th>SFR</th> <th>Service</th> </tr> </thead> <tbody> <tr> <td rowspan="2">EC-DH</td> <td rowspan="2">NIST SP 800-56A Revision 3</td> <td>FCS_TLSC_EXT.1</td> <td>Transmit generated audit data to an external IT entity</td> </tr> <tr> <td>FCS_SSHS_EXT.1</td> <td>SSH Remote Administration</td> </tr> </tbody> </table>	Scheme	Standard	Key Size/ NIST Curve	SFR	Service	ECC	FIPS PUB 186-4	P-256 P-384 P-521	FCS_TLSC_EXT.1	Transmit generated audit data to an external IT entity	ECC	FIPS PUB 186-4	P-256 P-384	FCS_SSHS_EXT.1	SSH Remote Administration	Scheme	Standard	SFR	Service	EC-DH	NIST SP 800-56A Revision 3	FCS_TLSC_EXT.1	Transmit generated audit data to an external IT entity	FCS_SSHS_EXT.1	SSH Remote Administration
Scheme	Standard	Key Size/ NIST Curve	SFR	Service																						
ECC	FIPS PUB 186-4	P-256 P-384 P-521	FCS_TLSC_EXT.1	Transmit generated audit data to an external IT entity																						
ECC	FIPS PUB 186-4	P-256 P-384	FCS_SSHS_EXT.1	SSH Remote Administration																						
Scheme	Standard	SFR	Service																							
EC-DH	NIST SP 800-56A Revision 3	FCS_TLSC_EXT.1	Transmit generated audit data to an external IT entity																							
		FCS_SSHS_EXT.1	SSH Remote Administration																							
FCS_CKM.4	The TOE meets all requirements specified in FIPS 140-2 for destruction of keys and Critical Security Parameters (CSPs) when no longer required for use. See section 6.1 below for additional details on key zeroization.																									
FCS_COP.1/DataEncryption	The TOE provides symmetric encryption and decryption capabilities using AES in CBC mode (SSH only) and GCM mode (128 and 256 bits) as described in ISO/IEC 18033-3, ISO/IEC 10116, and ISO/IEC 19772. AES is implemented in the SSH and TLS protocols. Refer to Table 21 above for the FIPS validated algorithm certificate numbers.																									
FCS_COP.1/SigGen	The TOE provides cryptographic signature services using a RSA Digital Signature Algorithm with key size of 2048 or 3072 as specified in FIPS PUB 186-4. Refer to Table 21 above for the FIPS validated algorithm certificate numbers.																									
FCS_COP.1/Hash FCS_COP.1/KeyedHash	<p>The TOE provides cryptographic hashing services using SHA-256, SHA-384, and SHA-512 as specified in ISO/IEC 10118-3:2004 (with key sizes and message digest sizes of 256, 384, and 512 bits respectively).</p> <p>The TOE provides keyed-hashing message authentication services using HMAC-SHA-256 (SSH only) that operates on 512-bit blocks with key size and message digest size of 256 bits as specified in ISO/IEC 9797-2:2011, Section 7 “MAC Algorithm 2”.</p> <p>SHA-512 hashing is used for verification of software image integrity.</p> <p>Refer to Table 21 above for the FIPS validated algorithm certificate numbers.</p>																									

TOE SFRs	How the SFR is Met
FCS_COP.1/CMAC FCS_COP.1/MACSEC	<p>The TSF implements keyed-hash message authentication in accordance with AES-CMAC and cryptographic key sizes 128 and 256 bits with message digest size of 128 bits, block size of 128 bits, and MAC length of 128 bits which meets NIST SP 800-38B.</p> <p>The TSF implements symmetric encryption and decryption capabilities using AES GCM mode (128 and 256 bits) as described in ISO/IEC 18033-3 and ISO/IEC 19772. The TSF implements AES Key Wrap with a key size of 128 bits as specified in NIST SP800-38F.</p> <p>AES is implemented in the MACsec protocol.</p> <p>Refer to Table 21 above for the FIPS validated algorithm certificate numbers.</p>
FCS_RBG_EXT.1	<p>All cryptography in the TOE is implemented using the IOS Common Cryptographic Module (IC2M) and CiscoSSL FOM cryptographic modules. Each cryptographic module implements a NIST-approved AES-CTR DRBG, as specified in ISO/IEC 18031:2011 seeded by an entropy source that accumulates entropy from a TSF-platform-based noise source. CiscoSSL FOM uses the Cisco TRNG Core (CTC) entropy source. IC2M uses a CPU Jitter Entropy (JENT) entropy source.</p> <p>Each DRBG is seeded with a minimum of 256 bits of entropy, which is at least equal to the greatest security strength of the keys and hashes that it will generate.</p>
FCS_MACSEC_EXT.1	<p>The TOE implements MACsec in compliance with Institute of Electrical and Electronics Engineers (IEEE) Standard 802.1AE-2018. The MACsec connections maintain confidentiality of transmitted data and takes measures against frames transmitted or modified by unauthorized devices.</p> <p>The Secure Channel Identifier (SCI) is composed of a globally unique 48-bit Message Authentication Code (MAC) Address and the Secure System Address (port). The SCI is part of the SecTAG if the Secure Channel (SC) bit is set and will be at the end of the tag. Any MAC Protocol Data Units (MPDUs) during a given session that contain an SCI other than the one used to establish that session is rejected.</p> <p>Only Extensible Authentication Protocol over LAN (EAPOL) (Physical Address Extension (PAE) EtherType 88-8E), MACsec frames (EtherType 88-E5), and MAC control frames (EtherType 88-08) are permitted. All others are rejected.</p>
FCS_MACSEC_EXT.2	<p>The TOE implements the MACsec requirement for integrity protection with the confidentiality offsets of 0, 30 and 50 using the 'mka-policy confidentiality-offset' command.</p> <p>An offset value of 0 does not offset the encryption and offset values of 30 and 50 offset the encryption by 30 and 50 characters respectively.</p> <p>An Integrity Check Value (ICV) of 16-bytes derived with the SAK is used to provide assurance of the integrity of MPDUs.</p> <p>The TOE derives the ICK from a CAK using KDF, using the SCI as the most significant bits of the Initialization Vector (IV) and the 32 least significant bits of the PN as the IV.</p>
FCS_MACSEC_EXT.3	<p>Each SAK is generated using the KDF specified in IEEE 802.1X-2010 section 6.2.1 using the following transform - KS-nonce = a nonce of the same size as the required SAK, obtained from a Random Number Generator (RNG) each time an SAK is generated.</p> <p>Each of the keys used by MKA is derived from the CAK.</p> <p>The key string is the CAK that is used for ICV validation by the MKA protocol. The CAK is not used directly but derives two further keys from the CAK using the AES cipher in CMAC mode.</p>



TOE SFRs	How the SFR is Met
	<p>The derived keys are tied to the identity of the CAK, and thus restricted to use with that particular CAK. These are the ICV Key (ICK) used to verify the integrity of MPDUs and to prove that the transmitter of the MKPDU possesses the CAK, and the Key Encrypting Key (KEK) used by the Key Server, elected by MKA, to transport a succession of SAKs, for use by MACsec, to the other member(s) of a CA.</p> <p>The key size is 32-bit hexadecimal in length for AES 128-bit CMAC mode encryption and 64-bit hexadecimal in length for AES 256-bit CMAC mode encryption.</p>
FCS_MACSEC_EXT.4	<p>MACsec peer authentication is achieved by only using pre-shared keys.</p> <p>The SAKs are distributed between these peers using AES Key Wrap. Prior to distribution of the SAKs between these peers, the TOE uses AES Key Wrap in accordance with AES as specified in ISO/IEC 18033-3, AES in CMAC mode as specified in NIST SP800-38B, and GCM as specified in ISO/IEC 19772.</p>
FCS_MKA_EXT.1	<p>The TOE implements the MKA Protocol in accordance with IEEE 802.1X-2010 and 802.1Xbx-2014.</p> <p>The data delay protection is enabled for MKA as a protection guard against an attack on the configuration protocols that MACsec is designed to protect by alternately delaying and delivering their MPDUs. The "Delay Protection" does not operate if MKA operation is suspended. An MKA Lifetime Timeout limit of 6.0 seconds and Hello Timeout limit of 2.0 seconds is enforced by the TOE.</p> <p>The TOE discards MACsec Key Agreement Protocol Data Units (MKPDUs) that do not satisfy the requirements listed under FCS_MKA_EXT.1.7. All valid MKPDUs that meet the requirements as defined under FCS_MKA_EXT.1.7 are decoded in a manner conformant to IEEE 802.1x-2010 Section 11.11.4.</p> <p>On successful peer authentication, a unique connectivity association is formed between the peers and a secure Connectivity Association Key Name (CKN) is exchanged. After the exchange, the MKA ICV is validated with a Connectivity Association Key (CAK), which is effectively a secret key. The TOE does not support group CAKs.</p> <p>For the Data Integrity Check, MACsec uses MKA to generate an ICV for the frame arriving on the port. If the generated ICV is the same as the ICV in the frame, then the frame is accepted; otherwise, it is dropped. The key string is the CAK that is used for ICV validation by the MKA protocol.</p>
FCS_SSHS_EXT.1	<p>The TSF implements SSHv2 conformant to RFCs 4251, 4252, 4253, 4254, 5656, 6668, 8308 section 3, and 8332 to provide a secure command line interface for remote administration. The TOE supports user public key and/or password based authentication.</p> <p>SSHv2 connections will be dropped if the TOE receives a packet larger than 65,806 bytes. Large packets are detected by the SSHv2 implementation and dropped internal to the SSH process.</p> <p>The TSF's SSH transport implementation supports the following encryption algorithms:</p> <ul style="list-style-type: none"> <li>■ aes128-cbc</li> <li>■ aes256-cbc</li> <li>■ aes128-gcm@openssh.com</li> <li>■ aes256-gcm@openssh.com</li> </ul> <p>All connection attempts from remote SSH clients requesting any other encryption algorithm is denied.</p> <p>The TSF's SSH transport implementation supports the following MAC algorithms when aes128-cbc or aes-256-cbc is used:</p> <ul style="list-style-type: none"> <li>■ hmac-sha2-256</li> </ul>

TOE SFRs	How the SFR is Met
	<p>When aes128-gcm@openssh.com or aes256-gcm@openssh.com is used as the encryption algorithm the MAC algorithm is implicit.</p> <p>All connection attempts from remote SSH clients requesting any other MAC algorithm is denied.</p> <p>The TSF's SSH transport implementation supports the following public-key algorithms for Hostkey authentication:</p> <ul style="list-style-type: none"> <li>■ rsa-sha2-256</li> <li>■ rsa-sha2-512</li> </ul> <p>The TSF's SSH transport implementation supports the following public-key algorithms for Client Authentication:</p> <ul style="list-style-type: none"> <li>■ ssh-rsa</li> </ul> <p>The public-key algorithm is consistent with the RSA digital signature algorithm in FCS_COP.1/SigGen.</p> <p>When the SSH client presents a public key, the TSF verifies it matches the one configured for the Administrator account. If the presented public key does not match the one configured for the Administrator account, access is denied.</p> <p>The TSF's SSH key exchange implementation supports the following key exchange algorithm:</p> <ul style="list-style-type: none"> <li>■ ecdh-sha2-nistp256</li> <li>■ ecdh-sha2-nistp384</li> </ul> <p>The TSF's SSH implementation will perform a rekey after no longer than one hour or more than one gigabyte of data has been transmitted with the same session key. Both thresholds are checked. Rekeying is performed upon reaching whichever threshold is met first. The Administrator can configure lower rekey values if desired. The minimum time value is 10 minutes. The minimum volume value is 100 kilobytes.</p>
FCS_TLSC_EXT.1	<p>The TSF implements TLS 1.2 conformant to RFC 5246 to provide secure TLS communication between itself and a Syslog server supporting the following ciphersuites:</p> <ul style="list-style-type: none"> <li>■ TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289</li> <li>■ TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289</li> </ul> <p>When establishing a TLS connection, the TOE supports reference identifiers of type DNS-ID and IP address and will seek a match to the DNS domain name or IP address respectively in the subjectAltName extension. If the TOE determines there is a mismatch in the presented identifier, it will not establish the TLS trusted channel connection. The TOE does not support the use of wildcards within certificates and does not support certificate pinning.</p> <p>For TLS 1.2 connections to the Syslog server, the TSF presents secp256r1, secp384r1, and secp521r1 and no other curves in the Supported Group extension of the Client Hello. This behavior is implemented by default and is not configurable.</p>
FIA_AFL.1	<p>To block password-based brute force attacks, the TOE uses an internal AAA function to detect and track failed login attempts. When an account attempting to log into an administrative interface reaches the set maximum number of failed authentication attempts, the account will not be granted access until the time period has elapsed or until the Administrator manually unblocks the account.</p> <p>The TOE provides the Administrator the ability to specify the maximum number of unsuccessful authentication attempts before an offending account will be blocked. The TOE also provides the ability to specify the time period to block offending accounts.</p>

TOE SFRs	How the SFR is Met
	To avoid a potential situation where password failures made by Administrators leads to no Administrator access until the defined blocking time period has elapsed, the CC Configuration Guide instructs the Administrator to configure the TOE for SSH public key authentication which is not subjected to password-based brute force attacks. During the block out period, the TOE provides the ability for the Administrator account to login remotely using SSH public key authentication.
FIA_PMG_EXT.1	The TOE supports the local definition of users with corresponding passwords. The passwords can be composed of any combination of upper and lower case letters, numbers, and special characters that include: “!”, “@”, “#”, “\$”, “%”, “^”, “&”, “*”, “(”, “)” and other special characters listed in table 16. Minimum password length is settable by the Authorized Administrator, and can be configured for minimum password lengths of 1 and maximum of 127 characters. A minimum password length of 8 is recommended.
FIA_PSK_EXT.1	The TOE supports use of pre-shared keys for MACsec key agreement protocols as defined by IEEE 802.1X. The pre-shared keys are not generated by the TOE, but the TOE accepts the keys in the form of HEX strings. This is done via the CLI configuration command ‘key chain test_key macsec’. The TOE accepts pre-shared keys that are 32 characters in length for AES 128-bit CMAC mode encryption and pre-shared keys that are 64 characters in length for AES 256-bit CMAC mode encryption.
FIA_UIA_EXT.1 FIA_UAU_EXT.2	<p>The TOE requires all users to be successfully identified and authenticated before allowing any TSF mediated actions to be performed. Prior to being granted access, a login warning banner is displayed.</p> <p>Administrative access to the TOE is facilitated through a local password-based authentication and SSH public key authentication mechanisms on the TOE through which all Administrator actions are mediated. Once a potential (unauthenticated) administrative user attempts to access the TOE through an interactive administrative interface, the TOE prompts the user for a user name and password or SSH public key authentication. No access is allowed to the administrative functionality of the TOE until the administrator is successfully identified and authenticated</p> <p>The process for authentication is the same for administrative access whether administration is occurring via a directly connected console or remotely via SSHv2 secured connection.</p> <p>At initial login, the administrative user is prompted to provide a username. After the user provides the username, the user is prompted to provide the administrative password associated with the user account. The TOE then either grants administrative access (if the combination of username and password is correct) or indicates that the login was unsuccessful. The TOE does not provide a reason for failure in the cases of a login failure.</p>
FIA_UAU.7	<p>When a user enters their password at the local console, the TOE does not echo any characters as the password is entered.</p> <p>For remote session authentication, the TOE does not echo any characters as they are entered.</p>
FIA_X509_EXT.1/Rev	<p>The TOE uses X.509v3 certificates to support authentication for TLS connections. The TSF determines the validity of certificates at the time of authentication by ensuring that the certificate and the certificate path are valid in accordance with RFC 5280. The certificate path is validated by ensuring that all the CA certificates have the basicConstraints extension and the CA flag is set to TRUE and the certificate path must terminate with a trusted CA certificate.</p> <p>CRL revocation checking is supported by the TOE. Revocation checking is performed on the leaf and intermediate certificate(s) when authenticating a certificate chain provided by the remote peer. There are no functional differences if a full certificate chain or only a leaf certificate is presented.</p>
FIA_X509_EXT.2	The TOE determines which certificate to use based upon the trustpoint configured. The instructions for configuring trustpoints is provided in CC Configuration Guide. In the event that a network connection cannot be established to verify the revocation status of certificate for an external peer, the certificate will be rejected and the connection will not be established.
FMT_MOF.1/ManualUpdate FMT_MTD.1/CoreData FMT_MTD.1/CryptKeys	<p>The TOE provides the ability for Security Administrators to access TOE data, such as audit data, configuration data, security attributes, routing tables, and session thresholds and to perform manual updates to the TOE. Only Security Administrators can access the TOE’s trust store. Each of the predefined and administratively configured roles has create (set), query, modify, or delete access to the TOE data, though with some privilege levels, the access is limited.</p> <p>The TOE performs role-based authorization, using TOE platform authorization mechanisms, to grant access to the privileged and semi-privileged roles. For the purposes of this evaluation, the privileged level is equivalent</p>

TOE SFRs	How the SFR is Met
	<p>to full administrative access to the CLI, which is the default access for IOS-XE privilege level 15; and the semi-privileged level equates to any privilege level that has a subset of the privileges assigned to level 15. Privilege levels 0 and 1 are defined by default and are customizable, while levels 2-14 are undefined by default and customizable.</p> <p>The term “Authorized Administrator” is used in this ST to refer to any user that has been assigned to a privilege level that is permitted to perform the relevant action; therefore, has the appropriate privileges to perform the requested functions. The semi-privileged Administrators with only a subset of privileges may also manage and modify TOE data based on the privileges assigned.</p> <p>The TOE provides the ability for Authorized Administrators to access TOE data, such as audit data, configuration data, security attributes, session thresholds, cryptographic keys, and updates. Each of the predefined and administratively configured privilege levels has a set of permissions that will grant access to the TOE data, though with some privilege levels, the access is limited.</p> <p>The TOE does not provide automatic updates to the software version running on the TOE.</p> <p>The Authorized Administrator can query the software version running on the TOE and can initiate updates to (replacements of) software images. When software updates are made available by Cisco, the Authorized Administrators can obtain, verify the integrity of, and install those updates.</p> <p>The Authorized Administrator generates RSA key pairs to be used in the TLS and SSH protocols. Zeroization of these keys is provided in Table 20 below.</p> <p>Prior to authentication the TOE may be configured by the Administrator to display a customized login banner, which describes restrictions of use, legal agreements, or any other appropriate information to which users consent by accessing the TOE. No administrative functionality is available prior to administrative login. TOE Administrators can control (generate/delete) the following keys, RSA Key Pairs and SSH RSA Key Pairs by following the instruction in the AGD.</p>
<p>FMT_SMF.1 FMT_SMF.1/MACSEC</p>	<p>The TOE provides all capabilities necessary to securely manage the TOE and the services provided by the TOE. The management functionality of the TOE is provided through the TOE CLI. The Authorized Administrator can perform all management functions by accessing the TOE directly via connected console cable or remote administration via SSHv2 secure connection.</p> <p>The specific management capabilities available from the TOE include:</p> <ul style="list-style-type: none"> <li>• Local and remote administration of the TOE and the services provided by the TOE via the TOE CLI</li> <li>• The ability to manage the warning banner message and content which allows the Authorized Administrator the ability to define warning banner that is displayed prior to establishing a session (note this applies to the interactive (human) users, e.g., administrative users</li> <li>• The ability to set and modify the time limits of session inactivity</li> <li>• The ability to configure the number of failed Administrator logon attempts that will cause the account to be locked until a specified time period has elapsed.</li> <li>• The ability to update the IOS-XE software. The validity of the image is provided using a digital signature prior to installing the update</li> <li>• The ability to modify the behavior of the transmission of audit data to an external IT entity.</li> <li>• The ability to manage cryptographic keys</li> <li>• The ability to manage the cryptographic functionality which allows the Authorized Administrator the ability to identify and configure the algorithms used to provide protection of the data, such as generating the RSA keys to enable SSHv2</li> <li>• Ability to manage the TOE’s trust store and designate X509.v3 certificates as trust anchor</li> <li>• Ability to configure thresholds for SSH rekeying</li> <li>• Ability to re-enable an Administrator account</li> <li>• The ability to manage the trusted public keys database</li> <li>• The ability to manage the Key Server and associated MKA participants</li> </ul>

TOE SFRs	How the SFR is Met
	<ul style="list-style-type: none"> <li>• Manage a PSK-based CAK and install it in the device</li> <li>• The ability to specify the lifetime of a CAK and to enable, disable or delete a PSK in the CAK cache of a device</li> <li>• The ability to configure and set the time clock</li> <li>• The ability to configure the reference identifiers for peers, which can be IP address, FQDN identifier or can be the same as the peer's name</li> <li>• Ability to import X.509v3 certificates to the TOE's trust store</li> </ul>
FMT_SMR.2	<p>The TOE maintains privileged and semi-privileged Administrator roles.</p> <p>The TOE performs role-based authorization, using TOE platform authorization mechanisms, to grant access to TOE functions. For the purposes of this evaluation, the privileged role is equivalent to full administrative access to the CLI, which is the default access for IOS-XE privilege level (PL) 15. Semi-privileged roles are assigned a PL of 0 – 14. PL 0 and 1 are defined by default and are customizable, while PL 2-14 are undefined by default and are also customizable. Note: Levels 0 – 14 are a subset of PL 15 and the levels are not hierarchical.</p> <p>The term “Authorized Administrator” is used in this ST to refer to any user which has been assigned to a privilege level that is permitted to perform the relevant action; therefore, has the appropriate privileges to perform the requested functions.</p> <p>The privilege level determines the functions the user can perform, hence the Authorized Administrator with the appropriate privileges.</p> <p>The TOE can and shall be configured to authenticate all access to the command line interface using a username and password.</p> <p>The TOE supports both local administration via a directly connected console cable and remote administration via SSHv2 secure connection.</p>
FPT_CAK_EXT.1	<p>A CAK value is specified in the configuration file by the Administrator using a bit-based (hex) format. The interface specifically implemented in the TSF for viewing the configuration file is the “show running-config” or “show startup-config” CLI commands. When the TOE is operating in the evaluated configuration, and the Administrator executes the “show running-config” or “show startup-config” CLI commands, the CAK data will not be displayed. This protects the CAK data from unauthorized disclosure.</p>
FPT_FLS.1.	<p>Whenever a failure occurs (power-on self-tests, integrity check of the TSF executable image and/or the noise source health-tests) within the TOE, the TOE securely disables its interfaces to prevent the unintentional flow of any information to or from the TOE and reloads.</p> <p>If the failures persist, the TOE will continue to reload in an attempt to correct the failure. This functionally prevents any failure from causing an unauthorized information flow. There are no failures that circumvent this protection. If the rebooting continues, the Authorized Administrator must contact Cisco Technical Assistance Center (TAC).</p>
FPT_RPL.1 FPT_RPL_EXT.1	<p>Replayed data is discarded by the TOE and the attempt to replay data is logged.</p> <p>The TOE ensures MPDUs are replay protected by ensuring the received 32-bit PN in the SecTAG of the frame is not less than the lowest acceptable 32-bit PN for the SA. With Extended Packet Numbering (XPN) which uses a 64-bit PN, the TOE enforces replay detection by ensuring the received 64-bit PN in the SecTAG of the frame is not less than the lowest acceptable 64-bit PN for the SA.</p> <p>If the PN is less than the lowest acceptable PN for the SA, the MPDU will be dropped and not processed further. The Replay Protection Window Size determines the lowest acceptable PN for the SA and must be enabled in the evaluated configuration. The Replay Protection Window Size may be set to zero to enforce strict replay protection.</p> <p>The TOE protects against replayed MKPDUs by ensuring if a MKPDU contains a duplicate Member Number (MN) and not the most current MN in the Basic Parameter set, then the MKPDU will be dropped and not processed further.</p>

TOE SFRs	How the SFR is Met
FPT_APW_EXT.1	<p>The TOE is designed specifically to not disclose any passwords stored in the TOE. All passwords are stored using a SHA-2 hash. 'Show' commands display only the hashed password.</p> <p>The CC Configuration Guide instructs the Administrator to use the algorithm-type script sub-command when passwords are created or updated. The script is password type 9 and uses a SHA-2 hash.</p>
FPT_SKP_EXT.1	<p>The TOE is designed specifically to not disclose any keys stored in the TOE. The TOE stores all private keys in a secure directory that cannot be viewed or accessed, even by the Administrator. The TOE stores symmetric keys only in volatile memory. Pre-shared keys may be specified in the configuration file by the Administrator using a bit-based (hex) format. While only the Administrator may view the configuration file, the CAKeys can be configured so they are excluded from display when viewing the configuration file via "show running-config" or "show startup-config" CLI commands.</p>
FPT_STM_EXT.1	<p>The TSF implements a clock function to provide a source of date and time. The clock function is reliant on the system clock provided by the underlying hardware. All Switch models have a real-time clock (RTC) with battery to maintain time across reboots and power loss.</p> <p>The TOE relies upon date and time information for the following security functions:</p> <ul style="list-style-type: none"> <li>■ To monitor local and remote interactive administrative sessions for inactivity (FTA_SSL_EXT.1, FTA_SSL.3);</li> <li>■ Validating X.509 certificates to determine if a certificate has expired (FIA_X509_EXT.1/Rev);</li> <li>■ To determine when SSH session keys have expired and to initiate a rekey (FCS_SSHS_EXT.1);</li> <li>■ To provide accurate timestamps in audit records (FAU_GEN.1.2).</li> </ul>
FPT_TUD_EXT.1	<p>An Authorized Administrator can query the software version running on the TOE and can initiate updates to (replacements of) software images. The current active version can be verified by executing the "show version" command from the TOE's CLI. When software updates are made available by Cisco, an Administrator can obtain, verify the integrity of, and install the updates. The updates can be downloaded from <a href="https://software.cisco.com/">https://software.cisco.com/</a>. Trusted updates can be installed on the TOE in one shot or as a multi-stage process with a delayed activation. The inactive version will become active when the Administrator responds 'y' at the reboot prompt. The updates can be downloaded from software.cisco.com.</p> <p>The TOE will authenticate the image using a digital signature verification check to ensure it has not been modified since distribution using the following process: Prior to being made publicly available, the software image is hashed using a SHA512 algorithm and then digitally signed. The digital signature is embedded to the image (hence the image is signed). The TOE uses a Cisco public key to validate the digital signature to obtain the SHA512 hash. The TOE then computes its own hash of the image using the same SHA512 algorithm and verifies the computed hash against the embedded hash. If they match the image has not been modified or tampered since distributed from Cisco meaning the software is authenticated and the image is ready to be activated automatically in the one stage upgrade or by the administrator in the multistage upgrade. If they do not match the image will not install.</p>
FPT_TST_EXT.1	<p>The TOE runs a suite of self-tests during initial start-up to verify correct operation of the cryptographic module. 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, the system halts and a message is displayed to the local console. These tests include:</p> <p><b>AES Known Answer Test:</b> 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. If the encrypted texts match, the test passes; otherwise, the test fails. 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. If the decrypted texts match, the test passes; otherwise, the test fails.</p> <p><b>RSA Signature Known Answer Test (both signature/verification):</b> 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. If the encrypted values, the test passes; otherwise, the test fails. The encrypted data is then decrypted using the private key. This value is compared to the original plaintext value. If the decrypted values match, the test passes; otherwise, the test fails.</p> <p><b>RNG/DRBG Known Answer Test:</b></p>

TOE SFRs	How the SFR is Met
	<p>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. If the random bits match, the test passes; otherwise, the test fails.</p> <p><b>HMAC Known Answer Test:</b> 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. If the MAC values match, the test passes; otherwise, the test fails.</p> <p><b>Software Integrity Test:</b> The Software Integrity Test uses HMAC-SHA256 (IC2M) and HMAC-SHA-1 (CiscoSSL FOM) verification to confirm the cryptographic module has maintained its integrity. The Software Integrity Test is run automatically when the module is loaded.</p> <p><b>SHA-256/384/512 Known Answer Test:</b> For each of the values listed, the SHA implementation is fed known data and a key. These values are used to generate a hash. This hash is compared to a known value. If the hash values match, the test passes; otherwise, the test fails.</p> <p>If any component reports failure for the POST, the system crashes. Appropriate information is displayed on the screen and saved in the crashinfo file.</p> <p>All ports are blocked during the POST. If all components pass the POST, the system is placed in FIPS PASS state and ports can forward data traffic.</p> <p>If an error occurs during the self-test, a SELF_TEST_FAILURE system log is generated.</p> <p>Example Error Message: %CRYPTO-0-SELF_TEST_FAILURE: Crypto algorithms self-test failed (SHA hashing)</p> <p>These tests are sufficient to verify that the correct version of the TOE software is running as well as that the cryptographic operations are all performing as expected because any deviation in the TSF behaviour will be identified by the failure of a self-test.</p>
FTA_SSL_EXT.1 FTA_SSL.3	<p>An Authorized Administrator can configure maximum inactivity times individually for both local and remote administrative sessions using the “exec-timeout” command applied to the console and virtual terminal (vty) lines. The allowable inactivity timeout range is from is &lt;0-35791&gt; minutes. A value of 0 means there is no inactivity timeout enforced.</p> <p>The configuration of the vty lines sets the configuration for the remote console access.</p> <p>The line console settings are not immediately activated for the current session. The current line console session must be exited. When the user logs back in, the inactivity timer will be activated for the new session. The local interactive session terminates and does not lock. If a local user session is inactive for a configured period, the session will be terminated and will require re-identification and authentication to login. If a remote user session is inactive for a configured period, the session will be terminated and will require re-identification and authentication to establish a new session.</p>
FTA_SSL.4	<p>An Authorized Administrator can exit out of both local and remote administrative sessions by issuing the ‘exit’ or ‘logout’ command.</p>
FTA_TAB.1	<p>The Administrator can configure an access banner that describes restrictions of use, legal agreements, or any other appropriate information to which users consent by accessing the TOE. The banner will display on the local console port and SSH interfaces prior to allowing any administrative access.</p>
FTP_ITC.1 FTP_ITC.1/MACSEC	<p>The TOE uses secure protocols to provide trusted communications between itself and authorized IT entities as specified in the table below:</p>

TOE SFRs	How the SFR is Met			
	IT Entity	TOE Acting as Client or Server	Secure Communication Mechanism/ Protocol	Non-TSF Endpoint Identification
	Syslog Server	Client	TLS	X.509 Certificate
	MACsec Peer	Client or Server	MACsec	Pre-Shared Key
FTP_TRP.1/Admin	All remote administrative communications take place over a secure encrypted SSHv2 session. The SSHv2 session is encrypted using AES encryption. The remote users (Authorized Administrators) can initiate SSHv2 communications with the TOE.			

## 6.1. Key Zeroization

The table below describes the key zeroization referenced by FCS\_CKM.4 provided by the TOE.

**Table 20. Key Zeroization**

Key	Description	Storage Location	Zeroization Method
MACsec SAK	The SAK is used to secure the control plane traffic.	internal ASIC register	Overwritten automatically with 0x00 when the MACsec session expires.
MACsec CAK	The CAK secures the control plane traffic.	internal ASIC register	Overwritten with a new value of the key.  (config-key-chain) # key-string <32 or 64 hex-bit CAK>
MACsec Key Encryption Key (KEK)	The Key Encrypting Key (KEK) is used by Key Server, elected by MKA, to transport a succession of SAKs, for use by MACsec, to the other member(s) of a Secure Connectivity Association (SCA).	internal ASIC register	Overwritten automatically with 0x00 when the MACsec session expires.
MACsec Integrity Check Key (ICK)	The ICK is used to verify the integrity of MPDUs and to prove that the transmitter of the MKPDU possesses the CAK.	internal ASIC register	Overwritten automatically with 0x00 when the MACsec session expires.
SSH Session Key	Used to encrypt SSH traffic	SDRAM	Overwritten automatically with 0x00 when the SSH trusted channel is no longer in use.
SSH Private Key	Used in establishing a secure SSH session	NVRAM	Overwritten with 0x00 by using the following command:  #crypto key zeroize <label>



Key	Description	Storage Location	Zeroization Method
TLS Pre-Master secret	Shared secret created using asymmetric cryptography from which new TLS session keys can be created.	SDRAM	Overwritten automatically with 0x00 when the TLS session is no longer in use.
TLS Encryption Key	TLS Encryption Key	SDRAM	Overwritten automatically with 0x00 when the TLS session is no longer in use.
TLS Integrity Key	Used for TLS integrity protection	SDRAM	Overwritten automatically with 0x00 when the TLS session is no longer in use.
TLS Private Key	Used in establishing a secure TLS session	NVRAM	Overwritten with 0x00 by using the following command:  #crypto key zeroize <label>

## 6.2. CAVP Certificates

The table below lists the CAVP certificates for the TOE

**Table 21. CAVP Certificates**

SFR	Selection	Algorithm	Implementation	Certificate Number
FCS_CKM.1 – Cryptographic Key Generation (RSA & ECDSA) and Key Verification (ECDSA only)	2048 3072	RSA	IC2M	A1462
	P-256 P-384	ECDSA	IC2M	A1462
	P-256 P-384 P-521	ECDSA	CiscoSSL FOM	A1420
FCS_CKM.2 – Cryptographic Key Establishment	P-256 P-384	KAS ECC	IC2M	A1462
	P-256 P-384 P-521	KAS ECC	CiscoSSL FOM	A1420
FCS_COP.1/DataEncryption – AES Data Encryption/Decryption	AES-CBC-128 AES-CBC-256 AES-GCM-128 AES-GCM-256	AES	IC2M	A1462
	AES-GCM-128 AES-GCM-256	AES	CiscoSSL FOM	A1420
FCS_COP.1/MACSEC	AES-GCM-128 AES-GCM-256	AES	UADP MSC	AES 4769 <sup>1</sup>
			CDR5M PHY	A1929 <sup>2</sup>

<sup>1</sup> The Tested Environment is Synopsys VCS v2011.12mx-SP1-3

<sup>2</sup> The Tested Environment is Synopsys VCS version R-2020.12-SP2-0\_Full64

SFR	Selection	Algorithm	Implementation	Certificate Number
	AES-KW 128 bits	AES	IC2M	A1462
FCS_COP.1/SigGen – Cryptographic Operation (Signature Generation and Verification)	2048 3072	RSA	IC2M	A1462
	2048 3072	RSA	CiscoSSL FOM	A1420
FCS_COP.1/Hash – Cryptographic Operation (Hash Algorithm)	SHA-256 SHA-512	SHS	IC2M	A1462
	SHA-256 SHA-384	SHS	CiscoSSL FOM	A1420
FCS_COP.1/KeyedHash – Cryptographic Operation (Keyed Hash Algorithm)	HMAC-SHA-256	HMAC	IC2M	A1462
FCS_COP.1/CMAC	AES-CMAC 128, 256 bits	AES-CMAC	IC2M	A1462
FCS_RBG_EXT.1– Random Bit Generation	CTR_DRBG (AES) 256 bits	DRBG	IC2M	A1462
	CTR_DRBG (AES) 256 bits	DRBG	CiscoSSL FOM	A1420

## 7. References

The documentation listed below was used to prepare this ST.

**Table 22. References**

Identifier	Description
[CC_PART1]	Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model, dated September 2012, version 3.1, Revision 5, CCMB-2017-04-001
[CC_PART2]	Common Criteria for Information Technology Security Evaluation – Part 2: Security functional components, dated September 2012, version 3.1, Revision 5, CCMB-2017-04-002
[CC_PART3]	Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance components, dated September 2012, version 3.1, Revision 5, CCMB-2017-04-003
[CEM]	Common Methodology for Information Technology Security Evaluation – Evaluation Methodology, dated September 2012, version 3.1, Revision 5, CCMB-2017-04-004
[NDcPP]	collaborative Protection Profile for Network Devices, version 2.2e, March 23, 2020
[SD]	Supporting Document – Evaluation Activities for Network Device cPP, version 2.2, December-2019
[MOD_MACSEC]	PP-Module for MACsec Ethernet Encryption Version 1.0, 2023-03-02
[AGD]	Cisco Catalyst 9400X/9600X Series Switches 17.12 CC Configuration Guide, version 0.4, September 17, 2024
[AGD]	Cisco Catalyst 9400X/9600X Series Switches 17.12 CC Configuration Guide, Version 0.3, September 11, 2024
IEEE 802.1X-2010	IEEE Standard for Local and metropolitan area networks—Port-Based Network Access Control
IEEE Standard 802.1AE-2018	IEEE Standard for Local and metropolitan area networks-Media Access Control (MAC) Security
ISO 18033-3	Information technology -- Security techniques -- Encryption algorithms -- Part 3: Block ciphers
ISO 10116	Information technology -- Security techniques -- Modes of operation for an n-bit block cipher
ISO 19772	Information technology -- Security techniques -- Authenticated encryption
ISO/IEC 10118-3:2004	Information technology -- Security techniques -- Hash-functions -- Part 3: Dedicated hash-functions
ISO/IEC 9797-2:2011	Information technology -- Security techniques -- Message Authentication Codes (MACs) -- Part 2: Mechanisms using a dedicated hash-function
ISO/IEC 18031:2011	Information technology -- Security techniques -- Random bit generation
NIST SP800-38B	Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication
NIST SP800-38F	Recommendation for Block Cipher Modes of Operation: Methods for Key Wrapping

### 7.1. Acronyms and Terms

The following acronyms and terms are common and may be used in this Security Target.

Table 23. Acronyms and Terms

Acronym/Term	Definition
AAA	Administration, Authorization, and Accounting
ACL	Access Control Lists
AES	Advanced Encryption Standard
AES-CMAC	Advanced Encryption Standard - Cipher-based Message Authentication Code
CAK	Connectivity Association Key
CC	Common Criteria for Information Technology Security Evaluation
CEM	Common Evaluation Methodology for Information Technology Security
CM	Configuration Management
CMAC	Cipher-based Message Authentication Code
DHCP	Dynamic Host Configuration Protocol
EAL	Evaluation Assurance Level
EAP	Extensible Authentication Protocol
GE	Gigabit Ethernet port
ICMP	Internet Control Message Protocol
IT	Information Technology
KCK	Key Confirmation Key
KEK	Key Encryption Key
MACsec	Media Access Control Security
MKA	MACsec Key Agreement
MKPDU	MACsec Key Agreement Protocol Data Unit
MU-MIMO	Multi-User Multiple-Input Multiple-Output
NDcPP	collaborative Network Device Protection Profile
OFDMA	Orthogonal Frequency-Division Multiple Access
OS	Operating System
PoE	Power over Ethernet
POST	Power On Self Test
PRF	Pseudo-random function
PP	Protection Profile
RFC	Request for Comment

SFP	Small-form-factor pluggable port
SHS	Secure Hash Standard
SSHv2	Secure Shell (version 2)
ST	Security Target
TCP	Transport Control Protocol
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Function
TSP	TOE Security Policy
TSS	TOE Summary Specification
UDP	User datagram protocol
WAN	Wide Area Network

## 7.2. Obtaining Documentation and Submitting a Service Request

The Cisco Catalyst 9400X/9600X Series Switches 17.12 CC Configuration Guide (AGD) should be obtained from the Product Listing on the NIAP site.

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

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

## 7.3. Contacting Cisco

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