



Cisco Unified Communications Manager IM and Presence Service (IM & P)11.5SU3 running on Cisco Unified Computing System™ (Cisco UCS) C220 M4S and UCS C240 M4S

Common Criteria Security Target

Version 1.0

15 November 2017



Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© 2017 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public.

Table of Contents

1	SECURITY TARGET INTRODUCTION	8
1.1	ST and TOE Reference	8
1.2	TOE Overview	8
1.2.1	TOE Product Type	9
1.2.2	Supported non-TOE Hardware/ Software/ Firmware	9
1.3	TOE DESCRIPTION	10
1.4	TOE Evaluated Configuration.....	12
1.5	Physical Scope of the TOE.....	13
1.6	Logical Scope of the TOE.....	16
1.6.1	Security Audit	16
1.6.2	Cryptographic Support.....	16
1.6.3	Identification and authentication.....	17
1.6.4	Security Management	17
1.6.5	Protection of the TSF	18
1.6.6	TOE Access	18
1.6.7	Trusted path/Channels	18
1.7	Excluded Functionality	18
2	Conformance Claims.....	19
2.1	Common Criteria Conformance Claim	19
2.2	Protection Profile Conformance.....	19
2.3	Protection Profile Conformance Claim Rationale.....	20
2.3.1	TOE Appropriateness.....	20
2.3.2	TOE Security Problem Definition Consistency	20
2.3.3	Statement of Security Requirements Consistency	20
3	SECURITY PROBLEM DEFINITION.....	21
3.1	Assumptions	21
3.2	Threats	22
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.....	25
5	SECURITY REQUIREMENTS	27
5.1	Conventions.....	27
5.2	TOE Security Functional Requirements	27
5.2.1	Security audit (FAU).....	28
5.2.2	Cryptographic Support (FCS).....	30
5.2.3	Identification and authentication (FIA)	33
5.2.4	Security management (FMT).....	34
5.2.5	Protection of the TSF (FPT)	35
5.2.6	TOE Access (FTA)	36
5.2.7	Trusted Path/Channels (FTP).....	37
5.3	TOE SFR Dependencies Rationale for SFRs Found in NDcPPv1.0.....	38

5.4	Security Assurance Requirements.....	38
5.4.1	SAR Requirements.....	38
5.4.2	Security Assurance Requirements Rationale	38
5.5	Assurance Measures	38
6	TOE Summary Specification	40
6.1	TOE Security Functional Requirement Measures.....	40
7	Annex A: Key Zeroization	53
7.1	Key Zeroization.....	53
8	Annex B: References.....	54

List of Tables

TABLE 1 ACRONYMS.....	5
TABLE 2 TERMINOLOGY.....	6
TABLE 3 ST AND TOE IDENTIFICATION.....	8
TABLE 4 IT ENVIRONMENT COMPONENTS.....	9
TABLE 5 HARDWARE MODEL AND SPECIFICATIONS.....	14
TABLE 6 ALGORITHM CERTIFICATE REFERENCES.....	16
TABLE 7 EXCLUDED FUNCTIONALITY.....	18
TABLE 8 PROTECTION PROFILES.....	19
TABLE 9 TOE ASSUMPTIONS.....	21
TABLE 10 THREATS.....	22
TABLE 11 ORGANIZATIONAL SECURITY POLICIES.....	23
TABLE 12 SECURITY OBJECTIVES FOR THE ENVIRONMENT.....	25
TABLE 13 SECURITY FUNCTIONAL REQUIREMENTS.....	27
TABLE 14 AUDITABLE EVENTS.....	29
TABLE 15: ASSURANCE MEASURES.....	38
TABLE 16 ASSURANCE MEASURES.....	39
TABLE 17 HOW TOE SFRs MEASURES.....	40
TABLE 18: TOE KEY ZEROIZATION.....	53
TABLE 19: REFERENCES.....	54

List of Figures

FIGURE 1 CISCO UCS C220 M4 RACK SERVER (M4S).....	10
FIGURE 2 CISCO UCS C240 M4 SERVER (M4S).....	11
FIGURE 3 TOE EXAMPLE DEPLOYMENT.....	11

Acronyms

The following acronyms and abbreviations are common and may be used in this Security Target:

Table 1 Acronyms

Acronyms / Abbreviations	Definition
AAA	Administration, Authorization, and Accounting
ACL	Access Control Lists
AES	Advanced Encryption Standard
BRI	Basic Rate Interface
CC	Common Criteria for Information Technology Security Evaluation
CEM	Common Evaluation Methodology for Information Technology Security
CM	Configuration Management
CUCM	Cisco Unified Communications Manager
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name Server
EAL	Evaluation Assurance Level
EHWIC	Ethernet High-Speed WIC
ESP	Encapsulating Security Payload
GE	Gigabit Ethernet port
HTTP	Hyper-Text Transport Protocol
HTTPS	Hyper-Text Transport Protocol Secure
ICMP	Internet Control Message Protocol
IEEE	Institute of Electrical and Electronics Engineers
IGMP	Internet Group Management Protocol
IM&P	Instant Message (IM) and Presence Service
IP	Internet Protocol
IPsec	IP Security
ISDN	Integrated Services Digital Network
IT	Information Technology
MAC	Media Access Control
NDcPP	collaborative Network Device Protection Profile
NVRAM	Non-volatile random access memory, specifically the memory in the switch where the configuration parameters are stored.
OS	Operating System
Packet	A block of data sent over the network transmitting the identities of the sending and receiving stations, error-control information, and message.
PBKDF2	Password-Based Key Derivation Function version 2
PoE	Power over Ethernet
PP	Protection Profile
PRNG	Pseudo Random Number Generator
RADIUS	Remote Authentication Dial In User Service
RNG	Random Number Generator
RSA	Rivest, Shamir and Adleman (algorithm for public-key cryptography)
SA	Security Association
SFP	Small-form-factor pluggable port
SHS	Secure Hash Standard
SIP	Session Initiation Protocol
SM	Service Module

Acronyms / Abbreviations	Definition
SSHv2	Secure Shell (version 2)
ST	Security Target
TCP	Transport Control Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol
TOE	Target of Evaluation (in this evaluation the TOE is the Cisco Unified Communications Manager IM and Presence Service product)
TSC	TSF Scope of Control
TSF	TOE Security Function
TSP	TOE Security Policy
UCM	Unified Communications Manager
UDP	User datagram protocol
VoIP	Voice over IP
WAN	Wide Area Network
WIC	WAN Interface Card

Terminology

Table 2 Terminology

Term	Definition
Authorized Administrator	Any user which has been assigned to a privilege level that is permitted to perform all TSF-related functions.
Peer IM&P	Another IM&P on the network that the TOE interfaces with.
Security Administrator	Synonymous with Authorized Administrator for the purposes of this evaluation.
CUCM	Cisco Unified Communications Manager (CUCM) serves as the software-based call-processing component of the Cisco Unified Communications family of products. The CUCM extends enterprise telephony features and functions to packet telephony network devices such as IP phones, media processing devices, voice-over-IP (VoIP) gateways, and multimedia applications.
User	Any entity (human user or external IT entity) outside the TOE that interacts with the TOE.
Firmware (per NIST for FIPS validated cryptographic modules)	The programs and data components of a cryptographic module that are stored in hardware (e.g., ROM, PROM, EPROM, EEPROM or FLASH) within the cryptographic boundary and cannot be dynamically written or modified during execution.

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), the Cisco Unified Communications Manager IM and Presence Service (IM&P) 11.5SU3SU3 running on Cisco Unified Computing System™ (Cisco UCS) C220 M4S, UCS C240 M4S. 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.

1 SECURITY TARGET INTRODUCTION

The Security Target contains the following sections:

- Security Target Introduction [Section 1]
- Conformance Claims [Section 2]
- Security Problem Definition [Section 3]
- Security Objectives [Section 4]
- IT Security Requirements [Section 5]
- TOE Summary Specification [Section 6]

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 3 ST and TOE Identification

Name	Description
ST Title	Cisco Unified Communications Manager IM and Presence Service (IM&P) 11.5SU3SU3 running on Cisco Unified Computing System™ (Cisco UCS) C220 M4S, UCS C240 M4S Common Criteria Security Target
ST Version	1.0
Publication Date	8 November 2017
Vendor and ST Author	Cisco Systems, Inc.
TOE Reference	Cisco IM and Presence (Cisco IM&P)
TOE Hardware Models	Cisco Unified Computing System™ (Cisco UCS) C220 M4S, UCS C240 M4S
TOE Software Version	Cisco Unified Communications Manager IM and Presence Service (IM&P) 11.5SU3SU3 software
Keywords	IM& P, CUCM, Data Protection, Authentication, Voice, Telephony

1.2 TOE Overview

The TOE is Cisco Unified Communications Manager IM and Presence Service running IM&P 11.5SU3 (herein after referred to as IM&P). The TOE is a hardware and software-based network device that provides native standards-based, dual-protocol, enterprise instant messaging (IM) and network-based presence as part of Cisco Unified Communications capabilities.

The evaluated configuration of the TOE includes the IM&P 11.5SU3 software installed on either the Cisco Unified Computing System™ (Cisco UCS) C220 M4 Rack Server [1RU] or UCS C240 M4 2 Rack Server [2RU].

1.2.1 TOE Product Type

The Cisco Unified Communications Manager IM and Presence Service (IM&P) is a hardware and software-based, native standards-based enterprise instant messaging (IM) and network-based presence as part of Cisco Unified Communications family of products. IM&P is a secure and scalable service that offers users feature-rich communications capabilities within the enterprise as well as with external partners.

IM and Presence Service provides the foundation to deliver enterprise IM and network-based presence-enabled collaboration capabilities that allows users to view the presence status or availability of the people they want to communicate with, exchange instant messages with these individuals, and escalate to a voice and video call or a rich collaborative session.

1.2.2 Supported non-TOE Hardware/ Software/ Firmware

The TOE supports the following hardware, software, and firmware components in its operational environment. Each component is identified as being required or not based on the claims made in this Security Target. All of the following environment components are supported by all TOE evaluated configurations.

Table 4 IT Environment Components

Component	Required	Usage/Purpose Description for TOE performance
Local Console	Yes	This includes any IT Environment Console that is directly connected to the TOE via the Serial Console Port and is used by the TOE administrator to support TOE administration.
Management Workstation using web browser for HTTPS	Yes	This includes any IT Environment Management workstation with a web browser installed that is used by the TOE administrator to support TOE administration through HTTPS protected channels. Any web browser that supports TLSv1.1 with the supported ciphersuites may be used.
NTP Server	Yes	The TOE supports communications with CUCM in order to synchronize the date and time on the TOE. CUCM maintains and synchronizes with an NTP server for a reliable timestamp. The NTP Server is required in the IT environment in support of synchronize time stamps for both CUCM and subsequently the TOE.
RADIUS or TACACS+ AAA Server	No	This includes any IT environment RADIUS or TACACS+ AAA server that provides single-use authentication mechanisms. This can be any RADIUS or TACACS+ AAA server that provides single-use authentication.
Syslog Server	Yes	This includes any syslog server to which the TOE would transmit syslog messages using TLS to secure the connection. The audit records are automatically sent to the remote syslog once the configuration and settings are complete.
Cisco Unified Communications Manager (CUCM)	Yes	CUCM serves as the component of the Cisco Unified Communications family of products with which the TOE communicates over a protected TLS channel.
DNS Server		The TOE supports communications with the DNS Server that is required for communications with other components (CUCM and other IM&P clusters). The DNS is required to support IP addressing schemes for traffic and access control. Cisco recommends that all IM and Presence Service node names in the cluster be set to the FQDN or IP address rather than the hostname.

1.3 TOE DESCRIPTION

This section provides an overview of the Cisco Unified Communications Manager IM and Presence Service (IM&P) Target of Evaluation (TOE). The TOE is comprised of both software and hardware.

Integrated with Cisco Unified Communications Manager (CUCM), IM&P service lays the foundation to deliver enterprise IM and network-based presence-enabled collaboration capabilities. The IM&P services enables users to view the presence status or availability of the people they want to communicate with, exchange instant messages with these individuals, and escalate to a rich collaborative session.

A web-browsable interface to the configuration database provides the capability for remote device and system configuration for administrators. IM&P Administration supports the following operating system browsers:

- Microsoft Internet Explorer (IE) 8 and later when running on Microsoft Windows 8 and later
- Firefox 4.x and later when running on Microsoft Windows 8 and later

HTTPS is used to secure the connection between IM&P and the browser.

The IM&P software can be installed on two different models of the Cisco Unified Computing System™ (Cisco UCS), both of which are described below. The Cisco UCS boxes are administered through a single management entity called the Cisco UCS Manager (Cisco Unified Computing System (UCS) Manager 2.2(3a)). It is assumed the Cisco UCS is setup, configured in their evaluated configurations and ready for use.

The Cisco Unified Computing System™ (Cisco UCS) C220 M4 Rack Server (one rack unit [1RU]) offers up to two Intel® Xeon® processor E5-2600 v4 and v3 processors, 24 DIMM slots, eight small form-factor (SFF) disk drives or four large form-factor (LFF) drives, and two 1 Gigabit Ethernet LAN-on-motherboard (LOM) ports. Refer to Table 5 Hardware Models and Specifications for the primary features of the Cisco UCS C220 M4S.



Figure 1 Cisco UCS C220 M4 Rack Server (M4S)

The Cisco Unified Computing System™ (Cisco UCS) C240 M4 Rack Server (two rack unit [2RU]) offers up to two Intel® Xeon® processor E5-2600 v4 and v3 processors, 24 DIMM slots, 24 small form-factor (SFF) disk drives or 12 large form-factor (LFF) drives, and two 1 Gigabit Ethernet LAN-on-motherboard (LOM) ports. Refer to Table 5 Hardware Models and Specifications for the primary features of the Cisco UCS C240 M3S.



Figure 2 Cisco UCS C240 M4 Server (M4S)

The software is comprised of the IM&P software image Release 11.5SU3. Cisco IM&P is a Cisco-developed highly configurable proprietary operating system that provides enterprise instant messaging (IM) and network-based presence as part of Cisco Unified Communications solution. Although IM&P software provides numerous functions such as instant messaging, presence, click-to-call, phone control, voice, video, visual voicemail, and web collaboration, this TOE only addresses the functions that provide for the security of the TOE itself as described in Section 1.7 Logical Scope of the TOE below.

The following figure provides a visual depiction of an example TOE deployment. The TOE boundary is surrounded with a hashed red line.

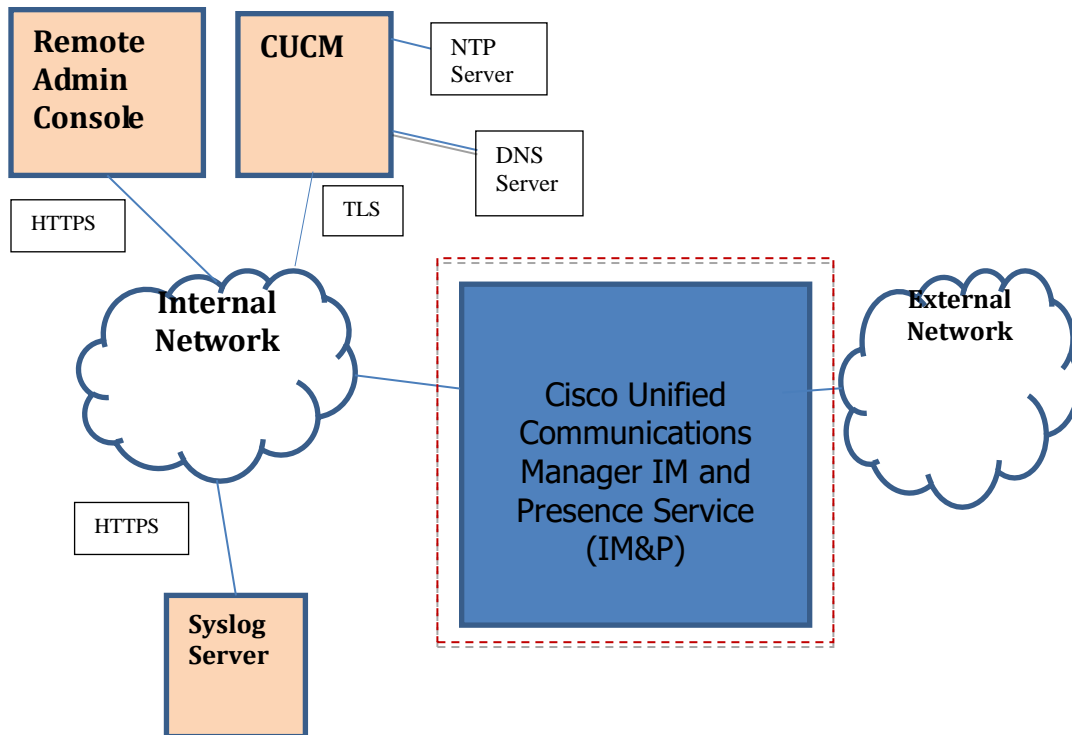


Figure 3 TOE Example Deployment

The previous figure includes the following:

- The TOE
 - Cisco UCS C220 M4S or UCS C240M4S
 - Cisco Unified Communications Manager IM and Presence Service (IM&P) 11.5SU3 software
- The following are considered to be in the IT Environment:
 - Cisco Unified Communications Manager (CUCM) 11.5SU3
 - Management Workstation
 - Syslog Server
 - NTP Server
 - DNS Server

1.4 TOE Evaluated Configuration

The TOE consists of IM&P software installed on one or more appliances as specified in section 1.5 below. The IM&P service is integrated with Cisco Unified Communications Manager (CUCM) that includes a suite of integrated applications that accelerate communication, and enable collaboration with either colleagues within the enterprise or external partners and suppliers.

This suite of basic enterprise instant messaging (IM), network-based presence (availability) and group and persistent chats are the core features that are available for use in the basic deployment. IM is an important communication option that lets users efficiently interact in today's business environment. IM and Presence Service provides personal chat, group chat, and persistent chat capabilities that can quickly connect individuals and groups and conduct ongoing conversations.

- Group chat users to create a temporary IM enterprise chat room and invite internal and external colleagues to the chat room to join an IM conference.
- Persistent chat is a permanent chat room that offers users ongoing access to a discussion thread. It is available even if no one is currently in the chat and remains available until explicitly removed from the system. It allows workers in different locations, countries, and time zones to participate with fellow team members, customers, partners, and suppliers to communicate, quickly gain context to ongoing conversations, and easily collaborate in real time.



The TOE configuration specifies the configuration settings for communications with CUCM and other properties such as the server name and date-time settings. The TOE connects to an NTP server on its internal network for time services. The TOE is administered using the Cisco Unified Communications Manager IM and Presence Service Administration program from an administrative workstation that has Cisco Unified Communications Manager IM and Presence Service installed. No browser software exists on the IM&P server. When connecting to the IM&P the management station must be connected to an internal network, HTTPS/TLS must be used to connect to the TOE. An external audit server is also used to store audit records. These servers must be attached to the internal (trusted) network. The internal (trusted) network is



meant to be separated effectively from unauthorized individuals and user traffic; one that is in a controlled environment where implementation of security policies can be enforced.

1.5 Physical Scope of the TOE

The TOE is a hardware and software solution that makes up the IM&P. The TOE hardware platform is the UCS C220 M4S or the UCS C240 M4S. The TOE software is the IM&P 11.5SU3 software. The network, on which they reside, is considered part of the environment. The TOE guidance documentation that is considered to be part of the TOE can be found listed in the Cisco Unified Communications Manager IM and Presence Service Common Criteria Configuration Guide document and are downloadable from the <http://cisco.com> web site. The TOE is comprised of the following physical specifications as described in Table 5 below:

Table 5 Hardware Model and Specifications

Hardware/ Processor/ Software	Picture	Size	Power	Interfaces
<p>UCS C220 M4S</p> <p>Intel® Xeon® processor E5-2600 v4 or E5-2600 v3 processors</p> <p>IM&P 11.5SU3 software</p>	 <p>(front view)</p>  <p>(rear view)</p>	<p>1RU: 1.7 x 16.9 x 29.8 in. (4.32 x 43 x 75.6 cm)</p>	<p>Up to two 770 W (AC) hot swappable power supplies or two 1050 W (DC) power supplies. One is mandatory; one more can be added for 1 + 1 redundancy.</p>	<ul style="list-style-type: none"> • Up to 4 LFF or 8 SFF front-accessible, hot-swappable, internal SAS, SATA, or SSD drives, providing redundancy options and ease of serviceability • Various PCIe card ports (dependent on which cards are installed), • Virtual Interface Card (VIC) ports, Converged Network Adapter (CNA) ports, Network Interface Card (NIC) ports, Host Bus Adapter (HBA) ports • I/O performance and flexibility with one x8 half-height and half-length slot, and one x16 full-height and half-length slot • Up to two internal 326GB or two 64GB Cisco FlexFlash drives (SD cards) • One internal USB flash drive • Front panel - One KVM console connector (supplies two USB 2.0 connectors, one GA DB15 connector, and one serial port (RS232) RJ45 connector) • Rear panel - One DB15 VGA connector, One RJ45 serial port connector, Two USB 3.0 port connectors, One RJ-45 10/100/1000 Ethernet management port, using Cisco Integrated Management Controller (CIMC) firmware, Two Intel i350 embedded (on the motherboard) GbE LOM ports, One flexible modular LAN on motherboard (mLOM) slot that can accommodate various interface cards

Hardware/ Processor/ Software	Picture	Size	Power	Interfaces
<p>UCS C240 M4S</p> <p>Intel® Xeon® processor E5-2600 v4 or E5-2600 v3 processors</p> <p>IM&P 11.5SU3 software</p>	 <p>(front view)</p>  <p>(rear view)</p>	<p>2RU: 3.43 x 17.65 x 29.0 in. (8.7 x 44.8 x 73.8 cm)</p>	<p>The server is available with four types of power supplies:</p> <ul style="list-style-type: none"> • 650 W (AC) • 930 W (DC) • 1200 W (AC) • 1400 W (AC) 	<ul style="list-style-type: none"> • Up to 12 LFF or 24 SFF front-accessible, hot-swappable, SAS, SATA, or SSD drives for local storage, providing redundancy options and ease of serviceability • Rear panel <ul style="list-style-type: none"> • One DB15 VGA connector • One RJ45 serial port connector • Two USB 3.0 port connectors • One RJ-45 10/100/1000 Ethernet management port, using Cisco Integrated Management Controller (CIMC) firmware • Two Intel i350 embedded (on the motherboard) GbE LOM ports • One flexible modular LAN on motherboard (mLOM) slot that can accommodate various interface cards <ul style="list-style-type: none"> • Various PCIe card ports (dependent on which cards are installed) <ul style="list-style-type: none"> • Virtual Interface Card (VIC) ports • Converged Network Adapter (CNA) ports • Network Interface Card (NIC) ports • Host Bus Adapter (HBA) ports <ul style="list-style-type: none"> • Front panel <ul style="list-style-type: none"> • One KVM console connector (supplies two USB 2.0 connectors, one VGA, DB15 video connector, and one serial port (RS232) RJ45 connector) support the InfiniBand architecture. <ul style="list-style-type: none"> • A front panel controller provides status indications and control buttons

1.6 Logical Scope of the TOE

The TOE is comprised of several security features. Each of the security features identified above consists of several security functionalities, as identified below.

- 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 subsections below. In addition, the TOE implements all RFCs of the NDcPP v1.0 as necessary to satisfy testing/assurance measures prescribed therein.

1.6.1 Security Audit

The Cisco IM&P provides extensive auditing capabilities. The TOE can audit events related to cryptographic functionality, identification and authentication, and administrative actions. The Cisco IM&P generates an audit record for each auditable event. Each security relevant audit event has the date, timestamp, event description, and subject identity. The administrator configures auditable events, performs back-up operations, and manages audit data storage. The TOE audit event logging is centralized and enabled by default. Audit logs can be backed up over a secure TLS channel to an external audit server.

1.6.2 Cryptographic Support

The TOE provides cryptography in support of other Cisco IM&P security functionality. The IM&P software calls the Cisco FIPS Object Module (FOM) v6.0 that has been validated in accordance with the specified standards to meet the requirements listed below in Table 6

Table 6 Algorithm Certificate References

Algorithm	Description	Supported Mode	Cert. #	Module	SFR
RSA	Signature generation and Verification, and key generation and transport	FIPS PUB 186-4 Key Generation	#1743	FOM	FCS_CKM.1(1) FCS_COP.1(2)
AES	Used for symmetric encryption/decryption	AES in CBC and GCM (128 and 256 bits)	#3404	FOM	FCS_COP.1(1)
SHS (SHA-1, 256, 384)	Cryptographic hashing services	Byte Oriented	#2817	FOM	FCS_COP.1(3)
HMAC SHA-1, SHA-256, SHA-384	Keyed hashing services and software integrity test	Byte Oriented	#2172	FOM	FCS_COP.1(4)

Algorithm	Description	Supported Mode	Cert. #	Module	SFR
DRBG	Deterministic random bit generation services in accordance with ISO/IEC 18031:2011	CTR_DRBG (AES 256)	#817	FOM	FCS_RBG_EXT.1

The algorithm certificates are applicable to the TOE based on IM&P which has Linux kernel 2.6 and Intel® Xeon® processors.

The TOE provides cryptography in support of remote administrative management via HTTPS to secure the connection to an external audit server using TLS. The TOE uses the X.509v3 certificate for securing TLS connections.

The TOE also authenticates software updates to the TOE using a published hash.

1.6.3 Identification and authentication

The TOE provides authentication services for administrative users to connect to the TOEs GUI administrator interface. The TOE requires Authorized Administrators to be successfully identified and authenticated prior to being granted access to any of the management functionality. The TOE can be configured to require a minimum password length of 15 characters. The TOE provides administrator authentication against a local user database using the GUI interface accessed via secure HTTPS connection.

1.6.4 Security Management

The TOE provides secure administrative services for management of general TOE configuration and the security functionality provided by the TOE. All TOE administration occurs either through a secure HTTPS session or via a local console connection. The TOE provides the ability to securely manage:

- the configuration of the TOE;
- the configuration of access banners;
- the configuration of session inactivity;
- the verification and installation of TOE updates;
- the auditing behavior; and
- the cryptographic functionality

The TOE supports the security administrator role. Only the privileged administrator can perform the above security relevant management functions.

Administrators can create configurable login banners to be displayed at time of login, and can define an inactivity timeout for each admin interface to terminate sessions after a set period of inactivity.

1.6.5 Protection of the TSF

The TOE protects against interference and tampering by untrusted subjects by implementing identification, authentication, and access controls to limit configuration to Authorized Administrators. The TOE prevents reading of cryptographic keys and passwords. Additionally Cisco IM&P is not a general-purpose operating system and access to Cisco IM&P memory space is restricted to only Cisco IM&P functions.

The TOE initially synchronizes time with CUCM that maintains and synchronizes with an NTP server and then internally maintains the date and time. This date and time is used as the timestamp that is applied to audit records generated by the TOE.

The TOE performs testing to verify correct operation of the system itself and that of the cryptographic module.

Finally, the TOE is able to verify any software updates prior to the software updates being installed on the TOE to avoid the installation of unauthorized software.

1.6.6 TOE Access

The TOE can terminate inactive sessions after an Authorized Administrator configurable time-period. Once a session has been terminated the TOE requires the user to re-authenticate to establish a new session.

The TOE can also display an Authorized Administrator specified banner on the GUI management interface prior to allowing any administrative access to the TOE.

1.6.7 Trusted path/Channels

The TOE allows trusted paths to be established to itself from remote administrators over HTTPS and initiates secure HTTPS connections to transmit audit messages to remote syslog servers.

1.7 Excluded Functionality

The following functionality is excluded from the evaluation.

Table 7 Excluded Functionality

Excluded Functionality	Exclusion Rationale
Non-FIPS mode of operation on the TOE	This mode of operation includes non-FIPS allowed operations.

These services will be disabled by configuration. The exclusion of this functionality does not affect compliance to the collaborative Protection Profile for Network Devices Version 1.0.

2 CONFORMANCE CLAIMS

2.1 Common Criteria Conformance Claim

The TOE and ST are compliant with the Common Criteria (CC) Version 3.1, Revision 4, dated: July 2009. For a listing of Assurance Requirements claimed see section 5.4.

The TOE and ST are CC Part 2 extended and CC Part 3 conformant.

2.2 Protection Profile Conformance

The TOE and ST are conformant with the Protection Profiles as listed in Table 8 below. The following NIAP Technical Decisions (TD) have also been applied to the claims in this document. Each posted TD was reviewed and considered based on the TOE product type, the PP claims and the security functions claimed in this document.

TD0235, TD0228, TD0227, TD0226, TD0201, TD0188, TD0187, TD0185, TD0184, TD0181, TD0169, TD0168, TD0165, TD0156, TD0154, TD0153, TD0152, TD0151, TD0143, TD0130, TD0126, TD0125, TD0117, TD0116, TD0114, TD0113, TD0112, TD0111, TD0095, TD0094, TD0090

The following NIAP Technical Decisions (TD) were reviewed, though considered not applicable based on TOE product type, the PP claims and the security functions claimed in this document.

TD0245, TD0243, TD0241, TD0239, TD0238, TD0237, TD0236, TD0234, TD0233, TD0232, TD0231, TD0230, TD0229, TD0225, TD0224, TD0223, TD0222, TD0221, TD0219, TD0218, TD0217, TD0215, TD0214, TD0213, TD0212, TD0211, TD0210, TD0209, TD0208, TD0207, TD0206, TD0204, TD0203, TD0202, TD0200, TD0199, TD0197, TD0196, TD0194, TD0193, TD0192, TD0190, TD0189, TD0186, TD0183, TD0182, TD0180, TD0179, TD0178, TD0177, TD0176, TD0175, TD0174, TD0172, TD0171, TD0170, TD0167, TD0166, TD0164, TD0163, TD0160, TD0159, TD0158, TD0157, TD0155, TD0150, TD0148, TD0147, TD0146, TD0145, TD0144, TD0142, TD0140, TD0139, TD0138, TD0137, TD0136, TD0135, TD0134, TD0133, TD0131, TD0127, TD0124, TD0123, TD0121, TD0120, TD0119, TD0118, TD0115, TD0107, TD0105, TD0104, TD0103, TD0097, TD0096, TD0092, TD0086, TD0083, TD0079, TD0076, TD0074, TD0071, TD0069, TD0068, TD0067, TD0066, TD0065, TD0055, TD0053, TD0042, TD0037, TD0014

Table 8 Protection Profiles

Protection Profile	Version	Date
collaborative Protection Profile for Network Devices (NDCPP)	1.0	February 27, 2015

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:

- collaborative Protection Profile for Network Devices, Version 1.0

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 the collaborative Protection Profile for Network Devices, Version 1.0 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 the NDcPPv1.0, 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 the NDcPPv0, for which conformance is claimed verbatim. All concepts covered in the Protection Profile's Statement of Security Requirements are included in this Security Target. Additionally, the Security Assurance Requirements included in this Security Target are identical to the Security Assurance Requirements included in the NDcPPv1.0.

3 SECURITY PROBLEM DEFINITION

This section identifies the following:

- Significant assumptions about the TOE’s operational environment.
- IT related threats to the organization countered by the TOE.
- Environmental threats requiring controls to provide sufficient protection.
- Organizational security policies for the TOE as appropriate.

This document identifies assumptions as A.assumption with “assumption” specifying a unique name. Threats are identified as T.threat with “threat” specifying a unique name. Organizational Security Policies (OSPs) are identified as P.osp with “osp” specifying a unique name.

3.1 Assumptions

The specific conditions listed in the following subsections are assumed to exist in the TOE’s 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.

Table 9 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 and/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 will not include any requirements on physical tamper protection or other physical attack mitigations. The cPP will 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.
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).
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	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 being 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

Assumption	Assumption Definition
	compromise the security of the device.
A.REGULAR_UPDATES	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.
A.ADMIN_CREDENTIALS_SECURE	The administrator's credentials (private key) used to access the network device are protected by the platform on which they reside.

3.2 Threats

The following table lists the threats addressed by the TOE and the IT Environment. The assumed level of expertise of the attacker for all the threats identified below is Enhanced-Basic.

Table 10 Threats

Threat	Threat Definition
T.UNAUTHORIZED_ADMINISTRATOR_ACCESS	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.
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.

Threat	Threat Definition
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	A component of the network device may fail during start-up or during operations causing a compromise or failure in the security functionality of the network device, leaving the device susceptible to attackers.

3.3 Organizational Security Policies

The following table lists the Organizational Security Policies imposed by an organization to address its security needs.

Table 11 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 collaborative Protection Profile for Network Devices v1.0 does not define any security objectives for the TOE.

4.2 Security Objectives for the Environment

All of the assumptions stated in section 3.1 are considered to be security objectives for the environment. The following are the Protection Profile non-IT security objectives, which, in addition to those assumptions, are to be satisfied without imposing technical requirements on the TOE. That is, they will not require the implementation of functions in the TOE hardware and/or software. Thus, they will be satisfied largely through application of procedural or administrative measures.

Table 12 Security Objectives for the Environment

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

Security Objective for the Operational Environment	Definition of the Security Objective	Responsibility of the Administrators
OE.UPDATES	The TOE firmware and software is updated by an administrator on a regular basis in response to the release of product updates due to known vulnerabilities.	Administrators must download updates, including psirts (bug fixes) to the evaluated image to ensure that the security functionality of the TOE is maintained
OE.ADMIN_CREDENTIALS_SECURE	The administrator's credentials (private key) used to access the TOE must be protected on any other platform on which they reside.	Administrators must securely store and appropriately restrict access to credentials that are used to access the TOE (i.e. private keys and passwords)

5 SECURITY REQUIREMENTS

This section identifies the Security Functional Requirements for the TOE. The Security Functional Requirements included in this section are derived from Part 2 of the *Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 4, dated: September 2012* and all international interpretations.

5.1 Conventions

The CC defines operations on Security Functional Requirements: assignments, selections, assignments within selections and refinements. This document uses the following font conventions to identify the operations defined by the CC:

- Assignment: Indicated with *italicized* text;
- Refinement made by PP author: Indicated with **bold text** and ~~strikethroughs~~, if necessary;
- Selection: Indicated with underlined text;
- Assignment within a Selection: Indicated with *italicized and underlined text*;
- Iteration: Indicated by appending the iteration number in parenthesis, e.g., (1), (2), (3) and/or by adding a string starting with “/”..
- Where operations were completed in the NDcPP itself, the formatting used in the NDcPP has been retained.

Explicitly stated SFRs are identified by having a label ‘EXT’ after the requirement name for TOE SFRs. Formatting conventions outside of operations and iterations matches the formatting specified within the NDcPPv1.0.

5.2 TOE Security Functional Requirements

This section identifies the Security Functional Requirements for the TOE. The TOE Security Functional Requirements that appear in the following table are described in more detail in the following subsections.

Table 13 Security Functional Requirements

Class Name	Component Identification	Component Name
FAU: Security audit	FAU_GEN.1	Audit data generation
	FAU_GEN.2	User Identity Association
	FAU_STG_EXT.1	Security audit event storage
FCS: Cryptographic support	FCS_CKM.1	Cryptographic Key Generation (for asymmetric keys)
	FCS_CKM.2	Cryptographic Key Establishment (Refined)
	FCS_CKM.4	Cryptographic Key Zeroization
	FCS_COP.1(1)	Cryptographic Operation (AES Data Encryption/Decryption)
	FCS_COP.1(2)	Cryptographic Operation (Signature Generation and Verification)
	FCS_COP.1(3)	Cryptographic Operation (Hash Algorithm)
	FCS_COP.1(4)	Cryptographic Operation (Keyed Hash Algorithm)
	FCS_HTTPS_EXT.1	HTTPS Protocol

Class Name	Component Identification	Component Name
	FCS_RBG_EXT.1	Random Bit Generation
	FCS_TLSC_EXT.1	TLS Client Protocol
	FCS_TLSS_EXT.1	TLS Server Protocol
FIA: Identification and authentication	FIA_PMG_EXT.1	Password Management
	FIA_UIA_EXT.1	User Identification and Authentication
	FIA_UAU_EXT.2	Password-based Authentication Mechanism
	FIA_UAU.7	Protected Authentication Feedback
	IA_X509_EXT.1	X.509 Certificate Validation
	FIA_X509_EXT.2	X.509 Certificate Authentication
	FIA_X509_EXT.3	X.509 Certificate Requests
FMT: Security management	FMT_MOF.1(1)/TrustedUpdate	Management of security functions behaviour
	FMT_MTD.1	Management of TSF Data
	FMT_SMF.1	Specification of Management Functions
	FMT_SMR.2	Restrictions on Security Roles
FPT: Protection of the TSF	FPT_SKP_EXT.1	Extended: Protection of TSF Data (for reading of all symmetric keys)
	FPT_APW_EXT.1	Extended: Protection of Administrator Passwords
	FPT_STM.1	Reliable Time Stamps
	FPT_TUD_EXT.1	Trusted update
	FPT_TST_EXT.1	TSF Testing (Extended)
FTA: TOE Access	FTA_SSL_EXT.1	TSF-initiated Session Locking
	FTA_SSL.3	TSF-initiated Termination
	FTA_SSL.4	User-initiated Termination
	FTA_TAB.1	Default TOE Access Banners
FTP: Trusted path/channels	FTP_ITC.1	Trusted Channel
	FTP_TRP.1	Trusted Path

5.2.1 Security audit (FAU)

5.2.1.1 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 shut-down 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).*
 - *Security related 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 (if applicable)*
 - [no other actions];

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 PP/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(1)	None.	None.
FCS_COP.1(2)	None.	None.
FCS_COP.1(3)	None.	None.
FCS_COP.1(4)	None.	None.
FCS_HTTPS_EXT.1	Failure to establish a HTTPS Session	Reason for failure
FCS_RBG_EXT.1	None.	None.
FCS_TLSC_EXT.1	Failure to establish a TLS Session	Reason for failure
FCS_TLSS_EXT.1	Failure to establish a TLS Session	Reason for failure
FIA_PMG_EXT.1	None.	None.
FIA_UIA_EXT.1	All use of the identification and authentication mechanism.	Provided user identity, origin of the attempt (e.g., IP address).
FIA_UAU_EXT.2	All use of the authentication mechanism.	Origin of the attempt (e.g., IP address).
FIA_UAU.7	None.	None.
FIA_X509_EXT.1	Unsuccessful attempt to validate a certificate	None
FIA_X509_EXT.2	None.	None.
FIA_X509_EXT.3	None.	None.
FMT_MOF.1(1)/Trusted Update	Any attempt to initiate a manual update	None.
FMT_MTD.1	All management activities of TSF data	None.
FMT_SMF.1	None.	None.
FMT_SMR.2	None.	None.
FPT_SKP_EXT.1	None.	None.
FPT_APW_EXT.1	None.	None.
FPT_STM.1	Changes to the 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)	No additional information.
FTA_SSL_EXT.1	Any attempts at unlocking of an interactive session.	None.
FTA_SSL.3	The termination of a remote session by the session locking mechanism.	None.
FTA_SSL.4	The termination of an interactive	None.

SFR	Auditable Event	Additional Audit Record Contents
	session.	
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	Initiation of the trusted channel. Termination of the trusted channel. Failures of the trusted path functions.	Identification of the claimed user identity.

5.2.1.2 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.

5.2.1.3 FAU_STG_EXT.1 External Audit Trail 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.

FAU_STG_EXT.1.3 The TSF shall [overwrite previous audit records according to the following rule: [when allotted space has reached its threshold], [no other action]] when the local storage space for audit data is full.

5.2.2 Cryptographic Support (FCS)

5.2.2.1 FCS_CKM.1 Cryptographic Key Generation (Refined)

FCS_CKM.1.1 Refinement: 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

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

5.2.2.1 FCS_CKM.2 Cryptographic Key Establishment (Refined)

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

- RSA-based key establishment schemes that meets the following: NIST Special Publication 800-56B Revision 1, “Recommendation for Pair-Wise Key Establishment Schemes Using Integer Factorization Cryptography”;

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

5.2.2.2 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];
- 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];

that meets the following: *No Standard*.

5.2.2.3 FCS_COP.1(1) Cryptographic Operation (AES Data Encryption/Decryption)

FCS_COP.1.1(1) Refinement: 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 met the following: *AES as specified in ISO 18033-3, [CBC as specified in ISO 10116, GCM as specified in ISO 19772]*.

5.2.2.4 FCS_COP.1(2) Cryptographic Operation (Signature Generation and Verification)

FCS_COP.1.1(2) Refinement: 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 or greater],

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,

].

5.2.2.5 FCS_COP.1(3) Cryptographic Operation (Hash Algorithm)

FCS_COP.1.1(3) The TSF shall perform *cryptographic hashing services* in accordance with a specified cryptographic algorithm [SHA-1, SHA-256, SHA-384] ~~and cryptographic key sizes [assignment: cryptographic key sizes]~~ that meet the following: ISO/IEC 10118-3:2004.

5.2.2.6 FCS_COP.1(4) Cryptographic Operation (Keyed Hash Algorithm)

FCS_COP.1.1(4) The TSF shall perform *keyed-hash message authentication* in accordance with a specified cryptographic algorithm [HMAC-SHA-1, HMAC-SHA-256, HMAC-SHA-384] and cryptographic key sizes [160-bit, 256-bit, 384-bit] **and message digest sizes [160, 256, 384] bits** that meet the following: ISO/IEC 9797-2:2011, Section 7 “MAC Algorithm 2”.

5.2.2.1 FCS_HTTPS_EXT.1 HTTPS Protocol

FCS_HTTPS_EXT.1.1 The TSF shall implement the HTTPS protocol that complies with RFC 2818.

FCS_HTTPS_EXT.1.2 The TSF shall implement HTTPS using TLS.

FCS_HTTPS_EXT.1.3 The TSF shall establish the connection only if [the peer presents a valid certificate during the handshake].

5.2.2.2 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] software based noise source] with minimum of [256 bits] of entropy at least equal to the greatest security strength, according to ISO/IEC 18031:2011 Table C.1

5.2.2.3 FCS_TLSC_EXT.1 TLS Client Protocol

FCS_TLSC_EXT.1.1 The TSF shall implement [TLS 1.2 (RFC 5246), TLS 1.1 (RFC 4346)] supporting the following ciphersuites: [

- TLS_RSA_WITH_AES_128_CBC_SHA as defined in RFC 3268
 - TLS_RSA_WITH_AES_256_CBC_SHA as defined in RFC 3268
 - TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289
 - TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289
-].

FCS_TLSC_EXT.1.2 The TSF shall verify that the presented identifier matches the reference identifier according to RFC 6125.

FCS_TLSC_EXT.1.3 The TSF shall [perform RSA key establishment with key size [2048 bits]].

FCS_TLSC_EXT.1.4 The TSF shall present the Supported Elliptic Curves Extension in the Client Hello with the following NIST curves: [secp256r1, secp384r1] and no other curves.

5.2.2.4 FCS_TLSS_EXT.1 TLS Server Protocol

FCS_TLSS_EXT.1.1 The TSF shall implement [TLS 1.2 (RFC 5246), TLS 1.1 (RFC 4346)] supporting the following ciphersuites:

- *Mandatory Ciphersuites:*
 - *TLS_RSA_WITH_AES_128_CBC_SHA as defined in RFC 3268*

- [Optional Ciphersuites:
 - [TLS_RSA_WITH_AES_256_CBC_SHA as defined in RFC 3268
 - [TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289].

FCS_TLSS_EXT.1.2 The TSF shall deny connections from clients requesting SSL 2.0, SSL 3.0, TLS 1.0, and [none].

FCS_TLSS_EXT.1.3 The TSF shall generate key establishment parameters using RSA with key size 2048 bits and [no other size] and [and no other curves]; [no other].

5.2.3 Identification and authentication (FIA)

5.2.3.1 FIA_PMG_EXT.1 Password Management

FIA_PMG_EXT.1.1 The TSF shall provide the following password management capabilities for administrative passwords:

- a) *Passwords shall be able to be composed of any combination of upper and lower case letters, numbers, and the following special characters: [“!” , “@” , “#” , “\$” , “%” , “^” , “&” , “*” , “(” , “)”” ,];*
- b) *Minimum password length shall be settable by the Security Administrator, and support passwords of 15 characters or greater.*

5.2.3.2 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.

5.2.3.3 FIA_UAU_EXT.2 Password-based Authentication Mechanism

FIA_UAU_EXT.2.1 The TSF shall provide a local password-based authentication mechanism, [none] to perform administrative user authentication.

5.2.3.4 5.3.4.5 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.

5.2.3.5 FIA_X509_EXT.1 X.509 Certificate Validation

FIA_X509_EXT.1.1 The TSF shall validate certificates in accordance with the following rules:

- RFC 5280 certificate validation and certificate path validation.
- The certificate path must terminate with a trusted CA certificate.
- The TSF shall validate a certificate path by ensuring the presence of the basicConstraints extension and that the CA flag is set to TRUE for all CA certificates.
- The TSF shall validate the revocation status of the certificate using [the Online Certificate Status Protocol (OCSP) as specified in RFC 2560].
- 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 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.

5.2.3.6 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 [accepts the certificate].

5.2.3.7 FIA_X509_EXT.3 X.509 Certificate Requests

FIA_X509_EXT.3.1 The TSF shall generate a Certificate Request Message as specified by RFC 2986 and be able to provide the following information in the request: public key and [Common Name].

FIA_X509_EXT.3.2 The TSF shall validate the chain of certificates from the Root CA upon receiving the CA Certificate Response.

5.2.4 Security management (FMT)

5.2.4.1 FMT_MOF.1(1)/TrustedUpdate Management of security functions behaviour

FMT_MOF.1.1(1)/TrustedUpdate The TSF shall restrict the ability to enable the functions to perform manual update to Security Administrators.

5.2.4.2 FMT_MTD.1 Management of TSF Data

FMT_MTD.1.1 The TSF shall restrict the ability to *manage* the *TSF data* to the *Security Administrators*.

5.2.4.3 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 [hash comparison] capability prior to installing those updates;*
- [
 - Ability to configure the cryptographic functionality;
].

5.2.4.4 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.

5.2.5 Protection of the TSF (FPT)

5.2.5.1 FPT_SKP_EXT.1 Extended: Protection of TSF Data (for reading of all symmetric keys)

FPT_SKP_EXT.1.1 The TSF shall prevent reading of all pre-shared keys, symmetric keys, and private keys.

5.2.5.2 FPT_APW_EXT.1: Protection of Administrator Passwords

FPT_APW_EXT.1.1 The TSF shall store passwords in non-plaintext form.

FPT_APW_EXT.1.2 The TSF shall prevent the reading of plaintext passwords.

5.2.5.3 FPT_STM.1 Reliable time stamps

FPT_STM.1.1 The TSF shall be able to provide reliable time stamps for its own use.

5.2.5.4 FPT_TST_EXT.1: TSF Testing (Extended)

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: [

- *Power-on Self-Tests:*
 - *Software Integrity Test*
 - *Firmware Integrity Test*
- *Conditional Self-Tests:*
 - *Continuous Random Number Generator test for the FIPS-approved RNG*
 - *Continuous Random Number Generator test for the non-approved RNG*
 - *Conditional Bypass Test*
- *Powerup bypass test*

].

5.2.5.5 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 a means to authenticate firmware/software updates to the TOE using a [published hash] prior to installing those updates.

5.2.6 TOE Access (FTA)

5.2.6.1 FTA_SSL_EXT.1 TSF-initiated Session Locking

FTA_SSL_EXT.1.1 The TSF shall, for local interactive sessions, [

- lock the session - disable any activity of the user's data access/display devices other than unlocking the session, and requiring that the administrator re-authenticate to the TSF prior to unlocking the session]

after a Security Administrator-specified time period of inactivity.

5.2.6.2 FTA_SSL.3 TSF-initiated Termination

FTA_SSL.3.1 Refinement: The TSF shall terminate a **remote** interactive session after a [*Security Administrator-configurable time interval of session inactivity*].

5.2.6.3 FTA_SSL.4 User-initiated Termination

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

5.2.6.4 FTA_TAB.1 Default TOE Access Banners

FTA_TAB.1.1 Refinement: 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.

5.2.7 Trusted Path/Channels (FTP)

5.2.7.1 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 IT entities]** 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 [*audit storage with syslog server (over TLS)*].

5.2.7.2 FTP_TRP.1 Trusted Path

FTP_TRP.1.1 Refinement: The TSF shall **be capable of using [HTTPS]** 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 The TSF shall permit **remote administrators** to initiate communication via the trusted path.

FTP_TRP.1.3 The TSF shall require the use of the trusted path for **initial administrator authentication and all remote administration actions**.

5.3 TOE SFR Dependencies Rationale for SFRs Found in NDcPPv1.0

The Security Functional Requirements (SFRs) in this Security Target represent the SFRs identified in the NDcPPv1.0. As such, the NDcPPv1.0 SFR dependency rationale is deemed acceptable since the PP itself has been validated.

5.4 Security Assurance Requirements

5.4.1 SAR Requirements

The TOE assurance requirements for this ST are taken directly from the NDcPPv1.0 which are derived from Common Criteria Version 3.1, Revision 4. The assurance requirements are summarized in the table below.

Table 15: Assurance Measures

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

5.4.2 Security Assurance Requirements Rationale

The Security Assurance Requirements (SARs) in this Security Target represent the SARs identified in the NDcPPv1.0. As such, the NDcPPv1.0 SAR rationale is deemed acceptable since the PP itself has been validated.

5.5 Assurance Measures

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

Table 16 Assurance Measures

Assurance Class / Component	How requirement will be met
Security Target (ASE) / ASE_CCL.1 / ASE_ECD.1 / ASE_INT.1 / ASE_OBJ.1 / ASE_REQ.1 / ASE_SPD.1 / ASE_TSS.1	<p>Section 2 of this ST includes the TOE and ST conformance claim to CC Version 3.1, Revision 4, dated: July 2009, CC Part 2 extended and CC Part 3 conformant and NDcPPv1.0 and the rationale of how TOE provides all of the functionality at a level of security commensurate with that identified in NDcPPv1.0. Section 2 also includes the consistency rationale for the TOE Security Problem Definition and the Security Requirements to include the extended components definition.</p> <p>Section 1 of the this ST provides the introduction of the ST, the TOE and its references, an overview of the TOE, the TOE product type and the description of the TOE to include the evaluated configuration and the physical and logical cope of the TOE.</p> <p>Section 5 of this ST identifies the security functional requirements, the assurance requirements and how the assurance requirements are met. Section 6 provides the rationale of how the Security Functional Requirements are met by the TOE</p>
Development (ADV) / ADV_FSP.1	<p>The functional specification describes the external interfaces of the TOE; such as the means for a user to invoke a service and the corresponding response of those services. The description includes the interface(s) that enforces a security functional requirement, the interface(s) that supports the enforcement of a security functional requirement, and the interface(s) that does not enforce any security functional requirements. The interfaces are described in terms of their purpose (general goal of the interface), method of use (how the interface is to be used), parameters (explicit inputs to and outputs from an interface that control the behaviour of that interface), parameter descriptions (tells what the parameter is in some meaningful way), and error messages (identifies the condition that generated it, what the message is, and the meaning of any error codes). The development evidence also contains a tracing of the interfaces to the SFRs described in this ST.</p>
Guidance documents (AGD) / AGD_OPE.1	<p>The Administrative Guide provides the descriptions of the processes and procedures of how the administrative users of the TOE can securely administer the TOE using the interfaces that provide the features and functions detailed in the guidance.</p>
Guidance documents (AGD) / AGD_PRE.1	<p>The Installation Guide describes the installation, generation and startup procedures so that the users of the TOE can put the components of the TOE in the evaluated configuration.</p>
Life cycle support (ALC) / ALC_CMC.1	<p>The Configuration Management (CM) document(s) describes how the consumer (end-user) of the TOE can identify the evaluated TOE (Target of Evaluation). The CM document(s) identifies the configuration items, how those configuration items are uniquely identified, and the adequacy of the procedures that are used to control and track changes that are made to the TOE. This includes details on what changes are tracked, how potential changes are incorporated, and the degree to which automation is used to reduce the scope for error.</p>
Life cycle support (ALC) / ALC_CMS.1	
Tests (ATE) / ATE_IND.1	<p>Cisco will provide the TOE for testing.</p>
Vulnerability assessment (AVA) / AVA_VAN.1	<p>Cisco will provide the TOE for testing.</p>

6 TOE SUMMARY SPECIFICATION

6.1 TOE Security Functional Requirement Measures

This section identifies and describes how the Security Functional Requirements identified above are met by the TOE.

Table 17 How TOE SFRs Measures

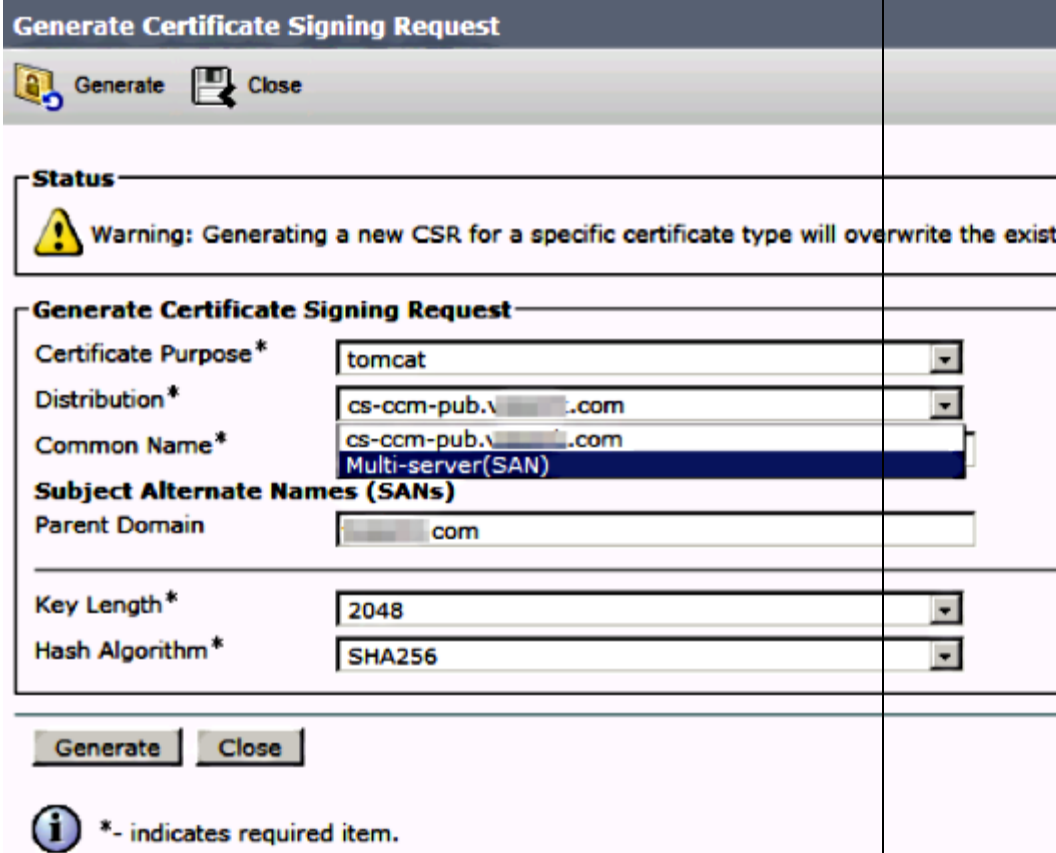
TOE SFRs	How the SFR is Met
FAU_GEN.1	<p>The TOE generates an audit record that is stored internally within the TOE whenever an audited event occurs. The types of events that cause audit records to be generated include, cryptography related events, identification and authentication related events, and administrative events, the specific events and the contents of each audit record are listed in Table 14. Each of the events is specified in the syslog internal to the TOE 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. Additionally, the startup and shutdown of the audit functionality is audited.</p> <p>Audit event logging is centralized and enabled by default. The start and stop of auditing is equated with turning on/booting IM&P and shut-down. An alarm monitor called Syslog Audit writes the logs. By default, the logs are configured to rotate when the storage threshold has been exceeded. If the AuditLogAlarmMonitor cannot write an audit event, the AuditLogAlarmMonitor logs this failure as a critical error in the syslog file. The Alert Manager reports this error as part of a SeverityMatchFound alert. The actual operation continues even if the event logging fails. All audit logs get collected, viewed, and deleted from Trace and Log Central in the Cisco Unified Real-Time Monitoring Tool.</p> <p>Example audit events are included below:</p> <p style="padding-left: 40px;">Audit logging framework - The framework comprises an API that uses an alarm library to write audit events into audit logs. An alarm catalog that is defined as GenericAlarmCatalog.xml applies for these alarms. Different system components provide their own logging. The following example displays an API that a Cisco Unified Communications Manager component can use to send an alarm:</p> <p style="padding-left: 80px;">User ID: CCIMPAdministrator Client IP Address: 172.19.240.207 Severity: 3 EventType: ServiceStatusUpdated ResourceAccessed: CCIMPService EventStatus: Successful Description: IMP Service status is stopped</p> <p>Audit event logging - An audit event represents any event that is required to be logged. The following example displays a sample audit event:</p> <p style="padding-left: 80px;">CCIMP_TOMCAT-GENERIC-3-AuditEventGenerated: Audit Event Generated UserID:CCIMPAdministrator Client IP Address:172.19.240.207 Severity:3 EventType:ServiceStatusUpdated ResourceAccessed:</p>






TOE SFRs	How the SFR is Met
	<p>CCMSERVICE EventStatus:Successful Description: IMP Service status is stopped App ID: Cisco Tomcat Cluster ID: StandAloneCluster Node ID: sa-cm1-3</p> <p>(ref - http://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/service/10_0_1/admin/CUCM_BK_CDDBCDEB_00_cisco-unified-servicability-merge-100/CUCM_BK_CDDBCDEB_00_cisco-unified-servicability-merge-100_chapter_0110.html)</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> <p>Refer to the Common Criteria Operational User Guidance and Preparative Procedures for command description and usage information.</p>
FAU_STG_EXT.1	<p>Log Partition Monitoring (LPM), which is installed automatically with the IM&P, uses configurable thresholds to monitor the disk usage of the log partition on a server. The Cisco Log Partition Monitoring Tool service starts automatically after installation of the IM&P.</p> <p>Every 5 minutes, Log Partition Monitoring uses the following configured thresholds to monitor the disk usage of the log partition and the spare log partition on a server:</p> <ul style="list-style-type: none"> • LogPartitionLowWaterMarkExceeded (% disk space): When the disk usage is above the percentage that you specify, LPM sends out an alarm message to syslog.. • LogPartitionHighWaterMarkExceeded (% disk space): When the disk usage is above the percentage that you specify, LPM sends an alarm message to syslog. • SparePartitionLowWaterMarkExceeded (% disk space): When the disk usage is above the percentage that you specify, LPM sends out an alarm message to syslog.. • SparePartitionHighWaterMarkExceeded (% disk space): When the disk usage is above the percentage that you specify, LPM sends an alarm message to syslog. <p>When the log partition monitoring services starts at system startup, the service checks the current disk space utilization. If the percentage of disk usage is above the low water mark, but less than the high water mark, the service sends an alarm message to syslog.</p> <p>If the percentage of disk usage is above the high water mark that was configured, the system sends an alarm message to syslog and automatically purges log files until the value reaches the low water mark.</p> <p>The audit log records can also be sent to a remote syslog server. For a secure connection to the remote syslog server, TLS is used. Once the configuration settings to the remote syslog server and the desired severity level are selected, as the audit records are generated they are automatically sent to the remote syslog server.</p> <p>The configuration of audit logging is performed using the IM&P serviceability GUI</p>

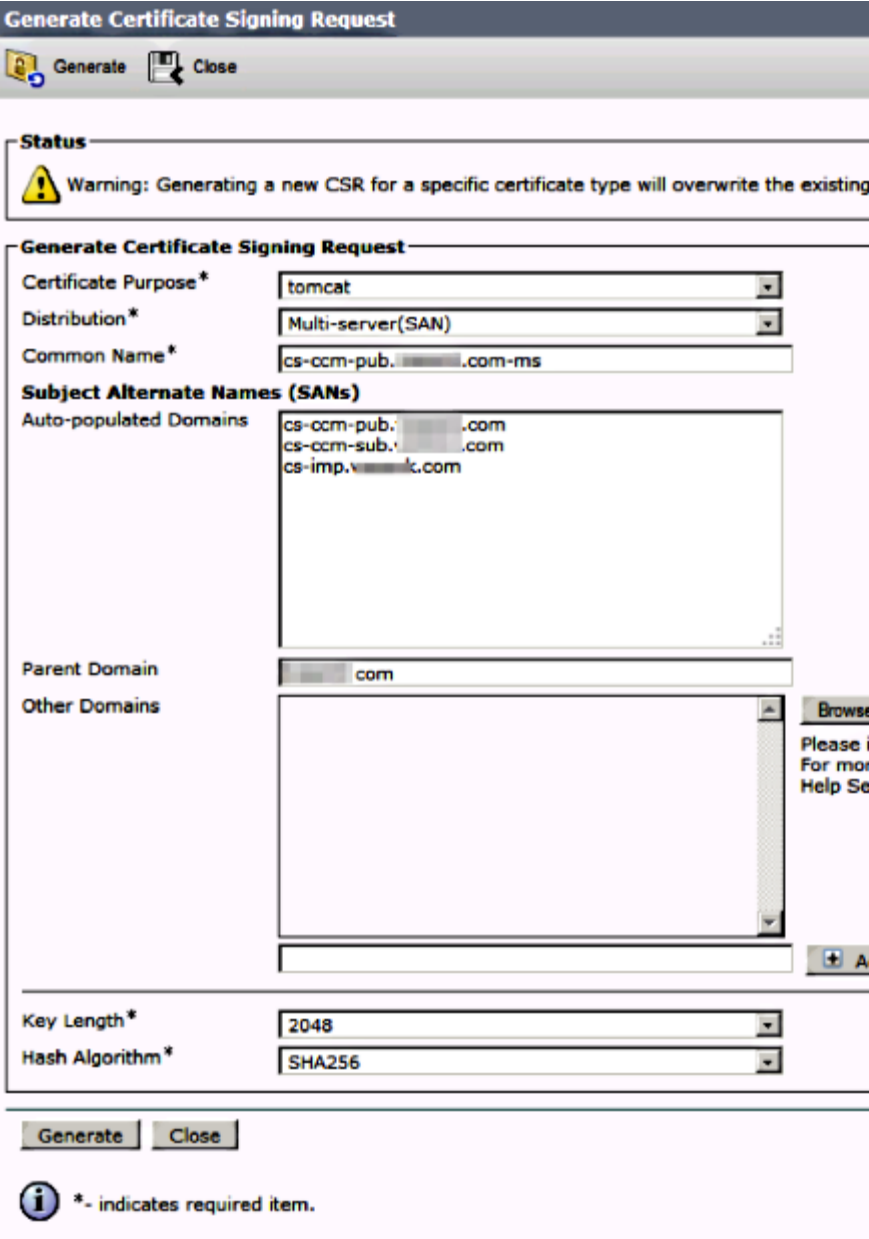


TOE SFRs	How the SFR is Met
FCS_CKM.1	<p>The TOE implements a random number generator for RSA key establishment schemes (conformant to FIPS PUB 186-4, “Digital Signature Standard (DSS)”, Appendix B.3).</p> <p>The TOE can create a RSA public-private key pair, with a minimum RSA key size of 2048 bits. The RSA key pair can be used to generate a Certificate Signing Request (CSR). The TOE can also use the X.509v3 certificate for securing TLS sessions.</p>
FCS_CKM.2	<p>The TOE employs RSA-based key establishment used in cryptographic operations (conformant to NIST Special Pub 800-56b).</p> <p>The TOE operates as both a TLS Server and a TLS client, thus it functions as both a sender and recipient for RSA-based key establishment schemes.</p>
FCS_CKM.4	<p>The TOE meets all requirements as specified by the cryptographic key destruction method of the keys and the Critical Security Parameters (CSPs) when no longer required for use. The keys are destroyed by overwriting and verified through the command show crypto key mypubkey.</p> <p>Additionally, none of the symmetric keys, pre-shared keys, or private keys is stored in plaintext form.</p> <p>See 7.1 Key Zeroization for more information on the key zeroization.</p>
FCS_COP.1(1)	<p>The TOE provides symmetric encryption and decryption capabilities using AES in CBC and GCM mode (128, 256 bits) as described in FIPS PUB 197, NIST SP 800-38A and NIST SP 800-38D.</p> <p>Through the implementation of the cryptographic module, the TOE provides AES encryption and decryption in support of and TLS for secure communications.</p> <p>Management of the cryptographic algorithms is provided through the GUI with auditing of those commands. AES data encryption (128-bit and 256-bit GCM and CBC mode) is the encryption/decryption option that is used within HTTPS/TLS communications with the TOE.</p> <p>The relevant FIPS certificate numbers are listed in Table 6 Algorithm Certificate References</p>
FCS_COP.1(2)	<p>The TOE provides cryptographic signature services using RSA Digital Signature Algorithm with key size of 2048 and greater as specified in FIPS PUB 186-4, “Digital Signature Standard” and FIPS PUB 186-4, “Digital Signature Standard”.</p> <p>Through the implementation of the cryptographic module, the TOE provides cryptographic signatures in support of TLS for secure communications. Management of the cryptographic algorithms is provided through the GUI with auditing of those commands.</p>

TOE SFRs	How the SFR is Met
FCS_COP.1(3) FCS_COP.1(4)	<p>The TOE provides cryptographic hashing services using SHA-1, SHA-256 and SHA-384 as specified in FIPS Pub 180-3 “Secure Hash Standard.”</p> <p>Through the implementation of the cryptographic module, the TOE provides SHS hashing and HMAC message authentication in support of TLS for secure communications. Management of the cryptographic algorithms is provided through the GUI with auditing of those commands.</p> <p>The SHS hashing and HMAC message authentication (SHA-1, SHA-256, SHA-384) is used in the establishment of TLS sessions. The TOE provides keyed-hashing message authentication services using HMAC-SHA-1 (operates on 64-bit blocks), HMAC-SHA-256 (operates on 512-bit blocks of data, and HMAC-SHA-384 (operates on 1024-bit blocks of data (with key sizes and message digest sizes of 160, 256, and 384 bits respectively) as specified in ISO/IEC 9797-2:2011, Section 7 “MAC Algorithm 2”.</p>
FCS_HTTPS_EXT.1, FCS_TLSC_EXT.1 and FCS_TLSS_EXT.1	<p>The TOE supports both TLS v1.1 and TLS v1.2 to protect the TLS sessions for remote administration management and the secure connection to the remote audit server. The supported ciphersuites including the following:</p> <ul style="list-style-type: none"> • TLS_RSA_WITH_AES_128_CBC_SHA as defined in RFC 3268 • TLS_RSA_WITH_AES_256_CBC_SHA as defined in RFC 3268 • TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289 • TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289 <p>The following NIST curves are supported by default on the TOE: <u>secp256r1, secp384r1</u>. <u>No administrator configuration is required in order to use these curves.</u></p> <p>The TOE will not establish TLS v1.0 connections if offered by the client. In addition, the TOE will only establish a connection if the peer presents a valid certificate during handshake.</p> <p>Following is the TLS handshake and exchange of parameters between the client and the TOE.</p>

TOE SFRs	How the SFR is Met
	<div style="border: 1px solid black; padding: 10px;"> <div style="display: flex; justify-content: space-between;"> <div style="width: 45%;"> <p style="text-align: center;">Client</p> <p>Client Hello Client sends the server the version of TLS it would like to use along with supported cipher. The client also sends a random string to be used later in the negotiation</p> <p>Client sends secret that was generated using the random strings that is encrypted with the public key from the server's certificate. The client lets the server know that all messages will now be encrypted and 'finished'</p> <p style="text-align: center;"><i>data</i></p> </div> <div style="width: 10%; text-align: center;"> <pre> sequenceDiagram participant Client participant Server Client->>Server: Client Hello Server-->>Client: Server Hello Client->>Server: Encrypted secret Server-->>Client: done Server-->>Client: message Client<->>Server: data </pre> </div> <div style="width: 45%;"> <p style="text-align: center;">Server</p> <p>Server Hello The server sends the TLS version and cipher that will be used. The server also sends a random string that will be used by the client later in the session. The server sends its certificate; proof of identification and 'done'</p> <p>The server sends a message to the client that all messages will now be encrypted using the keys that were negotiated and 'finished'.</p> <p style="text-align: center;"><i>data</i></p> </div> </div> </div> <p>Using wildcards is not supported in identity certificates, such as when you import the certificate and private key into IM&P/CUCM. However, wild card certificates can be used as a trust certificate where it is the leftmost identifier, for example CN=*.webexconnect.com.</p> <p>Certificate pinning is not supported.</p> <p>The reference identifiers are determined when the CSR is generated for the various applications and devices. For example the certificate for Tomcat that supports HTTP web server environment on multiple nodes, for CUCM that supports SIP calls and video (VVoIP). Following is an example of how the certificate request is generated for the referenced services:</p>

TOE SFRs	How the SFR is Met
	 <p>Select Multi-Server SAN in Distribution.</p>

TOE SFRs	How the SFR is Met
	<div data-bbox="574 237 1620 1081"> <h3>Generate Certificate Signing Request</h3> <p>Generate Close</p> <p>Status</p> <p> Warning: Generating a new CSR for a specific certificate type will overwrite the existing one.</p> <p>Generate Certificate Signing Request</p> <p>Certificate Purpose* tomcat</p> <p>Distribution* cs-ccm-pub.\.com</p> <p>Common Name* cs-ccm-pub.\.com Multi-server(SAN)</p> <p>Subject Alternate Names (SANs)</p> <p>Parent Domain  com</p> <hr/> <p>Key Length* 2048</p> <p>Hash Algorithm* SHA256</p> <p>Generate Close</p> <p> *- indicates required item.</p> </div> <p data-bbox="574 1155 1323 1186">It auto-populates the SAN domains and the parent domain.</p>

TOE SFRs	How the SFR is Met
	 <p>Generate Certificate Signing Request</p> <p>Generate Close</p> <p>Status</p> <p> Warning: Generating a new CSR for a specific certificate type will overwrite the existing CSR for that type</p> <p>Generate Certificate Signing Request</p> <p>Certificate Purpose* tomcat</p> <p>Distribution* Multi-server(SAN)</p> <p>Common Name* cs-ccm-pub.com-ms</p> <p>Subject Alternate Names (SANS)</p> <p>Auto-populated Domains</p> <ul style="list-style-type: none"> cs-ccm-pub.com cs-ccm-sub.com cs-imp.com <p>Parent Domaincom</p> <p>Other Domains</p> <p>Key Length* 2048</p> <p>Hash Algorithm* SHA256</p> <p>Generate Close</p> <p> *- indicates required item.</p>
<p>FCS_RBG_EXT.1</p>	<p>The TOE is hardware and software comprised of the IM&P OS software image Release 11.5SU3 and the hardware as described Table 5 Hardware Models and Specifications.</p> <p>Included as part of the TOE is the Truerand technique to harvest entropy used for cryptographic functions. The deterministic random bit generator used is the AES-256 CTR DRBG.</p>
<p>FIA_PMG_EXT.1</p>	<p>The TOE supports the configuration of passwords to be composed of any combination of upper and lower case letters, numbers, and special characters (that include: “!”, “@”, “#”,</p>

TOE SFRs	How the SFR is Met
	<p>“\$”, “%”, “^”, “&”, “*”, “(”, and “)”. Minimum password length is settable by the Authorized Administrator, and can be configured for minimum password lengths of 15 characters.</p> <p>The administrator accesses the TOE through the GUI via HTTPS. Once a potential administrative user attempts to access the management functionality of the TOE, the TOE prompts the user for a user name and password. Only after the administrative user presents the correct authentication credentials will access to the TOE administrative functionality be granted. No access is allowed to the administrative facilities of the TOE until an administrator is authenticated.</p>
<p>FIA_UIA_EXT.1 FIA_UAU_EXT.2</p>	<p>The TOE requires all users to be successfully identified and authenticated before allowing any TSF mediated actions to be performed except for the login banner that is displayed prior to user authentication.</p> <p>The TOE provides a local password based authentication mechanism.</p> <p>The process for authentication is the same for administrative access whether administration is occurring via a directly connected console cable or remotely via HTTPS. 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 grant administrative access (if the combination of username and password is correct) or indicate that the login was unsuccessful. The TOE does not provide a reason for failure in the cases of a login failure.</p>
<p>FIA_UAU.7</p>	<p>When a user enters their password at the local console, the TOE displays only ‘*’ characters so that the user password is obscured. For remote session authentication, the TOE does not echo any characters as they are entered.</p>
<p>FIA_X509_EXT.1, FIA_X509_EXT.2 and FIA_X509_EXT.3</p>	<p>The TOE uses X.509v3 certificates as defined by RFC 5280 to support authentication for TLS connections. The certificate request message includes the public key and common name per RFC 2986.</p> <p>The TOE supports the following methods to obtain a certificate from a CA:</p> <ul style="list-style-type: none"> • Third-party-signed certificates – the certificates are uploaded, to include the certificate authority root certificate of the certificate authority that signed an application certificate. You can also upload the PKCS#7 format certificate chain of all certificate authority certificates • Self-signed certificate enrollment for a trust point <p>Only one Tomcat certificate may be installed on the TOE at a time. If a new certificate, whether third-party-signed or self-signed, is installed, it will overwrite the old certificate.</p> <p>The certificate chain establishes a sequence of trusted certificates, from a peer certificate to the root CA certificate. Within the PKI hierarchy, all enrolled peers can validate the certificate of one another if the peers share a trusted root CA certificate or a common subordinate CA. Each CA corresponds to a trust point. When a certificate chain is received from a peer, the default processing of a certificate chain path continues until the first trusted certificate, or trust point, is reached. The administrator may configure the level to which a certificate chain is processed on all certificates including subordinate CA certificates.</p> <p>The certificates themselves provide protection in that they are digitally signed. If a certificate is modified in any way, it would be invalidated. The digital signature</p>

TOE SFRs	How the SFR is Met
	<p>verifications process would show that the certificate had been tampered with when the hash value would be invalid.</p> <p>The physical security of the TOE (A.PHYSICAL_PROTECTION) protects the switch and the certificates from being tampered with or deleted. In addition, the TOE identification and authentication security functions protect an unauthorized user from gaining access to the TOE.</p> <p>Furthermore, the certificates are stored in a hidden and protected directory on the TOE that has no external interfaces to gain access.</p> <p>If the connection to determine the certificate validity cannot be established, the administrator is able to accept the certificate.</p>
FMT_MOF.1(1)/TrustedUpdate	<p>The TOE does not provide automatic updates to the software version running on the TOE.</p> <p>The Authorized Administrators 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>
FMT_MTD.1	<p>The TOE provides the ability for Authorized Administrators to access TOE data, such as audit data, configuration data, security attributes and login banners via the GUI.</p> <p>The term “Authorized Administrator” is used in this ST to refer to any user which is permitted to perform the relevant action.</p>
FMT_SMF.1	<p>The TOE provides all the capabilities necessary to securely manage the TOE. The administrative user can connect to the TOE using the GUI via HTTPS to perform these functions or at the local console.</p> <p>The specific management capabilities available from the TOE include:</p> <ul style="list-style-type: none"> • Local and remote administration of the TOE and the services provided by the TOE via the TOE GUI as described above; • The ability to configure a notice and consent warning banner that is displayed prior to logging on the TOE; • The ability to configure inactivity session time periods; • The ability to update the IM&P software (image integrity verification is provided using digital signature) and • The ability to configure the cryptographic functionality
FMT_SMR.2	<p>The term “Authorized Administrator” is used in this ST to refer to any user which is permitted to perform the relevant action.</p> <p>The TOE supports both local administration via a directly connected console and remote authentication via HTTPS.</p>
FPT_SKP_EXT.1 and FPT_APW_EXT.1	<p>The TOE stores all private keys in a secure directory that is not readily accessible to administrators; hence no interface access. Additional, all pre-shared and symmetric keys are stored in encrypted form to prevent access.</p>

TOE SFRs	How the SFR is Met
	<p>The TOE ensures that plaintext user passwords will not be disclosed even to administrators.</p> <p>Refer to the Common Criteria Operational User Guidance and Preparative Procedures for command description and usage information.</p>
FPT_STM.1	<p>The TOE provides a source of date and time information that is used as the time stamp applied to the generated audit records and used to track inactivity of administrative sessions. This source is also used for cryptographic functions. A reliable timestamp is also required to display the correct data and time for the users and tags the correct date and time to IM and chats. In the evaluated configuration, Cisco Unified Communications Manager (CUCM) is a required component in the operating environment. CUCM serves as the component of the Cisco Unified Communications family of products with which the TOE communicates over a protected TLS channel. The TOE supports communications with CUCM in order to synchronize the date and time on the TOE.</p> <p>For this reason, IM&P synchronizing with CUCM timestamp always have an accurate time clock and all associated Cisco IM&P clients on the network will have the exact same time.</p> <p>Note, NTP uses Coordinated Universal Time (UTC) to synchronize computer clock times to a millisecond, and sometimes to a fraction of a millisecond¹.</p>
FPT_TUD_EXT.1	<p>Authorized Administrator can query the software version running on the TOE by accessing the Administration web page that displays the system version, and can initiate updates to (replacements of) software images.</p> <p>When software updates are made available by Cisco, an administrator can obtain, verify the integrity of, and install those updates. The updates can be downloaded from Cisco.com website.</p> <p>The TOE image files are digitally signed so their integrity can be verified during the download and the boot process. An image that fails an integrity check will not be loaded. The digital certificates used by the update verification mechanism are contained on the TOE. Detailed instructions for how to do this verification are provided in the administrator guidance for this evaluation. Briefly, the software version and digital signature information for the TOE is displayed when the download completes, for example:</p> <p style="padding-left: 40px;">Verify the checksum value: MD5: 5d40c79102be57f1bfd737fa8394bf74 SHA1: 1ccea2f0d8d29e94c7e176ac8aa2c6364abfb713</p> <p>This information is verified with the information that is on Cisco CCO where the file was downloaded from. An image that fails an integrity check will not be loaded.</p> <p>The digital signature and image verification with a SHA-512 hash is used to verify software/firmware update files (to ensure they have not been modified from the originals distributed by Cisco) before they are used to actually update the TOE.</p>

¹ <http://searchnetworking.techtarget.com/definition/Network-Time-Protocol>

TOE SFRs	How the SFR is Met
	<p>The TOE files include the software authentication information, such as the image credentials, signing information and type of keys used for verification. During the validation process if the signature or the file itself has been tampered with, the hash value would be invalid.</p> <p>When an invalid image is attempted to be installed, the TOE will display an error and will reject the image as an invalid or corrupt image. If this happens, the Administrator is instructed to contact Cisco Technical Assistance Center (TAC).</p>
FPT_TST_EXT.1	<p>The TOE runs a suite of self-test during initial start-up to verify its correct operation. 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.</p> <p>The TOE also runs a periodic continuous random number generator health test which will also be run any time a request for entropy is made by the application.</p> <p>If any of the tests fail, the TOE will not boot and the Authorized Administrator is instructed to contact Cisco Technical Assistance Center (TAC).</p> <p>During the system bootup process (power on or reboot), all the Power on Startup Test (POST) components for all the cryptographic modules perform the POST for the corresponding component (hardware or software). These tests include:</p> <ul style="list-style-type: none"> • Self-Tests Self-tests are performed automatically at power-up and do not require operator intervention in order to run. Once the module is turned on or reloaded, the power-up self-tests are initiated automatically. If the self-tests are passed successfully, the user is presented with the normal login prompt. • Software and firmware integrity test The Software Integrity Test is run automatically whenever the IM&P system images is loaded and confirms through use of digital signature verification that the image file that's about to be loaded was properly signed and has maintained its integrity since being signed. The system image is digitally signed by Cisco prior to being made available for download from CCO.
FTA_SSL_EXT.1 and FTA_SSL.3	<p>An Authorized Administrator can configure maximum inactivity times individually for both local and remote administrative sessions through the use of the IM&P Administration window. By default, the IM&P will log out the administrator after 30 minutes of inactivity. To re-gain access, the Authorized Administrator will have to log back in with the correct user name and password credentials.</p>
FTA_SSL.4	<p>An Authorized Administrator is able to exit out of both local and remote administrative sessions.</p>
FTA_TAB.1	<p>The TOE can be configured to display a customized login message on the GUI management interface and the local console interface prior to allowing any administrative access to the TOE. This is applicable for both local and remote TOE administration.</p>
FTP_ITC.1	<p>The TOE protects communications between the TOE and the remote audit server using TLS that provides a secure channel to transmit the log events.</p>
FTP_TRP.1	<p>All remote administrative communications take place over a secure encrypted HTTPS session. The remote users are able to initiate HTTPS communications with the TOE.</p>

7 ANNEX A: KEY ZEROIZATION

7.1 Key Zeroization

The following table describes the key zeroization referenced by FCS_CKM.4 provided by the TOE.

The Keys residing in internally allocated data structures can only be accessed using the FIPS validated cryptographic module defined API. Zeroization of sensitive data is performed automatically by API function calls for intermediate data items and the Keys are overwritten with zeros (0x00).

Table 18: TOE Key Zeroization

Name	Description	Zeroization
User Password	This is a variable 15+ character password that is used to authenticate local users. The password is stored in NVRAM.	Zeroized by overwriting with new password
TLS server private key	This key is used for authentication, so the server can prove who it is. The private key used for SSLv3.1/TLS secure connections. The key is stored in NVRAM.	CLI command zeroize RSA Command: crypto key zeroize verify with command: show crypto key mypubkey all
TLS server public key	This key is used to encrypt the data that is used to compute the secret key. The public key used for SSLv3.1/TLS secure connection. The key is stored in NVRAM.	CLI command zeroize RSA Command: crypto key zeroize verify with command: show crypto key mypubkey all
TLS pre-master secret	The pre-master secret is the client and server exchange of random numbers and a special number, the pre-master secret, This pre-master secret is using asymmetric cryptography from which new TLS session keys can be created. The key is stored in SDRAM.	Automatically after TLS session terminated.
TLS session encryption key	The session encryption key is unique for each session and is based on the shared secrets that were negotiated at the start of the session. The Key is used to encrypt TLS session data. The key is stored in SDRAM.	Automatically after TLS session terminated.
TLS session integrity key	This key is used to provide the privacy and TLS data integrity protection. The key is stored in SDRAM.	Automatically after TLS session terminated. The entire object is overwritten with zeros

8 ANNEX B: REFERENCES

The following documentation was used to prepare this ST:

Table 19: 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 4, CCMB-2012-009-001
[CC_PART2]	Common Criteria for Information Technology Security Evaluation – Part 2: Security functional components, dated September 2012, version 3.1, Revision 4, CCMB-2012-009-002
[CC_PART3]	Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance components, dated September 2012, version 3.1, Revision 4, CCMB-2012-009-003
[CEM]	Common Methodology for Information Technology Security Evaluation – Evaluation Methodology, dated September 2012, version 3.1, Revision 4, CCMB-2012-009-004
[NDcPP]	collaborative Protection Profile for Network Devices, Version 1.0, 27 Feb 2015