Cisco Unified Communications Manager

Security Target

Version 1.0

10 August 2015

EDCS - 1502591

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 8
1.2.2 Supported non-TOE Hardware/ Software/ Firmware 9
1.3 TOE DESCRIPTION 9
1.4 TOE Evaluated Configuration 12
1.5 Physical Scope of the TOE 12
1.6 Logical Scope of the TOE 15
1.6.1 Security Audit 15
1.6.2 Cryptographic Support 15
1.6.3 Full Residual Information Protection 16
1.6.4 Identification and authentication 16
1.6.5 Security Management 16
1.6.6 Protection of the TSF 17
1.6.7 TOE Access 17
1.6.8 Trusted path/Channels 17
1.7 Excluded Functionality 17
2 Conformance Claims 18
2.1 Common Criteria Conformance Claim 18
2.2 Protection Profile Conformance 18
2.3 Protection Profile Conformance Claim Rationale 18
2.3.1 TOE Appropriateness 18
2.3.2 TOE Security Problem Definition Consistency 18
2.3.3 Statement of Security Requirements Consistency 18
3 SECURITY PROBLEM DEFINITION 20
3.1 Assumptions 20
3.2 Threats 20
3.3 Organizational Security Policies 21
4 SECURITY OBJECTIVES 22
4.1 Security Objectives for the TOE 22
4.2 Security Objectives for the Environment 24
5 SECURITY REQUIREMENTS 25
5.1 Conventions 25
5.2 TOE Security Functional Requirements 25
5.3 SFRs from NDPP and SIP Server EP 26
5.3.1 Security audit (FAU) 26
5.3.2 Cryptographic Support (FCS) 28
5.3.3 User data protection (FDP) 30
5.3.4 Identification and authentication (FIA) 31
5.3.5 Security management (FMT) 32
5.3.6 Protection of the TSF (FPT) 33

5.3.7 TOE Access (FTA) 34
5.3.1 Trusted Path/Channels (FTP).. 34
5.4 TOE SFR Dependencies Rationale for SFRs Found in PP 36
5.5 Security Assurance Requirements.. 36
5.5.1 SAR Requirements.. 36
5.5.2 Security Assurance Requirements Rationale 36
5.6 Assurance Measures... 36
6 TOE Summary Specification 38
6.1 TOE Security Functional Requirement Measures... 38
7 Annex A: Key Zeroization 52
7.1 Key Zeroization.. 52
8 Annex B: References..53

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 MODELS AND SPECIFICATIONS 13
TABLE 6 FIPS REFERENCES 15
TABLE 7 TOE PROVIDED CRYPTOGRAPHY 16
TABLE 8 EXCLUDED FUNCTIONALITY 17
TABLE 9 PROTECTION PROFILES 18
TABLE 10 TOE ASSUMPTIONS 20
TABLE 11 THREATS 20
TABLE 12 ORGANIZATIONAL SECURITY POLICIES 21
TABLE 13 SECURITY OBJECTIVES FOR THE TOE 22
TABLE 14 SECURITY OBJECTIVES FOR THE ENVIRONMENT 24
TABLE 15 SECURITY FUNCTIONAL REQUIREMENTS 25
TABLE 16 AUDITABLE EVENTS 27
TABLE 17: ASSURANCE MEASURES 36
TABLE 18 ASSURANCE MEASURES 36
TABLE 19 HOW TOE SFRS ARE MET 38
TABLE 20: TOE KEY ZEROIZATION 52
TABLE 21: REFERENCES 53

List of Figures

FIGURE 1 CISCO UCS C220 M3 SERVER 10
FIGURE 2 CISCO UCS C210 M2 SERVER 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
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
IT	Information Technology
NDPP	Network Device Protection Profile
OS	Operating System
PoE	Power over Ethernet
PP	Protection Profile
SBC	Session Border Controllers
SHS	Secure Hash Standard
SIP	Session Initiation Protocol
ST	Security Target
TCP	Transport Control Protocol
TLS	Transport Layer Security
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Function
TSP	TOE Security Policy
UCM	Unified Communications Manager
UDP	User datagram protocol
UCS	Unified Computing System
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 CUCM	Another CUCM on the network that the TOE interfaces with.
Security Administrator	Synonymous with Authorized Administrator for the purposes of this evaluation.
SIP Server	The SIP Server (the TOE) interacts with a VoIP client (user smartphone) and provides registrar and proxy capabilities required for call-session management as well as establishing, processing, and terminating VoIP calls.
User	Any entity (human user or external IT entity) outside the TOE that interacts with the TOE.

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 (CUCM). 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 Security Target
ST Version	1.0
Publication Date	10 August 2015
Vendor and ST Author	Cisco Systems, Inc.
TOE Reference	Cisco Unified Communications Manager, CUCM
TOE Hardware Models	Cisco Unified Computing System™ (Cisco UCS) C220 M3 Rack Server or the Cisco Unified Computing System™ (Cisco UCS) C210 M2 Rack Server.
TOE Software Version	CUCM 11.0
Keywords	CUCM, Data Protection, Authentication, Voice, Telephony

1.2 TOE Overview

The Cisco Unified Communications Manager (CUCM) TOE serves as the hardware and software-based call-processing component of the Cisco Unified Communications family of products. The TOE 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.

The evaluated configuration of the TOE includes the CUCM 11.0 software installed on either the Cisco Unified Computing System™ (Cisco UCS) C220 M3 Rack Server or the Cisco Unified Computing System™ (Cisco UCS) C210 M2 Rack Server.

1.2.1 TOE Product Type

The Cisco Unified Communications Manager (CUCM) is a hardware and software-based, call-processing product that provides call processing, services, and applications. The integration of real-time enterprise communications include, but not limited to instant messaging (e.g. chat), voice that includes IP telephony, mobility features, call control and unified messaging.

CUCM serves as the hardware and software-based call-processing component of the Cisco Unified Communications family of products.

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	No	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 TLSv1.0 with the supported ciphersuites may be used.
NTP Server	Yes	The TOE supports communications with an NTP server in order to synchronize the date and time on the TOE with the NTP server's date and time.
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.
Remote Endpoint	Yes	This includes any peer (other SIP servers) or VoIP client with which the TOE communicates with the end points over a protected TLS channel.

1.3 TOE DESCRIPTION

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

The CUCM system includes a suite of integrated voice applications that perform voice-conferencing and manual attendant console functions. This suite of voice applications means that no need exists for special-purpose voice-processing hardware. Supplementary and enhanced services such as hold, transfer, forward, conference, multiple line appearances, automatic route selection, speed dial, last-number redial, and other features extend to IP phones and gateways.

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

- Microsoft Internet Explorer (IE) 7 and later when running on Microsoft Windows 8 and later
- Microsoft Internet Explorer (IE) 8 and later when running on Microsoft Windows 8 and later
- Firefox 3.x and later when running on Microsoft Windows 8 or Apple MAC OS X and later
- Safari 4.x and later when running on Apple MAC OS X and later

HTTPS is used to secure the connection between CUCM and the browser.

The CUCM software can be installed on two different models of the Cisco Unified Computing System™ (Cisco UCS). Both of which are described below.

The Cisco Unified Computing System™ (Cisco UCS) C220 M3. Rack Server (one rack unit [1RU]) offers up to two Intel® Xeon® processor E5-2600 or E5-2600 v2 processors, 16 DIMM slots, eight disk 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 M3.

Figure 1 Cisco UCS C220 M3 Server

OR

The Cisco Unified Computing System™ (Cisco UCS) C210 M2 General-Purpose Rack-Mount Server is a two-socket, two-rack-unit (2RU) rack-mount server housing up to 16 internal small form-factor (SFF) SAS, SATA or SSD drives for a total of up to 16 terabytes (TB) of storage. Based on six-core Intel® Xeon® 5600 series processors, the server is built for applications including virtualization, network file servers and appliances, storage servers, database servers, and content-delivery servers Refer to Table 5 Hardware Models and Specifications for the primary features of the Cisco UCS C210 M2.

Figure 2 Cisco UCS C210 M2 Server

The software is comprised of the CUCM software image Release 11.0. Cisco CUCM is a Cisco-developed highly configurable proprietary operating system that provides for efficient and effective enterprise telephony features and functions. Although CUCM software provides many signaling and call control services to Cisco integrated telephony applications functions, 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.

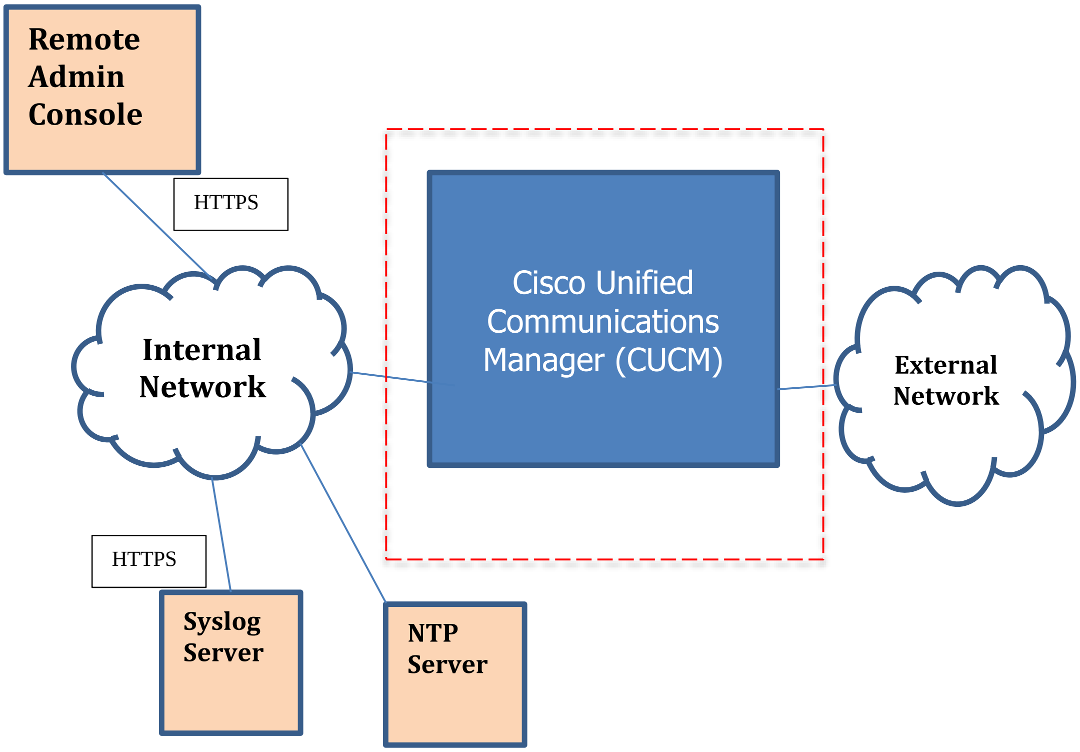

Figure 3 TOE Example Deployment

The previous figure includes the following:

- The TOE
  - Cisco UCS C220 M3S or Cisco UCS C210 M2
  - Cisco CUCM 11.0 software
- The following are considered to be in the IT Environment:
  - Management Workstation
  - NTP Server (does not require a secure connection)
  - Syslog Server

1.4 TOE Evaluated Configuration

The TOE consists of CUCM software installed on one or more appliances as specified in section 1.5 below. The Cisco Unified Communications Manager system includes a suite of integrated voice applications that perform voice-conferencing and manual attendant console functions. This suite of voice applications means that no need exists for special-purpose voice-processing hardware. Supplementary and enhanced services such as hold, transfer, forward, conference, multiple line appearances, automatic route selection, speed dial, last-number redial and other features extend to IP phones and gateways. Because Cisco Unified Communications Manager is a software application, enhancing its capabilities in production environments requires only upgrading software on the UCS server platform.

The TOE configuration specifies the SIP ports 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 Administration program from a PC that is not the web server or has Cisco Unified Communications Manager installed. No browser software exists on the CUCM server. When connecting to the CUCM the management station must be connected to an internal network, HTTPS/TLS must be used to connect to the TOE. A syslog 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 CUCM. The hardware platform is the UCS C220 M3S or the UCS C210 M2. The software is the CUCM 11.0 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 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 Models and Specifications

Hardware	Picture	Size	Power	Interfaces
UCS C220 M3S		1.7 x 16.9 x 28.5 in. (4.32 x 43 x 72.4 cm)	Dual-redundant fans and hot-swappable, redundant power supplies (Cisco Common Form-Factor Platinum Power Supplies (450W and 650W)) for enterprise-class reliability and uptime	• Up to 4 LFF or 8 SFF front-accessible, hot-swappable, internal SAS, SATA, or SSD drives, providing redundancy options and ease of serviceability • 2 PCIe Generation 3.0 slots • 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 16GB Cisco FlexFlash drives (SD cards) • One internal USB flash drive • Front panel - One KVM console connector (supplies 2 USB, 1 VGA, and 1 serial connector) • Rear panel - VGA video port, 2 USB 2.0 ports, an RJ45 serial port, 1 Gigabit Ethernet management port, and dual 1 Gigabit Ethernet ports

Hardware	Picture	Size	Power	Interfaces
UCS C210 M2		2RU: 3.45 x 17.2 x 28.4 in. (8.76 x 43.69 x 72.14 cm)	Dual-redundant fans and power supplies for enterprise-class reliability and uptime	• Up to 16 front-accessible, hot-swappable, SFF SAS, SATA or SSD drives for local storage, providing redundancy options and ease of serviceability • Balanced performance and capacity to best meet application needs: ○ 15,000 RPM SAS drives for highest performance ○ 10,000 RPM SAS drives for high performance and value ○ 7200-RPM SATA drives for high capacity and value • A choice of RAID controllers to provide data protection for up to 16 SAS, SATA or SSD drives in PCIe and mezzanine card form factors • Hard drive ○ Up to 16 front-accessible, hot-swappable, 2.5-inch SAS, SATA or SSD drives • Ease of access to front-panel video, 2 USB ports, and serial console • Management ○ Integrated ServerEngines Pilot-2 BMC ○ IPMI 2.0 compliant for management and control ○ One 10/100BASE-T out-of-band management interface ○ CLI and WebGUI management tool for automated, lights-out management ○ KVM

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.

1. Security Audit
2. Cryptographic Support
3. Full Residual Information Protection
4. Identification and Authentication
5. Security Management
6. Protection of the TSF
7. TOE Access
8. Trusted Path/Channels

These features are described in more detail in the subsections below. In addition, the TOE implements all RFCs of the NDPP v1.1 and SIP EP v1.1 as necessary to satisfy testing and assurance measures prescribed therein.

1.6.1 Security Audit

The Cisco CUCM provides extensive auditing capabilities. The TOE can audit events related to cryptographic functionality, identification and authentication, and administrative actions. The Cisco CUCM 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 CUCM security functionality. This cryptography has been validated for conformance to the requirements of FIPS 140-2 Level 1 (see Table 6 for certificate references). Refer to FIPS certificate 2100; Cisco FIPS Object Module (Software Version: 4.1).

Table 6 FIPS References

Algorithm	Cert. #
RSA	#1377 and #1385
AES	#2678 and #2685
SHS (SHA-1, 256, 384)	#2247 and #2256
HMAC SHA-1, SHA-256, SHA-384	#1664 and #1672
DRBG	#431 and #435
EDCSA	#467 and #471

There are two algorithm certificates because the processor was tested with AES-NI enabled and with AES-NI disabled.

The algorithm certificates are applicable to the TOE based on the underlying OS of the CUCM is RHEL 6 which has Linux kernel 2.6 and the processor is Intel Xeon.

The TOE provides cryptography in support of remote administrative management via HTTPS. The cryptographic services provided by the TOE are described in Table 7 below.

Table 7 TOE Provided Cryptography

Cryptographic Method	Use within the TOE
RSA/DSA Signature Services	X.509 certificate signing

The TOE can also use the X.509v3 certificate for securing TLS sessions.

1.6.3 Full Residual Information Protection

The TOE ensures that all information flows from the TOE do not contain residual information from previous traffic. Residual data is never transmitted from the TOE.

1.6.4 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.

1.6.5 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:

- All TOE administrative users;
- All identification and authentication;
- All audit functionality of the TOE;
- All TOE cryptographic functionality;
- Update to the TOE; and
- TOE configuration

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.

1.6.6 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 CUCM is not a general-purpose operating system and access to Cisco CUCM memory space is restricted to only Cisco CUCM functions.

The TOE initially synchronizes time 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.

1.6.7 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 be configured to display an Authorized Administrator specified banner on the GUI management interface prior to accessing the TOE.

1.6.8 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. The TOE also allows secure communications between itself and a SIP Client and between itself and another SIP Server using TLS.

1.7 Excluded Functionality

The following functionality is excluded from the evaluation.

Table 8 Excluded Functionality

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

These services will be disabled by configuration. The exclusion of this functionality does not affect compliance to the U.S. Government Protection Profile for Security Requirements for Network Devices Version 1.1 or the Network Device Protection Profile Extended Package SIP Server Version 1.1.

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: September 2012. For a listing of Assurance Requirements claimed see section 5.5.

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 9 below:

Table 9 Protection Profiles

Protection Profile	Version	Date
Protection Profile for Network Devices (NDPP)	1.1	8 June 2012
Security Requirements for Network Devices Errata	#3	3 November 2014
Network Device Protection Profile Extended Package SIP Server (SIPEP)	1.1	5 November 2014

2.3 Protection Profile Conformance Claim Rationale

2.3.1 TOE Appropriateness

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

- Protection Profile for Network Devices, Version 1.1, including Errata #3
- Network Device Protection Profile Extended Package SIP Server, Version 1.1

2.3.2 TOE Security Problem Definition Consistency

The Assumptions, Threats, and Organizational Security Policies included in the Security Target represent the Assumptions, Threats, and Organizational Security Policies specified in the Protection Profile for Network Devices Version 1.1 and Network Device Protection Profile Extended Package SIP Server, Version 1.1 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 NDPPv1.1 and SIPEP v1.1 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 NDPPv1.1 and SIPEP v1.1 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 section 4.3 of the NDPPv1.1 and SIPEP v1.1.

3 SECURITY PROBLEM DEFINITION

This chapter 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 10 TOE Assumptions

Assumption	Assumption Definition
Reproduced from the NDPPv1.1	
A.NO_GENERAL_PURPOSE	It is assumed that 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.
A.PHYSICAL	Physical security, commensurate with the value of the TOE and the data it contains, is assumed to be provided by the environment.
A.TRUSTED_ADMIN	TOE Administrators are trusted to follow and apply all administrator guidance in a trusted manner.
Reproduced from the SIPEP v1.1	
A.NO_GENERAL_PURPOSE	It is assumed that 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.
A.PHYSICAL	Physical security, commensurate with the value of the TOE and the data it contains, is assumed to be provided by the environment.
A.TRUSTED_ADMIN	TOE Administrators are trusted to follow and apply all administrator guidance in a trusted manner.

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 11 Threats

Threat	Threat Definition
Reproduced from the NDPPv1.1	
T.ADMIN_ERROR	An administrator may unintentionally install or configure the TOE incorrectly, resulting in ineffective security mechanisms.
T.TSF_FAILURE	Security mechanisms of the TOE may fail, leading to a compromise of the TSF.

Threat	Threat Definition
T.UNDETECTED_ACTIONS	Malicious remote users or external IT entities may take actions that adversely affect the security of the TOE. These actions may remain undetected and thus their effects cannot be effectively mitigated.
T.UNAUTHORIZED_ACCESS	A user may gain unauthorized access to the TOE data and TOE executable code. A malicious user, process, or external IT entity may masquerade as an authorized entity in order to gain unauthorized access to data or TOE resources. A malicious user, process, or external IT entity may misrepresent itself as the TOE to obtain identification and authentication data.
T.UNAUTHORIZED_UPDATE	A malicious party attempts to supply the end user with an update to the product that may compromise the security features of the TOE.
T.USER_DATA_REUSE	User data may be inadvertently sent to a destination not intended by the original sender.
Reproduced from the SIPEP v1.1	
T.ADMIN_ERROR	An administrator may unintentionally install or configure the TOE incorrectly, resulting in ineffective security mechanisms.
T.TSF_FAILURE	Security mechanisms of the TOE may fail, leading to a compromise of the TSF.
T.UNDETECTED_ACTIONS	Malicious remote users or external IT entities may take actions that adversely affect the security of the TOE. These actions may remain undetected and thus their effects cannot be effectively mitigated.
T.UNAUTHORIZED_ACCESS	A user may gain unauthorized access to the TOE data and TOE executable code. A malicious user, process, or external IT entity may masquerade as an authorized entity in order to gain unauthorized access to data or TOE resources. A malicious user, process, or external IT entity may misrepresent itself as the TOE to obtain identification and authentication data.
T.UNAUTHORIZED_UPDATE	A malicious party attempts to supply the end user with an update to the product that may compromise the security features of the TOE.
T.USER_DATA_REUSE	User data may be inadvertently sent to a destination not intended by the original sender.

3.3 Organizational Security Policies

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

Table 12 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 Chapter 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.

This document identifies objectives of the TOE as O.objective with objective specifying a unique name. Objectives that apply to the IT environment are designated as OE.objective with objective specifying a unique name.

4.1 Security Objectives for the TOE

The following table, Security Objectives for the TOE, identifies the security objectives of the TOE. These security objectives reflect the stated intent to counter identified threats and/or comply with any security policies identified. An explanation of the relationship between the objectives and the threats/policies is provided in the rationale section of this document.

Table 13 Security Objectives for the TOE

TOE Objective	TOE Security Objective Definition
Reproduced from the NDPPv1.1	
O.PROTECTED_COMMUNICATIONS	The TOE will provide protected communication channels for administrators, other parts of a distributed TOE, and authorized IT entities.
O.VERIFIABLE_UPDATES	The TOE will provide the capability to help ensure that any updates to the TOE can be verified by the administrator to be unaltered and (optionally) from a trusted source.
O.SYSTEM_MONITORING	The TOE will provide the capability to generate audit data and send those data to an external IT entity.
O.DISPLAY_BANNER	The TOE will display an advisory warning regarding use of the TOE.
O.TOE_ADMINISTRATION	The TOE will provide mechanisms to ensure that only administrators are able to log in and configure the TOE, and provide protections for logged-in administrators.
O.RESIDUAL_INFORMATION_CLEARING	The TOE will ensure that any data contained in a protected resource is not available when the resource is reallocated.
O.SESSION_LOCK	The TOE shall provide mechanisms that mitigate the risk of unattended sessions being hijacked.
O.TSF_SELF_TEST	The TOE will provide the capability to test some subset of its security functionality to ensure it is operating properly.
Reproduced from the SIPEP v1.1	
O.PROTECTED_COMMUNICATIONS	The TOE will provide protected communication channels for administrators, other parts of a distributed TOE, and authorized IT entities.
O.VERIFIABLE_UPDATES	The TOE will provide the capability to help ensure that any updates to the TOE can be verified by the administrator to be unaltered and (optionally) from a trusted source.
O.SYSTEM_MONITORING	The TOE will provide the capability to generate audit data and send those data to an external IT entity.
O.DISPLAY_BANNER	The TOE will display an advisory warning regarding use of the TOE.

TOE Objective	TOE Security Objective Definition
O.TOE_ADMINISTRATION	The TOE will provide mechanisms to ensure that only administrators are able to log in and configure the TOE, and provide protections for logged-in administrators.
O.RESIDUAL_INFORMATION_CLEARING	The TOE will ensure that any data contained in a protected resource is not available when the resource is reallocated.
O.SESSION_LOCK	The TOE shall provide mechanisms that mitigate the risk of unattended sessions being hijacked.
O.TSF_SELF_TEST	The TOE will provide the capability to test some subset of its security functionality to ensure it is operating properly.

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 14 Security Objectives for the Environment

Environment Security Objective	IT Environment Security Objective Definition
Reproduced from the NDPPv1.1	
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.
OE.PHYSICAL	Physical security, commensurate with the value of the TOE and the data it contains, is provided by the environment.
OE.TRUSTED_ADMIN	TOE Administrators are trusted to follow and apply all administrator guidance in a trusted manner.
Reproduced from the SIPEP v1.1	
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.
OE.PHYSICAL	Physical security, commensurate with the value of the TOE and the data it contains, is provided by the environment.
OE.TRUSTED_ADMIN	TOE Administrators are trusted to follow and apply all administrator guidance in a trusted manner.

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 within brackets;
- Refinement: Indicated with **bold** text;
- Selection: Indicated with [<u>underlined</u>] text within brackets;
- Iteration: Indicated by appending the iteration number in parenthesis, e.g., (1), (2), (3).

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 NDPP.

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 15 Security Functional Requirements

Class Name	Component Identification	Component Name
Security Functional Requirements Drawn from NDPP		
FAU: Security audit	FAU_GEN.1	Audit data generation
	FAU_GEN.2	User Identity Association
	FAU_STG_EXT.1	External Audit Trail Storage
FCS: Cryptographic support	FCS_CKM.1	Cryptographic Key Generation (for asymmetric keys)
	FCS_CKM_EXT.4	Cryptographic Key Zeroization
	FCS_COP.1(1)	Cryptographic Operation (for data encryption/decryption)
	FCS_COP.1(2)	Cryptographic Operation (for cryptographic signature)
	FCS_COP.1(3)	Cryptographic Operation (for cryptographic hashing)
	FCS_COP.1(4)	Cryptographic Operation (for keyed-hash message authentication)
	FCS_HTTPS_EXT.1	Explicit: HTTPS
	FCS_RBG_EXT.1	Extended: Cryptographic Operation (Random Bit Generation)
	FCS_TLS_EXT.1	Explicit: TLS
FDP: User data protection	FDP_RIP.2	Full Residual Information Protection
	FIA_PMG_EXT.1	Password Management

Class Name	Component Identification	Component Name
FIA: Identification and authentication	FIA_PSK_EXT.1	Extended: Pre-Shared Key Composition
	FIA_UIA_EXT.1	User Identification and Authentication
	FIA_UAU_EXT.2	Password-based Authentication Mechanism
	FIA_UAU.7	Protected Authentication Feedback
FMT: Security management	FMT_MTD.1	Management of TSF Data (for general 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	Extended: Trusted Update
	FPT_TST_EXT.1	TSF Testing
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
Reproduced from the Network Device Protection Profile Extended Package SIP Server		
FCS: Cryptographic support	FCS_COP.1(1)	Cryptographic Operation (Data Encryption/Decryption)
	FCS_TLS_EXT.1	Transport Level Security
FIA: Identification and authentication	FIA_SIPS_EXT.1	Session Initiation Protocol (SIP) Server
	FIA_X509_EXT.1	Extended: X.509 Certificates
FMT: Security management	FMT_SMF.1	Specification of Management Functions
FPT: Protection of the TSF	FPT_TUD_EXT.1	Extended: Trusted Update
FTP: Trusted path/channels	FTP_ITC.1(2)	Inter-TSF Trusted Channel (TLS/SIP)
FTP: Trusted path/channels	FTP_ITC.1(3)	Inter-TSF Trusted Channel (Protection from Modification or Disclosure – SIP Server)

5.3 SFRs from NDPP and SIP Server EP

5.3.1 Security audit (FAU)

5.3.1.1 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 administrative actions;

d) [*Specifically defined auditable events listed in* **Table 16**].

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 16**].

Table 16 Auditable Events

SFR	Auditable Event	Additional Audit Record Contents
Audit Events and Details from NDPP		
FAU_GEN.1	None.	None.
FAU_GEN.2	None.	None.
FAU_STG_EXT.1	None.	None.
FCS_CKM.1	None.	None.
FCS_CKM_EXT.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 an HTTPS session. Establishment/Termination of an HTTPS session.	Reason for failure. Non-TOE endpoint of connection (IP address) for both successes and failures.
FCS_RBG_EXT.1	None.	None.
FCS_TLS_EXT.1	Failure to establish an TLS session Establishment/Termination of an TLS session.	Reason for failure. Non-TOE endpoint of connection (IP address) for both successes and failures.
FDP_RIP.2	None.	None.
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.
FMT_MTD.1	None.	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 (e.g., IP address).
FPT_TUD_EXT.1	Initiation of update.	No additional information.
FPT_TST_EXT.1	None.	None.
FTA_SSL_EXT.1	Any attempts at unlocking of an interactive session.	No additional information.
FTA_SSL.3	The termination of a remote session by the session locking mechanism.	No additional information.
FTA_SSL.4	The termination of an interactive session.	No additional information.
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.
Audit Events and Details from Network Device Protection Profile Extended Package SIP Server		
FCS_TLS_EXT.1	Session Establishment with peer	Source and destination addresses Source and destination ports

SFR	Auditable Event	Additional Audit Record Contents
		TOE Interface
FIA_X509_EXT.1	Establishing session with CA	Source and destination addresses Source and destination ports TOE Interface
FIA_SIPS_EXT.1	Session Establishment with peer	Source and destination addresses Source and destination ports TOE Interface

5.3.1.2 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.

5.3.1.3 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 implementing the [TLS/HTTPS] protocol.

5.3.2 Cryptographic Support (FCS)

5.3.2.1 FCS_CKM.1 Cryptographic Key Generation (for asymmetric keys)

FCS_CKM.1.1 Refinement: The TSF shall generate **asymmetric** cryptographic keys **used for key establishment** in accordance with

> [NIST Special Publication 800-56B, “Recommendation for Pair-Wise Key Establishment Schemes Using Integer Factorization Cryptography” for RSA-based key establishment schemes]

and specified cryptographic key sizes *equivalent to, or greater than, a symmetric key strength of 112 bits.*

5.3.2.2 FCS_CKM_EXT.4 Cryptographic Key Zeroization

FCS_CKM_EXT.4.1 The TSF shall zeroize all plaintext secret and private cryptographic keys and CSPs when no longer required.

5.3.2.3 FCS_COP.1(1) Cryptographic Operation (Data Encryption/Decryption)

FCS_COP.1.1 The TSF shall perform *encryption and decryption* in accordance with a specified cryptographic algorithm *AES operating in GCM*, [*CBC modes*] and cryptographic key sizes *128-bits, 256-bits*, and [*no other key sizes*] that meets the following:

- *FIPS PUB 197, "Advanced Encryption Standard (AES)"*
- [NIST SP 800-38A, NIST SP 800-38D]

5.3.2.4 FCS_COP.1(2) Cryptographic Operation (for cryptographic signature)

FCS_COP.1.1(2) Refinement: The TSF shall perform **cryptographic signature services** in accordance with a [RSA Digital Signature Algorithm (rDSA) with a key size (modulus) of 2048 bits or greater] that meets the following:

[Case: RSA Digital Signature Algorithm

- FIPS PUB 186-3, "Digital Signature Standard].

5.3.2.5 FCS_COP.1(3) Cryptographic Operation (for cryptographic hashing)

FCS_COP.1.1(3) Refinement: The TSF shall perform [*cryptographic hashing services*] in accordance with a specified cryptographic algorithm [SHA-1, SHA-256, SHA-384**] and message digest sizes [selection:** 160, 256, 384] **bits** that meet the following: *FIPS Pub 180-3, "Secure Hash Standard."*

5.3.2.6 FCS_COP.1(4) Cryptographic Operation (for keyed-hash message authentication)

FCS_COP.1.1(4) Refinement: The TSF shall perform [*keyed-hash message authentication*] in accordance with a specified cryptographic algorithm HMAC-[SHA-1, SHA-256, SHA-384], **key size** [160, 256, 384***) used in HMAC***], **and message digest sizes** [160, 256, 384] **bits** that meet the following: *FIPS Pub 198-1, "The Keyed-Hash Message Authentication Code", and FIPS Pub 180-3, "Secure Hash Standard."*

5.3.2.7 FCS_HTTPS_EXT.1 Explicit: HTTPS

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 as specified in FCS_TLS_EXT.1.

5.3.2.8 FCS_RBG_EXT.1 Extended: Cryptographic Operation (Random Bit Generation)

FCS_RBG_EXT.1.1 The TSF shall perform all random bit generation (RBG) services in accordance with [NIST Special Publication 800-90 using [CTR_DRBG (AES), Dual_EC_DRBG] seeded by an entropy source that accumulated entropy from [a software-based noise source].

FCS_RBG_EXT.1.2 The deterministic RBG shall be seeded with a minimum of [256 bits] of entropy at least equal to the greatest security strength of the keys and hashes that it will generate.

5.3.2.9 FCS_TLS_EXT.1 Explicit: TLS

FCS_TLS_EXT.1.1 The TSF shall implement one or more of the following protocols [TLS 1.0 (RFC 2246)] and TLS 1.2 (RFC 5246) using mutual authentication with certificates and supporting the following ciphersuites:

Mandatory Ciphersuites:
TLS_RSA_WITH_AES_128_CBC_SHA

Optional Ciphersuites:
[
TLS_RSA_WITH_AES_256_CBC_SHA
TLS_DHE_RSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256,
TLS_ECDHE_RSA_WITH _AES_256_GCM_SHA384,
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
].

5.3.3 User data protection (FDP)

5.3.3.1 FDP_RIP.2 Full Residual Information Protection

FDP_RIP.2.1 The TSF shall ensure that any previous information content of a resource is made unavailable upon the [deallocation of the resource from] all objects.

5.3.4 Identification and authentication (FIA)

5.3.4.1 FIA_PMG_EXT.1 Password Management

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

1. Passwords shall be able to be composed of any combination of upper and lower case letters, numbers, and the following special characters: [“!”, “@”, “#”, “$”, “%”, “^”, “&”, “*”, “(“,”)”, [*none*]];
2. Minimum password length shall settable by the Security Administrator, and support passwords of 15 characters or greater;

5.3.4.2 FIA_SIPS_EXT.1 Session Initiation Protocol (SIP) Server

FIA_SIPS_EXT.1.1 The TSF shall implement the Session Initiation Protocol (SIP) that complies with RFC 3261 using the Session Description Protocol (SDP) complying with RFC 4566 to describe the multimedia session that will be used to carry the VOIP traffic.

FIA_SIPS_EXT.1.2 The TSF shall require password authentication for SIP REGISTER function requests as specified in section 22 of RFC 3261.

FIA_SIPS_EXT.1.3 The TSF shall support SIP authentication passwords that contain at least [*8*] characters in the set of {upper case characters, lower case characters, numbers, and the following special characters: “!”, “@”, “#”, “$”, “%”, “^”, “&”, “*”, “(“, and “)”, and [*none*]}.

5.3.4.3 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.

5.3.4.4 FIA_UAU_EXT.2 Extended: 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.

5.3.4.5 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.

5.3.4.6 FIA_X509_EXT.1 Extended: X.509 Certificates

FIA_X509_EXT.1.1 The TSF shall use X.509v3 certificates as defined by RFC 5280 to support authentication for TLS connections.

FIA_X509_EXT.1.2 The TSF shall provide the capability for the Enterprise to load X.509v3 certificates into the TOE for use by the security functions specified in this PP.

FIA_X509_EXT.1.3 The TSF shall validate the certificate using [<u>Online Certificate Status Protocol (OCSP) as specified in RFC 2560</u>].

FIA_X509_EXT.1.4 The TSF shall not establish a TLS connection if a certificate is deemed invalid.

FIA_X509_EXT.1.5 When the TSF cannot establish a connection to determine the validity of a certificate, the TSF shall, as configured by the Enterprise, establish the TLS connection or disallow the establishment of the TLS connection.

FIA_X509_EXT.1.6 The TSF shall store and protect certificate(s) from unauthorized deletion and modification.

5.3.5 Security management (FMT)

5.3.5.1 FMT_MTD.1 Management of TSF Data (for general TSF data)

FMT_MTD.1.1 The TSF shall restrict the ability to *<u>manage</u>* the *TSF data* to the *Security Administrators*.

5.3.5.2 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 update the TOE, and to verify the updates using [<u>digital signature</u>] capability prior to installing those updates;*
- *Ability to configure the SIP;*
- *Ability to configure mechanisms implemented with respect to FCS_TLS_EXT.1;*
- *Ability to configure SIP client password;*
- *Ability to configure a notice and consent warning message for FTA_TAB.1.*
- *Ability to configure inactivity time period for local sessions time period for FTA_SSL_EXT.1.*
- *[<u>Ability to configure the cryptographic functionality</u>*

].

5.3.5.3 FMT_SMR.2 Restrictions on Security Roles

FMT_SMR.2.1 The TSF shall maintain the roles:

- **Authorized 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

- **Authorized Administrator role shall be able to administer the TOE locally;**
- **Authorized Administrator role shall be able to administer the TOE remotely;**

are satisfied.

5.3.6 Protection of the TSF (FPT)

5.3.6.1 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.

5.3.6.2 FPT_APW_EXT.1 Extended: 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.

5.3.6.3 FPT_STM.1 Reliable time stamps

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

5.3.6.4 FPT_TST_EXT.1: TSF Testing

FPT_TST_EXT.1.1 The TSF shall run a suite of self tests during initial start-up (on power on) to demonstrate the correct operation of the TSF.

5.3.6.5 FPT_TUD_EXT.1 Extended: Trusted Update

FPT_TUD_EXT.1.1 The TSF shall provide security administrators the ability to query the current version of the TOE firmware/software.

FPT_TUD_EXT.1.2 The TSF shall provide security administrators the ability to initiate updates to TOE firmware/software.

FPT_TUD_EXT.1.3 The TSF shall provide a means to verify firmware/software updates to the TOE using a digital signature mechanism and [no other functions] prior to installing those updates.

5.3.7 TOE Access (FTA)

5.3.7.1 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.

5.3.7.2 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*].

5.3.7.3 FTA_SSL.4 User-initiated Termination

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

5.3.7.4 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.

5.3.1 Trusted Path/Channels (FTP)

5.3.1.1 FTP_ITC.1(1) Inter-TSF trusted channel

FTP_ITC.1.1(1) Refinement: The TSF shall **use** [TLS/HTTPS] 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(1) The TSF shall permit *the TSF****, or the authorized IT entities*** to initiate communication via the trusted channel.

FTP_ ITC.1.3(1) The TSF shall initiate communication via the trusted channel for [*audit storage with syslog server (over TLS/HTTPS)*].

5.3.1.2 FTP_ITC.1(2) Inter-TSF Trusted Channel (TLS/SIP)

FTP_ITC.1.1(2) Refinement: The TSF shall provide a communication channel between itself and a SIP Client using TLS [and no other protocol] as specified in FCS_TLS_EXT.1 [only] that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification and ~~or~~ disclosure.

FTP_ITC.1.2(2) The TSF shall permit the TSF Client to initiate communication via the trusted channel.

FTP_ITC.1.3(2) The TSF Client shall initiate communication via the trusted channel for [*all communications with the SIP server*]**.**

5.3.1.3 FTP_ITC.1(3) Inter-TSF Trusted Channel (Protection from Modification or Disclosure – SIP Server)

FTP_ITC.1.1(3) Refinement: The TSF shall provide a communication channel between itself and another SIP Server using [TLS] that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification and disclosure.

FTP_ITC.1.2(3) The TSF shall permit the TOE or the peer SIP Server to initiate communication via the trusted channel.

FTP_ITC.1.3(3) The TSF shall initiate communication via the trusted channel [*to pass SIP data to a SIP Server Peer*].

5.3.1.4 FTP_TRP.1 Trusted Path

FTP_TRP.1.1 Refinement: The TSF shall **use** [TLS/HTTPS] provide a **trusted** communication path between itself and **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 detection of modification of the communicated data*.

FTP_TRP.1.2 Refinement: 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.*

5.4 TOE SFR Dependencies Rationale for SFRs Found in PP

The Security Functional Requirements (SFRs) in this Security Target represent the SFRs identified in the NDPPv1.1 and SIPEPv1.1. As such, the NDPP and SIPEP SFR dependency rationale is deemed acceptable since the PPs themselves have been validated.

5.5 Security Assurance Requirements

5.5.1 SAR Requirements

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

Table 17: Assurance Measures

Assurance Class	Components	Components Description
DEVELOPMENT	ADV_FSP.1	Basic Functional Specification
GUIDANCE DOCUMENTS	AGD_OPE.1	Operational user guidance
	AGD_PRE.1	Preparative User guidance
LIFE CYCLE SUPPORT	ALC_CMC.1	Labeling of the TOE
	ALC_CMS.1	TOE CM coverage
TESTS	ATE_IND.1	Independent testing - conformance
VULNERABILITY ASSESSMENT	AVA_VAN.1	Vulnerability analysis

5.5.2 Security Assurance Requirements Rationale

The Security Assurance Requirements (SARs) in this Security Target represent the SARs identified in the NDPPv1.1 and SIPEPv1.1. As such, the NDPP and SIPEP SAR dependency rationale is deemed acceptable since the PPs themselves have been validated.

5.6 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 18 Assurance Measures

Component	How requirement will be met
ADV_FSP.1	There are no specific assurance activities associated with ADV_FSP.1. The requirement on the content of the functional specification information is implicitly assessed by virtue of the other assurance activities being performed. The functional specification is comprised of the information contained in the AGD_OPE and AGD_PRE documentation, coupled with the information provided in the TSS of the ST. The assurance activities in the functional requirements point to evidence that should exist in the documentation and TSS section; since these are directly associated with the SFRs, the tracing in element ADV_FSP.1.2D is implicitly already done and no additional documentation is necessary.
AGD_OPE.1	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.
AGD_PRE.1	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.

Component	How requirement will be met
ALC_CMC.1	The AGD and ST implicitly meet this assurance requirement. The evaluator shall check the ST to ensure that it contains an identifier (such as a product name/version number) that specifically identifies the version that meets the requirements of the ST. Further, the evaluator shall check the AGD guidance and TOE samples received for testing to ensure that the version number is consistent with that in the ST.
ALC_CMS.1	
ATE_IND.1	Cisco provided the TOE for testing and, in coordination with the evaluation team, determined that the TOE was suitable for testing. All information provided met the requirements for content and presentation of evidence and testing was successfully completed based upon the requirements of the PP and extended package.
AVA_VAN.1	Cisco provided the TOE for testing and it was determined to be suitable for completion of the requirements. All information provided met the requirements for content and presentation of evidence. The evaluation team conducted a public search of potential vulnerabilities and ensured no issues resulted in a potential risk to the end user(s).

6 TOE SUMMARY SPECIFICATION

6.1 TOE Security Functional Requirement Measures

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

Table 19 How TOE SFRs are Met

TOE SFRs	How the SFR is Met
Security Functional Requirements Drawn from NDPP	
FAU_GEN.1	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, events related to SIP connections, identification and authentication related events, and administrative events (the specific events and the contents of each audit record are listed in Table 16. 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. Audit event logging is centralized and enabled by default. An alarm monitor called Syslog Audit writes the logs. By default, the logs are configured to rotate. 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. Example audit events are included below: 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: User ID: CCMAdministratorClient IP Address: 172.19.240.207 Severity: 3 EventType: ServiceStatusUpdated ResourceAccessed: CCMService EventStatus: Successful Description: CallManager Service status is stopped Audit event logging - An audit event represents any event that is required to be logged. The following example displays a sample audit event: CCM_TOMCAT-GENERIC-3-AuditEventGenerated: Audit Event Generated UserID:CCMAdministrator Client IP Address:172.19.240.207 Severity:3 EventType:ServiceStatusUpdated ResourceAccessed: CCMService EventStatus:Successful Description: Call Manager

<table>
<tr><th>TOE SFRs</th><th>How the SFR is Met</th></tr>
<tr><td></td><td>
Service status is stopped App ID:Cisco Tomcat Cluster ID:StandAloneCluster Node ID:sa-cm1-3
(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)
<table>
<tr><th>Auditable Event</th><th>Sample Audit Record</th><th>Rationale</th></tr>
<tr><td>All use of the user identification mechanism.</td><td rowspan="2">05/04/2015 17:54:01.881, acumenadmin, 192.168.50.60, Info, UserLogging, Cisco CallManager Administration, Success, No, AdministrativeEvent, Cisco CCM Application, Successfully Logged into Cisco CCM Webpages, Cisco Tomcat, , CUCM1, 0
05/04/2015 19:39:00.331, acumenadmin, 192.168.50.60, Info, UserLogging, CUCMAdmin, Success, No, CriticalEvent, Cisco CUCM Administration, Successfully Logged out Cisco CCM Web Pages, Cisco Tomcat, , CUCM1, 15
05/04/2015 22:09:56.498, acumensec, 192.168.50.60, Warning, UserLogging, Cisco CallManager Administration, Failure, No, AdministrativeEvent, Cisco CCM Application, Failed to Log into Cisco CCM Webpages, Cisco Tomcat, , CUCM1, 16</td><td>Events will be generated for attempted identification/ authentication, and the username attempting to authenticate and source address or interface will be included in the log record.</td></tr>
<tr><td>Any use of the authentication mechanism.</td><td>Events will be generated for attempted identification/ authentication, and the username attempting to authenticate will be included in the log record, along with the origin or source of the attempt.</td></tr>
<tr><td>Management functions</td><td>05/04/2015 19:08:59.564, acumenadmin, 192.168.50.60, Notice, UserRoleMembershipUpdate, CUCMAdmin, Success, No, AdministrativeEvent, Cisco CUCM Administration, End user acumensec added to usergroup Standard CCM End Users, Cisco Tomcat, , CUCM1, 12
05/04/2015 22:18:41.070, acumenadmin, 192.168.50.60, Notice, DeviceUpdate, CUCMAdmin, Success, No,</td><td>The use of the security management functions is logged; modifications of the behavior of the functions in the TSF and modifications of default settings.</td></tr>
</table>
</td></tr>
</table>

TOE SFRs	How the SFR is Met		
		AdministrativeEvent, Cisco CUCM Administration, New Phone added with MAC address=UPCDIVICE , CAL mode=< None > and CAL value=< None >, Cisco Tomcat, , CUCM1, 21 05/04/2015 22:55:44.631, acumenadmin, 192.168.50.60, Info, GeneralConfigurationUpdate, CUCMServiceability, Success, No, AdministrativeEvent, Cisco CCM Servicability, Cisco Location Bandwidth Manager Was Activated on node CUCM1, Cisco Tomcat, , CUCM1, 35	
	Changes to the time.	Dec 17 16:22:23 ryhooper-cucm-dev Info ntpd : synchronized to 10.122.81.30, stratum 11 Dec 18 02:19:53 ryhooper-cucm-dev Notice ntpd : time reset +35850.207006 s Dec 18 02:19:53 ryhooper-cucm-dev Notice ntpd : kernel time sync status change 2001 Dec 18 02:20:56 ryhooper-cucm-dev Info ntpd : synchronized to 10.122.81.30, stratum 11	Changes to the time are logged.
	Failure to establish and/or establishment/termination of a TLS session	: 6: dchokshi-cucm1.cisco.com Dec 16 2014 15:12:10 UTC : %UC_CALLMANAGER-6-EndPointRegistered: %[DeviceName=SEP001B545235C9][IPAddress=10.116.81.152][Protocol=SIP][DeviceType=119][PerfMonObjType=2][Description=SEP001B545235C9][LoadID=SIP70.9-4-2-1S][AssociatedDNs=2002][MACAddress=001B545235C9][IPAddrAttributes=0][ActiveLoadId=SIP70.9-4-2-1S][ClusterID=StandAloneCluster][NodeID=dchokshi-cucm1]: Endpoint registered : 7: dchokshi-cucm1.cisco.com Dec 16 2014 15:12:10 UTC : %UC_CALLMANAGER-6-DeviceDnInformation:	Attempts to establish a TLS session or the failure to establish a TLS session is logged as well as successfully established and terminated TLS sessions.

TOE SFRs	How the SFR is Met		
		%[DeviceName=SEP001B545235C9][DeviceType=119][StationDesc=SEP001B545235C9][StationDn=2002][ClusterID=StandAloneCluster][NodeID=dchokshi-cucm1]: List of directory numbers (DN) associated with this device Dec 16 10:34:42 dchokshi-cucm1 local7 3 : 18: dchokshi-cucm1.cisco.com: Dec 16 2014 15:34:42.155 UTC : %UC_CALLMANAGER-3-ServicePortOnline: %[Protocol=Secure SCCP][PortNumber=2443][AppID=Cisco CallManager][ClusterID=StandAloneCluster][NodeID=dchokshi-cucm1]: A Cisco CallManager service port is online	
	Failure to establish and/or establishment/termination of a HTTPS session	11:51:57.849 |LogMessage UserID : appadmin ClientAddress : 10.116.81.148 Severity : 3 EventType : UserLogging ResourceAccessed: Cisco CallManager Serviceability RTMT Servlet EventStatus : Success CompulsoryEvent : No AuditCategory : AdministrativeEvent ComponentID : Cisco CCM Application AuditDetails : Login Authentication Successful App ID: Cisco Tomcat Cluster ID: Node ID: dchokshi-cucm1 12:11:31.121 |LogMessage UserID : fakeuser ClientAddress : 10.116.81.148 Severity : 3 EventType : UserLogging ResourceAccessed: Cisco CallManager Serviceability RTMT Servlet EventStatus : Failure CompulsoryEvent : No AuditCategory : AdministrativeEvent ComponentID : Cisco CCM Application AuditDetails : Login Authentication Failed App ID:	Attempts to establish a HTTPS session or the failure to establish a HTTPS session is logged as well as successfully established and terminated HTTPS sessions.

TOE SFRs	How the SFR is Met		
		Cisco Tomcat Cluster ID: Node ID: dchokshi-cucm1	
	Session Establishment with peer (TLS)	11:51:57.849 |LogMessage UserID : appadmin ClientAddress : 10.116.81.148 Severity : 3 EventType : UserLogging ResourceAccessed: Cisco CallManager Serviceability RTMT Servlet EventStatus : Success CompulsoryEvent : No AuditCategory : AdministrativeEvent ComponentID : Cisco CCM Application AuditDetails : Login Authentication Successful App ID: Cisco Tomcat Cluster ID: Node ID: dchokshi-cucm1 12:11:31.121 |LogMessage UserID : fakeuser ClientAddress : 10.116.81.148 Severity : 3 EventType : UserLogging ResourceAccessed: Cisco CallManager Serviceability RTMT Servlet EventStatus : Failure CompulsoryEvent : No AuditCategory : AdministrativeEvent ComponentID : Cisco CCM Application AuditDetails : Login Authentication Failed App ID: Cisco Tomcat Cluster ID: Node ID: dchokshi-cucm1	The establishment of a TLS session is logged
	Session Establishment with peer (SIP)	00162750.001 |13:23:05.002 |AppInfo |SIPTcp - wait_SdlSPISignal: Outgoing SIP TCP message to 10.116.81.152 on port 53092 index 5 00162756.002 |13:23:06.221 |AppInfo |SIPTcp - wait_SdlReadRsp: Incoming SIP TCP message from 10.116.81.152 on port 53092 index 5 with 1478 bytes: 00162891.031 |13:23:07.301 |AppInfo |//SIP/SIPHandler/ccbId=1677/scbId=0/insertContactIntoContainer: Outgoing Contact=[<sip:2002@10.122.81.3:5061;transport=tls>]	The establishment of a SIP session is logged

TOE SFRs	How the SFR is Met		
	Establishing session with CA	05/04/2015 22:55:44.644, acumenadmin, 192.168.50.60, Info, GeneralConfigurationUpdate, CUCMServiceability, Success, No, AdministrativeEvent, Cisco CCM Servicability, Self Provisioning IVR Was Activated on node CUCM1, Cisco Tomcat, , CUCM1, 43 05/04/2015 22:55:44.649, acumenadmin, 192.168.50.60, Info, GeneralConfigurationUpdate, CUCMServiceability, Success, No, AdministrativeEvent, Cisco CCM Servicability, Cisco Certificate Authority Proxy Function Was Activated on node CUCM1, Cisco Tomcat, , CUCM1, 52	The connection to CA's for the purpose of certificate verification is logged.
	Indication that TSF self-test was completed.	The status of startup operation is currently being audited as syslog entries. Examples are pasted below: Sep 4 17:56:30 Infy-S64-cucm6 local7 2 : 7: Infy-S64-cucm6.cisco.com: Sep 04 2014 12:26:30.313 UTC : %UC_SERVICEMANAGER-2-ServiceFailed: %[ServiceName=Cisco CallManager Admin][Reason=Service stopped abruptly][AppID=Cisco Service Manager][ClusterID=][NodeID=Infy-S64-cucm6]: Service terminated. Sep 4 17:56:30 Infy-S64-cucm6 local7 6 : 8: Infy-S64-cucm6.cisco.com: Sep 04 2014 12:26:30.314 UTC : %UC_GENERIC-6-ServiceStarted: %[ServiceName=Cisco Trust Verification Service][ProcessID=25112][AppID=Cisco Service Manager][ClusterID=][NodeID=Infy-S64-cucm6]: Service started.	During bootup, if the self-test fails, the failure is logged.

TOE SFRs	How the SFR is Met		
		1411760392262,0,CiscoSystemInDemo, Reason : CiscoSystemInDemo AppID : Cisco License Manager ClusterID : NodeID : Infy-S64-cucm6 TimeStamp : Sat Sep 27 01:09:37 IST 2014. The alarm is generated on Sat Sep 27 01:09:37 IST 2014., ,4,1, ,Infy-S64-cucm6.cisco.com,UCM 1412017344060,1,AuthenticationFailed, Number of AuthenticationFailed events exceeds configured threshold during configured interval of time 1 within 3 minutes on cluster StandAloneCluster. There are 2 AuthenticationFailed events (up to 30) received during the monitoring interval From Tue Sep 30 00:31:24 IST 2014 to Tue Sep 30 00:34:24 IST 2014: TimeStamp : 9/30/14 12:31 AM LoginFrom : 10.106.211.201 Interface : Cisco RTMT Reporter Servlet UserID : CUCService AppID : Cisco Tomcat ClusterID : NodeID : Infy-S64-cucm6 TimeStamp : Tue Sep 30 00:31:59 IST 2014 TimeStamp : 9/30/14 12:31 AM LoginFrom : 10.106.211.201 Interface : Cisco RTMT Reporter Servlet UserID : CUCService AppID : Cisco Tomcat ClusterID : NodeID : Infy-S64-cucm6 TimeStamp : Tue Sep 30 00:31:28 IST 2014 , ,2,0, , ,System	
	Initiation of update	16:43:21.574 |LogMessage UserID : admin ClientAddress : 10.77.25.43 Severity : 6 EventType : CLICommand ResourceAccessed: GenericCLI EventStatus : Success CompulsoryEvent : No AuditCategory : AdministrativeEvent ComponentID : CLI AuditDetails : utils system upgrade status Command status= App ID:	Audit event is generated for the initiation of a software update.

TOE SFRs	How the SFR is Met		
		Command Line Cluster ID: Node ID: infyvoscm30-lnx	
	Any attempts at unlocking of an interactive session.	This requirement is satisfied based on CUCM does not provide the ability to 'lock' the admin's session. The sessions are terminated when the admin logs-out or session is terminated due to inactivity. The admin must re-establish the session and log-on to gain access. We will reference the FIA audit logs.	Audit event is generated after a user's session is locked and the admin user is required to re-authenticate.
	Once a remote interactive session is terminated after a Security Administrator-configurable time interval of session inactivity.	16:50:45.034 |LogMessage UserID : admin ClientAddress : 10.77.24.223 Severity : 6 EventType : UserLogging ResourceAccessed: CUCMAdmin EventStatus : Success CompulsoryEvent : No AuditCategory : CriticalEvent ComponentID : Cisco CUCM Administration AuditDetails : Successfully Logged out Cisco CCM Web Pages App ID: Cisco Tomcat Cluster ID: Node ID: infyvoscm28-lnx	An audit event is generated by when sessions are terminated after exceeding the inactivity settings.
	The termination of an interactive session.	15:46:35.085 |LogMessage UserID : admin ClientAddress : 10.77.24.223 Severity : 6 EventType : UserLogging ResourceAccessed: CUCMAdmin EventStatus : Success CompulsoryEvent : No AuditCategory : CriticalEvent ComponentID : Cisco CUCM Administration AuditDetails : Successfully Logged out Cisco CCM Web Pages App ID: Cisco Tomcat Cluster ID: Node ID: infyvoscm28-lnx	An audit event is generated by an authorized administrator when the exit command is used.
	Initiation of the trusted channel/ path. Termination of the trusted channel/ path.	11:51:57.849 |LogMessage UserID : appadmin ClientAddress : 10.116.81.148 Severity : 3 EventType : UserLogging ResourceAccessed: Cisco CallManager Serviceability RTMT Servlet EventStatus : Success CompulsoryEvent : No AuditCategory : AdministrativeEvent	Also see the rows for TLS above.

<table>
<tr><th>TOE SFRs</th><th>How the SFR is Met</th></tr>
<tr><td></td><td>
<table>
<tr><td>Failure of the trusted channel/ path functions.</td><td>ComponentID : Cisco CCM Application AuditDetails : Login Authentication Successful App ID: Cisco Tomcat Cluster ID: Node ID: dchokshi-cucm1

12:11:31.121 |LogMessage UserID : fakeuser ClientAddress : 10.116.81.148 Severity : 3 EventType : UserLogging ResourceAccessed: Cisco CallManager Serviceability RTMT Servlet EventStatus : Failure CompulsoryEvent : No AuditCategory : AdministrativeEvent ComponentID : Cisco CCM Application AuditDetails : Login Authentication Failed App ID: Cisco Tomcat Cluster ID: Node ID: dchokshi-cucm1</td><td></td></tr>
</table>
</td></tr>
<tr><td>FAU_GEN.2</td><td>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.

See sample records above</td></tr>
<tr><td>FAU_STG_ EXT.1</td><td>Using Cisco Unified Real-Time Monitoring Tool (RTMT), which runs as a client-side application, monitors the real-time behaviour of CUCM and components.

RTMT is also used to review and collect the log files from CUCM and store them to a remote server. Log Partition Monitoring (LPM), which is installed automatically with the CUCM, 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 CUCM.
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:
• LogPartitionLowWaterMarkExceeded (% disk space): When the disk usage is above the percentage that you specify, LPM sends out an alarm message to syslog and an alert to RTMT Alert central. To save the log files and regain disk space, you can use trace and log central option in RTMT.
• LogPartitionHighWaterMarkExceeded (% disk space): When the disk usage is above the percentage that you specify, LPM sends an alarm message to syslog and an alert to RTMT Alert central.
• SparePartitionLowWaterMarkExceeded (% disk space): When the disk usage is above the percentage that you specify, LPM sends out an alarm message to</td></tr>
</table>

TOE SFRs	How the SFR is Met
	syslog and an alert to RTMT Alert central. To save the log files and regain disk space, you can use trace and log central option in RTMT. • SparePartitionHighWaterMarkExceeded (% disk space): When the disk usage is above the percentage that you specify, LPM sends a n alarm message to syslog and an alert to RTMT Alert central. 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 and generates a corresponding alert in RTMT Alert central. If the percentage of disk usage is above the high water mark that you configured, the system sends an alarm message to syslog, generates a corresponding alert in RTMT Alert Central, and automatically purges log files until the value reaches the low water mark. Unified RTMT uses HTTPS for a secure connection to CUCM.
FCS_CKM.1	The TOE implements a random number generator for RSA key establishment schemes (conformant to NIST SP 800-56B). The TOE can also use the X.509v3 certificate for securing TLS and SIP sessions.
FCS_CKM_ EXT.4	The TOE meets all requirements specified in FIPS 140-2 for destruction of keys and Critical Security Parameters (CSPs) in that none of the symmetric keys, pre-shared keys, or private keys are stored in plaintext form.. See Table 20: TOE Key Zeroization for more information on the key zeroization.
FCS_COP.1(1)	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. Through the implementation of the cryptographic module, the TOE provides AES encryption and decryption in support of and TLS for secure communications. 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.
FCS_COP.1(2)	The TOE provides cryptographic signature services using RSA Digital Signature Algorithm with key size of 2048 and greater as specified in FIPS PUB 186-3, “Digital Signature Standard” and FIPS PUB 186-2, “Digital Signature Standard”. 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.

FCS_COP.1(3)
FCS_COP.1(4)
	The TOE provides cryptographic hashing services using SHA-1, SHA-256 and SHA-384 as specified in FIPS Pub 180-3 “Secure Hash Standard.”
	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.

TOE SFRs	How the SFR is Met
	The TOE provides the SHS hashing option in support of SSHv2 key establishment. SHS hashing and HMAC message authentication (SHA-1, SHA-256, SHA-384) is used in the establishment of TLS sessions.
FCS_RBG_EXT.1	The TOE is hardware and software comprised of the CUCM OS software image Release 11.0 and the hardware as described Table 5 Hardware Models and Specifications. 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
FCS_HTTPS_EXT.1 FCS_TLS_EXT.1	TLS v1.2 is used to protect the TLS sessions with the TOE for administration management, which supports the mandatory ciphersuites as well as the following optional ciphersuites: Mandatory Ciphersuites: TLS_RSA_WITH_AES_128_CBC_SHA Optional Ciphersuites: TLS_RSA_WITH_AES_256_CBC_SHA TLS_DHE_RSA_WITH_AES_128_CBC_SHA For the SIP connections, TLS v1.2 is supported with the following ciphersuites: TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256, TLS_ECDHE_RSA_WITH _AES_256_GCM_SHA384, TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
FDP_RIP.2	The TOE ensures that packets transmitted from the TOE do not contain residual information from data allocated to or deallocated from previous packets. Residual data is never transmitted from the TOE. Once packet handling is completed its content is zeroized (overwritten with 0x00) before allocation to or deallocation from the memory buffer which previously contained the packet is reused. This applies to administrative session traffic.
FIA_PMG_EXT.1	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: "!", "@", "#", "$", "%", "^", "&", "*", "(", and ")". Minimum password length is settable by the Authorized Administrator, and can be configured for minimum password lengths of 15 characters. The administrator accesses the TOE through the GUI via HTTPS/TLS. 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.

TOE SFRs	How the SFR is Met
FIA_SIPS_EXT.1	The TOE requires the SIP register connection to be authenticated with password credentials. 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: “!”, “@”, “#”, “$”, “%”, “^”, “&”, “*”, “(“, and “)”. Minimum password length is settable by the Authorized Administrator, and can be configured for minimum password lengths of 8 characters.
FIA_UIA_EXT.1 FIA_UAU_EXT.2	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. The TOE provides a local password based authentication mechanism. The process for authentication is the same for administrative access whether administration is occurring via a directly connected console cable or remotely via HTTPS/TLS. At initial login in 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.
FIA_UAU.7	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.
FIA_X509_EXT.1	The TOE uses X.509v3 certificates as defined by RFC 5280 to support authentication for TLS connections. 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 verifications process would show that the certificate had been tampered with when the hash value would be invalid. The physical security of the CUCM (A.Physical) protects the UCUM 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. Furthermore, the certificates are stored in a hidden and protected directory on the TOE that has no external interfaces to gain access. OCSP is used for certificate validation.
FMT_MTD.1	The TOE provides the ability for Authorized Administrators to access TOE data, such as audit data, configuration data, security attributes, login banners, and SIP connections via the GUI. The term “Authorized Administrator” is used in this ST to refer to any user which is permitted to perform the relevant action.
FMT_SMF.1	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/TLS to perform these functions or at the local console. The specific management capabilities available from the TOE include: • Local and remote administration of the TOE and the services provided by the TOE via the TOE GUI as described above;

TOE SFRs	How the SFR is Met
	• The ability to update the CUCM software (image integrity verification is provided using digital signature) • Ability to configure the cryptographic functionality; • Ability to configure the TLS functionality, • Ability to configure SIP functionality, • Ability to configure a notice and consent warning message • Ability to configure inactivity time period • Ability to enable, disable, determine and modify the behaviour of all the security functions of the TOE
FMT_SMR.2	The term "Authorized Administrator" is used in this ST to refer to any user which is permitted to perform the relevant action. The TOE supports both local administration via a directly connected console and remote authentication via TLS/HTTPS.
FPT_SKP_EXT.1	The TOE stores all private keys in a secure directory that is not readily accessible to administrators.
FPT_APW_EXT.1	The TOE ensures that plaintext user passwords will not be disclosed even to administrators.
FPT_STM.1	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. Following are a few additional reasons why an accurate and reliable time stamp on CUCM: • It allows Cisco IP Phones to display the correct date and time to the users • It assigns the correct date and time to voicemail tags. • It gives accurate times on Call Detail Records (CDR), which are used to track calls on the network. In the evaluated configuration, NTP server(s) is required for the TOE to synchronizes the time-stamp. It is recommended that more than one NTP server is configured to support the various clusters and time zones. The NTP server time synchronization is critical to ensure IP phones that rely on CUCM SIP Server receive a reliable time stamp. NTP uses Coordinated Universal Time (UTC) to synchronize computer clock times to a millisecond, and sometimes to a fraction of a millisecond[1]. For this reason, using NTP to synchronize the timestamp always has a more accurate time clock than a manually set clock. Likewise, the TOE and all associated IP Phones on the network will have the exact same time.
FPT_TUD_EXT.1	The TOE has specific versions that can be queried by an administrator. When updates are made available by Cisco, an administrator can obtain and install those updates. The software has been digitally signed. 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. The TOE files include the software authentication information, such as the image credentials, signing information and type of keys used for verification. During the

[1] http://searchnetworking.techtarget.com/definition/Network-Time-Protocol

TOE SFRs	How the SFR is Met
	validation process if the signature or the file itself has been tampered with, the hash value would be invalid. 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).
FPT_TST_EXT.1	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. If any of the tests fail, the TOE will not boot and the Authorized Administrator is instructed to contact Cisco Technical Assistance Center (TAC).
FTA_SSL_EXT.1 FTA_SSL.3	An administrator can configure maximum inactivity times.
FTA_SSL.4	An administrator is able to exit out of both local and remote administrative sessions.
FTA_TAB.1	The TOE can be configured to display a customized login message on the GIU management interface prior to allowing any administrative access to the TOE. This is applicable for both local and remote TOE administration.
FTP_ITC.1(1)	The TOE protects communications between the TOE and the remote audit server using TLS that provides a secure channel to transmit the log events.
FTP_ITC.1(2)	The TOE protects communications between the TOE and SIP Client using TLS that provides a secure communication channel to send and receive calls.
FTP_ITC.1(3)	The TOE protects communications between the TOE and SIP Server using TLS that provides a secure communication channel to pass SIP data.
FTP_TRP.1	All remote administrative communications take place over a secure encrypted HTTPS/TLS session. The remote users are able to initiate HTTPS/TLS communications with the TOE.

7 ANNEX A: KEY ZEROIZATION

7.1 Key Zeroization

The following table describes the key zeroization referenced by FCS_CKM_EXT.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 20: TOE Key Zeroization

Name	**Description**	**Zeroization**
User Password	Shared Secret (8-25 characters); used to authenticate the user	Overwrite with new password (NVRAM)
TLS server private key	RSA (1024/1536/2048 bit); Private key used for SSLv3.1/TLS	CLI command zeroize RSA (NVRAM) Command: crypto key zeroise verify with command: show crypto key mypubkey all
TLS server public key	RSA (1024/2048/3072 bit); Public key used for SSLv3.1/TLS	CLI command zeroize RSA (NVRAM) Command: crypto key zeroise verify with command: show crypto key mypubkey all
TLS pre-master secret	Shared Secret (384-bits); Shared Secret created using asymmetric cryptography from which new TLS session keys can be created	Automatically after TLS session terminated. (SDRAM)
TLS session encryption key	Triple-DES (168-bits/AES (128/196/256-bits); Key used to encrypt TLS session data	Automatically after TLS session terminated. (SDRAM)
TLS session integrity key	HMAC-SHA-1 (160-bits); HMAC-SHA-1 used for TLS data integrity protection	Automatically after TLS session terminated. The entire object is overwritten by 0's. Overwritten with: 0x00 (SDRAM)

8 ANNEX B: REFERENCES

The following documentation was used to prepare this ST:

Table 21: 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
[NDPP]	Protection Profile for Network Devices, version 1.1, June 8, 2012
[SIP EP]	Network Device Protection Profile Extended Package SIP Server, version 1.1, 5 November 2014
[800-38A]	NIST Special Publication 800-38A Recommendation for Block 2001 Edition Recommendation for Block Cipher Modes of Operation Methods and Techniques December 2001
[800-56A]	NIST Special Publication 800-56A, March, 2007 Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography (Revised)
[800-56B]	NIST Special Publication 800-56B Recommendation for Pair-Wise, August 2009 Key Establishment Schemes Using Integer Factorization Cryptography
[FIPS 140-2]	FIPS PUB 140-2 Federal Information Processing Standards Publication Security Requirements for Cryptographic Modules May 25, 2001
[FIPS PUB 186-2]	FIPS PUB 186-2 Federal Information Processing Standards Publication 2000 January 27
[FIPS PUB 186-3]	FIPS PUB 186-3 Federal Information Processing Standards Publication Digital Signature Standard (DSS) June, 2009
[FIPS PUB 198-1]	Federal Information Processing Standards Publication The Keyed-Hash Message Authentication Code (HMAC) July 2008
[800-90]	NIST Special Publication 800-90A Recommendation for Random Number Generation Using Deterministic Random Bit Generators January 2012
[FIPS PUB 180-3]	FIPS PUB 180-3 Federal Information Processing Standards Publication Secure Hash Standard (SHS) October 2008