# National Information Assurance Partnership

# Common Criteria Evaluation and Validation Scheme


# Validation Report

# for the

# Cisco Unified Communications Manager (CUCM) 12.5, Version 1.0

**Report Number:** CCEVS-VR-VID11092-2020

**Dated:** 12/16/2020

**Version:** 1.0

**National Institute of Standards and Technology**
**Information Technology Laboratory**
**100 Bureau Drive**
**Gaithersburg, MD 20899**

**National Security Agency**
**Information Assurance Directorate**
**9800 Savage Road STE 6740**
**Fort George G. Meade, MD 20755-6740**

# ACKNOWLEDGEMENTS


## Validation Team

Jean Petty: Senior Validator

Patrick Mallett PhD: Lead Validator

Randy Heimann: Lead Validator (Trainee)
*The MITRE Corporation*

## Common Criteria Testing Laboratory

Minal Wankhede

Kamlesh Ahuja

Ken Lasoski

*Acumen Security, LLC*

# Table of Contents

# 1 Executive Summary

This Validation Report (VR) is intended to assist the end user of this product and any Security Certification Agent for that end user in determining the suitability of this Information Technology (IT) product for their environment. End users should review the Security Target (ST), which is where specific security claims are made, in conjunction with this VR, which describes how those security claims were tested, evaluated, and any restrictions on the evaluated configuration. Prospective users should carefully read the Assumptions and Clarification of Scope in Section 5, and the Validator Comments in Section 10, where any restrictions on the evaluated configuration are highlighted.

This report documents the National Information Assurance Partnership (NIAP) assessment of the evaluation of the Cisco Unified Communications Manager 12.5 Series Target of Evaluation (TOE). It presents the evaluation results, their justifications, and the conformance results. This VR is not an endorsement of the TOE by any agency of the U.S. Government and no warranty of the TOE is either expressed or implied. This VR applies only to the specific version and configuration of the product as evaluated and documented in the ST.

The evaluation was completed by Acumen Security in December 2020. The information in this report is derived from the Evaluation Technical Report (ETR) and associated test report, all written by Acumen Security. The evaluation determined that the product is both Common Criteria Part 2 Extended and Part 3 Conformant and meets the assurance requirements defined in the collaborative Protection Profile for Network Devices (NDcPP), Version 2.1 and Network Device Collaborative Protection Profile (NDcPP) Extended Package Enterprise Session Controller (ESC EP), Version 1.0.

The Target of Evaluation (TOE) identified in this Validation Report has been evaluated at a NIAP approved Common Criteria Testing Laboratory using the Common Methodology for IT Security Evaluation (Version 3.1, Rev. 5) for conformance to the Common Criteria for IT Security Evaluation (Version 3.1, Rev. 5), as interpreted by the Assurance Activities contained in the collaborative Protection Profile for Network Devices (NDcPP), Version 2.1 and Network Device Collaborative Protection Profile (NDcPP) Extended Package Enterprise Session Controller (ESC EP), version 1.0.

This Validation Report applies only to the specific version of the TOE as evaluated. The evaluation has been conducted in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme and the conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence provided.

The validation team provided guidance on technical issues and evaluation processes and reviewed the individual work units documented in the ETR and the Assurance Activities Report (AAR). The validation team found that the evaluation showed that the product satisfies all of the functional requirements and assurance requirements stated in the Security Target (ST). Based on these findings, the validation team concludes that the testing laboratory's findings are accurate, the conclusions justified, and the conformance results are correct. The conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence produced.

# 2 Identification

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards effort to establish commercial facilities to perform trusted product evaluations. Under this program, security evaluations are conducted by commercial testing laboratories called Common Criteria Testing Laboratories (CCTLs). CCTLs evaluate products against Protection Profiles which contain Assurance Activities, which are interpretations of CEM work units specific to the technology described by the PP.

The NIAP Validation Body assigns Validators to monitor the CCTLs to ensure quality and consistency across evaluations. Developers of information technology products desiring a security evaluation contract with a CCTL and pay a fee for their product's evaluation. Upon successful completion of the evaluation, the product is added to NIAP's Product Compliance List.

Table 1 provides information needed to completely identify the product, including:

- The Target of Evaluation (TOE): the fully qualified identifier of the product as evaluated.
- The Security Target (ST), describing the security features, claims, and assurances of the product.
- The conformance result of the evaluation.
- The Protection Profile(s) to which the product is conformant.
- The organizations and individuals participating in the evaluation.

**Table 1: Evaluation Identifiers**

| Item | Identifier |
|---|---|
| **Evaluation Scheme** | United States NIAP Common Criteria Evaluation and Validation Scheme |
| **TOE** | Cisco Unified Communications Manager 12.5 |
| **Protection Profile** | collaborative Protection Profile for Network Devices (NDcPP), Version 2.1 and Network Device Collaborative Protection Profile (NDcPP) Extended Package Enterprise Session Controller (ESC EP), Version 1.0. |
| **Security Target** | Cisco Unified Communications Manager 12.5 Common Criteria Security Target Version 1.3, 10 December 2020. |
| **Evaluation Technical Report** | Evaluation Technical Report for Cisco Unified Communication Manager (CUCM) 12.5 Version 1.0 |
| **CC Version** | Version 3.1, Revision 5 |
| **Conformance Result** | CC Part 2 Extended and CC Part 3 Conformant |
| **Sponsor** | Cisco Systems, Inc. |
| **Developer** | Cisco Systems, Inc. |
| **Common Criteria Testing Lab (CCTL)** | Acumen Security<br>2400 Research Blvd, Rockville MD 20850 |
| **CCEVS Validators** | Jean Petty, Randy Heimann, Patrick Mallett |

# 3 Architectural Information

The TOE is Cisco Unified Communications Manager (CUCM) v12.5. The TOE is a 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 which includes 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.

# 4 Security Policy

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

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

These features are described in more detail in the subsections below. In addition, the TOE implements all RFCs of the NDcPP v2.1 and ESC EP v1.0 as necessary to satisfy testing and assurance measures prescribed therein.

### 4.1.1 Security Audit

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

The TOE provides extensive capabilities to generate audit data targeted at detecting such activity. The TOE generates an audit record for each auditable event. Each security relevant audit event has the date, timestamp, event description, and subject identity.

The TOE also generates Call Detail Records (CDR) which contain log information about each VVoIP call processed by the CUCM TOE.

The TOE transmits its audit messages to an external syslog server over a secure TLS channel.

### 4.1.2 Cryptographic Support

The TOE provides cryptographic functions to support HTTPS/TLS communication protocols. The cryptographic algorithm implementation has been validated for CAVP conformance. This includes key generation and random bit generation, key establishment methods, key destruction, and the various types of cryptographic operations to provide AES encryption/decryption, signature verification, hash generation, and keyed hash generation. All cryptography is implemented using the CiscoSSL FOM 6.2 cryptographic module. Refer to Table 2 for algorithm certificate references.

**Table 2: FIPS References**

| Algorithm | Description | Supported Mode/ Standard | CAVP Cert. # | Module | Operating Environment | SFR |
|---|---|---|---|---|---|---|
| RSA | Signature Generation, Verification, and key transport | FIPS PUB 186-4 | A511 | CiscoSSL FIPS Object Module (FOM) v6.2 | Intel Xeon Gold 6244 (Cascade Lake) w/ CentOS 7.6 on VMware ESXi v6 | FCS_CKM.1<br>FCS_CKM.2<br>FCS_COP.1/SigGen |
| ECDSA | Cryptographic Signature services | FIPS PUB 186-4 | A511 | CiscoSSL FIPS Object Module (FOM) v6.2 | Intel Xeon Gold 6244 (Cascade Lake) w/ CentOS 7.6 on VMware ESXi v6 | FCS_CKM.1<br>FCS_COP.1/SigGen |
| AES | Used for symmetric encryption/decryption | AES in CBC and GCM (128 and 256 bits) | A511 | CiscoSSL FIPS Object Module (FOM) v6.2 | Intel Xeon Gold 6244 (Cascade Lake) w/ CentOS 7.6 on VMware ESXi v6 | FCS_COP.1/DataEncryption |
| SHS (SHA-1, 256, 384) | Cryptographic hashing services | Byte Oriented | A511 | CiscoSSL FIPS Object Module (FOM) v6.2 | Intel Xeon Gold 6244 (Cascade Lake) w/ CentOS 7.6 on VMware ESXi v6 | FCS_COP.1//Hash |
| HMAC SHA-1, SHA-256, SHA-384 | Keyed hashing services and software integrity test | Byte Oriented | A511 | CiscoSSL FIPS Object Module (FOM) v6.2 | Intel Xeon Gold 6244 (Cascade Lake) w/ CentOS 7.6 on VMware ESXi v6 | FCS_COP.1/Keyed Hash |
| DRBG | Deterministic random bit generation services in accordance | CTR_DRBG (AES 256) | A511 | CiscoSSL FIPS Object Module (FOM) v6.2 | Intel Xeon Gold 6244 (Cascade Lake) w/ CentOS 7.6 on | FCS_RBG_EXT.1 |

| Algorithm | Description | Supported Mode/ Standard | CAVP Cert. # | Module | Operating Environment | SFR |
|---|---|---|---|---|---|---|
| | with ISO/IEC 18031:2011 | | | | VMware ESXi v6 | |
| KAS-ECC | Key Agreement | NIST Special Publication 800-56A Revision 3 | A511 | CiscoSSL FIPS Object Module (FOM) v6.2 | Intel Xeon Gold 6244 (Cascade Lake) w/ CentOS 7.6 on VMware ESXi v6 | FCS_CKM.2 |

The algorithm certificates are applicable to the TOE based on CUCM and Intel® Xeon® processors as noted in Physical Scope of the TOE in ST.

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

The TOE also ensures software updates to the TOE are from Cisco Systems, Inc. using digital signature verification.

### 4.1.3 User Data Protection

The TOE ensures VVoIP calls are set up using the SIP call control protocol prior to redirecting streaming media data between the endpoints.

If the organization has a policy that requires all data on all disks to be cleared, the TOE provides the Security Administrator the ability wipe all residual information from storage.

### 4.1.4 Identification and authentication

The TOE implements two types of authentication: 1) X.509v3 certificate-based authentication for remote devices; and 2) password-based authentication for Security Administrators. Device-level authentication allows the TOE to establish a secure communication channel with remote endpoints over TLS.

Security Administrators have the ability to compose strong passwords of 15 characters in length which are stored in an obscured form. Additionally, the TOE detects and tracks successive unsuccessful remote authentication attempts and will prevent the offending account from further attempts if a Security Administrator defined threshold is reached.

### 4.1.5 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:

- Ability to administer the TOE locally and remotely;
- Ability to configure the access banner;
- Ability to configure the session inactivity time before session termination or locking;
- Ability to update the TOE, and to verify the updates using digital signature capability prior to installing those updates;
- Ability to configure the authentication failure parameters for FIA_AFL.1;
- Configure the number of failed administrator authentication attempts;
- Ability to enable/disable voice and video recordings for any registered VVoIP endpoint;
- Ability to display the real-time connection status of all VVoIP endpoints (hardware and software) and telecommunications devices;
- Ability to clear all TSF data stored on disk;
- Ability to configure audit behavior;
- Ability to configure the cryptographic functionality;
- Ability to re-enable an Administrator account and
- Ability to configure NTP

The TOE supports the security administrator and user role. Both roles are considered to be Authorized Administrators that can perform the above security relevant management functions.

### 4.1.6 Protection of the TSF

The TOE protects critical security data including keys and passwords against tampering by untrusted subjects and prevents unintentional flow of any data or information should the TOE encounter a critical error. The TOE ensures software updates are authentic by verifying those updates are from Cisco Systems, Inc.

The TOE ensures accurate date and time by implementing a clock function reliant upon NTP Servers in the IT Environment. Accurate system time is used by the TOE to support monitoring local and remote interactive administrative sessions for inactivity, validating X.509 certificates (to determine if a certificate has expired), and to support accurate timestamps in audit records.

### 4.1.7 TOE Access

At each administrative interface, the TOE is capable of displaying a Security Administrator specified advisory notice and consent warning message prior to initiating identification and authentication. Once the Security Administrator has successfully authenticated, the TOE monitors both local and remote admin sessions for inactivity and terminates when a threshold time period is reached. If a session has been terminated the TOE requires the user to re-authenticate.

### 4.1.8 Trusted path/Channels

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

The connection to NTP is secured using NTPv4. The TOE also allows secure communications between itself and a VVoIP endpoint using TLS and between itself and another ESC Server using TLS.

# 5 Assumptions, Threats & Clarification of Scope

## 5.1 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 3 TOE Assumptions**

| Assumption | Assumption Definition |
|---|---|
| A.PHYSICAL_PROTECTION | The network device is assumed to be physically protected in its operational environment and not subject to physical attacks that compromise the security and/or interfere with the device's physical interconnections and correct operation. This protection is assumed to be sufficient to protect the device and the data it contains. As a result, the cPP will not include any requirements on physical tamper protection or other physical attack mitigations. The cPP will not expect the product to defend against physical access to the device that allows unauthorized entities to extract data, bypass other controls, or otherwise manipulate the device. |
| A.LIMITED_FUNCTIONALITY | The device is assumed to provide networking functionality as its core function and not provide functionality/ services that could be deemed as general purpose computing. For example the device should not provide computing platform for general purpose applications (unrelated to networking functionality). |
| A.NO_THRU_TRAFFIC_PROTECTION | A standard/generic network device does not provide any assurance regarding the protection of traffic that traverses it. The intent is for the network device to protect data that originates on or is destined to the device itself, to include administrative data and audit data. Traffic that is traversing the network device, destined for another network entity, is not covered by the ND cPP. It is assumed that this protection will be covered by cPPs and PP-Modules for particular types of network devices (e.g., firewall). |
| A.TRUSTED_ADMINISTRATOR | The Security Administrator(s) for the network device are assumed to be trusted and to act in the best interest of security for the organization. This includes being appropriately trained, following policy, and adhering to guidance documentation. Administrators are trusted to ensure passwords/credentials have sufficient strength and entropy and to lack malicious intent when administering the device. The network device is not expected to be capable of defending against a malicious administrator that actively works to bypass or compromise the security of the device.<br><br>For TOEs supporting X.509v3 certificate-based authentication, the Security Administrator(s) are expected to fully validate (e.g. offline verification) any CA certificate (root CA certificate or intermediate CA certificate) loaded into the TOE's trust store (aka 'root store', ' trusted CA Key Store', or similar) as a trust anchor prior to use (e.g. offline verification). |
| A.REGULAR_UPDATES | The network device firmware and software is assumed to be updated by an Administrator on a regular basis in response to the release of product updates due to known vulnerabilities. |
| A.ADMIN_CREDENTIALS_SECURE | The Administrator's credentials (private key) used to access the network device are protected by the platform on which they reside. |

| Assumption | Assumption Definition |
|---|---|
| A.RESIDUAL_INFORMATION | The Administrator must ensure that there is no unauthorized access possible for sensitive residual information (e.g. cryptographic keys, keying material, PINs, passwords etc.) on networking equipment when the equipment is discarded or removed from its operational environment. |

## 5.2 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 4 Threats**

| Threat | Threat Definition |
|---|---|
| T.UNAUTHORIZED_ADMINISTRATOR_ACCESS | Threat agents may attempt to gain Administrator access to the network device by nefarious means such as masquerading as an Administrator to the device, masquerading as the device to an Administrator, replaying an administrative session (in its entirety, or selected portions), or performing man-in-the-middle attacks, which would provide access to the administrative session, or sessions between network devices. Successfully gaining Administrator access allows malicious actions that compromise the security functionality of the device and the network on which it resides. |
| T.WEAK_CRYPTOGRAPHY | Threat agents may exploit weak cryptographic algorithms or perform a cryptographic exhaust against the key space. Poorly chosen encryption algorithms, modes, and key sizes will allow attackers to compromise the algorithms, or brute force exhaust the key space and give them unauthorized access allowing them to read, manipulate and/or control the traffic with minimal effort. |
| T.UNTRUSTED_COMMUNICATION_CHANNELS | Threat agents may attempt to target network devices that do not use standardized secure tunnelling protocols to protect the critical network traffic. Attackers may take advantage of poorly designed protocols or poor key management to successfully perform man-in-the-middle attacks, replay attacks, etc. Successful attacks will result in loss of confidentiality and integrity of the critical network traffic, and potentially could lead to a compromise of the network device itself. |
| T.WEAK_AUTHENTICATION_ENDPOINTS | Threat agents may take advantage of secure protocols that use weak methods to authenticate the endpoints – e.g., shared password that is guessable or transported as plaintext. The consequences are the same as a poorly designed protocol, the attacker could masquerade as the administrator or another device, and the attacker could insert themselves into the network stream and perform a man-in-the-middle attack. The result is the critical network traffic is exposed and there could be a loss of confidentiality and integrity, and potentially the network device itself could be compromised. |
| T.UPDATE_COMPROMISE | Threat agents may attempt to provide a compromised update of the software or firmware which undermines the security functionality of the device. Non-validated updates or updates validated using non-secure or weak cryptography leave the update firmware vulnerable to surreptitious alteration. |

| Threat | Threat Definition |
|---|---|
| T.UNDETECTED_ACTIVITY | Threat agents may attempt to access, change, and/or modify the security functionality of the network device without Administrator awareness. This could result in the attacker finding an avenue (e.g., misconfiguration, flaw in the product) to compromise the device and the Administrator would have no knowledge that the device has been compromised. |
| T.SECURITY_FUNCTIONALITY_COMPROMISE | Threat agents may compromise credentials and device data enabling continued access to the network device and its critical data. The compromise of credentials includes replacing existing credentials with an attacker's credentials, modifying existing credentials, or obtaining the Administrator or device credentials for use by the attacker. |
| T.PASSWORD_CRACKING | Threat agents may be able to take advantage of weak administrative passwords to gain privileged access to the device. Having privileged access to the device provides the attacker unfettered access to the network traffic, and may allow them to take advantage of any trust relationships with other network devices. |
| T.SECURITY_FUNCTIONALITY_FAILURE | An external, unauthorized entity could make use of failed or compromised security functionality and might therefore subsequently use or abuse security functions without prior authentication to access, change or modify device data, critical network traffic or security functionality of the device. |
| T.MALICIOUS_TRAFIC | A malformed packet is a protocol packet containing modified data not recognizable by the receiving device (e.g. TOE), or contains modified protocol packets intended to crash or cause the TOE to act in ways unintended. An attacker may attempt to use a VVoIP endpoint to send these malformed packets or malicious traffic towards the TOE in an attempt to control or crash the call control system and connected network devices. To mitigate VVoIP endpoint devices from being used to successfully launch malicious traffic, the TOE must provide encryption remedies to prevent modification of protocol packets. The TOE must also provide authentication mechanisms to prevent unauthorized VVoIP endpoints from improperly registering to the ESC for the purpose of launching malicious attacks. |
| T.NETWORK_DISCLOSURE | An attacker may attempt to "map" IP addresses of VVoIP endpoint/devices and other telecommunications equipment for the purpose of determining the organizational structure of the enterprise, providing reconnaissance for future targeted attacks. |
| T.UNAUTHORIZED_CLIENT | An attacker may attempt to register an unauthorized VVoIP endpoint to the TOE for the purpose of impersonating a legitimate end user device in order to gain unauthorized connectivity to other clients or active calls. |

## 5.3 Organizational Security Policies

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

**Table 5 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. |
| P.SECURED_PLATFORM | Administrators in the organization ensure that general purpose computers use secure operating systems and are configured in accordance with applicable security standards. |

## 5.4 Clarification of Scope

All evaluations (and all products) have limitations, as well as potential misconceptions that need clarifying. This text covers some of the more important limitations and clarifications of this evaluation. Note that:

- As with any evaluation, this evaluation only shows that the evaluated configuration meets the security claims made, with a certain level of assurance. The level of assurance for this evaluation is defined within the collaborative Protection Profile for Network Devices (NDcPP), Version 2.1 and Network Device Collaborative Protection Profile (NDcPP) Extended Package Enterprise Session Controller (ESC EP), Version 1.0.
- Consistent with the expectations of the Protection Profile, this evaluation did not specifically search for, nor seriously attempt to counter, vulnerabilities that were not "obvious" or vulnerabilities to objectives not claimed in the ST. The CEM defines an "obvious" vulnerability as one that is easily exploited with a minimum of understanding of the TOE, technical sophistication, and resources.
- The evaluation of security functionality of the product was limited to the functionality specified in the claimed PPs. Any additional security related functional capabilities included in the product were not covered by this evaluation.

In particular, the following functionality is excluded from the scope of the evaluation: Non-FIPS mode of operation on the TOE — This mode of operation includes non-FIPS allowed operations.

# 6 Documentation

The following document is delivered with the TOE. The vendor provided the document with the TOE for this evaluation.

- Cisco Unified Communications Manager (CUCM) 12.5 Common Criteria Configuration Guide Version 0.4, 13 November 2020.

Only this administrative guidance listed immediately above, and the specific sections of the other documents referenced by that guide should be trusted for the installation, administration and use of this product in its evaluated configuration.

# 7 TOE Evaluated Configuration

## 7.1 Evaluated Configuration

The TOE consists of CUCM v12.5 software installed on VMware ESXi 6.5 or higher running on one (1) or more UCS M5 appliances as specified in below. The evaluated configuration of the CUCM v12.5 TOE is limited to only one vND instance for each physical platform. In addition, there must be no other guest VMs providing non-network device functionality. The TOE must be configured in accordance with the documentation specified in section 6.

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 via NTPv4 on its internal network for time services. The TOE is administered using the Cisco Unified Communications Manager Administration program from a workstation 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 workstation must be connected to an internal network using HTTPS to secure the connection to the TOE. A syslog server is also required to store audit records. The audit server must be attached to the internal (trusted) network and the connection to the server must be secured using TLS.

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

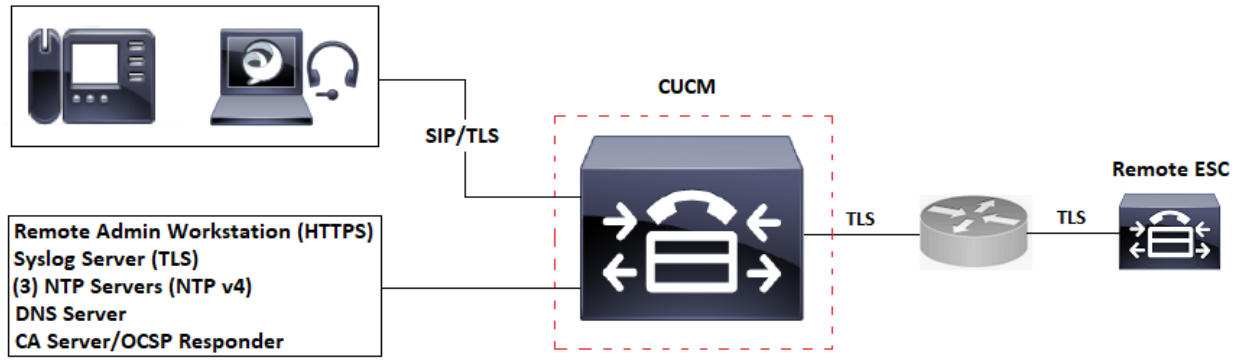


**Figure 1 TOE Example Deployment**

In figure 1 the following are considered to be in the IT Environment:

- DNS Server (does not require a secure connection)
- Certificate Authority (CA) and OCSP Responder (does not require a secure connection)
- Management Workstation (secure connection is HTTPS (over TLS))
- NTP Servers (connection is NTPv4)
- Peer ESC (secure connection is TLS)
- Syslog Server (secure connection is TLS)
- Video and Voice End-points (VVoIP) (secure connection is SIP over TLS)

## 7.2 Physical Scope of the TOE

The TOE is comprised of hardware and software. The hardware platform is the UCS C220 M5 or the UCS C240 M5 as described in 6 below. The software is VMware ESXi 6.5 and CUCM v12.5 with CentOS 7.6. The network, on which the TOE resides, is considered part of the environment.

**Table 6 Hardware/Software Models and Specifications**

| Hardware/ Software | Specifications |
|---|---|
| Cisco Unified Communications Manager v12.5 with CentOS 7.6<br>  | ■ Form Factor :<br>o UCS C220 M5: 1RU<br>o UCS C240 M5: 2RU<br>■ Memory: 24 DDR4 DIMM slots: 8, 16, 32, 64, and 128 GB up to 2666 MHz<br>■ Internal Storage, backplane options, UCS C220 M5:<br>o Up to 10 x 2.5-inch SAS and SATA HDDs and SSDs and up to 2 NVMe PCIe drives<br>o Up to 10 x 2.5-inch NVMe PCIe drives<br>o Up to 4 x 3.5-inch SAS and SATA HDDs and SSDs and up to 2 NVMe PCIe drive<br>■ Internal Storage, backplane options, UCS C220 M5:<br>o Up to 26 x 2.5-inch SAS and SATA HDDs and SSDs and up to 4 NVMe PCIe drives<br>o Up to 10 x 2.5-inch NVMe PCIe and 16 SAS and SATA HDDs and SSDs<br>o Up to 12 x 3.5-inch SAS and SATA HDDs and SSDs, and 2 rear 2.5-inch HDDs and SSDs and up to 4 NVMe PCIe drives<br>■ Ports:<br>o 1x RJ-45 console port<br>o 2x USB 3.0 ports<br>o 1x RJ-45 management port<br>o 2x 10GTbase-T ports<br>o VGA connector<br>o One KVM console connector (supplies two USB 2.0 connectors, one VGA DB15 video connector, and one serial port (RS232) RJ45 connector)<br>o and one serial port (RS232) RJ45 connector)<br>■ CPU: Intel Xeon Cascade Lake SP (Cascade Lake microarchitecture)[1] |

[1] The specific CPU used in the CC tested configuration was Intel Xeon Gold 6244 (Cascade Lake)

## 7.3 Excluded Functionality

The following functionality is excluded from the evaluation.

**Table 7 Excluded Functionality**

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

These services will be disabled by configuration. The exclusion of this functionality does not affect compliance to the collaborative Protection Profile for Network Devices (NDcPP) Version 2.1 or the Network Device Collaborative Protection Profile (NDcPP) Extended Package Enterprise Session Controller (ESC EP) Version 1.0.

# 8 IT Product Testing

This section describes the testing efforts of the developer and the evaluation team. It is derived from information contained in Evaluation Test Report for Cisco Unified Communications Manager 12.5, which is not publicly available. The Assurance Activities Report provides an overview of testing and the prescribed assurance activities.

## 8.1 Developer Testing

No evidence of developer testing is required in the Assurance Activities for this product.

## 8.2 Evaluation Team Independent Testing

The evaluation team verified the product according the vendor-provided guidance documentation and ran the tests specified in the collaborative Protection Profile for Network Devices (NDcPP), Version 2.1 and Network Device Collaborative Protection Profile (NDcPP) Extended Package Enterprise Session Controller (ESC EP), Version 1.0. The specific test configurations and test tools utilized may be found in the Assurance Activities Report section 4.1, which is publicly available.

# 9 Results of the Evaluation

The results of the assurance requirements are generally described in this section and are presented in detail in the proprietary documents: the Detailed Test Report (DTR) and the Evaluation Technical Report (ETR). The reader of this document can assume that activities and work units received a passing verdict.

A verdict for an assurance component is determined by the resulting verdicts assigned to the corresponding evaluator action elements. The evaluation was conducted based upon CC version (Version 3.1, Rev. 5) and CEM (Version 3.1, Rev. 5). The evaluation determined the Cisco Unified Communications Manager 12.5 to be Part 2 extended, and meets the SARs contained in the PP. Additionally the evaluator performed the Assurance Activities specified in the NDPP.

## 9.1 Evaluation of Security Target

The evaluation team applied each ASE CEM work unit. The ST evaluation ensured the ST contains a description of the environment in terms of policies and assumptions, a statement of security requirements claimed to be met by the Cisco Unified Communications Manager 12.5 that are consistent with the Common Criteria, and product security function descriptions that support the requirements. Additionally, the evaluator performed an assessment of the Assurance Activities specified in the collaborative Protection Profile for Network Devices (NDcPP), Version 2.1 and Network Device Collaborative Protection Profile (NDcPP) Extended Package Enterprise Session Controller (ESC EP), Version 1.0.

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

## 9.2 Evaluation of Development Documentation

The evaluation team applied each ADV CEM work unit. The evaluation team assessed the design documentation and found it adequate to aid in understanding how the TSF provides the security functions. The design documentation consists of a functional specification contained in the Security Target's TOE Summary Specification. Additionally, the evaluator performed the Assurance Activities specified in the collaborative Protection Profile for Network Devices (NDcPP), Version 2.1 and Network Device Collaborative Protection Profile (NDcPP) Extended Package Enterprise Session Controller (ESC EP), Version 1.0. related to the examination of the information contained in the TOE Summary Specification.

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the Assurance Activities, and that the conclusion reached by the evaluation team was justified.

### 9.3 Evaluation of Guidance Documents

The evaluation team applied each AGD CEM work unit. The evaluation team ensured the adequacy of the user guidance in describing how to use the operational TOE. Additionally, the evaluation team ensured the adequacy of the administrator guidance in describing how to securely administer the TOE. The guides were assessed during the design and testing phases of the evaluation to ensure they were complete. Additionally, the evaluator performed the Assurance Activities specified in collaborative Protection Profile for Network Devices (NDcPP), Version 2.1 and Network Device Collaborative Protection Profile (NDcPP) Extended Package Enterprise Session Controller (ESC EP), Version 1.0. related to the examination of the information contained in the operational guidance documents.

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the Assurance Activities, and that the conclusion reached by the evaluation team was justified.

### 9.4 Evaluation of Life Cycle Support Activities

The evaluation team applied each ALC CEM work unit. The evaluation team found that the TOE was identified.

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

### 9.5 Evaluation of Test Documentation and the Test Activity

The evaluation team applied each ATE CEM work unit. The evaluation team ran the set of tests specified by the Assurance Activities in the collaborative Protection Profile for Network Devices (NDcPP), Version 2.1 and Network Device Collaborative Protection Profile (NDcPP) Extended Package Enterprise Session Controller (ESC EP), Version 1.0. and recorded the results in a Test Report, summarized in the Evaluation Technical Report and Assurance Activities Report.

The validator reviewed the work of the evaluation team, and found that sufficient evidence was provided by the evaluation team to show that the evaluation activities addressed the test activities in the collaborative Protection Profile for Network Devices (NDcPP), Version 2.1 and Network Device Collaborative Protection Profile (NDcPP) Extended Package Enterprise Session Controller (ESC EP), Version 1.0. and that the conclusion reached by the evaluation team was justified.

### 9.6 Vulnerability Assessment Activity

The evaluation team applied each AVA CEM work unit. The evaluation team performed a public search for vulnerabilities, performed vulnerability testing and did not discover any issues with the TOE.

The evaluator searched the Internet for potential vulnerabilities in the TOE using the web sites listed below. The sources of the publicly available information are provided below:

- https://nvd.nist.gov/vuln/search
- https://cve.mitre.org/
- http://www.kb.cert.org/vuls/html/search
- http://www.exploitsearch.net
- http://www.securiteam.com
- http://nessus.org/plugins/index.php?view=search
- http://www.zerodayinitiative.com/advisories
- https://www.exploit-db.com/
- https://www.rapid7.com/db/vulnerabilities
- https://tools.cisco.com/security/center/publicationListing.x - Vendor Website

The evaluator performed the public domain vulnerability searches using the following key words: (The search was performed on December 8 2020.)

- Cisco CUCM 12.5
- CUCM 12.5
- Cisco SSL
- Cisco Unified Computing System (UCS) C220 M5S
- Cisco Unified Computing System (UCS) C240 M5S
- VMware ESXi 6.5
- Intel Xeon Gold 6244 (Cascade Lake)
- TLS 1.2
- TCP
- UDP
- CiscoSSL FIPS Object Module (FOM)
- SIP
- CentOS 7.6

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation addressed the vulnerability analysis Assurance Activities in the collaborative Protection Profile for Network Devices (NDcPP), Version 2.1 and Network Device Collaborative Protection Profile (NDcPP) Extended Package Enterprise Session Controller (ESC EP), Version 1.0 , and that the conclusion reached by the evaluation team was justified.

### 9.7 Summary of Evaluation Results

The evaluation team's assessment of the evaluation evidence demonstrates that the claims in the ST are met. Additionally, the evaluation team's test activities also demonstrated the accuracy of the claims in the ST.

The validation team's assessment of the evidence provided by the evaluation team is that it demonstrates that the evaluation team performed the Assurance Activities in the collaborative Protection Profile for Network Devices (NDcPP), Version 2.1 and Network Device Collaborative Protection Profile (NDcPP) Extended Package Enterprise Session Controller (ESC EP), Version

1.0., and correctly verified that the product meets the claims in the ST.

# 10 Validator Comments & Recommendations

The validation team notes that the evaluated configuration is dependent upon the TOE being configured per the evaluated configuration instructions in the Cisco Unified Communications Manager (CUCM) 12.5 Common Criteria Configuration Guide Version 0.4, 13 November 2020 document. No versions of the TOE and software, either earlier or later were evaluated. Please note that the functionality evaluated is scoped exclusively to the security functional requirements specified in the Security Target. Other functionality included in the product was not assessed as part of this evaluation. Other functionality provided by devices in the operational environment, such as the syslog server, need to be assessed separately and no further conclusions can be drawn about their effectiveness.

# 11 Annexes

Not applicable.

# 12 Security Target

Cisco Unified Communications Manager 12.5 Common Criteria Security Target, Version 1.3
Dated: December 10, 2020

# 13 Glossary

The following definitions are used throughout this document:

- **Common Criteria Testing Laboratory (CCTL).** An IT security evaluation facility accredited by the National Voluntary Laboratory Accreditation Program (NVLAP) and approved by the CCEVS Validation Body to conduct Common Criteria-based evaluations.
- **Conformance.** The ability to demonstrate in an unambiguous way that a given implementation is correct with respect to the formal model.
- **Evaluation.** The assessment of an IT product against the Common Criteria using the Common Criteria Evaluation Methodology to determine whether or not the claims made are justified; or the assessment of a protection profile against the Common Criteria using the Common Evaluation Methodology to determine if the Profile is complete, consistent, technically sound and hence suitable for use as a statement of requirements for one or more TOEs that may be evaluated.
- **Evaluation Evidence.** Any tangible resource (information) required from the sponsor or developer by the evaluator to perform one or more evaluation activities.
- **Feature.** Part of a product that is either included with the product or can be ordered separately.
- **Target of Evaluation (TOE).** A group of IT products configured as an IT system, or an IT product, and associated documentation that is the subject of a security evaluation under the CC.
- **Validation.** The process carried out by the CCEVS Validation Body leading to the issue of a Common Criteria certificate.
- **Validation Body.** A governmental organization responsible for carrying out validation and for overseeing the day-to-day operation of the NIAP Common Criteria Evaluation and Validation Scheme.

# 14 Bibliography

The Validation Team used the following documents to produce this Validation Report:


1. Common Criteria for Information Technology Security Evaluation - Part 1: Introduction and general model, Version 3.1 Revision 5.
2. Common Criteria for Information Technology Security Evaluation - Part 2: Security functional requirements, Version 3.1 Revision 5.
3. Common Criteria for Information Technology Security Evaluation - Part 3: Security assurance requirements, Version 3.1 Revision 5
4. Common Evaluation Methodology for Information Technology Security Evaluation, Version 3.1 Revision 5.
5. Cisco Unified Communications Manager (CUCM)12.5 Common Criteria Security Target Version 1.3
6. Assurance Activity Report for Cisco Unified Communications Manager (CUCM) 12.5, [AAR] Version 1.1, 13 December 2020.
7. Cisco Unified Communications Manager (CUCM)12.5 Common Criteria Configuration Guide, Version 0.4, 13 November 2020.
8. Evaluation Technical Report for Cisco Unified Communications Manager (CUCM)12.5 (ETR), Version 1.1, 10 December 2020.