National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

TM

Validation Report

for the

Cisco Unified Communications Manager (CUCM) 11.0

Report Number: **CCEVS-VR-10646-2015**

Dated: **August 25, 2015**

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 6940
Fort George G. Meade, MD 20755-6940

ACKNOWLEDGEMENTS

Validation Team

Jean Petty
The MITRE Corporation

Luke Florer
The Aerospace Corporation

Common Criteria Testing Laboratory

Acumen Security, LLC.

Table of Contents

1. EXECUTIVE SUMMARY

This report 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 Validation Report (VR), which describes how those security claims were tested and 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 Unified Communications Manager (CUCM) 11.0 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 August 2015. The information in this report is largely 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 Protection Profile for Network Devices Version 1.1 and Network Device Protection Profile Extended Package SIP Server, Version 1.1.

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. 4) for conformance to the Common Criteria for IT Security Evaluation (Version 3.1, Rev. 4), as interpreted by the Assurance Activities contained in the Protection Profile for Network Devices (NDPP) with Errata #3 and the Network Device Protection Profile Extended Package SIP Server (SIPEP). 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 is consistent with the evidence provided.

The validation team provided guidance on technical issues and evaluation processes, reviewed the individual work units of 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.

The technical information included in this report was obtained from the Cisco Unified Communications Manager Series ST, AAR, ETR and analysis performed by the Validation Team.

1.1. INTERPRETATIONS

Not applicable.

1.2. THREATS

The ST identifies the following threats that the TOE and its operational environment are intended to counter:

- An administrator may unintentionally install or configure the TOE incorrectly, resulting in ineffective security mechanisms.
- Security mechanisms of the TOE may fail, leading to a compromise of the TSF.
- 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.
- 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.
- A malicious party attempts to supply the end user with an update to the product that may compromise the security features of the TOE.
- User data may be inadvertently sent to a destination not intended by the original sender.
- An administrator may unintentionally install or configure the TOE incorrectly, resulting in ineffective security mechanisms.
- Security mechanisms of the TOE may fail, leading to a compromise of the TSF.
- 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.
- 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.
- A malicious party attempts to supply the end user with an update to the product that may compromise the security features of the TOE.
- User data may be inadvertently sent to a destination not intended by the original sender.

2. IDENTIFICATION

The National Information Assurance Partnership (NIAP) Common Criteria Evaluation and Validation Scheme (CCEVS) is a joint National Security Agency (NSA) and National Institute of Standards and Technology (NIST) 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 (PP) containing Assurance Activities, including interpretations of the Common Methodology for Information Technology Security Evaluation (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 CCEVS
TOE	Cisco Unified Communications Manager (CUCM) 11.0
Protection Profile	U.S. Government Protection Profile for Security Requirements for Network Devices (NDPP), Version 1.1 with Errata #3; Network Device Protection Profile Extended Package SIP Server (SIPEP), Version 1.1.
Security Target	Cisco Unified Communications Manager Security Target
Evaluation Technical Report	VID 10646 Common Criteria NDPP Assurance Activity Report, version 1.0
CC Version	Version 3.1, Revision 4
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 Montgomery Village, MD
CCEVS Validators	Jean Petty, Luke Florer

3. ARCHITECTURAL INFORMATION

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

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

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 1. 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 ST.

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

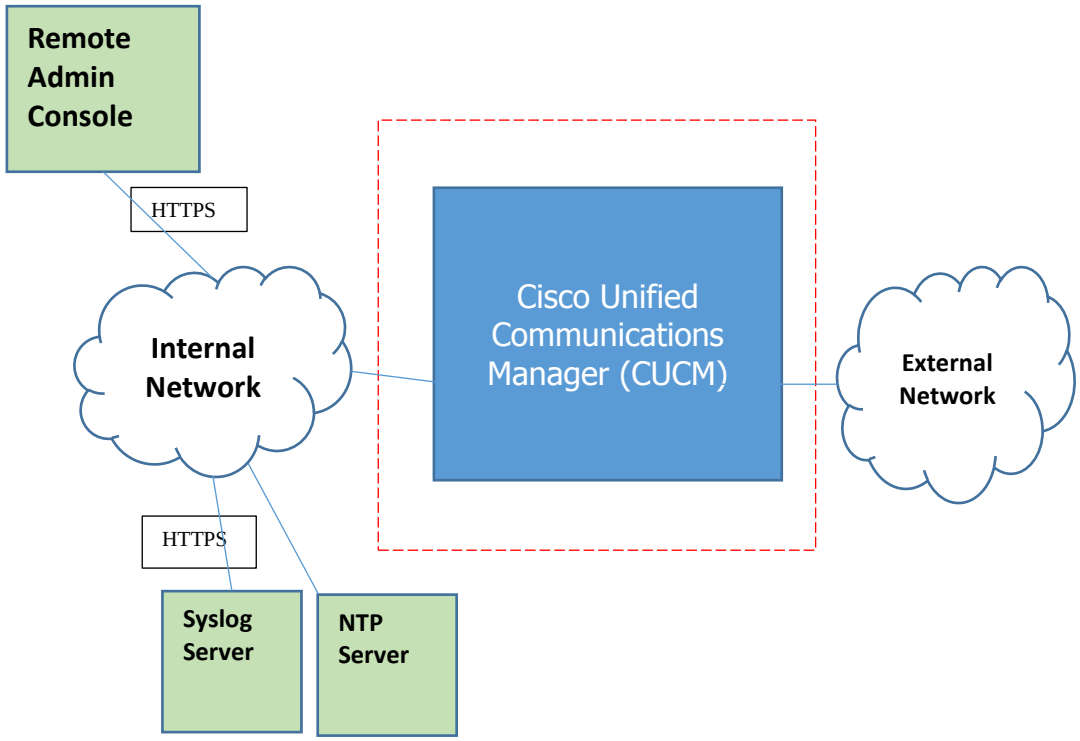


Figure 2. TOE Boundary (Red Dashed Line)

The previous figure includes the following:

- The TOE
  - Cisco UCS C220 M3 Server or Cisco UCS C210 M2 Server
  - 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

NOTE: While the previous figure includes the available TOE devices and several non-TOE IT environment devices, the TOE is only the CUCM hardware and software configuration. Only one TOE device is required in an evaluated configuration.

3.1. PHYSICAL SCOPE OF THE TOE

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.

The network on which the TOE resides is considered part of the environment. The software is pre-installed and is comprised of software release 11.0. In addition, the software image is also downloadable from the Cisco web site. A login id and password is required to download the software image.

4. Security Policy

4.1. Security Functionality

The TOE enforces the following security functionality as described in the ST.

- Security Audit
- Cryptography Support
- Full Residual Information Protection
- Identification & Authentication
- Security Management
- Protection of the TSF
- Trusted Path/Channel
- TOE Access

These are described in more detail in the subsections below.

4.1.1. 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. Note that logs are not automatically uploaded to the logging server, but require administrator action; if an administrator wishes to store or backup audit records externally that is done through the Cisco Unified Real-Time Monitoring Tool.

4.1.2. 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 for certificate references). Refer to FIPS certificate 2100; Cisco FIPS Object Module (Software Version: 4.1).

Table 2. FIPS References

Algorithm	Cert. #
RSA	#1377 and #1385
AES	#2678 and #2685
SHS (SHA-1, 256, 384)	#2247 and #2256

Algorithm	Cert. #
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 3.

Table 3. TOE Provided Cryptography

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

4.1.3. 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.

4.1.4. Identification & 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.

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:

- 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.

4.1.6. 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.

4.1.7. 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.

4.1.8. Trusted Path/Channel

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.

4.2. EXCLUDED FUNCTIONALITY

Non-FIPS mode of operation is excluded from the evaluation. These services will be disabled by configuration.

5. ASSUMPTIONS AND 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:

- 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.
- Physical security, commensurate with the value of the TOE and the data it contains, is assumed to be provided by the environment.
- TOE Administrators are trusted to follow and apply all administrator guidance in a trusted manner.
- 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.
- Physical security, commensurate with the value of the TOE and the data it contains, is assumed to be provided by the environment.
- TOE Administrators are trusted to follow and apply all administrator guidance in a trusted manner.

5.2. 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 NDPP and SIPEP.
- 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.
- No browser software exists on the CUCM server. When connecting to the CUCM the management station must be connected to an internal network and 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. All of these, the browser software, the syslog server, and the remote admin console, are a part of the environment. The TOE must be physically protected and the internal (trusted) network must be separated effectively from unauthorized individuals and user traffic. The internal network must be in a controlled environment where implementation of security policies can be enforced.

6. DOCUMENTATION

The primary guidance documentation for the TOE is the Cisco Unified Communications Manager Common Criteria Operational User Guidance and Preparative Procedures, version 1.0; references and links to additional guidance and operational information is provided within this guidance document.

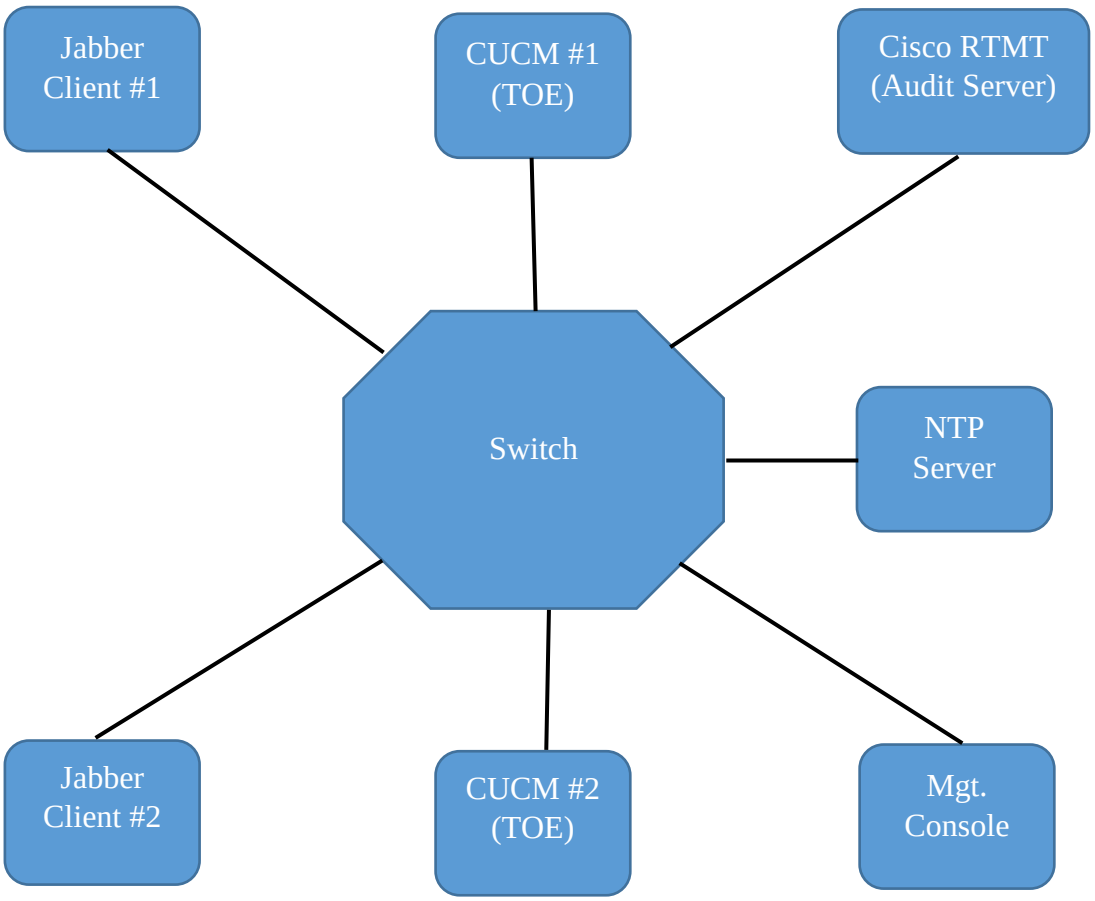
7. IT PRODUCT TESTING

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

7.1. EVALUATION TEAM INDEPENDENT TESTING

The evaluation team devised a test plan based on the Test Assurance Activities specified in NDPP and SIPEP. The test plan described how each test activity was to be instantiated within the TOE test environment. The evaluation team executed the tests specified in the test plan and documented the results in the team test report identified above.

The evaluation team verified the product according the Cisco Unified Communications Manager Common Criteria Operational User Guidance and Preparative Procedures and ran the tests specified in the NDPP and SIPEP. The test configuration consisted of two TOE instances as shown below.



Configuration details for the test configuration are as follows:

- CUCM#1 (TOE):
  - Hardware Model: C210 M2
  - Version: 11.0
  - IP address: 192.168.50.30
  - Configuration Details:
    - Phone Profile configured for Jabber1
    - Device configured Jabber1
    - User configured Jabber1
    - SIP Trunk Profile configured connecting CUCM#1 to CUCM#2
    - Packet Capture on outgoing/incoming interfaces configured
- CUCM #2 (TOE):
  - Hardware Model: C210 M2
  - Version: 11.0
  - IP address: 192.168.30.40
  - Configuration Details:
    - Phone Profile configured for device1
    - Device configured device1
    - User configured jabber1
    - SIP Trunk Profile configured connecting CUCM#2 to CUCM#1
    - Packet Capture on outgoing/incoming interfaces configured
- SIP Client #1
  - Windows 8
  - Cisco Jabber version 11.0 (SIPClient1)
  - IP address:192.168.50.90
  - Configuration/Installed tools:
    - Wireshark version 1.12.5
- SIP Client #2
  - Windows 8
  - Cisco Jabber version 11.0 (SIPClient2)
  - IP address:192.168.50.91
  - Configuration/Installed tools:
    - Wireshark version 1.12.5
- Management Console
  - Windows 8
  - IP address:192.168.50.90
  - Configuration/Installed tools:
    - Wireshark version 1.12.5
    - Vsphere 5.5.0
- NTP Server:
  - HW version: Cisco ISR 1921
  - IP address: 192.168.50.80
- Audit Server:
  - Windows 8 Workstation
  - Cisco Real-Time Monitoring Tool (RTMT) version 11.0 (audit server)

    - IP address: 192.168.50.90
    - Configuration/Installed tools:
        - Wireshark version 1.12.5
- Switch:
    - Linksys SRW2008

Only one TOE hardware appliance model was included in the test configuration, however, the CCTL provided an equivalency argument demonstrating that he hardware platforms do not provide any of the TSF functionality. The hardware within the TOE only differs by configuration and performance. There are no hardware specific dependencies of the product. There are not hardware specific functionality between appliance types.

The evaluators performed testing at the CCTL facility. The evaluators exercised all the test cases. All tests passed. A summary of the testing performed by the evaluation team is provided in the Common Criteria NDPP SIP Server EP Assurance Activity Report.

7.2. Penetration Testing

The evaluation team conducted an open source search for vulnerabilities in the product. The open source search did not identify any obvious vulnerabilities applicable to the TOE in its evaluated configuration.

8. EVALUATED CONFIGURATION

The TOE evaluated configuration consists of CUCM software installed on one or more UCS C220 M3S or the UCS C210 M2 appliances as specified in the ST, configured in FIPS mode as defined in the Cisco Unified Communications Manager Common Criteria Operational User Guidance and Preparative Procedures. 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.

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 3.1 rev 4 and CEM version 3.1 rev 4. The evaluation determined the Cisco Unified Communications Manager to be Part 2 extended, and meets the SARs contained in the PP. Additionally the evaluator performed the Assurance Activities specified in the NDPP and the SIPEP.

9.1. EVALUATION OF THE SECURITY TARGET (ASE)

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 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 NDPP and the SIPEP.

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 THE DEVELOPMENT (ADV)

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 NDPP 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 THE GUIDANCE DOCUMENTS (AGD)

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 the NDPP 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 THE LIFE CYCLE SUPPORT ACTIVITIES (ALC)

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 THE TEST DOCUMENTATION AND THE TEST ACTIVITY (ATE)

The evaluation team ran the set of tests specified by the Assurance Activities in the NDPP and SIPEP 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 NDPP and the SIPEP, and that the conclusion reached by the evaluation team was justified.

9.6. VULNERABILITY ASSESSMENT ACTIVITY (VAN)

The evaluation team performed a public search for vulnerabilities, performed vulnerability testing and did not discover any issues with the TOE.

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

10. VALIDATOR COMMENTS & RECOMMENDATIONS

The validators suggest that the consumer pay particular attention to the evaluated configuration of the device(s). In order to remain CC compliant, the device(s) must first be configured in FIPS mode as defined in the Cisco Unified Communications Manager Common Criteria Operational User Guidance and Preparative Procedures. Significant physical and administrative protection is assumed to be in place in order to maintain security of the TOE; the internal (trusted) network must be secure to ensure secure functionality of the TOE. Note that the product includes FIPS validated cryptographic algorithms.

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. Please note further that certain functionality is excluded from the approved configuration and that some functions relative to the devices were not tested, nor are any claims made relative to their security.

The product contains more functionality than was covered by the evaluation. Only the functionality implemented by the SFR's within the Security Target was evaluated. All other functionality provided by the devices needs to be assessed separately and no further conclusions can be drawn about their effectiveness.

TOE administrators should note in particular that audit logs are not automatically uploaded to the logging server, but require administrator action; if an administrator wishes to store or backup audit records externally that is done through the Cisco Unified Real-Time Monitoring Tool, which is not a part of the TOE.

11. ANNEXES

Not applicable.

12. SECURITY TARGET

The security target for this product's evaluation is *Cisco Unified Communications Manager Security Target, Version 1.0*.

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 4.
2. Common Criteria for Information Technology Security Evaluation - Part 2: Security functional requirements, Version 3.1 Revision 4.
3. Common Criteria for Information Technology Security Evaluation - Part 3: Security assurance requirements, Version 3.1 Revision 4.
4. Common Evaluation Methodology for Information Technology Security Evaluation, Version 3.1 Revision 4.
5. Cisco Unified Communications Manager Security Target, Version 1.0
6. [ETR] Cisco Unified Communications Manager Common Criteria Security Target Evaluation Technical Report, version 1.0
7. [Guidance Docs] Cisco Unified Communications Manager Common Criteria Operational User Guidance and Preparative Procedures [AGD], version 1.0
8. [AAR] VID 10646 Common Criteria Assurance Activity Report, version 1.0