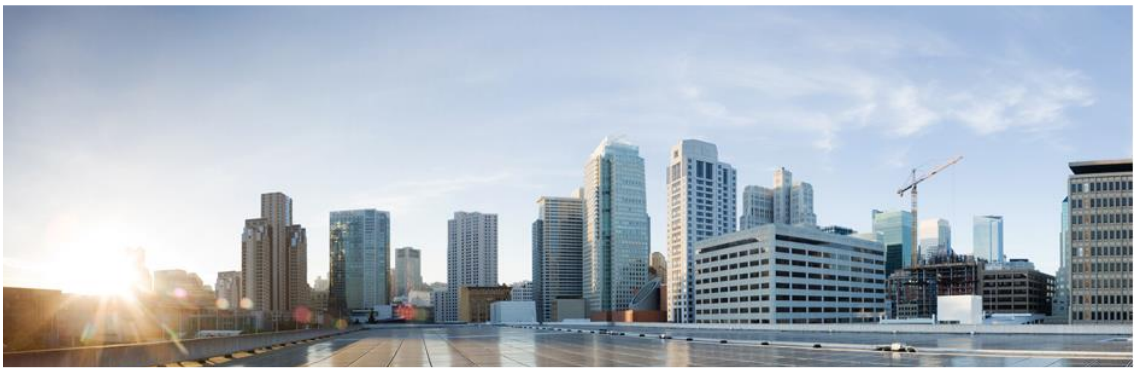


Cisco Unified Communications Manager (CUCM) 12.5

Common Criteria Configuration Guide

Version 0.4

13 November 2020

Table of Contents

1 Introduction 9
1.1 Audience 9
1.2 Purpose 9
1.3 Document References 10
1.4 Supported Hardware and Software 13
1.5 Operational Environment 15
1.5.1 Supported non-TOE Hardware/ Software/ Firmware 15
1.6 Excluded Functionality 16
2 Secure Acceptance of the TOE 17
3 Secure Installation and Configuration 20
3.1 Physical Installation 20
3.2 Initial Setup of CUCM 20
3.2.1 Enabling FIPS Mode 21
3.2.2 ECDSA Support 23
3.2.3 Administrator Configuration, Credentials and Session Termination 24
3.2.4 Logging Configuration 25
3.3 System Logs 47
3.4 VVoIP Endpoint Devices and User Association 47
3.5 Network Protocols and Cryptographic Settings 48
3.5.1 Certificates 48
3.5.2 Generating a Certificate Signing Request (CSR) 51
3.5.3 Remote Administration Protocols 52
3.5.4 SIP Connections and Protocols 54

3.5.5 Clusters and Nodes 55
3.5.6 Clusters and Route Patterns 56
4 Secure Management 57
4.1 User Roles 57
4.2 Clock Management 57
4.3 Identification and Authentication 58
4.4 Login Banners 58
4.5 Product Updates 59
5 Security Relevant Events 59
6 Network Services and Protocols 61
7 Modes of Operation 62
8 Disk Erasure 63
9 Security Measures for the Operational Environment 64
10 Related Documentation 66
10.1 Documentation Feedback 66
10.2 Obtaining Technical Assistance 67

List of Tables

Table 1: Acronyms 5
Table 2 Terminology 7
Table 3 Cisco Documentation 11
Table 4: Operational Environment Components 15
Table 5 Excluded Functionality 16
Table 6 TOE External Identification 19
Table 7 Evaluated Software Images 19
Table 8 Audit Entries 30
Table 9 Audit Record Contents 30
Table 10: Protocols and Services 61
Table 11 Operational Environment Security Measures 64

Acronyms

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

Table 1: Acronyms

Acronyms / Abbreviations	Definition
AAA	Administration, Authorization, and Accounting
AES	Advanced Encryption Standard
CC	Common Criteria for Information Technology Security Evaluation
CEM	Common Evaluation Methodology for Information Technology Security
CM	Configuration Management
ESC	Enterprise Session Controller
GCM	Galois Counter Mode
HTTP	Hyper-Text Transport Protocol
HTTPS	Hyper-Text Transport Protocol Secure
IEEE	Institute of Electrical and Electronics Engineers
IP	Internet Protocol
IT	Information Technology
NDcPP	collaborative Network Device Protection Profile
OS	Operating System
Packet	A block of data sent over the network transmitting the identities of the sending and receiving stations, error-control information, and message.
PP	Protection Profile
PRNG	Pseudo Random Number Generator
RADIUS	Remote Authentication Dial In User Service
RNG	Random Number Generator
RSA	Rivest, Shamir and Adleman (algorithm for public-key cryptography)
SHS	Secure Hash Standard
SIP	Session Initiation Protocol
SRTP	Secure Real-time Transport Protocol
SSHv2	Secure Shell (version 2)
ST	Security Target
TCP	Transport Control Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol
TLS	Transport Layer Security

Acronyms / Abbreviations	Definition
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Function
TSP	TOE Security Policy
VoIP	Voice over Internet Protocol
VVoIP	Video and Voice over Internet Protocol

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.
Call Detail Record	A log of call metadata that can be used to determine characteristics of a call, such as its length and involved parties, without recording any of its content.
Enterprise Session Controller (ESC)	The ESC (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.
Firmware (per NIST for FIPS validated cryptographic modules)	The programs and data components of a cryptographic module that are stored in hardware (e.g., ROM, PROM, EPROM, EEPROM or FLASH) within the cryptographic boundary and cannot be dynamically written or modified during execution.
Peer CUCM or ESC	Another CUCM or ESC on the network that the TOE interfaces.
Security Administrator	Synonymous with Authorized Administrator for the purposes of this evaluation.
Session Boarder Controller	A type of network device that resides on the edge of a VVoIP network that is responsible for filtering corrupted or potentially malicious traffic and preventing it from entering or leaving the network.
Trunking	The concept of connecting multiple networks together; analogous to the use of a T1 line in a legacy telephone network.
User	Any entity (human user or external IT entity) outside the TOE that interacts with the TOE.
VVoIP Endpoint	A VVoIP-capable phone or software application that a human user can use to make or receive a voice or video call.

DOCUMENT INTRODUCTION

Prepared By:

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

This document provides supporting evidence for an evaluation of a specific Target of Evaluation (TOE), the Cisco Unified Communications Manager (CUCM). This Operational User Guidance with Preparative Procedures addresses the administration of the TOE software and hardware and describes how to install, configure, and maintain the TOE in the Common Criteria evaluated configuration.

REVISION HISTORY

Rev	Date	Description
0.1	20 September 2019	Initial Draft
0.2	15 October 2020	Updates from testing
0.3	5 November 2020	Additional Updates from testing
0.4	13 November 2020	Final Updates from testing

1 Introduction

This Operational User Guidance with Preparative Procedures documents the administration of the Cisco Unified Communications Manager (CUCM) 12.5 running on Cisco Unified Computing System™ (Cisco UCS) UCS C220 M5 or UCS C240 M5, the TOE, as it was certified under Common Criteria. The Cisco Unified Communications Manager (CUCM) may be referenced below as the Cisco Unified Communications Manager, CUCM, or simply TOE.

1.1 Audience

This document is written for administrators configuring the TOE. This document assumes that you are familiar with Cisco Unified Communications Manager or equivalent call processing and unified communications products. It is also assumed that you have a general understanding and knowledge with the basic concepts and terminologies used in 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, that you are a trusted individual, and that you are trained to use the operating systems on which you are running your network.

1.2 Purpose

This document is the Operational User Guidance with Preparative Procedures for the Common Criteria evaluation. It was written to highlight the specific TOE configuration and administrator functions and interfaces that are necessary to configure and maintain the TOE in the evaluated configuration. The evaluated configuration is the configuration of the TOE that satisfies the requirements as defined in the Security Target (ST). This document covers all of the security functional requirements specified in the ST and as summarized in Section 3 of this document. This document does not mandate configuration settings for the features of the TOE that are outside the evaluation scope, which should be set according to your organizational security policies.

This document is not meant to detail specific actions performed by the administrator but rather is a road map for identifying the appropriate locations within Cisco documentation to get the specific details for configuring and maintaining CUCM operations. It is recommended that you read all instructions in this document and any references before performing steps outlined and entering commands. Section 10 of this document provides information for obtaining assistance.

1.3 Document References

This section lists the Cisco Systems documentation that is also the Common Criteria Configuration Item (CI) List. The documents used are shown below in Table 3. Throughout this document, the guides will be referred to by the "#", such as [**1**].

Table 3 Cisco Documentation

#	Title	Link
[1]	Cisco Unified Communications Manager (CallManager) Maintain and Operate Guides	https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html
[2]	Hardware Install Guides: (a) Cisco UCS C220 M5 Server Installation and Service Guide (b) Cisco UCS C240 M5 Server Installation and Service Guide	 (a) https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/c/hw/C220M5/install/C220M5.html (b) https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/c/hw/C240M5/install/C240M5.html
[3]	Administration Guide for Cisco Unified Communications Manager and IM and Presence Service, Release 12.5	https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/admin/12_5_1/admin/cucm_b_administration-guide-1251/cucm_b_administration-guide-1251_chapter_01111.html
[4]	Cisco Unified CDR Analysis and Reporting Administration Guide, Release 12.5(1)	https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/service/12_5_1/Car/cucm_b_cdr-analysis-reporting-admin-guide-1251.html
[5]	System Configuration Guide for Cisco Unified Communications Manager, Release 12.5(1)SU2	https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/admin/12_5_1SU2/systemConfig/cucm_b_system-configuration-guide-1251su2.html
[6]	Security Guide for Cisco Unified Communications Manager, Release 12.5(1)SU2	https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/security/12_5_1SU2/cucm_b_security-guide-1251SU2.html
[7]	Cisco Unified Communications Manager FIPS 140-2 Certificate	https://csrc.nist.gov/projects/cryptographic-algorithm-validation-program
[8]	Cisco Unified Communications Manager Common Criteria Guidance, version 1.0	See NIAP webpage for certified products - https://www.niap-ccevs.org/CCEVS_Products/pcl.cfm

#	Title	Link
[9]	Cisco Unified Communications Manager Security Target, version 1.0	See NIAP webpage for certified products - https://www.niap-ccevs.org/CCEVS_Products/pcl.cfm
[10]	Installation Guide for Cisco Unified Communications Manager and IM and Presence Service Release 12.5(1)	https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/install/12_5_1/cucm_b_install-guide-cucm-imp-1251.html
[11]	Release Notes for Cisco Unified Communications Manager and IM & Presence Service, Release 12.5(1) Release Notes for Cisco Unified Communications Manager and the IM and Presence Service, Release 12.5(1)SU1	https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/rel_notes/12_5_1/cucm_b_release-notes-cucm-imp-1251.html https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/rel_notes/12_5_1/SU1/cucm_b_release-notes-for-cucm-imp-1251su1.html
[12]	Cisco Collaboration on Virtual Servers	https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/virtual/CUCM_BK_C90D1BE9_00_cisco-collaboration-on-virtual-servers.html
[13]	Manage Certificates	https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/security/12_5_1/cucm_b_security-guide-1251.html
[14]	Cisco Unified Serviceability Administration Guide, Release12.5(1)	https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/admin/12_5_1/admin/cucm_b_serviceability-admin-guide-1251.html
[15]	Feature Configuration Guide for Cisco Unified Communications Manager, Release 12.5(1)	https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/admin/12_0_1/featureConfig/cucm_b_cucm-feature-configuration-guide_1201.html https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/srnd/collab12/collab12/recordng.html
[16]	Command Line Interface Guide for Cisco Unified Communications Solutions, Release 12.5(1)	https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/cli_ref/12_5_1/cucm_b_cli-reference-guide-1251.html

#	Title	Link
[17]	Cisco Unified Reporting Administration Guide, Release 12.0(1)	https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/service/12_0_1/report/cucm_b_cisco-unified-reporting-administration-1201.html
[18]	Cisco UCS C-Series Integrated Management Controller GUI Configuration Guide, Release 3.1 Cisco UCS C-Series Integrated Management Controller GUI Configuration Guide, Release 4.0	https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/c/sw/gui/config/guide/3_1/b_Cisco_UCS_C-series_GUI_Configuration_Guide_31.html https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/c/sw/gui/config/guide/4_0/b_Cisco_UCS_C-series_GUI_Configuration_Guide_40.html
[19]	Cisco UCS Manager Administration Management Guide 3.1 Cisco UCS Manager Administration Management Guide 4.0	https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/ucs-manager/GUI-User-Guides/Admin-Management/3-1/b_Cisco_UCS_Admin_Mgmt_Guide_3_1.html https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/ucs-manager/GUI-User-Guides/Admin-Management/4-0/b_Cisco_UCS_Admin_Mgmt_Guide_4-0.html
[20]	Upgrade and Migration Guide for Cisco Unified Communications Manager	https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/upgrade/12_5_1/cucm_b_upgrade-migration-guide-125x.html

1.4 Supported Hardware and Software

Only the hardware and software listed in section 1.5 of the Security Target (ST) is compliant with the Common Criteria evaluation. Using hardware not specified in the ST invalidates the secure configuration. Likewise, using any software version other than the evaluated software listed in the ST will invalidate the secure configuration. The TOE is a hardware and software solution that makes up the CUCM system as follows:

- The hardware is comprised of the Cisco Unified Computing System™ (Cisco UCS) Cisco UCS C220 M5 Rack Server is a two-socket 1 Rack Unit [1RU] and Cisco Unified Computing System™ (Cisco UCS) C240 M5 2 Rack Unit [2RU]
- The software is comprised of the CUCM software image Release 12.5

The software comes pre-installed on the Cisco Unified Computing System™ (UCS) UCS C220 M5 and UCS C240 M5 Servers though it may not be the CC evaluated and certified version. Therefor you may need to follow the steps listed in Section 2 Secure Acceptance of the TOE of this document.

Cisco Unified CM Administration is a web-based application that is the main administration and configuration interface for Cisco Unified Communications Manager. The CUCM Administration is used to manage the system to include the features, server settings, call routing rules, phones and end users. CUCM Administration supports the following operating system and browsers:

- Firefox with Windows 10 (64 bit)-Latest browser version only
- Chrome with Windows 10 (64 bit)-Latest browser version only
- Internet Explorer 11 with Windows 10 (64 bit)
- Internet Explorer 11 with Windows 8.1 (64 bit)
- Internet Explorer 11 with Windows 7 (64 bit)
- Microsoft Edge browser with Windows 10 (32 bit/64 bit)
- Safari with MacOS (10.x)-Latest browser version only

HTTPS is used to secure the connection between CUCM and the browser. Refer to **[6]** Hypertext Transfer Protocol Over Secure Sockets Layer (HTTPS), **[11]** New and Changed Features and **[14]** Getting Started.

Cisco Unified Communications Manager works as an Appliance on a non-Windows-based Operating System. The Cisco Unified Communications Manager appliance refers to the following functions:

- Works on a specific hardware platform(s) that Cisco specifies and supplies and, in some cases, the customer supplies
- Works in a carefully controlled software environment that Cisco specifies and installs
- Includes all software that is required to operate, maintain, secure, and manage servers

Cisco Unified Communications Manager servers are preinstalled with software to ease customer and partner deployment and automatically search for updates and notify

administrators when key security fixes and software upgrades are available for their system. This process comprises Electronic Software Delivery.

Since Cisco Unified Communications Manager is a software application, enhancing its capabilities in production environments requires only upgrading software on the server platform.

1.5 Operational Environment

1.5.1 Supported non-TOE Hardware/ Software/ Firmware

The TOE supports (in some cases optionally) the following hardware, software, and firmware in its environment:

Table 4: Operational Environment Components

Component	Required	Usage/Purpose Description for TOE performance
Local Console	Yes	This includes any IT Environment Console that is directly connected to the TOE via the Serial Console Port and is used by the TOE administrator to support TOE administration.
Management Workstation using web browser for HTTPS	Yes	This includes any IT Environment Management workstation with a web browser installed that is used by the TOE administrator to support TOE administration through HTTPS protected channels. Any web browser that supports TLSv1.2 with the supported ciphersuites may be used.
NTP Server	Yes	CUCM maintains a reliable date and timestamp by synchronizing with an NTP server for its own reliable timestamp. The NTP Server is required in the IT environment in support of synchronize time stamps for the TOE and subsequently the various endpoints.
LDAP Server	Yes	This includes any IT environment LDAP AAA server that provides provisioning and configuration of end users
Syslog Server	Yes	This includes any syslog server to which the TOE would transmit syslog messages using TLS to secure the connection. The audit records are automatically sent to the remote syslog once the configuration and settings are complete.
DNS Server	Yes	The TOE supports communications with the DNS Server that is required for communications with other components (peer CUCM clusters). The DNS is required to support IP addressing schemes for traffic and access control. Cisco recommends that

Component	Required	Usage/Purpose Description for TOE performance
		all CUCM node names in the cluster be set to the FQDN or IP address rather than the hostname.
Peer ESC and VVoIP Endpoint	Yes	This includes any peer ESC and VoIP client with which the TOE communicates with over a protected TLS and SRTP channel respectively.

1.6 Excluded Functionality

Table 5 Excluded Functionality

Excluded Functionality	Exclusion Rationale
Non-FIPS mode of operation on the router.	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.

2 Secure Acceptance of the TOE

To ensure the correct TOE is received, the TOE should be examined to ensure that that is has not been tampered with during delivery.

Verify that the TOE software and hardware were not tampered with during delivery by performing the following actions:

Step 1 Before unpacking the TOE, inspect the physical packaging the equipment was delivered in. Verify that the external cardboard packing is printed with the Cisco Systems logo and motifs. If it is not, contact the supplier of the equipment (Cisco Systems or an authorized Cisco distributor/partner).

Step 2 Verify that the packaging has not obviously been opened and resealed by examining the tape that seals the package. If the package appears to have been resealed, contact the supplier of the equipment (Cisco Systems or an authorized Cisco distributor/partner).

Step 3 Verify that the box has a white tamper-resistant, tamper-evident Cisco Systems bar coded label applied to the external cardboard box. If it does not, contact the supplier of the equipment (Cisco Systems or an authorized Cisco distributor/partner). This label will include the Cisco product number, serial number, and other information regarding the contents of the box.

Step 4 Note the serial number of the TOE on the shipping documentation. The serial number displayed on the white label affixed to the outer box will be that of the device. Verify the serial number on the shipping documentation matches the serial number on the separately mailed invoice for the equipment. If it does not, contact the supplier of the equipment (Cisco Systems or an authorized Cisco distributor/partner).

Step 5 Verify that the box was indeed shipped from the expected supplier of the equipment (Cisco Systems or an authorized Cisco distributor/partner). This can be done by verifying with the supplier that they shipped the box with the courier company that delivered the box and that the consignment note number for the shipment matches that used on the delivery. Also verify that the serial numbers of the items shipped match the serial numbers of the items delivered. This verification should be performed by some mechanism that was not involved in the actual equipment delivery, for example, phone/FAX or other online tracking service.

Step 6 Inspect the TOE according to the instructions in **[2]** Unpack and Inspect the Cisco Unified Computing System™ (Cisco UCS) UCS C220 M5 or the UCS C240 M5 Rack Servers

installed with CUCM software image Release 12.5. Verify that the serial number displayed on the unit itself matches the serial number on the shipping documentation and the invoice. If it does not, contact the supplier of the equipment (Cisco Systems or an authorized Cisco distributor/partner). Also, verify that the unit has the following external identification as described in Table 6 below.

Table 6 TOE External Identification

Product Name	Model Number	External Identification
Cisco Unified Computing System™ (Cisco UCS)	C220 M5S	UCS C220 M5S
Cisco Unified Computing System™ (Cisco UCS)	C240 M5S	UCS C240 M5S

Step 7 To verify the software version and to register the license, from a PC in your network that has been installed with one of the supported browsers, browse into a server that is running Cisco CUCM Administration and log in with administrative privileges. Follow the instructions in **[3]** Administration Overview -> Getting Started -> Sign In.

Step 8 To verify the software version CUCM 12.5 from the Cisco Unified Operating System Administration window, choose Show > Software and review the fields in the Software Packages window. See Table 7 below for the CC validated software version.

Table 7 Evaluated Software Images

Software Version	Image Name
Unified Communications Manager Version 12.5.1.12900-115	Bootable_UCSInstall_UCOS_12.5.1.12900-115.sgn.iso

If the version is not 12.5.1.12900-115 you will need to obtain the CC validated version. Navigate to Cisco Software Central at https://software.cisco.com/. Use your Cisco Care Online (CCO) or SMART account and download the image name in table 7.

Refer to Upgrade Planning and Upgrade Tasks section of [**20**] to perform an upgrade of the CUCM software.

If the digital certificate signatures on the software were modified in any way, the installation would halt, and a warning may be displayed at which time you need to call Cisco TAC, refer to, section 10.2 Obtaining Technical Assistance in this document.

3 Secure Installation and Configuration

3.1 Physical Installation

Follow the instructions for the UCS model in **[2]** Preparing for Server Installation following with Installing the Server In a Rack and Initial Setup. There are network requirements that must be met before deploying CUCM.

3.2 Initial Setup of CUCM

Follow the instructions in Configure Initial Parameters for the System in **[5]** for the initial setup configurations. There are network requirements that must be met before deploying CUCM such as IP addressing, DNS requirements, end user provisioning and configuration using the LDAP Server, syslog and VVR server configurations and supported browsers and their associated certificates.

During the initial startup of the Cisco Unified Communications Manager (CUCM), you will be required to reset the Administrator default password/credential setting. Refer to the password requirements listed below in Section 3.2.3 Administrator Configuration, Credentials and Session Termination.

The Initial configuration setup the licensing requirements, the server name and ports, system-wide parameters that are required when you setup a node for the first time and the core settings for server groups, time zone information and regions.

The Post-Installation Tasks for Cisco Unified Communications Manager in **[10]** will guide you through activating services and installing the license and **[11]** will provide information on running in FIPS and Common Criteria mode.

After the initial setup and activating licenses and services are completed, the remainder of this guide along with the referenced documents will guide you through setting up enterprise parameters for end users, endpoint devices and call administration control **[5]** and **[6].**

Using a secure TLS connection for peer device and end users is required in the evaluated configuration Chapter: TLS Setup **[6]** to set the minimum TLS version for use to TLSv1.2 with support for the following ciphers.

- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_AES_256_CBC_SHA

- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384

To restrict usage to the above ciphersuites, in the Cisco Unified OS Administration menu, navigate to Security --> Cipher Management. Under All TLS sections insert the following:

> ECDHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-SHA384:ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES256-SHA384:AES256-SHA:AES128-SHA

TLS v1.2 is the only version of TLS allowed by default. No configuration is necessary. Also refer to **[11]** for additional information on TLS support.

The default method to administer is CUCM is securely connecting to the CUCM GUI interface using HTTPS over TLS. Using a secure connection is required in the evaluated configuration.

To enable HTTPS, you must download a certificate that identifies the server during the connection process. You can accept the server certificate for the current session only, or you can download the certificate to a trust folder (file) to secure the current session and future sessions with that server. The trust folder stores the certificates for all your trusted sites.

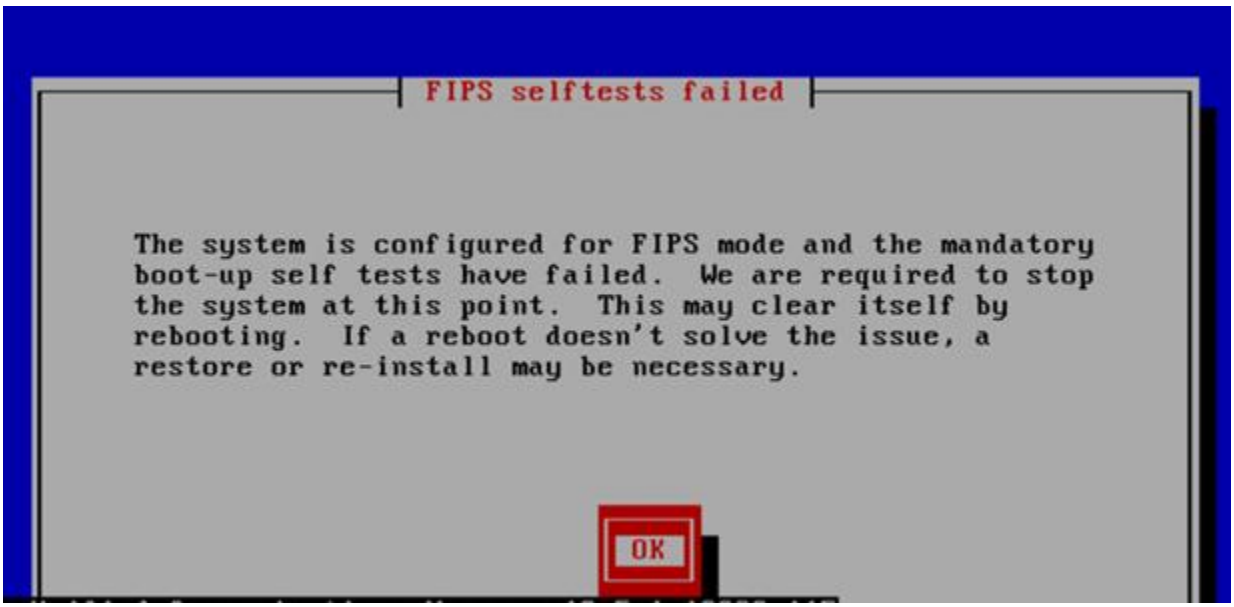
If local administration is required via directly connected to the UCS appliance, refer to Administration in **[12]** using vSphere client. In the evaluated configuration, only authorized administrators are granted access and privileges to manage the TOE.

3.2.1 Enabling FIPS Mode

The TOE must be run in the FIPS mode of operation. Refer to **[6]** Security for SRST References, Trunks, and Gateways -> FIPS 140-2 Mode Setup for the configuration settings.

The self-tests for the cryptographic functions in the TOE are run automatically during power-on as part of the POST. The same POST self-tests for the cryptographic operations are also run periodically during operational state.

If any of the FIPS POST self-tests fail, the TOE transitions into an error state and will display the following on the local console:



In the error state, all secure management and data transmission that is affected by the failure is halted and the TOE outputs status information indicating the failure. In an error state, the Administrator may be able to log in to troubleshoot the issue.

During the POST, all ports are blocked from moving to forwarding state. If all components of all modules pass the POST, the system is placed in FIPS PASS state and ports are allowed to forward management and data traffic. If the POST fails, the TOE ceases operation. During this state no one can login, no traffic is passed, the TOE is not operational. If the problem is not corrected by the reboot, Cisco Technical Support provides 24-hour-a-day award-winning technical assistance. The Cisco Technical Support & Documentation website on Cisco.com features extensive online support resources. In addition, if you have a valid Cisco service contract, Cisco Technical Assistance Center (TAC) engineers provide telephone support. Contact Cisco TAC as described in section 10.2 Obtaining Technical Assistance of this document.

In this 12.5 release of CUCM, the TOE provides support to monitor the Entropy Monitoring Daemon. This feature does not require any configuration but should be started by executing the following CLI commands:

- utils service start Entropy Monitoring Daemon
- utils service activate Entropy Monitoring Daemon

Refer to **[6]** Default Security Setup -> Entropy

3.2.2 ECDSA Support

The CUCM supports self-signed and third party signed certificates. The certificates are used to securely authenticate devices, encrypt data and to hash data to ensure its integrity. The most important part of certificates is that you know and define how your data is encrypted and shared with entities such as the intended website, phone, or FTP server. When your system trusts a certificate, this means that there is a preinstalled certificate on your system which states it is fully confident that it shares information with the correct destination. Otherwise, it terminates the communication between these points. In order to trust a certificate, trust must already be established with a third-party certificate authority (CA). Your devices must know that they can trust both the CA and intermediate certificates first, before they can trust the server certificate presented by the exchange of messages called the secure sockets layer (SSL) handshake. Refer to Manage Certificates in **[3]** and Security Overview -> Certificates and Security Overview -> Certificate Setup in **[6]**.

The CUCM also supports ECDSA certificates and in the evaluated configuration, it is required to use these certificates **[6]** and **[10]**. When you install Cisco Unified Communications Manager, the self-signed certificate is generated. Cisco Unified Communications Manager Release 12.5 always has an ECDSA certificate and uses that certificate in its SIP interface. All SIP connections support the ECDSA ciphers and use ECDSA certificates.

For third-party signed certificates or certificate chain, you will need to upload the certificate authority root certificate of the certificate authority that signed an application certificate. If a subordinate certificate authority signs an application certificate, you must upload the certificate authority root certificate of the subordinate certificate authority. You can also upload the PKCS#7 format certificate chain of all certificate authority certificates. You can upload certificate authority root certificates and application certificates by using the **Upload Certificate** dialog box. When you upload a certificate authority root certificate or certificate chain that contains only certificate authority certificates, choose the certificate name with the format certificate type-trust. When you upload an application certificate or certificate chain that contains an application certificate and certificate authority certificates, choose the certificate name that includes only the certificate type.

To download certificates, on the Cisco Unified OS Administration page, choose **Security** > **Certificate Management**. Next, specify the search criteria and then click **Find**, then choose the file name of the certificate or certificate trust list (CTL) and click **Download**.

To upload any new certificates or certificate chains that you want your system to trust, from the **Cisco Unified OS Administration**, choose **Security** -> **Certificate Management**, click **Upload Certificate/Certificate Chain,** choose the certificate name from the **Certificate Purpose** drop-down list, then choose the file to upload by performing one of the following steps:

- In the **Upload File** text box, enter the path to the file.
- Click **Browse**, navigate to the file, and then click **Open**.

To upload the file to the server, click **Upload File**

Certificates will also be required for each device that communicates with CUCM.

Refer to **[3]** Manage Security -> Manage Certificates and **[13]**.

3.2.3 Administrator Configuration, Credentials and Session Termination

The CUCM must be configured to use a username and password for each administrator. Once the CUCM has been setup and configured, the Administrator can create additional administrative user accounts, refer to **[3]** Manage Users -> Manage User Access. Also, refer to Manage User Access -> Standard Roles and Access Control Groups.

The security policies for administrative users include the settings for:

- idle timeouts (session termination) is set by default to 30 minutes
- password criteria
    - by default, is set to a minimum of eight (8) characters. In the evaluated configuration the password must be set to a minimum of at least 15 characters
    - password complexity include the following settings:
        - password must be a combination of upper and lower case letters (a-z and A-Z), numbers (0-9) and the following special characters “!”, “@”, “#”, “$”, “%”, “^”, “&”, “*”, “(“,”)”
- pins (personal identification number) needs to be set to at least eight (8) characters

The credential policies control the authentication process for resources (users) of the TOE. The defines password requirements and account lockout details such as failed login attempts, expiration periods and lockout durations for end user passwords, end user PINs, and application user passwords. Credential policies can be assigned broadly to all accounts of a specific credential type, such as all end user PINs, or they can be customized for a specific

application user, or end user. Refer to Provisioning End Users -> Configure Provisioning Profiles -> Configure Default Credential Policy section of **[5].** Inactivity settings must trigger termination of the administrator session. The default value is 30 minutes. If the TOE detects there is no activity for 30 minutes, the CUCM (Web Interface or local console) times out and the Administrator will be logged off. These settings are only configurable by using the Command Line Interface. It is recommended to accept the default time in the evaluated configuration as the CLI was not included.

The inactivity setting for the UCS platform GUI is enforced with the Web Session Timeout Period. The time values that can be set are between 300 and 172800 seconds. The default is 7200 seconds (120 minutes). When the threshold has been reached, the session will end and the Administrator will have to reestablish the session and will be required to be successfully identified and authenticated before accessing the TOE. Refer to **[19]** Remote Authentication -> Web Session Refresh and Web Session Timeout Period.

It is recommended to not leave the administrative Interface unattended and that all active sessions be logged out and closed when not being used.

Account Lockout settings defined in the credential policy do not apply to the local console interface. In the event the Admin account is locked-out due to incorrect passwords entered at the HTTPS remote interface, the administrator will be able to access the local console interface.

3.2.4 Logging Configuration

Once the TOE becomes operational, auditing is on by default, though can be configured via the access the Audit Log Configuration window in the serviceability GUI to configure the settings for the audit logs **[14]** Audit Logs -> Audit Log Configuration Settings.

When audit logging has been enabled, with the detailed logging option selected, the audit logging includes configuration changes to the system are logged in separate log files for auditing. The Cisco Audit Event Service, which displays under Control Center - Network Services in the serviceability GUI, monitors and logs any configuration changes to the system that are made by a user or as a result of the user action **[14]**.

Cisco Unified Serviceability logs the following events:

- Activation, deactivation, start, or stop of a service.

- Changes in trace configurations and alarm configurations.
- Changes in CDR management.
- Review of any report in the Serviceability Reports Archive. This log gets viewed on the reporter node.

Cisco Unified Communications Manager Standard Events Logging:

- Cisco CDR Analysis and Reporting (CAR) creates audit logs for these events:
    - Loader scheduling
    - Daily, weekly, and monthly reports scheduling
    - Mail parameters configuration
    - Dial plan configuration
    - Gateway configuration
    - System preferences configuration
    - Autopurge configuration
    - Rating engine configurations for duration, time of day, and voice quality
    - QoS configurations
    - Automatic generation/alert of pregenerated reports configurations.
    - Notification limits configuration
- Cisco Unified CM Administration Standard Events Logging
    - The following events get logged for various components of Cisco Unified Communications Manager Administration:
        - User logging (user logins and user logouts)
        - User role membership updates (user added, user deleted, user role updated)
        - Role updates (new roles added, deleted, or updated)
        - Device updates (phones and gateways)
        - Server configuration updates (changes to alarm or trace configurations, service parameters, enterprise parameters, IP addresses, hostnames, Ethernet settings, and Cisco Unified Communications Manager server additions or deletions)
- Command-Line Interface Standard Events Logging
    - All commands issued via the command-line interface are logged (for both Cisco Unified Communications Manager and Cisco Unity Connection).

- System Audit Logs
    - System audit logs track activities such as the creation, modification, or deletion of users, log tampering, and any changes to file or directory permissions. This type of audit log is disabled by default due to the high volume of data gathered. To enable this function, you must manually enable **utils auditd** using the CLI **[16]**.
- System Health Status Logs
    - There are no configuration settings required for the system health logs, as this information is provided by default once the UCS platform is up and operational. The health and system logs provide the Authorized Administrator the current status and health of the UCS platform **[18]**. The CUCM also provides cluster node status and hardware status by default **[3]** Monitor System Status.

To setup remote logging to a syslog server, first you must have the syslog server setup and operational. Refer to Audit Logs -> Configure Remote Audit Log Transfer Protocol (Chapter 7) in **[14]**.

To set up audit logging, the steps are as follows **[14]**:

Step 1 In Cisco Unified Serviceability, choose Tools > Audit Log Configuration.

Step 2 From the Server drop-down menu, select any server in the cluster and click Go.

Step 3 To log all cluster nodes, check the Apply to All Nodes check box.

Step 4 In the Server Name field, enter the IP Address or fully qualified domain name of the remote syslog server.

Step 5 Optional. To log configuration updates, including items that were modified, and the modified values, check the Detailed Audit Logging check box.

Step 6 Complete the remaining fields in the Audit Log Configuration window. For help with the fields and their descriptions, see the online help.

Step 7 Click Save.

In the Cisco Unified CM Administration Menu, Navigate to System -> Enterprise Parameters. In the Cisco Syslog Agent section, enter a Parameter Value. This is where the admin configures the DNS-ID reference identifier, which must match the FQDN contained in the SAN extension presented in the Syslog Server certificate.

The default transfer protocol to the syslog server is UDP. You will need to change this setting.

Step 1 Log in to the Command Line Interface.

Step 2 Run the utils remotesyslog show protocol command to confirm which protocol is configured.

Step 3 If you need to change the protocol on this node, do the following:

To configure TCP, run the utils remotesyslog set protocol tcp command.

To configure UDP, run the utils remotesyslog set protocol udp command.

Step 4 If you changed the protocol, restart the node.

Step 5 Repeat this procedure for all Cisco Unified Communications Manager and IM and Presence Service cluster nodes

In the evaluated configuration, you must use TLS to secure the connection to the remote syslog server. You will have to configure TLS to secure the connection to the syslog server using the run the *utils remotesyslog set protocol tls* command. The connection is using TLSv1.2 and associated ciphersuites that was configured during installation as defined in 3.2 Initial Setup of CUCM. Refer to Security Guide for CUCM **[6]** Security Basics section.

Refer to **Audit Log Configuration Settings** in **[14]** to set remote syslog audit event level, log rotation, maximum number of files and size and warning threshold for log rotation overwrite. Logs are written to both the local storage and transferred to the remote audit log simultaneously.

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.

Audit logging contains the following parts:

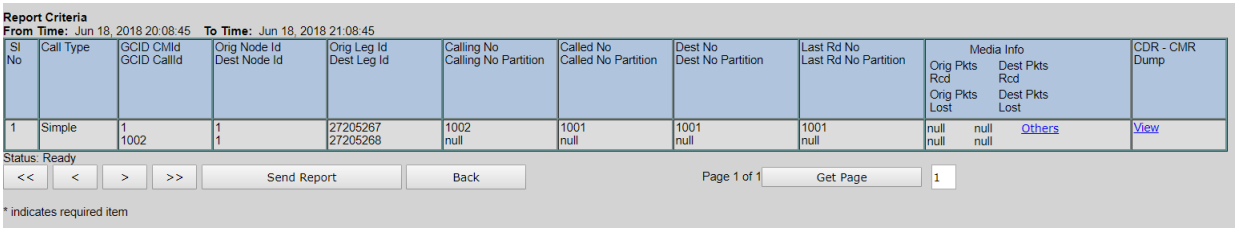
- Audit logging framework - The framework comprises an API that uses an alarm library to write audit events into audit logs. An alarm catalog that is defined as GenericAlarmCatalog.xml applies for these alarms. Different system components provide their own logging. The following example displays an API 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 Service
status is stopped App ID:Cisco Tomcat Cluster
ID:StandAloneCluster Node ID:sa-cm1-3
```

The follow shows a typical, CDR generated by the TOE:



Report Criteria
From Time: Jun 18, 2018 20:08:45 **To Time:** Jun 18, 2018 21:08:45

Sl No	Call Type	GCID CMId GCID CallId	Orig Node Id Dest Node Id	Orig Leg Id Dest Leg Id	Calling No Calling No Partition	Called No Called No Partition	Dest No Dest No Partition	Last Rd No Last Rd No Partition	Media Info Orig Pkts Rcd Dest Pkts Rcd Orig Pkts Lost Dest Pkts Lost	CDR - CMR Dump
1	Simple	1 1002	1 1	27205267 27205268	1002 null	1001 null	1001 null	1001 null	null null Others null null	View

Status: Ready

<< < > >> Send Report Back Page 1 of 1 Get Page 1

* indicates required item

For troubleshooting and reporting, refer to **[17]** Consolidated Data Reporting. The report is a consolidation of reports from existing sources, compares the data and reports irregularities.

3.2.4.1 Audit Trail Log Entries

The following table identifies the elements of the TOE audit record.

Table 8 Audit Entries

Heading	Definition
User ID	The user that triggered the event
Client IP Address	IP address of the client device used
Severity	Level of the event
EventType	The type of event that was performed
ResourceAccessed	The resource that was accessed
EventStatus	The status of the event; successful, failed
Description	The description of the event; CallManager service status is stopped

Audit trail records capture the following activities and any additional information:

Table 9 Audit Record Contents

Requirement	Auditable Events	Additional Audit Record Contents	Sample Audit Record
FCS_HTTPS_EXT.1 FCS_TLSS_EXT.1	Failure to establish a HTTPS Session Failure to establish a TLS Session;	Reason for failure.	10/09/2020 08:32:07.656, acumensec, 192.168.254.177, Warning, UserLogging, Cisco CallManager Administration, Failure, No, AdministrativeEvent, Cisco CallManager Administration CorrelationID :, Failed to Log into Cisco Unified CM Admin Webpages, Cisco Tomcat, , jabber.acumensec.local, 431 2020-07-08 04:49:29,911 FATAL [localhost-startStop-2] security.Log4jEncLogger - javax.crypto.IllegalBlockSizeException: ../Source/Block_Ciphers/Block_Cipher.cpp:do_evp_final: Bad ciphertext data size provided.: error:0606506D:digital envelope routines:EVP_DecryptFinal_ex:wrong final block length 2020-11-14 20:17:07,652 INFO [http-bio-8443-exec-2] impl.DatabaseAccessor - readCredentialsFromDB: Data in credDet before data read userOID_ =null credentialOID_=null isInactive_ =false daysToExpiry_=0 needWarning_ =0 timeLastAccessed_=0 hackCount_ =0 timeHackedLockout_=0 timeOfLockout_ =0 timeLastChanged_=0 timeLastHacked_ =0 userType_=1 endUserStatus_ =2 lastSuccessfulLoginTime_ = 0 lastSuccessfulLoginIp_ = null lastUnsuccessfulLoginIp_ = null minCharsToChange_ = 0 2020-11-14 20:17:07,893 INFO [http-bio-8443-exec-2] impl.DatabaseAccessor - readCredentialsFromDB: Data read from IMSReadCredentials userOID_ =06bae444-79f0-34bc-0b73-042e90ad941b credentialOID_=aec694b2-b7f3-47ed-936b-ac402a87c82d isInactive_ =false daysToExpiry_=0 needWarning_ =0 timeLastAccessed_=1605403027

Requirement	Auditable Events	Additional Audit Record Contents	Sample Audit Record
			hackCount_ =0 timeHackedLockout_=0 timeOfLockout_ =0 timeLastChanged_=1583438452 timeLastHacked_ =1605402202 userType_=2 endUserStatus_ =1 lastSuccessfulLoginTime_ = 1605402218 lastSuccessfulLoginIp_ = 10.1.2.122 lastUnsuccessfulLoginIp_ = 10.1.2.122 minCharsToChange_ = 1
FCS_TLSC_EXT.1 FCS_TLSC_EXT.2 FCS_TLSS_EXT.2	Failure to establish a TLS Session	Reason for failure	00236072.001 |05:07:37.040 |AppInfo |SSLConnectionFailure - SSLConnectionfailedtoPeer PEER IPADDRESS:10.1.2.126PEER PORTNO:5061 SSL ERROR CODE:0 SSL REASON: HandleSSLError - TLS protocol error(ssl reason code=(null) [0]),lib=(null) [0], fun=(null) [0], for 10.1.2.126:5061 App ID:Cisco CallManager Cluster ID:StandAloneCluster Node ID:jabber.acumensec.local Oct 7 03:04:27, jabber, Info, Cisco CallManager, ccm: 212: jabber.acumensec.local: Oct 07 2020 07:04:27.384 UTC : %UC_CALLMANAGER-6-SSLConnectionFailure: %[PeerAddr=10.1.2.171][PeerPortNo=5061][ReasonCode=0][Reason= HandleSSLError - TLS protocol error(ssl reason code=(null) [0]),lib=(null) [0], fun=(null) [0], for 10.1.2.171:5061][ClusterID=StandAloneCluster][NodeID=jabber.acumensec.local]: SSLConnectionfailedtoPeer, 15
FCS_NTP_EXT.1	Configuration of a new time server Removal of configured time server	Identity if new/removed time server	Oct 9 09:02:09 jabber Info systemd:Started "NTP server".Oct 9 09:02:09 jabber Info ilog_impl : NTP servers list: 10.1.2.122 10.1.2.181

Requirement	Auditable Events	Additional Audit Record Contents	Sample Audit Record
FIA_AFL.1	Unsuccessful login attempts limit is met or exceeded	Origin of the attempt (e.g., IP address).	10/09/2020 09:11:49.061 Temp 192.168.254.177 Warning UserLogging Cisco CallManager Administration Failure No AdministrativeEvent Cisco CallManager Administration CorrelationID : Failed to Log into Cisco Unified CM Admin Webpages Cisco Tomcat jabber.acumensec.local Nov 12 2020 12:39:27.732 UTC : %UC_LOGIN-4-AuthenticationFailed: %[TimeStamp=11/12/20 7:39 AM][LoginFrom=192.168.254.121][Interface=Cisco CallManager Administration][UserID=TEST1][ClusterID=][NodeID=jabber.acumensec.local]: Login Authentication failed. 2020-11-13 14:15:47,286 INFO [http-bio-443-exec-25] impl.DatabaseAccessor - readCredentialsFromDB: Data read from IMSReadCredentials userOID_ =29a2a00a-c19e-6b0e-8f47-d373b90fc6fd credentialOID_=1922bcad-a231-4382-9001-d2a6a412680d isInactive_ =false daysToExpiry_=-119 needWarning_ =1 timeLastAccessed_=1605294947 hackCount_ =6 timeHackedLockout_=1605294901 timeOfLockout_ =0 timeLastChanged_=1592469414 timeLastHacked_ =1605294947 userType_=2 endUserStatus_ =1 lastSuccessfulLoginTime_ = 1592473104 lastSuccessfulLoginIp_ = 192.168.254.241 lastUnsuccessfulLoginIp_ = 192.168.254.177 minCharsToChange_ = 1 2020-11-13 14:15:47,289 WARN [http-bio-443-exec-25] impl.AuthenticationDB - authenticateUser: Account locked due to hack attempt.
FIA_UIA_EXT.1	All use of the identification and authentication mechanism.	Origin of the attempt (e.g., IP address).	11/06/2020 09:57:14.571, acumensec, 192.168.254.177, Info, UserLogging, CUCMAdmin, Success, No, CriticalEvent, Cisco CUCM Administration

Requirement	Auditable Events	Additional Audit Record Contents	Sample Audit Record
FIA_UAU_EXT.2	All use of the identification and authentication mechanism.	Origin of the attempt (e.g., IP address).	CorrelationID :, Successfully Logged out Cisco Unified Administration Web Pages, Cisco Tomcat, , jabber.acumensec.local, 9 07/14/2020 04:30:25.553, acumensec, 192.168.254.177, Info, UserLogging, Cisco CallManager Administration, Success, No, AdministrativeEvent, Cisco CallManager Administration CorrelationID :, Successfully Logged into Cisco Unified CM Admin Webpages, Cisco Tomcat, , jabber.acumensec.local, 5 10/09/2020 09:13:43.732 acumensec 192.168.254.177 Warning UserLogging Cisco CallManager Administration Failure No AdministrativeEvent Cisco CallManager Administration CorrelationID : Failed to Log into Cisco Unified CM Admin Webpages Cisco Tomcat jabber.acumensec.local

Requirement	Auditable Events	Additional Audit Record Contents	Sample Audit Record
FIA_UAU.2/TC	Successful or failed authentication of trunk connected network component	ID of Administrator that attempts to connect trunk to external device (if available);	00340047.004 |00:00:15.952 |AppInfo |//SIP/Stack/Transport/0x0x5bfd4478/sipSPISendResponse: Sending REGISTER Response to the transport layer 00340047.005 |00:00:15.952 |AppInfo |//SIP/Stack/Transport/0x0x5bfd4478/sipSPITransportSendMessage: msg=0x5bd0c420, addr=10.1.2.122, port=61190, sentBy_port=5061, is_req=0, tran 00340047.006 |00:00:15.952 |AppInfo |//SIP/Stack/Transport/0x0/sipInstanceGetConnectionId: gcb=0x5bfd4478 is already on connection=0x5bfcbc40 context_list : 4141: jabber.acumensec.local: Nov 15 2020 03:51:14.088 UTC : %UC_CALLMANAGER-6-SSLConnectionFailure: %[PeerAddr=10.1.2.171][PeerPortNo=5061][ReasonCode=0][Reason= HandleSSLError - TLS protocol error(ssl reason code=(null) [0]),lib=(null) [0], fun=(null) [0], for 10.1.2.171:5061][ClusterID=StandAloneCluster][NodeID=jabber.acumensec.local]: SSLConnectionfailedtoPeer

Requirement	Auditable Events	Additional Audit Record Contents	Sample Audit Record
FIA_UAU.2/VVoIP	Successful or failed registration of VVoIP endpoint/device	ID of Administrator that attempt to register VVoIP endpoint to TOE (if available); IP-address of device where registration attempt was initiated (if available); IP-address of VVoIP endpoint that attempt to register to ESC (if available).	Jun 19 08:02:42, jabber, Info, Cisco CallManager, ccm: 337: jabber.acumensec.local Jun 19 2020 12:02:42.295 UTC : %UC_CALLMANAGER-6-EndPointUnregistered: %[DeviceName=CSFJABBERUSER1][IPAddress=10.1.2.122][Protocol=SIP][DeviceType=503][Description=CSFJabberuser1][Reason=15][IPAddrAttributes=0] [ClusterID=StandAloneCluster][NodeID=jabber.acumensec.local]: An endpoint has unregistered, 3795 Jun 19 08:02:43, jabber, Info, Cisco CallManager, ccm: 338: jabber.acumensec.local Jun 19 2020 12:02:43.061 UTC : %UC_CALLMANAGER-6-EndPointRegistered: %[DeviceName=CSFJABBERUSER1][IPAddress=10.1.2.122][Protocol=SIP][DeviceType=503][PerfMonObjType=2][Description=CSFJabberuser1][UserID=jabberuser1][AssociatedDNs=1075][MACAddress=000C29D81263][IPAddrAttributes=0][ActiveLoadId=Jabber_for_Windows-12.8.0.51973][InactiveLoadId=Jabber_for_Windows-12.8.0.51973][ClusterID=StandAloneCluster][NodeID=jabber.acumensec.local]: Endpoint registered, 3796 May 7 06:01:14, jabber, Error, Cisco CallManager, ccm: 2044: jabber.acumensec.local May 07 2020 10:01:14.079 UTC : %UC_CALLMANAGER-3-EndPointTransientConnection: %[ConnectingPort=5060][DeviceName=CSFJABBERUSER1][DeviceType=503][Reason=28][Protocol=SIP][MACAddress=000C29D81263][LastSignalReceived=SIPRegisterInd][StationState=wait_register] [ClusterID=StandAloneCluster][NodeID=jabber.acumensec.local]: An endpoint attempted to register but did not complete registration, 0
FIA_UAU.2/VVoIP	Authentication of external VVoIP endpoint/device	NOTE: Same as above for FIA_UAU.2/VVoIP. Authentication of external VVoIP endpoints must occur before registration. In short, no successful registration of VVoIP endpoint can happen until after the successful authentication of the VVoIP endpoint.	

FIA_X509_EXT.1/Rev	Unsuccessful attempt to validate a certificate Any addition, replacement or removal of trust anchors in the TOE's trust store.	Reason for failure Identification of certificates added, replaced or removed as trust anchor in the TOE's trust store.	14:00:00.048 |Online Certificate Verification Failed with Error code:- 0 Nov 9 12:29:08 jabber local7 6 : 9689: jabber.acumensec.local: Nov 09 2020 17:29:08.915 UTC : %UC_CALLMANAGER-6-SSLConnectionFailure: %[PeerAddr=10.1.2.122][PeerPortNo=5061][ReasonCode=1046][Reason= HandleSSLError - TLS protocol error(ssl reason code=sslv3 alert certificate unknown [1046]),lib=SSL routines [20], fun=ssl3_read][AppID=Cisco CallManager][ClusterID=StandAloneCluster][NodeID=jabber.acumensec.local]: SSLConnectionfailedtoPeer Nov 9 10:00:00, jabber, Error, Cisco Certificate Monitor, : 279: jabber.acumensec.local: Nov 9 2020 14:00:00.046 UTC : %UC_-3-UNKNOWN_ALARM:CertExpired: %[Message=Certificate expiration Notification. Certificate name:tomcat Unit:CAPF Type:own-cert Expiration:Sat Oct 10 17:07:00:000 EDT 20][ClusterID=][NodeID=jabber.acumensec.local]:, 2316 2020-11-13 08:16:32,219 INFO [Timer-0] - Certificate Path : /usr/local/platform/.security/tomcat/trust-certs/ROOT.pem 2020-11-13 08:16:32,219 INFO [Timer-0] - Unit : tomcat-trust 2020-11-13 08:16:32,219 INFO [Timer-0] - Group Type: trust-certs 2020-11-13 08:16:32,219 INFO [Timer-0] - IN -- RSACiscoJCryptoEngine.java - loadCertificate(..) - 2020-11-13 08:16:32,219 INFO [Timer-0] - OUT -- RSACiscoJCryptoEngine.java - loadCertificate -

			2020-11-13 08:16:32,225 INFO [Timer-0] - Calling overloaded method for populating CertInfo 2020-11-13 08:16:32,225 INFO [Timer-0] - IN -- CertUtil.java - populateCertInfo(cert, opInfo, certFilePemLocation) - 2020-11-13 08:16:32,225 INFO [Timer-0] - IN -- CertUtil.java - getHostName(..) - 2020-11-13 08:16:32,225 INFO [Timer-0] - OUT -- CertUtil.java - getHostName - jabber 2020-11-13 08:16:32,225 INFO [Timer-0] - IN -- CryptoUtil.java - saveAsPEM(..) - 2020-11-13 08:16:32,225 INFO [Timer-0] - OUT -- CryptoUtil.java - saveAsPEM - 2020-11-13 08:16:32,225 INFO [Timer-0] - Cluster info passed from certsync 2020-11-13 08:16:32,225 INFO [Timer-0] - The SAN field in the Certificate is NULL or the Certificate doesn't contain SAN 2020-11-13 08:16:32,225 INFO [Timer-0] - So by default the Distribution Type is set to SINGLE_SERVER(1) in order to avoid exception 2020-11-13 08:16:32,225 INFO [Timer-0] - OUT -- CertUtil.java - populateCertInfo - 2020-11-13 08:16:32,225 INFO [Timer-0] - IN -- CertDBImpl.java - insertCertificate(certInfo, con) - 2020-11-13 08:16:32,225 INFO [http-bio-443-exec-7] actions.CertificateAction - certificateUpload

FMT_MOF.1/ManualUpdate	Any attempt to initiate a manual update	None	09/29/2020 13:42:10 file_list.sh|(CAPTURE) <InstallItem type="patch" secure-file="UCSInstall_UCOS_12.5.1.13900-152.sgn.iso" version="12.5.1.13900-152" file="UCSInstall_UCOS_12.5.1.13900-152.sgn.iso" reboot="no" signed="yes" unrestricted="no"/>|<LVL::Debug> 09/29/2020 13:42:10 file_list.sh|(CAPTURE) </InstallList>|<LVL::Debug> 09/29/2020 13:42:17 upgrade_validate_file.sh|Parse argument file_name=UCSInstall_UCOS_12.5.1.13900-152.sgn.iso|<LVL::Debug> 09/29/2020 13:42:18 upgrade_get_file.sh|Parse argument file_name=UCSInstall_UCOS_12.5.1.13900-152.sgn.iso|<LVL::Debug> 09/29/2020 13:42:19 upgrade_get_file.sh|src_file=/mnt/source//UCSInstall_UCOS_12.5.1.13900-152.sgn.iso, dest_file=/common/download/UCSInstall_UCOS_12.5.1.13900-152.sgn.iso, file_type=patch|<LVL::Debug> 09/29/2020 13:42:19 upgrade_get_file.sh|Create md5 "/common/download/UCSInstall_UCOS_12.5.1.13900-152.sgn.iso.md5"|<LVL::Info> 09/29/2020 13:42:19 upgrade_get_file.sh|Create md5 complete|<LVL::Info> 09/29/2020 13:42:19 upgrade_get_file.sh|Authenticate file "/common/download/12.5.1.13900-152/checksum_file.sgn"|<LVL::Info> 09/29/2020 13:43:24 upgrade_install.sh|Parse argument version=12.5.1.13900-152|<LVL::Debug> 09/29/2020 13:43:26 upgrade_install.sh|Copy /mnt/source/Cisco/base_scripts/upgrade_manager.sh to /common/download/12.5.1.13900-152/upgrade_manager.sh|<LVL::Info> 09/29/2020 13:43:26 upgrade_install.sh|Copy /mnt/source/Cisco/base_scripts/upgrade_manager.sh to

Requirement	Auditable Events	Additional Audit Record Contents	Sample Audit Record
			/common/download/12.5.1.13900-152/upgrade_manager.sh complete|<LVL::Info> 09/29/2020 13:43:27 upgrade_manager.sh|Parse argument intf_file=/common/download/12.5.1.13900-152/upgrade_manager.xml|<LVL::Debug> 09/29/2020 13:43:27 upgrade_manager.sh|Parse argument to_version=12.5.1.13900-152|<LVL::Debug> 09/29/2020 13:43:27 upgrade_manager.sh|new upgrade version=12.5.1.13900-152|<LVL::Info> 09/29/2020 13:43:27 upgrade_manager.sh|Cleanup data from a prior upgrade attempt|<LVL::Info> 09/29/2020 13:49:02 file_list.sh|success|<LVL::Info>
FMT_SMF.1	Modification of TOE Call Details Records (CDR)	ID of Administrator attempting to query or modify database; IP-address of device where database query was initiated; the exact SQL command/instruction that was executed.	20:04:39.383 |LogMessage UserID : acumensec ClientAddress : 10.1.2.186 Severity : 6 EventType : UserAccess ResourceAccessed: Cisco AXL EventStatus : Success CompulsoryEvent : No AuditCategory : AdministrativeEvent ComponentID : Cisco CCM Application CorrelationID : AuditDetails : Attempt to access data was successful.User is authorized to access executeSQLQuery App ID: Cisco Tomcat Cluster ID: Node ID: jabber.acumensec.local

	Enabling/disabling VVoIP endpoint/device features	ID of Administrator attempting to enable/disable service or feature on ESC or on external registered device; IP-address of device where enabling/disabling of services or features was initiated; the feature or service that was enabled/disabled.	11/13/2020 20:42:18.657, acumensec, 10.1.2.186, Info, UserAccess, Cisco AXL, Success, No, AdministrativeEvent, Cisco CCM Application CorrelationID :, Attempt to access data was successful.User is authorized to access executeSQLQuery, Cisco Tomcat, , jabber.acumensec.local, 237 11/13/2020 20:46:29.813, acumensec, 192.168.254.15, Info, UserLogging, Cisco CallManager Administration, Success, No, AdministrativeEvent, Cisco CallManager Administration CorrelationID :, Successfully Logged into Cisco Unified CM Admin Webpages, Cisco Tomcat, , jabber.acumensec.local, 238 11/13/2020 20:47:08.798, acumensec, 192.168.254.15, Info, UserAccess, CUCMAdmin, Success, No, AdministrativeEvent, Cisco CUCM Administration CorrelationID :, Attempt to access data was successful. User is authorized to access callParkFindList, Cisco Tomcat, , jabber.acumensec.local, 239 11/13/2020 20:47:20.780, , , Notice, UserLogging, CUCMServiceability, Success, No, CriticalEvent, Cisco Trace Collection Servlet CorrelationID :, Successfully logged out of trace collection service, Cisco Tomcat, , jabber.acumensec.local, 240 11/13/2020 20:47:20.820, acumensec, 10.1.2.122, Info, UserLogging, CUCMServiceability, Success, No, CriticalEvent, ast CorrelationID :, Successfully Timed out of ast soap services, Cisco Tomcat, , jabber.acumensec.local, 241

Requirement	Auditable Events	Additional Audit Record Contents	Sample Audit Record
			11/13/2020 20:47:56.071, acumensec, 192.168.254.15, Info, UserAccess, CUCMAdmin, Success, No, AdministrativeEvent, Cisco CUCM Administration CorrelationID :, Attempt to access data was successful. User is authorized to access sipProfileFindList, Cisco Tomcat, , jabber.acumensec.local, 242 11/13/2020 20:47:58.727, acumensec, 192.168.254.15, Info, UserAccess, CUCMAdmin, Success, No, AdministrativeEvent, Cisco CUCM Administration CorrelationID :, Attempt to access data was successful. User is authorized to access sipProfileFindList, Cisco Tomcat, , jabber.acumensec.local, 243 11/13/2020 20:48:06.547, acumensec, 192.168.254.15, Info, UserAccess, CUCMAdmin, Success, No, AdministrativeEvent, Cisco CUCM Administration CorrelationID :, Attempt to access data was successful. User is authorized to access sipProfileEdit, Cisco Tomcat, , jabber.acumensec.local, 244 11/13/2020 20:48:22.603, acumensec, 192.168.254.15, Info, UserAccess, CUCMAdmin, Success, No, AdministrativeEvent, Cisco CUCM Administration CorrelationID :, Attempt to access data was successful. User is authorized to access resetApplyConfigMultiple, Cisco Tomcat, , jabber.acumensec.local, 245
FPT_TUD_EXT.1	Initiation of update; result of the update attempt (success and failure)	None.	See FMT_MOF.1/ManualUpdate

FPT_STM_EXT.1	Discontinuous changes to time – either Administrator actuated or changed via an automated process. (Note that no continuous changes to time need to be logged. See also application note on FPT_STM_EXT.1)	For discontinuous changes to time: The old and new values for the time. Origin of the attempt to change time for success and failure (e.g., IP address).	06/26/2020 10:08:46 ntp_validate_servers.sh|response=26 Jun 10:08:37 ntpdate[13308]: ntpdate 4.2.6p5@1.2349-o Wed Aug 21 19:36:39 UTC 2019 (1) Looking for host 10.1.2.181 and service ntp transmit(10.1.2.181) receive(10.1.2.181) transmit(10.1.2.181) receive(10.1.2.181) transmit(10.1.2.181) transmit(10.1.2.181) transmit(10.1.2.181) server 10.1.2.181, port 123 stratum 3, precision -26, leap 00, trust 000 refid [10.1.2.181], delay 0.02671, dispersion 24.00006 transmitted 4, in filter 4 reference time: e29f2677.c4c30db8 Thu, Jun 26 2020 9:34:47.768 originate timestamp: e29f2e67.fb735f5f Thu, Jun 26 2020 10:08:39.982 transmit timestamp: e29f2e6b.fb05c76a Thu, Jun 26 2020 10:08:43.980 filter delay: 0.02671 0.02699 0.00000 0.00000 0.00000 0.00000 0.00000 0.00000 filter offset: 0.001282 0.001417 0.000000 0.000000

Requirement	Auditable Events	Additional Audit Record Contents	Sample Audit Record
			0.000000 0.000000 0.000000 0.000000 delay 0.02671, dispersion 24.00006 offset 0.001282 26 Jun 10:08:45 ntpdate[13308]: adjust time server 10.1.2.181 offset 0.001282 sec|<LVL::Debug>
FTA_SSL_EXT.1	The termination of a local session by the session locking mechanism.	None.	Nov 14 19:32:09, jabber, Info, login, : pam_unix(login:session): session closed for user acumensec, 6498
FTA_SSL.3	The termination of a remote session by the session locking mechanism.	None.	11/14/2020 20:13:39.920, acumensec, 10.1.2.122, Info, UserLogging, CUCMAdmin, Success, No, CriticalEvent, Cisco CUCM Administration CorrelationID :, Successfully Logged out Cisco Unified Administration Web Pages, Cisco Tomcat, , jabber.acumensec.local, 7422020
FTA_SSL.4	The termination of an interactive session.	None.	Nov 14 20:46:38, jabber, Info, login, : pam_unix(login:session): session closed for user acumensec, 6730 11/14/2020 20:59:36.378, acumensec, 10.1.2.122, Info, UserLogging, CUCMAdmin, Success, No, CriticalEvent, Cisco CUCM Administration CorrelationID :, Successfully Logged out Cisco Unified Administration Web Pages, Cisco Tomcat, , jabber.acumensec.local, 783

Requirement	Auditable Events	Additional Audit Record Contents	Sample Audit Record
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.	See FCS_TLSC_EXT.1/2, FCS_TLSS_EXT.1/2, FCS_NTP_EXT.1
FTP_TRP.1/Admin	Initiation of the trusted path. Termination of the trusted path. Failures of the trusted path functions.	None	See FCS_HTTPS_EXT.1

3.2.4.2 Audit Trail Capacities

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.
- LogPartitionHighWaterMarkExceeded (% disk space): When the disk usage is above the percentage that you specify, LPM sends an alarm message to syslog.
- SparePartitionLowWaterMarkExceeded (% disk space): When the disk usage is above the percentage that you specify, LPM sends out an alarm message to syslog.
- SparePartitionHighWaterMarkExceeded (% disk space): When the disk usage is above the percentage that you specify, LPM sends a n alarm message to syslog.

To utilize log partition monitor, verify that the Cisco Log Partitioning Monitoring Tool service, a network service, is running on Cisco Unified Serviceability on the server or on each server in the cluster (if applicable). ***Warning***, stopping the service causes a loss of feature functionality.

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.

To configure Log Partitioning Monitoring, set the alert properties for the LogPartitionLowWaterMarkExceeded and LogPartitionHighWaterMarkExceeded alerts in Alert Central.

If the percentage of disk usage is above the high water mark that you configured, the system sends an alarm message to and automatically purges log files until the value reaches the low water mark.

Also, see Alarms, Trace and Tools and Reports in **[14]**.

3.3 System Logs

The UCS platform system log records provide real-time status of the system as it relates to current connections, CPU usage, storage capacity and fan and power status. The Authorized Administrator can access the UCS server properties using the GUI.

The UCS server properties includes information on the CPU, memory and storage properties. Accessing the Chassis Sensors page, the Authorized Administrator can view current connections, NTP status CPU usage, memory usage disk and file storage and audit storage status. The GUI also provides fault summary and history and system events for troubleshooting. To access the health status and logs using the GUI, refer to **[18]** Viewing Server Properties, Viewing Sensors, Viewing Faults and Logs and Troubleshooting sections.

No additional configuration is required to ensure protection/prevent unauthorized deletion of audit records. Only Authorized Administrators are granted access to the log files. Any non-authorized access is denied. No specific configuration is required to implement the logging access control.

The CUCM also has the capabilities to provide alarms that provides information on the runtime status and state of the system, so that the Authorized Administrator can troubleshoot problems that are associated with the system. See Manage Reports **[17]** and **[3]** Monitor System Status.

3.4 VVoIP Endpoint Devices and User Association

The TOE supports analog telephone adapter that acts as an interface between analog VVoIP endpoints such as telephones,Cisco IP Phones, and third party SIP endpoints. To configure the profiles and templates that define the services, features, and directory numbers that associate with a particular device refer to **[5]** Endpoint Devices Overview.

- Device Profiles
  - A device profile defines the services, features, and directory numbers that associate with a particular device. You can configure a device profile and then you can assign the user device profile to a user, so that when the user logs in to a device, those features and services are available on that device.
- SIP Profiles for End Points
  - A SIP profile comprises the set of SIP attributes that are associated with SIP endpoints. SIP profiles include information such as name, description, timing,

retry, call pickup URI, and so on. The profiles contain some standard entries that cannot be deleted or changed.

- Device Profiles and Templates
  - Cisco Unified Communications Manager also supports a default device profile. Cisco Unified Communications Manager uses the default device profile whenever a user logs on to a phone model for which no user device profile exists.

To associate users to endpoints, first you must configure end users and application users. The end user can control devices that they are associated with, whereas applications that are identified as users can control devices, such as phones and CTI ports. Refer to **[5]** Associate Users with Endpoints.

3.5 Network Protocols and Cryptographic Settings

3.5.1 Certificates

CUCM uses certificates to secure client and server identities. After root certificates are installed, certificates are added to the root trust stores to secure connections between endpoints (users), including devices and application users, peer ESCs and servers (e.g, syslog). Peer ESCs and syslog servers are referenced by DNS name which must match the DNS name in the subjectAltName-DNS extension of the presented certificate. To add a syslog server refer to section 3.2.4 in this document. To add a peer ESC, refer to the Add Subscriber Nodes step in the Installation Tasks chapter of [**10**].

Cisco Certificate Authority Proxy Function (CAPF) is a Cisco proprietary service that issues Locally Significant Certificates (LSCs) to VVoIP endpoints and authenticates those endpoints. CAPF must configured for Offline usage. Refer to the CAPF Configuration Task Flow chapter in the Security Guide [**6**]. VOIP clients are referenced by DNS name or Distinguished Name which must match the subjectAltName-DNS extension or DN field, respectively, in the presented certificate.

To enable the secure communications on CUCM service nodes, perform the following steps from the CUCM Administrator GUI:

- Configure certificate exchange between CUCM, remote syslog server and VVR server.
- Upload CA signed certificates to CUCM.

- Configure SIP security settings on CUCM for the TLS peer subject.

The Authorized Administrator can view the fingerprint of server certificates, regenerate self-signed certificates, and delete trust certificates using the CUCM Administrator GUI **[6]** Security Basics -> Certificate Setup. Administrators can also regenerate and view self-signed certificates at the command line interface (CLI).

To find a certificate, perform the following steps from the CUCM Administrator GUI:

Step 1 In Cisco CUCM Administration, choose System > Security > Certificate.

The Find and List Certificates window displays. Records from an active (prior) query may also display in the window.

Step 2 To find all records in the database, ensure the dialog box is empty; go to Step 3.

To filter or search records

a. From the first drop-down list box, choose a search parameter.
b. From the second drop-down list box, choose a search pattern.
c. Specify the appropriate search text, if applicable.

Note To add additional search criteria, click the + button. When you add criteria, the system searches for a record that matches all criteria that you specify. To remove criteria, click the – button to remove the last added criterion or click the Clear Filter button to remove all added search criteria.

Step 3 Click Find.

All matching records display. You can change the number of items that display on each page by choosing a different value from the Rows per Page drop-down list box.

Step 4 From the list of records that display, click the link for the record that you want to view.

Note To reverse the sort order, click the up or down arrow, if available, in the list header.

The window displays the item that you choose.

To upload certificates, perform the following steps from the CUCM Administrator GUI:

Step 1 From Cisco CUCM Administration, choose Security > Certificate Management. The Certificate List window appears.

Step 2 Click Upload Certificate/Certificate chain. The Upload Certificate/Certificate chain window appears.

Step 3 From the Certificate Purpose drop-down box, select a system security certificate, such as CallManager-CERT.

Step 4 In the Description field, enter a name for the certificate.

Step 5 In the Upload File field, click Choose File to browse for the certificate file that you want to distribute for all the servers in the cluster.

Step 6 Click Upload.

The following procedure describes how to import the Cisco CUCM certificate to the root certificate trust store for Internet Explorer 8.

Step 1 Browse to application on the Tomcat server (for example, enter the hostname, localhost, or IP address for Cisco CUCM Administration in the browser). The browser displays a Certificate Error: Navigation Blocked message to indicate that this website is untrusted.

Step 2 To access the server, click Continue to this website (not recommended). The Cisco CUCM Administration window displays, and the browser displays the address bar and Certificate Error status in red.

Step 3 To import the server certificate, click the Certificate Error status box to display the status report. Click the View Certificates link in the report.

Step 4 Verify the certificate details.

Step 5 Select the General tab in the Certificate window and click Install Certificate. The Certificate Import Wizard launches.

Step 6 To start the Wizard, click Next. The Certificate Store window displays.

Step 7 Verify that the Automatic option, which allows the wizard to select the certificate store for this certificate type, is selected and click Next.

Step 8 Verify the setting and click Finish. A security warning displays for the import operation.

Step 9 To install the certificate, click Yes. The Import Wizard displays "The import was successful."

Step 10 Click OK. The next time that you click the View certificates link, the Certification Path tab in the Certificate window displays "This certificate is OK."

Step 11 To verify that the trust store contains the imported certificate, click Tools > Internet Options in the Internet Explorer toolbar and select the Content tab. Click Certificates and select the Trusted Root Certifications Authorities tab. Scroll to find the imported certificate in the list. After importing the certificate, the browser continues to display the address bar and a Certificate Error status in red. The status persists even if you reenter the hostname, localhost, or IP address or refresh or relaunch the browser.

If the validity of a certificate cannot be established, refer to Manage Certificates **[13]** for troubleshooting certificate errors.

3.5.2 Generating a Certificate Signing Request (CSR)

You can generate a certificate signing request (CSR) that contains the certificate application information that the certificate authority uses to generate the trusted certificate. Following are the primary steps to follow, also refer to **[13]** for more details.

Procedure

Step 1 From Cisco Unified OS Administration, choose Security > Certificate Management.

Step 2 Click Generate CSR.

Step 3 Configure the fields on the Generate Certificate Signing Request window (these fields include Common Name, as required). See the online help for more information about the fields and their configuration options.

Step 4 Click Generate CSR.

After the CSR has been generated, you will need to download the CSR to submit to the certificate authority.

Procedure

Step 1 From Cisco Unified OS Administration, choose Security > Certificate Management.

Step 2 Click Download CSR.

Step 3 Choose the certificate name from the Certificate Purpose drop-down list.

Step 4 Click Download CSR.

Step 5 (Optional) If prompted, click Save.

The CSR can now be submitted to your certificate authority.

3.5.3 Remote Administration Protocols

The Authorized Administrates manages the TOE by connecting via a web browser. The remote administration sessions are protected by HTTPS/TLS. The evaluated configuration requires that when connecting to the TOE over HTTPS/TLS for administrative management, TLS1.2 is used with the following ciphersuites:

- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384

To restrict usage to the above ciphersuites, in the Cisco Unified OS Administration menu, navigate to Security --> Cipher Management

Under All TLS sections insert the following:

ECDHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-SHA384:ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES256-SHA384:AES256-SHA:AES128-SHA

TLS v1.2 is the only version of TLS allowed by default. No configuration is necessary.

To enable HTTPS, you must download a certificate that identifies the server during the connection process. You can accept the server certificate for the current session only, or you can download the certificate to a trust folder (file) to secure the current session and future sessions with that server. The trust folder stores the certificates for all your trusted sites.

Cisco CUCM supports the following operating systems and browsers for connection to the Cisco Tomcat web server application in Cisco CUCM Service:

- Firefox with Windows 10 (64 bit)—Latest browser version only
- Chrome with Windows 10 (64 bit)—Latest browser version only
- Internet Explorer 11 with Windows 10 (64 bit)
- Internet Explorer 11 with Windows 8.1 (64 bit)
- Internet Explorer 11 with Windows 7 (64 bit)
- Microsoft Edge browser with Windows 10 (32 bit/64 bit)
- Safari with MacOS (10.x)—Latest browser version only

For instructions on how to download and store the certificate, see 3.5.1 Certificates in this document for more information, setup and configuration.

After the initial configuration, use the following procedures to log into the server and log in to Cisco CUCM Administration.

Step 1 **Start your preferred operating system browser**.

Step 2 **In the address bar of the web browser, enter the following case-sensitive URL**:

https://<Unified CM-server-name>:{8443}/ccmadmin/showHome.do

where: <Unified CM-server-name> **equals the name or IP address of the server**

Note: You can optionally specify a port number.

Step 3 A Security Alert dialog box displays. Click the appropriate button.

Step 4 At the main Cisco Unified Communications Manager Administration window, enter the username and password that you specified during Cisco Unified Communications Manager installation and click Login.

For security purposes, Cisco Unified Communications Manager Administration logs you out after 30 minutes of inactivity, and you must log back in.

If the HTTPS/TLS connection fails for an unknown reason, you can attempt to re-establish the connection and you will want to check the alert and trace logs for a possible cause. You may also need to use the Cisco Unified Serviceability application to start or restart services on the Cisco Unified Communications Manager nodes. Cisco Unified Serviceability is a web-

based troubleshooting tool. Refer to **[10]** Installation Planning, **[6]** Security Basics and **3]** Manage Security.

3.5.4 SIP Connections and Protocols

The Assured Services SIP (AS-SIP) endpoints are SIP endpoints compliant with MLPP, DSCP, TLS/SRTP, and IPv6 requirements. AS-SIP provides for multiple endpoint interfaces on the TOE. The Third-Party AS-SIP Endpoint device type allows a third-party AS-SIP-compliant generic endpoint to be configured and used with CUCM **[5]**.

In the evaluated configuration, the SIP connections are secured with TLS.

For the SIP connections, TLS v1.2 is supported with the following ciphersuites:

- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384

To restrict usage to the above ciphersuites, in the Cisco Unified OS Administration menu, navigate to Security --> Cipher Management

Under All TLS sections insert the following:

ECDHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-SHA384:ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES256-SHA384:AES256-SHA:AES128-SHA

TLS v1.2 is the only version of TLS allowed by default. No configuration is necessary.

Setting up a SIP Trunk profile allows you to a single security profile to multiple SIP trunks. Security-related settings include device security mode, digest authentication, encryption (including TLS settings), port settings (should be set to port 5061) and incoming/outgoing transport type settings.

Refer to Security for SRST References, Trunks, and Gateways -> SIP Trunk Security Profile Setup in **[6].**

The SIP profile configuration settings contain an 'Is Assured SIP Service Enabled' checkbox. This should be checked for third-party AS-SIP endpoints, as well as AS-SIP trunks. This

setting provides specific Assured Service behavior that affects services such as Conference factory and SRTP. Refer to Security for SRST References, Trunks, and Gateways -> Secure Survivable Remote Site Telephony (SRST) Reference in **[6]. Note,** SRTP allowed must be set.

For the phone security profile configuration, use the System > Security > Phone Security Profile menu path to configure phone security profiles. The Phone Security Profile window includes security-related settings such as device security mode, CAPF settings, digest authentication settings (only for phones that are running SIP), and encrypted configuration file settings. You must apply a security profile to all phones that are configured in Unified CM Administration. Refer to Security for Cisco Unified IP Phone and Cisco Voice-Messaging Ports -> Phone Security -> Phone Security Profile Setup in **[3]**.

To set the TLS enterprise parameters for all SIP connections, refer to **[5]** Configure Initial Parameters for the System -> Configure System and Enterprise Parameters. Also refer to SIP Trunk Encryption in **[6]** for TLS and SRTP settings to support secure calls.

3.5.5 Clusters and Nodes

A cluster comprises a set of Cisco CUCM servers that share the same database and resources. You can configure the servers in a cluster in various ways to perform various functions such as database replication.

For the Cisco CUCM servers that form a cluster, you should, as much as possible, evenly balance the CUCM services load across the system by distributing the devices (such as users per cluster and number of contacts per user) among the various Cisco CUCM servers in the cluster.

Following are the stability requirements for CUCM:

- Six nodes per cluster
- 45,000 users per cluster with a maximum of 15,000 users per node in a full Unified Communication (UC) mode deployment
- 15,000 users per cluster in a presence redundancy group, and 45,000 users per cluster in a deployment with High Availability.
- Administrable customer-defined limit on the maximum contacts per user (default unlimited)

- The IM and Presence Service continues to support inter-cluster deployments with the multi-node feature.

Scalability depends on the number of clusters in your deployment. CUCM clusters can support up to six nodes. If you originally installed less than six nodes, then you can install additional nodes at any time. Refer to **[10]** Installation Planning -> Subnet Limitations and Cluster Size and **[11]** for updates and changes.

You will also need to ensure the DNS Server is configured to include the all CUCM Service node names in the cluster and set to the FQDN or IP address rather than the hostname. Refer to Installation Tasks **[10]** and Configure Server Information **[5]**.

3.5.6 Clusters and Route Patterns

A cluster comprises a set of Cisco Unified Communications Manager servers that share the same database and resources. You can configure the servers in a cluster in various ways to perform various functions such as database replication.

For the Cisco Unified Communications Managers that form a cluster, you should, as much as possible, evenly balance the call-processing load across the system by distributing the devices (such as phones, gateways, CTI route points, CTI ports, and route lists) among the various Cisco Unified Communications Managers in the cluster. To distribute the devices, you configure Cisco Unified Communications Manager groups and device pools and then assign the devices to the device pools in a way that achieves the balance that you want.

You can use various nodes in the cluster for call-processing redundancy and for load balancing Cisco Unified Communications Manager uses route patterns to route or block both internal and external calls.

For ease of balancing, you can setup and configure route patterns. Cisco Unified Communications Manager uses route patterns to route or block internal and external calls. You can assign route patterns to gateways, to trunks, or to a route list, that contains one or more route groups. The route pattern can point directly to a gateway; it is recommend that you configure route lists and route groups. This approach provides the greatest flexibility in call routing and scalability. Refer to **[5]** Enable Inbound and Outbound Calling and Configure the Dial Plan.

4 Secure Management

4.1 User Roles

During the initial setup of the TOE the user that installs the TOE is deemed the Authorized Administrator and has full permissions and access to manage the TOE. Refer to **[3]**, **[5]** and **[6]**

The Authorized Administrator is responsible for managing users and users' access. The end users can be assigned to access control groups, which are associated to a role. Each role defines a set of permissions for a specific resource within Cisco Unified Communications Manager.

When you assign a role to an access control group and then assign end users to that access control group, you grant those end users all the access permissions that are defined by the role. Upon installation Cisco Unified Communications Manager comes with predefined default roles that are assigned to predefined default access control groups. You can assign your end users to the default access control groups, or you can customize access settings by setting up new access control groups and roles. Refer to **[3]** Manage Users.

The Authorized Administrator will also need to configure end users. The end users are the consumers of the TOE. End users can be assigned to phones and directory numbers thereby allowing your end users to make calls and communicate with other users in the system as well as placing calls. Refer to Configure End User **[5]**.

4.2 Clock Management

The TOE maintains a clock that is used as the source for the date and time stamp in the audit trail records to record the time of the event. The clock timing is also used to monitor inactivity of administrator sessions.

In the evaluated configuration, it is required to configure CUCM with NTP to synchronize time. CUCM supports NTP v4 and by default, the TOE does not accept broadcast and multicast NTP packets. The administrator must configure CUCM to update its time using NTP with SHA1 symmetric-key enabled. Refer to "Add an NTP Server" and "Configure NTP Authentication via Symmetric Key" sections of [**5**]. Multiple NTP servers may be configured.

When the time clock is synchronized with NTP you will want to setup Phone NTP references and date/time groups **[5]** Core Settings for Device Pools Overview -> Phone NTP References.

The Phone NTP reference ensures that an IP phone that is running SIP gets its date and time from an NTP server. If a phone that is running SIP cannot get its date and time information from the provisioned “Phone NTP Reference,” the phone receives this information when it registers with Cisco Unified Communications Manager.

The date/time groups define time zones for the various devices that are connected to Cisco Unified Communications Manager. The default group, CMLocal, configures automatically upon installation. However, it is recommended that you configure a group for each local time zone.

The TOE is configured to sync time with an NTP server using the GUI configuration window under System the NTP server and settings can be configured. Refer to Administration Overview -> Configuration Menus and Administration Overview -> Operating System Administration Overview -> NTP Server settings **[3]**.

4.3 Identification and Authentication

Configuration of Identification and Authentication settings is restricted to the Administrator.

The CUCM can be configured to use any of the following authentication methods. Local authentication is the default setting and is required in the evaluated configuration.

- Local authentication (password authentication);
    - Note: this is the default authentication configuration and should also be configured as a fallback authentication mechanism if the remote authentication server is not available.

Users log off the TOE on the GUI by selecting “Logout” in the upper right hand corner of the administrative interface and by the “logout” command at the local CLI interface.

4.4 Login Banners

The TOE may be configured by the Administrator to display a login warning banner that displays in the following CUCM interfaces: Cisco CUCM Administration, Cisco CUCM Operating System Administration, Cisco CUCM Serviceability, Cisco CUCM Reporting, and CUCM Disaster Recovery System. Refer to **[14]** Serviceability Administration Overview -> Customized Login Message.

To upload a customized log-on message, follow this procedure:

Step 1 Create a .txt file with the contents you want to display in the banner.

Step 2 Sign in to Cisco CUCM Operating System Administration.

Step 3 Choose Software Upgrades > Customized Logon Message.

Step 4 Click Browse and locate the .txt file.

Step 5 Click Upload File.

The banner will appear before and after login on most CUCM Service interfaces.

The .txt file must be uploaded to each CUCM Service node separately

This banner is displayed before the username and password prompts.

4.5 Product Updates

Verification of authenticity of updated software is done in the same manner as ensuring that the TOE is running a valid image. Refer to Upgrade Planning and Upgrade Tasks section of [**20**] to perform an upgrade of the CUCM software.

5 Security Relevant Events

The TOE is able to generate audit records that are stored internally within the TOE whenever an audited event occurs, as well as archiving to a remote storage area/syslog server. The details for protection of that communication are covered in Section 3.2.4 Logging Configuration of this document. Also, refer to the following sections in **[14]**, Alarms Trace, Tools and Reports and Audit Logs.

The TOE generates an audit record whenever an audited event occurs. The types of events that cause audit records to be generated include, cryptography related events, identification and authentication related events, and administrative events (the specific events and the contents of each audit record are listed in the table below). Each of the events is specified in syslog records 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.

The local audit trail consists of the individual audit records; one audit record for each event that occurred. Refer to 3.2.4 Logging Configuration of this document for the security relevant events that are applicable to the TOE.

The TOE also provides alarms related to the system health, such as current connections, CPU usage, memory usage, disk and file storage capacity, as well as fan and poser status as applicable.

6 Network Services and Protocols

The table below lists the network services/protocols available on the TOE as a client (initiated outbound) and/or server (listening for inbound connections), all of which run as system-level processes. The table indicates whether each service or protocol is allowed to be used in the certified configuration.

For more detail about each service, including whether the service is limited by firewall mode (routed or transparent), or by context (single, multiple, system), refer to the ***Command Reference*** guides listed in Table 3.

Table 10: Protocols and Services

Service or Protocol	Description	Client (initiating)	Allowed	Server (terminating)	Allowed	Allowed use in the certified configuration
FTP	File Transfer Protocol	Yes	No	No	n/a	Use HTTPS instead.
HTTP	Hypertext Transfer Protocol	Yes	No	Yes	No	Use HTTPS instead.
HTTPS	Hypertext Transfer Protocol Secure	Yes	Yes	Yes	Yes	No restrictions.
NTP	Network Time Protocol	Yes	Yes	No	n/a	If used for time synchronization, secure through NTPv4.
SNMP	Simple Network Management Protocol	Yes (snmp-trap)	Yes	Yes	No	Outbound (traps) only.
SSH	Secure Shell	Yes	No	Yes	No	Use HTTPS instead
SSL (not TLS)	Secure Sockets Layer	Yes	No	Yes	No	Use TLS instead.

Service or Protocol	Description	Client (initiating)	Allowed	Server (terminating)	Allowed	Allowed use in the certified configuration
Telnet	A protocol used for terminal emulation	Yes	No	Yes	No	Use HTTPS instead.
TLS	Transport Layer Security	Yes	Yes	Yes	Yes	As described in the section 3.3 of this document.

7 Modes of Operation

The CUCM has two modes of operation, a non-secure mode (default mode) and a mixed mode (secure mode). The Non-secure mode is the default mode when a CUCM cluster (or server) is installed fresh. In this mode, CUCM cannot provide secure signaling or media services. To enable secure mode on a CUCM server/cluster, the Certificate Authority Proxy Function (CAPF) service must be enabled on the publisher and the Certificate Trust List (CTL) service must be enabled on the publisher and subscribers. Then the cluster can be changed from non-secure mode to mixed mode. The reason it is known as mixed mode is that in this mode CUCM can support both secured and non-secured endpoints. For endpoint security, Transport Layer Security (TLS) is used for signaling and Secure RTP (SRTP) is used for media.

8 Disk Erasure

The TOE provides the ability to sanitize physical/logical media. This is provided via the Module RAID Configuration Utility within the TOE. The following steps must be executed in order to perform the disk sanitation.

Step 1 Access the Module RAID Configuration Utility within the TOE

Step 2 Select the drive for sanitation

Step 3 Select the “Erase VD” option

Step 4 Select the “Thorough” option

Step 5 Select “yes”

After this is complete, the interface will provide you progress of the deletion until it is 100% complete. This operation will sanitize all data store on the disk.

9 Security Measures for the Operational Environment

Proper operation of the TOE requires functionality from the environment. It is the responsibility of the authorized administrator of the TOE to ensure that the Operational Environment provides the necessary functions, and adheres to the environment security objectives listed below. The environment security objective identifiers map to the environment security objectives as defined in the Security Target.

Table 11 Operational Environment Security Measures

Environment Security Objective	IT Environment Security Objective Definition
OE.PHYSICAL	Physical security, commensurate with the value of the TOE and the data it contains, is provided by the environment.
OE.NO_GENERAL_PURPOSE	There are no general-purpose computing capabilities (e.g., compilers or user applications) available on the TOE, other than those services necessary for the operation, administration and support of the TOE.
OE.NO_THRU_TRAFFIC_PROTECTION	The TOE does not provide any protection of traffic that traverses it. It is assumed that protection of this traffic will be covered by other security and assurance measures in the operational environment.
OE.TRUSTED_ADMIN	Security Administrators are trusted to follow and apply all guidance documentation in a trusted manner.
OE.UPDATES	The TOE firmware and software is updated by an Administrator on a regular basis in response to the release of product updates due to known vulnerabilities.
OE.ADMIN_CREDENTIALS_SECURE	The Administrator's credentials (private key) used to access the TOE must be protected on any other platform on which they reside.
OE.RESIDUAL_INFORMATION	The Security Administrator ensures that there is no unauthorized access possible for sensitive residual information (e.g. cryptographic keys, keying material, PINs, passwords etc.) on networking equipment when the equipment is discarded or removed from its operational environment.

Environment Security Objective	IT Environment Security Objective Definition
OE_SECURED_PLATFORM	The operating system of the network device does not provide an interface or other capability that can be used to adversely affect the TOE or its own functionality.

10 Related Documentation

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation at:

With CCO login:
http://www.cisco.com/en/US/partner/docs/general/whatsnew/whatsnew.html

Without CCO login:
http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS version 2.0.

You can access the most current Cisco documentation on the World Wide Web at the following sites:

- http://www.cisco.com
- http://www-china.cisco.com
- http://www-europe.cisco.com

10.1 Documentation Feedback

If you are reading Cisco product documentation on the World Wide Web, you can submit technical comments electronically. Click Feedback in the toolbar and select Documentation. After you complete the form, click Submit to send it to Cisco.

You can e-mail your comments to bug-doc@cisco.com.

To submit your comments by mail, for your convenience many documents contain a response card behind the front cover. Otherwise, you can mail your comments to the following address:

Cisco Systems, Inc., Document Resource Connection
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

10.2 Obtaining Technical Assistance

Cisco provides Cisco.com as a starting point for all technical assistance. Customers and partners can obtain documentation, troubleshooting tips, and sample configurations from online tools. For Cisco.com registered users, additional troubleshooting tools are available from the TAC website.

Cisco.com is the foundation of a suite of interactive, networked services that provides immediate, open access to Cisco information and resources at anytime, from anywhere in the world. This highly integrated Internet application is a powerful, easy-to-use tool for doing business with Cisco.

Cisco.com provides a broad range of features and services to help customers and partners streamline business processes and improve productivity. Through Cisco.com, you can find information about Cisco and our networking solutions, services, and programs. In addition, you can resolve technical issues with online technical support, download and test software packages, and order Cisco learning materials and merchandise. Valuable online skill assessment, training, and certification programs are also available.

Customers and partners can self-register on Cisco.com to obtain additional personalized information and services. Registered users can order products, check on the status of an order, access technical support, and view benefits specific to their relationships with Cisco.

To access Cisco.com, go to the following website:

http://www.cisco.com