Cisco Unified Communications Manager and the IM and Presence Service v12.5

CC Configuration Guide

Version: 0.5
Date: December 28, 2020

Table of Contents

Document Introduction

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

This document provides Guidance to IT personnel for the TOE, Cisco Unified Communications Manager and the IM and Presence Service v12.5. This Guidance document includes instructions to successfully install the TOE in the Operational Environment, instructions to manage the security of the TSF, and instructions to provide a protected administrative capability.

Revision History

Version	Date	Change
0.1	July 15, 2020	Initial Version
0.2	November 20, 2020	Updates for Check-Out
0.3	December 2, 2020	Additional Updates for Check-Out
0.4	December 7, 2020	Final Updates for Check-Out
0.5	December 28, 2020	Final Updates for Check-Out

1. Introduction

This Operational User Guidance with Preparative Procedures documents the administration of the Cisco Unified Communications Manager (CUCM) and the IM and Presence Service 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.

1.1. Audience

This document is written for administrators installing and configuring the TOE. This document assumes that you are familiar with the basic concepts and terminologies used in internetworking, and understand your network topology and the protocols that the devices in your network can use, 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. 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 Cisco Unified Communications Manager (CUCM) and the IM and Presence Service operations. All security relevant commands to manage the TSF data are provided within this documentation within each functional section.

1.3. Document References

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

Table 1 Cisco Documentation

#	Title	Link
[1]	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

#	Title	Link
[2]	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
[3]	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
[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]	Administration 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_5_1/admin/cucm_b_administration-guide-1251/cucm_b_administration-guide-1251_chapter_01111.html
[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
[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]	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
[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

#	Title	Link
[12]	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
[13]	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
[14]	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
[15]	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
[16]	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
[17]	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
[18]	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

#	Title	Link
[19]	Upgrade and Migration Guide for Cisco Unified Communications Manager and the IM and Presence Service, Release 12.5(1)	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. TOE Overview

The TOE is Cisco Unified Communications Manager (CUCM) and Instant Message and Presence Service v12.5. The TOE is an IP-based communications system integrating voice, video, data, and mobility products and applications enabling more effective and secure user communications.

1.5. Operational Environment

The TOE requires the following IT Environment Components when the TOE is configured in its evaluated configuration:

Table 2. Operational Environment Components

Component	Usage/Purpose/Description
Local Console	This includes any IT Environment Console that is directly connected to the CUCM and IM&P TOE components via the Serial Console Port. This is used by the Security Administrator to perform local administration.
Management Workstation	This includes any IT Environment Management workstation that can remotely access CUCM and IM&P administration interfaces with a web browser using HTTPS. This provides the Security Administrator the capability to perform remote administration over a trusted path.
(3) NTP Servers	The NTP servers provides the CUCM TOE component the ability to synchronize its clock to an accurate source of time and date. At least 3 NTP time sources must be provided to the CUCM TOE component.
Syslog Server	The Syslog server provides the TOE with the capability to transmit generated audit data over TLS.
Remote Endpoint	This includes any VoIP client with which the TOE communicates with over a protected TLS channel.

DNS Server	A DNS server provides the TOE with the capability to translate domain names to numeric IP addresses.
Certificate Authority (CA) and OCSP Responder	The Certificate Authority provides the TOE and VVoIP clients with valid certificates. The CA also provides the TOE with an OCSP Responder to check the peer certificate revocation status of devices the TOE communicates with on the network.

1.6. Excluded Functionality

The functionality listed below is not included in the evaluated configuration.

Table 3. Excluded Functionality and Rationale

Function Excluded	Rationale
Non-FIPS 140-2 mode of operation	The TOE includes FIPS mode of operation. The FIPS modes allows the TOE to use only approved cryptography. FIPS mode of operation must be enabled in order for the TOE to be operating in its evaluated configuration.

Additionally, the TOE includes a number of functions where there are no Security Functional Requirements that apply from the collaborative Protection Profile for Network Devices v2.1 or the Extended Package Enterprise Session Controller (ESC EP) Version 1.0. The excluded functionality does not affect the TOE's conformance to the claimed Protection Profiles.

1.7. TOE Acceptance

The administrator should perform the following actions to ensure the TOE is correct and that it has not been tampered with during delivery.

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).

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).

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.

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).

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.

6. Once the TOE is unpacked, inspect the unit. 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).

2. Installation

2.1. 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 the CUCM TOE component.

- 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**].

2.2. Physical Installation

Follow the instructions for the UCS model in [**1**] 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.

2.3. Hypervisor Installation

Follow the “Install and Configure VMware ESXi 6.5” section of the Installation and Configuration chapter in [**2**].

Note: The evaluated configuration of each CUCM and IM&P component is limited to only one vND instance for each physical platform. In addition there must be no other guest VMs providing non-network device functionality.

2.4. Initial Installation of CUCM

Follow the "Installation Tasks" Chapter of [**3**] to install Unified Communications Manager.

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

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 "Postinstall Tasks for Cisco Unified Communications Manager" section of the "Post-Installation Tasks" chapter in [**3**] will guide you through activating services and installing the license and [**6**] 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**].

2.5. Access Web GUI over HTTPS

From the Management workstation open a web browser to the IP address or fully-qualified domain name of the CUCM TOE component. To login use the username and password credentials created during installation. Users log off the TOE on the GUI by selecting "Logout" in the upper right hand corner of the administrative interface.

2.6. Access Local Console CLI

From the VMWare Host Client, open a console window to the virtual machine. To login use the username and password credentials created during installation. Users log off by entering "logout" command at the local CLI interface.

2.7. Initial Installation of IM&P

Follow the "Installation Tasks" Chapter of [**3**] to install the IM and Presence Service. Be sure to perform the steps to Add Subscriber Nodes to the Unified Communications Manager publisher node before installing IM&P.

The Initial configuration will setup the server name, IP Address, Admin ID, default certificate information. You will need to provide the CUCM publisher host name, IP address, and Security Password.

Follow the "Troubleshooting " Chapter of [**3**] should an error occur during the installation process where the IM&P node fails to register with the CUCM TOE Component.

2.8. Verify TOE Software

The TOE ships with the correct software image pre-installed however this may not be the CC validated version. Follow the steps below to verify if you have the CC validated version.

1. In the Administrator Window, click "About" and not the System Version.

Table 4. Evaluated Software Images

TOE Component	Software Version	Image
Unified Communications Manager	12.5.1.12900-115	UCSInstall_UCOS_12.5.1.12900-115.sgn.iso
IM and Presence Service	12.5.1.12900-25	UCSInstall_CUP_12.5.1.12900-25.sgn.iso

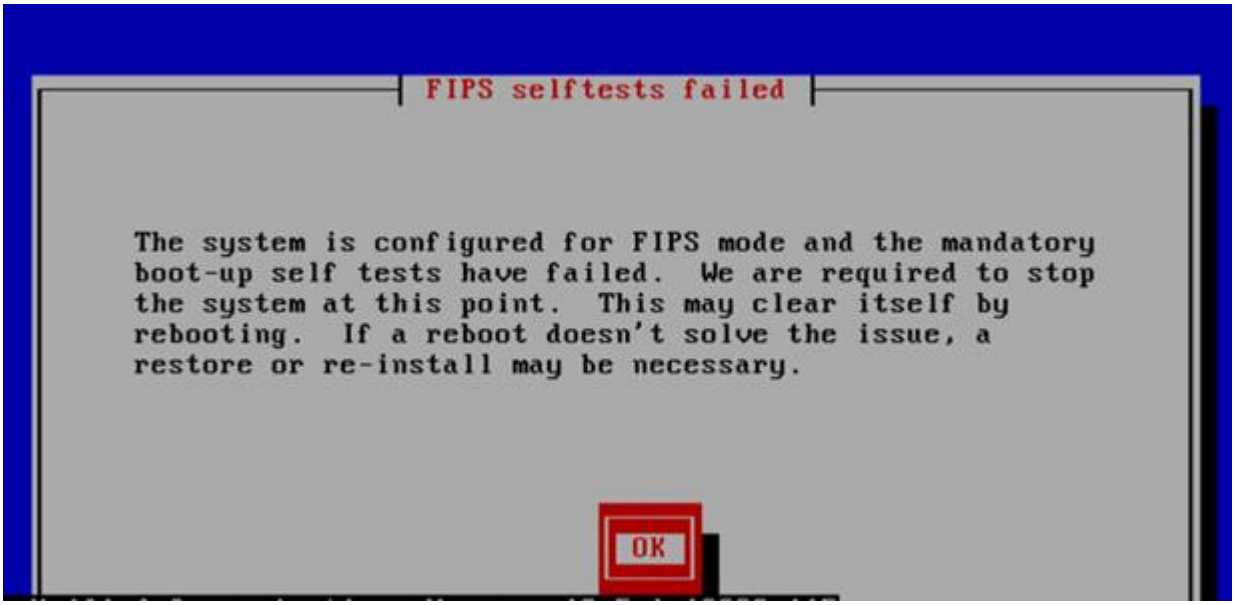
2. If the version does not correspond to the table above, you will need to contact Cisco and obtain an updated image. Refer to Upgrade Planning and Upgrade Tasks section of [**19**] to perform an upgrade of the CUCM and IM and Presence software. If the digital certificate signatures on the software were modified in any way, the installation would halt, and a warning may be displayed at which time you need to Contact Cisco Technical Suppor. Refer to section 6, Contacting Cisco, in this document.

2.9. Enable FIPS Mode

All TOE components must be run in the FIPS mode of operation. Refer to FIPS 140-2 Mode Setup chapter of [**6**].

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 the "Contacting Cisco" section 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

2.10. Access Banner

On each TOE component, the administrator should configure an initial banner that describes restrictions of use, legal agreements, or any other appropriate information to which users consent by accessing the Controller. The banner will display on the CLI and HTTPS interface prior to allowing any administrative access.

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

1. Create a .txt file with the contents you want to display in the banner.
2. Sign in to Cisco CUCM Operating System Administration.
3. Choose Software Upgrades > Customized Logon Message.
4. Click Browse and locate the .txt file.
5. Click Upload File.

The .txt file must be uploaded to each TOE Component separately.

2.11. Administrator Configuration, Credentials and Session Termination

Note: The guidance in this section is performed on the CUCM TOE Component but will apply to both CUCM and IM&P TOE Components.

The CUCM TOE component 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 [**7**] 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 is recommended to be set to a minimum of at least 15 characters.
    - The TOE supports passwords which meet the following complexity requirements:
        - 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 [**5**] Configure Default Credential Policy. 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 a remote 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 [**18**] 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. Locked accounts may be unlocked by an administrator using the GUI by navigating to User Management > End User and unchecking the box for "Locked by Administrator".

3. Configuration

3.1. Certificates

3.1.1. CA Certificates

The evaluated configuration requires use of third-party CA certificates. 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. CA Certificates must select one of the "-Trust" certificate purposes. Next 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

Refer to [**7**] Manage Security -> Manage Certificates and [**13**].

3.1.2. Device Certificates (non-VVoIP Endpoints)

After CA certificates are installed, device certificates are added to the appropriate trust stores to secure connections between peer ESCs and syslog server. 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 peer ESC, refer to the Add Subscriber Nodes step in the Installation Tasks chapter of [**10**].

3.1.3. Generate 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.

1. From Cisco Unified OS Administration, choose Security > Certificate Management.
2. Click Generate CSR.
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.
4. Click Generate CSR.

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

1. From Cisco Unified OS Administration, choose Security > Certificate Management.
2. Click Download CSR.
3. Choose the certificate name from the Certificate Purpose drop-down list.
4. Click Download CSR.
5. If prompted, click Save.

The CSR can now be submitted to your certificate authority.

3.1.4. Import Certificates

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

1. From Cisco Unified OS Administration, choose Security > Certificate Management. The Certificate List window appears.
2. Click Upload Certificate/Certificate chain. The Upload Certificate/Certificate chain window appears.
3. From the Certificate Purpose drop-down box, select an identity:
    a. CallManager (CUCM only)
    b. CallManager-ECDSA (CUCM only)
    c. Tomcat
    d. Tomcat-ECDSA
    e. CAPF (CUCM only)

4. 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.
5. Click Upload.

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

3.2. TLS

The TOE implements TLS 1.2 in order to :

- Provide secure connections to a remote syslog server.
- Provide a secure HTTPS interface to the Administrator for remote administration.
- Provide secure SIP signaling (SIP over TLS).
- Provide secure inter-TOE communication between CUCM and IM&P TOE components.
- Provide secure connections to remote CUCM nodes.

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 when FIPS mode is enabled. No additional configuration is necessary.

3.3. Audit Logging Configuration

On each TOE component, the administrator must setup remote logging to a syslog server. Be sure you first have the syslog server setup and operational.

To set up audit logging, refer to the steps from the "Setup Audit Logging" chapter of [**13**]:

1. In Cisco Unified Serviceability, choose Tools > Audit Log Configuration.
2. From the Server drop-down menu, select any server in the cluster and click Go.
3. To log all cluster nodes, check the Apply to All Nodes check box.
4. In the Server Name field, enter the IP Address or fully qualified domain name of the remote syslog server.
5. Optional. To log configuration updates, including items that were modified, and the modified values, check the Detailed Audit Logging check box.
6. Complete the remaining fields in the Audit Log Configuration window. For help with the fields and their descriptions, see the online help.
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 of Syslog Server certificate.

The default transfer protocol to the syslog server is UDP. You will need to change this setting as described in the "Configure Remote Audit Log Transfer Protocol" section of [**13**]

1. Log in to the local Command Line Interface.
2. Run the **utils remotesyslog set protocol tls**

3.3.1. Audit Trail Capacities

Log Partition Monitoring (LPM), which is installed automatically with the CUCM and IM&P, uses configurable thresholds to monitor the disk usage of the log partition on a server. The Cisco Log Partition Monitoring Tool service starts automatically after installation of the 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 [**13**].

3.3.2. 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 [**17**] 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 [**7**] Monitor System Status.

3.4. Configure Time and Date

Each TOE component 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 the CUCM TOE component 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**].

The IM&P TOE component will automatically synchronize time to the CUCM TOE component over TLS.

3.5. CUCM Mixed Mode (Secure Mode)

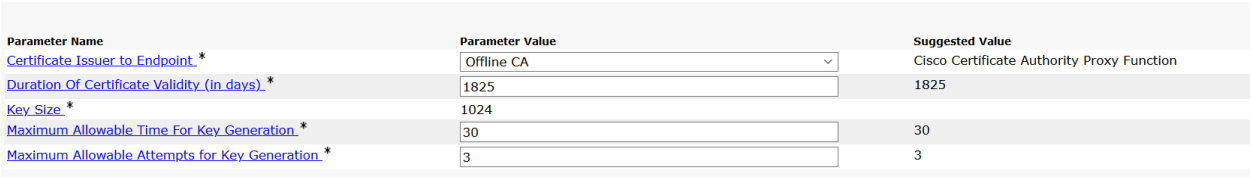
The CUCM TOE component must be configured in mixed mode (secure mode). To enable secure mode on a CUCM server/cluster, the Certificate Authority Proxy Function (CAPF) service must be enabled on the publisher and the Certificate Trust List (CTL) service must be enabled on the publisher and subscribers. 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. Refer to the “Cisco CTL Client Setup” Chapter of [**6**].

3.6. Device Certificates (VVoIP Endpoints)

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.

1. Ensure CA Third Party CA certificates are uploaded and the CAPF Service is running. Refer to the CAPF Configuration Task Flow chapter in the Security Guide [**6**].

2. From Service Parameter page set “certificate issuer to endpoint” field to Offline CA. (Restart CAPF service every time you change this field).



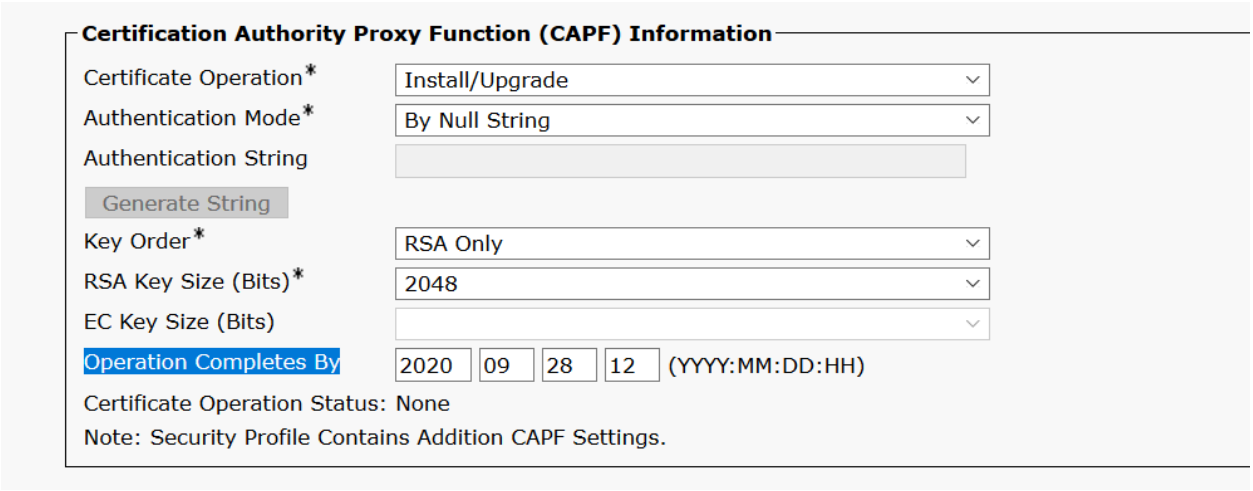
Parameter Name	Parameter Value	Suggested Value
Certificate Issuer to Endpoint *	Offline CA	Cisco Certificate Authority Proxy Function
Duration Of Certificate Validity (in days) *	1825	1825
Key Size *	1024	
Maximum Allowable Time For Key Generation *	30	30
Maximum Allowable Attempts for Key Generation *	3	3

3. Register an endpoint over 5060 port.

4. On the Phone Configuration page under “Certification Authority Proxy Function (CAPF) Information” configure the following fields. The other fields can have default values.

   - Certificate Operation – Install/Upgrade
   - Authentication Mode – Null string
   - Operation Completes By – Future date.

   Once the above values are set save the configuration and apply config. Do not reset the endpoint. After apply config “Certificate Operation Status” should change from None to Operation Pending.



5. Log into admin CLI and execute the command “utils capf csr count”:

   The Valid CSR count should increase depending on how many endpoints you have initiated Install/Upgrade

   (If there are 3 devices where you have initiated Install/Upgrade Valid CSR count should be 3)

   Count CSR/Certificate files.

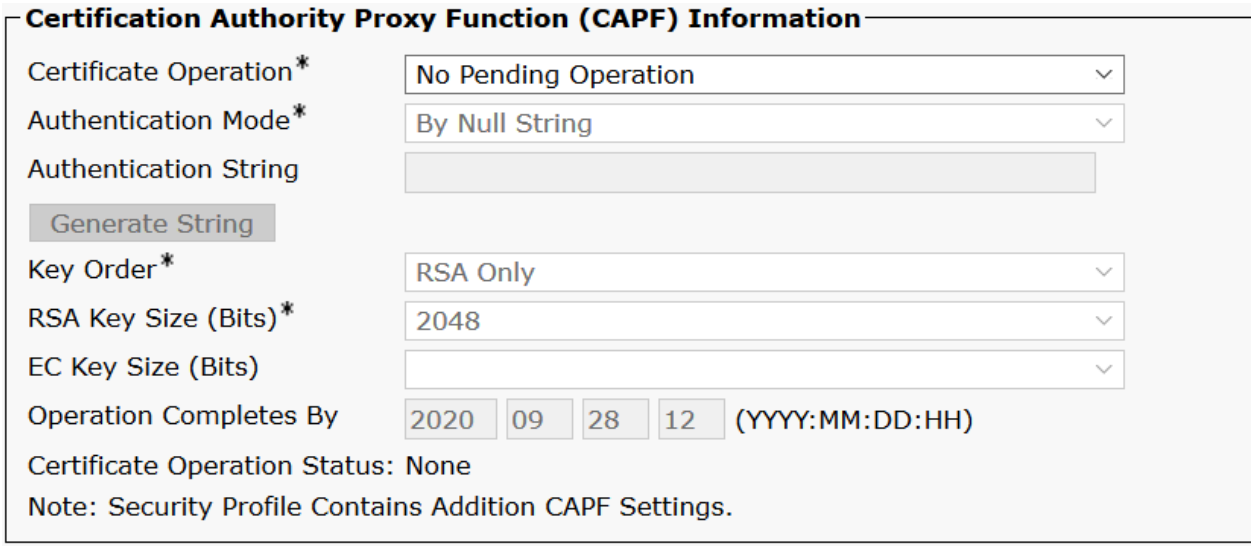
   Valid CSR : 0

   Invalid CSR : 0

Certificates: 0

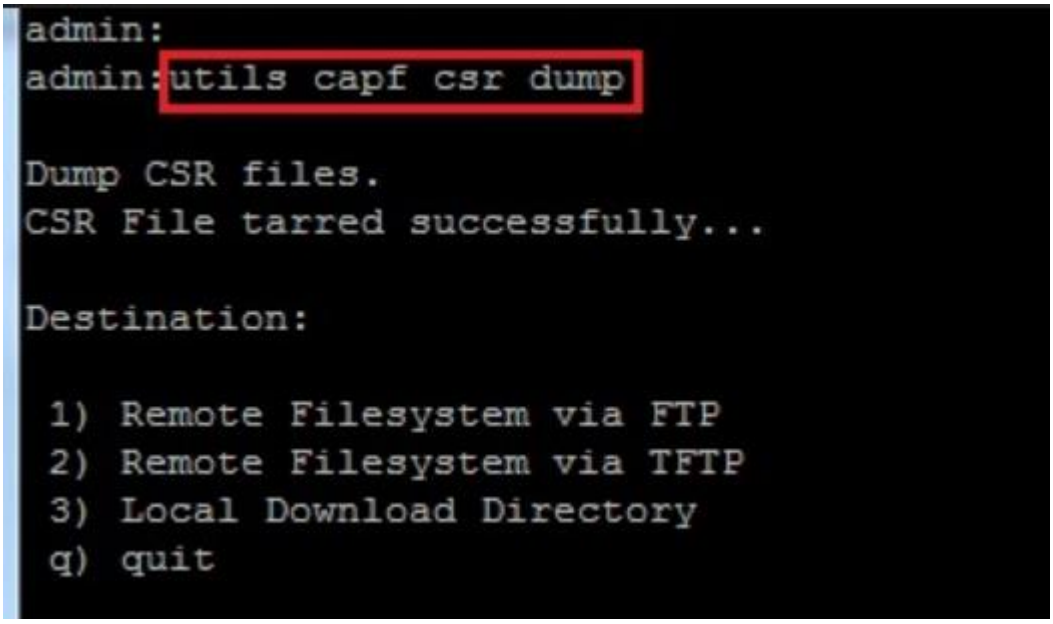
Note: If in the above step CSR count does not reflect properly.

a. Please set the “Certificate Operation” on the device page to “No Operation Pending”. Save, Apply Config and Reset Device.



b. Restart the Cisco Certificate Authority Proxy Function service and then repeat step 4 and step 5.

6. Dump the CSRs to the local server using the command “utils capf csr dump”, you can select option 3 to dump the tar file on the CUCM. The filename that needs to be specified has to be in the format “filename.tar”



7. Restart TFTP service from serviceability page. The dumped tar file can be retrieved from any server running tftp:

- Tftp <ip of the cucm where you have dumped the csr tar file>
- Get <filename.tar>

8. Untar the .tar file get the CSRs signed by the CA. If the certificates received are in .pem convert it to der format using the command “openssl x509 -in csr.pem -out csr.der -outform DER.
9. Once you have all the CA signed certificates, the tar them into one file using command ‘tar cvzf newFilename.tgz csr1.der
10. From OSAdmin page navigate to TFTPManagement page under Software Upgrades. Restart TFTP service after uploading the file to TFTPManagement page.
11. Run the command “utils capf cert import” from CLI:

    admin:utils capf cert import

    Importing files.

    Source:

    1) Remote Filesystem via FTP

    2) Remote Filesystem via TFTP

    q) quit

    Please select an option (1 - 2 or "q"): 2

    File Path: newFilename.tgz

    Server: <IP of the CUCM where you have uploaded the .tgz file>

    Certificate file imported successfully

    Certificate files extracted successfully.

    Please wait. Processing 1 files

12. On the Phone configuration page under “Certification Authority Proxy Function (CAPF) Information” the “Certificate Operation Status” should change from Operation pending to Upgrade success.

3.7. 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.

3.8. SIP Connections and Protocols

VVoIP endpoints uses SIP which is secured using 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.

3.9. Product Updates

Refer to “Upgrade Planning” and “Upgrade Tasks” section of [**19**] to perform an upgrade of the CUCM and IM&P software. The "Upgrade Sequence" and "Sequence Rules" in the Appendix of [**19**] provide guidance to the Administrator on the order to update TOE components. Table 3 in the Appendix describes the Service Impact when performing an upgrade task.

If the digital certificate signatures on the software updates for the CUCM or IM&P components were modified in any way, the update would halt, and a warning displayed at which time you need contact Cisco for support. Refer to the "Troubleshooting Unified Communications Manager Upgrades" and "Troubleshooting IM and Presence Upgrades" in the Appendix for information regarding upgrade errors or failures.

3.10. Disable IM&P TOE Component

To disable the IM&P TOE component from communicating with the CUCM TOE component, IM&P must be removed as a subscriber node.

Before proceeding, users must be assigned from the IM and Presence server before it can be removed. Follow the steps in the section below to unassign users from the IM and Presence server:

1. Select User Management > Assign Presence Users
2. Select optional end-user search parameters, and then click Find.

Matching records appear.

3. Check the check box beside the user records to unassign those users from the selected server.
4. Select Unassigned in the Assign Users pane, and then click Save.

   The selected users are unassigned from the IM and Presence Service servers.

Follow the steps below to remove the IM&P TOE component as a subscriber node:

1. Log in to the Unified Communications Manager publisher node.
2. From Cisco Unified CM Administration choose System > Server.
3. (Optional) Enter a search criteria filter
4. Click Find.
5. Click the Host Name/IP Address of the IM&P Server you wish to disable
6. If the “Presence Redundancy Group” does not equal “None”, Click the link next to “Presence Redundancy Group”
   a. Click Delete to remove the Presence Server from the Presence Redundancy Group Configuration
   b. Click OK.
7. From Cisco Unified CM Administration choose System > Server.
8. (Optional) Enter a search criteria filter
9. Click Find.
10. Click the Host Name/IP Address of the IM&P Server you wish to disable
11. Click Delete
12. Click OK.

3.11. 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.

1. Access the Module RAID Configuration Utility within the TOE
2. Select the drive for sanitation
3. Select the “Erase VD” option
4. Select the “Thorough” option

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.

4. Auditing

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

The TOE 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 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.

Each TOE component stores audit data locally and also transmit all audit messages in real-time to a specified external syslog server.

Table 5. Sample Audit Events

Requirement	Auditable Events	Additional Audit Record Contents	Sample Audit Record
FCS_TLSC_EXT.1 FCS_TLSC_EXT.2 FCS_TLSS_EXT.2	Failure to establish a TLS Session	Reason for failure	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 23:38:08.767 |ProcessReadData MESSAGE TEXT -- : 2308: jabber.acumensec.local: Nov 23 2020 04:38:08.767 UTC : %UC_CALLMANAGER-6-SSLConnectionFailure: %[PeerAddr=10.1.2.186][PeerPortNo=5061][ReasonCode=0][Reason= HandleSSLError - TLS protocol error(ssl reason code=(null) [0]),lib=(null) [0], fun=(null) [0], for 10.1.2.186:5061][AppID=Cisco CallManager][ClusterID=StandAloneCluster][NodeID=jabber.acumensec.local]: SSLConnectionfailedtoPeer Nov 22 05:09:42, jabber, Notice, Cisco CallManager, : 47: jabber.acumensec.local: Nov 22 2020 10:09:42.028 UTC : %UC_CALLMANAGER-5-SIPTrunkISV: %[DeviceName=CUCMIMPSIP][AvailableRemotePeers=cucmimp.acumensec.local, 10.1.2.186, 5061][ClusterID=StandAloneCluster][NodeID=jabber.acumensec.local]: All remote peers are available to handle calls for this SIP trunk, 8534

FCS_HTTPS_EXT.1 FCS_TLSS_EXT.1	Failure to establish a HTTPS Session Failure to establish a TLS Session;	Reason for failure.	**CUCM:** 10/09/2020 08:32:07.656, acumensec, 192.168.254.177, Warning, UserLogging, Cisco Call-Manager Administration, Failure, No, AdministrativeEvent, Cisco CallManager Administration CorrelationID :, Failed to Log into Cisco Unified CM Admin Webpages, Cisco Tomcat, , jabber.acumensec.local, 431 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 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 hackCount_ =0 timeHackedLockout_=0 timeOfLockout_ =0 timeLastChanged_=1583438452 timeLastHacked_

			=1605402202 userType_=2 endUserStatus_ =1 lastSuccessfulLoginTime_ = 1605402218 last-SuccessfulLoginIp_ = 10.1.2.122 lastUnsuccessfulLoginIp_ = 10.1.2.122 minCharsToChange_ = 1 **IM&P:** 11/17/2020 06:30:03.214, Some User, 192.168.254.177, Warning, UserLogging, Cisco Call-Manager User Console, Failure, No, AdministrativeEvent, Cisco CallManager User Console CorrelationID :, Failed to Log into Cisco Unified OS Admin Webpages, Cisco Tomcat, , CUCMIMP, 32 2020-11-17 04:56:19,666 INFO [http-bio-443-exec-12] services.ServiceUtil - Establishing a TLS connection to node :cucmimp.acumensec.local 2020-11-17 04:56:19,678 INFO [http-bio-443-exec-12] services.ServiceUtil - Successfully established TLS connection : Socket[addr=CUCMIMP.acumensec.local/10.1.2.186,port=8443,localport=60582]
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 11/30/2020 02:54:21 sd_ntp|[749] There are 1 NTP servers configured in the /etc/ntp.conf|<LVL::Info>

FIA_AFL.1	Unsuccessful login attempts limit is met or exceeded	Origin of the attempt (e.g., IP address).	**CUCM:** 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. **IM&P** 11/17/2020 06:30:03.214, Some User, 192.168.254.177, Warning, UserLogging, Cisco CallManager User Console, Failure, No, AdministrativeEvent, Cisco CallManager User Console CorrelationID :, Failed to Log into Cisco Unified OS Admin Webpages, Cisco Tomcat, , CUCMIMP, 32

FIA_UIA_EXT.1	All use of the identification and authentication mechanism.	Origin of the attempt (e.g., IP address).	**CUCM:** 11/06/2020 09:57:14.571, acumensec, 192.168.254.177, Info, UserLogging, CUCMAdmin, Success, No, CriticalEvent, Cisco CUCM Administration 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 **IM&P:** 10/13/2020 19:35:02.134, acumensec, 192.168.254.177, Info, UserLogging, CUCM IM&P Admin, Success, No, AdministrativeEvent Cisco Unified CM IM and Presence Administration CorrelationID :, Successfully Logged into Cisco Unified CM IM and Presence Web Pages, Cisco Tomcat, , CUCMIMP, 154 10/13/2020 19:45:29.201, acumensec, 192.168.254.177, Info, UserLogging, CUCM IM&P Admin, Success, No, CriticalEvent, Cisco Unified CM IM and Presence Administration CorrelationID :, Successfully Logged out Cisco Unified CM IM and Presence Web Pages, Cisco Tomcat, , CUCMIMP, 186 11/17/2020 06:30:17.746, Some User, 192.168.254.177, Warning, UserLogging, Cisco CallManager User Console, Failure, No, AdministrativeEvent, Cisco CallManager User Console CorrelationID :, Failed to Log into Cisco Unified OS Admin Webpages, Cisco Tomcat, , CUCMIMP, 33

FIA_UAU_EXT.2	All use of the identification and authentication mechanism.	Origin of the attempt (e.g., IP address).	
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 Nov 17 05:05:24, jabber, Info, Cisco CallManager, ccm: 12183: jabber.acumensec.local: Nov 17 2020 10:05:24.707 UTC : %UC_CALLMANAGER-6-SSLConnectionFailure: %[PeerAddr=10.1.2.186][PeerPortNo=5061][ReasonCode=0][Reason= HandleSSLError - TLS protocol error(ssl reason code=(null) [0]),lib=(null) [0], fun=(null) [0], for 10.1.2.186:5061][ClusterID=StandAloneCluster][NodeID=jabber.acumensec.local]: SSLConnectionfailedtoPeer, 8452

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.	**CUCM:** 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][Peer-PortNo=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]: SSLConnection-failedtoPeer

FIA_X509_EXT.1/Rev FIA_X509_EXT.1/ITT	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.	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 **IM&P:** 06:00:00.155 |ProcessReadData MESSAGE TEXT -- : 423: cucmimp.acumensec.local: Nov 79 2020 11:00:00.053 UTC : %UC_-3-UNKNOWN_ALARM:CertExpired: %[Message=Certificate expiration Notification. Certificate name:CA_RSA.der Unit:CAPF-trust Type:own-cert Expiration:Thu Sep 17 10:10:00:000][AppID=Cisco Certificate Monitor][ClusterID=][NodeID=cucmimp.acumensec.local]: 2020-12-07 05:41:45,854 INFO [http-bio-443-exec-16] element.Certificate.setRootCertificate - rootCertificate = [] 2020-12-07 05:41:45,855 INFO [http-bio-443-exec-16] element.PlatformFile.setName - name = [ICA.pem] 2020-12-07 05:41:45,855 INFO [http-bio-443-exec-16] element.PlatformFile.setPath - path = [/usr/local/sip/.security/proxy/trust-certs/ICA.pem] 2020-12-07 05:41:45,855 INFO [http-bio-443-exec-16] element.Certificate.setDescription - certificateDescription = [Trust Certificate]

			2020-12-07 05:41:45,855 INFO [http-bio-443-exec-16] manager.PlatformManager.readFile - Reading [/usr/local/sip/.security/proxy/trust-certs/CUCMIMP-EC.acumensec.local.description] 2020-12-07 05:41:45,855 INFO [http-bio-443-exec-16] manager.PlatformManager.readFile - Created reader [java.io.BufferedReader@49376f] 2020-12-07 05:41:45,855 INFO [http-bio-443-exec-16] manager.PlatformManager.readFile - Reading [/usr/local/sip/.security/proxy/trust-certs/CUCMIMP-EC.acumensec.local.description] 2020-12-07 05:41:45,855 INFO [http-bio-443-exec-16] manager.PlatformManager.readFile - Created reader [java.io.BufferedReader@d683a4] 2020-12-07 05:41:45,855 INFO [http-bio-443-exec-16] manager.PlatformManager.getUnitFromDescriptionFile - Unit from description File :null 2020-12-07 05:41:45,856 INFO [http-bio-443-exec-16] element.Certificate.setCertificateName - certificateName = [cup-trust]

FMT_MOF.1/ManualUpdate	Any attempt to initiate a manual update	None	**CUCM:** 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 /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> **IM&P:** 11/02/2020 12:47:15 file_list.sh|Parse argument fromVersion=12.5.1.12900-25|<LVL::Debug> 11/02/2020 12:47:15 file_list.sh|_set_upgrade_status_attribute: fromVersion set to 12.5.1.12900-25|<LVL::Debug> 11/02/2020 12:47:15 file_list.sh|Parse argument status=upgrade.stage.determining.files|<LVL::Debug> 11/02/2020 12:47:15 file_list.sh|_set_upgrade_status_attribute: status set to upgrade.stage.determining.files|<LVL::Debug> 11/02/2020 12:47:16 file_list.sh|Process local file system request|<LVL::Info> 11/02/2020 12:47:16 file_list.sh|Checking /common/download existence|<LVL::Debug> 11/02/2020 12:47:16 file_list.sh|List local directory /common/download|<LVL::Debug> 11/02/2020 12:47:16 file_list.sh|List directory complete (0)|<LVL::Debug> 11/02/2020 12:47:16 file_list.sh|List file (pre-filtered):|<LVL::Debug> 11/02/2020 12:47:16 file_list.sh|(CAPTURE) 12.5.1.13900-17|<LVL::Debug> 11/02/2020 12:47:16 file_list.sh|(CAPTURE) tmp|<LVL::Debug> 11/02/2020 12:47:16 file_list.sh|(CAPTURE) UCSInstall_CUP_12.5.1.13900-17.sgn.iso|<LVL::Debug>

			11/02/2020 12:47:16 file_list.sh|(CAPTURE) UCSInstall_CUP_12.5.1.13900-17.sgn.iso.md5|<LVL::Debug> 11/02/2020 12:47:16 file_list.sh|/opt/cisco/install/bin/filter file=/var/log/install/downloaded_versions|<LVL::Debug> 11/02/2020 12:47:56 file_list.sh|(CAPTURE) <InstallItem type="patch" secure-file="UCSInstall_CUP_12.5.1.13900-17.sgn.iso" version="12.5.1.13900-17" file="UCSInstall_CUP_12.5.1.13900-17.sgn.iso" reboot="no" signed="yes" unrestricted="no"/>|<LVL::Debug> 11/02/2020 12:47:56 file_list.sh|(CAPTURE) <FilteredItem type="unknown" file="UCSInstall_CUP_12.5.1.13900-17.sgn.iso.md5" result="7"/>|<LVL::Debug> 11/02/2020 12:47:56 file_list.sh|(CAPTURE) </InstallList>|<LVL::Debug> 11/02/2020 12:47:56 file_list.sh|success|<LVL::Info> 11/02/2020 12:47:56 file_list.sh|file_list.sh complete (rc=0)|<LVL::Info> 11/02/2020 12:47:56 file_list.sh|is_upgrade_lock_available: Upgrade lock is not available.|<LVL::Debug> 11/02/2020 12:47:56 file_list.sh|is_upgrade_in_progress: Already locked by this process (pid: 17558).|<LVL::Debug> 11/02/2020 12:47:56 file_list.sh|release_upgrade_lock: Releasing lock (pid: 17558)|<LVL::Debug> 11/02/2020 14:11:19 file_list.sh|(CAPTURE) 12.5.1.13900-17|<LVL::Debug> 11/02/2020 14:11:19 file_list.sh|(CAPTURE) tmp|<LVL::Debug>

			11/02/2020 14:11:19 file_list.sh|(CAPTURE) UCSInstall_CUP_12.5.1.13900-17.sgn.iso|<LVL::Debug> 11/02/2020 14:11:19 file_list.sh|(CAPTURE) UCSInstall_CUP_12.5.1.13900-17.sgn.iso.md5|<LVL::Debug> 11/02/2020 14:11:19 file_list.sh|/opt/cisco/install/bin/filter file=/var/log/install/downloaded_versions|<LVL::Debug> 11/02/2020 16:08:30 upgrade_manager.sh|Parse argument to_version=2.5.1.13900-17|<LVL::Debug> 11/02/2020 16:08:30 upgrade_manager.sh|new upgrade version=2.5.1.13900-17|<LVL::Info> 11/02/2020 16:08:30 upgrade_manager.sh|Cleanup data from a prior upgrade attempt|<LVL::Info> 11/02/2020 16:08:30 file_list.sh|success|<LVL::Info>
FMT_SMF.1	All management activities of TSF data.	None.	**CUCM:** 11/13/2020 20:04:29.074, 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, 5 **IM&P:** 12/06/2020 18:54:47.859, acumensec, 10.1.2.122, Info, UserAccess, tracecollection, Success, No, AdministrativeEvent, Cisco CCM Application CorrelationID :, Attempt to access data was successful.User is authorized to access /tracecollection/MainServlet.class?htxtFunctionName=FileDownloadController, Cisco Tomcat, , CUCMIMP, 904

	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

			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).	**CUCM:** 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 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> 11/30/2020 16:51:18 ntp_validate_servers.sh|-s 10.1.2.134|<LVL::Debug> 11/30/2020 16:51:18 ntp_validate_servers.sh|servers='10.1.2.134'|<LVL::Debug> 11/30/2020 16:51:18 ntp_validate_servers.sh|ntpdate -d 10.1.2.134|<LVL::Debug> 11/30/2020 16:51:24 ntp_validate_servers.sh|rc=0|<LVL::Debug> 11/30/2020 16:51:24 ntp_validate_servers.sh|response=30 Nov 16:51:18 ntpdate[339]: ntpdate 4.2.6p5@1.2349-o Wed May 21 19:36:39 UTC 2019 (1) Looking for host 10.1.2.134 and service ntp transmit(10.1.2.134)

			receive(10.1.2.134) transmit(10.1.2.134) receive(10.1.2.134) transmit(10.1.2.134) receive(10.1.2.134) transmit(10.1.2.134) receive(10.1.2.134) server 10.1.2.134, port 123 stratum 2, precision -20, leap 00, trust 000 refid [10.1.2.134], delay 0.02570, dispersion 0.00000 transmitted 4, in filter 4 reference time: e2166c77.b36a38da Mon, Nov 30 2020 16:32:55.700 originate timestamp: e21670cc.799e244b Mon, Nov 30 2020 16:51:24.475 transmit timestamp: e21670cc.79bcb313 Mon, Nov 30 2020 16:51:24.475 filter delay: 0.02573 0.02570 0.02576 0.02579 0.00000 0.00000 0.00000 0.00000 filter offset: -0.00062 -0.00062 -0.00063 -0.00063

			0.000000 0.000000 0.000000 0.000000 delay 0.02570, dispers **IM&P:** 04:27:49.488 | Copy: ilog_impl: ntpdate jabber response: 3 Dec 10:23:45 ntpdate[20870]: adjust time server 10.1.2.134 offset 0.000014 sec 04:27:49.489 |(FromMsg) - Year (10:23:45) not found in the log message(Dec 3 10:23:45 CUCMIMP user 6 ilog_impl: NTP time snchronization successful.). Message could be in old format. Check if this field contains TIME. 04:27:49.489 |(FromMsg) - Time Value is 10:23:45 04:27:49.489 |Severity in DB - 2 : Msg in MSG - 6 04:27:49.489 |ProcessReadData MESSAGE TEXT -- ilog_impl: NTP time snchronization successful. 04:27:49.489 | SyslogMsgFields.MessageText ilog_impl: NTP time snchronization successful. 04:27:49.489 | Copy: ilog_impl: NTP time snchronization successful.
FTA_SSL_EXT.1	The termination of a local session by the session locking mechanism.	None.	**CUCM:** Nov 14 19:32:09, jabber, Info, login, : pam_unix(login:session): session closed for user acumensec, 6498 **IM&P:** Oct 13 16:30:56, CUCMIMP, Info, login, : pam_unix(login:session): session closed for user acumensec, 21828

FTA_SSL.3	The termination of a remote session by the session locking mechanism.	None.	**CUCM:** 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 **IM&P:** 10/13/2020 19:45:29.201, acumensec, 192.168.254.177, Info, UserLogging, CUCM IM&P Admin, Success, No, CriticalEvent, Cisco Unified CM IM and Presence Administration CorrelationID :, Successfully Logged out Cisco Unified CM IM and Presence Web Pages, Cisco Tomcat, , CUCMIMP, 186
FTA_SSL.4	The termination of an interactive session.	None.	**CUCM:** Nov 14 20:46:38, jabber, Info, login, : pam_unix(login:session): session closed for user acumen-sec, 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 **IM&P:** Oct 13 10:04:19, CUCMIMP, Info, su, : pam_unix(su-l:session): session closed for user acumen-sec, 13437 10/13/2020 19:45:29.201, acumensec, 192.168.254.177, Info, UserLogging, CUCM IM&P Admin, Success, No, CriticalEvent, Cisco Unified CM IM and Presence Administration CorrelationID :, Successfully Logged out Cisco Unified CM IM and Presence Web Pages, Cisco Tomcat, , CUCMIMP, 186

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

FCO_CPC_EXT.1	Enabling communications between a pair of components. Disabling communications between a pair of components.	Identities of the endpoints pairs enabled or disabled.	<187>243108: : ccm: 3325: jabber.acumensec.local: Dec 04 2020 16:56:58.733 UTC : %UC_CALL-MANAGER-3-SIPTrunkOOS: %[DeviceName=CUCMIMPSIP][UnavailableRemote-PeersWithReasonCode=cucmimp.acumensec.local, 10.1.2.186, 5061, local=2][AppID=Cisco Call-Manager][ClusterID=StandAloneCluster][NodeID=jabber.acumensec.local]: All remote peers are out of service and unable to handle calls for this SIP trunk <190>243106: : ccm: 3324: jabber.acumensec.local: Dec 04 2020 16:56:58.733 UTC : %UC_CALL-MANAGER-6-SSLConnectionFailure: %[PeerAddr=10.1.2.186][PeerPortNo=5061][Rea-sonCode=0][Reason= HandleSSLError - TLS protocol error(ssl reason code=(null) [0]),lib=(null) [0], fun=(null) [0], for 10.1.2.186:5061][AppID=Cisco CallManager][ClusterID=StandAloneClus-ter][NodeID=jabber.acumensec.local]: SSLConnectionfailedtoPeer <187>243108: : ccm: 3325: jabber.acumensec.local: Dec 04 2020 16:56:58.733 UTC : %UC_CALL-MANAGER-3-SIPTrunkOOS: %[DeviceName=CUCMIMPSIP][UnavailableRemote-PeersWithReasonCode=cucmimp.acumensec.local, 10.1.2.186, 5061, local=2][AppID=Cisco Call-Manager][ClusterID=StandAloneCluster][NodeID=jabber.acumensec.local]: All remote peers are out of service and unable to handle calls for this SIP trunk <186>243123: : : 26709: jabber.acumensec.local: Dec 04 2020 16:57:02.917 UTC : %UC_RTMT-2-RTMT_ALERT: %[AlertName=SyslogSeverityMatchFound][AlertDetail= At Fri Dec 04 11:57:02 EST 2020 on node cucmimp.acumensec.local, the following SyslogSeverityMatchFound events generated: #012SeverityMatch : Critical#012MatchedEvent : Dec 4 11:49:15 CUCMIMP local7 2 : 0: CUCMIMP.acumensec.local: Dec 04 2020 16:49:14.446 UTC : %UC_PE-2-PEIDSQueryError: %[PEIDSQueryErrorAlarmMessage=Exception in get_assigned_endusers][AppID=Cisco Presence Engine][ClusterID=StandAloneCluster][NodeID=CUCMIMP]:The Cisco Presence Engine service has detected an error while querying the IM and Presence Service database#012AppID : Cisco Syslog Agent#012ClusterID : #012NodeID : CUCMIMP#012 TimeStamp : Fri Dec 04 11:49:15 EST 2020 #012#012SeverityMatch : Critical#012MatchedEvent : Dec 4 11:49:15 CUCMIMP local7 2 : 1: CUCMIMP.acumensec.local: Dec 04 2020 16:49:15.646 UTC : %UC_][AppID=Cisco AMC Service][ClusterID=][NodeID=jabber.acumensec.local

FPT_ITT.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.	**CUCM:** Dec 6 23:00:03, jabber, Notice, Cisco CallManager, ccm: 3031: jabber.acumensec.local: Dec 07 2020 04:00:03.009 UTC : %UC_CALLMANAGER-5-SIPTrunkISV: %[Device-Name=CUCMIMPSIP][AvailableRemotePeers=cucmimp.acumensec.local, 10.1.2.186, 5061][Clus-terID=StandAloneCluster][NodeID=jabber.acumensec.local]: All remote peers are available to handle calls for this SIP trunk, 6442 08:41:43.463 | SyslogMsgFields.MessageText ccm: 3110: jabber.acumensec.local: Nov 29 2020 13:41:43.462 UTC : %UC_CALLMANAGER-6-SSLConnectionFailure: %[PeerAddr=10.1.2.186][PeerPortNo=5061][ReasonCode=0][Reason= HandleSSLError - TLS protocol error(ssl reason code=(null) [0]),lib=(null) [0], fun=(null) [0], for 10.1.2.73:5060][Ap-pID=Cisco CallManager][ClusterID=StandAloneCluster][NodeID=jabber.acumensec.local]: SSLConnectionfailedtoPeer **IM&P:** Nov 18 06:12:26, CUCMIMP, Alert, Cisco Cluster Manager, : 4: CUCMIMP.acumensec.local: Nov 18 2020 11:12:26.494 UTC : %UC_CLUSTERMANAGER-1-CLM_ConnectivityTest: %[No-deIP=10.1.2.134][ErrorString=CLM_TEST_UNABLE_TO_CONNECT_TCP][ClusterID=][No-deID=CUCMIMP]: CLM Connectivity Test Failed., 3147 Dec 6 22:56:50, CUCMIMP, Alert, Cisco Cluster Manager, : 6: CUCMIMP.acumensec.local: Dec 07 2020 03:56:50.102 UTC : %UC_CLUSTERMANAGER-1-CLM_PeerState: %[NodeName=jab-ber][NodeState=POLICY_INJECTED][ClusterID=][NodeID=CUCMIMP]: Current ClusterMgr ses-sion state., 3149

5. Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see *What's New in Cisco Product Documentation*.

To receive new and revised Cisco technical content directly to your desktop, you can subscribe to the What's New in Cisco Product Documentation RSS feed. The RSS feeds are a free service.

6. Contacting Cisco

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco website at www.cisco.com/go/offices.