



Cisco Jabber 15.2

Common Criteria Configuration Guide

Version: 0.5

Date: February 12, 2026

Cisco Systems, Inc.

All printed copies and duplicate soft copies are considered un-Controlled copies and the original on-line version should be referred to for latest version.

© 2026 Cisco Systems, Inc. All rights reserved.

Table of Enterprise Session Controller Contents

1	Introduction	6
1.1	Audience	6
1.2	Purpose	6
1.3	Documentation and References	6
1.4	Overview	7
1.5	Operational Environment.....	8
1.5.1	Required non-TOE Hardware/Software/Firmware.....	8
1.6	Excluded and Functionality Not Covered	8
2	Preparative Procedures and Operational Guidance for IT Environment	9
2.1	Overview	9
2.2	Prerequisites	9
2.3	Domain Name Services (DNS) Configuration	10
2.4	Installation of Cisco Unified Communications Manager (CUCM)	10
2.5	Service Activation and General Configuration of Cisco Unified Communications Manager (CUCM).....	12
2.5.1	CUCM Service Activation	12
2.5.2	CUCM Service Parameters – Allowed Codecs	13
2.5.3	CUCM Security Settings	14
2.5.3.1	CUCM Certificates	14
2.5.3.2	CUCM Mixed Mode	16
2.5.3.3	CUCM Service Parameters – CAPF.....	17
2.5.3.4	CUCM Phone Security.....	18
2.5.3.5	CUCM TLS Configuration.....	19
2.5.4	CUCM Jabber User and Device Configurations.....	20
2.5.4.1	CUCM UC Service	21
2.5.4.2	CUCM Service Profile.....	22
2.5.4.3	CUCM End User.....	23
2.5.4.4	CUCM Device - Softphone.....	24
2.5.5	CUCM Dial-Plan Configurations.....	27
3	TOE Installation	28
3.1	Deploy CUCM Certificate Trust Chain to Client Machines	28
3.2	Download Jabber	29
3.3	Install Jabber	29

3.4	First Registration Attempt	30
3.5	Microsoft Outlook Integration	31
3.5.1	Microsoft Outlook Calendar	31
3.5.2	Microsoft Outlook Contacts	32
4	Secure Management	34
4.1	Network Protocols and Cryptographic Settings	34
4.1.1	SIP Connections and Protocols	34
4.2	Product Updates	35
4.3	Jabber Features and Calls	36
4.3.1	Contacts	37
4.3.2	Call	37
5	Modes of Operation	39
5.1	Troubleshooting	39
6	Security Measures for the Operational Environment	40
7	Obtaining Documentation and Technical Assistance	41
8	Annex A: Acronyms	42
9	Annex B: Terminology	45

Table of Tables

Table 1.	Cisco Documentation	6
Table 2.	Required Operational Environment Components	8
Table 3.	Required Operational Environment Components	8
Table 4.	Operational Environment Security Measures	40
Table 5.	Acronyms	42
Table 6.	Terms	45

Table of Figures

Figure 1.	Cisco Software Download Homepage	11
Figure 2.	ISO File for Download	11
Figure 3.	CUCM Service Activation Page	13
Figure 4.	CUCM Service Parameters – Codec Selection	14
Figure 5.	CUCM Certificate Management – CSR Creation	15
Figure 6.	CUCM Certificate Management – CSR Download	15
Figure 7.	CUCM Certificate Management – Certificate Upload	16
Figure 8.	Enabling Mixed-Mode on CUCM	17
Figure 9.	Verifying Mixed-Mode Operation	17
Figure 10.	CUCM CAPF Settings	18
Figure 11.	CUCM Phone Security Profile	19
Figure 12.	Set CUCM Minimum TLS Version to 1.2	20

Figure 13. Verify CUCM Minimum TLS Setting	20
Figure 14. CUCM UC Service Profile	22
Figure 15. CUCM Service Profile	23
Figure 16. CUCM End User Profile.....	24
Figure 17. CUCM Device Profile	26
Figure 18. Adding Root Certificate to Windows Device	28
Figure 19. Viewing Windows Trusted Certificates contains Root Certificate	29
Figure 20. Jabber Install from Windows Command Prompt	30
Figure 21. Changing CAPF Certificate Operation after Initial Registration	31
Figure 22. UC Service Change for Microsoft Outlook Calendar Integration	32
Figure 23. Certificate Error Notification	35
Figure 24. Jabber Software Status Message	35
Figure 25. Jabber Application Hub Window.....	36

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 Jabber for Windows. 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

Version	Date	Change
0.1	October 15, 2024	Initial Version
0.2	May 21, 2025	Response to Lab Comments
0.3	June 23, 2025	Response to Lab Comments
0.4	February 11, 2026	Response to Lab Comments
0.5	February 12, 2026	Response to Validator Comments
0.6		

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

© 2026 Cisco Systems, Inc. All rights reserved.

1 Introduction

This document provides supporting evidence for an evaluation of a specific Target of Evaluation (TOE), the Cisco Jabber 15.2. 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.

1.1 Audience

This document is written for Authorized Administrators, referred to as Administrators for the remainder of this document, configuring the TOE, Cisco Jabber, and required non-TOE environmental components, such as Cisco Unified Communications Manager (CUCM) and Domain Name System (DNS) servers. This document assumes that you are familiar with Cisco, 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 in 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 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 Cisco Jabber operations. It is recommended that you read all instructions in this document and any references before performing steps outlined and entering commands.

1.3 Documentation and 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 1. Cisco Documentation

#	Title	Link
[1]	Planning Guide for Cisco Jabber 14.1	https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/jabber/14_1/cjab_b_planning-guide-for-jabber141.html
[2]	On-Premise Deployment for Cisco Jabber 14.1	https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/jabber/14_1/cjab_b_onprem-deployment-for-jabber141.html
[3]	Feature Configuration for Cisco Jabber 14.1	https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/jabber/14_1/cjab_b_feature-config-for-jabber141.html

#	Title	Link
[4]	Parameters Reference Guide for Cisco Jabber 14.1	https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/jabber/14_1/cjab_b_param-reference-for-jabber141.html
[5]	Release Notes for Cisco Jabber 15.2	https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/jabber/ReleaseNotes/release-notes-for-cisco-jabber-15_2.html
[6]	Installation Guide for Cisco Unified Communications Manager and the IM and Presence Service, Release 15 and SUs	https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/install/15/cucm_b_install-guide-cucm-imp-15.html
[7]	Administration Guide for Cisco Unified Communications Manager, Release 15 and SUs	https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/admin/15/adminGd/cucm_b_administration-guide-15.html
[8]	Security Guide for Cisco Unified Communications Manager, Release 15 and SUs	https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/security/15_0/cucm_b_security-guide-release-15.html
[9]	Virtualization for Cisco Unified Communications Manager (CUCM)	https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/uc_system/virtualization/virtualization-cisco-unified-communications-manager.html
[10]	System Configuration Guide for Cisco Unified Communications Manager, Release 15 and SUs	https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/admin/15/systemConfig/cucm_b_system-configuration-guide-15.html

NOTE: The Cisco “documents” referenced above are web pages hosted on Cisco servers.

1.4 Overview

Cisco Jabber provides users within an organization several features for collaborative communication:

- Integrated voice and video telephony - Securely make, receive, and control phone calls. Users have a variety of call-control options including mute, call transfer, call forwarding, and impromptu conferencing.
- Instant Messaging and Presence - View real-time availability of co-workers and securely chat in real time using instant messaging to save time and reduce phone tag.
- Online web conferencing – Securely access online web conferencing services to collaborate in real-time.

The focus of the Common Criteria evaluation is on the Video and Voice over IP telephony features of Cisco Jabber that it secured with SRTP and TLS 1.2.

1.5 Operational Environment

1.5.1 Required non-TOE Hardware/Software/Firmware

The table below lists required IT environment components.

Table 2. Required Operational Environment Components

Component	Required	Usage/Purpose Description
Windows 11 Platform	Yes	The TOE requires a Windows 11 OS platform
Enterprise Session Controller	Yes	The Cisco Unified Communications Manager (CUCM) is the SIP Server that provides the TOE with call control and management.
Remote VoIP Application	Yes	This is the peer VoIP Application that the TOE interacts with using Security Real Time Transport Protocol (SRTP).
Certificate Authority	Yes	The Certification Authority (CA) provides X.509 certificates. The CA also provides a method to check the certificate revocation status of the CUCM Server certificates.

1.6 Excluded and Functionality Not Covered

The table below lists exclusions and functionality not covered.

Table 3. Required Operational Environment Components

Functionality	Usage/Purpose Description
Non-FIPS 140-2 and CC mode of operation	This mode of operation includes non-FIPS allowed operations.
Jabber to Jabber calling. Jabber to Jabber calling provides basic voice and video calling capabilities between different Cisco Jabber clients without registering to Cisco Unified Communications Manager.	No security claims related to this mode of operation are being claimed.
SRTP with NULL cipher	SRTP with the NULL cipher does not provide encryption.
Cisco Instant Message and Presence Service	This feature is not covered in the CC evaluation
Cisco Webex® Meetings Server	This feature is not covered in the CC evaluation
Cisco Unity® Connection	This feature is not covered in the CC evaluation

These services will be disabled by configuration.

2 Preparative Procedures and Operational Guidance for IT Environment

The following sections discuss installation and configuration of required non-TOE environmental components.

2.1 Overview

Cisco Jabber is a suite of Unified Communications applications that allow seamless interaction with your contacts from anywhere. Cisco Jabber offers IM, presence, audio and video calling, voicemail, and conferencing. Jabber is available for several platforms, including Windows. For this evaluation, Jabber for Windows will be evaluated as an On-Premise device operating in Phone-Only Mode in Softphone Mode. This means the Jabber device communicates directly with the Cisco Unified Communication Manager (CUCM), no other Unified Communications servers are involved, and it will be evaluated as a softphone making and receiving VoIP calls.

Jabber clients work in tandem with CUCM, which is Cisco's Enterprise Session Controller (ESC) product. Jabber clients register to CUCM and all call setup message is between Jabber and CUCM. CUCM serves as the call-processing component for voice that includes IP telephony and call control. Jabber clients may be used On-Premise, in which case the Jabber client registers directly to the CUCM, or Off-Premise, in which case Jabber makes use of a VPN product or Expressway to reach the CUCM. For this evaluation, only the On-Premise deployment will be evaluated.

Jabber used the Session Initiation Protocol (SIP) for call control. For security purposes, SIP messaging will utilize TLS, and Secure RTP (SRTP) will be used media exchange.

The sections below will provide some guidance to the Administrator regarding install and configuration of both CUCM and the Jabber client to ensure compliance of the TOE (Jabber Client). This Admin Guide is not assumed to be a complete configuration guide, and as such, references will be made to additional publicly available documents.

2.2 Prerequisites

Jabber (the TOE) requires an installed and functioning CUCM to act as a SIP server for call processing. For Jabber 15.2 the CUCM version needs to be 11.5(1)SU3 or later. For evaluation a CUCM 15)SU2 was used.

It is also required that the environment has reachable DNS and NTP servers and that there be a Certificate Authority to sign CUCM certificates. Certificates are discussed more in section 2.5.3.1 CUCM Certificates.

As the Jabber clients are applications running on the OS of another device, those devices will need to have network connectivity to the CUCM to which Jabber will register.

Before beginning configuration, the Administrator is strongly encouraged to review the following documents:

- Planning Guide for Cisco Jabber 14.1 [1]
- On-Premise Deployment for Cisco Jabber 14.1 [2]
- Installation Guide for Cisco Unified Communications Manager, Release 15 and SUs [6]
- Administration Guide for Cisco Unified Communications Manager, Release 15 and SUs [7]
- Security Guide for Cisco Unified Communications Manager, Release 15 and SUs [8]
- Virtualization for Cisco Unified Communications Manager (CUCM) [9]

When reviewing these documents, the Administrator is recommended to focus on sections related to On-Premise Deployment, Jabber Phone-Only Mode, Softphone Mode, installing CA signed certificates in CUCM, and Cisco Certificate Authority Proxy Function (CAPF).

Planning Guide for Cisco Jabber 14.1 [1] provides an overview of the features available in Jabber for Windows, deployment scenarios, and the requirements for hardware, software, network, and certificates. On-Premise Deployment for Cisco Jabber

14.1 [2] provides the steps required for a Phone-Only Mode Deployment in its “Configuration and Installation Workflows” chapter.

There are configuration settings pushed to the Cisco Jabber TOE that are required in the evaluated configuration. This form of management is permitted in [VoIP PP].

The Cisco CUCM is required to deploy Cisco Jabber in the following manner:

- On-Premise: An on-premises deployment is one in which the Administrator set ups, manages, and maintains all services on the organization’s network.
- Phone-Only Mode: In Phone-Only mode, the user's primary authentication is to Cisco Unified Communications Manager. The device is only provisioned for VVoIP. No other services, such as IM and Presence, are supported.
- Softphone Mode: Softphone mode downloads the configuration file from the Cisco Unified Communications Manager and operates as a SIP registered endpoint. The soft client registers with Cisco Unified Communications Manager.

2.3 Domain Name Services (DNS) Configuration

On-Premise Jabber does require DNS SRV record(s) be configured. Jabber needs to resolve the “_cisco-uds” service address to retrieve service profiles from CUCM. As an example, the most basic DNS entry may appear as follows:

```
_cisco-uds._tcp.example.com
priority = 0
weight = 0
port = 8443
host = CUCM.example.com (a DNS A query will resolve to the CUCM IP address)
```

For additional details, the Administrator may reference section “Cisco UDS SRV Record” in chapter “Service Discovery” of Planning Guide for Cisco Jabber 14.1 [1].

2.4 Installation of Cisco Unified Communications Manager (CUCM)

The TOE requires CUCM as the SIP Server. CUCM serves as the call-processing component for voice that includes IP telephony, mobility features and calls controls. Refer to the following documentation to install and configure CUCM:

- Installation Guide for Cisco Unified Communications Manager, Release 15 and SUs [6]
- Virtualization for Cisco Unified Communications Manager (CUCM) [9]

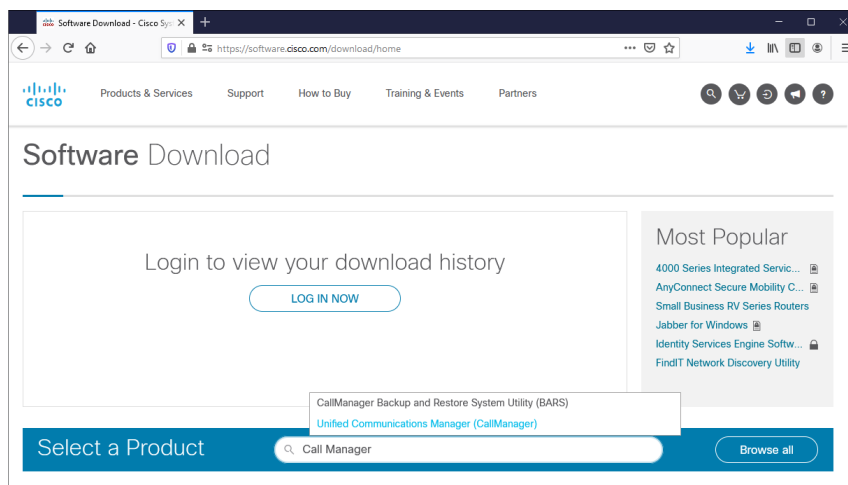
In addition to selecting the CUCM version, the Administrator will need to determine the installation capacity. Virtualization for Cisco Unified Communications Manager (CUCM) [9] can then be used by the Administrator to determine/confirm the hardware (UCS Server and CPU) and virtualization requirements (ESXi version, virtual HDD, virtual RAM, virtual CPU, virtual NIC) for the CUCM install. The Administrator can download the CUCM software (ISO file which installs the guest OS and CUCM application on the VM) and CUCM OVA file (which build the CUCM VM).

Software can be found at:

<https://software.cisco.com/download/home>

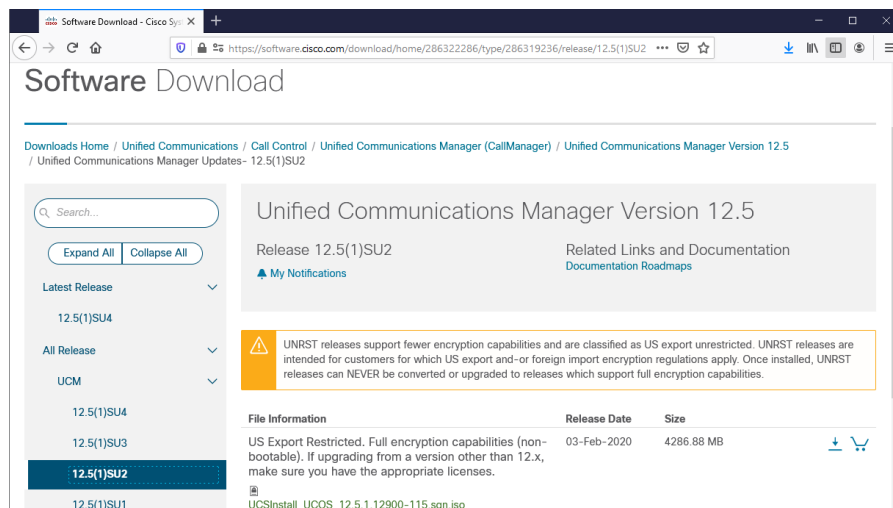
From here search for “Unified Communications Manager” or “Call Manager” (see below).

Figure 1. Cisco Software Download Homepage



Find and click the desired CUCM version, from select **“Select a Software Type”**, select **“Unified Communications Manager Updates”**, select the specific Service Update release (SU), and download the **“US Export Restricted”** ISO file (see below).

Figure 2. ISO File for Download



Please note, the ISO files are intended upgrade purposes and are non-bootable. If a fresh install is being performed a bootable ISO is required, and the Administrator is advised to engage their Account Team. The ISO file is used to install the guest operating VM and the CUCM application. To ensure the VM is built in accordance with Cisco recommendations, use an OVA file to build the VM itself. To find OVA files, when given the option to **“Select a Software Type”**, select **“Unified Communications Manager Virtual Machine Templates”** rather than **“Unified Communications Manager Updates”**.

Before beginning the CUCM install it is advised that:

- The Administrator has verified the hardware and virtualization requirements are met in accordance with Virtualization for Cisco Unified Communications Manager (CUCM) [9].
- The Administrator has familiarized themselves with the install process by reading Installation Guide for Cisco Unified Communications Manager, Release 15 and SUs [6].
- The administrator assigned/reserved the following for the CUCM server:
 - IP address and subnet

- Default GW address
- Hostname
- Domain
- DNS server(s)
- NTP server(s)
- DNS servers contain entries for the CUCM.
- Default GW, DNS server(s), and NTP server(s) are reachable.

When reviewing the Installation Guide, the Administrator should pay specific attention to the sections related to Basic and CUCM Only installations.

The CUCM is part of the Operational Environment of the TOE but is not being evaluated itself. For more detail and additional information regarding CUCM installation, the Administrator is referred to Installation Guide for Cisco Unified Communications Manager, Release 15 and SUs [6].

2.5 Service Activation and General Configuration of Cisco Unified Communications Manager (CUCM)

Once installed CUCM Services needed for Jabber operation need to be started and basic configurations added.

2.5.1 CUCM Service Activation

When initially installed, a CUCM servers Network Services are running, however, there are no Feature Services enabled. To register a Jabber Client, at a minimum, the following services need to be activated:

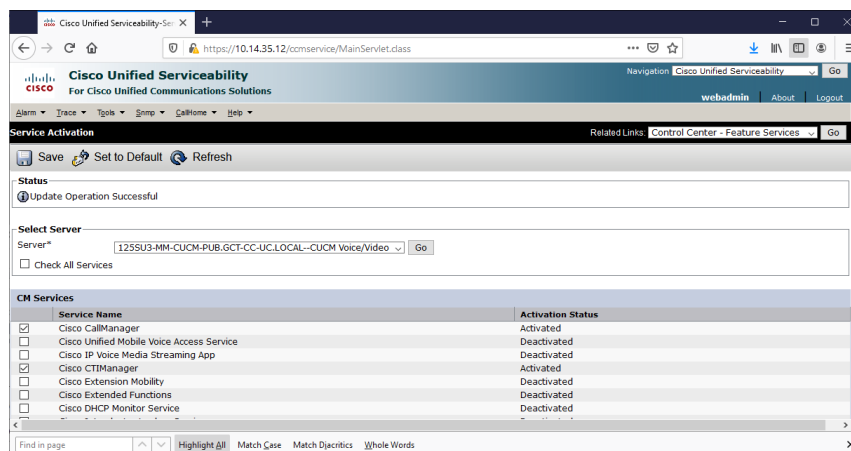
- Cisco CallManager
- Cisco CTIManager
- Cisco Tftp¹
- Cisco Certificate Authority Proxy Function
- Cisco Certificate Enrollment Service
- Cisco CTL Provider

To enable services, the Administrator should log into the CUCM GUI for Serviceability, [https://\[CUCM IP or FQDN\]/cmplat-form/](https://[CUCM IP or FQDN]/cmplat-form/), then:

- Choose **Tools > Service Activation**.
- Select the **Server** in question.
- **Check** the services to be active, and then click **Save**.

¹ TFTP Service refers to the routines running that are responsible for storing and deploying endpoint configurations files. The naming convention is a legacy term, however TFTP protocol is not used to deploy the configuration files.

Figure 3. CUCM Service Activation Page



In a single node deployment, there will be no other options. In a multi-nodal deployment, each node needs to be selected and services activated on each node for which the service should run. Note the CAPF, Certificate Enrollment Service, and CTL Provider only need to be activated on the Publisher.

2.5.2 CUCM Service Parameters – Allowed Codecs

Common Criteria compliance requires Jabber codec usage is limited to fixed bit-rate codecs. As Jabber is registered to CUCM and receives configurations from CUCM, this requirement is met by disabling non-allowed codecs.

To disable non-allowed codecs the Administrator should log into the CUCM GUI for Call Manager Administration, [https://\[CUCM IP or FQDN\]/ccmadmin/](https://[CUCM IP or FQDN]/ccmadmin/), then:

- Choose **System > Service Parameters**.
- Select the **Server** in question.
- When the **Service** drop down appears, select **Cisco CallManager**.
- Search for the **Clusterwide Parameters (System - Location and Region)** and change the following parameters to “Disabled”:
 - “iLBC Codec Enabled”
 - “iSAC Codec Enabled”
 - “Opus Codec Enabled”
- Click **Save** and the settings will be applied to all nodes in the cluster.

NOTE: The remaining supported codecs (G.722, G.711a, G.711mu, and G.729) are fixed bit-rate codecs. Should a future release of CUCM include other codecs, the Administrator should disable them and only use these supported codecs.

Figure 4. CUCM Service Parameters – Codec Selection

The screenshot shows the Cisco Unified CM Administration web interface. The browser address bar displays the URL: <https://10.14.35.12/cmadmin/serviceParamEdit.do?server=2b575f2b-cfbd-4250-ab11-98cd601>. The page title is "Service Parameter Configuration". The navigation menu includes System, Call Routing, Media Resources, Advanced Features, Device, Application, User Management, Bulk Administration, and Help. The main content area shows the "Service Parameter Configuration" page for the selected server and service.

Status: Ready

Select Server and Service:

Server: 125S03-MM-CUCM-PUB.GCT-CC-UC-LOCAL--CUCM

Service: Cisco CallManager (Active)

All parameters apply only to the current server except parameters that are in the cluster-wide group(s).

Cisco CallManager (Active) Parameters on server 125S03-MM-CUCM-PUB.GCT-CC-UC-LOCAL--CUCM Voice/Video (Active)

Parameter Name	Parameter Value	Suggested Value
Clusterwide Parameters (System - Location and Region)		
Enforce Millisecond Packet Size *	True	True
Locations Trace Details Enabled *	False	False
Preferred G.711 Millisecond Packet Size *	20	20
Preferred G.722 Millisecond Packet Size *	20	20
Preferred G.722.1 Millisecond Packet Size *	30	30
Preferred G.729 Millisecond Packet Size *	20	20
Always Use Preferred G.729 Packet Size For SIP Trunk Answers *	False	False
Preferred GSH RFB Bytes Packet Size *	31	31
G.711 A-law Codec Enabled *	Enabled for All Devices	Enabled for All Devices
G.711 mu-law Codec Enabled *	Enabled for All Devices	Enabled for All Devices
G.722 Codec Enabled *	Enabled for All Devices	Enabled for All Devices
UBC Codec Enabled *	Disabled	Enabled for All Devices
G.722.1 and G.722.2 Codecs Enabled *	Enabled for All Devices	Enabled for All Devices
ISAC Codec Enabled *	Disabled	Enabled for All Devices
Ocus Codec Enabled *	Disabled	Enabled for All Devices
Default Intra-region Max Audio Bit Rate *	64 kbps (G.722, G.711)	64 kbps (G.722, G.711)
Default Inter-region Max Audio Bit Rate *	9.6 kbps (G.729)	9.6 kbps (G.729)

Find in page: [] Highlight All Match Case Match Diacritics Whole Words

2.5.3 CUCM Security Settings

Common Criteria requires that SIP signaling to/from the Jabber client using TLS and that media be encrypted using SRTP. TLS and SRTP make use of Certificates. To use TLS and SRTP, the CUCM must be placed into “mixed mode”. It is strongly recommended that the Administrator read/review Security Guide for Cisco Unified Communications Manager, Release 15 and SUs [8] prior to configuring the CUCM, and pay specific attention to the sections on TLS Setup, Certificates and Certificate Authority Proxy Function, Phone Security, and Phone Security Profile Setup.

2.5.3.1 CUCM Certificates

Cisco Jabber uses certificate validation to establish secure connections with CUCM SIP Servers. When attempting to establish secure connections, CUCM SIP Servers present Cisco Jabber with certificates. Certificates are required for each service to which the Jabber clients connect. The following CUCM certificates are required for the on-premise server configurations to establish secure connection with the TOE:

- Tomcat Certificate (required for HTTP), and
- Call Manager certificate (required for secure SIP call signaling for secure phone)

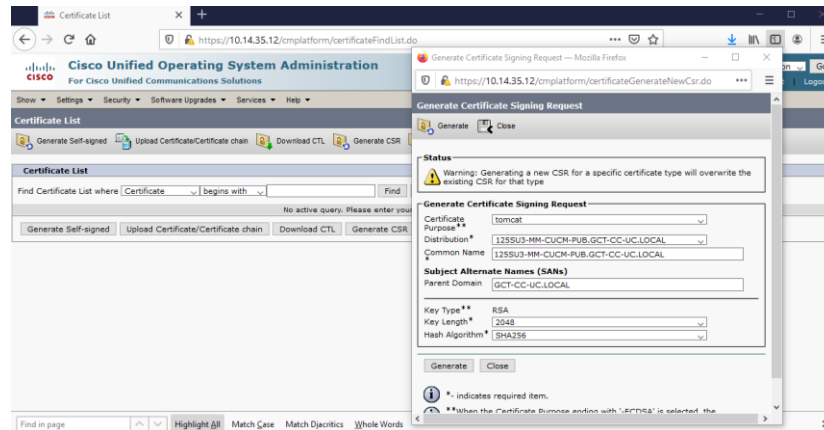
Cisco Jabber uses the client platform to verify the certificate information and validation.

The Administrator will need to generate CSRs for the Tomcat and CallManager Services, have them signed by a Certificate Authority, and then upload the signed certificates to the call manager. To manage certificates the Administrator should log into the CUCM GUI for OS Administration [https://\[CUCM IP or FQDN\]/cmplatform/](https://[CUCM IP or FQDN]/cmplatform/), then:

- Choose **Security > Certificate Management**.
- Click **Generate CSR**.
- From the pop-up window that appears for the “**Certificate Purpose**” select “**tomcat**”. The other parameters can remain default.

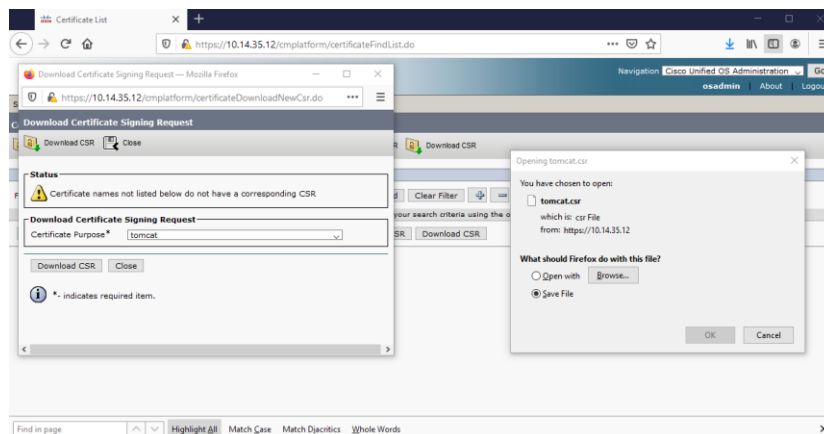
- The Key Length may also be set to 3072 or 4096-bit RSA from the default of 2048.
- Then click **Generate**.
- From the same pop-up window, for the “**Certificate Purpose**” select “**CallManager**”. The other parameters can remain default.
 - The Key Length may also be set to 3072 or 4096-bit RSA from the default of 2048.
- Then click **Generate**.
- Close the pop-up window.

Figure 5. CUCM Certificate Management – CSR Creation



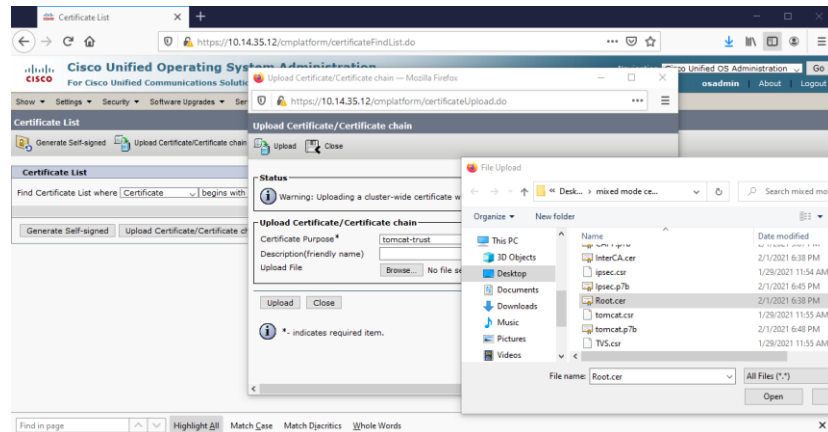
- Click **Download CSR**.
- From the pop-up window that appears, select “**tomcat**”, and then click **Download CSR**.
- On the second pop-up window that appears select **Save** then **OK**.
- The second pop-up window will close automatically, now **Close** the first pop-up window.
- Click **Download CSR**.
- From the pop-up window that appears, select “**CallManager**”, and then click **Download CSR**.
- On the second pop-up window that appears select “**Save**” then “**OK**”.
- The second pop-up window will close automatically, now **Close** the first pop-up window.

Figure 6. CUCM Certificate Management – CSR Download



- Submit the CSR to the Certificate Authority for signing. Ensure the CA signs the certificate with the key usages and extended key usages requested in the CSRs. You will need root chain (root and intermediate certificates) as well as the signed tomcat and CallManager certificate.
- From CUCM Certificate List, click **Upload Certificate/Certificate Chain** and from the pop-up window that appears select **“tomcat trust”** and **Browse** for the **root certificate** and then select upload. Perform this same operation a second time selecting **“tomcat trust”** and **Browse** for the **intermediate certificate** then select upload. Perform this same operation a third and final time selecting **“tomcat”** and **Browse** for the **signed tomcat certificate**, then select upload.

Figure 7. CUCM Certificate Management – Certificate Upload



- After uploading the tomcat trust and tomcat certificates, restart the tomcat service from CUCM CLI using the command **“utils service restart Cisco Tomcat”**. Note the command is case sensitive.
- From CUCM Certificate List, click **Upload Certificate/Certificate Chain** and from the pop-up window that appears select **“CallManager trust”** and **Browse** for the **root certificate** and then select upload. Perform this same operation a second time selecting **“CallManager trust”** and **Browse** for the **intermediate certificate** then select upload. Perform this same operation a third and final time selecting **“CallManager”** and **Browse** for the **signed CallManager certificate**, then select upload.

To ensure that certificate validation occurs without users receiving a prompt to accept or decline CA certificates, it's recommended that you deploy certificates to the local certificate store of the endpoint clients. Refer to the “Manually Deploy CA Certificates to Cisco Jabber for Windows Clients” section in the “Configure Certificate Validation” chapter in On-Premises Deployment for Cisco Jabber 14.1 [2].

In addition, to determine the revocation status of certificates issued by the organization's certificate authority, the Windows platform needs the appropriate network connectivity to the OCSP responder.

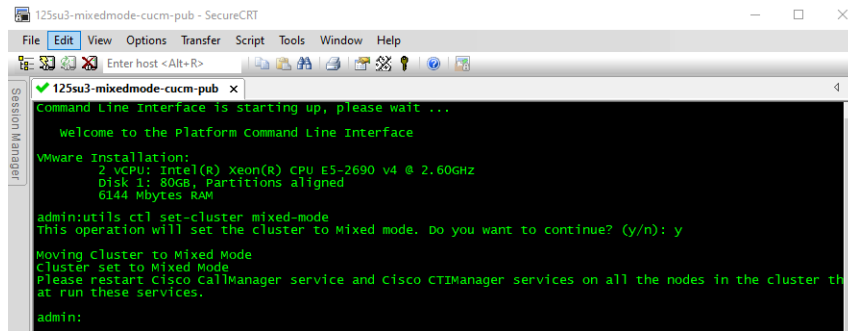
2.5.3.2 CUCM Mixed Mode

To use TLS and SRTP, the CUCM must be placed into “mixed mode”. Prior to enabling mixed mode, the CAPF and CTL services should already be running on the publisher. Reference section 2.5.1 CUCM Service Activation above.

The CUCM must be pointed to a licensing server to use encryption. Mixed mode does not perform encryption in “demo mode”. For smart licensing, the Registration Token received from the Smart account or Virtual account must have Allow Export-Controlled functionality enabled while registering with the cluster.

To place the cluster into mixed mode from the CUCM Publishers command line interface (CLI), the Administrator enters the following command, “**utils ctl set-cluster mixed-mode**”. When prompted type “**y**” and then press **Enter**. This action will require a restart of the Cisco CallManager and Cisco CTIManager services. The TFTP Service² should also be restarted.

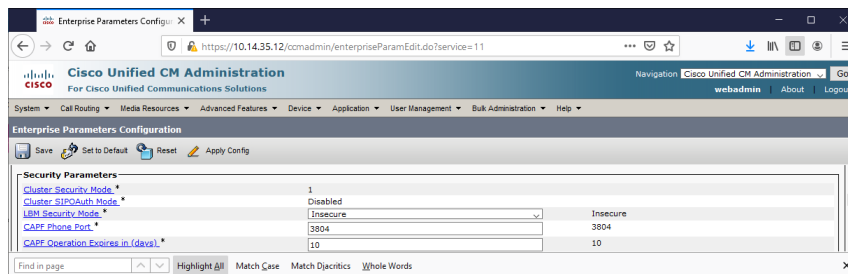
Figure 8. Enabling Mixed-Mode on CUCM



After the Publisher restart, the Administrator can confirm the cluster is in mixed mode. The Administrator should log into the CUCM GUI for Call Manager Administration, [https://\[CUCM IP or FQDN\]/ccmadmin/](https://[CUCM IP or FQDN]/ccmadmin/), then:

- Choose **System > Enterprise Parameters**.
- Search for **Cluster Security Mode**.

Figure 9. Verifying Mixed-Mode Operation



A value of “1” indicates true (cluster is in mixed mode).

2.5.3.3 CUCM Service Parameters – CAPF

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 be configured for Offline usage.

To configure CAPF settings, the Administrator should log into the CUCM GUI for Call Manager Administration, [https://\[CUCM IP or FQDN\]/ccmadmin/](https://[CUCM IP or FQDN]/ccmadmin/), then:

- Choose **System > Service Parameters**.
- Select the **Server** in question.
- When the **Service** drop down appears, select **Cisco Certificate Authority Proxy Function**.

² TFTP Service refers to the routines running that are responsible for storing and deploying endpoint configurations files. The naming convention is a legacy term, however TFTP protocol is not used to deploy the configuration files.

- The “**Certificate Issuer to Endpoint**” setting is by default “**Cisco Certificate Authority Proxy Function**”. Verify this to be the case. If not, select “**Cisco Certificate Authority Proxy Function**” from the drop down, then click save.
- The remaining Parameters should be the default settings and the “**Online CA Parameters**” should be blank (except the “**Online CA Type**” which is set to “**Microsoft CA**” by default).

Figure 10. CUCM CAPF Settings

The screenshot shows the 'Service Parameter Configuration' page in the Cisco Unified CM Administration GUI. The 'Status' is 'Ready'. The 'Select Server and Service' section shows the server '1255U3-HH-CUCH-PUB-GCT-CC-UC-LOCAL-CUCM' and the service 'Cisco Certificate Authority Proxy Function (Active)'. Below this, the 'Cisco Certificate Authority Proxy Function (Active) Parameters on server 1255U3-HH-CUCH-PUB-GCT-CC-UC-LOCAL-CUCM Voice/Video (Active)' are listed in a table.

Parameter Name	Parameter Value	Suggested Value
Certificate Issuer to Endpoint *	Cisco Certificate Authority Proxy Function	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

Below the table, the 'Online CA Parameters' section is visible, with 'Online CA Hostname' currently blank.

The above CAPF setting should be used in any CUCM server running the CAPF service.

2.5.3.4 CUCM Phone Security

In order use SIP via TLS and SRTP, the Jabber device in CUCM will need to be configured with a Phone Security Profile. The Administrator configures a Phone Security Profile from the CUCM Call Manager Administration GUI. The Administrator logs into the CUCM GUI for Call Manager Administration [https://\[CUCM IP or FQDN\]/ccmadmin/](https://[CUCM IP or FQDN]/ccmadmin/), then:

- Choose **System > Security > Phone Security Profile**.
- Search for “**Client Services Framework**”. Which will find the **Non-Secure Profile for a Cisco Client Services Framework**, which is used by Jabber.
- Click the hyperlink for **Cisco Unified Client Services Framework - Standard SIP Non-Secure Profile**. This is a read only profile, so any changes not explicitly mentioned below will use the default settings.
- Click **Copy**.
- After clicking copy, do the following:
 - Provide a new name, such as “**CSF – Secure SIP Profile**”.
 - Set “**Device Security Mode**” to “**Encrypted**”.
 - Set “**Transport Type**” to “**TLS**”.
 - Set “**Authentication Mode**” to “**By Authentication String**”.
 - Verify/set **RSA Key Size (Bits)** to at least **2048**.
 - The value may also be set to a Key Size of 3072 or 4096.
 - Set “**SIP Phone Port**” to “**5061**”.
- Click **Save**.

Figure 11. CUCM Phone Security Profile

The screenshot shows the Cisco Unified CM Administration web interface. The browser address bar displays the URL: <https://10.14.35.12/cmadmin/phoneSecurityProfileEdit.do?key=d2ea769e-9d3b-f54c-b74b-40b>. The page title is "Phone Security Profile Configuration".

Status: Ready

Phone Security Profile Information

- Product Type: Cisco Unified Client Services Framework
- Device Protocol: SIP
- Name: Cisco Unified CSF - Standard SIP Secure Profile
- Description: Cisco Unified Client Services Framework - Standard SIP Secure
- Device Security Mode: Encrypted
- Transport Type: TLS
- ☐ TFTP Encrypted Config
- ☐ Enable OAuth Authentication

Phone Security Profile CAPF Information

- Authentication Mode: By Authentication String
- Key Order: RSA Only
- RSA Key Size (Bits): 2048
- EC Key Size (Bits): < None >

Note: These fields are related to the CAPF Information settings on the Phone Configuration page.

Parameters used in Phone

- SIP Phone Port: 5061

Find in page: [] Highlight All Match Case Match Diacritics Whole Words

The Phone Security Profile will be used when configuring the Jabber Device in section.

2.5.3.5 CUCM TLS Configuration

In the evaluated configuration, the TOE is configured for secure connections with CUCM SIP Server, using TLS 1.2 (RFC 5246) with the following ciphersuites:

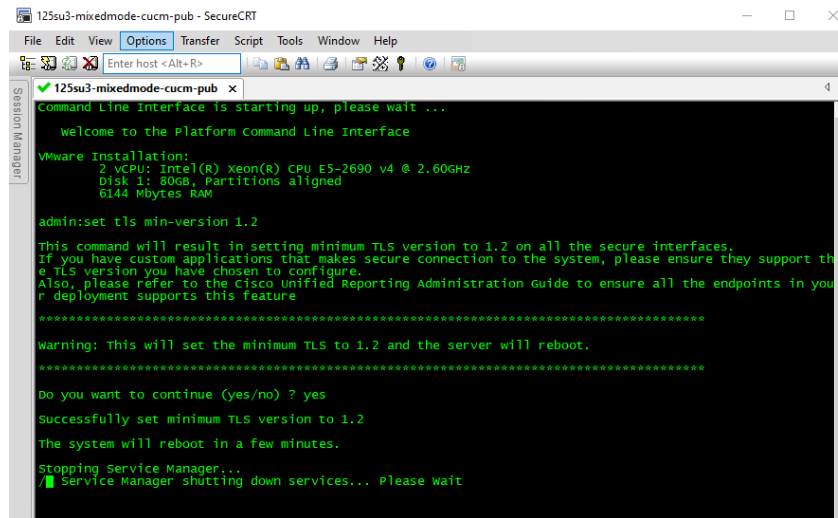
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384

The TOE additionally uses the following ciphersuite for the CAPF functionality:

- TLS_RSA_WITH_AES_128_CBC_SHA

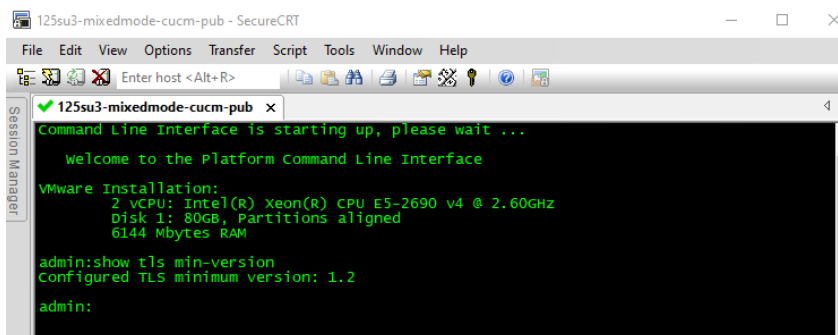
To limit the minimum TLS version to TLS 1.2, from the CUCM Publishers CLI, the Administrator enters the following command, **"set tls min-version 1.2"**. When prompted, type **"yes"**. This action will restart the Publisher.

Figure 12. Set CUCM Minimum TLS Version to 1.2



Once the system restarts, the Administrator may verify the minimum TLS version by running the command “**show tls min-version**” command from the Publisher CLI.

Figure 13. Verify CUCM Minimum TLS Setting



Additionally, the Administrator will configure the Jabber Client for FIPS and CC mode during the installation of the client itself, which restricts TLS to versions 1.2 and 1.3 by default. While both TLS 1.2 and 1.3 are supported, only TLS 1.2 claimed and evaluated.

Additionally, the Administrator will configure the Jabber Client for FIPS and CC mode during the installation of the client itself. This restricts the TLS version to 1.2 and 1.3 by default. The use of TLS version 1.3 was not evaluated. The CUCM SIP Server must also be configured to restrict the maximum TLS version to 1.2 which will ensure that the TOE is limited to TLS 1.2 for communications with CUCM. This can be accomplished by placing the CUCM in FIPS and CC mode with the command “**utils fips_common_criteria enable**” from the Publisher CLI. When prompted, type “**yes**”. This action will restart the Publisher.

2.5.4 CUCM Jabber User and Device Configurations

The configurations in this section are required to successfully register a Jabber Client to the CUCM. These configurations are performed by the Administrator. The list of configurations to be performed can be found in section “Phone Only Mode Deployment” in chapter “Configuration and Installation Workflows” of On-Premise Deployment for Cisco Jabber 14.1 [2] and

serves as the basis for this Phone-Only Mode Deployment. Steps related to non-evaluated features (Voicemail and WebEx Conferencing” have been omitted).

2.5.4.1 CUCM UC Service

The UC Service information is used to set the Jabber mode and define the CUCM server from which the Jabber client will pull configuration information. To configure a UC Service profile, the Administrator should log into the CUCM GUI for Call Manager Administration, [https://\[CUCM IP or FQDN\]/ccmadmin/](https://[CUCM IP or FQDN]/ccmadmin/), then:

- Choose **User Management > User Settings > UC Service**.
- Select **Add New**.
- From the dropdown select UC Service Type **Jabber Client Configuration (jabber-config.xml)**.
- Provide a **Name** and **Description**.
- Under Jabber Configuration Parameters section:
 - Set Section to **Phone**, Parameter to **TftpServer1**³, and set the Value to the **FQDN of the CUCM Server**
 - Set Section to **Client**, Parameter to **TelephoneOnlyDiscovery**, and set the Value to **“true”**.
 - Set Section to **Client**, Parameter to **UpdateURL**, and set the Value to the **the URL to update XML definition file**.

NOTE: The URL to update XML definition file has the following format “http://http_servername/UpdateURL_file”. For example, if the TFTP service on the CUCM was being used as the server and the update file name was jabber-update.xml, the Value would be **https://cucm.example.com:6970/jabber-update.mxl**.

- **[Optional]** Set Section to **Policies**, Parameter to **CommonCriteriaEndCallTimeout**, and set the Value to the number of seconds after which an idle call (client no longer receiving media packets) is ended.
 - The minimum value is 60 (seconds = 1 minute)
 - The maximum value is 28800 (seconds = 480 minutes = 8 hours)
 - The default value is 300. This is also the value used if the parameter is not set when the TOE is operating in FIPS and CC mode
- Click **Save**.

³ TftpServer1 refers to the CUCM, which contains the configuration files. Reference to TFTP is legacy terminology, however TFTP protocol is not used to deploy the configuration files.

Figure 14. CUCM UC Service Profile

Cisco Unified CM Administration
For Cisco Unified Communications Solutions

System | Call Routing | Media Resources | Advanced Features | Device | Application | User Management | Bulk Administration | Help

UC Service Configuration | Related Links: Back To Find/List | Go

Save | Delete | Copy | Add New

Status: Update successful

UC Service Information
 UC Service Type: Jabber Client Configuration (jabber-config.xml)
 Product Type: Jabber
 Name: Jabber-15.1.0
 Description: Jabber-15.1.0-config

Section	Parameter	Parameter Description	Value	Operations
Phone	TftpServer	The address of the primary CUCM TFTP service	CUCM.example.com	Delete
Client	TelephonyOnlyDiscovery	Restrict client users to access phone only service	true	Delete
Client	UpdateURL	The URL to update XML definition file	CUCM.example.com	Delete
Policies	CommonCriteriaEndCallTimeout	End call timeout for CC_MODE deployment	300	Delete Add Add Custom
Section: -- Not Selected -- Multipart Parameter: -- Not Selected -- Parameter Description: -- Not Selected -- Value: -- Not Selected -- Operations: Add				

Save | Delete | Copy | Add New

* indicates required item.

2.5.4.2 CUCM Service Profile

The Service Profile Information uses the previously configured UC Service policy to apply those configurations to an End User. To configure Service Profile Information, the Administrator should log into the CUCM GUI for Call Manager Administration, [https://\[CUCM IP or FQDN\]/ccmadmin/](https://[CUCM IP or FQDN]/ccmadmin/), then:

- Choose **User Management > User Settings > Service Profile Configuration**.
- Select **Add New**.
- Provide a **Name** and **Description**.
- Search for the section named **Jabber Client Configuration (jabber-config.xml) Profile**.
- For the **Common** setting use the dropdown to select the previously configured **UC Service** policy.
- Click **Save**.

Figure 15. CUCM Service Profile

Service Profile Configuration

Save Delete Copy Add New

Status
Update successful

Service Profile Information
Name * Jabber-15.1.0-service
Description Jabber-15.1.0 service profile
☐ Make this the default service profile for the system

Voicemail Profile
Primary <None>
Secondary <None>
Tertiary <None>
Credentials source for voicemail service * Not set

MailStore Profile
Primary <None>
Secondary <None>
Tertiary <None>
Inbox Folder * INBOX
Trash Folder * Deleted Items
Polling Interval (in seconds) * 60
☒ Allow dual folder mode

Video Conference Scheduling Portal Profile
Primary <None>
Secondary <None>
Tertiary <None>

Jabber Client Configuration (Jabber-config.xml) Profile
Common Jabber-15.1.0
Desktop <None>
Mobile <None>

Save Delete Copy Add New

* indicates required item.

The above action will apply one UC Service policy to Desktop and Mobile Jabber clients. If desired, individual UC Service profiles may be configured for mobile and desktop, and then applied as Desktop and Mobile, respectively.

2.5.4.3 CUCM End User

The End User configurations allow for Jabber Users to authenticate when logging in, assigning necessary permission of Jabber use, and applying Service Profiles used by Jabber. To configure an End User, the Administrator should log into the CUCM GUI for Call Manager Administration, [https://\[CUCM IP or FQDN\]/ccmadmin/](https://[CUCM IP or FQDN]/ccmadmin/), then:

- Choose **User Management > End User**.
- Select **Add New**.
- Under **User Settings** provide a:
 - **User ID** (required)
 - **Lastname** (required)
 - **Password** (and confirm the password)
 - **Directory URI** (of the form of "name@domain")
 - **Mail ID** (of the form of "name@domain")
- Under **Service Settings** for the **UC Service Profile** select the previously configured **Service Profile**.
- Click **Save**.
- Once saved, the **Permissions Information** section will be available. Click **Add to Access Control Group**.
- In the pop-up window that appears, click **Find**, then search through the list and **Check**:
 - **Standard CCM End Users**
 - **Standard CTI Enabled**
- Click **Add Selected**.
- Click **Save**.

Figure 16. CUCM End User Profile
(Image edited to show relevant parameters only)

Cisco Unified CM Administration
For Cisco Unified Communications Solutions

Skip to Content Navigation Cisco Unified CM Administration Go

admin About Logout

System Call Routing Media Resources Advanced Features Device Application User Management Bulk Administration Help

End User Configuration Related Links: Back to Find List Users Go

Save Delete Add New Revoke Refresh Token

Status
Status: Ready

User Information

User Status: Enabled Local User

User ID*: User1

Password: [Edit Credential](#)

Confirm Password:

Self-Service User ID:

PIN: [Edit Credential](#)

Confirm PIN:

Last name*: User1

Middle name:

First name:

Display name:

Title:

Directory URI: user@gct-cc-uc.local

Telephone Number:

Home Number:

Mobile Number:

Pager Number:

Mail ID: user@gct-cc-uc.local

Manager User ID:

Department:

User Locale: < None >

Associated PC/Site Code:

Digest Credentials:

Confirm Digest Credentials:

User Profile: Use System Default("Standard (Factory Default) U... [View Details](#)

User Rank*: 1-Default User Rank

Service Settings

☒ Home Cluster

☐ Enable User for Unified CM IM and Presence (Configure IM and Presence in the associated UC Service Profile)

☐ Include meeting information in presence(Requires Exchange Presence Gateway to be configured on CUCM IM and Presence server)

UC Service Profile: Jabber-15.1.0-service [View Details](#)

Permissions Information

Groups: Standard CCM End Users
Standard CTI Enabled

Roles: Standard CCM End Users
Standard CCMUSER Administration
Standard CTI Enabled

[Add to Access Control Group](#)
[Remove from Access Control Group](#)

[View Details](#)

2.5.4.4 CUCM Device - Softphone

Before deploying a Jabber client, the Administrator will need to configure a device in CUCM for the corresponding Jabber Client. To configure the device in CUCM, the Administrator should log into the CUCM GUI for Call Manager Administration, [https://\[CUCM IP or FQDN\]/ccmadmin/](https://[CUCM IP or FQDN]/ccmadmin/), then:

- Choose **Device > Phone**.
- Select **Add New**.
- For **Phone Type** select **Cisco Unified Client Services Framework** and click **Next**.

- Under **Device Information** provide the following information:
 - **Device Name** (15-character alphanumeric limit)
 - **Owner** is set to **User**
 - From the **Owner User ID** select a previously created **End User**
 - Select options for other required fields (annotated by a *)
- Under Protocol Specific Information provide the following information:
 - For **Device Security Profile** use the previously created Phone Security Profile
 - Select a **SIP Profile**
- Under Certification Authority Proxy Function (CAPF) Information perform the following:
 - Set **Certificate Operation** to **Install/Upgrade**
 - Set **Authentication Mode** to **By Authentication String**
 - Enter an **Authentication String** or click **Generate String** for CUCM to create one
 - Verify/ set **RSA Key Size (Bits)** to at least **2048**
 - [Optional, if EC is desired] set the **EC Key Size (Bits)** to **256, 384, or 521**
- Click **Save**.
- Click the hyperlink for **Line [1] - Add a new DN**.
- On the Directory Number Configuration page, perform the following:
 - Enter the **Directory Number**
 - Select the **Partition** from the dropdown (<None> is an option)
 - Enter other parameters if needed.
- Click **Save**.
- Click **Apply Config**.
- Click **Go** next to the Related Links dropdown to return to the Device configuration page.
- Click **Save**.
- Click **Apply Config**.

Figure 17. CUCM Device Profile
(Image edited to show relevant parameters only)

Phone Configuration

Navigation: Cisco Unified CM Administration | webadmin | About | Logout

System | Call Routing | Media Resources | Advanced Features | Device | Application | User Management | Bulk Administration | Help

Phone Configuration | Related Links: Back To Find/List | Go

Save | Delete | Copy | Reset | Apply Config | Add New

Association

Modify Button Items

- Line [1] - 9195551000 in PT-INTERNAL
- Line [2] - Add a new DN
- Line [3] - Add a new DN
- Line [4] - Add a new DN
- Line [5] - Add a new DN
- Line [6] - Add a new DN
- Line [7] - Add a new DN
- Line [8] - Add a new DN

Phone Type

Product Type: Cisco Unified Client Services Framework
Device Protocol: SIP

Real-time Device Status

Registration: Unknown
IPv4 Address: None

Device Information

☒ Device is Active
☒ Device is trusted

Device Name*: JFWclient01
Description: JFWclient01
Device Pool*: DP-PHONE [View Details](#)
Common Device Configuration: < None > [View Details](#)
Phone Button Template*: Standard Client Services Framework
Common Phone Profile*: Standard Common Phone Profile [View Details](#)
Calling Search Space: < None >
AAR Calling Search Space: < None >
Media Resource Group List: < None >
User Hold MOH Audio Source: < None >
Network Hold MOH Audio Source: < None >
Location*: LOC-PHONE
AAR Group: < None >
User Locale: < None >
Network Locale: < None >
Built In Bridge*: Default
Privacy*: Default
Device Mobility Mode: Default [View Current](#)
Owner: ☒ User ☐ Anonymous (Public/Shared Space)
Owner User ID*: User1

Protocol Specific Information

Packet Capture Mode*: None
Packet Capture Duration: 0
BLF Presence Group*: Standard Presence group
SIP Dial Rules: < None >
MTP Preferred Originating Codec*: 711ulaw
Device Security Profile*: Cisco Unified CSF - Standard SIP Secure Profile
Rerouting Calling Search Space: < None >
SUBSCRIBE Calling Search Space: < None >
SIP Profile*: Standard SIP Phone Profile [View Details](#)
Digest User: < None >
☐ Media Termination Point Required
☐ Unattended Port
☐ Require DTMF Reception

Certification Authority Proxy Function (CAPF) Information

Certificate Operation*: No Pending Operation
Authentication Mode*: By Authentication String
Authentication String: 1385241504
[Generate String](#)
Key Order*: RSA Only
RSA Key Size (Bits)*: 2048
EC Key Size (Bits):
Operation Completes By: 2021 03 27 12 (YYYY:MM:DD:HH)
Certificate Operation Status: None
Note: Security Profile Contains Addition CAPF Settings.

2.5.5 CUCM Dial-Plan Configurations

Numbering-plans and dial-plans are beyond the scope of this document as they are highly customizable, and deployment depends on the needs of an organization. In the absence of any configured Partitions and Calling Search spaces, devices will be able to call one another. The same is true of Locations, Regions, Media Resource Groups (MRG), Media Resource Group Lists (MRGL), Device Pools, etc. As they do not affect any security claims, the configuration of these parameters is not discussed. The Administrator may find additional information on the configurable parameters related to call routing in System Configuration Guide for Cisco Unified Communications Manager, Release 15 and SUs [10].

3 TOE Installation

This section provides instructions for securely accepting the TOE and any subsequent TOE updates. “Updates” are a new version of the TOE.

The evaluated configuration requires Cisco Jabber to be installed in FIPS and CC mode. FIPS mode results in the client managing certificates more strictly. Users in FIPS mode may see certificate errors in the client if a certificate for a service expires and users do not reenter their credentials before they expire.

Setting FIPS and CC Mode is performed using Command Line Installation Arguments.

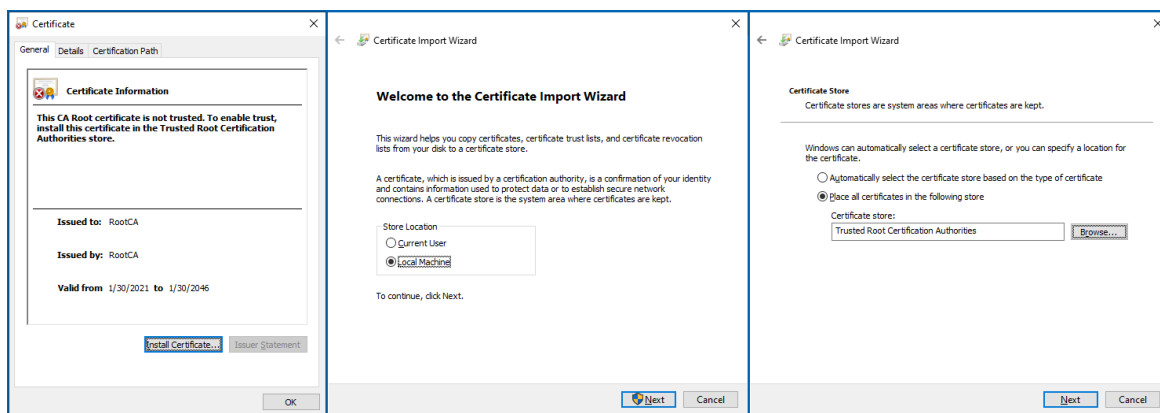
Before launching the Jabber Client (TOE) on the local machine (Windows 11 laptop), the local machine should have the root and intermediate certifies used to sign the CUCM Tomcat and CallManager certificates installed onto the local machines local certificate store.

3.1 Deploy CUCM Certificate Trust Chain to Client Machines

Installing the root and intermediate certificates (trust chain) used to sign the CUCM certificates allows the host machine, and hence TOE, trust the certificates used by the CUCM. The instructions for installing the trust chain certificates are found in On-Premise Deployment for Cisco Jabber 14.1 [2] in the section “Manually Deploy CA Certificates to Cisco Jabber for Windows” in the chapter “Configure Certificate Validation”. This is done by the Administrator using the following step:

- Make the **CA Root and Intermediate Certificates** available to the Cisco Jabber for Windows client machine.
- From the Windows machine, open the **Root Certificate** file.
- Click **Install Certificate** and then select **Next**.
- Select **Local Machine** and then select **Next**.
- Select **Place all certificates in the following store** and then select **Browse**.
- Select the **Trusted Root Certification Authorities** store and then click **OK** and then **Next**.
- When you **Finish** the wizard, a message is displayed to verify successful certificate import.

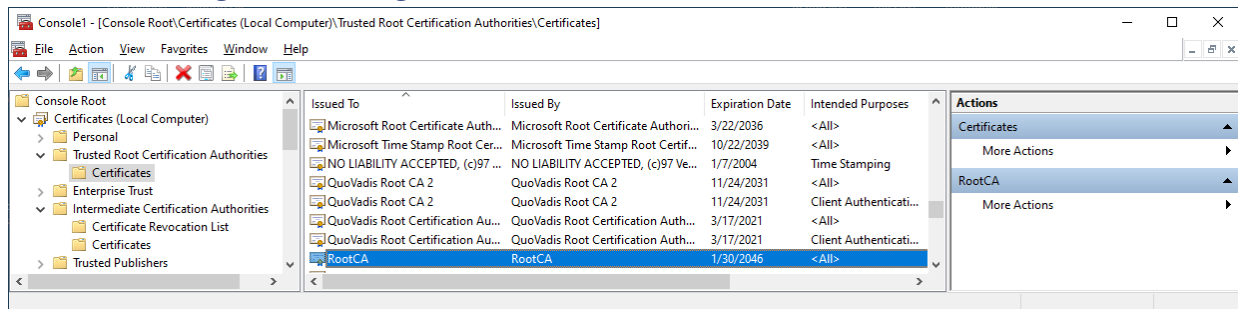
Figure 18. Adding Root Certificate to Windows Device



- Verify that the certificate is installed in the correct certificate store by opening the Windows Certificate Manager tool:
 - From Windows Start search and launch **MMC**
 - Select **File > Add/Remove Snap-in...**
 - Add **Certificates**
 - Select **Computer account** and then **Finish** and then **OK**

- **Browse to Trusted Root Certification Authorities > Certificates.** The CA Root Certificate is listed in the certificate store.

Figure 19. Viewing Windows Trusted Certificates contains Root Certificate



- From the Windows machine, open the **Root Certificate** file.
- Click **Install Certificate** and then select **Next**.
- Select **Local Machine** and then select **Next**.
- Select **Place all certificates in the following store** and then select **Browse**.
- Select the **Intermediate Certification Authorities** store and then click **OK** and then **Next**.
- When you **Finish** the wizard, a message is displayed to verify successful certificate import.
- Verify that the certificate is installed in the correct certificate store by opening the Windows Certificate Manager tool. This will be like the steps above, except **Browse to Intermediate Certification Authorities > Certificates** to verify the **CA Intermediate Certificate** is listed in the certificate store.

The above is an example of how to manually deploy root and intermediate certificate and is included only as one example, these certificates could just as easily be distributed using a certificate deployment tool, such as Group Policy or a certificate deployment management application. The use of Root and Intermediate certificates are required as part of the evaluated configuration, however there is no requirement as to how that deployment is carried out.

3.2 Download Jabber

Download the “Cisco Jabber for Windows Install.zip” file for version 14.0 from the Cisco Software Center into a directory on the TOE platform. The Administrator may download the file by:

- Visiting Cisco’s Software Download page at: <https://software.cisco.com/download/home>
- Searching for **Jabber for Windows**.
- Locating release **15.2(0)**.
- Clicking on and downloading the “Cisco Jabber for Windows Install” ZIP file: **CiscoJabber-Install-ffr.15-2-0.zip** to a folder on the local machine.

The ZIP folder contains an .MSI file that will be used to install the Jabber client. Extract that file.

3.3 Install Jabber

General installation instructions for the Jabber Client are detailed in On-Premise Deployment for Cisco Jabber 14.1 [2] in the section “Install Cisco Jabber for Windows” in the Chapter “Deploy Cisco Jabber Applications and Jabber Softphone for VDI”. The client will be deployed from the Windows Command Line. The Administrator will perform the installation.

The Command Line installation allows enabling, or disabling, various features while deploying the Jabber Client. Many parameters, and details related to them, may be found in the guide references above. For the evaluation, the Administrator will deploy the Jabber Client enabling FIPS mode and CC mode. This allows the TOE to meet two requirements.

The Jabber Client must exclusively use TLS 1.2, which was previously in the CUCM Security section. Enabling FIPS mode and CC mode also limits the TOE to using only TLS, regardless of the settings on CUCM.

An additional restriction is that the TOE terminates the voice/video media transmission to the remote peer if it determines it is no longer receiving SRTP/SDS traffic after 300 seconds (5 minutes). When in CC mode, the default behavior of Jabber is to terminate the voice/video media transmission to the remote peer if it determines it is no longer receiving SRTP/SDS traffic after 300 seconds (5 minutes), which meets the requirement.

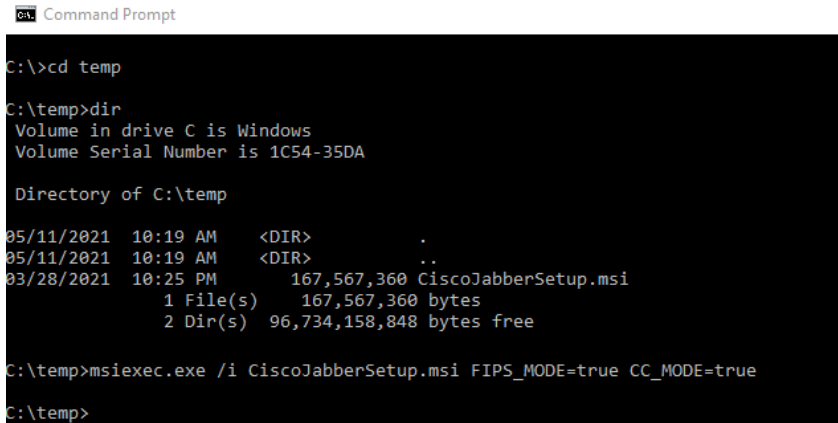
The administrator installs the Jabber Client by:

- Launching the **Windows Command Prompt**.
- Navigating to the directory/folder containing the .MSI file.
- Execute the following command:

```
msiexec.exe /i CiscoJabberSetup.msi FIPS_MODE=true CC_MODE=true
```

- Clicking **Accept and Install**.
- Clicking **Finish** when completed.

Figure 20. Jabber Install from Windows Command Prompt

A screenshot of a Windows Command Prompt window titled "Command Prompt". The prompt shows the user navigating to the C:\temp directory and listing its contents. The directory listing shows a file named CiscoJabberSetup.msi with a size of 167,567,360 bytes. The user then executes the command msiexec.exe /i CiscoJabberSetup.msi FIPS_MODE=true CC_MODE=true. The prompt ends with C:\temp>.

```
C:\>cd temp

C:\temp>dir
Volume in drive C is Windows
Volume Serial Number is 1C54-35DA

Directory of C:\temp

05/11/2021  10:19 AM    <DIR>          .
05/11/2021  10:19 AM    <DIR>          ..
03/28/2021  10:25 PM             167,567,360 CiscoJabberSetup.msi
               1 File(s)      167,567,360 bytes
               2 Dir(s)  96,734,158,848 bytes free

C:\temp>msiexec.exe /i CiscoJabberSetup.msi FIPS_MODE=true CC_MODE=true
C:\temp>
```

The Jabber Client installation is complete when the Windows MSI installer reports the message “Cisco Jabber installer completed”. If the installation fails, the Windows MSI installer will instead report an error message indicating that the installation failed or could not be completed.

3.4 First Registration Attempt

During the initial registration process, the User will be prompted for the Authentication String created/input into the CUCM device configuration earlier (refer to 2.5.4.4 CUCM Device – Softphone). Use that Authentication String when prompted.

After initial login success, The Administrator should log into the CUCM and change the devices “Certification Authority Proxy Function (CAPF) Information” settings. To make the change in CUCM, the Administrator should log into the CUCM GUI for Call Manager Administration, [https://\[CUCM IP or FQDN\]/ccmadmin/](https://[CUCM IP or FQDN]/ccmadmin/), then:

- Choose **Device > Phone**
- Scroll to **Certification Authority Proxy Function (CAPF) Information**
- Change **Certificate Operation** from **Install/Upgrade** to **No Pending Operation**
- Click **Save**

Figure 21. Changing CAPF Certificate Operation after Initial Registration

The screenshot shows the Cisco Unified CM Administration interface. The browser address bar displays <https://10.14.35.12/ccmadmin/phoneEdit.do?key=aa3ec487>. The page title is "Phone Configuration". The navigation menu includes System, Call Routing, Media Resources, Advanced Features, Device, Application, User Management, Bulk Administration, and Help. The "Phone Configuration" section is active, showing a "Related Links" dropdown set to "Back To Find/List". The "Certification Authority Proxy Function (CAPF) Information" section is expanded, displaying the following settings:

- Certificate Operation*: No Pending Operation
- Authentication Mode*: By Authentication String
- Authentication String: 1385241504
- Generate String: (button)
- Key Order*: RSA Only
- RSA Key Size (Bits)*: 2048
- EC Key Size (Bits):
- Operation Completes By: 2021 03 27 12 (YYYY:MM:DD:HH)
- Certificate Operation Status: None
- Note: Security Profile Contains Addition CAPF Settings.

This change only needs to be made during the first registration attempt.

3.5 Microsoft Outlook Integration

Jabber may be integrated with Microsoft to allow users to display Microsoft Outlook Calendar events in Jabber and search for contacts in Microsoft Outlook using Jabber.

3.5.1 Microsoft Outlook Calendar

To allow integration of Jabber with Microsoft Outlook Calendar, the user should perform the following steps:

Step 1 - On the UC Service Configuration (see section 2.5.4.1 CUCM UC Service), create an entry for Section **Options**, Parameter **ExchangeAuthenticateWithSystemAccount**, set “Enables exchange authenticate with system account” to **true**, add the line, and **Save** the change.

Figure 22. UC Service Change for Microsoft Outlook Calendar Integration

The screenshot shows the Cisco Unified CM Administration web interface. The main heading is "UC Service Configuration". Below it, there's a "Status" section showing "Status: Ready". The "UC Service Information" section shows "UC Service Type: Jabber Client Configuration (jabber-config.xml)", "Product Type: Jabber", "Name: Jabber-15.1.0", and "Description: Jabber-15.1.0-config". The "Jabber Configuration Parameters" section contains a table with columns for Section, Parameter, Parameter Description, Value, and Operations. The table has two rows: one for "Options" with "ExchangeAuthenticateWithSystemAccount" set to "true", and another for "Multisync Parameter" which is currently empty.

Section	Parameter	Parameter Description	Value	Operations
Options	ExchangeAuthenticateWithSystemAccount	Enables exchange authenticate with system account	true	Delete
-- Not Selected --	-- Not Selected --			Delete Add Add Custom
Section	Multisync Parameter	Parameter Description	Value	Operations
-- Not Selected --	-- Not Selected --			Add

Step 2 - Open the email account settings in Microsoft Outlook, as in the following example:

- a. Select **File > Account Settings**.
- b. Select the **Email** tab on the **Account Settings** window.

Step 3 - Double-click the server name. In most cases, the server name is **Microsoft Exchange**.

Step 4 - Select the **Use Cached Exchange Mode** checkbox.

Step 5 - Apply the setting and then restart Microsoft Outlook.

Step 6 - Once the Outlook account is configured, on the Jabber client, select **Settings > Calendar** and then check **Microsoft Outlook**.

3.5.2 Microsoft Outlook Contacts

Contact information, including user profile pictures, may be retrieved by Jabber from Microsoft Outlook. This requires action on the parts of both the Administrator and User. To allow Contact integration, the Administrator must:

- Enable Cached Exchange Mode on the Microsoft Exchange server.
- Set user profiles set in Microsoft Outlook.

With the Administrator requirement fulfilled users need to perform the following actions in Jabber:

Step 1 - Select **File > Options**.

Step 2 - Select the **Calendar** tab.

Step 3 - Select **Microsoft Outlook**.

Step 4 - Restart Cisco Jabber to apply the change.

As noted, profile pictures in the Microsoft Outlook Contact list may be used by Jabber. Users may upload pictures to Outlook (from the contact page, click on the generic icon image, then follow the prompts to upload an image).

NOTE: The optimum dimensions for contact photos are 128 pixels by 128 pixels with an aspect ratio of 1:1. 128 pixels by 128 pixels are the maximum dimensions for local contact photos in Microsoft Outlook.

4 Secure Management

4.1 Network Protocols and Cryptographic Settings

Cisco Jabber provides cryptography in support of SIP connections via Security Real-Time Transport Protocol (SRTP) that has been established using the Session Description Protocol (SDP) and the Security Descriptions for Media Streams (SDES) for SDP independently from any other encryption on the device. The TOE also protects communications between itself and the CUCM SIP Server by using a Transport Layer Security (TLS)-protected signaling channel.

4.1.1 SIP Connections and Protocols

Users must specify the authentication string in the client interface to access their devices and securely register with Cisco Unified Communications Manager. When users enter the authentication string in the client interface, the Certificate Authority Proxy Function (CAPF) enrollment process begins. The CAPF process will issue an X.509 certificate for use by the TOE.

There is no direct admin or user interaction on the TOE to configure or set the SRTP channel and no user configuration is required for the cryptographic features of the TOE. The CUCM SIP Server administrator configures the required settings appropriately and then each time a call is made the TOE automatically starts SRTP streams are negotiated. To ensure the SRTP AEAD_AES_256_GCM cipher is used, the CUCM Administrator must configure SRTP ciphers to select the “Strongest Cipher” setting only. The SRTP NULL algorithm is not supported on CUCM and cannot be enabled. There is no user or admin interaction per-SRTP-channel. The CUCM SIP Server administrator can also configure the port ranges for the voice and video streams.

As described above in Section 2 Preparative Procedures and during the initial setup and configuration, the CUCM SIP Server pushes the required configuration settings for establishing secure connections to the prescribed CUCM SIP Server.

If network loss on the SRTP sessions occurs, the TOE automatically attempts to recover. If the user remains dissatisfied with the result, they can end the call and redial. The communication is initiated on the TOE by the user dialing a number.

The SIP connections between the TOE and the CUCM SIP Server are over TLS. The evaluated configuration requires the CUCM SIP Server configured to Encrypted as the value for the Device Security Mode field on the phone security profile.

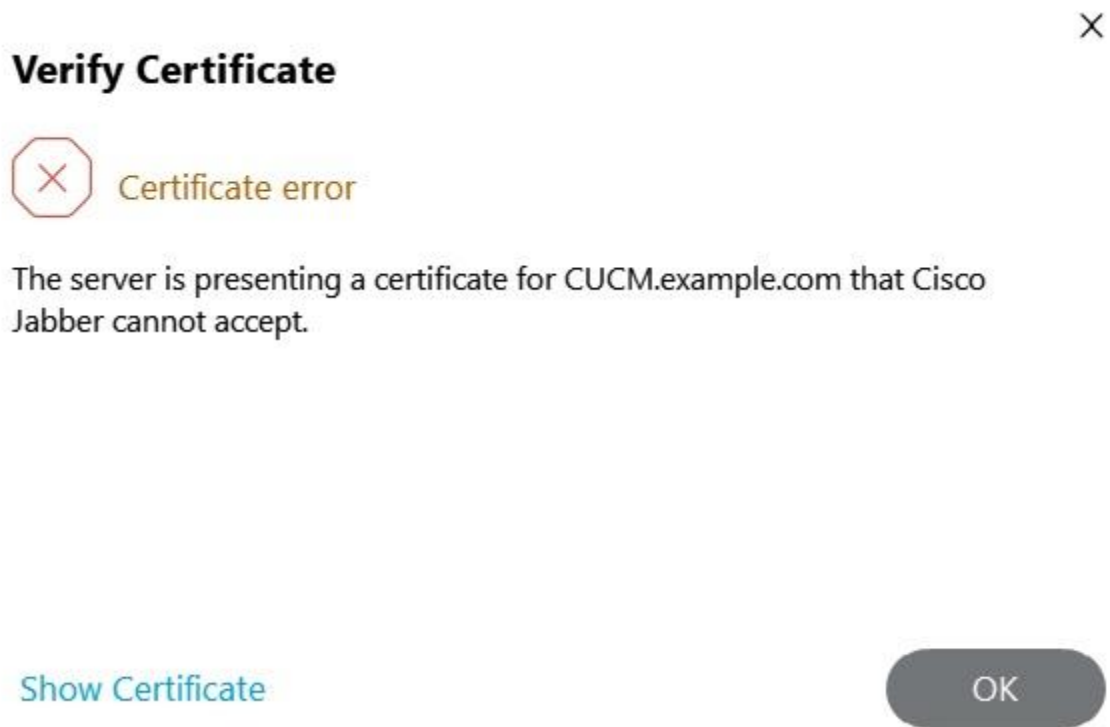
By default, the TOE supports TLS mutual authentication – no configuration is required to enable this feature. TLS mutual authentication ensures that only Client Services Framework (CSF) devices (i.e. the TOE) with the correct certificates can register to CUCM SIP Server. Likewise, CSF devices can register only to CUCM SIP Server instances that provide the correct certificate.

For setting the reference identifier to establish TLS connection to CUCM refer to the “Service Discovery Options” and “Manual Connection Settings” sections in the “Configure Service Discovery” chapter in On-Premise Deployment for Cisco Jabber 14.1 [2]. Cisco Jabber compares the FQDN of the CUCM server against the Subject Alternate Name-dnsName attributes in the certificate. If Jabber determines there is a mismatch, it will not establish the TLS trusted channel. Note that if the server certificate does not contain a SAN, the CN of the certificate is used for comparison purposes instead.

The evaluated configuration requires that Jabber operate in both FIPS and CC modes. Jabber manages certificates more strictly when in FIPS mode. For example, users may see certificate errors in the client if a certificate for a service expires and users do not reenter their credentials before they expire.

If certificate validation fails, the following notification will be displayed, and the user will not have the option to accept the invalid certificate:

Figure 23. Certificate Error Notification

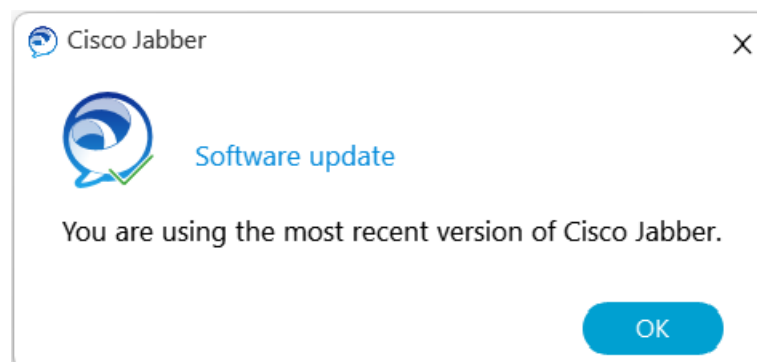


4.2 Product Updates

To check the current version, on the TOE click on the menu button and select Help and then select About Cisco Jabber.

To check for updates, on the TOE click on the menu button and select Help and then select Check for Updates. The following message shows what is expected when Jabber is running the most recent version of software:

Figure 24. Jabber Software Status Message



When software updates are made available by Cisco, an administrator can obtain, verify the integrity of, and install those updates. The updates are a new version of the TOE and can be downloaded from Cisco.com.

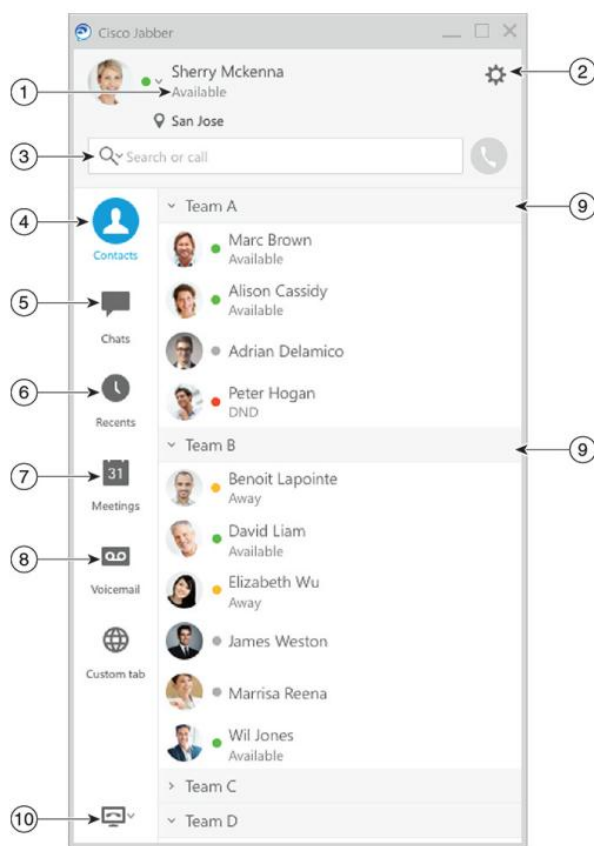
Refer to the “Configure Automatic Updates for Windows” section in the “Deploy Cisco Jabber Applications and Jabber Softphone for VDI” chapter of On-Premises Deployment for Cisco Jabber 14.1 [2].

The client device platform automatically verifies the digital signature of the TOE software to ensure it has not been modified from the originals distributed by Cisco Systems, Inc.

4.3 Jabber Features and Calls

The following diagram is an example for the Cisco Jabber for Windows ‘hub window’.

Figure 25. Jabber Application Hub Window



1. Your status	6. Recent calls
2. Menu	7. Meetings
3. Search or call bar	8. Voicemail
4. Contacts	9. Custom groups
5. Chats	10. Phone controls

For more details and information related to the TOE features refer to the “Voice and Video” chapter of Feature Configuration for Cisco Jabber 14.1 [3]. Note, some options may not be available depending on the deployment options that were configured or covered by this certification.

4.3.1 Contacts

Directory groups are maintained by Authorized Administrator of the Client Platform for your enterprise. When a directory group to your Contacts list is added the list of people assigned to that directory group are automatically added to the group in your contacts. You do not have to maintain the list because it synchronizes automatically with the directory for your enterprise, meaning that people are added and removed from the group in your Contacts whenever the administrator adds or removes them from the enterprise directory. You can remove a directory group from your contacts list at any time.

You can also add contacts that are external to the organization if the Authorized Administrator of the Client Platform has enabled this feature.

Procedure:

Step 1 - Select **File > New** and select the type of contact that you want to add.

Step 2 - Enter the email address of your contact. For custom contacts without an IM address, enter the contact details that you want to use.

Step 3 - Select a contact group.

Step 4 - Select **Add**.

4.3.2 Call

Procedure:

Step 1 - Access the phone number options for your contact.

For example, right-click on a contact in your contact list and choose Call, or from a chat window, click on the phone numbers/address list drop-down list.

Step 2 - Choose Jabber Call.

There are several features that suspend or stop voice media on a call, such as setting the call on hold, transfer, or end call. In addition, entering/leaving a conference can also interrupt voice data briefly.

When a call is placed on voice mute (silence), the connections is not ended or stopped, simply voice data from the microphone is no longer being sent.

Using the Jabber call screen, selecting the 'Mute' icon will mute the voice audio. Selecting the 'Mute' icon again will unmute.

You can also place a call on 'Hold'. By using the Jabber call screen, selecting the 'More' icon and then selecting 'Hold' will place the call on hold or resume the call.

You can also 'Transfer' a call to another person. Using the Jabber call screen, selecting 'More' icon, then selecting 'Transfer', then enter the number you wish to transfer the call too, will transfer the call. End the call by selecting the 'telephone icon'.

For all these functions, the implementation is via SIP and SDP messaging, and the SDP messaging includes the necessary crypto options for secure connections. Any change of participant results in re-keying (unless they are connected to a conference bridge and each endpoint has a unique set of keys applied only to the call leg between it and the bridge).

5 Modes of Operation

Cisco Jabber operates in the On-Premise Deployment mode for Softphones. In this mode the user's primary authentication is to Cisco Unified Communications Manager.

5.1 Troubleshooting

When there is an issue with a feature, for example, if a call is unexpectedly interrupted or disconnected, you should examine the connection status. In the TOE 'hub window' click on the menu button and select Help and then "Show Connection Status". For each server listed, verify that the status displayed is connected.

Additionally, Cisco.com serves 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. For more information, reference Section 7 Obtaining Documentation and Technical Assistance of this document.

6 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 4. Operational Environment Security Measures

Environment Security Objective	IT Environment Security Objective Definition
OE.PLATFORM	The TOE relies upon a trustworthy computing platform for its execution. This includes the underlying operating system and any discrete execution environment provided to the TOE.
OE.PROPER_USER	The user of the application software is not willfully negligent or hostile, and uses the software within compliance of the applied enterprise security policy.
OE.PROPER_ADMIN	The administrator of the application software is not careless, willfully negligent or hostile, and administers the software within compliance of the applied enterprise security policy.

7 Obtaining Documentation and Technical Assistance

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>

Additionally, Cisco.com serves 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 any time, 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.

8 Annex A: Acronyms

The following acronyms and terms are common and may be used in this Security Target.

Table 5. Acronyms

Acronym/Term	Definition
AES	Advanced Encryption Standards
API	Application Programming Interface
CA	Certificate Authority
CAPF	Certificate Authority Proxy Function
CBC	Cipher Block Chaining
CBR	Constant bitrate
CC	Common Criteria
CDP	Certificate Distribution Point
CEM	Common Evaluation Methodology
CLI	Command Line Interface
CM	Configuration Management
CRL	Certificate Revocation List
CSR	Certificate Signing Request
CTI	Computer Telephony Integration
CTL	Certificate Trust List
CUCM	Cisco Unified Communication Manager
DN	Directory Number
DNS	Domain Name System
DRBG	Deterministic Random Bit Generator
EC-DH	Elliptic Curve-Diffie-Hellman
ECDHE	Elliptic Curve Diffie Hellman Ephemeral
ECDSA	Elliptic Curve Digital Signature Algorithm
ESC	Enterprise Session Controller
ESP	Encapsulating Security Payload
FIPS	Federal Information Processing Standards

FQDN	Fully Qualified Domain Name
GCM	Galois Counter Mode
GUI	Graphical User Interface
HDD	Hard Disk Drive
HMAC	Hash Message Authentication Code
IP	Internet Protocol
IT	Information Technology
MMC	Microsoft Management Console
NIC	Network Interface Card
NTP	Network Time Protocol
OCSP	Online Certificate Status Protocol
OS	Operating System
OVA	Open Virtual Appliance
PP	Protection Profile
PRF	Pseudo-Random Functions
RAM	Random Access Memory
RFC	Request For Comment
RSA	Rivest–Shamir–Adleman
SAR	Security Assurance Requirement
SDES	Security Descriptions for Media Streams
SDP	Session Description Protocol
SHS	Secure Hash Standard
SIP	Session Initiation Protocol
SRTP	Security Real-Time Transport Protocol
ST	Security Target
TCP	Transport Control Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol
TFTP	Trivial File Transfer Protocol
TLS	Transport Layer Security
TOE	Target of Evaluation

TSC	TSF Scope of Control
TSF	TOE Security Function
TSP	TOE Security Policy
UC	[Cisco] Unified Communications
UCM	[Cisco] Unified Communications Manager
UDP	User datagram protocol
VoIP	Voice over IP
VM	Virtual Machine
VPN	Virtual Private Network
VVoIP	Voice and Video over IP

9 Annex B: Terminology

The following terms are common and may be used in this Security Target.

Table 6. Terms

Term	Definition
Authorized Administrator	Any user which has been assigned to a privilege level that is permitted to perform all TSF-related functions. Referred to simply as Administrator throughout this document.
Certificate Authority Proxy Function (CAPF)	Process by which supported devices can request locally significant certificates by using Cisco Unified Communications Manager Administration.
Cisco Unified Communications Manager (CUCM)	Cisco Unified Communications Manager (CUCM) serves as the software-based call-processing component of the Cisco Unified Communications family of products. The CUCM extends enterprise telephony features and functions to packet telephony network devices such as IP phones, media processing devices, voice-over-IP (VoIP) gateways, and multimedia applications. CUCM is an Enterprise Session Controller.
Certificate Trust List (CTL)	A file signed by the Cisco Site Administrator Security Token (security token), that contains a list of certificates for servers that the phone is to trust.
CUCM (Call Manger) Cluster	A cluster refers to a CUCM Publisher (first CUCM server installed) and any associated Subscribers (CUCM servers installed after the Publisher and included in the Publishers servers list). For purposes of redundancy, Cisco recommends deployment of at least a Publisher and one subscriber, however from a functional standpoint, Jabber clients only register to a single server at a time.
CUCM (Call Manager) Node	A node refers to a member of a CUCM cluster. The term is used in reference to a publisher or associated Subscribers.
Enterprise Session Controller (ESC)	A VVoIP infrastructure device that is used to set up and tear down calls between VVoIP endpoints
Peer	Another VVoIP device also in communication with the CUCM that is capable of exchanging media packets with the TOE as part of an establishes media session.
Session Initiation Protocol (SIP)	A communications protocol defined by IETF that is used for creating, modifying, and terminating multimedia sessions with multiple participants.
Secure Real-Time Transport Protocol (SRTP)	A protocol that is used to provide multimedia (voice/video) streaming services with added security of encryption, message authentication and integrity, and replay protection.
SIP Server	The SIP Server (in this evaluation it is the Cisco Unified Communications Manager (CUCM) interacts with a VoIP client (TOE) and provides registrar and proxy capabilities required for call-session management as well as establishing, processing, and terminating VoIP calls.
User	Any entity (human user or external IT entity) outside the TOE that interacts with the TOE.