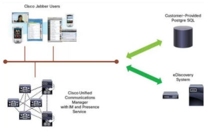
Manuals+ — User Manuals Simplified.


Cisco Jabber Users
Customer-Provided Postgre SQL
eDiscovery System
Cisco Unified Communications Manager with IM and Presence Service

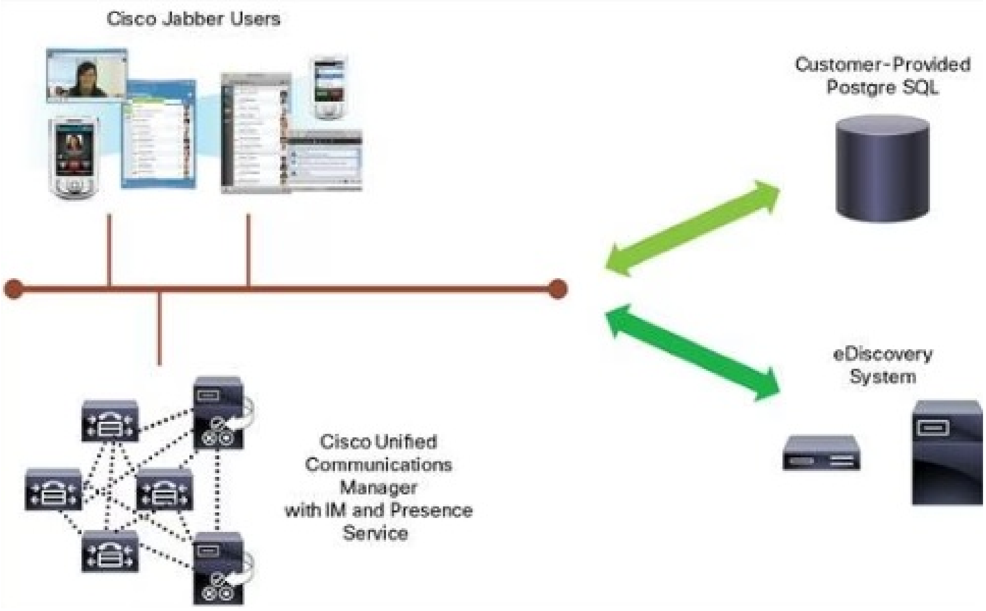
CISCO 800 Series Unified Communications Manager IM Presence Service User Guide

Home » Cisco » CISCO 800 Series Unified Communications Manager IM Presence Service User Guide

Contents

1 CISCO 800 Series Unified Communications Manager IM Presence Service
2 Product Information
3 Compatibility Matrix for Cisco Unified Communications Manager and the IM and Presence Service, Release 12.5(X)
4 Purpose of this Document
5 Required COP Files
6 Supported Versions
7 Version Compatibility Between Unified CM and the IM and Presence Service
8 Unified Communications Manager Compatibility Information
9 Cisco Endpoint Support
10 Virtualization Requirements
11 Supported LDAP Directories 12.5(x)
12 Secure Connections
13 Supported Ciphers for Unified Communications Manager
14 Supported Ciphers for SSH
15 Supported Platforms for Cisco Unified JTAPI and TAPI
16 External Database Support
17 Intercluster Peering Support
18 Calendar Integration with Microsoft Outlook
19 Supported Ciphers for the IM and Presence Service
20 Remote Call Control with Microsoft Lync
21 Configuration
22 Documents / Resources
22.1 References
23 Related Posts

CISCO 800 Series Unified Communications Manager IM Presence Service


Cisco Jabber Users
Customer-Provided Postgre SQL
eDiscovery System
Cisco Unified Communications Manager with IM and Presence Service

Product Information

Compatibility Matrix for Cisco Unified Communications Manager and the IM and Presence Service, Release 12.5(X)

- The Compatibility Matrix provides information on the compatibility of Cisco Unified Communications Manager and the IM and Presence Service. This document is applicable to Release 12.5(X) and includes compatibility information for subsequent SU releases as well, unless indicated otherwise.

Revision History

The following is the revision history of the Compatibility Matrix:

- August 30, 2023
- August 03, 2023
- January 31, 2023
- November 29, 2022
- December 08, 2022
- February 15, 2022
- May 05, 2022
- August 03, 2021
- February 22, 2021
- March 25, 2021
- April 28, 2021
- August 13, 2020
- October 19, 2020
- December 13, 2020
- June 19, 2019

Compatibility Matrix for Cisco Unified Communications Manager and the IM and Presence Service, Release 12.5(X)

- Compatibility Matrix for Cisco Unified Communications Manager and the IM and Presence Service 2 Revision History 2
- Purpose of this Document 3
- Supported Upgrade and Migration Paths 4
- Supported Versions 6
- Unified Communications Manager Compatibility Information 8
- IM and Presence Service Compatibility Information 25

Revised: August 31, 2023
Compatibility Matrix for Cisco Unified Communications Manager and the IM and Presence Service

Revision History

Date	Revision
August 30, 2023	Initial release version for 12.5(1)SU8a.
August 30, 2023	Updated support version for Unified CM Release 12.5(1)SU8a.
August 03, 2023	Initial release version for 12.5(1)SU8.
August 03, 2023	Updated support versions for 12.5(1)SU8.
August 03, 2023	Added support for Cisco Video Phone 8875 and Cisco Video Phone 8875NR.
January 31, 2023	Initial release version for 12.5(1)SU7a.
January 31, 2023	Updated support version for Unified CM Release 12.5(1)SU7a.
November 29, 2022	Initial release version for 12.5(1)SU7.
December 08, 2022	Updated upgrade paths and version support for 12.5(1)SU7.
December 08, 2022	WebEx Desk Camera is rebranded to Cisco Desk Camera 4K.
December 08, 2022	Added support for Cisco Desk Camera 1080p.
December 08, 2022	Added support for Cisco Headset 320 Series and Cisco Headset 720 Series.
February 15, 2022	Initial release version for 12.5(1)SU6.
February 15, 2022	Updated upgrade paths and version support for 12.5(1)SU6.
February 15, 2022	Added support for WebEx Desk Hub and WebEx Wireless Phone 800 Series
May 05, 2022	Renamed some of the ROOM device names to remove WebEx from them.
August 03, 2021	Initial release version for 12.5(1)SU5.
August 03, 2021	Updated upgrade paths and version support for 12.5(1)SU5.
August 03, 2021	Added Microsoft Exchange Server 2019 support for the IM and Presence Service Calendar Integration with Microsoft Outlook.
February 22, 2021	Initial release version for 12.5(1)SU4.
February 22, 2021	Updated upgrade paths and version support for 12.5(1)SU4.

Date	Revision
February 22, 2021	Added IM and Presence Service support for the advertisement of XMPP stream features/services over Mobile and Remote Access.
February 22, 2021	Added support for Cisco VG420 Analog Voice Gateway and Cisco Catalyst 8300 Series Edge Platforms.
March 25, 2021	Fixed the 7941 G Series EOS URL.
April 28, 2021	Added support for Ciphers for Application and OS End Users.
August 13, 2020	Updated version support for 12.5(1)SU3.
August 13, 2020	Added support for Microsoft® Active Directory® Federation Services 3.0, 4.0, and 5.0, and Microsoft Azure.
October 19, 2020	Corrected list of WebEx endpoints.
November 18, 2020	Corrected dates.
December 13, 2020	Renamed Cisco Weber Teams to Cisco WebEx.
June 19, 2019	Added OpenJDK version for 12.5(1)SU1 release.
	Updated for 12.5(1)SU1. Changed title to 12.5(x)
February 03, 2020	Updated upgrade paths, LDAP support, version support for 12.5(1)SU2.
February 20, 2020	Updated LDAPv3 Compliant Directories.
March 09, 2020	Updated Cisco Endpoint Support section.
March 11, 2020	Added Cisco Headsets to Endpoint Support.
April 06, 2020	Removed non-supported Cisco endpoints.
May 12, 2020	Added JTAPI Support information.
July 8, 2020	Updated SSL Connections and SSH Clients.
July 27, 2020	Updated supported ciphers list for IM and Presence Service.

Purpose of this Document

- This document contains compatibility information for 12.5(x) releases of Cisco Unified Communications Manager (Unified Communications Manager) and the Cisco Unified Communications Manager IM and Presence Service (IM and Presence Service). This includes subsequent SU releases as well, unless indicated otherwise.

Supported Upgrade and Migration Paths

The following table highlights supported upgrade paths to upgrade to 12.5(x) releases of Unified Communications Manager and the IM and Presence Service.

Note

- Unless indicated otherwise, each release category includes the SU releases within that category. For example, 12.5(x) includes 12.5(1)SU releases. In addition, releases like 10.5(x) and 11.x include any SU releases within those categories as well.

Table 1: Supported Upgrade Paths for Cisco Unified Communications Manager and the IM and Presence Service

Source	**Destination**	**Supported Upgrade Method**	**Version Switching* (Source to Destination and Vice Versa)**
Cisco Unified Communications Manager Upgrade Paths			
Unified CM 10.0(x)	12.5(x)	PCD Migration**	Version switching not supported
Unified CM 10.5(x), 11.x, 12.0(x)	12.5(x)	• Unified OS Admin upgrade (direct refresh) CLI upgrade (direct refresh) • PCD Upgrade (direct refresh)** PCD Migration** • Fresh Install with Data Import only to destination 12.5(1)SU5 or later. **Note** If the source release is 10.5(x) and the destination release is 12.5(1) through 12.5(1)SU5, PCD Upgrade Task is supported. If the source release is 10.5(x) and the destination release is 12.5(1)SU6 and above, PCD Upgrade Task is not supported.	Version switching supported for upgrades, but not for migrations
Unified CM 12.5(x)	12.5(y)	• Unified OS Admin upgrade (direct standard) CLI upgrade (direct standard) • PCD Upgrade (direct standard)** • Fresh Install with Data Import only to destination 12.5(1)SU5 or later.	Version switching supported for upgrades, but not for migrations
IM and Presence Service Upgrade Paths			
IM and Presence 10.0(x)	IM and Presence 12.5(x)	PCD Migration**	Version switching not supported

Source	Destination	Supported Upgrade Method	Version Switching* (Source to Destination and Vice Versa)
IM and Presence 10.5(x), 11.x or 12.0(x)	12.5(x)	• Unified OS Admin upgrade (direct refresh) CLI upgrade (direct refresh) • PCD upgrade (direct refresh) • PCD Migration	Version switching supported for upgrades, but not supported for migrations.
		Fresh Install with Data Import only to destination 12.5(1)SU5 or later.	
IM and Presence 12.5(x)	12.5(y)	• Unified OS Admin upgrade (direct standard) CLI upgrade (direct standard) • PCD upgrade (direct standard)** • Fresh Install with Data Import only to destination 12.5(1)SU5 or later.	Version switching supported for upgrades, but not supported for migrations.

- Version switching refers to the ability to install the new version as an inactive version and switch to the new version, and revert to the old version, whenever you want. This capability is supported with most direct upgrades, but not with migrations.
- PCD Upgrades and Migrations—Use Cisco Prime Collaboration Deployment Release 12.6 or later for all PCD tasks. If you want to upgrade or migrate to Unified CM Release 12.5(1)SU6 and above, ensure that you use the Release 14 version of the Cisco Prime Collaboration Deployment.

Required COP Files

- The tables below lists the upgrade paths that require COP files. You must install COP files on each node before you begin an upgrade using the Cisco Unified OS Administration interface, or before you begin an upgrade or migration using the Prime Collaboration Deployment (PCD) tool.
- If you are using PCD, you can perform a bulk installation of the COP files before you begin the upgrade.
- You can download COP files for Cisco Unified Communications Manager and the IM and Presence Service at https://software.cisco.com/download/home/268439621. After you select the destination version for the upgrade, choose Unified Communications Manager Utilities to see the list of COP files.

Note

You should run the Upgrade Readiness COP file prior to the upgrade in order to maximize upgrade success. If you do not run this COP file, you increase the risk of an unsuccessful upgrade due to undetected issues on the source release. Cisco TAC may require that you run this COP file to provide effective technical support.

Table 2: Required COP Files

From	To	COP Files
Unified Communications Manager Upgrades		

From	To	COP Files
Unified CM 10.5(x), 11.0(x)	12.5(x)	Direct Refresh upgrade Required COP file: ciscocm.enable-sha512sum-2021-signingkey-v1.0.cop.sgn. See the COP file for more information.
Unified CM 11.5(x)	12.5(x)	Direct Refresh upgrade; COP file is required to increase the disk space. ciscocm.free_common_space_v<latest_ version>.cop sgn. To download the COP files and the Readme files, go to https://software.cisco.com, click **Software Download** link under **Download & Upgrade** section, and navigate to the **Unified Communications** > **Call Control** > **Cisco Unified Communications Manager (Call Manager)** > ***<Version>*** > **Unified Communications Manager/Call Manager/Cisco Unity Connection Utilities**. Required COP file: ciscocm.enable-sha512sum-2021-signingkey-v1.0.cop.sgn. See the COP file for more information.
Unified CM 12.0(1)	12.5(x)	PCD Migrations require a COP file - ciscocm-slm-migration.k3.cop.sgn **Note** This requirement applies only for Prime Collaboration Deployment migrations from Release 12.0(1) of Unified Communications Manager (build 12.0.1.10000-10). If you are migrating from a higher release, such as Unified Communications Manager 12.0(1)SU1, you don’t need to install the COP file. - Required COP file: ciscocm.enable-sha512sum-2021-signingkey-v1.0.cop.sgn. See the COP file for more information.
Unified CM 12.5(x)	12.5(y)	Direct Standard upgrade Required COP file: ciscocm.enable-sha512sum-2021-signingkey-v1.0.cop.sgn. See the COP file for more information.
IM and Presence Service Upgrades		
10.5(x), 11.x, 12.x	12.5(x)	No COP files required

Supported Versions

- The following table outlines which Unified Communications Manager and IM and Presence Service versions are supported with each release:

For this Release…	The Following Versions are Supported…
12.5(1)	• Unified Communications Manager 12.5.1.10000-22 • IM and Presence Service 12.5.1.10000-22

For this Release…	The Following Versions are Supported…
12.5(1)SU1	• Unified Communications Manager 12.5.1.11900-146 • IM and Presence Service 12.5.1.11900-117
12.5(1)SU2	• Unified Communications Manager 12.5.1.12900-115 • IM and Presence Service 12.5.1.12900-25
12.5(1)SU3	• Unified Communications Manager 12.5.1.13900-152 • IM and Presence Service 12.5.1.13900-17
12.5(1)SU4	• Unified Communications Manager 12.5.1.14900-63 • IM and Presence Service 12.5.1.14900-4
12.5(1)SU5	• Unified Communications Manager 12.5.1.15900-66 • IM and Presence Service 12.5.1.15900-5
12.5(1)SU6	• Unified Communications Manager 12.5.1.16900-48 • IM and Presence Service 12.5.1.16900-3
12.5(1)SU7	• Unified Communications Manager 12.5.1.17900-64 • IM and Presence Service 12.5.1.17900-7
12.5(1)SU7a	• Unified Communications Manager 12.5.1.18100-14 • IM and Presence Service 12.5.1.17900-7
12.5(1)SU8	• IM and Presence Service 12.5.1.18900-6
12.5(1)SU8a	• Unified Communications Manager 12.5.1.18901-1

Version Compatibility Between Unified CM and the IM and Presence Service

- Version compatibility depends on the IM and Presence Service deployment type. The following table outlines the options and whether a release mismatch is supported between the telephony deployment and the IM and Presence Service deployment. A release mismatch, if it is supported, would let you deploy your Unified Communications Manager telephony deployment and your IM and Presence Service deployment using different releases.

Note

- Any respin or ES that is produced between Cisco.com releases is considered part of the previous release. For example, a Unified Communications Manager ES with a build number of 12.5.1.18[0-2]xx would be considered part of the 12.5(1)SU7 (12.5.1.17900-x) release.
- For Release 12.5(1)SU7a, a Unified Communications Manager ES with a build number of 12.5.1.181xx would be considered part of the 12.5(1)SU7a (12.5.1.18100-x) release.
- For Release 12.5(1)SU8a, a Unified Communications Manager ES with a build number of 12.5.1.19[0-2]xx would be considered part of the 12.5(1)SU8a (12.5.1.18901-1) release.

Table 3: Version Compatibility between Unified Communications Manager and the IM and Presence Service

Deployment Type	Release Mismatch	Description
Standard Deployment of IM and Presence Service	Not supported	Unified Communications Manager and the IM and Presence Service are in the same cluster and must run the same release—a release mismatch is not supported.
Centralized Deployment of IM and Presence Service	Supported	The IM and Presence Service deployment and the telephony deployment are in different clusters and can run different releases—a release mismatch is supported. **Note** The IM and Presence Service central cluster also includes a standalone Unified CM publisher node for database and user provisioning. This non-telephony node must run the same release as the IM and Presence Service.

Unified Communications Manager Compatibility Information

Cisco Collaboration System Applications

- The 12.5.x release of Cisco Unified Communications Manager and the IM and Presence Service is a part of the Cisco Collaboration Systems Release 12.5 through 12.8 and is compatible with the other Cisco Collaboration applications and versions in Cisco Collaboration Systems Release 12.5.
- **Note** Note that Release 12.5(1)SU3 is compatible with the 12.8 version of the Cisco Collaboration Systems.
- For a full list of Cisco Collaboration applications that are a part of Cisco Collaboration Systems Release

12.5(x), and the supported versions for each, see the Cisco Collaboration Systems Release Compatibility Matrix at:

- **https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/uc_system/unified/communications/system/C Compatibility-Matrix-InteractiveHTML.html.**

Android Push Notifications Compatibility Recommendations

- Android Push Notification feature is supported from the following software versions:
- Unified Communications Manager 12.5(1)SU3
- IM and Presence Service 12.5(1)SU3
- Cisco Jabber 12.9.1
- Cisco Expressway X12.6.2

Note This compatibility information isn't applicable for Cisco WebEx.

Table 4: Recommended Release Requirements for Android Push Notifications Support

Unified Communications Manager and IM and Presence Service Version	Expressway Version	Unified Communications Mobile and Remote Access	On-Premises Deployments
All clusters on: • 11.5(1)SU8 or earlier • 12.5(1)SU2 or earlier	X12.6.2	Android Push Notification is not supported	Android Push Notification is not supported
• All clusters on • 12.5(1)SU3 and onwards	X12.6.2	Enable Android Push Notification using the CLI **configuration XCP Config FcmService: On** on Expressway for messaging only	Android Push Notification is supported
Cluster with mixed versions (11.5(1)SU8 or earlier, OR 12.5(1)SU2 or earlier, AND 12.5(1)SU3 onwards)	X12.6.2	Android Push Notification for Messaging is not supported VOIP is supported from Release 12.5(1)SU3 onwards	Android Push Notification is supported from Release 12.5(1)SU3 onwards

IM and Presence Stream Features/Services Advertisement Compatibility Recommendations

- IM and Presence Service supports the advertisement of XMPP stream features/services to the clients connecting over Cisco Expressway's Mobile and Remote Access.
- Depending on your current IM and Presence Service version mix, you may need to enable or disable push notifications feature using FCM service flag on the Expressway as per the information given in the following table:

- configuration XCP Config FcmService: On/Off

Note Apple Push Notification Service (APNS) is not affected by the FCM service flag status.

Table 5: Solution Matrix from the Perspective of Expressway CLI Enable/Disable Command for Android Push Notifications (FCM)

Mixed Versions IM and Presence Clusters	Expected Status of FCM Flag on Expressway X12.7	Comment
• Any 11.5(1)SU with • 12.5(1)SU2 and lower	OFF	Android Push (FCM) NOT supported.

Mixed Versions IM and Presence Clusters	Expected Status of FCM Flag on Expressway X12.7	Comment
11.5(1)SU8 (and lower) or 12.5(1)SU2 (and lower) with 12.5(1)SU3	OFF	Android push (FCM) NOT supported
11.5(1)SU8 (and lower) or 12.5(1)SU2 (and lower) with 12.5(1)SU4 (and higher)	OFF	Android push (FCM) supported on 12.5(1)SU4 (or newer) versions
11.5(1)SU9 (and higher) or 12.5(1)SU4 (and higher) with 12.5(1)SU3	ON	Android push (FCM) supported on version 12.5(1)SU3 and higher
11.5(1)SU9 (and higher) with 12.5(1)SU4 (and higher)	Flag not required (Expressway 12.7 relies fully on the new discovery mechanism)	Android push (FCM) supported on 12.5(1)SU4 (or newer) versions

Cisco Endpoint Support

- All end of Life and End of Sale announcements are listed here: https://www.cisco.com/c/en/us/products/eos-eol-listing.html.

Supported Cisco Endpoints

- The following table lists Cisco endpoints that are supported with this release of Cisco Unified Communications Manager. For endpoints that have reached End of Sale (EOS), or End of Software Maintenance, click the EOS link to view support details.

Note

Unless they are specified in the “Deprecated Phone Models” list, phone models that are End of Software Maintenance will continue to be supported on the latest Unified Communications Manager releases. However, they will not take advantage of any new Unified Communications Manager or firmware features associated with that release.

Table 6: Supported Cisco Endpoints

Device Series	**Device Model**
Cisco Unified SIP Phone 3900 Series	Cisco Unified SIP Phone 3905
Cisco Unified IP Phone 6900 Series	Cisco Unified IP Phone 6901
Cisco IP Phone 7800 Series	Cisco IP Phone 7811 Cisco IP Phone 7821 Cisco IP Phone 7841 Cisco IP Phone 7861 Cisco IP Conference Phone 7832

Device Series	**Device Model**
Cisco Unified IP Phone 7900 Series	Cisco Unified IP Phone Expansion Module 7915—**EOS Notice** Cisco Unified IP Phone Expansion Module 7916—**EOS Notice** Cisco Unified IP Phone 7942G—**EOS Notice** Cisco Unified IP Phone 7945G—**EOS Notice** Cisco Unified IP Phone 7962G—**EOS Notice** Cisco Unified IP Phone 7965G—**EOS Notice** Cisco Unified IP Phone 7975G—**EOS Notice**
Cisco IP Phone 8800 Series	Cisco IP Phone 8811, 8831, 8841, 8845, 8851, 8851NR, 8861, 8865, 8865NR Cisco Wireless IP Phone 8821, 8821-EX—**EOL Notice** Cisco Unified IP Conference Phone 8831—**EOS Notice** Cisco IP Conference Phone 8832 Cisco Video Phone 8875 Cisco Video Phone 8875NR
Cisco Unified IP Phone 8900 Series	Cisco Unified IP Phone 8945—**EOS Notice** Cisco Unified IP Phone 8961—**EOS Notice**
Cisco Unified IP Phone 9900 Series	Cisco Unified IP Phone 9951—**EOS Notice** Cisco Unified IP Phone 9971—**EOS Notice**
Cisco Jabber	• Cisco Jabber for Android • Cisco Jabber for iPhone and iPad Cisco Jabber for Mac • Cisco Jabber for Windows • Cisco Jabber Softphone for VDI – Windows (formerly Cisco Virtualization Experience Media Edition for Windows) • Cisco Jabber Guest • Cisco Jabber Software Development Kit Cisco Jabber for Tablet
Cisco Headset Series	• Cisco Headset 320 • Cisco Headset 520 • Cisco Headset 530 • Cisco Headset 560 • Cisco Headset 720 • Cisco Headset 730

Device Series	**Device Model**
Cisco IP Communicator	Cisco IP Communicator—EOS Notice
Webex	Webex App - Webex Room Phone Webex Desk - Webex Desk Hub Webex Desk Pro - Webex Desk Limited Edition Webex Share—EOS Notice Board 55, 55S, 70, 70S, 85, 85S - Webex Room Panorama Webex Room 70 Panorama - Webex Room 70 Panorama Upgrade Room 70 - Room 70 G2 - Room 55 - Room 55 Dual Room Kit Pro Room Kit Plus Room Kit Room Kit Mini - Webex Room USB
Webex Wireless Phone 800 Series	- Webex Wireless Phone 840 - Webex Wireless Phone 860
Webex Meetings	- Webex Meetings for iPad and iPhone - Webex Meetings for Android
Cisco Analog Telephony Adapters	- Cisco ATA 190 Series Analog Telephone Adapters—EOS/EOL Notice - Cisco ATA 191 Series Analog Telephone Adapters
Cisco DX Series	- Cisco Webex DX70—EOS Notice Cisco Webex DX80—EOS Notice - Cisco DX650—EOS Notice
Cisco Tele Presence IX5000	Cisco Tele Presence IX5000
Cisco Tele Presence EX Series	Cisco Tele Presence System EX90—EOS Notice

Device Series	Device Model
Cisco Tele Presence MX Series	• Cisco Tele Presence MX200 G2—EOS Notice Cisco Tele Presence MX300 G2—EOS Notice Cisco Tele Presence MX700D—EOS Notice Cisco Tele Presence MX800S—EOS Notice • Cisco Tele Presence MX800D—EOS Notice
Cisco Tele Presence SX Series	• Cisco Tele Presence SX10—EOS Notice Cisco Tele Presence SX20—EOS Notice • Cisco Tele Presence SX80—EOS Notice

- Cisco Unified Communications Manager Release 12.5(1) is a part of Cisco Collaboration Systems Release 12.5. For a list of firmware versions that are used for each Cisco endpoint, see the Cisco Collaboration Systems Release Compatibility Matrix at
- **http://www.cisco.com/c/en/us/td/docs/voice_ip_comm/uc_system/unified/communications/system/Compa**
- CSR-Compatibility-Matrix.html.
- For information about Device Pack compatibility to support the phones, see the Cisco Unified Communications Manager Device Package Compatibility Matrix at **http://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/compat/matrix/CMDP_BK_CCBDA741_** 00_cucm-device-package-compatibility-matrix.html.

End of Support

- The following table lists Cisco endpoints that have reached the End of Support date, but which are not yet deprecated. Unlike deprecated endpoints, you can still deploy these endpoints in the latest release, but they are not supported actively, are not tested, and may not work.
- Click the links to view support announcements for each endpoint.
- For information on all of the End of Support and End-of-Life products, see **https://www.cisco.com/c/en_ca/products/eos-eol-listing.html.**

Table 7: Cisco Endpoints at End of Support

Cisco Endpoints at End of Support

- Cisco Unified SIP Phone 3911, 3951
- Cisco Unified IP Phone 6911, 6921, 6941, 6945, 6961, 7906G, 7911G, 7931G, 7940G, 7941G, 7960G, 7961G, 8941
- Cisco Unified IP Phone Expansion Module 7925G, 7925G-EX, 7926G
- Cisco Unified IP Conference Station 7935, 7936, 7937G
- Cisco Tele Presence EX60
- Cisco Tele Presence MX200-G1, MX200-G2, MX300-G1, MX300-G2
- Cisco Tele Presence 500-32, 500-37, 1000 MXP, 1100, 1300-65, 1300-47, 3000 Series

Deprecated Phone Models

- The following table lists all the phone models that are deprecated for this release of Unified Communications Manager, along with the Unified CM release where the phone model first became deprecated. For example, a phone model that was first deprecated in Release 11.5(1) is deprecated for all later releases, including all 12.x releases.
- If you are upgrading to the current release of Unified Communications Manager and you have any of these phone models deployed, the phone will not work after the upgrade.

Table 8: Deprecated Phone Models for this Release

Deprecated Phone Models for this Release	First Deprecated as of Unified C M…
• Cisco Unified Wireless IP Phone 7921 • Cisco Unified IP Phone 7970 • Cisco Unified IP Phone 7971	12.0(1) and later releases
• Cisco IP Phone 12 S • Cisco IP Phone 12 SP • Cisco IP Phone 12 SP+ • Cisco IP Phone 30 SP+ • Cisco IP Phone 30 VIP • Cisco Unified IP Phone 7902G • Cisco Unified IP Phone 7905G • Cisco Unified IP Phone 7910 • Cisco Unified IP Phone 7910G • Cisco Unified IP Phone 7910+SW • Cisco Unified IP Phone 7910G+SW • Cisco Unified IP Phone 7912G • Cisco Unified Wireless IP Phone 7920 • Cisco Unified IP Conference Station 7935	11.5(1) and later releases

- For additional information, refer to Field **Notice**: Cisco Unified Communications Manager Release 11.5(x) does not support some deprecated phone models at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/rel_notes/11_5_1/fieldNotice/cucm_b_ fn-deprecated-phone-
- models-1151.html.
- For additional information refer to the Field **Notice**: Cisco Unified Communications Manager Release 12.0(x) does not support some deprecated phone models at http://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/rel_notes/12_0_1/deprecated_phones/cucm_

- b_deprecated-phone-models-for-1201.html.
- Upgrades that Involve Deprecated Phones
- If you are using any of these phones on an earlier release and you want to upgrade to this release, do the following

1. Confirm whether the phones in your network will be supported in this release.
2. Identify any non-supported phones.
3. For any non-supported phones, power down the phone and disconnect the phone from the network.
4. Provision a supported phone for the phone user. You can use the following methods to migrate from older model to newer model phones

   Migration FX tool
5. Once all the phones in your network are supported by this release, upgrade your system.

Note

- Deprecated phones can also be removed after the upgrade. When the administrator logs in to Unified Communications Manager after completing the upgrade, the system displays a warning message notifying the administrator of the deprecated phones.

Licensing

- You do not need to purchase a new device license to replace a deprecated phone with a supported phone. The device license becomes available for a new phone when you either remove the deprecated phone from the system, or when you switch to the new Unified Communications Manager version, and the deprecated phone fails to register.

Virtualization Requirements

- This release of Unified Communications Manager and the IM and Presence Service supports virtualized deployments only. Deployments on bare-metal servers are not supported. For more information, see **http://www.cisco.com/go/virtualized-collaboration.** See the following table for virtualization requirements.

Table 9: Virtualization Requirements

Virtualization Requirements for	For information, go to…
Unified Communications Manager	For information about Unified Communications Manager virtualization requirements, go to https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/uc_system/virtualization/ virtualization-cisco-unified-communications-manager.html.
IM and Presence Service	For information about the IM and Presence Service virtualization requirements, go to https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/uc_system/virtualization/ virtualization-cisco-ucm-im-presence.html.
Cisco Business Edition Deployments	For information on the virtualization requirements for Unified Communications Manager in a collaboration solution deployment such as Cisco Business Edition, go to https://www.cisco.com/ c/dam/en/us/td/docs/voice_ip_comm/uc_system/virtualization/ cisco-collaboration-infrastructure.html.

Supported LDAP Directories 12.5(x)

The following LDAP directories are supported

- Microsoft Active Directory 2008 R1/ R2
- Microsoft Active Directory 2012 R1/ R2
- Microsoft Active Directory 2016
- Microsoft Active Directory 2019—Supported for 12.5(1)SU2 and later
- Microsoft Lightweight Directory Services 2008 R1/ R2
- Microsoft Lightweight Directory Services 2012 R1/ R2
- Microsoft Lightweight Directory Services 2019—Supported for 12.5(1)SU2 and later
- Oracle Directory Services Enterprise Edition 11gR1 (11.1.1.7.x or newer)
- Oracle Unified Directory 11gR2 (11.1.2.2.0 or 11.1.2.3.0)
- Open LDAP 2.4.45 or later
- Other LDAPv3 Compliant Directories—Unified Communications Manager uses standard LDAPv3 for accessing the user’s data. Ensure that the supported control attribute is configured in the LDAPv3 compliant directory servers to be used with DirSync.(The supported control attribute may return the pagecontrolsupport and persistent control support sub attributes, if configured.)

Supported Web Browsers

The following web browsers are supported

- Chrome with Windows 10 (64 bit)
- Firefox with Windows 10 (64 bit)
- Internet Explorer 11 with Windows 7 (64 bit)
- Internet Explorer 11 with Windows 10 (64 bit)

- Microsoft Edge browser with Windows 10 (32 bit/64 bit)
- Safari with MacOS (10.x)

Note We recommend that you use the latest version for all the web browsers supported.

SFTP Server Support

- For internal testing, we use the SFTP Server on Cisco Prime Collaboration Deployment (PCD) which is provided by Cisco, and which is supported by Cisco TAC. Refer to the following table for a summary of the SFTP server options:

Table 10: SFTP Server Support

SFTP Server	Support Description
SFTP Server on Cisco Prime Collaboration Deployment	This server is the only SFTP server that is provided and tested by Cisco, and fully supported by Cisco TAC. Version compatibility depends on your version of Emergency Responder and Cisco Prime Collaboration Deployment. See the Cisco Prime Collaboration Deployment Administration Guide before you upgrade its version (SFTP) or Emergency Responder to ensure that the versions are compatible.
SFTP Server from a Technology Partner	These servers are third party provided and third party tested. Version compatibility depends on the third-party test. See the Technology Partner page if you upgrade their SFTP product and/or upgrade Unified Communications Manager for which versions are compatible https://marketplace.cisco.com
SFTP Server from another Third Party	• These servers are third party provided and are not officially supported by Cisco TAC. • Version compatibility is on a best effort basis to establish compatible SFTP versions and Emergency Responder versions. **Note** These products have not been tested by Cisco and we cannot guarantee functionality. Cisco TAC does not support these products. For a fully tested and supported SFTP solution, use Cisco Prime Collaboration Deployment or a Technology Partner.

SAML SSO Support

Although Cisco Collaboration infrastructure may prove to be compatible with other IdPs claiming SAML 2.0 compliance, only the following Dips' have been tested with Cisco Collaboration solutions:

- Microsoft® Active Directory® Federation Services 2.0, 3.0, 4.0, and 5.0
- Microsoft Azure AD
- Okta
- OpenAM
- Pin federate®

- F5 BIG-IP

For additional information on SAML SSO, see the SAML SSO Deployment Guide for Cisco Unified Communications Applications.

API Development

- The following table provides information on the API Development package that is supported with this release.

Table 11: Supported API Package

Package Type	Details
API Development	Cisco Unified Communications Manager and the IM and Presence Service support OpenJDK for application development. - Release 12.5(1) uses OpenJDK version 1.7.0.191 - Release 12.5(1)SU1 uses OpenJDK version 1.7.0.201. - Release 12.5(1)SU4 uses OpenJDK version 1.8.0.262. - Release 12.5(1)SU5 uses OpenJDK version 1.8.0.262. - Release 12.5(1)SU6 uses OpenJDK version 1.8.0.262. - Release 12.5(1)SU7 uses OpenJDK version 1.8.0.262. - Release 12.5(1)SU8 uses OpenJDK version 1.8.0.262.

Secure Connections

TLS 1.2 Support

- Unified Communications Manager and the IM and Presence Service support the use of TLS 1.2. For detailed information on TLS 1.2 support, see the TLS 1.2 Compatibility Matrix for Cisco Collaboration Products.

SSL Connections

- For Secure Sockets Layer (SSL) connections, this release supports both Cisco SSL and Cisco SSH:
- Cisco OpenSSL 1.0.2zf.6.2.511 and Cisco’s 1.0.2zf.6.2.511
- Cisco OpenSSH client version 7.5.14i.1.5.18 and Cisco’s 7.5.14i.1.5.18

Supported Ciphers for Unified Communications Manager

- The following ciphers are supported by Unified Communications Manager:

Table 12: Unified Communications Manager Cipher Support for TLS Ciphers

Application / Process	Protocol	Port	Supported Ciphers
Cisco Call Manager	TCP / TLS	2443	• ECDHE-RSA-AES256-GCM-SHA384: • ECDHE-RSA-AES256-SHA384: • AES256-GCM-SHA384: • AES256-SHA256: • AES256-SHA: • ECDHE-RSA-AES128-GCM-SHA256: • ECDHE-RSA-AES128-SHA256: • ECDHE-RSA-AES128-SHA: • AES128-GCM-SHA256: • AES128-SHA256:AES128-SHA: • ECDHE-RSA-AES256-SHA: **Note** The following ciphers are not supported from Release 14SU2 onwards: CAMELLIA128-SHA CAMELLIA256-SHA:
DRS	TCP / TLS	4040	• ECDHE-RSA-AES256-GCM-SHA384: ECDHE-RSA-AES256-SHA384: • AES256-GCM-SHA384:AES256-SHA256: AES256- • SHA:CAMELLIA256-SHA: ECDHE-RSA-AES128-GCM-SHA256: ECDHE-RSA-AES128-SHA256: • ECDHE-RSA-AES128-SHA: • AES128-GCM-SHA256:AES128-SHA256: AES128-SHA: • ECDHE-RSA-AES256-SHA: DHE-RSA-CAMELLIA256-SHA: • DHE-RSA-CAMELLIA128-SHA: CAMELLIA128-SHA

Application / Process	Protocol	Port	Supported Ciphers

Cisco Tomcat	TCP / TLS	8443 / 443	• ECDHE-RSA-AES256-GCM-SHA384: • ECDHE-RSA-AES256-SHA384: • DHE-RSA-AES256-GCM-SHA384: • DHE-RSA-AES256-SHA256: • DHE-RSA-AES256-SHA: • AES256-GCM-SHA384:AES256-SHA256: • AES256-SHA: • ECDHE-RSA-AES128-GCM-SHA256: • ECDHE-RSA-AES128-SHA256: • ECDHE-RSA-AES128-SHA: • DHE-RSA-AES128-GCM-SHA256: • DHE-RSA-AES128-SHA256: • DHE-RSA-AES128-SHA: • AES128-GCM-SHA256:AES128-SHA256: • AES128-SHA: • ECDHE-ECDSA-AES256-GCM-SHA384: • ECDHE-ECDSA-AES256-SHA384: • ECDHE-ECDSA-AES256-SHA: • ECDHE-ECDSA-AES128-GCM-SHA256: • ECDHE-ECDSA-AES128-SHA256: • ECDHE-ECDSA-AES128-SHA: • ECDHE-RSA-AES256-SHA: **Note** The following ciphers are not supported from Release 14SU2 onwards: • DHE-RSA-CAMELLIA256-SHA: CAMELLIA256-SHA: • DHE-RSA-CAMELLIA128-SHA: CAMELLIA128-SHA: • ECDHE-RSA-DES-CBC3-SHA: EDH-RSA-DES-CBC3-SHA: DES-CBC3-SHA: • ECDHE-ECDSA-DES-CBC3-SHA:

Cisco CallManager	TCP / TLS	5061	ECDHE-RSA-AES256-GCM-SHA384: • ECDHE-ECDSA-AES256-GCM-SHA384 ECDHE-RSA-AES256-SHA384: • ECDHE-ECDSA-AES256-SHA384: • AES256-GCM-SHA384:AES256-SHA256: • AES256-SHA: • ECDHE-ECDSA-AES128-GCM-SHA256: • ECDHE-RSA-AES128-GCM-SHA256: • ECDHE-RSA-AES128-SHA256 ECDHE-ECDSA-AES128-SHA256: • ECDHE-RSA-AES128-SHA ECDHE-ECDSA-AES128-SHA: • AES128-GCM-SHA256:AES128-SHA256: • AES128-SHA: • ECDHE-RSA-AES256-SHA: **Note** The following ciphers are not supported from Release 14SU2 onwards: • ECDHE-ECDSA-AES256-SHA: CAMELLIA256-SHA: CAMELLIA128-SHA: • ECDHE-ECDSA-DES-CBC3-SHA

Application / Process	Protocol	Port	Supported Ciphers
Cisco CTL Provider **Note** Cisco CTL Provider is not available from Release 14SU3 onwards.	TCP / TLS	2444	AES256-GCM-SHA384:AES256-SHA256: AES256-SHA:CAMELLIA256-SHA: AES128-GCM-SHA256:AES128-SHA256: AES128-SHA:CAMELLIA128-SHA:
Cisco Certificate Authority Proxy Function	TCP / TLS	3804	AES256-GCM-SHA384:AES256-SHA256: AES256-SHA: AES128-GCM-SHA256:AES128-SHA256: AES128-SHA:
			Note The following ciphers are not supported from Release 14SU2 onwards:
			CAMELLIA256-SHA: CAMELLIA128-SHA:
CTIManager	TCP / TLS	2749	• ECDHE-RSA-AES256-GCM-SHA384: • ECDHE-RSA-AES256-SHA384: • AES256-GCM-SHA384:AES256-SHA256: • AES256-SHA: • ECDHE-RSA-AES128-GCM-SHA256: • ECDHE-RSA-AES128-SHA256: • ECDHE-RSA-AES128-SHA: • AES128-GCM-SHA256:AES128-SHA256: • AES128-SHA: • ECDHE-RSA-AES256-SHA: **Note** The following ciphers are not supported from Release 14SU2 onwards: CAMELLIA256-SHA: CAMELLIA128-SHA
Cisco Trust Verification Service	TCP / TLS	2445	• AES256-GCM-SHA384:AES256-SHA256: AES256-SHA: • AES128-GCM-SHA256:AES128-SHA256: AES128-SHA:
			Note The following ciphers are not supported from Release 14SU2 onwards:
			CAMELLIA256-SHA: CAMELLIA128-SHA

Application / Process	Protocol	Port	Supported Ciphers
Cisco Intercluster Lookup Service	TCP / TLS	7501	• ECDHE-RSA-AES256-GCM-SHA384: ECDHE-RSA-AES256-SHA384: AES256-GCM-SHA384: • AES256-SHA256:AES256-SHA: ECDHE-RSA-AES128-GCM-SHA256: ECDHE-RSA-AES128-SHA256: ECDHE-RSA-AES128-SHA: • AES128-GCM-SHA256:AES128-SHA256: AES128-SHA: • ECDHE-RSA-AES256-SHA:
			Note The following ciphers are not supported from Release 14SU2 onwards:
			CAMELLIA256-SHA: CAMELLIA128-SHA:
Secure Configuration download (HAPROXY)	TCP / TLS	6971, 6972	• ECDHE-RSA-AES256-GCM-SHA384: ECDHE-RSA-AES256-SHA384: • AES256-GCM-SHA384:AES256-SHA256: AES256-SHA: • ECDHE-RSA-AES128-GCM-SHA256: ECDHE-RSA-AES128-SHA256: ECDHE-RSA-AES128-SHA: • AES128-GCM-SHA256:AES128-SHA256: AES128-SHA: • ECDHE-ECDSA-AES256-GCM-SHA384: ECDHE-ECDSA-AES256-SHA384: ECDHE-ECDSA-AES128-SHA256: ECDHE-ECDSA-AES128-SHA: • ECDHE-RSA-AES256-SHA:
			Note The following ciphers are not supported from Release 14SU2 onwards:
			• DHE-RSA-CAMELLIA256-SHA: CAMELLIA256-SHA: • DHE-RSA-CAMELLIA128-SHA: ECDHE-ECDSA-AES256-SHA: ECDHE-ECDSA-DES-CBC3-SHA: CAMELLIA128-SHA:

Application / Process	**Protocol**	**Port**	**Supported Ciphers**
Authenticated Contact Search	TCP / TLS	9443	ECDHE-RSA-AES256-GCM-SHA384: ECDHE-RSA-AES256-SHA384: - AES256-GCM-SHA384:AES256-SHA256: AES256-SHA: - ECDHE-RSA-AES128-GCM-SHA256: ECDHE-RSA-AES128-SHA256: ECDHE-RSA-AES128-SHA: - AES128-GCM-SHA256:AES128-SHA256: AES128-SHA: - ECDHE-ECDSA-AES256-GCM-SHA384: ECDHE-ECDSA-AES256-SHA384: ECDHE-ECDSA-AES128-SHA256: ECDHE-ECDSA-AES128-SHA: - ECDHE-RSA-AES256-SHA:
			Note The following ciphers are not supported from Release 14SU2 onwards:
			- DHE-RSA-CAMELLIA256-SHA: CAMELLIA256-SHA: - DHE-RSA-CAMELLIA128-SHA: CAMELLIA128-SHA: - ECDHE-ECDSA-AES256-SHA: ECDHE-ECDSA-DES-CBC3-SHA:

Supported Ciphers for SSH

The following ciphers are supported by SSH

Table 13: Cipher Support for SSH Ciphers

Service	**Ciphers/Algorithms**
SSH Server	- **Ciphers aes128-ctr aes192-ctr aes256-ctr** aes128-gcm@openssh.com aes256-gcm@openssh.com - **MAC algorithms: hmac-sha2-256 hmac-sha2-512 hmac-sha1** - **Kex algorithms:** ecdh-sha2-nistp521 ecdh-sha2-nistp384 ecdh-sha2-nistp256 diffie-hellman-group14-sha1 diffie-hellman-group14-sha256 diffie-hellman-group16-sha512

Service	Ciphers/Algorithms
SSH Client	- Ciphers: aes128-ctr aes192-ctr aes256-ctr aes128-gcm@openssh.com aes256-gcm@openssh.com - **MAC algorithms**: hmac-sha2-256 hmac-sha2-512 hmac-sha1 - **Kex algorithms**: ecdh-sha2-nistp521 ecdh-sha2-nistp384 ecdh-sha2-nistp256 diffie-hellman-group14-sha1 diffie-hellman-group14-sha256 diffie-hellman-group16-sha512
DRS Client	- **Ciphers**: aes256-ctr aes256-cbc aes128-ctr aes128-cbc aes192-ctr aes192-cbc - **MAC algorithms**: hmac-md5 hmac-sha2-256 hmac-sha1 hmac-sha1-96 hmac-md5-96 - **Keg algorithms:** ecdh-sha2-nistp256 ecdh-sha2-nistp384 ecdh-sha2-nistp521 diffie-hellman-group14-sha1 diffie-hellman-group-exchange-sha256 diffie-hellman-group-exchange-sha1 diffie-hellman-group1-sha1 **Note** The Key algorithms diffie-hellman-group-exchange-sha256, diffie-hellman-group-exchange-sha1, and diffie-hellman-group1-sha1 are not supported from Release 12.5(1)SU4 if you have configured Cipher Management functionality in your Unified CM server. If the ciphers are not configured, DRS Client uses these algorithms.

Service	Ciphers/Algorithms
SFTP client	- **Ciphers**: aes128-ctr aes192-ctr aes256-ctr - **MAC algorithms**: hmac-sha2-256 hmac-sha1 - Kex **algorithms**: ecdh-sha2-nistp521 ecdh-sha2-nistp384 diffie-hellman-group14-sha1 diffie-hellman-group1-sha1 diffie-hellman-group-exchange-sha256 diffie-hellman-group-exchange-sha1
End Users	hmac-sha512 SHA-256 – Hashing (salted)
DRS Backups / RTMT SFTPs	AES-128 – Encryption
Application Users	AES-256 – Encryption

Supported Platforms for Cisco Unified JTAPI and TAPI

Cisco Unified JTAPI

- For a detailed breakdown of supported Windows, Linux, and VMware platforms for Cisco Unified JTAPI, see

- https://developer.cisco.com/site/jtapi/documents/cisco-unified-jtapi-supported-jvm-versions/.
- For additional information that is related to Cisco Unified JTAPI, see Cisco Unified JTAPI Developers Guide for Cisco Unified Communications Manager.

Cisco Unified TAPI

- For a detailed breakdown of supported Windows platforms for Cisco Unified TAPI, see https://developer.cisco.com/site/tapi/documents/supported-windows-os/.
- For additional information that is related to Cisco Unified TAPI, see Cisco Unified TAPI Developers Guide for Cisco Unified Communications Manager.
- IM and Presence Service Compatibility Information

Platform Compatibility

- The IM and Presence Service shares a platform with Unified Communications Manager. Many of the compatibility topics for Unified Communications Manager double as support topics for the IM and Presence Service. You can refer to the Unified Communications Manager compatibility chapter for information on the following items
- Secure Connections
- Virtualization Requirements
- Supported Web Browsers

External Database Support

- Many IM and Presence Service features such as Persistent Chat, High Availability for Persistent Chat, Message Archiver, and Managed File Transfer require that you deploy an external database. For information on database support, see the Database Setup Guide for the IM and Presence
- Service.

Supported LDAP Directories 12.5(x)

The following LDAP directories are supported

- Microsoft Active Directory 2008 R1/ R2
- Microsoft Active Directory 2012 R1/ R2
- Microsoft Active Directory 2016
- Microsoft Active Directory 2019—Supported for 12.5(1)SU2 and later
- Microsoft Lightweight Directory Services 2008 R1/ R2
- Microsoft Lightweight Directory Services 2012 R1/ R2
- Microsoft Lightweight Directory Services 2019—Supported for 12.5(1)SU2 and later
- Oracle Directory Services Enterprise Edition 11gR1 (11.1.1.7.x or newer)
- Oracle Unified Directory 11gR2 (11.1.2.2.0 or 11.1.2.3.0)
- Open LDAP 2.4.45 or later
- Other LDAPv3 Compliant Directories—Unified Communications Manager uses standard LDAPv3 for

accessing the user's data. Ensure that the supported control attribute is configured in the LDAPv3 compliant directory servers to be used with DirSync.(The supported control attribute may return the pagecontrolsupport and persistent control support sub attributes, if configured.)

Federation Support

- SIP Federation/SIP Open Federation Support
- SIP Open Federation is supported as of 12.5(1)SU3.
- The following table lists supported SIP Controlled and SIP Open Federation integrations:

Table 14: Supported SIP Controlled and Open Federations

Third-Party Syste m	**Single Enterprise Network*** **(Intradomain or Interdomain Federation)**		**Business to Business** **(Interdomain Federation)**
	Direct Federation	**via Expressway**	**via Expressway**
Skype for Business 2015 (on-premise)	Y	Not supported	Y (Traffic Classification)
Office 365 (uses a cloud-hosted Skype for Business)	Not applicable	Not applicable	Y (Traffic Classification)

- The Single Enterprise Network can be partitioned intradomain federation or interdomain federation as the support values are the same for each. Business to Business integrations are always interdomain federation.

Supported XMPP Federations

- This release of IM and Presence Service supports XMPP Federation with the following systems:
- Cisco Weber Messenger
- IM and Presence Service Release 10.x and up
- Any other XMPP-compliant system

Intercluster Peering Support

- This release of the IM and Presence Service supports intercluster peering with the following IM and Presence Service releases:
- Note Intercluster peering is not supported if the IM and Presence Service version has gone EOL/EOS.
- Release 11.x
- Release 12.x

Calendar Integration with Microsoft Outlook

- The IM and Presence Service supports Microsoft Outlook Calendar Integration with either an on-premise

Exchange server or a hosted Office 365 server. See the table below for support information

Note For technical support on any third-party products, contact the respective organization.

Table 15: Support Information for Calendar Integration

Component	**Install Compatible Version**
Windows Server	• Service Packs for Windows Server 2012 (Standard) • Windows Server 2016 • Windows Server 2019—With 11.x releases, the minimum IM and Presence Service Release is 11.5(1)SU7. With 12.x releases, the minimum IM and Presence Service Release is 12.5(1)SU2.
Microsoft Exchange Server 2016	Microsoft Exchange 2016
Microsoft Exchange Server 2019	Microsoft Exchange 2019
Microsoft Office 365	See your Microsoft documentation for details on deploying a hosted Office 365 server. **Note** As of October 2020, Microsoft is changing the authentication mechanism that is supported by Exchange Online to use OAuth-based authentication only. After the change, if you want to deploy calendar integration between the IM and Presence Service and Office 365, you will need to upgrade the IM and Presence Service to Release 12.5(1)SU2. This change will not affect integration with an on-premises Exchange server.
Active Directory	• Active Directory 2012 with Windows Server 2012 • Active Directory 2016 with Windows Server 2016 **Note** User names configured in Active Directory must be identical to those names defined in Unified Communications Manager.
A Third-Party Certificate OR Certificate Server	One or the other of these are required to generate the certificates. **Note** Microsoft Exchange integration with IM and Presence Service supports certificates using RSA 1024 or 2048-bit keys and SHA1 and SHA256 signature algorithms.

Supported Ciphers for the IM and Presence Service

IM and Presence Service supports the following ciphers:

Table 16: Unified Communications Manager IM & Presence Cipher Support for TLS Ciphers

Application / Process	**Protocol**	**Port**	**Supported Ciphers**
Cisco SIP Proxy	TCP / TLS	5061	• ECDHE-RSA-AES256-GCM-SHA384: • ECDHE-ECDSA-AES256-GCM-SHA384: • ECDHE-RSA-AES256-SHA384: • ECDHE-ECDSA-AES256-SHA384: • AES256-GCM-SHA384:AES256-SHA256: • AES256-SHA: • ECDHE-RSA-AES128-GCM-SHA256: • ECDHE-ECDSA-AES128-GCM-SHA256: • ECDHE-RSA-AES128-SHA256: • ECDHE-ECDSA-AES128-SHA256: • ECDHE-RSA-AES128-SHA: • ECDHE-ECDSA-AES128-SHA: • AES128-GCM-SHA256: • AES128-SHA256: • AES128-SHA: • ECDHE-RSA-AES256-SHA: **Note** The following ciphers are not supported from Release 14SU2 onwards: • CAMELLIA256-SHA: CAMELLIA128-SHA: • DES-CBC3-SHA: • ECDHE-ECDSA-DES-CBC3-SHA: ECDHE-RSA-DES-CBC3-SHA: ECDHE-ECDSA-AES256-SHA:

Cisco SIP Proxy	TCP / TLS	5062	• ECDHE-RSA-AES256-GCM-SHA384: • ECDHE-ECDSA-AES256-GCM-SHA384: • ECDHE-RSA-AES256-SHA384: • ECDHE-ECDSA-AES256-SHA384: • AES256-GCM-SHA384: • AES256-SHA256:AES256-SHA: • ECDHE-RSA-AES128-GCM-SHA256: • ECDHE-ECDSA-AES128-GCM-SHA256: • ECDHE-RSA-AES128-SHA256: • ECDHE-ECDSA-AES128-SHA256: • ECDHE-RSA-AES128-SHA: • ECDHE-ECDSA-AES128-SHA: • AES128-GCM-SHA256:AES128-SHA256: • AES128-SHA: • ECDHE-RSA-AES256-SHA: • **Note** The following ciphers are not supported from Release 14SU2 onwards: • CAMELLIA256-SHA: CAMELLIA128-SHA: • DES-CBC3-SHA: • ECDHE-ECDSA-DES-CBC3-SHA: ECDHE-RSA-DES-CBC3-SHA: ECDHE-ECDSA-AES256-SHA:

Application / Process	**Protocol**	**Port**	**Supported Ciphers**

Cisco SIP Proxy	TCP / TLS	8083	• ECDHE-RSA-AES256-GCM-SHA384: • ECDHE-ECDSA-AES256-GCM-SHA384: • ECDHE-RSA-AES256-SHA384: • ECDHE-ECDSA-AES256-SHA384: • AES256-GCM-SHA384:AES256-SHA256: • AES256-SHA: • ECDHE-RSA-AES128-GCM-SHA256: • ECDHE-ECDSA-AES128-GCM-SHA256: • ECDHE-RSA-AES128-SHA256: • ECDHE-ECDSA-AES128-SHA256: • ECDHE-RSA-AES128-SHA: • ECDHE-ECDSA-AES128-SHA: • AES128-GCM-SHA256:AES128-SHA256: • AES128-SHA: • ECDHE-RSA-AES256-SHA: **Note** The following ciphers are not supported from Release 14SU2 onwards: • CAMELLIA256-SHA: CAMELLIA128-SHA: • DES-CBC3-SHA: • ECDHE-ECDSA-DES-CBC3-SHA: ECDHE-RSA-DES-CBC3-SHA: • ECDHE-ECDSA-AES256-SHA:

Cisco Tomcat	TCP / TLS	8443, 443	- ECDHE-RSA-AES256-GCM-SHA384: - ECDHE-RSA-AES256-SHA384: - DHE-RSA-AES256-GCM-SHA384: - DHE-RSA-AES256-SHA256: - DHE-RSA-AES256-SHA: - AES256-GCM-SHA384:AES256-SHA256: - AES256-SHA: - ECDHE-RSA-AES128-GCM-SHA256: - ECDHE-RSA-AES128-SHA256: - ECDHE-RSA-AES128-SHA: - DHE-RSA-AES128-GCM-SHA256: - DHE-RSA-AES128-SHA256: - DHE-RSA-AES128-SHA: - AES128-GCM-SHA256: - AES128-SHA256:AES128-SHA: - EDH-RSA-DES-CBC3-SHA: - ECDHE-ECDSA-AES256-GCM-SHA384: - ECDHE-ECDSA-AES256-SHA384: - ECDHE-ECDSA-AES128-GCM-SHA256: - ECDHE-ECDSA-AES128-SHA256: - ECDHE-ECDSA-AES128-SHA: - ECDHE-RSA-AES256-SHA: **Note** The following ciphers are not supported from Release 14SU2 onwards: - CAMELLIA128-SHA: CAMELLIA256-SHA: DES-CBC3-SHA: - ECDHE-ECDSA-DES-CBC3-SHA: ECDHE-RSA-DES-CBC3-SHA: - DHE-RSA-CAMELLIA128-SHA: DHE-RSA-CAMELLIA256-SHA: - ECDHE-ECDSA-AES256-SHA:

Application / Process	**Protocol**	**Port**	**Supported Ciphers**

Cisco XCP XMPP Federation Connection Manager	TCP /TLS	5269	• ECDHE-RSA-AES256-GCM-SHA384: ECDHE-ECDSA-AES256- • GCM-SHA384: ECDHE-RSA-AES256-SHA384: • ECDHE-ECDSA-AES256-SHA384: AES256-GCM-SHA384:AES256-SHA256: AES256-SHA: • ECDHE-RSA-AES128-GCM-SHA256: ECDHE-ECDSA-AES128- • GCM-SHA256: ECDHE-RSA-AES128-SHA256: • ECDHE-ECDSA-AES128-SHA256: ECDHE-RSA-AES128-SHA: • ECDHE-ECDSA-AES128-SHA: • AES128-GCM-SHA256:AES128-SHA256: AES128-SHA:
			Note The following ciphers are not supported from Release 14SU2 onwards:
			• CAMELLIA256-SHA: CAMELLIA128-SHA: • DES-CBC3-SHA: • ECDHE-ECDSA-DES-CBC3-SHA: ECDHE-RSA-DES-CBC3-SHA: • ECDHE-ECDSA-AES256-SHA: ECDHE-RSA-AES256-SHA:
Cisco XCP Client Connection Manager	TCP / TLS	5222	• ECDHE-RSA-AES256-GCM-SHA384: ECDHE-ECDSA-AES256-GCM-SHA384: ECDHE-RSA-AES256-SHA384: • ECDHE-ECDSA-AES256-SHA384: AES256-GCM-SHA384:AES256-SHA256: AES256-SHA: • ECDHE-RSA-AES128-GCM-SHA256: ECDHE-ECDSA-AES128-GCM-SHA256: ECDHE-RSA-AES128-SHA256: • ECDHE-ECDSA-AES128-SHA256: ECDHE-RSA-AES128-SHA: • ECDHE-ECDSA-AES128-SHA: • AES128-GCM-SHA256:AES128-SHA256: AES128-SHA:
			Note The following ciphers are not supported from Release 14SU2 onwards:

			• CAMELLIA128-SHA: CAMELLIA256-SHA: • DES-CBC3-SHA: • ECDHE-ECDSA-DES-CBC3-SHA: ECDHE-RSA-DES-CBC3-SHA: • ECDHE-ECDSA-AES256-SHA: ECDHE-RSA-AES256-SHA:

Remote Call Control with Microsoft Lync

Microsoft Remote Call Control (RCC) allows enterprise users to control their Cisco Unified IP Phone or Cisco IP Communicator Phone through Microsoft Lync, a third-party desktop instant-messaging (IM) application. When a user signs in to the Microsoft Lync client, the Lync server sends instructions, through the IM and Presence Service node, to the Cisco Unified Communications Manager to set up, tear down and maintain calling features based on a user's action at the Lync client.

Note

- SIP federation and Remote Call Control (RCC) do not work together on the same IM and Presence Service cluster. This is because for SIP federation a user cannot be licensed for both Cisco IM and Presence Service and Microsoft Lync/OCS, but for RCC a user must be licensed for Cisco IM and Presence Service and Microsoft Lync/OCS at the same time.

Note

- An IM and Presence Service cluster that is used for RCC does not support Jabber or other IM and Presence Service functionality.

Software Requirements
The following software is required for integrating IM and Presence Service with Microsoft Lync Server:

- IM and Presence Service, current release
- IM and Presence Service Lync Remote Call Control Plug-in
- Cisco Unified Communications Manager, current release
- Microsoft Lync Server 2013 Release 4.x, Standard Edition or Enterprise Edition
- Lync Server Control Panel
- Lync Server Deployment Wizard
- Lync Server Logging Tool
- Lync Server Management Shell
- Lync Server Topology Builder
- Microsoft 2013 Lync Client
- (Optional) Upgraded Skype for Business 2015 Client

Note

The Skype for Business 2015 client must have been upgraded from a Lync 2013 client and must be registered to a Lync 2013 server.

- (Optional) Cisco CSS 11500 Content Services Switch
- Microsoft Domain Controller
- Microsoft Active Directory
- DNS
- Certificate Authority

Configuration

For additional details, including configuration information, see Remote Call Control with Microsoft Lync Server for the IM and Presence Service at **https://www.cisco.com/c/en/us/support/unified-communications/unified-presence/**
products-installation-and-configuration-guides-list.html.

- Americas Headquarters Cisco Systems, Inc. San Jose, CA 95134-1706 USA
- Asia Pacific Headquarters Cisco Systems(USA)Pte. Ltd. Singapore
- Europe Headquarters Cisco Systems International Iava Amsterdam, The Netherlands
- 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**.

Documents / Resources

 Compatibility Matrix for Cisco Unified Communications Manager and the IM and Presence Service, Release 12.5(X) Compatibility Matrix for Cisco Unified Communications Manager and the IM and Presence Service 2 Revision History 2 Purpose of this Document 3 Supported Upgrade and Migration Paths 4 Supported Versions 6 Unified Communications Manager Compatibility Information 8 IM and Presence Service Compatibility Information 25	**CISCO 800 Series Unified Communications Manager IM Presence Service** [pdf] User Guide 800 Series Unified Communications Manager IM Presence Service, 800 Series, Unified Communications Manager IM Presence Service, Communications Manager IM Presence Service, Manager IM Presence Service, Presence Service, Service

References

- **User Manual**