Revised: March 28, 2024

Compatibility Matrix for Cisco Unified Communications Manager and the IM and Presence Service, Release 15x

Compatibility Matrix for Cisco Unified Communications Manager and the IM and Presence Service

Revision History

Date	Revision
March 28, 2024	Added version support for 15SU1.
March 28, 2024	Updated API and Secure Connection Packages information for 15SU1.
December 18, 2023	Added version support for 15.
December 18, 2023	Updated LDAP Directory support information.
December 18, 2023	Updated Supported browser section.
December 18, 2023	Removed support for Active Directory 2012 with Windows Server 2012 from the "Calendar Integration with Microsoft Outlook" section.
December 18, 2023	Removed support for "Remote Call Control with Microsoft Lync Server" for IM and Presence Service as Microsoft Lync Server 2013 is past Microsoft's Mainstream End of Support (EOS) dated April 10, 2018 and also extended EOS dated April 11, 2023.

Purpose of this Document

This document contains compatibility information for 15x releases of Cisco Unified Communications Manager (Unified Communications Manager) and Cisco Unified Communications Manager IM and Presence Service (IM and Presence Service). This will include subsequent SU releases as well, unless indicated otherwise.

Supported Upgrade and Migration Paths with COP Files

The following table highlights supported upgrade paths to upgrade to Release 15 and later of Cisco Unified Communications Manager and the IM and Presence Service. It also 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 Admin interface, or before you begin an upgrade or migration using the Cisco

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.

Note Unless indicated otherwise, each release category includes the SU releases within that category.

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 Although it is not mandatory, we strongly recommend that you run the Upgrade Readiness COP file prior to the upgrade to maximize the upgrade success. Cisco TAC may require that you run this COP file to provide effective technical support.

Note If the source is in FIPS mode and/or PCD in FIPS mode, see https://www.cisco.com/web/software/286319173/139477/ciscocm.ciscossl7_upgrade_CSCwa48315_CSCwa77974_v1.0.k4.cop-ReadMe.pdf for information on the COP file `ciscocm.ciscossl7_upgrade_CSCwa48315_CSCwa77974_v1.0.k4.cop`. This document details the pre-requisites required for direct upgrade or direct migration to the 15 destination versions.

Note If a direct standard upgrade to Release 15 or later is available from your source release, you can choose either a single-node or the clusterwide upgrade.

If you want to upgrade an entire cluster and expect least duration, downtime, service impact, or administration intervention, use the "Clusterwide Upgrade Task Flow (Direct Standard)" procedure that details Cluster Upgrade via Unified CM publisher using Unified OS Admin upgrade or CLI upgrade. Here, you will upgrade only the Unified CM publisher, and it orchestrates the upgrade or reboot of all other nodes in the cluster.

If you are planning to upgrade your source node-by-node or using a single-node only using the local Unified OS Admin upgrade or CLI upgrade, see the "Upgrade Cluster Nodes (Direct Standard)" section. For more information, see the Upgrade and Migration Guide for Cisco Unified Communications Manager and the IM and Presence Service.

Note You must ensure that your upgrade plan follows the node sequencing rules as mentioned in the Upgrade guide. Before you switch versions on the IM and Presence Service nodes, you must first switch the Unified Communications Manager nodes, starting with the publisher node and then the subscriber nodes.

If you do not follow the mentioned sequence, and then if the Unified Communications Manager Publisher node is switched to version 15 or later, and the IM and Presence Service Publisher node version is still in the 12.5.x or 14 and SUs versions and is not upgraded, the following pages in the Software Upgrades menu will not display or work for the IM and Presence Service nodes:

- Restart/Switch-Version Cluster
- Cluster Software Location
- Software Installation and Upgrade Cluster

Note There are no Direct Refresh Upgrade supported paths for Unified Communications Manager and the IM and Presence Service Release 15 and later versions. Refresh Upgrades from Pre-12.5.x source to Release 15 and later isn't supported.

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

Source	Destination	Mechanism	Pre-requisites	Version Switching* (Source to Destination and Vice Versa)
10.0	15	PCD 15 Migration Task (V2V)	Direct upgrade to 15 isn't supported. When the destination version is 15 and the source version is 10.0, then the Cisco Prime Collaboration Deployment (PCD) must be used for migration. If the destination version is 15 and the source version 10.0 is in FIPS mode, then the Cisco Prime Collaboration Deployment (PCD) must be in (or placed in) non-FIPS mode.	Not applicable
10.5	15	PCD 15 Migration Task (V2V)	Run pre-upgrade-check COP file. You must install the `ciscocm.CSCwi52160_15-direct-migration_v1.0.k4.cop.sha512` COP file before migration. Direct upgrade to 15 is not supported. When the destination version is 15 and the source version is 10.5, then the Cisco Prime Collaboration Deployment (PCD) must be used for migration. If the destination version is 15 and the source version 10.5 is in FIPS mode, then either: • PCD must be in (or placed in) non-FIPS mode. • Use Fresh Install with Data Import instead of using the PCD Migration Task.	Not applicable
		Fresh Install with Data Import (V2V)	• Run pre-upgrade-check COP file. • `ciscocm.CSCwi52160_15-direct-migration_v1.0.k4.cop.sha512` • `ciscocm.DataExport_v1.0.cop.sgn`	Not supported

Source	Destination	Mechanism	Pre-requisites	Version Switching* (Source to Destination and Vice Versa)
11.0	15	PCD 15 Migration Task (V2V)	Run pre-upgrade-check COP file. You must install the `ciscocm.CSCwi52160_15-direct-migration_v1.0.k4.cop.sha512` COP file before migration. If the destination version is 15 and the source version 11.0 is in FIPS mode, then either: • PCD must be in (or placed in) non-FIPS mode. • Use Fresh Install with Data Import instead of using the PCD Migration Task.	Not supported
		Fresh Install with Data Import (V2V)	• Run pre-upgrade-check COP file. • `ciscocm.CSCwi52160_15-direct-migration_v1.0.k4.cop.sha512` • `ciscocm.DataExport_v1.0.cop.sgn`	Not supported
11.5	15	PCD 15 Migration Task (V2V)	Run pre-upgrade-check COP file. You must install the `ciscocm.CSCwi52160_15-direct-migration_v1.0.k4.cop.sha512` COP file before migration. If the destination version is 15 and the source version 11.5 is in FIPS mode, then either: • PCD must be in (or placed in) non-FIPS mode. • Use Fresh Install with Data Import instead of using the PCD Migration Task.	Not supported
		Fresh Install with Data Import (V2V)	• Run pre-upgrade-check COP file. • `ciscocm.CSCwi52160_15-direct-migration_v1.0.k4.cop.sha512` • `ciscocm.DataExport_v1.0.cop.sgn`	Not supported

Source	Destination	Mechanism	Pre-requisites	Version Switching* (Source to Destination and Vice Versa)
12.0	15	PCD 15 Migration Task (V2V)	Run pre-upgrade-check COP file. You must install the `ciscocm.CSCwi52160_15-direct-migration_v1.0.k4.cop.sha512` COP file before migration. If the source version is Release 12.0(1) of Unified Communications Manager (12.0.1.10000-10), then you must install the following COP file: `ciscocm-slm-migration.k3.cop.sgn`. This is not required if the source version is higher, for example, Release 12.0(1)SU1.	Not supported
		Fresh Install with Data Import (V2V)	• Run pre-upgrade-check COP file. • `ciscocm.CSCwi52160_15-direct-migration_v1.0.k4.cop.sha512` • `ciscocm.DataExport_v1.0.cop.sgn`	Not supported

Source	Destination	Mechanism		Pre-requisites	Version Switching* (Source to Destination and Vice Versa)
12.5	15	Direct Standard Upgrade (simple upgrades)	Via OS Admin or CLI	• Run pre-upgrade-check COP file.	Supported

		Direct Standard Upgrade	Via PCD 15 Upgrade Task	• Run pre-upgrade-check COP file.
				• If the Unified CM source is older than 12.5.1.14900-63, then install the following COP file: `ciscocm.enable-sha512sum-2021-signing-key-v1.0.cop.sgn`.
				• If the IM and Presence Service source is older than 12.5.1.14900-4, then install the following COP file: `ciscocm.enable-sha512sum-2021-signing-key-v1.0.cop.sgn`.
				• If the destination version is 15 and the source version 12.5 is in FIPS mode, then either:
				  • PCD must be in (or placed in) non-FIPS mode.
				  • Use Fresh Install with Data Import instead of using the PCD Upgrade Task.
				• If you're using Cisco Prime Collaboration Deployment to upgrade an IM and Presence Service cluster from Release 12.5.x to Release 15, you must install the following COP file on the Release 12.5.x systems before you begin the upgrade: `ciscocm.imp15_upgrade_v1.0.k4.cop.sha512`.
				Note that the COP file is applicable only if:
				  • Unified Communications Manager destination version is in Release 15.
				  • Unified Communications Manager destination version is in Release 15 and you are trying to upgrade your IM and Presence Service source from a restricted version to an unrestricted version.
					Supported

		PCD 15 Migration Task (V2V)			Not supported

Source	Destination	Mechanism	Pre-requisites	Version Switching* (Source to Destination and Vice Versa)
			Run pre-upgrade-check COP file. You must install the `ciscocm.CSCwi52160_15-direct-migration_v1.0.k4.cop.sha512` COP file before migration. If the destination version is 15 and the source version 12.5 is in FIPS mode, then either: • PCD must be in (or placed in) non-FIPS mode. • Use Fresh Install with Data Import instead of using the PCD Migration Task.	
		Fresh Install with Data Import (V2V)	• Run pre-upgrade-check COP file. • `ciscocm.CSCwi52160_15-direct-migration_v1.0.k4.cop.sha512` • `ciscocm.DataExport_v1.0.cop.sgn`	Not supported

Source	Destination	Mechanism		Pre-requisites	Version Switching* (Source to Destination and Vice Versa)
14 and SUs	15	Direct Standard Upgrade (simple upgrades)	Via OS Admin or CLI	Run pre-upgrade-check COP file.	Supported

		Direct Standard Upgrade	Via PCD Upgrade Task	Run pre-upgrade-check COP file.
				• If the destination version is 15 and the source version is 14 and SUs in FIPS mode, then either:
				  • PCD must be in (or placed in) non-FIPS mode.
				  • Use Fresh Install with Data Import instead of using the PCD Upgrade Task.
				• If you're using Cisco Prime Collaboration Deployment to upgrade an IM and Presence Service cluster from Release 14 or SUs to Release 15, you must install the following COP file on the Release 14 or SU systems before you begin the upgrade: `ciscocm.imp15_upgrade_v1.0.k4.cop.sha512`. Note that the COP file is applicable only if:
				  • Unified Communications Manager destination version is in Release 15 and the IM and Presence Service source nodes are in 14 or 14SU1 versions.
				  • Unified Communications Manager destination version is in Release 15 and you are trying to upgrade your IM and Presence Service source from a restricted version to an unrestricted version.
					Supported

		PCD 15 Migration Task (V2V)		Run pre-upgrade-check COP file. You must install the `ciscocm.CSCwi52160_15-direct-migration_v1.0.k4.cop.sha512` COP file before migration. If the destination version is 15 and the source version is 14 or SUs in FIPS mode, then either: • PCD must be in (or placed in) non-FIPS mode. • Use Fresh Install with Data Import instead of using the PCD Migration Task.	Not supported

Source	Destination	Mechanism	Pre-requisites	Version Switching* (Source to Destination and Vice Versa)
		Fresh Install with Data Import (V2V)	• Run pre-upgrade-check COP file. • ciscocm.CSCwi52160_15-direct-migration_v1.0.k4.cop.sha512 • ciscocm.CSCwi52160_15-direct-migration_v1.0.k4.cop.sha512 • ciscocm.DataExport_v1.0.cop.sgn	Not supported

* 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.

Note PCD Upgrades and Migrations—For all the supported paths using the PCD Upgrade Task or PCD Migration Task in the above table, you must use PCD Release 15.

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...
15	• Cisco Unified Communications Manager 15.0.1.10000-32 • IM and Presence Service 15.0.1.10000-10
15SU1	• Cisco Unified Communications Manager 15.0.1.11900-23 • IM and Presence Service 15.0.1.11900-4

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 15.0.1.13[0-2]xx would be considered part of the 15 (15.0.1.10900-x) release.

Table 2: 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

This release of Cisco Unified Communications Manager and the IM and Presence Service is a part of the Cisco Collaboration Systems Release 15 and is compatible with the other Cisco Collaboration applications and versions in Cisco Collaboration Systems Release 15.

For a full list of Cisco Collaboration applications that are a part of Cisco Collaboration Systems Release 15, 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/Compatibility/CSR-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 3: 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 **xConfiguration 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:

```
xConfiguration XCP Config FcmService: On/Off
```

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

Table 4: 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.
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

Mixed Versions IM and Presence Clusters	Expected Status of FCM Flag on Expressway X12.7	Comment
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 Cisco will not issue bug fixes or security enhancements for endpoints that have reached End of Software Maintenance or End of Support status, regardless of whether those endpoints are deprecated or not deprecated. Cisco will not test Unified Communications Manager with End of Life phones. Nor will we fix Unified Communications Manager bugs that are related to End of Life phones unless the issue can be replicated on a phone that is not End of Life.

Table 5: 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
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

Device Series	Device Model
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
Cisco IP Communicator	Cisco IP Communicator—EOS Notice

Device Series	Device Model
Webex	Webex App Webex Room Phone Webex Desk Cisco Desk Camera 4K Cisco Desk Camera 1080p 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 TelePresence IX5000	Cisco TelePresence IX5000

Device Series	Device Model
Cisco TelePresence EX Series	Cisco TelePresence System EX90—EOS Notice
Cisco TelePresence MX Series	Cisco TelePresence MX200 G2—EOS Notice Cisco TelePresence MX300 G2—EOS Notice Cisco TelePresence MX700D—EOS Notice Cisco TelePresence MX800S—EOS Notice Cisco TelePresence MX800D—EOS Notice
Cisco TelePresence SX Series	Cisco TelePresence SX10—EOS Notice Cisco TelePresence SX20—EOS Notice Cisco TelePresence SX80—EOS Notice

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/Compatibility/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 6: 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 TelePresence EX60 • Cisco TelePresence MX200-G1, MX200-G2, MX300-G1, MX300-G2 • Cisco TelePresence 500-32, 500-37, 1000 MXP, 1100, 1300-65, 1300-47, 3000 Series • Cisco ATA 190 Series Analog Telephone Adapters

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 7: Deprecated Phone Models for this Release

Deprecated Phone Models for this Release	First Deprecated as of Unified CM...
No additional endpoints deprecated	Release 15
No additional endpoints deprecated	Release 14
• 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

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 8: 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

The following LDAP directories are supported:

- Microsoft Active Directory on Windows Server 2016
- Microsoft Active Directory on Windows Server 2019—Supported for 15 and later releases
- Microsoft Active Directory on Windows Server 2022—Supported for 15 and later releases
- Microsoft Lightweight Directory Services 2019 and 2022—Supported for 15 and later releases
- Oracle Unified Directory 12cPS4
- OpenLDAP Long Term Support (LTS) Release 2.5.16
- Other LDAPv3 Compliant Directories—Unified Communications Manager uses standard LDAPv3 for accessing the user's data. Ensure that the supportedcontrol attribute is configured in the LDAPv3 compliant directory servers to be used with DirSync. (The supportedcontrol attribute may return the `pagecontrolsupport` and `persistentcontrolsupport` sub attributes, if configured.)

Supported Web Browsers

The following web browsers are supported:

- Firefox, Chrome, and Microsoft Edge browser with Windows 10 and 11 (64 bit)
- Safari, Chrome, and Firefox on MacOS Ventura 13.4.1

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 9: 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 IdPs have been tested with Cisco Collaboration solutions:

- Microsoft® Active Directory® Federation Services 2.0
- Microsoft Azure AD
- Okta
- OpenAM
- PingFederate®
- F5 BIG-IP

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

API and Secure Connection Packages

The following table provides information on the API Development and secure connection packages that are supported with this release.

Table 10: Supported Packages

Package Type	Details
API Development	Release 15 and 15SU1 of Cisco Unified Communications Manager and the IM and Presence Service support OpenJDK version 1.8.0.362 for application development.
TLS Connections	For Transport Layer Security (TLS) connections, this release support CiscoSSL 1.1.1t.7.2.500.
SSH Clients	Release 15 and 15SU1 supports CiscoSSH 1.10.32 which is based on OpenSSH_8.8p1.

Note For additional information on the packages that are installed on your system, run the `show packages active` CLI command. See the *Command Line Interface Reference Guide for Cisco Unified Communications Solutions* for more information about this command and its options.

Supported Ciphers for Unified Communications Manager

The following ciphers are supported by Unified Communications Manager:

Table 11: Unified Communications Manager Cipher Support for TLS Ciphers

Application / Process	Protocol	Port	Supported Ciphers

Cisco CallManager	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:`

Application / Process	Protocol	Port	Supported Ciphers
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
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:

Application / Process	Protocol	Port	Supported Ciphers
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
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:

Application / Process	Protocol	Port	Supported Ciphers
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
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:

Application / Process	Protocol	Port	Supported Ciphers
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:
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 12: 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`
	• Host Key algorithms in non-FIPS mode:
	`rsa-sha2-256`
	`rsa-sha2-512`
	`ssh-rsa`
	• Host Key algorithms in FIPS mode:
	`rsa-sha2-256`
	`rsa-sha2-512`

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`
	• Host Key algorithms in non-FIPS mode:
	`rsa-sha2-256`
	`rsa-sha2-512`
	`ssh-rsa`
	• Host Key algorithms in FIPS mode:
	`rsa-sha2-256`
	`rsa-sha2-512`

Service	Ciphers/Algorithms

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`
	• Kex 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 Kex 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.

SFTP client	• Ciphers:
	`aes128-ctr`
	`aes192-ctr`
	`aes256-ctr`
	• MAC algorithms:
	`hmac-sha2-256`
	`hmac-sha2-512`
	`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`
DRS Backups / RTMT SFTPs	`AES-128 - Encryption`
Application Users	`AES-256 - Encryption`

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

The following LDAP directories are supported:

- Microsoft Active Directory on Windows Server 2016
- Microsoft Active Directory on Windows Server 2019—Supported for 15 and later releases
- Microsoft Active Directory on Windows Server 2022—Supported for 15 and later releases
- Microsoft Lightweight Directory Services 2019 and 2022—Supported for 15 and later releases
- Oracle Unified Directory 12cPS4
- OpenLDAP Long Term Support (LTS) Release 2.5.16
- Other LDAPv3 Compliant Directories—Unified Communications Manager uses standard LDAPv3 for accessing the user's data. Ensure that the supportedcontrol attribute is configured in the LDAPv3 compliant directory servers to be used with DirSync. (The supportedcontrol attribute may return the `pagecontrolsupport` and `persistentcontrolsupport` 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 13: Supported SIP Controlled and Open Federations

Third-Party System	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 Webex 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 11.5
- Release 12.x
- Release 14 and SUs
- Release 15 and SUs

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:

Table 14: Support Information for Calendar Integration

Component	Install Compatible Version
Windows Server	• 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 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 is 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 15: 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: 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: EDH-RSA-DES-CBC3-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: