Compatibility Matrix for Cisco Unified Communications Manager and the IM and Presence Service, Releases 11.5(1)SU5—SU11

Revised: April 7, 2022

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

Revision History

Date	Revision
Sept. 19, 2018	Added LDAP directory support for the IM and Presence Service
Dec. 19, 2019	Initial doc version for release 11.5(1)SU7
May. 21, 2020	Initial doc version for release 11.5(1)SU8
Dec 15, 2020	Initial doc version for release 11.5(1)SU9
Dec 15, 2020	Updated version support for 11.5(1)SU9
Dec 15, 2020	Renamed Cisco Webex Teams to Webex App
June 07, 2021	Initial doc version for release 11.5(1)SU10
June 07, 2021	Updated version support for 11.5(1)SU10
Dec 01, 2021	Updated supported ciphers/algorithms for DRS Client in Table 12
April 07, 2022	Initial doc version for release 11.5(1)SU11
April 07, 2022	Updated version support for 11.5(1)SU11
April 07, 2022	Added support for Webex Desk Hub and Webex Wireless Phone 800 Series

Software Versions

The following table highlights the full software versions supported for Cisco Unified Communications Manager and the IM and Presence Service with these releases:

Release	Full Version Number
Release 11.5(1)SU5	• Cisco Unified Communications Manager 11.5.1.15900-18 • IM and Presence Service 11.5.1.1.15900-33
Release 11.5(1)SU6	• Cisco Unified Communications Manager 11.5.1.16900-16 • IM and Presence Service 11.5.1.16910-12

Release	Full Version Number
Release 11.5(1)SU7	• Cisco Unified Communications Manager 11.5.1.17900-52 • IM and Presence Service 11.5.1.17900-8
Release 11.5(1)SU8	• Cisco Unified Communications Manager 11.5.1.18900-97 • IM and Presence Service 11.5.1.18900-15
Release 11.5(1)SU9	• Cisco Unified Communications Manager 11.5.1.21900-40 • IM and Presence Service 11.5.1.21900-5
Release 11.5(1)SU10	• Cisco Unified Communications Manager 11.5.1.22900-28 • IM and Presence Service 11.5.1.22900-6
Release 11.5(1)SU11	• Cisco Unified Communications Manager 11.5.1.23900-30 • IM and Presence Service 11.5.1.23900-3

Version Compatibility Between Unified CM and the IM and Presence Service

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

Table 1: Version Compatibility between Unified Communications Manager and the IM and Presence Service

Deployment Type	Release Mismatch	Description
Standard Deployment of IM and Presence	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	Supported	The IM and Presence deployment and the telephony deployment are in different clusters and can run different releases—a release mismatch is supported. **Note** The IM and Presence 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. **Note** Centralized Deployment is supported for the IM and Presence Service from Release 11.5(1)SU4 onward.

Upgrade Paths

This release of Cisco Unified Communications Manager and the IM and Presence Service supports virtualized deployments only. However, your pre-upgraded system may or may not be running on a virtualized machine and the upgrade paths differ depending on

the pre-upgrade deployment type. The upgrade paths are different for both pre-upgrade states. Choose the upgrade path that applies, depending on the pre-upgrade deployment type:

- Pre-upgrade deployment is running on Cisco Media Convergence Server 7800 Series Hardware
- Pre-upgrade deployment is running on a virtualized machine

Pre-upgrade Deployment is Running on Cisco Media Convergence Server Hardware

You cannot run Release 11.5(x) of Cisco Unified Communications Manager and the IM and Presence Service on server hardware directly; you must run these applications on virtual machines. The tables below list the supported migration paths for deployments where the pre-upgrade version is running on Cisco 7800 Series Media Convergence Server (MCS 7800) hardware. You must migrate to a system that is running on a virtual machine. All of the supported migration paths listed below are physical-to-virtual (P2V) migrations. Also note that "11.5(x)" includes 11.5(1) and subsequent SU releases.

Note The tables below list the upgrade paths supported for MCS 7800 Series servers, with the following exceptions:

- MCS 7816-C1 for Business Edition 3000 (BE3000)
- MCS 7828 for Business Edition 5000 (BE5000)

PCD migrations are not supported for BE3000 and BE5000 deployments. We recommend a fresh installation for upgrades from these products.

Table 2: Upgrade Paths when Pre-Upgrade Version is Running on Cisco MCS 7800 Series Hardware

From	To	Supported Methods
Unified Communications Manager Upgrades		
Unified CM (on MCS 7800 Series HW) 6.1(5), 7.1(3), 7.1(5), 8.x, 9.x	11.5(x)	PCD Migration
IM and Presence Service Upgrades		
Cisco Unified Presence (on MCS 7800 Series HW) 8.5(4), 8.6(3), 8.6(4), 8.6(5)	IM and Presence Service 11.5(x)	PCD Migration
IM and Presence Service (on MCS 7800 Series HW) 9.0(x), 9.1(x)	11.5(x)	PCD Migration

Pre-upgrade Deployment is Running on a Virtual Machine

The table below lists the supported upgrade and migration paths where the pre-upgrade version is running on a virtual machine. All of the supported upgrade and migration paths listed below are virtual-to-virtual (V2V). Service Updates (SU) within each path are supported, unless otherwise indicated. Also note that "11.5(x)" includes 11.5(1) and subsequent SU releases.

Table 3: Upgrade Paths when Pre-upgrade Version is Running on Virtual Machine

From	To	Supported Methods
Unified Communications Manager Upgrades		
Unified CM 8.6(x)	11.5(x)	Cisco Unified OS Admin (Direct Refresh) PCD Migration PCD Upgrade (Direct Refresh)
Unified CM 9.0(x)	11.5(x)	PCD Migration PCD Upgrade (Direct Refresh)
Unified CM 9.1(x)	11.5(x)	Cisco Unified OS Admin (Direct Refresh) PCD Migration PCD Migration (Direct Refresh)
Unified CM 10.0(x)	11.5(x)	PCD Migration PCD Upgrade (Direct Standard)
Unified CM 10.5(x), 11.0(x), 11.5(x)	11.5(x)	Cisco Unified OC Admin (Direct Standard) PCD Migration PCD Migration (Direct Standard)
IM and Presence Service Upgrades		
Cisco Unified Presence 8.5(4)	IM and Presence 11.5(x)	PCD Migration
Cisco Unified Presence 8.6(3), 8.6(4), 8.6(5)	IM and Presence 11.5(x)	PCD Migration PCD Upgrade (Direct Refresh)
Cisco Unified Presence 8.6(x)	IM and Presence 11.5(x)	Cisco Unified OS Admin
IM and Presence 9.0(x)	11.5(x)	PCD Migration PCD Upgrade (Direct Refresh)
IM and Presence 9.1(x)	11.5(x)	PCD Migration PCD Upgrade (Direct Standard) Cisco Unified OS Admin (Direct Refresh)
IM and Presence 10.0(x), 10.5(x), 11.0(x), 11.5(x)	11.5(x)	PCD Migration PCD Upgrade (Direct Standard) Cisco Unified OS Admin (Direct Standard)

Required COP Files

The table 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 Admin 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.

Table 4: COP File Requirements for Upgrades

From	To	COP Files
Unified Communications Manager Upgrades		
Unified CM 8.6(x), 9.1(x)	11.5(x)	Refresh upgrade. Required COP files: • ciscocm.version3-keys.cop.sgn Optional COP files: • ciscocm.vmware-disk-size-reallocation-<latest_version>.cop.sgn) • ciscocm.free_common_space_v<latest_version>.cop.sgn
Unified CM 10.5(x), 11.0(x), 11.5(x)	11.5(x)	Standard upgrade; no COP file required
IM and Presence Service Upgrades		
Cisco Unified Presence 8.5(4) through 8.6(1)	IM and Presence 11.5(x)	Refresh upgrade. Requires the following COP files: • cisco.com.cup.refresh_upgrade_v<latest_version>.cop • ciscocm.version3-keys.cop.sgn
IM and Presence 9.1(x)	11.5(x)	Refresh upgrade. Requires the following COP file: • ciscocm.version3-keys.cop.sgn
IM and Presence 10.5(x), 11.0(x), 11.5(x)	11.5(x)	Standard upgrade; no COP file required

Upgrade Restriction for 11.5(1)SU9

If your pre-upgrade version is Release 11.5(1)SU9 of Cisco Unified Communications Manager and the IM and Presence Service, you cannot upgrade to Releases 12.0(x), 12.5(1), 12.5(1)SU1, or 12.5(1)SU2. The minimum Release that you can upgrade to is 12.5(1)SU3.

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 11.5 and is compatible with the other Cisco Collaboration applications and versions that are a part of Cisco Collaboration System Release 11.5.

For a complete listing of Cisco Collaboration applications and versions that make up Release 11.5, 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

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 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

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 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 520 Cisco Headset 530 Cisco Headset 560
Cisco IP Communicator	Cisco IP Communicator—EOS Notice

Device Series	Device Model
Webex	Webex App Webex Room Phone Webex Desk Camera Webex Desk Webex Desk Hub Webex Desk Pro Webex Desk Limited Edition Webex Board 55, 55s, 70, 70s, 85, 85s Webex Room Panorama Webex Room 70 Panorama Webex Room 70 Webex Room 70 G2 Webex Room 55 Webex Room 55 Dual Webex Room Kit Pro Webex Room Kit Plus Webex Room Kit Webex 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
Cisco TelePresence EX Series	Cisco TelePresence System EX90—EOS Notice

Device Series	Device Model
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

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...
• 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 Cisco Media Convergence Servers are not supported. 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 2019 (Minimum supported release is 11.5(1)SU7)
- Microsoft Active Directory 2016
- Microsoft Active Directory 2012
- Microsoft Active Directory 2008 R1 (32-bit) / R2 (64-bit)

- Microsoft Active Directory 2003 R1/R2 (32-bit)
- Microsoft Active Directory Application Mode 2003 R1/R2 (32-bit)
- Microsoft Lightweight Directory Services 2019 (Minimum supported release is 11.5(1)SU7)
- Microsoft Lightweight Directory Services 2008 R1(32-bit) / R2(64-bit)
- Microsoft Lightweight Directory Services 2012
- Sun ONE Directory Server 7.0
- Open LDAP 2.3.39
- Open LDAP 2.4
- Oracle Directory Server Enterprise Edition 11gR1
- 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.)

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:

- OpenAM 10.0.1
- Microsoft® Active Directory Federation Services 2.0 (AD FS 2.0)
- Microsoft Azure (Minimum supported release is 11.5(1)SU8)
- PingFederate® 6.10.0.4
- F5 BIG-IP 11.6.0

Supported Web Browsers

The following web browsers are supported:

- Firefox with Windows 10 (64-bit)
- Chrome with Windows 10 (64-bit)
- Internet Explorer 11 with Windows 10 (64-bit)
- Internet Explorer 11 with Windows 7 (64-bit)
- Internet Explorer 11 with Windows 8.1 (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 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.

TLS 1.2 Support

With Release 11.5(1)SU3 and later releases, Cisco Unified Communications Manager and the IM and Presence Service support the use of TLS 1.2 for secure signaling. This supports includes the disabling of less secure TLS 1.0 and 1.1 connections, so that 1.2 is used for all TLS connections. For configuration details, see the *Security Guide for Cisco Unified Communications Manager*.

For additional information about TLS 1.2 support across the Cisco Collaboration deployment, see *TLS 1.2 Compatibility Matrix for Cisco Collaboration Products* at: https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/uc_system/unified/communications/system/Compatibility/TLS/TLS1-2-Compatibility-Matrix.html.

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	Cisco Unified Communications Manager and the IM and Presence Service support OpenJDK for application development. • Release 11.5(1)SU5 and SU6 use OpenJDK version 1.7.0.181. • Release 11.5(1)SU7 uses OpenJDK version 1.7.0.231. • Release 11.5(1)SU8 uses OpenJDK version 1.7.0.251. • Release 11.5(1)SU9 uses OpenJDK version 1.8.0.262. • Release 11.5(1)SU10 uses OpenJDK version 1.8.0.275. • Release 11.5(1)SU11 uses OpenJDK version 1.8.0.275.
SSL Connections	For Secure Sockets Layer (SSL) connections, these releases support either OpenSSL or Cisco SSL. You can use either of the following for your respective versions: • Release 11.5(1)SU7 uses OpenSSL 1.0.1e 57.el6 and CiscoSSL 1_0_2s_6_1_512 • Release 11.5(1)SU8 uses OpenSSL 1.0.1e-58.el6_10 and CiscoSSL 1.0.2u.6.1.533 • Release 11.5(1)SU9 uses OpenSSL 1.0.1e-58.el6_10 and CiscoSSL 1_0_2u_6_1_533 • Release 11.5(1)SU10 uses OpenSSL 1.0.1e-59.el6_10 and CiscoSSL 1_0_2y_6_1_559 • Release 11.5(1)SU11 uses OpenSSL 1.0.1e-59.el6_10 and CiscoSSL 1_0_2y_6_1_559
SSH Clients	• Release 11.5(1)SU7 supports OpenSSH client version 5.3p1 123.el6_9 for SSH connections. • Release 11.5(1)SU8 supports OpenSSH client version 5.3p1-124.el6_10 for SSH connections. • Release 11.5(1)SU9 supports OpenSSH client version 5.3p1-124.el6_10 for SSH connections. • Release 11.5(1)SU10 supports OpenSSH client version 5.3p1-124.el6_10 for SSH connections. • Release 11.5(1)SU11 supports OpenSSH client version 5.3p1-124.el6_10 for SSH connections.

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 Cisco Unified Communications Manager

The following ciphers are supported by Cisco Unified Communications Manager:

Table 11: Unified Communications Manager Cipher Support for TLS Ciphers

Application / Process	Protocol	Port	Supported Ciphers
Cisco CallManager	TCP / TLS	2443	AES128-SHA: NULL-SHA :
DRS	TCP / TLS	4040	ECDHE-RSA-AES256-GCM-SHA384: ECDHE-RSA-AES256-SHA384: ECDHE-RSA-AES256-SHA: DHE-RSA-AES256-GCM-SHA384: DHE-RSA-AES256-SHA: AES256-GCM-SHA384: AES256-SHA ECDHE-RSA-AES128-GCM-SHA256: ECDHE-RSA-AES128-SHA256: ECDHE-RSA-AES128-SHA: DHE-RSA-AES128-GCM-SHA256: DHE-RSA-AES128-SHA AES128-GCM-SHA256: AES128-SHA ECDHE-RSA-DES-CBC3-SHA EDH-RSA-DES-CBC3-SHA DES-CBC3-SHA
Cisco Tomcat	TCP / TLS	8443 / 443	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384: TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256: TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384: TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256: TLS_RSA_WITH_AES_256_CBC_SHA: TLS_RSA_WITH_AES_128_CBC_SHA: TLS_DHE_RSA_WITH_AES_128_CBC_SHA: TLS_DHE_DSS_WITH_AES_256_CBC_SHA
Cisco CallManager	TCP / TLS	5061	ECDHE-RSA-AES256-GCM-SHA384: ECDHE-ECDSA-AES256-GCM-SHA384: ECDHE-RSA-AES128-GCM-SHA256: ECDHE-ECDSA-AES128-GCM-SHA256: AES128-SHA: NULL-SHA:
Cisco CTL Provider	TCP / TLS	2444	AES256-SHA: AES128-SHA:
Cisco Certificate Authority Proxy Function	TCP / TLS	3804	AES256-SHA: AES128-SHA:
CTIManager	TCP / TLS	2749	ECDHE-RSA-AES256-GCM-SHA384: ECDHE-ECDSA-AES256-GCM-SHA384: ECDHE-RSA-AES128-GCM-SHA256: ECDHE-ECDSA-AES128-GCM-SHA256: AES128-SHA:
Cisco Trust Verification Service	TCP / TLS	2445	AES256-SHA: AES128-SHA:
Cisco Intercluster Lookup Service	TCP / TLS	7501	AES128-SHA:

Application / Process	Protocol	Port	Supported Ciphers
Secure Configuration download (HAPROXY)	TCP / TLS	6971, 6972	ECDHE-RSA-AES256-GCM-SHA384: ECDHE-ECDSA-AES256-GCM-SHA384: ECDHE-RSA-AES128-GCM-SHA256: ECDHE-ECDSA-AES128-GCM-SHA256: AES128-SHA:
Authenticated Contact Search	TCP / TLS	9443	ECDHE-RSA-AES256-GCM-SHA384: ECDHE-ECDSA-AES256-GCM-SHA384: AES256-SHA: ECDHE-RSA-AES128-GCM-SHA256: ECDHE-ECDSA-AES128-GCM-SHA256: AES128-SHA:

Supported Ciphers for SSH

Table 12: Cipher Support for SSH Ciphers

Service	Ciphers/Algorithms
SSH Server	• Ciphers: aes128-ctr aes192-ctr aes256-ctr aes128-cbc aes192-cbc aes256-cbc • MAC algorithms: hmac-sha1 • Kex algorithms: diffie-hellman-group14-sha1 diffie-hellman-group-exchange-sha256 diffie-hellman-group-exchange-sha1

Service	Ciphers/Algorithms

SSH Client	• Ciphers:
	`aes128-ctr`
	`aes192-ctr`
	`aes256-ctr`
	`aes128-cbc`
	`3des-cbc`
	`aes192-cbc`
	`aes256-cbc`
	`rijndael-cbc@lysator.liu.se`
	• MAC algorithms:
	`hmac-sha2-512`
	`hmac-sha2-256`
	`hmac-sha1`
	• Kex algorithms:
	`diffie-hellman-group14-sha1`
	`diffie-hellman-group-exchange-sha256`
	`diffie-hellman-group-exchange-sha1`

DRS Client	• Ciphers:
	`aes256-ctr`
	`aes256-cbc`
	`aes128-ctr`
	`aes128-cbc`
	• MAC algorithms:
	`hmac-sha1`
	`hmac-sha2-256`
	`hmac-sha1-96`
	• Kex algorithms:
	`ecdh-sha2-nistp256`
	`ecdh-sha2-nistp384`
	`ecdh-sha2-nistp521`
	`diffie-hellman-group14-sha1`
	`diffie-hellman-group-exchange-sha256`

Service	Ciphers/Algorithms

SFTP client	• Ciphers:
	`aes128-ctr`
	`aes192-ctr`
	`aes256-ctr`
	`aes128-cbc`
	`aes192-cbc`
	`aes256-cbc`
	• MAC algorithms:
	`hmac-sha2-512`
	`hmac-sha2-256`
	`hmac-sha1`
	• Kex algorithms:
	`diffie-hellman-group14-sha1`
	`diffie-hellman-group-exchange-sha256`
	`diffie-hellman-group-exchange-sha1`

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.

LDAP Directory Servers Supported

IM and Presence Service integrates with these LDAP directory servers:

- Microsoft Active Directory 2012, 2016, and 2019—The minimum 11.5(x) release for AD2019 is 11.5(1)SU7.
- Microsoft Lightweight Directory Services 2019 (Minimum supported release is 11.5(1)SU7)
- Netscape Directory Server
- Sun ONE Directory Server 5.2
- Open LDAP 2.3.39

- Open LDAP 2.4

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.

** The minimum IM and Presence Service release for Federation with an on-premises Skype for Business or an Office 365-hosted Skype for Business is Release 11.5(1)SU2.

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:

- Release 10.x
- Release 11.x
- Release 12.x
- Release 14 and above

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 14: 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.
Microsoft Exchange Server 2010	Service Packs for Microsoft Exchange 2010 (SP1)
Microsoft Exchange Server 2013	Service Packs for Microsoft Exchange 2013 (SP1)
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. The minimum IM and Presence Service release for Office 365 integration is Release 11.5(1)SU3. **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 • Active Directory 2019 with Windows Server 2019—With 11.x releases, the minimum IM and Presence Service Release is 11.5(1)SU7. **Note** User names configured in Active Directory must be identical to those names defined in Unified Communications Manager.

Component	Install Compatible Version
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.

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.

Supported Ciphers for the IM and Presence Service

The following ciphers are supported by the IM and Presence Service.

Table 15: Cisco Unified Communications Manager IM & Presence Cipher Support for TLS Ciphers

Application / Process	Protocol	Port	Supported Ciphers
Cisco SIP Proxy	TCP / TLS	8083	ECDHE-RSA-AES256-GCM-SHA384: ECDHE-ECDSA-AES256-GCM-SHA384: AES256-SHA: ECDHE-RSA-AES128-GCM-SHA256: ECDHE-ECDSA-AES128-GCM-SHA256: AES128-SHA DES-CBC3-SHA
Cisco SIP Proxy	TCP / TLS	5061	ECDHE-RSA-AES256-GCM-SHA384: ECDHE-ECDSA-AES256-GCM-SHA384: AES256-SHA: ECDHE-RSA-AES128-GCM-SHA256: ECDHE-ECDSA-AES128-GCM-SHA256: AES128-SHA: DES-CBC3-SHA:
Cisco SIP Proxy	TCP / TLS	5062	ECDHE-RSA-AES256-GCM-SHA384: ECDHE-ECDSA-AES256-GCM-SHA384: AES256-SHA: ECDHE-RSA-AES128-GCM-SHA256: ECDHE-ECDSA-AES128-GCM-SHA256: AES128-SHA: DES-CBC3-SHA:
Cisco Tomcat	TCP / TLS	8443, 443	ECDHE-RSA-AES256-GCM-SHA384: AES256-SHA: ECDHE-RSA-AES128-GCM-SHA256: DHE-RSA-AES128-SHA: AES128-SHA:

Application / Process	Protocol	Port	Supported Ciphers
Cisco XCP XMPP Federation Connection Manager	TCP /TLS	5269	AES128-GCM-SHA256 AES128-SHA AES128-SHA256 AES256-GCM-SHA384 AES256-SHA AES256-SHA256 CAMELLIA128-SHA CAMELLIA256-SHA ECDHE-ECDSA-AES128-GCM-SHA256 ECDHE-ECDSA-AES128-SHA ECDHE-ECDSA-AES128-SHA256 ECDHE-ECDSA-AES256-GCM-SHA384 ECDHE-ECDSA-AES256-SHA ECDHE-ECDSA-AES256-SHA384 ECDHE-RSA-AES128-GCM-SHA256 ECDHE-RSA-AES128-SHA ECDHE-RSA-AES128-SHA256 ECDHE-RSA-AES256-GCM-SHA384 ECDHE-RSA-AES256-SHA ECDHE-RSA-AES256-SHA384
Cisco XCP Client Connection Manager	TCP /TLS	5222	AES128-GCM-SHA256 AES128-SHA AES128-SHA256 AES256-GCM-SHA384 AES256-SHA AES256-SHA256 CAMELLIA128-SHA CAMELLIA256-SHA ECDHE-ECDSA-AES128-GCM-SHA256 ECDHE-ECDSA-AES128-SHA ECDHE-ECDSA-AES128-SHA256 ECDHE-ECDSA-AES256-GCM-SHA384 ECDHE-ECDSA-AES256-SHA ECDHE-ECDSA-AES256-SHA384 ECDHE-RSA-AES128-GCM-SHA256 ECDHE-RSA-AES128-SHA ECDHE-RSA-AES128-SHA256 ECDHE-RSA-AES256-GCM-SHA384 ECDHE-RSA-AES256-SHA ECDHE-RSA-AES256-SHA384

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA 95134-1706
USA

Asia Pacific Headquarters
CiscoSystems(USA)Pte.Ltd.
Singapore

Europe Headquarters
CiscoSystemsInternationalBV
Amsterdam,TheNetherlands

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.