Planning the Upgrade

Upgrade and Migration Overview

The procedures in this guide describe how to upgrade Cisco Unified Communications Manager (Unified Communications Manager) and Cisco Unified Communications Manager IM and Presence Service (IM and Presence Service) from an earlier version to the current version.

Use the procedures in this guide as a starting point for all upgrades and migration paths. Note these upgrade usage terminologies when you read the term 'upgrade' used in this guide:

- The term "upgrade" refers to the scenario where all the cluster nodes complete the steps required for end-to-end processes. As an outcome, the entire cluster runs on the upgraded destination version. Then, the upgrade is considered to be 'complete/done'. The end-to-end process for "upgrade" is defined as all nodes completing upgrade-inactive versions, all nodes completing switch-version-reboot, and database replication completion across all the cluster nodes. Refer to the Switch Version Manually (Clusterwide) section for information on checking the upgrade status.
- The term "inactive version" or "upgrade inactive version" refers to only upgrading the inactive version, without or before performing switch-version-reboot, on one or more cluster nodes.

Recommended Upgrade Considerations:

1. Choose a "direct upgrade" method. We recommend you choose Simple Upgrades, but you can still perform the legacy Single-Node upgrade method. See Upgrade Methods, on page 2.
2. Regardless of the upgrade method chosen, all the cluster nodes must complete:
   - upgrade inactive version
   - switch version reboot

- wait for database replication to complete across all nodes in the cluster.

3. You must ensure that the points mentioned in step 2 of the upgrade plan follow the node sequencing rules as mentioned in the Sequencing Rules and Time Requirements chapter.
4. Upgrade is not complete unless all the requirements in Step 2 is finished. You can view the upgrade status from the Cisco Unified OS Administration user interface or use the CLI commands to monitor status. You can also see banner messages in the user interface to warn about potential blocks to cluster nodes and add/update/delete functionalities until all the conditions in Step 2 are complete across all the clusters.

Upgrade Methods

The following table explains the types of upgrades that you can complete with Cisco Unified Communications Manager and the IM and Presence Service and the upgrade tools that you can use to complete the upgrade.

Upgrade Type	Description	Upgrade Tools
Direct Standard Upgrade	A standard upgrade is a direct upgrade where you need to upgrade the application software, but not the underlying operating system. This is usually the simplest form of upgrade and would typically apply to upgrades from within the same major-minor release category, where the OS is the same for both releases. For release 12.5 or higher, direct standard upgrades have substantially improved durations, simpler procedures, and reduced service impact. **Example**: Upgrades from 12.5(1) to 12.5(1)SU1. **Note** For standard upgrades where the preupgrade release is 12.5(1) or later, you can use the simplified clusterwide upgrade to upgrade your entire cluster.	The following tools are used to complete standard upgrades: • Unified OS Admin • CLI • PCD Upgrade task
Direct Refresh Upgrade	A direct refresh upgrade is a direct upgrade where you need to upgrade both the application software and the underlying operating system software. This would typically be used if you're upgrading from one major-minor release to another where the OS is different for the two releases. **Example**: Refresh Upgrades from Pre-12.5.x source to Release 15 is not supported.	The following tools are used to complete refresh upgrades: • Unified OS Admin • CLI • PCD Upgrade task

Upgrade Type	Description	Upgrade Tools
Direct migration	A direct migration involves a 'repave' where multiple factors exist that can't address with just a direct upgrade. Direct Migration is used in the following cases: • Site moves • The desired upgrade requires you to change the infrastructure hardware and platform. **Example**: Upgrades from Unified CM 10.5(x) on ESXi 5.5 and Cisco UCS M3 generation hardware to 12.5(x) on ESXi 7.0 and Cisco UCS M5 generation hardware. • ESXi upgrade and/or Unified CM virtual machine configuration change • Unified CM address/hostname change • The desired upgrade requires a direct upgrade path that does not exist for the source release. **Example**: Unified CM 8.5(1) on ESXi to 12.5(x) on ESXi—no direct upgrade path exists making a migration mandatory. • "Virtual to Virtual (V2V)" migration, where even if a direct upgrade path exists, direct migration is preferred to mitigate upgrade path complexity factors such as duration, service impact, and a short outage window.	The following tool is used to complete migrations: • PCD Migration • Fresh Install with Data Import
Install with Data Import	A fresh installation with data import is an alternative to direct upgrades and direct migrations, from releases 10.5 and above, migrating to release 15. It involves the following: • Install the COP file **ciscocm.DataExport_v1.0.cop.sgn** on source release of 10x or 11x. • Export the source release's data to a Secure FTP (SFTP) server. • Install the new virtual machines of release 15, then import this data (usually a touchless cluster install where both answer files and import data are pre-staged). If you want to roll back to the previous release, install **ciscocm.DataExport_rollback_v1.0.cop.sgn** COP file.	CLI is used to complete installation with data import
Migration from legacy releases	A legacy release is a source release that is so old that the desired upgrade has no direct upgrade path and no direct migration path available to destination release 15. The only option is a direct upgrade to a later release that supports either PCD migration or Install with Data Import, followed by either a PCD migration or Fresh Install with Data Import to release 15. **Example**: Any desired upgrade to 15 from a pre-10.5 Unified CM or a pre-10.5 IM and Presence Service.	For details, see Upgrading from Legacy Releases.

Take Record of Your Current System

Before you begin the upgrading, take a record of the versioning within your current system setup. After you know the versions that your current system uses, you can begin planning your upgrade. This includes:

- Pre-upgrade versions for Unified Communications Manager and the IM and Presence Service
- Current Hardware version
- VMware Versioning

Note VMware was introduced as an optional deployment in Unified CM 8.x and 9.x. From Release 10.x forward, VMware became mandatory.

You can obtain versioning by running the Pre-upgrade Upgrade Readiness COP File. For details, see Run Upgrade Readiness COP File (Pre-upgrade).

Supported Upgrade and Migration Paths with COP Files

The following table highlights supported upgrade paths to upgrade to Release 15 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 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, 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. Refresh Upgrades from Pre-12.5.x source to Release 15 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		Supported

Source	Destination	Mechanism		Pre-requisites	Version Switching* (Source to Destination and Vice Versa)

				• 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.	

		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)			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 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.	
		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.

Choose Your Upgrade Tool

Refer to the table below for information that can help you to decide which upgrade tool to use when there are multiple mechanisms available to choose from.

Note For legacy upgrades, see Upgrading from Legacy Releases.

Table 2: Choose your Upgrade Method

Upgrade Method	Support	When to use this method...	How to complete the Upgrade or Migration
Unified OS Admin or CLI upgrades	Direct upgrades (standard or refresh) via the Cisco Unified OS Administration GUI or CLI.	Consider this tool for: • For simplified clusterwide upgrades. • You are only changing the application software and are not updating hardware or VMware. • A direct upgrade path exists. • You are only upgrading Unified CM and IM and Presence Service. There are no other UC applications. • You are upgrading a single Unified CM cluster and a single IM and Presence sub-cluster. **Note** CLI upgrades provide the same support as Unified OS Admin upgrades, but from a different interface.	Go to Upgrade Tasks
PCD Upgrades	Handles direct upgrades (Standard or Refresh) via Cisco Prime Collaboration Deployment's upgrade task.	Consider this tool when: • You have multiple clusters to upgrade. • Your cluster has a large number of nodes, and you need help orchestrating the upgrade to forward the schedule. • You need to upgrade other applications, such as Cisco Unity Connection or Cisco Unified Contact Center Express.	**From Release is 10.x or later** 1. Run Upgrade Readiness COP File (Pre-upgrade) 2. Refer to the Cisco Prime Collaboration Deployment Administration Guide to run an upgrade or migration task. 3. Run Upgrade Readiness COP File (Post-upgrade) **Note** If the From release is prior to 9.x, the Upgrade Readiness COP files do not work. You will need to complete the manual pre-upgrade tasks and post-upgrade tasks in the Appendix.
PCD Migrations	Handles migrations via Cisco Prime Collaboration Deployment.	Consider this tool when: • You are upgrading from an earlier release that did not use VMware. • Your source release is so old that it does not support VMware. • In addition to upgrading application versions, you must make ESXi updates as well. • You are changing infrastructure hardware and platform. • Your source release has previously direct upgraded from a pre-11.5 version and is having out of disk space issues. You may need to reinstall to the latest stack to maximize usable disk space. • You have available infrastructure for temporary duplicate VMs and their required hardware.	

Upgrade Method	Support	When to use this method...	How to complete the Upgrade or Migration
Fresh Install with Data Import	Handles migrations through exporting source release data to SFTP, and touchless installing a new 15 cluster with import of that data.	Consider this tool when: • You don't want to do direct refresh upgrade to 15, but that is the only direct upgrade path type available. • You don't want to do direct migration with PCD (with readdress and temporary extra hardware) as an alternative to that direct refresh upgrade.	1. Install COP if the source releases are: 10.5, 11.5, and 12.5.1 to 12.5(1)SU4 2. Run CLI to export data to SFTP. 3. Touchless install (see Install Guide) with new answer file fields and new installer GUI fields to import that data from SFTP.

Requirements and Limitations

The following sections describe requirements and limitations for upgrades to this release.

Hardware Requirements

You can install Unified Communications Manager and IM and Presence Service on a virtual server hosted on the following types of hardware. If your current deployment does not use one of these servers, then you must migrate to a supported hardware platform:

- Cisco Business Edition 6000 or 7000 appliance
- Virtualized Cisco hardware (such as Cisco UCS or Cisco HyperFlex) with VMware vSphere ESXi
- Virtualized Third-party hardware with VMware vSphere ESXi

The requirements and support policies are different for each of these options. Before you begin an upgrade, verify that your current hardware meets the requirements of the new release. You can find detailed information about the requirements by going to https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/uc_system/virtualization/cisco-collaboration-virtualization.html and following the links for the Unified Communications Manager and IM and Presence Service applications.

Platform Requirements

This section provides information about the platform requirements that you must meet before you can deploy Unified Communications Manager and the IM and Presence Service on virtual machines.

In this release, you cannot install or run Unified Communications Manager and the IM and Presence Service directly on server hardware; you must run these applications on virtual machines.

Before you can install or upgrade the software on a virtual machine, you must:

- Configure the platform.
- Install and configure ESXi virtualization software.

Note For the latest Unified Communications Manager compatible/supported ESXi versions, see https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/uc_system/virtualization/virtualization-cisco-unified-communications-manager.html and https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/uc_system/virtualization/cisco-collaboration-infrastructure.html#VMwareCompatibility.

- Deploy a virtual machine from the correct Cisco provided OVA file for the release. Depending on the installation method used, additional steps are required.

Virtual Machine Configuration

Before you begin an upgrade or migration, verify that your current virtual machine (VM) software meets the requirements of the new release.

Table 3: Virtual Machine Requirements

Item	Description
OVA templates	OVA files provide a set of predefined templates for virtual machine configuration. They cover items such as supported capacity levels and any required OS/VM/SAN alignment. You must use a VM configuration from the OVA file provided for the Unified Communications Manager and IM and Presence Service applications. The correct VM configuration to use from the OVA file is based on the size of the deployment. For information about OVA files, search for the topic "Unified Communications Virtualization Sizing Guidelines" at https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/uc_system/virtualization/collaboration-virtualization-sizing.html.
VMware vSphere ESXi	You must install a version of vSphere ESXi hypervisor that meets the compatibility and support requirements for the release. If you use Cisco Prime Collaboration Deployment (PCD) to perform an upgrade or migration, you must also ensure that you install vSphere ESXi with the correct license type. PCD is not compatible with all the license types of vSphere ESXi because some of these licenses don't enable the required VMware APIs.
VMware vCenter	VMware vCenter is optional when you deploy Unified Communications Manager or IM and Presence Service on Business Edition 6000/7000 appliances, or on UC on UCS tested reference configuration hardware. VMware vCenter is mandatory when you deploy on UC on UCS specs-based and third-party server specs-based hardware.

Item	Description
VM configuration virtual hardware specifications	Verify whether you need to change the vRAM on your VM to upgrade to a new release of Unified Communications Manager or IM and Presence Service. Your Unified Communications Manager or IM and Presence Service Release 15 version may require more vRAM than you are currently running. Direct upgrade to IM and Presence Service Release 15 will fail if the older release versions do not have enough vRAM size. The Unified Communications Manager or IM and Presence Service Release 15 versions may require more GB and different partitions than you are currently running. Direct upgrade to Unified Communications Manager and IM and Presence Service Release 15 will fail for all single 80GB vDisk deployments, even if you manually resized the HDD size to 110 GB. To check vRAM and vDisk specifications before upgrade, either refer to the Readme of the base OVA for Release 15 or use the QuoteCollab tool. For more references, see: • Virtual Machine Configuration Tasks to update your VMware. • To update the vDisk, either backup or restore your Release 12.5 or 14 and SU versions to a new VMware with vDisk installed as 110GB where Direst upgrade will be successful. Or use either PCD Migration or Fresh Install with Data Import Task migrations to move to a new node deployed with the Unified CM Release 15 OVA template.

Deprecated Phone Models

The following table lists all the phone models that are deprecated for this release of Cisco 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 Cisco Unified Communications Manager and you have any of these phone models deployed, the phone will not work after the upgrade.

Table 4: Deprecated Phone Models for this Release

Deprecated Phone Models for this Release	First Deprecated as of...
No additional endpoints deprecated	Release 15
No additional endpoints deprecated	Release 14
• Cisco Unified IP Phone 7970G • Cisco Unified IP Phone 7971G-GE • Cisco Unified Wireless IP Phone 7921G	12.0(1) and later releases

Deprecated Phone Models for this Release	First Deprecated as of...
• Cisco IP Phone 12 SP+ and related models • Cisco IP Phone 30 VIP and related models • Cisco Unified IP Phone 7902 • Cisco Unified IP Phone 7905 • Cisco Unified IP Phone 7910 • Cisco Unified IP Phone 7910SW • Cisco Unified IP Phone 7912 • Cisco Unified Wireless IP Phone 7920 • Cisco Unified IP Conference Station 7935	11.5(1) and later releases

For additional information, refer to Field Notices.

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 Migration FX tool to migrate from older model to newer model phones. For details, go to: https://www.unifiedfx.com/products/unifiedfx-migrationfx#endpoint_refresh_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.

Network Requirements

This section lists the requirements that your network must meet before you can deploy Unified Communications Manager and the IM and Presence Service.

IP Address Requirements

A complete collaboration solution relies on DNS in order to function correctly for a number of services and thus requires a highly available DNS structure in place. If you have a basic IP telephony deployment and do not want to use DNS, you can configure Unified Communications Manager and IM and Presence Service to use IP addresses rather than hostnames to communicate with gateways and endpoint devices.

You must configure the server to use static IP addressing to ensure that the server obtains a fixed IP address. Using a static IP address also ensures that Cisco Unified IP Phones can register with the application when you plug the phones into the network.

DNS requirements

Note the following requirements:

- Mixed-mode DNS deployments not supported—Cisco does not support mixed-mode deployments. Both Unified Communications Manager and IM and Presence Service must either use or not use DNS.
- If your deployment uses DNS—Unified Communications Manager and IM and Presence Service should use the same DNS server. If you use different DNS servers between IM and Presence Service and Unified Communications Manager, it is likely to cause abnormal system behavior.
- If your deployment does not use DNS, you will need to edit the following Host Name/IP Address fields:
  - Server—In the Cisco Unified CM Administration **Server Configuration** window, set IP addresses for your cluster nodes.
  - IM and Presence UC Service—In the Cisco Unified CM Administration **UC Service Configuration** window, create an IM and Presence UC service that points to the IP address of the IM and Presence database publisher node.
  - CCMCIP Profiles—In the Cisco Unified CM IM and Presence Administration **CCMCIP Profile Configuration** window, point any CCMCIP profiles to the IP address of the host.
- Multinode considerations—If you are using the multinode feature in IM and Presence Service, see the section regarding multinode deployments in the Configuration and Administration of the IM and Presence Service Guide for DNS configuration options.
- Ensure that the DNS server is configured on Windows 2019 or above or use the DNS server configured in any Linux Machine.

Firewall Requirements

Ensure that you configure your firewall so that connections to port 22 are open, and aren't throttled. During the installation of Unified Communications Manager and IM and Presence subscriber nodes, multiple connections to the Unified Communications Manager publisher node are opened in quick succession. Throttling these connections could lead to a failed installation. For general security considerations, see the Security Guide for Cisco Unified Communications Manager.

Note We recommend that you disable the "Intruder/Intrusion Detection" and/or "Brut Force Attack" features during upgrade and installs because these Firewall features are known to cause upgrades and installations to fail.

For more information on the port usage, see the chapter 'Cisco Unified Communications Manager TCP and UDP Port Usage' in the System Configuration Guide for Cisco Unified Communications Manager.

SFTP Server Support

Use the information in the following table to determine which SFTP server solution to use in your system.

Table 5: SFTP Server Information

SFTP Server	Information
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 Unified Communications Manager and Cisco Prime Collaboration Deployment. See the Cisco Prime Collaboration Deployment Administration Guide before you upgrade its version (SFTP) or Unified Communications Manager 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 Unified Communications Manager 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.

Subnet Limitations

Do not install Unified Communications Manager in a large Class A or Class B subnet that contains a large number of devices. For more information, see Cisco Collaboration System 12.x Solution Reference Network Designs (SRND).

Cluster Size

The number of Unified Communications Manager subscriber nodes in a cluster cannot exceed 4 subscriber nodes and 4 standby nodes, for a total of 8 subscribers. The total number of servers in a cluster, including the Unified Communications Manager publisher node, TFTP server, and media servers, cannot exceed 21.

The maximum number of IM and Presence Service nodes in a cluster is 6.

For more information, see *"Cisco Collaboration Solutions Design Guidance"* at http://www.cisco.com/go/ucsrnd.

IP Subnet Mask

If you are using a 24-bit IP subnet mask, ensure that you use the following format:255.255.255.0. Do not use the format 255.255.255.000. Although 255.255.255.000 is a valid format, it may cause problems during the upgrade process. We recommend that you change the format before you begin an upgrade to avoid possible problems. You can change the subnet mask by executing the **set network ip eth0 <server_IP_address> 255.255.255.0** command.

Other formats are supported for subnet masks and this limitation applies to 24-bit subnet masks only.

Software Requirements

This section refers to application software requirements for Cisco Unified Communications Manager and the IM and Presence Service upgrades and migrations.

Device Name for Cisco Unified Mobile Communicator

Ensure that the device name for the Cisco Unified Mobile Communicator device contains 15 or fewer characters. If the device name contains more than 15 characters for the Cisco Unified Mobile Communicator, the device does not migrate during the upgrade.

Export Restricted and Export Unrestricted Software

This release of Unified Communications Manager and IM and Presence Service supports an export unrestricted (XU) version, in addition to the export restricted (K9) version.

Note Unrestricted versions of software are intended only for a specific set of customers who do not want various security capabilities; unrestricted versions are not intended for general deployments.

Export unrestricted versions differs from restricted versions as follows:

- Encryption of user payload (information exchange) is not supported.
- External SIP interdomain federation with Microsoft OCS/Lync or AOL is not supported.
- After you install an unrestricted release, you can never upgrade to a restricted version. A fresh install of a restricted version on a system that contains an unrestricted version is also not supported.
- All nodes within a single cluster must be in the same mode. For example, Unified Communications Manager and IM and Presence Service in the same cluster must either all be in unrestricted mode or all be in restricted mode.
- IP Phone security configurations are modified to disable signaling and media encryption (including encryption provided by the VPN phone feature).

Note Be aware that after you install an unrestricted release, you can never upgrade to a restricted version. You are not allowed to perform a fresh installation of a restricted version on a system that contains an unrestricted version.

For all Graphical User Interfaces (GUIs) and Command Line Interfaces (CLIs), the Administrator can view the product version (restricted or export unrestricted).

The following table describes the GUI items that are not available for the export unrestricted version ofUnified Communications Manager and IM and Presence Service.

GUI Item	Location	Description
Cisco Unified CM Administration		
VPN Configuration	**Advanced Features** > **VPN**	This menu and its options are not available.
Phone Security Profile Configuration	**System** > **Security** > **Phone Security Profile**	The **Device Security Mode** is set to **Non Secure** and is not configurable.
Cisco Unified CM IM and Presence Administration		
Security Settings	**System** > **Security** > **Settings**	• You cannot check the **Enable XMPP Client to IM/P Service Secure Mode** setting. • You cannot check the **Enable XMPP Router-to-Router Secure Mode** setting. • You cannot check the **Enable Web Client to IM/P Service Secure Mode** setting. • The option to set **SIP intra-cluster Proxy-to-Proxy Transport Protocol** to **TLS** have been removed.
Service Parameter Configuration for Cisco SIP Proxy service	**System** > **Service Parameters** and choose **Cisco SIP Proxy** as the **Service**	• All TLS options have been removed for the **Transport Preferred Order** parameter. • The TLS option have been removed from the **SIP Route Header Transport Type** parameter.

GUI Item	Location	Description
SIP Federated Domains	**Presence** > **Inter-domain Federation** > **SIP Federation**	When you configure interdomain federation to OCS/Lync, you will receive warning popup to indicate that it is only possible to directly federate with another OCS/Lync within the enterprise. Interdomain federation to OCS/Lync outside the enterprise is not supported in unrestricted mode.
XMPP Federation Settings	**Presence** > **Inter-domain Federation** > **XMPP Federation** > **Settings**	You cannot configure the security mode. It is set to **NO TLS**.
Proxy Configuration Settings	**Presence** > **Routing** > **Settings**	You cannot set any TLS or HTTPS listeners as the preferred proxy listener.

Upgrades from Unified CM 9.x

Upgrades from Unified Communications Manager version 9.x to version 10.x or higher fail if you have a SIP Profile with any of the following names on version 9.x:

- Standard SIP Profile
- Standard SIP Profile For Cisco VCS
- Standard SIP Profile For TelePresence Conferencing
- Standard SIP Profile For TelePresence Endpoint
- Standard SIP Profile for Mobile Device

If you have a SIP Profile with any of these names, you need to rename or delete it before proceeding with the upgrade.

OS Admin Account Required for CLI-Initiated IM and Presence Upgrades

If you are using the **utils system upgrade** CLI command to upgrade IM and Presence Service nodes, you must use the default OS admin account, as opposed to a user with administrator privileges. Otherwise, the upgrade will not have the required privilege level to install essential services, thereby causing the upgrade to fail. You can confirm the account's privilege level by running the **show myself** CLI command. The account must have privilege level 4.

Note that this limitation exists for CLI-initiated upgrades of IM and Presence Service only and does not apply to Unified Communications Manager. Also note that this limitation may be fixed for newer ISO files. See your ISO Readme file for details on your specific ISO file. For-up-to date information on this limitation, see CSCvb14399.

Database Migration Required for Upgrades with Microsoft SQL Server

If you have Microsoft SQL Server deployed as an external database with the IM and Presence Service and you are upgrading from 11.5(1), 11.5(1)SU1, or 11.5(1)SU2, you must create a new SQL Server database and migrate to the new database. This is required due to enhanced data type support in this release. If you don't migrate your database, schema verification failure will occur on the existing SQL Server database and services that rely on the external database, such as persistent chat, will not start.

After you upgrade your IM and Presence Service, use this procedure to create a new SQL Server database and migrate data to the new database.

Note This migration is not required for Oracle or PostgreSQL external databases.

Before You Begin

The database migration is dependent on the `MSSQL_migrate_script.sql` script. Contact Cisco TAC to obtain a copy.

Table 6:

Step	Task
Step 1	Create a snapshot of your external Microsoft SQL Server database.
Step 2	Create a new (empty) SQL Server database. For details, see the following chapters in the Database Setup Guide for the IM and Presence Service: 1. "Microsoft SQL Installation and Setup"—See this chapter for details on how to create your new SQL server database on your upgraded IM and Presence Service. 2. "IM and Presence Service External Database Setup"—After your new database is created, refer to this chapter to add the database as an external database in the IM and Presence Service.
Step 3	Run the System Troubleshooter to confirm that there are no errors with the new database. 1. From Cisco Unified CM IM and Presence Administration, choose **Diagnostics** > **System Troubleshooter**. 2. Verify that no errors appear in the **External Database Troubleshooter** section.
Step 4	Restart the Cisco XCP Router on all IM and Presence Service cluster nodes: 1. From Cisco Unified IM and Presence Serviceability, choose **Tools** > **Control Center - Network Services**. 2. From the **Server** menu, select an IM and Presence Service node and click **Go**. 3. Under **IM and Presence Services**, select **Cisco XCP Router**, and click **Restart**.

Step	Task
Step 5	Turn off services that depend on the external database: **1.** From Cisco Unified IM and Presence Serviceability, choose **Tools** > **Control Center - Feature Services**. **2.** From the **Server** menu, select an IM and Presence node and click **Go**. **3.** Under **IM and Presence Services**, select the following services:. Cisco XCP Text Conference Manager Cisco XCP File Transfer Manager Cisco XCP Message Archiver **4.** Click **Stop**.
Step 6	Run the following script to migrate data from the old database to the new database `MSSQL_migrate_script.sql`. **Note** Contact Cisco TAC to obtain a copy of this script
Step 7	Run the System Troubleshooter to confirm that there are no errors with the new database. **1.** From Cisco Unified CM IM and Presence Administration, choose **Diagnostics** > **System Troubleshooter**. **2.** Verify that no errors appear in the **External Database Troubleshooter** section.
Step 8	Start the services that you stopped previously. **1.** From Cisco Unified IM and Presence Serviceability, choose **Tools** > **Control Center - Feature Services**. **2.** From the **Server** menu, select an IM and Presence node and click **Go**. **3.** Under **IM and Presence Services**, select the following services: Cisco XCP Text Conference Manager Cisco XCP File Transfer Manager Cisco XCP Message Archiver **4.** Click **Start**.
Step 9	Confirm that the external database is running and that all chat rooms are visible from a Cisco Jabber client. Delete the old database only after you're confident that the new database is working.

Upgrade Considerations with FIPS Mode

When you enable the FIPS mode in Unified Communications Manager Release 12.5 SU1, the lower key size IPsec DH groups 1, 2, or 5 are disabled. If you have already configured the IPSec policies with DH groups

1, 2 or 5 and enabled FIPS mode, the upgrade to Unified Communications Manager Release 12.5 SU1 is blocked.

Perform any one of the following procedures before you upgrade to Unified Communications Manager Release 12.5 SU1:

- Delete the previously configured IPsec policies and perform the upgrade. After the upgrade is complete, reconfigure the IPsec policies with DH groups 14–18.
- Install the COP file (latest_version.xxxx.cop.sgn) that supports DH groups 14–18, reconfigure the IPsec policies and then perform an upgrade.

When you enable FIPS mode in Unified Communications Manager Release 15, the 3DES algorithm is not supported for IPSec communication. If you have already configured the IPSec policies with ESP and Encryption Algorithm as 3DES and enabled FIPS mode, the upgrade to Unified Communications Manager Release 15 is blocked.

Note If you disable the FIPS mode after installing the COP file, the IPSEC configuration page doesn't appear.

Note In case you're planning to upgrade or migrate to Release 15, note that the IPSec policy with 3DES Algorithm isn't supported in FIPS mode. You must delete and recreate the IPSec policy with the Encryption and ESP Algorithms other than 3DES in both the nodes between which the IPSec tunnel is to be established, and then plan an upgrade or migration.

For more information on configuring the IPSec policies, see *Cisco Unified Operating System Administration Online Help*.

IPSec Requirements

If you have IPSec configured with certificate-based authentication, make sure that the IPsec policy uses a CA-signed certificate. If you attempt to upgrade Unified Communications Manager with IPsec configured to use certificate-based authentication with self-signed certificates, the upgrade fails. You must reconfigure the IPsec policy to use a CA-signed certificate.

Note Before starting the migration, disable IPsec policy on all the nodes in the cluster.

Support for Intercluster Peers

The IM and Presence Service supports intercluster peers to clusters that are running different software versions. To find the interdomain federations that are supported, see the "Intercluster Peering Support" section in the Compatibility Matrix for Cisco Unified Communications Manager and IM and Presence Service.

Spectre/Meltdown Vulnerabilities During Upgrade

This release of Unified Communications Manager, Cisco IM and Presence Service, Cisco Emergency Responder, and Cisco Prime Collaboration Deployment contain software patches to address the Meltdown and Spectre microprocessor vulnerabilities.

Before you upgrade to Release 12.5(1) or above, we recommend that you work with your channel partner or account team to use the Cisco Collaboration Sizing Tool to compare your current deployment to an upgraded deployment. If required, change VM resources to ensure that your upgraded deployment provides the best performance.

Duplicate ENUMS Break Upgrades and Migrations from 10.5(2)

If you are Direct upgrading or Direct migrating from Release 10.5(2) or 11.0(1) to any later release, an issue exists with older locale installations that causes upgrade and migration failures. This issue exists if any of the following Unified CM combined network locales have been installed:

- cm-locale-combined_network-9.1.2.1100-1
- cm-locale-combined_network-10.5.2.2200-1
- cm-locale-combined_network-11.0.1.1000-1

This issue can also occur if the following Unified CM locales are installed together in the same cluster:

- cm-locale-en_GB-9.1.2.1100-1
- cm-locale-pt_BR-9.1.2.1100-1
- cm-locale-en_GB-10.5.2.2200-1
- cm-locale-pt_BR-10.5.2.2200-1
- cm-locale-en_GB-11.0.1.1000-1
- cm-locale-pt_BR-11.0.1.1000-1

To ensure that your upgrade does not fail, update your Unified Communications Manager and phone locale installation to use a locale that is dated after August 31, 2017 as this issue does not exist for any locale file issued after that date. After you update your locale installation, you can begin the upgrade or migration. For details on the workaround, see https://bst.cloudapps.cisco.com/bugsearch/bug/CSCuz97687.

Licensing Requirements

The following sections provide information about the licensing requirements for Unified Communications Manager and the IM and Presence Service.

Smart Software Licensing Overview

Cisco Smart Software Licensing is a new way of thinking about licensing. It adds flexibility to your licensing and simplifies it across the enterprise. It also delivers visibility into your license ownership and consumption.

Cisco Smart Software Licensing helps you to procure, deploy, and manage licenses easily where devices self-register and report license consumption, removing the need for product activation keys (PAK). It pools license entitlements in a single account and allows you to move licenses freely through the network, wherever you need them. It is enabled across Cisco products and managed by a direct cloud-based or mediated deployment model.

The Cisco Smart Software Licensing service registers the product instance, reports license usage, and obtains the necessary authorization from Cisco Smart Software Manager or Cisco Smart Software Manager satellite.

You can use Smart Licensing to:

- See the license usage and count
- See the status of each license type
- See the product licenses available on Cisco Smart Software Manager or Cisco Smart Software Manager satellite
- Renew License Authorization with Cisco Smart Software Manager or Cisco Smart Software Manager satellite
- Renew the License Registration
- Deregister with Cisco Smart Software Manager or Cisco Smart Software Manager satellite

Note The License authorization is valid for 90 days with a renewal at least once in 30 days. The authorization will expire after 90 days if it is not connected to Cisco Smart Software Manager or Cisco Smart Software Manager satellite.

If the Cisco Smart Software Manager satellite option is selected, the satellite must have an internet connection to Cisco Smart Software Manager for the authorization to occur. The Cisco Smart Software Manager satellite can operate in 2 modes: Connected Mode in which the connection time is configurable, and Disconnected mode which requires a manual sync.

There are two main deployment options for Smart Licensing:

- Cisco Smart Software Manager
- Cisco Smart Software Manager satellite

Cisco Smart Software Manager

The Cisco Smart Software Manager is a cloud-based service that handles your system licensing. Use this option if Unified Communications Manager can connect to cisco.com, either directly or via a proxy server. Cisco Smart Software Manager allows you to:

- Manage and track licenses
- Move licenses across virtual account
- Remove registered product instance

Optionally, if Unified Communications Manager cannot connect directly to Cisco Smart Software Manager, you can deploy a proxy server to manage the connection.

Note If you are upgrading Unified Communications Manager registered to Cisco Smart Software Manager from Pre-15 releases to Release 15 or higher, Cisco Unified Communications Manager will not update the product version to 15 in the Cisco Smart Software Manager UI for the Product Instance. Refer to CSCwf94088 for more details.

For additional information about Cisco Smart Software Manager, go to https://software.cisco.com.

Cisco Smart Software Manager Satellite

Cisco Smart Software Manager satellite is an on-premise deployment that can handle your licensing needs if Unified Communications Manager cannot connect to cisco.com directly, either for security or availability reasons. When this option is deployed, Unified Communications Manager registers and report license consumption to the satellite, which synchronizes its database regularly with the backend Cisco Smart Software Manager that is hosted on cisco.com.

The Cisco Smart Software Manager satellite can be deployed in either Connected or Disconnected mode, depending on whether the satellite can connect directly to cisco.com.

- Connected—Used when there is connectivity to cisco.com directly from the Smart Software Manager satellite. Smart account synchronization occurs automatically.
- Disconnected—Used when there is no connectivity to cisco.com from the Smart Software Manager satellite. Smart Account synchronization must be manually uploaded and downloaded.

Note The Unified CM running in Dual Stack mode supports satellite configured with IPv4 and IPv6 address.

Note If you are upgrading Unified Communications Manager registered to Cisco Smart Software Manager Satellite from Pre-15 releases to Release 15 or higher, Cisco Unified Communications Manager will not update the product version to 15 in the Cisco Smart Software Manager UI for the Product Instance. Refer to CSCwf94088 for more details.

For Cisco Smart Software Manager satellite information and documentation, go to https://www.cisco.com/c/en/us/buy/smart-accounts/software-manager-satellite.html.

License Types

The following licensing types are available to cover your needs:

Cisco Unified Workspace Licensing

Cisco Unified Workspace Licensing (UWL) provides the most popular bundles of Cisco Collaboration applications and services in a cost-effective, simple package. It includes soft clients, applications server software, and licensing on a per-user basis.

Cisco User Connect Licensing

User Connect Licensing (UCL) is a per-user based license for individual Cisco Unified Communications applications, which includes the applications server software, user licensing, and a soft client. Depending on the type of device and number of devices that you require, UCL is available in Essential, Basic, Enhanced, and Enhanced Plus versions.

For more information about these license types and the versions in which they are available, see http://www.cisco.com/c/en/us/products/unified-communications/unified-communications-licensing/index.html.

Session Management Edition

Session Management Edition can be registered to either Cisco Smart Software Manager or Cisco Smart Software Manager satellite. You can register Session Management Edition using the same processes as

for Unified Communications Manager, register to a virtual account that Cisco Unified Communications Manager is registered or a separate virtual account, and fulfill a minimal set of licenses requirement.

Note The SME registered in Specific License Reservation (SLR) requires a minimum set of licenses reserved in CSSM while generating an SLR authorization code.

Product Instance Evaluation Mode

After installation, Unified Communications Manager runs under the 90-day evaluation period. At the end of the evaluation period, Unified Communications Manager stops allowing addition of new users or devices until registered with Cisco Smart Software Manager or Cisco Smart Software Manager satellite.

Note Evaluation period is before the product is registered.

Specific License Reservation

Specific License Reservation (SLR) allows the customer to reserve licenses from their virtual account, tie them to a devices UDI and use their device with these reserved licenses in a disconnected mode. The customer reserves specific licenses and counts for a UDI from their virtual account. The following options describe the new functionality and design elements for Specific Reservation.

Table 7: Specific License Reservation Commands

Command	Description
license smart reservation enable	Use this command to enable the license reservation feature.
license smart reservation disable	Use this command to disable the license reservation feature.
license smart reservation request	Use this command to generate reservation request code.
license smart reservation cancel	Use this command to cancel the reservation process before the authorization code is installed.
license smart reservation install "<authorization-code>"	Use this command to install the license reservation authorization-code generated on the Cisco Smart Software Manager.
license smart reservation return	Use this command to remove the license reservation authorization code that is installed and list of reserved entitlements. The device transitions back to an unregistered state.
license smart reservation return-authorization "<authorization code>"	Use this command to remove the license reservation authorization code that is entered by the user.

Note If you are upgrading from 12.0 to higher versions and enable license reservation feature on upgraded server, you should download `ciscocm-ucm-resetudi.k3.cop.sgn` from CCO and install on the upgraded CUCM before enabling reservation feature.

Note If you are upgrading the 12.5 system which is license reservation enabled to 14, see System Configuration Guide for Cisco Unified Communications Manager.

IM and Presence Service License Requirements

The IM and Presence Service does not require a server license or software version license. However, you must assign users and enable the IM and Presence Service for each assigned user.

Note With the Jabber for Everyone offer, no end user licenses are required to enable IM and Presence Service functionality. For more information, see Jabber for Everyone Quick Start Guide.

You can assign IM and Presence Service on a per user basis, regardless of the number of clients you associate with each user. When you assign IM and Presence Service to a user, this enables the user to send and receive IMs and availability updates. If users are not enabled for IM and Presence Service, they will not be able to log in to the IM and Presence Service server to view the availability of other users, send or receive IMs, and other users will not see their availability status.

You can enable a user for IM and Presence Service using any of the following options:

- The **End User Configuration** window in Unified Communications Manager. For more information, see the Administration Guide for Cisco Unified Communications Manager.
- The Bulk Administration Tool (BAT)
- Assign IM and Presence Service to a feature group template which you can reference from the **Quick User/Phone Add** window in Unified Communications Manager.

For more information, see the System Configuration Guide for Cisco Unified Communications Manager.

IM and Presence Service capabilities are included within both User Connect Licensing (UCL) and Cisco Unified Workspace Licensing (CUWL). IM and Presence Service capabilities can also be acquired for users that are not Unified Communications Manager IP Telephony users through the Jabber for Everyone Offer. For more information, see Jabber for Everyone Quick Start Guide.

Supporting Documentation

The following documents contain additional supporting information that helps you to upgrade in specific cases.

Task	
Setup virtualized Cisco hardware.	Refer to *Cisco Collaboration on Virtual Servers* in order to set up your virtualized platform. For details, see https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-guides-list.html.
Setup Cisco Business Edition 6000/7000 appliances	Refer to: • *Installation Guide for Cisco Business Edition 6000 and 7000*—https://www.cisco.com/c/en/us/support/unified-communications/business-edition-6000/tsd-products-support-series-home.html • *Installation Guide for Cisco Business Edition 6000 and 7000*—https://www.cisco.com/c/en/us/support/unified-communications/business-edition-7000/tsd-products-support-series-home.html
Replace existing hardware while preserving the configuration	*Replace a Single Server or Cluster for Cisco Unified Communications Manager* at https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-guides-list.html.
Review VMware requirements	For VMware requirements and best practices, go to https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/uc_system/virtualization/cisco-collaboration-virtualization.html. For VMware vendor documentation, go to http://www.VMware.com.
Additional Planning and Sizing Resources	These documents also contain information that may help you to plan and size your upgraded system: • *Cisco Collaboration Systems Solution Reference Network Designs (SRND)* for at http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-system/products-implementation-design-guides-list.html. • *Cisco Preferred Architecture* guides and *Cisco Validated Design* guides at http://www.cisco.com/c/en/us/solutions/enterprise/design-zone-collaboration/index.html. • Collaboration Virtual Machine Replacement Tool at http://ucs.cloudapps.cisco.com/. • Cisco Quote Collab Tool at http://www.cisco.com/go/quotecollab. • Cisco Collaboration Sizing Tool at http://tools.cisco.com/cucst.