Upgrade and Migration Guide for Cisco Unified Communications Manager and the IM and Presence Service, Release 15

First Published: 2023-12-18

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Full Cisco Trademarks with Software License

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

CONTENTS

CHAPTER 1

New and Changed Information

New and Changed Information

The following table provides an overview of the significant changes to the features in this guide up to this current release. The table does not provide an exhaustive list of all changes made to the guide or of the new features up to this release.

Table 1:

Date	Description	See
December 18, 2023	Unified Communications Manager and IM and Presence Service and all applications have moved to a 64-bit architecture. Some of the affected areas are: • Unified Communications Manager and IM and Presence Service 15 requires a minimum ESXi version of 7.0 U3 or 8.0 U1. • Release 15 of Unified Communications Manager supports only virtual disks of minimum 110 GB at install-time. Virtual disks of 80GB at install-time are not supported. • Direct Refresh Upgrades from Pre-12.5.x source to Release 15 is not supported. • Pre-upgrade Readiness COP File has new checks added for Unified Communications Manager and IM and Presence Service. • Unified Communications Manager and IM and Presence Service 15 supports only Open VM Tools. • IPSec policy with 3DES Algorithm is not supported in FIPS mode for Release 15.	• Requirements and Limitations, on page 17 • Virtual Machine Configuration, on page 18 • Supported Upgrade and Migration Paths with COP Files, on page 6 • Run Upgrade Readiness COP File (Pre-upgrade), on page 39 • Updating VMware Tools, on page 107 • IPSec Requirements, on page 28
December 18, 2023	You can upgrade Cisco Unified Real-Time Monitoring Tool (Unified RTMT) on workstations running on both Windows or Linux operating systems using a single 'CiscoRTMTPlugin.zip' plug-in.	Upgrade RTMT, on page 110

CHAPTER 2

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), on page 44 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 4.

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, on page 117.

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), on page 39.

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 2: 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, on page 117.

Table 3: 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, on page 35
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), on page 39 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), on page 53 **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 4: 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, on page 59 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 5: 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 6: 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 7:

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 8: 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.

CHAPTER 3

Upgrade Tasks

Upgrade Overview

Use the procedures in this chapter to complete one of the following upgrade types using either the Cisco Unified OS Admin GUI or the CLI. For procedures, refer to the task flow that covers your upgrade type.

- Clusterwide Upgrades (Direct Standard)—Pre-upgrade version must be 12.5(1) minimum. Otherwise, you must use the other method.
- Upgrade Cluster Nodes (Direct Standard)

Note Direct upgrades from pre-12.5 source to Release 15 is not supported.

Note If your Unified Communications Manager publisher node is on Release 15 and the subscribers nodes are in Release 12.5.x or 14 and SUs, the nodes in the cluster will not be authenticated. Only when the subscribers nodes are upgraded to Release 15, all the nodes will be in the authenticated state.

Note For upgrades and migrations that use Cisco Prime Collaboration Deployment, see the Cisco Prime Collaboration Deployment Administration Guide to set up an upgrade task or migration task.

Before You Begin

Caution Stop all configuration tasks. Don't make any configuration changes during the upgrade. For example, don't change passwords, perform LDAP synchronizations, or run any automated jobs. Don't remove, readd, or reinstall any nodes in the cluster during the upgrade process. You can make configuration changes only when you have completed the upgrade on all nodes and completed postupgrade tasks. The upgrade overwrites configuration changes that you make during the upgrade, and some configuration changes can cause the upgrade to fail.

We recommend that you suspend user synchronization with LDAP. Don't resume synchronization until you have completed the upgrade on all Unified Communications Manager and IM and Presence Service cluster nodes.

- Don't rename or compress the upgrade file. Otherwise, the system rejects the file as a valid upgrade file.
- For IM and Presence Service upgrades, check that the contact list size for users is below the maximum. Use the System Troubleshooter in Cisco Unified CM IM and Presence Administration to verify that no users have exceeded the limit.
- Modify the network adapter to VMXNET3 before the upgrade process. For details, see your OVA readme file.
- If you're upgrading a node in FIPS mode, make sure that your security password has a minimum of 14 characters. To change passwords, see the 'Reset the Administrator or Security Password' section in the "Getting Started" chapter of the Administration Guide for Cisco Unified Communications Manager.

Note From Release 12.5(1) SU2 onwards, it's recommended to perform both the upgrade stages [Install and Switch Version] during the same Maintenance Window to avoid an impact on the other AXL-dependent integrations.

Note During the switch version, only User Facing Features (UFF) in dynamic tables (numplandynamic, devicedynamic, and more) gets updated. Other tables are migrated during the upgrade. Any configuration changes after the upgrade or before the switch versions are lost.

Note In the upgrade logs, it's observed that there is time discrepancy or time jumps during certain intervals. This time jump is an expected behavior since the hardware clock is disabled until the system synchronizes with the NTP server.

Note

If you have different security passwords in the active and inactive versions, and when you switch back to a lower version, ensure that you change the security password in the lower version to be same as the higher version. Follow these steps to change the security password:

1. Switch the publisher node to a lower version.
2. Change the security password of the publisher node to the new password which is same as the higher version.
3. Switch the subscriber to a lower version.
4. Change the security password of the subscriber node to the new password which is same as the higher version.

Note

Use this procedure to verify the NTP configurations before you upgrade to Release 15:

1. Ensure that you always use an NTP source with lesser offset and jitter from a reliable source.
2. We recommend that you have one good NTP server configured for time synchronization. If you are configuring more than one NTP server, you must configure a minimum of four NTP servers so that chrony can have a tie breaker if each of the clocks is pointing to different time zones.
3. You must always upgrade ESXi to match the compatible versions supported by the Cisco Voice Operating System (VOS) servers.
4. During network migrations between different hosts, ensure that you use the same NTP source (OR) NTP source with a reliable clock.

Download Upgrade Files

Before you upgrade, download the files that you need:.

Note

To optimize the upgrade, make sure to save the downloaded files in the same directory.

Table 9: Upgrade Files to Download

Files to Download	Download Site
Unified CM Upgrade ISO	Go to Unified Communications Manager Downloads—Select your version and then look under **Unified Communications Manager Updates** for upgrade ISOs. For example, `UCSInstall_UCOS_<XXXXXXXX>.sha512.iso`.
IM and Presence Service Upgrade ISO	Go to IM and Presence Service Downloads—Select your version and look under **Unified Presence Server (CUP) updates** for upgrade ISOs. For example, `UCSInstall_CUP_<XXXXXXXX>.sha512.iso`.

Files to Download	Download Site
Upgrade Readiness COP Files (pre-upgrade and post-upgrade)	You can download the pre-upgrade COP file and post-upgrade COP file from either of the above download sites: • For Unified CM, the COP files appear under **Unified Communications Manager Updates** • For IM and Presence Servivce, the COP files appear under **Unified Presence Server (CUP) Updates > UTILS** For example, `ciscocm.preUpgradeCheck-XXXXX.cop.sgn` and `ciscocm.postUpgradeCheck-XXXXX.cop.sgn` **Note** When you try to upgrade, using COP files it shows the number of files installed in the system. Once the upgrade is done the list of COP files will not match previous versions. If you need the previous files you need to install COP files manually.

Clusterwide Upgrade Task Flow (Direct Standard)

Complete the following tasks to complete a simplified clusterwide upgrade. This will complete a clusterwide direct standard upgrade.

Note The Clusterwide Upgrade option is available only for direct standard upgrades where the pre-upgrade version is a minimum release of 12.5(1).

Note Ensure that you verify the software location details of each node before you start the upgrade process.

Before you begin

Download upgrade ISO files and Upgrade Readiness COP files and save them in the same directory. For download information, go to Download Upgrade Files, on page 37.

Procedure

	Command or Action	Purpose
Step 1	Run Upgrade Readiness COP File (Pre-upgrade), on page 39	Run the Upgrade Readiness COP file to check connectivity and health of the system. If there are issues, fix them before proceeding with the upgrade.
Step 2	Configure Clusterwide Reboot Sequence, on page 41	Specify the reboot sequence beforehand in order to minimize downtime.

	Command or Action	Purpose
Step 3	Configure Cluster Software Location, on page 41	Before upgrade, you can choose to configure the cluster software location details for all the nodes associated within the cluster.
Step 4	Upgrade the cluster using either one of these methods: • Complete Clusterwide Upgrade via OS Admin, on page 42 • Complete Clusterwide Upgrade via CLI, on page 43	During the upgrade, you can switch versions automatically as a part of the upgrade, or you can save the upgraded version to the inactive partition.
Step 5	Switch Version Manually (Clusterwide), on page 44	Optional. If you chose not to switch versions automatically during the upgrade, switch versions manually.
Step 6	Run Upgrade Readiness COP File (Post-upgrade), on page 45	Run the post-upgrade COP file to guage the post-upgrade health of your system.

Run Upgrade Readiness COP File (Pre-upgrade)

The Upgrade Readiness COP file checks for the following things:

- Installed COP Files
- Network services and connectivity (DNS, NTP, intra-cluster)
- Licensing sync
- VMware tools compatibility
- Hard disk partition size
- Swap size check
- Filesystem type and guest OS checks
- Usable Disk space for destination versions
- ESXi version check
- SIP and H.323 trunk registrations
- Database authentication and replication status
- Database sanity
- Status of last DRS backup
- Remote Call Control (RCC) feature status
- Services status
- Installed COPs and Locales
- Device Registration Status Count

- Enterprise Parameter and Service Parameters settings
- TFTP Maximum Service Counts
- Active and Inactive versions
- List the expired certificates
- FIPS mode password length restrictions
- IPSec Policy configuration check for ESP and Encryption Algorithm in FIPS mode

Note

- It's strongly recommended that you run the Upgrade Readiness COP file before you upgrade as it reduces significantly the chances of a failed upgrade.
- The COP file is fully supported where the pre-upgrade version is 10.x or later.
- Since the 3DES Algorithm isn't supported in FIPS mode, you must delete the IPSec policy with the 3DES Algorithm and recreate the IPSec policy with the Encryption and ESP Algorithms other than 3DES in both the nodes where IPSec tunnel is to be established.

Procedure

Step 1 Download the Upgrade Readiness COP file to run pre upgrade tests.

a) Go to the Downloads site.
b) Select the destination release and then select **Unified Communications Manager Utilities**.
c) Download the **Upgrade Readiness COP file in order to run pre-upgrade tests** (For example, `ciscocm.preUpgradeCheck-00019.cop.sgn`. Note that the latest file may have a different filename and version).

Step 2 Check your system readiness for upgrades:

a) Run the COP file.
b) Resolve any issues that the COP file returns.
c) Run the COP file again.
d) Repeat this process until the COP file returns no errors.

Step 3 Install the cop file from GUI or CLI. Once the installation is complete, from CLI run **file view install PreUpgradeReport.txt** to view the report.

Step 4 To view the report from RTMT

a) Log in into RTMT.
b) In **Trace and Log Central** double click on **Remote Browse** and select **Trace files** and click **Next**.
c) Select **Select all Services on all servers** and click **Next**.
d) Click **Finish** and **Close**.
e) Double-click on nodes, expand **CUCM Publisher** > **System** > **Install upgrade Logs**.
f) Double-click on **Install** and select the file which you require and download.

Configure Clusterwide Reboot Sequence

For simplified cluster-wide upgrades, use this procedure before you upgrade to set the reboot sequence for the cluster upgrade. This option is available only if the pre-upgrade version is 12.5(1) minimum.

Note If you don't configure a reboot sequence, the clusterwide upgrade uses the last saved reboot sequence or the default sequence.

Procedure

Step 1 On the publisher node, login to Cisco Unified OS Administration or Cisco Unified CM IM and Presence OS Administration.

Step 2 Choose **Software Upgrades** > **Restart/Switch-Version Cluster**.
The **Reboot Cluster Settings** window appears with sliders that display the reboot sequence per node.

Step 3 Use the sliders to adjust the reboot sequence according to your needs.

Step 4 Click **Save**.

What to do next

Complete one of the following tasks, depending on which interface you want to use:

- Complete Clusterwide Upgrade via OS Admin, on page 42
- Complete Clusterwide Upgrade via CLI, on page 43

Configure Cluster Software Location

Use this procedure to add, edit, or modify any of the existing configurations for a node in the same cluster.

Note You may only use this feature if all the nodes in your cluster are Release 14SU2 or later.

Procedure

Step 1 Log in to **Cisco Unified OS Administration** user interface.

Step 2 Choose **Software Upgrades > Cluster Software Location**.

Step 3 Select a node to add or edit the server location details from the list.

Step 4 Check the **Apply to All Nodes** check box if you want the same software location details to be applied for all the other nodes in the cluster including the publisher.

This check box is displayed only when you select the Unified CM publisher from the **Select Node** drop-down list.

Step 5 Use the **Use download credentials and software location from Publisher** if you want to use the source configuration and software location details from the publisher node.

By default, the **Use download credentials and software location from Publisher** option is selected.

Note This option is available only for the subscriber nodes.

Step 6 (Optional) If you do not want to use the **Use download credentials and software location from Publisher** option, use the **Use below download credentials and software location** option before you upgrade your server.

Note This option is available only for the subscriber nodes.

Step 7 From the **Source** drop-down list, select the option that matches where the upgrade file is saved:

- **DVD/CD**
- **Local filesystem**—This option is available only if you are resuming a previous upgrade that was cancelled
- **SFTP server**—You must also enter the SFTP server details, including the Directory, Server address and login credentials.

Step 8 (Optional) To receive an email notification when the upgrade is complete, enter the **SMTP Server** address and an **Email Destination** so that you can be emailed when the upgrade completes.

Step 9 Check the **Continue with upgrade after download** check box if you want the upgrade to commence automatically once the upgrade file is downloaded. If you don't check this check box, you will need to manually initiate the upgrade later using **Local filesystem** as the **Source**.

Step 10 Check the **Switch-version server after upgrade (valid only for ISO)** check box to reboot the system automatically after the completion of successful upgrade.

Step 11 Click **Save** to update all the configuration changes for that particular node that is added or modified.

Complete Clusterwide Upgrade via OS Admin

Use this procedure to complete a simplified clusterwide upgrade of Unified Communications Manager and the IM and Presence Service. This option is available for standard upgrades only where the pre-upgrade version is 12.5(1) or later.

Note You can also complete a standard clusterwide upgrade by running the `utils system upgrade cluster` CLI command.

Before you begin

Make sure that you have downloaded the upgrade file to a location that you can access.

Procedure

Step 1 Log in to **Cisco Unified OS Administration** or **Cisco Unified IM and Presence OS Administration**.

Step 2 Choose **Software Upgrades > Install/Upgrade Cluster**. This option is not available if the From version is pre-12.5(1).

Step 3 You can view the following configuration information required to upgrade an existing node:

Note In Release 14 SU2 and later, Software Location settings for all cluster nodes are centrally managed from the Publisher instead of locally on each cluster node. If you want to add, edit, or modify any of the existing configurations for any node in the same cluster, navigate to the **Software Upgrades > Cluster Software Location** menu from the Cisco Unified OS Administration user interface.

- **Credentials Information—**Displays the credentials of the server on which the upgrade image is saved.
- **Upgrade file source**— Displays the location for the server where your upgrade file is saved. You can upgrade from a local source (CD or DVD), or you can use FTP or SFTP to download a remote upgrade file, or if you want to resume an upgrade after a cancel operation, you can use the previously downloaded upgrade file through the local image source option.
- **Continue with upgrade after download**—Indicates the option selected whether you wanted the upgrade to proceed automatically once the upgrade file is downloaded (the default value is yes). If you had chosen to upgrade automatically, no checksum or SHA details get displayed. If you had set the value of to yes or no, the setting remains in the system.
- **Version switching**—Displays the option selected whether you wanted to switch to the new version automatically once the upgrade completes (the default value is no). If you had entered yes, the system switches to the new version and reboots automatically after the upgrade completes. If you had set the value to yes or no, the setting remains in the system.

Step 4 Click **Next**.

Step 5 Select the upgrade version that you want to install, and click **Next**.
The upgrade commences. The **Installation Status** page displays information about the upgrade.

Note During cluster wide upgrade, make sure to have the first 3 digits common between the selected Unified Communications Manager and IM and Presence Service upgrade files.

Step 6 Click **Finish** when the upgrade completes.
If you chose to switch versions automatically, the cluster reboots to the upgraded version according to the cluster reboot sequence. Otherwise, the upgrade saves to the inactive partition and you must switch versions manually in order to use the upgraded software.

Complete Clusterwide Upgrade via CLI

Use this procedure to complete a simplified clusterwide upgrade using the Command Line Interface.

Note This option is available only for direct standard upgrades where the pre-upgrade version is Release 12.5(x) or later.

Before you begin

Configure Clusterwide Reboot Sequence, on page 41—If you want to switch versions automatically after the upgrade, set the reboot sequence beforehand. Otherwise, the cluster reboots using the last saved sequence. If no reboot sequence has been saved, the default sequence is used.

Note In Release 14 SU2 and later, Software Location settings for all cluster nodes are centrally managed from the Publisher instead of locally on each cluster node. If you want to add, edit, or modify any of the existing configurations for any node in the same cluster, navigate to the **Software Upgrades** > **Cluster Software Location** menu from the Cisco Unified OS Administration user interface before you begin to upgrade your system.

Procedure

Step 1 Log in to the Command Line Interface on the Unified CM publisher node.

Step 2 Run the `utils system upgrade cluster` CLI command and the wizard displays the software location details to configure all the nodes in the same cluster.

Step 3 You can view the following configuration information required to upgrade an existing node:

- **Credentials Information—**Displays the credentials of the server on which the upgrade image is saved.
- **Upgrade file source**— Displays the location for the server where your upgrade file is saved. You can upgrade from a local source (CD or DVD), or you can use FTP or SFTP to download a remote upgrade file, or if you want to resume an upgrade after a cancel operation, you can use the previously downloaded upgrade file through the local image source option.
- **Continue with upgrade after download**—Indicates the option selected whether you wanted the upgrade to proceed automatically once the upgrade file is downloaded (the default value is yes). If you had chosen to upgrade automatically, no checksum or SHA details get displayed. If you had set the value of to yes or no, the setting remains in the system.
- **Version switching**—Displays the option selected whether you wanted to switch to the new version automatically once the upgrade completes (the default value is no). If you had entered yes, the system switches to the new version and reboots automatically after the upgrade completes. If you had set the value to yes or no, the setting remains in the system.

Step 4 If you are prompted to start the installation, enter **Yes**.
If you chose to switch versions automatically after the upgrade, the cluster reboots to the upgraded version after the upgrade. Otherwise, the upgrade saves to the inactive partition and you can switch versions manually later.

Switch Version Manually (Clusterwide)

Use this procedure for Direct Standard Upgrades where you switch the inactive and active versions across all cluster nodes through the Unified Communications Manager publisher node without having to UI or CLI to any other nodes.

Note You can use this procedure only for:

- Direct Standard Upgrades
- Using Simple Upgrades cluster-wide automation
- Pre-upgrade version 12.5(1) or later

Note The Add/update/delete functionalities will not be allowed as one or more cluster nodes are not yet finished with one or more of upgrading the inactive versions, switch-version reboots and database replication. From the Cisco Unified OS Administration UI, navigate to **Software Upgrade > Install/Upgrade** or **Software Upgrade > Cluster Install/Upgrade** to view the upgrade status. Or, execute the commands **utils system upgrade status** or **utils system cluster upgrade status** to monitor the upgrade status. See Upgrade and Migration Overview, on page 3 for more information.

Procedure

Step 1 Log in to Cisco Unified OS Administration or Cisco Unified CM IM and Presence OS Administration.

Step 2 Choose **Software Upgrades** > **Reboot Cluster**.

Step 3 Optional. If you haven't already configured the reboot sequence, use the sliders to edit the reboot sequence and click **Save**.

Step 4 Click **Switch Versions**.

Note If you prefer to use CLI, note that there is no CLI for Simple Upgrades cluster switch version automation. You can instead use the single-node switch version with the `utils system switch-version` CLI command, but this must be done on a node-by-node basis.

Run Upgrade Readiness COP File (Post-upgrade)

After upgrading, run the post-upgrade COP file, which checks the following:

- Installed COP Files
- Network services and connectivity (DNS, NTP, intra-cluster)
- FIPS mode password length restrictions
- Licensing sync
- VMware tools compatibility
- Disk space

- SIP and H.323 trunk registrations
- Database authentication and replication status
- Database sanity
- Status of last DRS backup
- Services status
- Installed COPs and Locales
- Device Registration Status Count
- Enterprise Parameter and Service Parameter settings
- TFTP Maximum Service Counts
- Active and Inactive versions

Note It's strongly recommended that you run the Upgrade Readiness COP file for post-upgrade checks after you upgrade in order to verify the health of your system.

Procedure

Step 1 Download the Upgrade Readiness COP file to run post upgrade tests.

a) Go to the Downloads site.
b) Select the destination release and then select **Unified Communications Manager Utilities**.
c) Download the **Upgrade Readiness COP file in order to run pre-upgrade tests** (For example, `ciscocm.postUpgradeCheck-00019.cop.sgn`. Note that the latest file may have a different filename and version.).

Step 2 Check your post-upgrade system health:

a) Run the COP file.
b) Resolve any issues that the COP file returns.
c) Repeat these steps until the COP file returns no errors.

Step 3 To view the reports from CLI for post-upgrade run **file get install/PostUpgradeReport.txt** command.

Step 4 To view the report from RTMT

a) Login into RTMT.
b) In **Trace and Log Central** double click on **Remote Browse** and select **Trace files** click **Next**.
c) Select **Select all Services on all servers** and click **Next**.
d) Click **Finish** and **Close**.
e) Double click on nodes, expand **CUCM Publisher** > **System** > **Install upgrade Logs**.
f) Double click on **Install** and select the file which you require and download.

What to do next

The upgrade is complete. You can begin using the new software.

Upgrade Cluster Nodes (Direct Standard)

Complete these tasks to upgrade cluster nodes on a node by node basis. You must use this process if you are completing a direct standard upgrade using the Unified OS Admin or CLI interfaces.

Note Direct Refresh Upgrades from Pre-12.5.x source to Release 15 is not supported. You might first upgrade your source to Release 12.5.x or 14 and SUs and then upgrade your source to Release 15.

Before you begin

Download upgrade ISO files and Upgrade Readiness COP files and save them in the same directory. For download information, go to Download Upgrade Files, on page 37.

Procedure

	Command or Action	Purpose
Step 1	Run Upgrade Readiness COP File (Pre-upgrade), on page 39	Run the Upgrade Readiness COP file to check connectivity and health of the system. If there are issues, fix them before proceeding with the upgrade.
Step 2	Configure Cluster Software Location, on page 41	Before upgrade, you can choose to configure the cluster software location details for all the nodes associated within the cluster.
Step 3	Upgrade cluster nodes using either the GUI or CLI interfaces. • Upgrade Cluster Nodes via OS Admin (Direct Standard), on page 50 • Upgrade Cluster Nodes via CLI (Direct Standard), on page 51	Upgrade the cluster nodes in your cluster.
Step 4	Switch Versions Manually, on page 53	Optional. If you did not switch versions automatically during the upgrade, use this procedure to switch versions manually.
Step 5	Run Upgrade Readiness COP File (Post-upgrade), on page 53	After the upgrade, run the post-upgrade COP file to gauge the post-upgrade health of your system.

Run Upgrade Readiness COP File (Pre-upgrade)

The Upgrade Readiness COP file checks for the following things:

- Installed COP Files
- Network services and connectivity (DNS, NTP, intra-cluster)
- Licensing sync
- VMware tools compatibility
- Hard disk partition size
- Swap size check
- Filesystem type and guest OS checks
- Usable Disk space for destination versions
- ESXi version check
- SIP and H.323 trunk registrations
- Database authentication and replication status
- Database sanity
- Status of last DRS backup
- Remote Call Control (RCC) feature status
- Services status
- Installed COPs and Locales
- Device Registration Status Count
- Enterprise Parameter and Service Parameters settings
- TFTP Maximum Service Counts
- Active and Inactive versions
- List the expired certificates
- FIPS mode password length restrictions
- IPSec Policy configuration check for ESP and Encryption Algorithm in FIPS mode

Note

- It's strongly recommended that you run the Upgrade Readiness COP file before you upgrade as it reduces significantly the chances of a failed upgrade.
- The COP file is fully supported where the pre-upgrade version is 10.x or later.
- Since the 3DES Algorithm isn't supported in FIPS mode, you must delete the IPSec policy with the 3DES Algorithm and recreate the IPSec policy with the Encryption and ESP Algorithms other than 3DES in both the nodes where IPSec tunnel is to be established.

Procedure

Step 1 Download the Upgrade Readiness COP file to run pre upgrade tests.

a) Go to the Downloads site.
b) Select the destination release and then select **Unified Communications Manager Utilities**.
c) Download the **Upgrade Readiness COP file in order to run pre-upgrade tests** (For example, `ciscocm.preUpgradeCheck-00019.cop.sgn`. Note that the latest file may have a different filename and version).

Step 2 Check your system readiness for upgrades:

a) Run the COP file.
b) Resolve any issues that the COP file returns.
c) Run the COP file again.
d) Repeat this process until the COP file returns no errors.

Step 3 Install the cop file from GUI or CLI. Once the installation is complete, from CLI run **file view install PreUpgradeReport.txt** to view the report.

Step 4 To view the report from RTMT

a) Log in into RTMT.
b) In **Trace and Log Central** double click on **Remote Browse** and select **Trace files** and click **Next**.
c) Select **Select all Services on all servers** and click **Next**.
d) Click **Finish** and **Close**.
e) Double-click on nodes, expand **CUCM Publisher** > **System** > **Install upgrade Logs**.
f) Double-click on **Install** and select the file which you require and download.

Configure Cluster Software Location

Use this procedure to add, edit, or modify any of the existing configurations for a node in the same cluster.

Note You may only use this feature if all the nodes in your cluster are Release 14SU2 or later.

Procedure

Step 1 Log in to **Cisco Unified OS Administration** user interface.

Step 2 Choose **Software Upgrades** > **Cluster Software Location**.

Step 3 Select a node to add or edit the server location details from the list.

Step 4 Check the **Apply to All Nodes** check box if you want the same software location details to be applied for all the other nodes in the cluster including the publisher.

This check box is displayed only when you select the Unified CM publisher from the **Select Node** drop-down list.

Step 5 Use the **Use download credentials and software location from Publisher** if you want to use the source configuration and software location details from the publisher node.

By default, the **Use download credentials and software location from Publisher** option is selected.

Note This option is available only for the subscriber nodes.

Step 6 (Optional) If you do not want to use the **Use download credentials and software location from Publisher** option, use the **Use below download credentials and software location** option before you upgrade your server.

Note This option is available only for the subscriber nodes.

Step 7 From the **Source** drop-down list, select the option that matches where the upgrade file is saved:

- **DVD/CD**
- **Local filesystem**—This option is available only if you are resuming a previous upgrade that was cancelled
- **SFTP server**—You must also enter the SFTP server details, including the Directory, Server address and login credentials.

Step 8 (Optional) To receive an email notification when the upgrade is complete, enter the **SMTP Server** address and an **Email Destination** so that you can be emailed when the upgrade completes.

Step 9 Check the **Continue with upgrade after download** check box if you want the upgrade to commence automatically once the upgrade file is downloaded. If you don't check this check box, you will need to manually initiate the upgrade later using **Local filesystem** as the **Source**.

Step 10 Check the **Switch-version server after upgrade (valid only for ISO)** check box to reboot the system automatically after the completion of successful upgrade.

Step 11 Click **Save** to update all the configuration changes for that particular node that is added or modified.

Upgrade Cluster Nodes via OS Admin (Direct Standard)

Use this procedure to complete a direct standard upgrade of Cisco Unified Communications Manager or IM and Presence Service cluster nodes.

Note Some upgrade options may differ slightly depending on which version you are upgrading from.

Note Direct Refresh Upgrades from Pre-12.5.x source to Release 15 is not supported. You might first upgrade your source to Release 12.5.x or 14 and SUs and then upgrade your source to Release 15.

Procedure

Step 1 Log in to **Cisco Unified OS Administration** or **Cisco Unified IM and Presence OS Administration**.

Step 2 Choose **Software Upgrades > Install/Upgrade**.

Step 3 You can view the following configuration information required to upgrade an existing node:

Note In Release 14SU3 and later, Software Location settings for all cluster nodes are centrally managed from the Publisher instead of locally on each cluster node. If you want to add, edit, or modify any of the existing configurations for any node in the same cluster, navigate to the **Software Upgrades** > **Cluster Software Location** menu from the Cisco Unified OS Administration user interface before you begin to upgrade your system.

- **Credentials Information**—Displays the credentials of the server on which the upgrade image is saved.
- **Upgrade file source**—Displays the location for the server where your upgrade file is saved. You can upgrade from a local source (CD or DVD), or you can use FTP or SFTP to download a remote upgrade file, or if you want to resume an upgrade after a cancel operation, you can use the previously downloaded upgrade file through the local image source option.
- **Continue with upgrade after download**—Indicates the option selected whether you wanted the upgrade to proceed automatically once the upgrade file is downloaded (the default value is yes). If you had chosen to upgrade automatically, no checksum or SHA details get displayed. If you had set the value of to yes or no, the setting remains in the system.
- **Version switching**—Displays the option selected whether you wanted to switch to the new version automatically once the upgrade completes (the default value is no). If you had entered yes, the system switches to the new version and reboots automatically after the upgrade completes. If you had set the value to yes or no, the setting remains in the system.

Step 4 Click **Next**.

Step 5 Select the upgrade version that you want to install, and click **Next**.
The upgrade commences. The **Installation Status** page displays information about the upgrade.

Step 6 Click **Finish** when the upgrade completes.
If you chose to switch versions automatically after the upgrade, the node reboots to the upgraded version after the upgrade. Otherwise, the upgrade saves to the inactive partition and you can switch versions manually later.

Step 7 Repeat this procedure for additional cluster nodes.

Upgrade Cluster Nodes via CLI (Direct Standard)

Use this procedure to upgrade individual cluster nodes via the CLI.

Note Upgrade options may differ depending on which version you are upgrading from.

Note Direct Refresh Upgrades from Pre-12.5.x source to Release 15 is not supported. You might first upgrade your source to Release 12.5.x or 14 and SUs and then upgrade your source to Release 15.

Note In Release 14SU3 onwards, Software Location settings for all cluster nodes are centrally managed from the Publisher instead of locally on each cluster node. If you want to add, edit, or modify any of the existing configurations for any node in the same cluster, navigate to the **Software Upgrades** > **Cluster Software Location** menu from the Cisco Unified OS Administration user interface before you begin to upgrade your system.

Procedure

Step 1 Log in to the Command Line Interface on the node that you want to upgrade.

Step 2 Run the `utils system upgrade initiate` CLI command and the wizard displays the software location details to configure all the nodes in the same cluster.

Step 3 When prompted, choose one of the following:

- If you choose **Yes**, the upgrade process checks for the upgrade files that you can use as the source file and proceeds to step **8**.
- If you choose **No**, you are prompted to choose the source (follow steps **4** to **8**).

Step 4 When prompted, choose the source where the upgrade file is saved:

- **Remote filesystem via SFTP or FTP**—You will be prompted to enter the server details and credentials.
- **Local DVD/CD**—The local CD or DVD only.
- **Local image**—This option is available only if you initiated an upgrade earlier and did not complete the upgrade.

Step 5 (Optional) Enter an **SMTP Host** for email notifications that tell you when the upgrade is complete.

Step 6 When prompted, enter whether to proceed with the upgrade automatically after the upgrade file downloads.

- **Yes**—The upgrade commences once the file downloads to all nodes.
- **No**—The upgrade file gets saved as a Local Image. You can restart the upgrade later.

Step 7 When prompted, enter whether to switch versions automatically after the upgrade:

- **Yes**—After the upgrade, the cluster switches to the new version and reboots automatically.
- **No**—The upgrade saves to the Inactive Partition. You can switch versions manually later.

Step 8 When prompted to start the installation, enter **Yes**.
If you chose to switch versions automatically after the upgrade, the node reboots to the upgraded version after the upgrade. Otherwise, the upgrade saves to the inactive partition and you can switch versions manually later.

Switch Versions Manually

If you did not switch versions automatically as a part of the upgrade, you can use this procedure to switch versions for cluster nodes manually. You can use either the GUI or the CLI.

Note The clusterwide version switch option is available only for direct standard upgrades where the pre-upgrade version is a minimum release of 12.5(x). For details, Switch Version Manually (Clusterwide), on page 44

Procedure

Step 1 If you want to use the GUI:

a) Log in to the Cisco Unified OS Administration or Cisco Unified IM and Presence OS Administration interface for the node that you want to switch and do the following:
b) Choose **Settings** > **Version**.
c) Verify the version of the active and inactive software.
d) Click **Switch Version**s to switch versions and restart the node.
e) Repeat these steps for additional cluster nodes.

Step 2 If you want to use the CLI:

a) Log in to the Command Line Interface for the node.
b) Run the `utils system switch-version` CLI command.
c) Repeat these steps for additional cluster nodes.

Run Upgrade Readiness COP File (Post-upgrade)

After upgrading, run the post-upgrade COP file, which checks the following:

- Installed COP Files
- Network services and connectivity (DNS, NTP, intra-cluster)
- FIPS mode password length restrictions
- Licensing sync
- VMware tools compatibility
- Disk space
- SIP and H.323 trunk registrations
- Database authentication and replication status
- Database sanity
- Status of last DRS backup
- Services status

- Installed COPs and Locales
- Device Registration Status Count
- Enterprise Parameter and Service Parameter settings
- TFTP Maximum Service Counts
- Active and Inactive versions

Note It's strongly recommended that you run the Upgrade Readiness COP file for post-upgrade checks after you upgrade in order to verify the health of your system.

Procedure

Step 1 Download the Upgrade Readiness COP file to run post upgrade tests.

a) Go to the Downloads site.
b) Select the destination release and then select **Unified Communications Manager Utilities**.
c) Download the **Upgrade Readiness COP file in order to run pre-upgrade tests** (For example, `ciscocm.postUpgradeCheck-00019.cop.sgn`. Note that the latest file may have a different filename and version.).

Step 2 Check your post-upgrade system health:

a) Run the COP file.
b) Resolve any issues that the COP file returns.
c) Repeat these steps until the COP file returns no errors.

Step 3 To view the reports from CLI for post-upgrade run **file get install/PostUpgradeReport.txt** command.

Step 4 To view the report from RTMT

a) Login into RTMT.
b) In **Trace and Log Central** double click on **Remote Browse** and select **Trace files** click **Next**.
c) Select **Select all Services on all servers** and click **Next**.
d) Click **Finish** and **Close**.
e) Double click on nodes, expand **CUCM Publisher** > **System** > **Install upgrade Logs**.
f) Double click on **Install** and select the file which you require and download.

What to do next

The upgrade is complete. You can begin using the new software.

Switch Cluster to Previous Version

To switch a cluster back to a previous version, complete these high-level tasks:

Procedure

Step 1 Switch back the publisher node.

Step 2 Switch back all backup subscriber nodes.

Step 3 Switch back all primary subscriber nodes.

Step 4 If you are reverting to an older product release, reset database replication within the cluster.

Switch Node to Previous Version

Procedure

Step 1 Log in to the management software for the node that you are upgrading:

- If you are upgrading an IM and Presence Service node, log in to Cisco Unified IM and Presence Operating System Administration.
- If you are upgrading a Unified Communications Manager node, log in to Cisco Unified Communications Operating System Administration.

Step 2 Choose **Settings** > **Version**.

The Version Settings window displays.

Step 3 Click the **Switch Versions** button.

After you verify that you want to restart the system, the system restarts, which might take up to 15 minutes.

Step 4 To verify that the version switch was successful, follow these steps:

a) Log in again to the management software for the node that you are upgrading.

b) Choose **Settings** > **Version**.

The Version Settings window displays.

c) Verify that the correct product version is now running on the active partition.

d) Verify that all activated services are running.

e) For the publisher node, log in to Cisco Unified CM Administration.

f) Verify that you can log in and that your configuration data exists.

Reset Database Replication

If you switch back the servers in a cluster to run an older product release, you must manually reset database replication within the cluster.

Procedure

Step 1 Log in to the Command Line Interface on the publisher node.

Step 2 Run the `utils dbreplication reset all` command.

PART I

Appendix

CHAPTER 4

Change the Virtualization Software

Complete the procedures in this appendix only if your upgrade requires you to update your VMware.

Virtual Machine Configuration Tasks

Use the procedures in this chapter if you need to change your virtual machine configuration to meet the requirements of the software version that you are upgrading to.

Before you begin

Verify whether you need to upgrade your virtual machine to meet the requirements of the new release. You can find the requirements by going to Cisco Collaboration Virtualization and following the links for the Unified Communications Manager and IM and Presence Service applications.

Procedure

	Command or Action	Purpose
Step 1	Install and Configure VMware vCenter, on page 60	VMware vCenter is required only when you are migrating from Cisco Business Edition or Tested Reference Configuration (TRC) hardware to UC on UCS specs-based or third-party server specs-based hardware. If you require VMware vCenter, install and configure it first. Using VMware vCenter is optional when you deploy Unified Communications Manager or IM and Presence Service on UC on UCS tested reference configuration hardware.
Step 2	Upgrade vSphere ESXi, on page 61	You must install a version of vSphere ESXi hypervisor that meets the requirements of the release. We recommend that you upgrade the ESXi hypervisor before you begin an upgrade of Unified Communications Manager or IM and

	Command or Action	Purpose
		Presence Service; however, if your currently installed version of these applications is not compatible with the ESXi version required for the new release, you can upgrade the ESXi version after you upgrade the Cisco applications.
Step 3	Download and Install OVA Templates, on page 61	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. This procedure is optional. If you are already running Unified Communications Manager or IM and Presence Service on a virtual machine, and your deployment size has not changed, you do not need to download and install a new OVA template. If you are changing the size of your system, download and install an OVA template for the new release that is sized for your deployment.
Step 4	Change Virtual Machine Configuration Specifications, on page 62	Use this procedure when you need to change the vCPU, vRAM, vDisk size, or vNIC type on your virtual machine (VM) in order to upgrade to a new release of Unified Communications Manager or IM and Presence Service. Do this step for only for direct upgrades, which use either the Unified CM OS Admin interface or the PCD Upgrade task to perform the upgrade.
Step 5	Migrate From Single to Multi-vDisk Virtual Machine, on page 63	Use this procedure if you are migrating to a larger virtual machine (VM) deployment that requires multiple vDisks.

Install and Configure VMware vCenter

Using VMware vCenter is optional when you deploy Unified Communications Manager or IM and Presence Service 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.

VMware vCenter allows you to collect performance data. For information about how to install and configure the application, see the VMWare documentation.

Procedure

Step 1 Install VMware vCenter.

Step 2 Set the level of detail tracked by the performance statistics. The statistics levels range from 1 to 4, with level 4 containing the most data. On a UCS specs-based or HP/IBM specs-based deployment, you must set the statistics level to 4.

Step 3 View the data size estimates to ensure there is enough space to keep all statistics.

Upgrade vSphere ESXi

Use the following procedure when you need to update your vSphere ESXi hypervisor in order to upgrade to a new release of Unified Communications Manager.

Procedure

Step 1 Move the virtual machine that is running Unified Communications Manager off the host server using one of the following methods:

- If you have a hot standby host, use vMotion to migrate the virtual machine from one physical server to another.
- If you do not have a hot standby host, power down the virtual machine and copy it to a different location.

Step 2 Upgrade the vSphere ESXi using the upgrade procedures provided by VMware.

Step 3 Verify that the vSphere ESXi upgraded successfully.

Step 4 Move the virtual machine that is running Unified Communications Manager back to the host server using one of the following methods:

- If you have a hot standby host, use vMotion to migrate the virtual machine from one physical server to another.
- If you do not have a hot standby host, power down the virtual machine and copy it the host server.

Download and Install 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. 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/cisco-collaboration-virtualization.html.

This procedure is optional. If you are already running Unified Communications Manager or IM and Presence Service on a virtual machine, and your deployment size has not changed, you do not need to download and install a new OVA template. If you are changing the size of your system, download and install an OVA template that is sized for your deployment.

Procedure

Step 1 Locate the OVA template for your release:

- For Unified Communications Manager, go to https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/uc_system/virtualization/cisco-collaboration-virtualization.html and search for the topic "Virtualization for Cisco Unified Communications Manager."
- For IM and Presence Service, go to https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/uc_system/virtualization/cisco-collaboration-virtualization.html and search for the topic "Virtualization for Unified CM IM and Presence."

Step 2 To download a single OVA file, click the **Download File** button next to that file. To download multiple OVA files, click the **Add to Cart** button next to each file that you want to download, then click on the **Download Cart** link.

Step 3 Click the **Proceed with Download** button on the **Download Cart** page.

Step 4 Read the information on the **Software License Agreement** page and click the **Agree** button.

Step 5 Click on one of the following links:

- **Download Manager** (requires Java)
- **Non Java Download Option**

A new browser window appears.

Step 6 Save the file:

- If you selected **Download Manager**, a **Select Location** dialog box appears. Specify the location where you want to save the file, and click **Open** to save the file to your local machine.
- If you selected **Non Java Download Option**, click the **Download** link on the new browser window. Specify the location and save the file to your local machine

Change Virtual Machine Configuration Specifications

Use the following procedure when you need to change the vCPU, vRAM, vDisk, or vNIC on your virtual machine (VM) in order to upgrade to a new release of Unified Communications Manager or IM and Presence Service.

For information about VM requirements, see the Readme file with the OVA template that supports your release. For details about OVA templates and requirements, go to www.cisco.com go virtualized-collaboration and search on the topic "Implementing Virtualization Deployments."

Before you begin

If you need to increase the vDisk storage space, you must remove your Virtual Machine (VM) snapshots before you being. Otherwise, the increase disk size option is greyed out. See Working with Snapshots.

Procedure

Step 1 Perform a Disaster Recovery System (DRS) backup.

Step 2 (Optional) For an upgrade from 9.x or earlier, if you need to increase the vDisk space to meet the space requirements of a refresh upgrade, install the following COP file:

```
ciscocm.vmware-disk-size-reallocation-<latest_version>.cop.sgn
```

Note Refresh Upgrades from Pre-12.5.x source to Release 15 is not supported.

Step 3 Shut down the virtual machine.

Step 4 Change the configuration of the virtual machine as needed:

a) Change the Guest OS version to match the requirements of the new release.
b) To change the vCPU, make the change in vSphere Client. Ensure that you change the reservation value to match the specifications of the new release.
c) To change the vRAM, make the change in vSphere Client. Ensure that you change the reservation value to match the specifications of the new release.
d) To increase the vDisk space, edit the storage size using vSphere Client. If the virtual machine has two disks, expand the second one.

   The new space is automatically added to the common partition when you restart the virtual machine.

   Note You need to change the disk size changes only if you need additional space to complete the upgrade. The disk space requirements are specified in the Readme file for the OVA template.

   Expanding the disk size to add space to the common partition will not increase the user capacity of your system. If you need to extend the user capacity of your system, you must migrate from a single-disk to a multi-disk virtual machine.

   If you need to shrink the vDisk or change the vDisk quantity, you must re-install the vDisk or install a new vDisk.

e) In vSphere Client, verify that the Network Adapter is configured to use the VMXNET 3 Adapter type. If the Network Adapter is set to a different type, modify it.

For more information about making configuration changes using vSphere Client, refer to the user manual for the product.

Step 5 Proceed with the upgrade and then power on the virtual machine.

Migrate From Single to Multi-vDisk Virtual Machine

If you are migrating to a larger virtual machine (VM) deployment that requires multiple vDisks, perform the following procedure. After you complete this procedure, you must Change Virtual Machine Configuration Specifications, on page 62 to ensure that the specifications match the requirements of the release.

Procedure

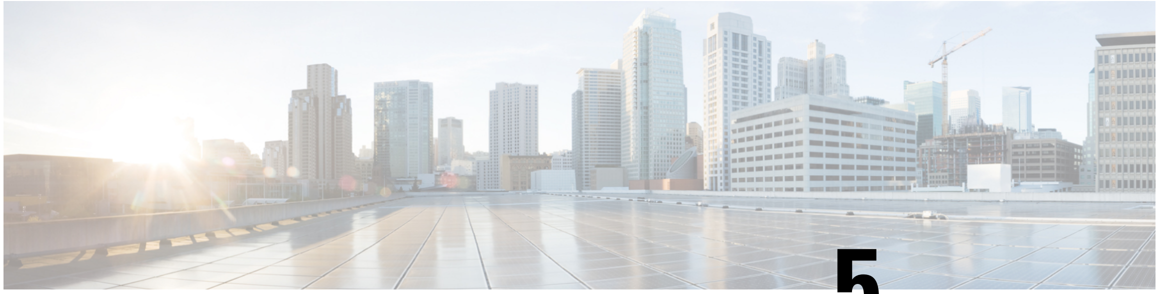
Step 1 Use the Disaster Recovery System (DRS) to perform a backup of the existing virtual machine (VM).

Step 2 Power off the existing VM and remove it from the network.

Step 3 Deploy a new VM at the correct user count using the appropriate OVA template.

Step 4 Perform a fresh installation of the same software release of IM and Presence Service or Unified Communications Manager on the new VM using the same hostname and IP address.

Step 5 Perform a DRS restore on the new VM.



CHAPTER 5

Sequencing Rules and Time Requirements

Upgrade Sequence and Time Requirements

The sequence in which you perform upgrade procedures depends on your deployment, and on how you want to balance the level of user impact with the amount of time required to complete the upgrade. You must identify the sequence that you will follow before you are ready to perform the upgrade process.

The information in this section applies only if you are performing a direct upgrade using either the Unified CM OS Administration interface or the PCD Upgrade task. PCD Migrations do not require this step.

Understanding Version Switching

When you upgrade a node, the new software is installed as an inactive version. To activate the new software, you must switch the node to the new software version. There are two ways to switch to the new software version:

- Automatic switching—the system switches the version automatically as part of the upgrade process
- Manual switching—physically switch the version using the OS Administration interface after the upgrade process is complete

The method that you choose depends on the type of upgrade that you are doing. During the upgrade process, the wizard prompts you to choose whether to switch the software version automatically by rebooting to the upgraded partition, or whether to switch the version manually at a later time. The table below lists the switching method to use for each type of upgrade.

Upgrade type	Switching type	When prompted, choose . . .	Result
Standard upgrade	Automatic	**GUI:** Reboot to upgraded partition **CLI:** Switch to new version after upgrade	When you choose this option, the system reboots to the new software version.
	Manual	**GUI:** Do not reboot after upgrade **CLI:** Do not switch to new version after upgrade	When you choose this option, the system continues to run the old software version when the upgrade is complete. You can manually switch to the new software later.
Refresh upgrade	Automatic	**GUI:** Reboot to upgraded partition **CLI:** Switch to new version after upgrade	Choose this option to use the new software version immediately following the upgrade.
	Manual	**GUI:** Do not reboot after upgrade **CLI:** Do not switch to new version after upgrade	Use this option only if you are performing a refresh upgrade in stages. When you choose this option the system reboots to the old software version when the upgrade is complete, and you can manually switch to the new software later.

When you switch versions, your configuration information migrates automatically to the upgraded version on the active partition.

If for any reason you decide to back out of the upgrade, you can restart the system to the inactive partition that contains the older version of the software. However, any configuration changes that you made since you upgraded the software will be lost.

For a short period of time after you install Unified Communications Manager or switch over after upgrading to a different product version, any changes made by phone users may be lost. Examples of phone user settings include call forwarding and message waiting indication light settings. This can occur because Unified Communications Manager synchronizes the database after an installation or upgrade, which can overwrite phone user settings changes.

Sequence Rules

When you are planning to perform an upgrade using either the Unified CM OS Admin interface or the PCD upgrade task, you must ensure that your plan takes the following sequencing rules into account.

- The Unified Communications Manager publisher node must be the first node that you upgrade. The new software is installed as an inactive version.
- You can begin upgrading Unified Communications Manager subscriber nodes as soon as the publisher node has been upgraded with an inactive version of the new software.
- You must switch the Unified Communications Manager publisher node to the new software version and reboot it before you switch the version on any subscriber nodes. The publisher node must be the first node to switch to the new software version and reboot.
- If you upgrade a group of subscriber nodes, after you switch the software version and reboot, you must wait for database replication to complete on all subscriber nodes before proceeding with any COP file installs or configuration changes.
- If you are upgrading Unified Communications Manager nodes to a Maintenance Release (MR) or an Engineering Special (ES) Release and you are not upgrading IM and Presence Service nodes, you must reboot all IM and Presence nodes after the Unified Communications Manager upgrade is complete.
- If you are upgrading IM and Presence Service nodes in addition to Unified Communications Manager nodes:
    - The IM and Presence Service database publisher node must be the first IM and Presence Service node that you upgrade. The new software is installed as an inactive version.
    - You can begin upgrading IM and Presence Service subscriber nodes as soon as the publisher node has been upgraded with an inactive version of the new software.
    - You can wait until all of the Unified Communications Manager nodes are upgraded to an inactive version before you upgrade the IM and Presence Service database publisher node, or you can choose to upgrade in parallel. If you upgrade in parallel, start upgrading the IM and Presence Service database publisher node at the same time that you upgrade the Unified Communications Manager subscriber nodes.
    - You must switch to the new software version and reboot all Unified Communications Manager nodes, starting with the publisher node, before you can switch versions on the IM and Presence Service nodes.
    - You must switch the IM and Presence Service database publisher node to the new software version and reboot it before you switch the software version on any IM and Presence Service subscriber nodes.
    - If you upgrade a group of IM and Presence Service subscriber nodes, after you switch the software version and reboot, you must wait for database replication to complete on all subscriber nodes before proceeding.
- If you are upgrading IM and Presence Service nodes to a Maintenance Release (MR) or an Engineering Special (ES) Release and you are not upgrading Unified Communications Manager nodes, the following additional sequencing rules apply:
    - For upgrades using the Unified CM OS Admin interface, you must upgrade the Unified Communications Manager publisher node and then upgrade the IM and Presence Service nodes to the Maintenance Release (MR) or an Engineering Special (ES) Release.
    - If you are using the Prime Collaboration Deployment migration task, you must select the Unified Communications Manager publisher node in addition to the IM and Presence Service nodes.

- If you are using the Prime Collaboration Deployment upgrade task, you do not need to select the Unified Communications Manager publisher node as long as the first 3 digits of new version of IM and Presence Service match the first 3 digits of the currently installed version of Unified Communications Manager.

Upgrade time requirements

The time required to upgrade the software is variable and depends on a number of factors. Use the information in the following sections to understand the steps you can take to optimize the upgrade process. The following sections also provide information and examples to help you to estimate the time requirements for an upgrade.

Factors that Affect Upgrade Time Requirements

The table below lists the factors that impact the amount of time that an upgrade requires. You can reduce the amount of time needed for an upgrade by ensuring that your system meets these conditions.

Table 10: Factors that Affect Time Requirements

Item	Description
External Services and Tools	Time requirements are reduced when external services and tools, such as NTP servers, DNS servers, LDAP directories, and other network services are reachable with response times as short as possible with no dropped packets. We recommend that you configure the ESXi server and the Unified Communications Manager publisher node to point to the same NTP server. **Note** To avoid upgrade failures due to time sync issues with VM, disable the VM's NTP sync with the ESXi host using the workaround mentioned in the following link: http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=1189
Accessibility of upgrade images	Save time by ensuring that ISO images are on DVD, or are already downloaded and staged on the same LAN as the Unified Communications Manager and IM and Presence Service virtual machines (VM).

Item	Description
System health	The virtual machine configuration impacts the time requirement for an upgrade. Use the virtual machine specifications that are correct for your deployment size. If your database exceeds the virtual machine's configuration limits, the upgrade process will take longer to complete or fail. For example, having too many devices for the VM configuration will impact the upgrade.
	Low memory or memory leaks will impact the upgrade.
	Round Trip Times (RTT) between nodes will extend the time required.
	Ensure that there are no OutOfSynch (OOS) tables in the database.
	Ensure that there are no SD link out-of -service events on the Unified Communications Manager node. These events typically indicate a network problem, which you must address before you begin the upgrade process.
	System errors can impact upgrade time. In the Real Time Monitoring Tool (RTMT) interface, double-click Alert Central in the left navigation pane and ensure that there are no errors.
Physical and virtual hardware infrastructure	Upgrade time is reduced when your infrastructure is configured for high-capacity and low-latency, and when there is low contention from other traffic. For example, you can optimize the upgrade process by ensuring that: • There are no infrastructure bottlenecks from VMs sharing same ESXi host, the same Direct Attached Storage (DAS) volume, the same Logical Unit Number (LUN), or the same congested network link. • Storage latencies meet the requirements specified at .. www.cisco.com go virtualized-collaboration. • The physical CPU cores and the virtualization design comply with virtualization requirements of Unified Communications Manager and IM and Presence Service. Do not oversubscribe CPUs by having VMs share the host resources; use logical cores or resource reservations • Unified Communications Manager and IM and Presence Service virtual machines are on same hosts, or on hosts wtih 1GbE LAN between them with low contention from other traffic. • If the cluster is over a WAN, ensure that you follow all bandwidth and latency rules listed in the *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.
System capacity	Reduce the upgrade time by purging unnecessary files, such as: • Call Detail Recording (CDR) records • Outdated files, such as TFTP files, firmware, and log files

Item	Description
Throttling	On IM and Presence Service nodes, the system throttles the upgrade process to preserve system stability during upgrades. Throttling may increase the time required to complete the upgrade. Although you can disable throttling to decrease the time it takes to perform the upgrade, doing so may degrade system performance.

Estimating the Minimum Time Requirements

The table below lists the minimum amount of elapsed time to expect for each task in the upgrade process under ideal conditions. Your upgrade may take longer than the times listed in this table, depending on your network conditions and on the upgrade sequence that you follow.

Note Once you begin the upgrade process, you cannot make configuration changes until the upgrade is complete and you have performed all of the post-upgrade tasks. Configuration changes include:

- changes made through any of the Unified Communications Manager or IM and Presence Service graphical user interfaces (GUI), the command line interface (CLI), or the AXL API
- LDAP synchronizations, including incremental synchronizations that are pushed to Unified Communications Manager from an Oracle LDAP
- automated jobs
- devices attempting to autoregister

Note Refresh Upgrades from Pre-12.5.x source to Release 15 is not supported.

Table 11: Minimum Time Required for Upgrade Tasks

Task	Minimum Time	Service Impact
Upgrade the Unified Communications Manager publisher node to an inactive version	2 to 4 hours Add 1 hour if a refresh upgrade	Refresh upgrades: no access to the UI
Upgrade the Unified Communications Manager subscriber nodes to an inactive version	1 to 2 hours	Refresh upgrades: phones are unavailable if no backup subscribers are configured
Switch the Unified Communications Manager publisher node to the new software version and reboot	30 minutes	—

Task	Minimum Time	Service Impact
Switch the Unified Communications Manager subscriber nodes to the new software version and reboot	30 minutes	Standard upgrades: phones are unavailable if no backup subscribers are configured
Unified Communications Manager database replication	30 minutes for deployments with small clusters or small databases 2 hours for megaclusters or large databases **Note** WAN latency of 80ms or more can significantly lengthen these times	Phones are available with dial tone but end-user features are unavailable until upgrade is complete
Upgrade the IM and Presence Service database publisher node to an inactive version	2 to 4 hours Add 1 hour if a refresh upgrade	At the time of L2 upgrade neither phone services nor IM and Presence should be impacted IM and Presence should be impacted only in the case of Refresh Upgrade
Upgrade the IM and Presence Service subscriber nodes to an inactive version	1 to 2 hours	During the switch version , irrespective of L2 or Refresh Upgrade phone services should continue to work while IM and Presence is impacted
Switch the IM and Presence Service publisher node to the new software version and reboot	30 minutes	IM and Presence high availability is disabled Jabber is unavailable
Switch the IM and Presence Service subscriber nodes to the new software version and reboot	30 minutes	IM and Presence high availability is disabled Jabber is unavailable

Task	Minimum Time	Service Impact
IM and Presence Service database replication	30 minutes for deployments with small clusters or small databases 2 hours for megaclusters or large databases **Note** WAN latency can significantly lengthen these times. The maximum WAN latency accepted is 80m.	IM and Presence high availability is disabled Jabber is unavailable

Examples

The examples in this section are based on the following upgrade scenario:

- a megacluster that includes Unified Communications Manager nodes as well as Instant Messaging and Presence nodes
- 75,000 users
- a system that is healthy and that has been optimized for the upgrade, as described in Factors that Affect Upgrade Time Requirements, on page 68

CHAPTER 6

Pre-Upgrade Tasks (Manual Process)

The manual pre-upgrade tasks in this appendix can be used if you are upgrading from a release prior to 10.0(1) or if you want to complete the pre-upgrade tasks manually.

Pre-Upgrade Tasks

Complete the following tasks before you begin an upgrade or migration.

Note The steps in this task flow apply to all upgrades and migrations, unless stated otherwise.

Procedure

	Command or Action	Purpose
Step 1	Read the release notes for the new release: http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-release-notes-list.html.	Ensure that you understand the new features and how the upgrade interacts with the other products that are associated with your system. Do this step for all upgrade and migration methods.
Step 2	Run Upgrade Readiness COP File (Pre-upgrade), on page 39	The Upgrade Readiness COP file checks your system for issues that may interfere with the upgrade. **Note** We strongly recommend that you run the COP file in order to reduce the possibility of an upgrade failure.
Step 3	Consider Smart Licensing Requirements	Release 12.x introduces Smart Licensing as a replacement for Prime License Manager. You must set up a Customer Smart account, and create the Virtual account (optionally) under the Smart account based on the organization structure. For more details on Cisco Smart

	Command or Action	Purpose
		Accounts, see https://www.cisco.com/c/en/us/buy/smart-accounts.html. For details on Smart Software Licensing Overview, see https://www.cisco.com/c/en/us/buy/smart-accounts/software-licensing.html.
Step 4	Check that the software version you are upgrading from is running on a virtual machine.	If your software is running on MCS hardware, you must complete the PCD migration task. See *Cisco Prime Collaboration Deployment Administration Guide* at http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html.
Step 5	Review the Requirements and Limitations, on page 17 for this release.	Ensure that your system meets all network, platform, and software requirements. Do this step for all upgrade and migration methods.
Step 6	Check the health of your network: • Read Factors that Affect Upgrade Time Requirementsand ensure that your system meets the conditions described in that section. • Generate a Database Status Report, on page 79 • Check Database Replication, on page 80 • Check Performance Reports, on page 80 • Run CLI Diagnostics, on page 81	The health of your system affects the amount of time that an upgrade requires. You can reduce the amount of time needed for an upgrade by ensuring that your system meets the conditions described in these sections.
Step 7	Ensure that there are no expired certificates on the partition, including any trust certificates in the certificate chain. If there are expired certificates: • Delete a Trust Certificate, on page 81 • Regenerate a Certificate, on page 82 if an Identity certificate is expired.	For Direct upgrades, ensure that your system meets all the certificate requirements. **Note** For Multi-server(SAN) certificates, ensure that SAN entries are present in all the nodes of the cluster.
Step 8	Take a Fresh Backup, on page 84	Complete a system backup. **Caution** You may lose data or you may be unable to restore your system if your backup is outdated.
Step 9	Back Up Custom Ringtones and Background Images, on page 85	If you have custom ring-tones or background images in the TFTP directory, create a separate backup for these files as they are not included in system backups.

	Command or Action	Purpose
Step 10	Check Network Connectivity, on page 86	Use this procedure to verify connectivity between Unified Communications Manager nodes and services in your network, such as NTP, SMTP, and DNS.
Step 11	Verify IPv6 Networking, on page 86	For Unified Communications Manager nodes only. Verify IPv6 networking between the publisher and subscriber nodes. Load detection may take 20 minutes if IPv6 is configured incorrectly.
Step 12	Check Connectivity between IM and Presence and Cisco Unified Communications Manager, on page 87	Verify that the IM and Presence Service has connectivity with Unified CM. For upgrades only. You can skip this task for migrations.
Step 13	Collect Configuration and Login Information, on page 87	Record the current configuration and login information for your Unified Communications Manager nodes in case any issues are encountered during the upgrade process.
Step 14	Record the Registered Device Count, on page 88	Use the Real Time Monitoring Tool (RTMT) to capture the device count so that you can verify your endpoints and resources after the upgrade is complete.
Step 15	Record the Number of Assigned Users, on page 88	Record the number of assigned users on IM and Presence Service nodes so that you can verify this information after the upgrade is complete.
Step 16	Record TFTP Parameters, on page 89	The upgrade process changes a TFTP parameter. Record the current setting so that you can reset the parameter after the upgrade is complete.
Step 17	Record Enterprise Parameters, on page 89	During the upgrade, the Unified Communications Manager enterprise parameter settings may overwrite the IM and Presence Service enterprise parameter settings if the configurations are different.
Step 18	Export User Records, on page 89	Export user records using the Bulk Administration Tool (BAT).
Step 19	Upgrade IP Phone Firmware, on page 90	You can upgrade your IP phones to the firmware that corresponds to the new release as a pre-upgrade task in order to minimize phone downtime after an upgrade. You can skip this task for migrations.

	Command or Action	Purpose
Step 20	Verify Critical Services, on page 91	Verify that all critical services are activated.
Step 21	Deactivate Cisco Extension Mobility, on page 91	For upgrades from Release 9.x or earlier only. You must stop Cisco Extension Mobility services on Unified CM nodes before you upgrade. You can skip this task for migrations.
Step 22	Stop the IM and Presence Sync Agent, on page 92	If you need to upgrade Unified Communications Manager as part of your IM and Presence upgrade, you must stop the IM and Presence Sync Agent service before you upgrade. You can skip this task for migrations.
Step 23	Check the Available Common Partition Space, on page 92	Verify that you have enough common partition space for the upgrade. You can skip this task for migrations.
Step 24	If you do not have enough common partition space, perform one or more of the following procedures: • Adjust High and Low Watermarks, on page 92 • Maximize Usable Disk Space, on page 93	Do this step for only for direct upgrades, which use either the Unified CM OS Administration interface or the PCD Upgrade task to perform the upgrade. **Caution** Performing an upgrade without sufficient disk space can cause the upgrade to fail.
Step 25	Obtain Upgrade Files, on page 94	Download the required upgrade files. For refresh upgrades, you must also download any required COP files. **Note** Refresh Upgrades from Pre-12.5.x source to Release 15 is not supported. You can skip this task for migrations.
Step 26	Increase the Database Replication Timeout, on page 95	Optional. Unified Communications Manager publisher node only. Use this procedure when you upgrade large clusters. You can skip this task for migrations.
Step 27	Disable High Availability on Presence Redundancy Groups, on page 95	IM and Presence Service only. If High Availability is enabled, disable it prior to the upgrade. You can skip this task for migrations.

	Command or Action	Purpose
Step 28	Add a Serial Port to the Virtual Machine, on page 96	Add a serial port to the virtual machine so that you can dump logs if an upgrade fails. Perform this procedure for all nodes.
Step 29	Configure High Availability for RTMT, on page 96	For megacluster deployments that monitor with RTMT, Cisco recommends configuring high availability for RTMT so that you don't lose connectivity during simplified clusterwide upgrades.
Step 30	Database Migration Required for Upgrades with Microsoft SQL Server, on page 97	This procedure applies to IM and Presence Service nodes only. 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.
Step 31	Before you upgrade your system, ensure that you configure the **Trusted List of Hosts in HTTP Referer/Host Header** and add the public IP address or DNS alias in the Cisco Unified CM Administration Enterprise Parameters page.	This configuration is necessary if your network topology has public IP address configured for external interfaces along with private IP address for the individual nodes in the cluster. Unified CM will now validate the IP address or hostname present in the Host header with the servers configured in the Unified CM cluster first before allowing access to Unified CM. You must also configure the DNS alias used to access the Unified CM under the Trusted List of Hosts configuration. For example, if your server is cm1.example.local, and you use phone.example.local to access the server, you must add phone.example.local to the Trusted List of Hosts configuration. From Cisco Unified CM Administration user interface, select **System** > **Enterprise Parameters** to configure the external IP addresses or DNS alias used. **Note** If you are performing this activity post-upgrade, then you need to restart the Cisco Tomcat service for all the web pages to load correctly.

Run Upgrade Readiness COP File (Pre-upgrade)

The Upgrade Readiness COP file checks for the following things:

- Installed COP Files
- Network services and connectivity (DNS, NTP, intra-cluster)
- Licensing sync
- VMware tools compatibility
- Hard disk partition size
- Swap size check
- Filesystem type and guest OS checks
- Usable Disk space for destination versions
- ESXi version check
- SIP and H.323 trunk registrations
- Database authentication and replication status
- Database sanity
- Status of last DRS backup
- Remote Call Control (RCC) feature status
- Services status
- Installed COPs and Locales
- Device Registration Status Count
- Enterprise Parameter and Service Parameters settings
- TFTP Maximum Service Counts
- Active and Inactive versions
- List the expired certificates
- FIPS mode password length restrictions
- IPSec Policy configuration check for ESP and Encryption Algorithm in FIPS mode

Note

- It's strongly recommended that you run the Upgrade Readiness COP file before you upgrade as it reduces significantly the chances of a failed upgrade.
- The COP file is fully supported where the pre-upgrade version is 10.x or later.
- Since the 3DES Algorithm isn't supported in FIPS mode, you must delete the IPSec policy with the 3DES Algorithm and recreate the IPSec policy with the Encryption and ESP Algorithms other than 3DES in both the nodes where IPSec tunnel is to be established.

Procedure

Step 1 Download the Upgrade Readiness COP file to run pre upgrade tests.

a) Go to the Downloads site.

b) Select the destination release and then select **Unified Communications Manager Utilities**.

c) Download the **Upgrade Readiness COP file in order to run pre-upgrade tests** (For example, `ciscocm.preUpgradeCheck-00019.cop.sgn`. Note that the latest file may have a different filename and version).

Step 2 Check your system readiness for upgrades:

a) Run the COP file.

b) Resolve any issues that the COP file returns.

c) Run the COP file again.

d) Repeat this process until the COP file returns no errors.

Step 3 Install the cop file from GUI or CLI. Once the installation is complete, from CLI run **file view install PreUpgradeReport.txt** to view the report.

Step 4 To view the report from RTMT

a) Log in into RTMT.

b) In **Trace and Log Central** double click on **Remote Browse** and select **Trace files** and click **Next**.

c) Select **Select all Services on all servers** and click **Next**.

d) Click **Finish** and **Close**.

e) Double-click on nodes, expand **CUCM Publisher** > **System** > **Install upgrade Logs**.

f) Double-click on **Install** and select the file which you require and download.

Generate a Database Status Report

Use Cisco Unified Reporting Tool (CURT) to generate a Database Status Report to verify that there are no network issues between cluster nodes. For example, verify that there are no issues with reachability or latency that affect database replication between nodes or that affect quality of service (QoS) for voice and video signaling.

Procedure

Step 1 Log in to the reporting interface for the node:

- For Unified CM nodes, log in to the Cisco Unified Reporting interface.
- For IM and Presence nodes, log in to the Cisco Unified IM and Presence Reporting interface.

Step 2 Select **System Reports**.

Step 3 Check database replication on the node:

- For Unified CM, select **Unified CM Database Status**.
- For IM and Presence, select **IM and Presence Database Status**.

Step 4 Click the **Generate Report** (bar chart) icon in the **Reports** window.

Step 5 Click the **View Details** link to expose details for a section that does not automatically appear.

Step 6 If the report indicates that there are errors, select the **Report Descriptions** report and review the troubleshooting information with possible remedies.

Check Database Replication

Use this procedure to verify that the database replication is functioning correctly before you begin an upgrade.

Procedure

Step 1 Start a CLI session using one of the following methods:

- From a remote system, use SSH to connect securely to the Cisco Unified Operating System. In your SSH client, enter your `ssh` ***`adminname@hostname`*** and enter your password.
- From a direct connection to the serial port, enter your credentials at the prompt that displays automatically.

Step 2 Execute the **utils dbreplication status** command to check for errors or mismatches in the database tables.

Step 3 Execute the **utils dbreplication runtimestate** command to check if the database replication is active on the node.

The output lists all the nodes and if database replication is set up and in a good state, the **replication setup** value for each node is **2**.

If a value other than 2 is returned, you must resolve the errors before proceeding.

Check Performance Reports

Procedure

Step 1 From the Cisco Unified Serviceability interface, select **Tools** > **Serviceability Reports Archive**.

Step 2 Click on the link and choose the most recent report.

Step 3 Click the **CallActivitiesRep** to open the Call Activities Report in a new tab and verify that the number of **Calls Attempted** is not too high for the capacity of the virtual machine. You can determine the threshold for the number of **Calls Attempted** by checking the recommendations for your system in the *Cisco Collaboration Systems Solution Reference Network Designs (SRND)* at https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-system/products-implementation-design-guides-list.html.

Step 4 Return to the Cisco Unified Serviceability interface and click the **PerformanceRep** link for each node to view the Performance Protection Statistics Reports.

Step 5 In each Performance Protection Statistics Report, verify that your system does not exceed the cluster-wide or per-node limits that are specified for your deployment size.

For information about deployment sizing, see:

- *Cisco Collaboration Systems Solution Reference Network Designs (SRND)* at https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-system/products-implementation-design-guides-list.html.
- Collaboration Sizing Tool at http://tools.cisco.com/cucst. Partners can use this tool to evaluate a customer's configuration.

Run CLI Diagnostics

Use the command line interface (CLI) diagnostic commands to diagnose and solve network problems before you begin and upgrade.

Procedure

Step 1 Start a CLI session using one of the following methods:

- From a remote system, use SSH to connect securely to the Cisco Unified Operating System. In your SSH client, enter your **`ssh`** ***`adminname@hostname`*** and enter your password.
- From a direct connection to the serial port, enter your credentials at the prompt that displays automatically.

Step 2 Execute the **utils diagnose test** command.

This command runs all diagnostic commands but does not attempt to fix problems. You can view a list of all the diagnostic commands by executing the **utils diagnose list** command.

Step 3 Execute the **utils diagnose fix** command to attempt to automatically fix system problems.

Delete a Trust Certificate

A trusted certificate is the only type of certificate that you can delete. You cannot delete a self-signed certificate that is generated by your system.

Caution Deleting a certificate can affect your system operations. It can also break a certificate chain if the certificate is part of an existing chain. Verify this relationship from the username and subject name of the relevant certificates in the **Certificate List** window. You cannot undo this action.

Procedure

Step 1 From Cisco Unified OS Administration, choose **Security** > **Certificate Management**.

Step 2 Use the **Find** controls to filter the certificate list.

Step 3 Choose the filename of the certificate.

Step 4 Click **Delete**.

Step 5 Click **OK**.

Note

- If you delete the “CAPF-trust”, “tomcat-trust”, “CallManager-trust”, or “Phone-SAST-trust” certificate type, the certificate is deleted across all servers in the cluster.
- Deletion of certificates from phone edge trust should be done from publisher.
- If you import a certificate into the CAPF-trust, it is enabled only on that particular node and is not replicated across the cluster.

Regenerate a Certificate

Before you begin an upgrade, ensure that there are no expired certificates on the partition, including any trust certificates in the certificate chain. Regenerate a certificate if it is expired. Follow this procedure after business hours, because you must restart phones and reboot services. You can regenerate only a certificate that is listed as type “cert” in Cisco Unified OS Administration.

Note Refresh Upgrades from Pre-12.5.x source to Release 15 is not supported.

Note During an upgrade, the ITLRecovery certificate is generated per cluster. If the cluster is in mixed mode, manually update the CTL file. Reset the phones to reflect the latest updates. This is applicable only for refresh upgrades. From Release 12.5(1)SU3 update CTL is no longer required.

Caution Regenerating a certificate can affect your system operations. Regenerating a certificate overwrites the existing certificate, including a third-party signed certificate if one was uploaded.

Procedure

Step 1 From Cisco Unified OS Administration, choose **Security** > **Certificate Management**.

Enter search parameters to find a certificate and view its configuration details. The system displays the records that match all the criteria in the **Certificate List** window.

Click **Regenerate** button in certificate details page, a self-signed certificate with the same key length is regenerated.

Note When regenerating a certificate, the **Certificate Description** field is not updated until you close the **Regeneration** window and open the newly generated certificate.

Click **Generate Self-Signed Certificate** to regenerate a self-signed certificate with a new key length of 3072 or 4096.

Step 2 Configure the fields on the **Generate New Self-Signed Certificate** window. See online help for more information about the fields and their configuration options.

Step 3 Click **Generate**.

Step 4 Restart all services that are affected by the regenerated certificate. See Certificate Names and Descriptions, on page 83 for more information.

Step 5 Update the CTL file (if configured) after you regenerate the CAPF, ITLRecovery Certificates or CallManager Certificates.

Note After you regenerate certificates, you must perform a system backup so that the latest backup contains the regenerated certificates. If your backup does not contain the regenerated certificates and you perform a system restoration task, you must manually unlock each phone in your system so that the phone can register.

What to do next

After you regenerate certificates, you must perform a system backup so that the latest backup contains the regenerated certificates.

Related Topics

Certificate Names and Descriptions, on page 83

Certificate Names and Descriptions

The following table describes the system security certificates that you can regenerate and the related services that must be restarted. For information about regenerating the TFTP certificate, see the *Cisco Unified Communications Manager Security Guide* at http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html.

Table 12: Certificate Names and Descriptions

Name	Description	Services to be Restarted
tomcat tomcat-ECDSA	This certificate is used by WebServices, Cisco DRF Services, and Cisco CallManager Services when SIP Oauth mode is enabled.	**Note** Restart of the below mentioned services are applicable for Release 14 onwards. Cisco Tomcat Services, Cisco Disaster Recovery System (DRS) Local and Master Services, Cisco UDS Tomcat, Cisco AXL Tomcat, and Cisco SSOSP tomcat web services. If SAML SSO is enabled with Tomcat certificate, you must re-provision the SP metadata on the IDP.

Name	Description	Services to be Restarted
ipsec	This self-signed root certificate is generated during installation for IPsec connections with Unified Communications Manager, MGCP, H.323, and IM and Presence Service.	IPsec Service.
CallManager CallManager-ECDSA	This is used for SIP, SIP trunk, SCCP, TFTP etc.	**Note** Restart of the below mentioned services are applicable for Release 14 onwards. CallManager - HAProxy Service, update CTL file if the server is in secure mode. CallManager-ECDSA - Cisco CallManager Service, HAProxy Service.
CAPF	Used by the CAPF service running on the Unified Communications Manager Publisher. This certificate is used to issue LSC to the endpoints (except online and offline CAPF mode)	N/A
TVS	This is used by Trust verification service, which acts as a secondary trust verification mechanism for the phones in case the server certificate changes.	N/A

Note

- A new enterprise parameter Phone Interaction on Certificate Update under section Security Parameter is introduced to reset phones either manually or automatically as applicable when one of the TVS, CAPF, or TFTP certificates are updated. This parameter is by default set to reset the phones automatically.
- After regeneration, deletion, and updation of certificates, ensure you restart the appropriate services mentioned in the column "Services to be Restarted".

Take a Fresh Backup

You must backup the system before you perform an upgrade to ensure that the backup file matches the currently-installed software exactly. If you try to restore the system from a backup file that does not match the current version, the restore will fail.

Perform this procedure for all upgrade and migration methods.

⚠

Caution You may lose data or you may be unable to restore your system if your backup is outdated.

Before you begin

- Ensure that you use a network device as the storage location for the backup files. Virtualized deployments of Unified Communications Manager do not support the use of tape drives to store backup files.
- Ensure that your system meets the version requirements:
  - All Unified Communications Manager cluster nodes must be running the same version of the Unified Communications Manager application.
  - All IM and Presence Service cluster nodes must be running the same version of the IM and Presence Service application.

  For each application, the entire version string must match. For example, if the IM and Presence database publisher node is at version 11.5.1.10000-1, then all IM and Presence subscriber nodes must be 11.5.1.10000-1, and you must create a backup file for version 11.5.1.10000-1.
- The backup process can fail due to non availability of space on a remote server or due to interruptions in the network connectivity. You need to start a fresh backup after addressing the issues that caused the backup to fail.
- Make sure that you have a record of the cluster security password. If the cluster security password changes after you complete this backup, you will need to know the password or you will not be able to use the backup file to restore your system.

Procedure

Step 1 From the Disaster Recovery System, select **Backup** > **Manual Backup**.

Step 2 In the **Manual Backup** window, select a backup device from the **Backup Device Name** area.

Step 3 Choose a feature from the **Select Features** area.

Step 4 Click **Start Backup.**

Back Up Custom Ringtones and Background Images

If you have custom ringtones or background images in the TFTP directory, you need to create a separate backup for these files. They are not included in the Disaster Recovery System (DRS) backup file.

Procedure

Step 1 Use a web browser or TFTP client to access the directories where the ringtones and background images are stored.

Step 2 Backup the following files: `Ringlist.xml` and `List.xml` .

Step 3 Back up the custom ringtones. These are located in the TFTP directory.

Step 4 Back up the background images. These are located in the folder `/Desktops` (and its subfolders) in the TFTP directory.

Check Network Connectivity

Use this procedure to verify connectivity between all nodes and services in your network.

Procedure

Step 1 Start a CLI session using one of the following methods:

- From a remote system, use SSH to connect securely to the Cisco Unified Operating System. In your SSH client, enter your **`ssh`** ***`adminname@hostname`*** and enter your password.
- From a direct connection to the serial port, enter your credentials at the prompt that displays automatically.

Step 2 Execute the **show network cluster** command on each node in your network to verify communication between Unified Communications Manager servers in the cluster.

Step 3 If you have an NTP server, execute the **utils ntp status** command to verify connectivity to the NTP server.

Step 4 If you have an SMTP server, ping the server to verify connectivity.

Step 5 If you are using DNS, execute the **show network eth0** command on each node in your network to verify that the DNS and domain are configured.

Step 6 Check that DNS name resolution is working correctly:

a) Ping the FQDN of each Unified Communications Manager node to ensure that it resolves to the IP address.
b) Ping the IP address of each Unified Communications Manager to ensure that it resolves to the FQDN.

Verify IPv6 Networking

This procedure applies to Unified Communications Manager nodes only.

Verify that IPv6 networking on the first node (Unified Communications Manager database publisher node) and Unified Communications Manager subscriber nodes. If IPv6 is configured incorrectly on the Unified Communications Manager subscriber nodes, load detection may take 20 minutes.

Procedure

Step 1 Start a CLI session using one of the following methods:

- From a remote system, use SSH to connect securely to the Cisco Unified Operating System. In your SSH client, enter your **`ssh`** ***`adminname@hostname`*** and enter your password.
- From a direct connection to the serial port, enter your credentials at the prompt that displays automatically.

Step 2 Execute the following command:**utils network ipv6 ping***destination [count]*

- *destination* is a valid IPv6 address or host name that you want to ping

- *count* is the number of times to ping the external server. The default is 4.

Check Connectivity between IM and Presence and Cisco Unified Communications Manager

Verify that the IM and Presence Service service node has connectivity with Unified Communications Manager.

Procedure

Step 1 From the Cisco Unified CM IM and Presence Administration interface, select **Diagnostics** > **System Troubleshooter** .
The system automatically runs a troubleshooting check.

Step 2 When the results of the troubleshooting check are loaded, verify that all of the **Sync Agent Troubleshooter** tests have a green checkmark in the **Outcome** column to indicate that the test was passed.

Step 3 If any of the **Sync Agent Troubleshooter** tests are failed, use the information in the **Problem** and **Solution** columns to resolve the issue before continuing with the upgrade process.

Collect Configuration and Login Information

Record the current configuration and login information for your Unified Communications Manager nodes in case any issues are encountered during the upgrade process.

Procedure

Step 1 Record the following login and password information:

- all application users credentials, such as DRS, AXL, and accounts for other third-party integrations
- administrator, cluster security, and Certificate Trust List (CTL) security token passwords

Step 2 Record the following information about your network configuration:

- IP addresses, hostnames, gateways, domain names, DNS servers, NTP servers, the Call Detail Recording (CDR) server, and SMTP information
- server versions and time zones
- services running on each server and the associated activation status
- LDAP information and access details
- SNMP information

Record the Registered Device Count

Use the Real Time Monitoring Tool (RTMT) to capture the device count before you begin an upgrade, so that you can verify your endpoints and resources after the upgrade is complete. You can also use this information to verify that you have not exceeded the capacity of the virtual machine (VM) that you are deploying.

Procedure

Step 1 From the Unified RTMT interface, select **CallManager** > **Device** > **Device Summary**.

Step 2 Record the number of registered devices for each node:

Item	Count
Registered Phones	
FSX	
FSO	
T1 CAS	
PRI	
MOH	
MTP	
CFB	
XCODE	

Record the Number of Assigned Users

Record the number of assigned users on IM and Presence Service nodes so that you can verify this information after the upgrade is complete.

Procedure

Step 1 From the Cisco Unified CM IM and Presence Administration interface, select **System** > **Cluster Topology**.
The Cluster Topology Details page displays information about nodes and subclusters.

Step 2 Record the number of users that are assigned to each node and cluster.

Record TFTP Parameters

During the upgrade process, the TFTP service parameter **Maximum Serving Count** is changed to allow for an increased number of device registration requests. Record the existing settings so that you can reset the parameter after the upgrade is complete.

Procedure

Step 1 From the Cisco Unified CM Administration interface, choose **System** > **Service Parameters**.

Step 2 From the **Server** drop-down list, select the node that is running the TFTP service.

Step 3 From the **Service** drop-down list, select **Cisco TFTP service**.

Step 4 Click **Advanced**.

Step 5 Click **Save**.

Step 6 Record the value that is configured for the **Maximum Serving Count**.

Record Enterprise Parameters

Record the settings for Enterprise Parameters on both Unified Communications Manager nodes and IM and Presence Service Service nodes. Some Enterprise Parameters exist on both Unified Communications Manager nodes and IM and Presence Service Service nodes. Where the same parameter exists, the settings that are configured on Unified Communications Manager nodes overwrite the settings configured on IM and Presence Service Service nodes during the upgrade process. Enterprise Parameters that are unique to IM and Presence Service Service nodes are retained during an upgrade.

Record the settings so that you can restore them as needed after the upgrade is complete.

Procedure

Step 1 From the Cisco Unified CM Administration interface, choose **System** > **Enterprise Parameters**.

Step 2 Take screen captures to record the settings that you have configured, and save the information so that you can restore the settings after the upgrade is complete.

Step 3 From the Cisco Unified CM IM and Presence Administration interface, choose **System** > **Enterprise Parameters**.

Step 4 Take screen captures to record the settings that you have configured, and save the information so that you can restore the settings after the upgrade is complete.

Export User Records

Export user records using the Bulk Administration Tool (BAT).

Procedure

Step 1 From Cisco Unified CM Administration, choose **Bulk Administration** > **Users** > **Export Users**.

Step 2 Click **Find** to display all user records.

Step 3 Click **Next**.

Step 4 Enter a filename in the in the **File Name** text box and choose file format from the **File Format** drop-down list.

Step 5 In the **Job Information** area, enter the Job description.

Step 6 Click **Run Immediately** to export user records immediately

Step 7 Click **Submit**.

Step 8 To download the exported file, choose **Bulk Administration** > **Upload/Download Files**.

Step 9 Enter search criteria for the file that you generated and click **Find**.

Step 10 Select the check box that corresponds to the file that you want to download and click **Download Selected**.

Step 11 In the File Download pop-up window, click **Save**.

Step 12 In the Save As pop-up window, choose the location where you want to save the file and click **Save**. Ensure that you copy the file off of the server and save it to a remote PC or device.

Upgrade IP Phone Firmware

You can upgrade your IP phones to the firmware that corresponds to the new release as a pre-upgrade task. Although phones automatically download their new firmware after an upgrade, you can choose to apply new firmware files to the endpoints in a controlled manner prior to the upgrade in order to minimize phone downtime after an upgrade.

When you apply new firmware to phones in groups, you can eliminate the load on the TFTP server after the upgrade and accelerate the upgrade of the individual devices. Afterwards, restart the TFTP service on the Unified Communications Manager servers, and restart the IP Phones in a controlled order to minimize downtime. Because the phones cannot be used for calls when their firmware is being upgraded, we recommend that you use a maintenance window outside of your upgrade window to upgrade phone firmware.

Before you begin

- Copy the new firmware load to the following directory on the TFTP server: `/usr/local/cm/tftp`
- Make a record of the system defaults and per-device assignments for your IP phones and registered endpoints.

Procedure

Step 1 From Cisco Unified OS Administration, choose **Software Upgrades** > **Install/Upgrade**.

Step 2 Fill in the applicable values in the Software Location section and click **Next**.

Step 3 In the **Available Software** drop-down list, select the device package file and click **Next**.

Step 4 Verify that the MD5 value is correct, and then click **Next**.

Step 5 In the warning box, verify that you selected the correct firmware, and then click **Install**.

Step 6 Check that you received a success message.

Note Skip to Step 8 if you are rebooting the cluster.

Step 7 Stop and restart the TFTP server.

Step 8 Reset the affected devices to upgrade the devices to the new load.

Step 9 From Cisco Unified CM Administration, choose **Device** > **Device Settings** > **Device Defaults** and manually change the name of the "Load Information" and "Inactive Load Information" for the specific Device Type fields for the new load on the TFTP server.

Step 10 Click **Save**, and then reset the devices.

Verify Critical Services

Use the Cisco Unified Real Time Monitoring Tool (RTMT) to verify that all critical services are activated.

Procedure

Step 1 From the Unified RTMT interface, select **System** > **Server** > **Critical Services**.

Step 2 To display system critical services, click the **System** tab.

Step 3 To display Unified Communications Manager critical services, select a Unified Communications Manager node from the drop-down list and click the **Voice/Video** tab.

Step 4 To display IM and Presence Service critical services, click the **IM and Presence** tab and select an IM and Presence Service Service node from the drop-down list.

Step 5 If the status indicates that any critical services are stopped, reactivate them before beginning the upgrade.

Deactivate Cisco Extension Mobility

Perform this procedure only if you are upgrading from Release 9.x or earlier. For upgrades from Release 9.x or earlier, you must stop Cisco extension mobility on Unified Communications Manager nodes before you begin an upgrade.

Procedure

Step 1 From Cisco Unified Serviceability, choose **Tools** > **Service Activation**.

Step 2 From the **Server** list, choose the node on which you want to deactivate services and click **Go**.

Step 3 Deselect the **Cisco Extension Mobility** services.

Step 4 Click **Stop**.

Step 5 Repeat Steps 2 through 4 for each node that is running **Cisco Extension Mobility** services.

Step 6 Make a list of all the nodes on which you have disabled these services. You will need to restart the services after the upgrade is complete.

Stop the IM and Presence Sync Agent

If you need to upgrade Unified Communications Manager as part of your IM and Presence Service upgrade, you must stop the IM and Presence Service Sync Agent service before you begin the upgrade process.

Procedure

Step 1 From the Cisco Unified Serviceability interface, select **Tools** > **Control Center - Network Services**.

Step 2 Select an IM and Presence Service Service node from the **Server** drop-down list and click **Go**.

Step 3 In the **IM and Presence Services** section, select the **Cisco Sync Agent** and click **Stop**.

Check the Available Common Partition Space

Use the Real-Time Monitoring Tool (RTMT) to verify that you have enough common partition space for the upgrade.

Procedure

Step 1 In the Real-Time Monitoring Tool, select **Disk Usage** from the list of **System** counters on the left navigation pane.
A page displays detailed information about disk usage.

Step 2 View the tables on the bottom of the page and compare the **Total Space** to the **Used Space** for the common partition. You need a minimum 25G of available common partition space before you begin an upgrade. However, your deployment may require more space if you have numerous TFTP data (device firmware loads), music-on-hold (MOH) files, or if you have many locale files installed. In some cases, even if 25GB of free space is available, upgrade may fail with the error message as insufficient space.The workaround is to delete the unnecessary files and create more space in the common partition.

Adjust High and Low Watermarks

Use this procedure to adjust the low and high watermarks to reduce the traces and remove unnecessary log files. After the upgrade, you must restore the high and low watermarks to their original values in order to avoid premature purging of traces. The default value for the high watermark is 85. The default value for the low watermark is 80.

Procedure

Step 1 In the Real Time Monitoring Tool (RTMT) interface, double-click **Alert Central** in the left navigation pane.

Step 2 On the **System** tab, right-click **LogPartitionLowWaterMarkExceeded** and select **Set Alert/Properties**.

Step 3 Select **Next**.

Step 4 Adjust the slider value to 30.

Step 5 On the **System** tab, right-click **LogPartitionHighWaterMarkExceeded** and select **Set Alert/Properties**.

Step 6 Select **Next**.

Step 7 Adjust the slider value to 40.

Maximize Usable Disk Space

When you upgrade from 11.5(X) to 12.5, verify the COP files that are required to be downloaded. To download the COP files and the Readme files, go to https://software.cisco.com > click **Software Download** link under **Download & Upgrade** section, and then, navigate to **Unified Communications** > **Call Control** > **Cisco Unified Communications Manager (CallManager)** > **<*Version*>** > **Unified Communications Manager/CallManager/Cisco Unity Connection Utilities**.

To create additional space in the common partition, you can perform one or more of the steps in this procedure.

If your current version has previously used a serial connection to upgrade from a pre-11.5(x) version then it's likely that have an older OS partitioning scheme and virtual disk layout. This will amplify "out of disk space" issues, thereby limiting the effectiveness of adding additional virtual disk space. The upgrade readiness COP file checks for these issues, and provides guidance on how to resolve them.

Procedure

Step 1 Manually remove outdated or unused firmware files from the TFTP directory using one of the following options:

- From the Cisco Unified OS Administration interface, select **Software Upgrades** > **TFTP File Management** and delete any unnecessary files.
- From the command line interface, use the `file list tftp` and `file delete tftp` commands delete any unnecessary files.
- From the Cisco Unified OS Administration interface, select **Software Upgrades** > **Device Load Management** and delete any unnecessary files.

Note Run the **show diskusage tftp <sort>** command, to check tftp device load size, which is sorted by descending file size.

Run the **show diskusage common <sort>** command, to check the common partition size for available, and free space, which is sorted by descending file size.

Step 2 Perform this step only if the previous steps did not create enough disk space for the upgrade. Use the Free Common Space COP file (ciscocm.free_common_space_v<latest_version>.cop.sgn).

This COP file removes the inactive side in the common partition to increase available disk space without requiring a system rebuild. Ensure that you review the Readme file that supports this COP file before you proceed.

Note You will not be able to switch back to the inactive version after installing this file because the inactive partition becomes unusable.

Note For 110G or two 80G disk deployments, available space for upgrade should be at least twice the active partition disk space. For example, in a two 80G disk deployment, active partition should not be more than 25G, and available space should be at least 50G. Following are commands to check the disk usage.

a. Run the **show diskusage activelog <sort>** command, to check active side partition size, which is sorted by descending file size.

b. Run the **show diskusage common <sort>** command, to check the common partition size for available, and free space, sorted by descending file size.

c. Run the **show diskusage tftp <sort>** command, to check tftp device load size, which is sorted by descending file size.

d. Run the **file delete activelog <filename>** command, to delete logs from active partition.

Obtain Upgrade Files

You must download the upgrade file for the new release, as well as any upgrade Cisco Option Package (COP) files that are required.

Procedure

Step 1 Refer to the table below this procedure to identify the COP files, if any, that you need.

Step 2 Download the upgrade files for the applications from Cisco.com. The software is available in export restricted (K9) and export unrestricted versions (XU), so be sure to confirm that you select the correct file.

- To download the Unified Communications Manager upgrade file, go to https://software.cisco.com > click **Software Download** link under **Download & Upgrade** section, and then, navigate to **Unified Communications** > **Call Control** > **Cisco Unified Communications Manager (CallManager)** > **<*Version*>** > **Unified Communications Manager/CallManager/Cisco Unity Connection Updates**.
- To download the IM and Presence Service Service upgrade file, go to https://software.cisco.com > click **Software Download** link under **Download & Upgrade** section, and then, navigate to **Unified Communications** > **Unified Communications Applications** > **Presence Software** > **Unified Communications Manager IM and Presence Service** > **<*Version*>** > **Unified Presence Service (CUP) Updates**.

Step 3 Go to https://software.cisco.com > click **Software Download** link under **Download & Upgrade** section, and then, navigate to **Unified Communications** > **Call Control** > **Cisco Unified Communications Manager (CallManager)** > **<*Version*>** > **Unified Communications Manager/CallManager/Cisco Unity Connection Utilities** to download COP files for Unified Communications Manager.

Step 4 Go to https://software.cisco.com > click **Software Download** link under **Download & Upgrade** section, and then, navigate to **Unified Communications** > **Unified Communications Applications** > **Presence Software** > **Unified Communications Manager IM and Presence Service** > **<*Version*>** > **Unified Presence Service (CUP) Updates** and select **UTILS** to download COP files for IM and Presence Service.

Required COP Files

The tables below lists the upgrade paths that require COP files. You must install COP files on each node before you begin an upgrade using the Cisco Unified OS 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.

For more information on the COP files that are required, see the *Supported Upgrade and Migration Paths with COP Files* section.

Increase the Database Replication Timeout

Perform this procedure on the Unified Communications Manager publisher node only.

Increase the database replication timeout value when you upgrade large clusters so that more Unified Communications Manager subscriber nodes have sufficient time to request replication. When the timer expires, the first Unified Communications Manager subscriber node, plus all other Unified Communications Manager subscriber nodes that requested replication within that time period, begin a batch data replication with the Unified Communications Manager database publisher node.

Procedure

Step 1 Start a CLI session using one of the following methods:

- From a remote system, use SSH to connect securely to the Cisco Unified Operating System. In your SSH client, enter your **`ssh`** ***`adminname@hostname`*** and enter your password.
- From a direct connection to the serial port, enter your credentials at the prompt that displays automatically.

Step 2 Execute the **utils dbreplication setrepltimeout** *timeout* command, where *timeout* is database replication timeout, in seconds. Ensure that the value is between 300 and 3600.

The default database replication timeout value is 300 (5 minutes).

Disable High Availability on Presence Redundancy Groups

This procedure applies to IM and Presence Service Service nodes only. Use it to disable high availability on the IM and Presence Service presence redundancy group.

Before you begin

Take a record of the number of active users for each cluster node in each Presence Redundancy Group. You can find this information in the (**System** > **Presence Topology**) window of Cisco Unified CM IM and Presence Administration. You will need this information later when you re-enable High Availability.

Procedure

Step 1 From the Cisco Unified CM Administration user interface, choose **System** > **Presence Redundancy Groups**.

Step 2 Click **Find** and select the group.

Step 3 On the Presence Redundancy Group Configuration window, uncheck the **Enable High Availability** check box.

Step 4 Click **Save**.

Step 5 Repeat this procedure for each Presence Redundancy Group.

Step 6 When you are done, wait at least two minutes to sync the new HA settings across the cluster before you make any further changes

Add a Serial Port to the Virtual Machine

Add a serial port to the virtual machine so that you can dump logs in the event of an upgrade failure.

Procedure

Step 1 Power off the virtual machine.

Step 2 Edit the settings to add a serial port. For more information about making configuration changes using vSphere Client, refer to the user manual for the product.

Step 3 Attach the serial port to a .tmp file.

Step 4 Power on the virtual machine and proceed with the upgrade.

What to do next

After you successfully upgrade the system, follow the procedure to Remove the Serial Port, on page 103. In the event of an upgrade failure, refer to Dump a Log File After an Upgrade Failure, on page 119.

Configure High Availability for RTMT

If you use Cisco Unified Real-Time Monitoring Tool (RTMT) and have a mega-cluster deployment, Cisco recommends configuring high availability for RTMT to avoid connectivity loss during a simplified cluster-wide upgrade.

Procedure

Step 1 Log in to any Cisco Unified Communications Manager node.

Step 2 From Cisco Unified CM Administration, choose **System** > **Service Parameters**.

Step 3 From the **Server** drop-down, select a Unified CM node.

Step 4 From the **Service** drop-down, select **Cisco AMC Service**.

Step 5 For the **Primary Collector** service parameter, select any subscriber node.

Step 6 For the **Failover Collector** service parameter, select a different subscriber node.

Step 7 Click **Save**.

Step 8 Connect the Cisco Unified Real-Time Monitoring Tool to any subscriber node.

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 occurs 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 depends on the `MSSQL_migrate_script.sql` script. Contact Cisco TAC to obtain a copy.

Procedure

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:

a. "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.

b. "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.

a. From Cisco Unified CM IM and Presence Administration, choose **Diagnostics** > **System Troubleshooter**.

b. 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:

a. From Cisco Unified IM and Presence Serviceability, choose **Tools** > **Control Center - Network Services**.

b. From the **Server** menu, select an IM and Presence Service node and click **Go**.

c. Under **IM and Presence Services**, select **Cisco XCP Router**, and click **Restart**.

Step 5 Turn off services that depend on the external database:

a. From Cisco Unified IM and Presence Serviceability, choose **Tools** > **Control Center - Feature Services**.

b. From the **Server** menu, select an IM and Presence node and click **Go**.

c. Under **IM and Presence Services**, select the following services:

   Cisco XCP Text Conference Manager

   Cisco XCP File Transfer Manager

   Cisco XCP Message Archiver

d. 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.

a. From Cisco Unified CM IM and Presence Administration, choose **Diagnostics** > **System Troubleshooter**.

b. Verify that no errors appear in the **External Database Troubleshooter** section.

Step 8 Start the services that you stopped previously.

a. From Cisco Unified IM and Presence Serviceability, choose **Tools** > **Control Center - Feature Services**.

b. From the **Server** menu, select an IM and Presence node and click **Go**.

c. Under **IM and Presence Services**, select the following services:

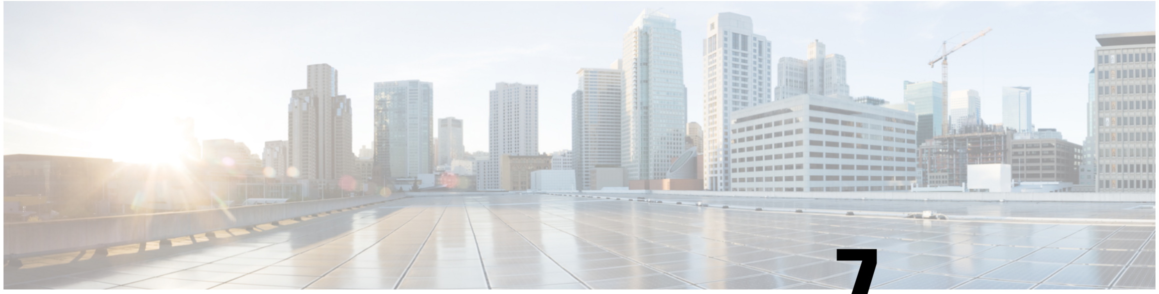
   Cisco XCP Text Conference Manager

   Cisco XCP File Transfer Manager

   Cisco XCP Message Archiver

d. 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.



CHAPTER 7

Post-Upgrade Tasks

Post-upgrade Task Flow

Perform the tasks in this list for all upgrade and migration methods.

Procedure

	Command or Action	Purpose
Step 1	Update CTL file, on page 103	If the cluster is in mixed mode, manually update the CTL file. Reset the phones to reflect the latest updates. **Note** You can skip this for Unified Communications Manger Migration.
Step 2	Remove the Serial Port, on page 103	Remove the serial port that you added during the pre-upgrade tasks so that it does not impact VM performance. Perform this procedure for all nodes.
Step 3	Restart Extension Mobility, on page 103	If you deactivated Cisco extension mobility as part of the pre-upgrade tasks, you can now restart it.
Step 4	Run the post upgrade COP.	The post-upgrade COP runs a series of tests to verify system stability. These tests compare pre and post upgrade settings in order identify differences. After you complete all the steps in this table, run the post-upgrade COP file again and verify the COP report.

	Command or Action	Purpose
		Note When you try to upgrade, using COP files it shows the number of files installed in the system. Once the upgrade is done the list of COP files will not match previous versions. If you need the previous files you need to install COP files manually. **Note** If you execute CLI command " show risdb query cti", it will show the details of the device registered with the node. The device must be at least registered once in that node to make the entry. For example, if the devices were registered in subscribe 2 and then got unregistered and moved to subscribe 1, and you execute this command in subscribe 2, it shows as unregistered.
Step 5	Reset TFTP Parameters, on page 105	Reset TFTP parameters that are changed during the upgrade process.
Step 6	Restore Enterprise Parameters, on page 106	Restore any Enterprise Parameter settings on IM and Presence Service nodes that may have been overwritten during the upgrade process.
Step 7	Reset High and Low Watermarks, on page 106	Use this procedure to restore the high and low watermarks to their original values in order to avoid premature purging of traces. You can skip this task for PCD migrations.
Step 8	Updating VMware Tools, on page 107	You must update the VMWare Tools after you complete the upgrade. Perform this procedure for all nodes.
Step 9	Install Locales, on page 107	After an upgrade, you must reinstall any locales that you are using, with the exception of US-English, which is installed by default. Perform this procedure for all nodes.
Step 10	Restore the Database Replication Timeout, on page 108	Use this procedure if you increased the database replication timeout value before you began the upgrade process.

	Command or Action	Purpose
		Perform this procedure on Unified Communications Manager nodes only.
Step 11	Verify the Registered Device Count, on page 109	Use this procedure to verify your endpoints and resources on Unified CM nodes after the upgrade is complete.
Step 12	Verify Assigned Users, on page 109	Use this procedure to verify the number of assigned users on IM and Presence Service nodes after the upgrade is complete.
Step 13	Test Functionality, on page 109	Verify phone functions and features are working correctly after the upgrade.
Step 14	Upgrade RTMT, on page 110	If you use Cisco Unified Real Time Monitoring Tool (RTMT), upgrade to the new software version.
Step 15	Manage TFTP Server Files, on page 111	Optional. Use this procedure to upload phone rings, callback tones, and backgrounds to a TFTP server so that they are available to Unfiied CM nodes.
Step 16	Set Up a Custom Log-On Message, on page 112	Optional. For Unified CM nodes only, upload a text file that contains a customized log-on message.
Step 17	Configure IPSec Policies, on page 113	If you are completing a PCD migration from Release 6.1(5), you must recreate your IPSec policies as they are not migrated to the new release.
Step 18	Assign New Manager Assistant Roles, on page 113	If you had Manager Assistant deployed before the upgrade and users were assigned to the InterCluster Peer-User or Admin-CUMA roles, you must reassign users to roles, as these roles do not exist in the current release.
Step 19	Verify IM and Presence Service Data Migration, on page 114	Use this procedure only if you performed an upgrade or migration from Cisco Unified Presence Release 8.x to an IM and Presence Service release.
Step 20	Enable High Availability on Presence Redundancy Groups, on page 115	If you disabled High Availability for the IM and Presence Service Service before the upgrade process, use this procedure to turn it back on.
Step 21	Restart the IM and Presence Sync Agent, on page 115	If you stopped the IM and Presence Service Sync Agent service before you began the upgrade process, restart it now.

	Command or Action	Purpose
Step 22	Restart Cisco Emergency Responder Service, on page 116	For the AXL Connection to be established after Unified Communications Manager upgrades, restart the CER service. You also need to restart the AXL Change notification toggle on the Unified CM publisher node.

Switch the Software Version

When you perform a standard upgrade, the new software is installed as an inactive version. You can reboot to the new software during the upgrade process or you can switch to the new version later.

If you did not switch versions immediately after completing the upgrade, do so now. You must switch versions so that the upgrade is complete and all nodes in the cluster are updated. Do not perform a backup until you have switched to the new software version.

When you switch versions, the system restarts, and the inactive software becomes active. The system restart may take up to 15 minutes. When you perform this procedure both the active and inactive software versions are indicated.

⚠

Caution This procedure causes the system to restart and become temporarily out of service.

Before you begin

The software versions on Unified Communications Manager and IM and Presence Service nodes must match according to the manual switching rules. Therefore, you must switch Unified Communications Manager before you switch IM and Presence Service.

Review the information in Understanding Version Switching, on page 65

Procedure

Step 1 If you switch versions in a multinode deployment, you must switch the publisher node first.

Step 2 Log in to the management software for the node that you are upgrading:

- If you are upgrading an IM and Presence Service node, log in to Cisco Unified IM and Presence Operating System Administration.
- If you are upgrading a Unified Communications Manager node, log in to Cisco Unified Communications Operating System Administration.

Step 3 Select **Settings** > **Version**.

Step 4 Verify the version of the active software and the inactive software.

Step 5 Select **Switch Versions** to switch versions and restart the system.

After you perform a switch version when you upgrade Unified Communications Manager, IP phones request a new configuration file. This request results in an automatic upgrade to the device firmware.

Update CTL file

During an upgrade from Unified Communications Manger pre 12.0 to 12.0 or later version, the ITLRecovery certificate is generated per cluster. If the cluster is in mixed mode, manually update the CTL file. Reset the phones to reflect the latest updates.

Note From Release 12.5(1)SU3 Update CTL is no longer required.

Procedure

Step 1 Verify Unified Communications Manager Security Mode in **Unified Communications Manager Administration** > **System** > **Enterprise Parameters Configuration**.

Locate the **Cluster Security Mode** field. If the value in the field displays as 1, Unified Communications Manager is configured for mixed mode.

Step 2 Manually update CTL file. For more information on how to update CTL file, see Security Guide for Cisco Unified Communications Manager.

Step 3 Reset the phones to reflect the updates.

Remove the Serial Port

During the pre-upgrade tasks, you added a serial port to the virtual machine to capture the upgrade logs. After you have successfully upgraded the system, you must remove the serial port so that it does not impact the performance of the virtual machine.

Procedure

Step 1 Power off the virtual machine.

Step 2 Edit the settings to remove the serial port. For information about how to edit the settings, see the VMWare documentation.

Step 3 Power on the virtual machine and proceed with the post-upgrade tasks.

Restart Extension Mobility

Upgrades from Release 9.x or earlier require you to stop Cisco extension mobility before you begin the upgrade process. If you deactivated Cisco extension mobility as part of your pre-upgrade tasks, use this procedure to restart the service on Unified Communications Manager nodes.

Procedure

Step 1 From Cisco Unified Serviceability, choose **Tools** > **Service Activation**.

Step 2 From the **Server** list, choose the node on which you want to deactivate services and click **Go**.

Step 3 Select the **Cisco Extension Mobility** services.

Step 4 Click **Restart**.

Run Upgrade Readiness COP File (Post-upgrade)

After upgrading, run the post-upgrade COP file, which checks the following:

- Installed COP Files
- Network services and connectivity (DNS, NTP, intra-cluster)
- FIPS mode password length restrictions
- Licensing sync
- VMware tools compatibility
- Disk space
- SIP and H.323 trunk registrations
- Database authentication and replication status
- Database sanity
- Status of last DRS backup
- Services status
- Installed COPs and Locales
- Device Registration Status Count
- Enterprise Parameter and Service Parameter settings
- TFTP Maximum Service Counts
- Active and Inactive versions

Note It's strongly recommended that you run the Upgrade Readiness COP file for post-upgrade checks after you upgrade in order to verify the health of your system.

Procedure

Step 1 Download the Upgrade Readiness COP file to run post upgrade tests.

a) Go to the Downloads site.

b) Select the destination release and then select **Unified Communications Manager Utilities**.

c) Download the **Upgrade Readiness COP file in order to run pre-upgrade tests** (For example, `ciscocm.postUpgradeCheck-00019.cop.sgn`. Note that the latest file may have a different filename and version.).

Step 2 Check your post-upgrade system health:

a) Run the COP file.

b) Resolve any issues that the COP file returns.

c) Repeat these steps until the COP file returns no errors.

Step 3 To view the reports from CLI for post-upgrade run **file get install/PostUpgradeReport.txt** command.

Step 4 To view the report from RTMT

a) Login into RTMT.

b) In **Trace and Log Central** double click on **Remote Browse** and select **Trace files** click **Next**.

c) Select **Select all Services on all servers** and click **Next**.

d) Click **Finish** and **Close**.

e) Double click on nodes, expand **CUCM Publisher > System > Install upgrade Logs**.

f) Double click on **Install** and select the file which you require and download.

What to do next

The upgrade is complete. You can begin using the new software.

Reset TFTP Parameters

During the upgrade process, the TFTP service parameter **Maximum Serving Count** is changed to allow for an increased number of device registration requests. Use this procedure to reset the parameter after the upgrade is complete.

Procedure

Step 1 From the Cisco Unified CM Administration interface, choose **System** > **Service Parameters**.

Step 2 From the **Server** drop-down list, select the node that is running the TFTP service.

Step 3 From the **Service** drop-down list, select **Cisco TFTP service**.

Step 4 Click **Advanced**.

Step 5 Click **Save**.

Step 6 Set the **Maximum Serving Count** to the same value that you used prior to the upgrade, or to the value that is recommended for your configuration.

The default value is 500. We recommend that you use the default value if you run the TFTP service with other Cisco CallManager services on the same server. For a dedicated TFTP server, use the following values:

- 1500 for a single-processor system
- 3000 for a dual-processor system

- 3500 for dedicated TFTP servers with higher CPU configurations

Restore Enterprise Parameters

Some Enterprise Parameters exist on both Unified Communications Manager nodes and IM and Presence Service nodes. Where the same parameter exists, the settings that are configured on Unified Communications Manager nodes overwrite the settings configured on IM and Presence Service nodes during an upgrade. Enterprise Parameters that are unique to IM and Presence Service nodes are retained during an upgrade.

Use this procedure to reconfigure the settings on IM and Presence Service nodes that have been overwritten during the upgrade process.

Before you begin

Make sure you have access to the settings that you recorded as part of the pre-upgrade tasks.

Procedure

Step 1 From the Cisco Unified CM IM and Presence Administration interface, choose **System** > **Enterprise Parameters**.

Step 2 Compare the current settings to the settings that existed prior to the upgrade and update the Enterprise Parameters as needed.

Step 3 Click **Save**.

Step 4 Click **Reset**, and then click **OK** to reset all devices.

Reset High and Low Watermarks

Use this procedure to restore the high and low watermarks to their original values in order to avoid premature purging of traces.

Procedure

Step 1 In the Real Time Monitoring Tool (RTMT) interface, double-click **Alert Central** in the left navigation pane.

Step 2 On the **System** tab, right-click **LogPartitionLowWaterMarkExceeded** and select **Set Alert/Properties**.

Step 3 Select **Next**.

Step 4 Adjust the slider value to 80.

Step 5 On the **System** tab, right-click **LogPartitionHighWaterMarkExceeded** and select **Set Alert/Properties**.

Step 6 Select **Next**.

Step 7 Adjust the slider value to 85.

Updating VMware Tools

VMware Tools are a set of utilities for management and performance optimization. Unified Communications Manager 15 supports only the Open VMware Tool.

- For upgrades or migrations from Unified Communications Manager Release 12.5(1) or 14 and SUs to 15 (for example, to a higher SU), the Open VMware tool is installed by default.
- For fresh installation and PCD migrations from Unified Communications Manager Release 11.5(1) onwards, the Open VMware tool is installed by default.

Execute the command **utils vmtools status** to ensure that VMware tools are currently running.

Install Locales

Use this procedure to install locales. After an upgrade, you must reinstall any locales that you are using, with the exception of US-English, which is installed by default. Install the latest version of the locales that match the major.minor version number of your Unified Communications Manager node orIM and Presence Service node.

You can install locales on Unified Communications Manager or on IM and Presence Service nodes. If you are installing a locale for both products, install the locale on all cluster nodes in the following order:

1. Unified Communications Manager publisher node
2. Unified Communications Manager subscriber nodes
3. IM and Presence database publisher node
4. IM and Presence subscriber nodes

If you want to install specific locales on IM and Presence Service nodes, you must first install the Unified Communications Manager locale file for the same country on the Unified Communications Manager cluster.

Procedure

Step 1 Find the locale installer for your release on cisco.com:

- For Cisco Unified Communications Manager, go to https://software.cisco.com/download/navigator.html?mdfid=268439621&i=rm
- For IM and Presence Service, go to https://software.cisco.com/download/navigator.html?mdfid=280448682&i=rm

Step 2 Download your release's locale installer to a server that supports SFTP. You need the following files:

- User Locale files—These files contain language information for a specific language and country and use the following convention:
  - `cm-locale-language-country-version.cop` (Cisco Unified Communications Manager)
  - `ps-locale-language_country-version.cop` (IM and Presence Service)

- Combined Network Locale file—Contains country-specific files for all countries for various network items, including phone tones, annunciators, and gateway tones. The combined network locale file uses the following naming convention:
    - `cm- locale-combinednetworklocale-version.cop` (Cisco Unified Communications Manager)

Step 3 Log in to Cisco Unified OS Administration using the administrator account.

Step 4 Choose **Software Upgrades** > **Install/Upgrade**.

Step 5 Complete the following fields in the **Software Installation/Upgrade** window:

- For the **Source**, choose **Remote file System**.
- From the **Directory**, enter the path to the directory where you saved the locale installer.
- From the **Server** field, enter the server name for the remote file system.
- Enter the credentials for the remote file system.
- From the **Transfer Protocol** drop-down list, choose **SFTP**. You must use SFTP for the transfer protocol.

Step 6 Click **Next**.

Step 7 Download and install the locale on the server.

Step 8 Restart the server. The updates take effect after the server restarts

Step 9 Repeat this procedure on all Unified Communications Manager and IM and Presence Service cluster nodes in the prescribed order.

Note Do not reset user locales for your end users until the new locale is installed on all cluster nodes. If you are installing the locale for both Unified Communications Manager and IM and Presence Service Service, you must install the locale for both products before you reset user locales. If you run into any issues, such as could occur if an end user resets a phone language before the locale installation is complete for IM and Presence Service Service, have your users reset their phone language in the Self-Care Portal to English. After the locale installation is complete, users can reset their phone language, or you use Bulk Administration to synchronize locales to the appropriate language by bulk.

Restore the Database Replication Timeout

This procedure applies to Unified Communications Manager nodes only.

Use this procedure if you increased the database replication timeout value before you began the upgrade process.

The default database replication timeout value is 300 (5 minutes). Restore the timeout to the default value after the entire cluster upgrades and the Unified Communications Manager subscriber nodes have successfully set up replication.

Procedure

Step 1 Start a CLI session using one of the following methods:

- From a remote system, use SSH to connect securely to the Cisco Unified Operating System. In your SSH client, enter your `ssh adminname@hostname` and enter your password.
- From a direct connection to the serial port, enter your credentials at the prompt that displays automatically.

Step 2 Execute the **utils dbreplication setrepltimeout** *timeout* command, where *timeout* is database replication timeout, in seconds. Set the value to 300 (5 minutes).

Verify the Registered Device Count

Use the Cisco Real -Time Monitoring Tool (RTMT) to view the device count and verify your endpoints and resources after the upgrade is complete.

Procedure

Step 1 From the Unified RTMT interface, select **Voice/Video** > **Device Summary**.

Step 2 Record the number of registered devices:

Item	Count
Registered Phones	
Registered Gateways	
Registered Media Resources	
Registered Other Station Devices	

Step 3 Compare this information to the device counts that you recorded before the upgrade and ensure that there are no errors.

Verify Assigned Users

Use this procedure to verify the number of assigned users on nodes after the upgrade is complete.

Procedure

Step 1 From the Cisco Unified CM IM and Presence Administration interface, select **System** > **Cluster Topology**.

Step 2 Compare this information to the number of assigned users that you recorded before the upgrade and ensure that there are no errors.

Test Functionality

After the upgrade, perform the following tasks:

- Run the post-upgrade COP.

  It runs a series of tests to verify that the system is stable. It also compares various parameters before the upgrade with the current version to identify any differences. After you complete all the steps in this list, run the post-upgrade COP file again and verify the COP report.

- Verify phone functions by making the following types of calls:
  - Voice mail
  - Interoffice
  - Mobile phone
  - Local
  - National
  - International
  - Shared line
- Test the following phone features:
  - Conference
  - Barge
  - Transfer
  - C-Barge
  - Ring on shared lines
  - Do Not Disturb
  - Privacy
  - Presence
  - CTI call control
  - Busy Lamp Field
- Test IM and Presence Service functions:
  - Basic presence states, such as available, unavailable, and busy
  - Send and receive files
  - Advanced features, such as persistent chat, federated users, and message archiving

Upgrade RTMT

Tip To ensure compatibility, we recommend that you upgrade RTMT after you complete the upgrade on all servers in the cluster.

RTMT saves user preferences and downloaded module jar files locally on the client machine. The system saves user-created profiles in the database, so you can access these items in Unified RTMT after you upgrade the tool.

Before you begin

Before you upgrade to a newer version of RTMT, we recommend that you delete the previous or older versions of the unzipped CiscoRTMTPlugin.zip folder.

Procedure

Step 1 From Unified Communications Manager Administration, choose **Application** > **Plugins**.

Step 2 Click **Find**.

Step 3 To install Unified RTMT on a client that is running on Linux or Microsoft Windows operating system, download the CiscoRTMTPlugin.zip from the **Download** link for the Cisco Unified Real-Time Monitoring Tool - Windows and Linux Tool.

Tip When you install Unified RTMT on Windows 10 or later, only administrators with privileges can launch RTMT.

Step 4 Download the CiscoRTMTPlugin.zip to the preferred location on your client.

Step 5 To install the Windows version,

a) Unzip the CiscoRTMTPlugin.zip file.
b) Double-click the `run.bat` file.

Step 6 To install the Linux version,

a) Unzip the CiscoRTMTPlugin.zip file.
b) Once the files are extracted, you must set permissions to the `run.sh` file by executing the command **chmod 755 run.sh**.
c) Double-click the `run.sh` file.

Manage TFTP Server Files

You can upload files for use by the phones to the TFTP server. Files that you can upload include custom phone rings, callback tones, and backgrounds. This option uploads files only to the specific server to which you connected, and other nodes in the cluster do not get upgraded.

Files upload into the **`tftp`** directory by default. You can also upload files to a subdirectory of the **`tftp`** directory.

If you have two Cisco TFTP servers that are configured in the cluster, you must perform the following procedure on both servers. This process does not distribute files to all nodes, nor to both Cisco TFTP servers in a cluster.

To upload and delete TFTP server files, follow this procedure:

Procedure

Step 1 From the Cisco Unified Communications Operating System Administration window, navigate to **Software Upgrades** > **TFTP** > **File Management**.

The TFTP File Management window displays and shows a listing of the current uploaded files. You can filter the file list by using the Find controls.

Step 2 To upload a file, follow this procedure:

a) Click **Upload File**.

   The Upload File dialog box opens.

b) To upload a file, click **Browse** and then choose the file that you want to upload.
c) To upload the file to a subdirectory of the `tftp` directory, enter the subdirectory in the **Directory** field.
d) To start the upload, click **Upload File**.

   The Status area indicates when the file uploads successfully.

e) After the file uploads, restart the Cisco TFTP service.

   Note If you plan to upload several files, restart the Cisco TFTP service only once, after you have uploaded all the files.

Step 3 To delete files, follow this procedure:

a) Check the check boxes next to the files that you want to delete.

   You can also click **Select All** to select all of the files, or **Clear All** to clear all selection.

b) Click **Delete Selected**.

   Note If you want to modify a file that is already in the `tftp` directory, you can use the CLI command **file list tftp** to see the files in the TFTP directory and **file get tftp** to get a copy of a file in the TFTP directory. For more information, see Command Line Interface Reference Guide for Cisco Unifed Communications Solutions.

Set Up a Custom Log-On Message

You can upload a text file that contains a customized log-on message that appears in Cisco Unified Communications Operating System Administration, Cisco Unified CM Administration, Cisco Unified Serviceability, Disaster Recovery System Administration, Cisco Prime License Manager, and the command line interface.

To upload a customized log-on message, follow this procedure:

Procedure

Step 1 From the Cisco Unified Communications Operating System Administration window, navigate to **Software Upgrades** > **Customized Logon Message**.

The Customized Logon Message window displays.

Step 2 To choose the text file that you want to upload, click **Browse**.

Step 3 Click **Upload File**.

Note You cannot upload a file that is larger than 10kB.

The system displays the customized log-on message.

Step 4 To revert to the default log-on message, click **Delete**.

Your customized log-on message gets deleted, and the system displays the default log-on message.

Note Check the **Require User Acknowledgment** checkbox if you want the custom message to be displayed on the login screens of the Cisco Unified Communications Operating System Administration, Cisco Unified CM Administration, Cisco Unified Serviceability, Disaster Recovery System Administration, Cisco Prime License Manager, and the command line interface.

Configure IPSec Policies

Use this procedure only if you are performing a PCD migration from Release 10.5. You must reconfigure your IPSec policies after the PCD migration is complete. Before migration, you must disable the IPSec policy in both the nodes of the cluster. And after successful migration, ensure that you enable the IPSec policy.

- IPSec requires bidirectional provisioning, or one peer for each host (or gateway).
- When you provision the IPSec policy on two Unified Communications Manager nodes with one IPSec policy protocol set to “ANY” and the other IPSec policy protocol set to “UDP” or “TCP”, the validation can result in a false negative if run from the node that uses the “ANY” protocol.
- IPSec, especially with encryption, affects the performance of your system.

Procedure

Step 1 From Cisco Unified OS Administration, choose **Security** > **IPSec Configuration**.

Step 2 Click **Add New**.

Step 3 Configure the fields on the **IPSEC Policy Configuration** window. See the online help for more information about the fields and their configuration options.

Step 4 Click **Save**.

Step 5 (Optional) To validate IPsec, choose **Services** > **Ping**, check the **Validate IPsec** check box, and then click **Ping**.

Assign New Manager Assistant Roles

Perform this procedure only if your previous release was configured to use the Cisco Unified Communications Manager Assistant feature, and you assigned application users to use either the InterCluster Peer-User or the

Admin-CUMA roles. The InterCluster Peer-User and Admin-CUMA roles are deprecated from release 10.0(1) onward and are removed during the upgrade process. You must assign new roles for those users.

Procedure

Step 1 To configure roles and users, see the chapter *Manage Users* in Administration Guide for Cisco Unified Communications Manager.

Step 2 Ensure that the AXL user defined on the IM and Presence Service service user interface (**Presence** > **Inter-Clustering**) has a Standard AXL API Access role associated with it on the Unified Communications Manager application user page.

Verify IM and Presence Service Data Migration

When you upgrade from Cisco Unified Presence Release 8.x to an IM and Presence Service Service release, user profiles are migrated to Unified Communications Manager. The user profile information is stored as new service profiles on Unified Communications Manager with the following name and description format:

Name: UCServiceProfile_Migration_x (where x is a number starting at 1)

Description: Migrated Service Profile Number x

To ensure that users can successfully log into Cisco Jabber after an upgrade from Cisco Unified Presence Release 8.x, you must verify that the user profile data migration was successful.

Profiles that are created but that are not assigned to users are *not* migrated to Unified Communications Manager.

Procedure

Step 1 From Cisco Unified CM Administration, select **User Management** > **User Settings** > **Service Profile**.

Step 2 Select **Find** to list all service profiles.

Step 3 Verify that there are migrated service profiles with the following name format: *UCServiceProfile_Migration_x*

Step 4 If there are no migrated service profiles, check the `installdb log` file for any errors.

Step 5 If the data migration fails, an import error alarm is raised on Unified Communications Manager and the Cisco Sync Agent sends a failure notification to the Cisco Unified CM IM and Presence Administration GUI.

Tip To view the alarm details, log into RTMT for Cisco Unified Communications Manager.

What to do next

You can edit these service profiles to give them more meaningful names. See Administration Guide for Cisco Unified Communications Manager for more information about configuring service profiles.

Run the post-upgrade COP file. It runs a series of tests to verify that the system is stable. It also compares various parameters before the upgrade with the current version to identify any differences.

Enable High Availability on Presence Redundancy Groups

This procedure applies to IM and Presence Service nodes only. If you disabled high availability on presence redundancy groups before beginning the upgrade process, use this procedure to enable it now.

Before you begin

If it has been less than 30 minutes since your services restarted, confirm that your Cisco Jabber sessions have been recreated before you enable High Availability. Otherwise, Presence will not work for Jabber clients whose sessions aren't created.

To obtain the number of Jabber sessions, run the `show perf query counter "Cisco Presence Engine" ActiveJsmSessions` CLI command on all cluster nodes. The number of active sessions should match the number of users that you recorded when you disabled high availability prior to the upgrade.

Procedure

Step 1 From the Cisco Unified CM Administration user interface, choose **System** > **Presence Redundancy Groups**.

Step 2 Click **Find** and select the Presence Redundancy Group.
The Presence Redundancy Group Configuration window displays.

Step 3 Check the **Enable High Availability** check box.

Step 4 Click **Save**.

Step 5 Repeat this procedure in each Presence Redundancy Group.

Restart the IM and Presence Sync Agent

If you stopped the IM and Presence Service Sync Agent service before you began the upgrade process, restart it now.

Procedure

Step 1 From the Cisco Unified Serviceability interface, select **Tools** > **Control Center - Network Services**.

Step 2 Select an IM and Presence Service node from the **Server** drop-down list and click **Go**.

Step 3 In the **IM and Presence Services** section, select the **Cisco Sync Agent** and click **Restart**.

Example

Note After the Cisco Intercluster Sync Agent has finished the initial synchronisation, manually load the new Tomcat certificate onto Unified Communications Manager. This ensures that the synchronisation does not fail.

Note Run the post-upgrade COP. It runs a series of tests to verify that the system is stable. It also compares various parameters before the upgrade with the current version to identify any differences.

Restart Cisco Emergency Responder Service

Procedure

If you stopped the Cisco Emergency Responder service before you began the upgrade process, restart it now.

Step 1 From the Cisco Emergency Responder serviceability interface, select **Tools** > **Control Center**.

Step 2 Select **Cisco Emergency Responder** and click **Restart**.

CHAPTER 8

Upgrading from Legacy Releases

Upgrading and Migrating from Legacy Releases

If a direct upgrade or migration from your current release is not supported, you can use the following process:

- perform a direct upgrade to an intermediate release using either the Unified CM OS Admin interface or the Cisco Prime Collaboration Deployment (PCD) Upgrade task
- perform a migration from the intermediate release to the current release using the PCD Migration task

Find your starting release in the table below and use it to identify the intermediate releases that you can use as steps in the upgrade and migration process. After you have identified the intermediate release, use the links in the steps below to find the documentation for that release.

If your starting release is not listed, it may require an upgrade to more than one intermediate release. See the "Supported Upgrade and Migration Paths with COP Files" table at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/compat/15_x/cucm_b_compatibility-matrix-cucm-imp-15x.html.

Table 13: Upgrade to Unified CM and IMP and Presence Service Release 15 from Legacy Releases

Installed Version	Migrate to this Version on a Virtual Machine
7.0(1) and older	Migration is not possible. You are recommended to rebuild to the latest release from scratch.
8.0(1) and 9.1	Using PCD 12.6 (not PCD 14 or PCD 15), direct migrate to version 12.5. See the initial chapters in this guide to go through the various migration options possible.

Procedure

Step 1 Refer to the upgrade documentation for the intermediate release and follow the instructions to upgrade your system.

- For Unified Communications Manager upgrade documentation, see http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-guides-list.html.
- For IM and Presence Service (formerly Cisco Unified Presence) upgrade documentation, see http://www.cisco.com/c/en/us/support/unified-communications/unified-presence/products-installation-guides-list.html.

Step 2 Refer to the *Cisco Prime Collaboration Deployment Administration Guide* at http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html and follow the instructions to perform a PCD migration to the current release.

CHAPTER 9

Troubleshooting

Dump a Log File After an Upgrade Failure

Use this procedure in the event of a failure when you are upgrading Unified Communications Manager or the IM and Presence Service.

Before you begin

You need the 7-Zip utility to open the log files. Go to http://www.7-zip.org/download.html

Procedure

Step 1 Attach a new, empty file to the serial port. Edit the settings on the VM and attach the file name where you want the logs dumped.

Note If the system stops running due to an upgrade failure and prompts you to dump the logs, you must attach the empty file before you answer **Yes** and proceed.

Step 2 Return to the VM console, and dump the logs into the serial port.

Step 3 When the process is complete, click **Inventory** > **Datastores and Datastore Clusters**.

Step 4 Select the datastore where you created the file.

Step 5 Right-click and choose **Browse Datastore** and browse to the file that you created.

Step 6 Right-click the file, select **Download**, and select a location on your PC to save the file.

Step 7 Open the file using 7-Zip and check the file size:

- If the size of the file is larger than 0, extract the files to your PC and then edit the settings on the virtual machine to remove the serial port.
- If the file size is 0, proceed to the next step.

Step 8 If the file size is zero, complete the following steps:

a) Power off the virtual machine.

b) Create a new file for log output.
c) Unmap the installation disk.
d) On the **Options** tab, select **Boot Options** and enable **Force BIOS Setup**.
e) Power on the virtual machine and wait for it to boot to the BIOS.
f) In the BIOS, select the hard drive as the first boot device and save and exit.
The system will boot to the hard drive and go back to the point where the upgrade failed. A failure notification displays.
g) Input **yes** to dump the contents of the log to a file.
h) Navigate to the file and open it using 7-Zip.

Step 9 If the size of the file is larger than 0, extract the files to your PC and then edit the settings on the virtual machine to remove the serial port.

Troubleshooting Unified Communications Manager Upgrades

This section provides information about troubleshooting Unified Communications Manager upgrades.

Upgrade Failure

Problem The upgrade of a subscriber node fails after you upgrade the Unified Communications Manager publisher node and switch it to the new version, or the upgrade of one of the subscriber nodes in your cluster failed during the upgrade cycle.

Solution Do one of the following:

- Correct the errors that caused the upgrade failure on the subscriber node. You may want to check the network connectivity of the nodes in your cluster, reboot the subscriber node, and ensure that the server memory and CPU usage on the subscriber node is not too high. Upgrade the subscriber node again.

- Make sure that the active partition of the Unified Communications Manager publisher node runs the newest version of software installed on the server. Perform a fresh installation on the subscriber node using the same software version as that running on the active partition of the publisher node. If you are reinstalling the subscriber node, you should delete the server from Cisco Unified CM Administration and add the server again as described in the Administration Guide for Cisco Unified Communications Manager.

Retrying a Cluster or Single-node Upgrade

If you are retrying an upgrade without performing a Switch Version or Reboot in the previous upgrade, then, reboot the nodes before retrying.

Reboot include on upgrade Success/Failed/Cancel case

Problem: Upgrades might fail or disturb if we didn’t reboot in below stages.

Solution: Reboot is required in the following scenarios:

1. Any upgrade (Legacy upgrade/Simple upgrade or Upgrade via PCD) get success or failure:

- When an L2 upgrade fails, a reboot is required only in case when an upgrade is required again.
- After a successful L2 upgrade, if you do not wish to switch to the new version and would like to upgrade again, you need to reboot the node first before starting the upgrade.
- When an RU upgrade fails, it automatically switches to old partition and an automatic reboot is performed (if upgrade status is failed, cancel the upgrade and reboot the node).

2. If the Switch version fails, you should reboot the server before you attempt any further action, as it may stop/ halt the Service Manager and other services that could impact functionalities.
3. If you cancel any upgrade at any stage, you should reboot the IM&P/ UCM servers before you attempt any other upgrade.

Troubleshooting Simplified Upgrade Issues

Download Failure in Some Nodes of the Cluster

Problem: Download failed in some nodes of the cluster while performing simplified upgrade.

Solution: Verify the Software location configuration for the nodes that failed to download. Invalid location or wrong credentials may cause the failure. If you are using the 'Use download credentials from publisher' option, then, ensure that the configuration of the failed node is correct.

To verify, perform one of the following:

- User Interface: Open the **Install/Upgrade** page of the node and see if the check box is checked. If it is checked, it indicates that the configuration is correct. If the check box is not checked, check it and click **Next** to save the configuration and then click **Cancel** to exit from the **Install/Upgrade** page.
- CLI: Use the **utils system upgrade initiate** command, and ensure that ‘Use download credentials from Publisher (yes/no)’ is set to ‘yes’. If it is set to ‘yes’, it indicates that the configuration is correct. If not, set it to ‘yes’ and come out by selecting ‘q’ and execute the **utils system upgrade cancel** command for a clean exit.

Note **Use download credentials from Publisher** is unselected and the Unified Communications Manager cluster upgrade may fail because the subscriber will not use the same download credentials of publisher. Need to go to each Subscriber and select the option "**Use download credential from Publisher**", for the subscriber to use the publisher download credentials.

Download or Installation Failure in Some Nodes of the cluster

Problem: Download or Installation failed in some nodes of the cluster while performing simplified upgrade.

Solution: Open the **Install/Upgrade Cluster** page using User Interface or the **utils system upgrade cluster status** command using the CLI and identify the failed nodes. Verify that the upgrade or install operation is not already in progress on those failed nodes by executing the **utils system upgrade status** command from the CLI. Follow the single node upgrade troubleshooting steps given in the 'Upgrade Failure' subsection in the 'Troubleshooting Unified Communications Manager Upgrades' section to continue the upgrade.

Note When simplified upgrade fails in Download or Install phase:

- User Interface: **Install/Upgrade Cluster** page displays the status of each node to identify the failed nodes until cancel is clicked.
- CLI: **utils system upgrade cluster initiate** or **utils system upgrade cluster status** displays the status of each node to identify the failed nodes until the **utils system upgrade cluster cancel** command is executed.

Switch Version or Reboot Failure in Some Nodes of the Cluster

Problem: Switch version or reboot failed in some nodes of the cluster while performing simplified upgrade.

Solution: Open the **Restart/Switch-Version Cluster** page using User Interface and identify the failed nodes. Fix the issues (network/certificate issue etc.) and retry the switch version or reboot on the failed nodes by skipping the completed nodes in the **Restart/Switch-Version Cluster** page.

Unified Communications Manager Publisher was rebooted/power-cycled During Cluster Upgrade and the Cluster Upgrade Status is not Visible

Problem: The Unified Communications Manager Publisher was rebooted/power cycled during cluster upgrade and the cluster upgrade status was not visible.

Solution: The Unified Communications Manager Publisher controls the cluster upgrade operations. You must not reboot or power cycle it during an upgrade. If you do that, the processes are killed and you cannot get status from other nodes. Also, the Unified Communications Manager Publisher will not be able to provide instructions to other nodes and results in upgrade failures. Login to each node and cancel the upgrade.

High CPU Alerts During Cluster Upgrade

Problem: High CPU alerts were received during Cluster upgrade

Solution: You need to schedule cluster upgrades during the least server usage. The upgrade processes are CPU and Disc-intensive and can cause CPU Alerts.

Retrying a Cluster Upgrade after a Failed Cluster Upgrade

Problem: How to retry a cluster upgrade after a failed cluster upgrade?

Solution: First, cancel the cluster upgrade. We recommend that you reboot the nodes after a failed upgrade before retrying an upgrade.

Download Failure due to SSL Error

Problem: Download failed in a few nodes nodes due to SSL error.

Solution: Ensure that the cluster has SSL trust set up between the nodes.

The Switch Version or Reboot of Cluster Nodes did not Occur as per the Modified Batch

Problem: The switch version or reboot of cluster nodes did not occur as per the modified batch.

Solution: Before starting a cluster reboot or switch version, ensure that the modified batch orders are saved.

Changes to 'Skip' Checkbox are not Saved

Problem: Skip check box selections are not saved.

Solution: The 'skip' option is used to exclude a node during reboot or switch version and this selection is not saved. You need to select the option every time.

Unable to Retry Cluster Upgrade or Single-node Upgrade

Problem: Unable to retry cluster upgrade or single-node upgrade.

Solution: Perform a cluster upgrade cancel by executing the **utils system upgrade cluster cancel** command using the CLI. Also, perform a single-node cancel on the Unified Communications Manager Publisher by executing the **utils system upgrade cancel** command using the CLI

Upgrade Fails with Insufficient Disk Space

Problem The upgrade of Unified Communications Manager fails with an error stating that the common partition is full.

Solution Typically, you need at least 25G of common partition space; however, your deployment may require more space if you have a lot of TFTP data (device firmware loads), music-on-hold (MOH) files, or if you have many locale files installed. Perform one or more of the following actions to create additional disk space:

- Use the Cisco Log Partition Monitoring Tool to adjust the low and high watermarks to reduce the traces and remove unnecessary log files. Cisco recommends that you adjust the low watermark value to 30, and the high watermark value to 40. After the upgrade, you must restore the high and low watermarks to their original values in order to avoid premature purging of traces. The default value for the high watermark is 85. The default value for the low watermark is 80. For more information about using the Cisco Log Partition Monitoring Tool, see the Cisco Unified Real-Time Monitoring Tool Administration Guide.

- Use the Disk Expansion COP file (ciscocm.vmware-disk-size-reallocation-<latest_version>.cop.sgn) to expand the vDisk size if your virtual environment has additional available disk space. Ensure that you review the Readme file that supports this COP file before you proceed.

- Use the Free Common Space COP file (ciscocm.free_common_space_v<latest_version>.cop.sgn). This COP file removes the inactive side in the common partition to increase available disk space without requiring a system rebuild. Ensure that you review the Readme file that supports this COP file before you proceed.

- Manually remove outdated or unused firmware files from the TFTP directory. You can remove these files using the TFTP File Management page in the OS Administration interface, or you can use the `file list tftp` and `file delete tftp` commands from the command line interface.

You can download COP files and their Readme files from Cisco.com. Navigate to **Support > Downloads > Cisco Unified Communications Manager Version 10.0 > Unified Communications Manager/CallManager/Cisco Unity Connection Utilities**.

Resuming a Failed Upgrade

If you find any errors in your system and you have to fix it before resuming an upgrade, follow this process:

Note You need to restart the node and reinitiate the upgrade process if there is a failure.

Procedure

Step 1 Cancel the upgrade.

The ISO file download is retained if fully downloaded, even if you cancel the upgrade.

Step 2 Fix your system issue.

Step 3 When you are ready to resume your upgrade, run the `utils system upgrade initiate` CLI command and select the `Local Image` option.

Step 4 Complete your system upgrade.

Reduced Permissions for Access Control Groups

Problem When you add a new access control group to existing users, the level of privileges for some pre-existing access control groups is unexpectedly reduced.

Solution Users can belong to multiple access control groups. When you add a new access control group to existing users, the current level of privileges for some pre-existing access control groups may be reduced if the new access control group has the “Effective Access Privileges for Overlapping User Groups and Roles” Enterprise parameter set to minimum.

Access privilege reduction can occur inadvertently, for example, during an upgrade of Cisco Unified CM Administration. If the upgrade version supports the Standard RealTimeAndTrace Collection user group, which has the “Effective Access Privileges for Overlapping User Groups and Roles” Enterprise parameter set to minimum, all users are automatically added to that user group during the upgrade. To resolve the permissions issue in this example, you can remove users from the Standard RealTimeAndTrace Collection user group.

Loss of Phone Settings

For a short period of time after you install Unified Communications Manager or switch over after upgrading to a different product version, settings that were configured by phone users may be reset. Examples of settings configured by phone users include call forwarding and message waiting indication settings. This situation can occur if there have been configuration changes during the upgrade window. When Unified Communications Manager synchronizes the database after an installation or upgrade, it can overwrite setting changes made by phone users. Cisco recommends that you do not make configuration changes during an upgrade.

Post-Upgrade Failure of Unified Communications Manager Publisher Node

Problem The upgrade is successful and the cluster is running the new release, but the Unified Communications Manager publisher node subsequently fails.

Solution Do one of the following:

- restore the Unified Communications Manager publisher node use a DRS backup file

- if you do not have a DRS backup file, you must reinstall the entire cluster, including any IM and Presence Service nodes

Post-Upgrade Failure of Unified Communications Manager Subscriber Nodes

Problem The upgrade is successful and the cluster is running the new release, but a Unified Communications Manager subscriber node subsequently fails.

Solution Do one of the following:

- Restore the Unified Communications Manager subscriber node use a DRS backup file.
- If you do not have a DRS backup file, you must perform the upgrade on the subscriber node again. You do not need to remove the subscriber node from the Unified Communications Manager publisher node's server page before you reinstall it.

Troubleshooting IM and Presence Upgrades

This section provides information about troubleshooting IM and Presence Service Service upgrades.

Upgrade Failure of IM and Presence Database Publisher Node

Problem You are upgrading a multinode cluster that includes both Unified Communications Manager and IM and Presence Service nodes, and the upgrade of the IM and Presence Service database publisher node fails.

Solution The action that you take depends on the point at which the failure occurred:

- If the failure occurred after the IM and Presence Service database publisher node switched to the new software version, you must switch back all the nodes and perform the upgrade again. Complete the following tasks in the order listed:
  - switch back the Unified Communications Manager publisher node
  - switch back the Unified Communications Manager subscriber nodes
  - switch back the IM and Presence Service database publisher node
  - upgrade the Unified Communications Manager publisher node again
  - switch the Unified Communications Manager publisher node forward to the new software version
  - upgrade the Unified Communications Manager subscriber nodes again
  - switch the Unified Communications Manager subscriber nodes forward to the new software version
  - upgrade the IM and Presence Service database publisher node again

Upgrade Failure of IM and Presence Subscriber Node

Problem You are upgrading a multinode cluster that includes both Unified Communications Manager and IM and Presence Service nodes, and the upgrade of the IM and Presence Service subscriber node fails.

Solution The action that you take depends on the point at which the failure occurred:

- if the upgrade on the IM and Presence Service subscriber node fails after the node switched to the new version, you must complete the following tasks in the order listed:
  - switch the Unified Communications Manager publisher node back to the earlier software version
  - switch the Unified Communications Manager subscriber node back to the earlier software version
  - switch the IM and Presence Service database publisher node back to the earlier software version
  - switch the IM and Presence Service subscriber nodes back to the earlier software version
  - switch the Unified Communications Manager publisher node pub forward to the new software version
  - switch the IM and Presence Service database publisher node forward to the new software version
  - perform the upgrade again on the IM and Presence Service subscriber node

IM and Presence user phone presence problems

Problem After an IM and Presence server upgrade, when all activated feature services and network services are started, IM and Presence phone presence from users is delayed or slow to update.

Solution You must restart the Cisco SIP Proxy service. In Cisco Unified IM and Presence Serviceability, select **Tools** > **Control Center - Features Services**.

Presence User Experiences Issues Obtaining Availability

Problem After an IM and Presence Service server upgrade, when all activated feature services and network services are started, a user experiences inconsistent presence availability. The user can log in to IM and Presence Service but experiences issues obtaining availability information mainly from SIP-based clients.

Solution This issue is caused when users are provisioned while IM and Presence Service is being upgraded. You must unassign and then reassign the user.

Real-Time Monitoring Tool alert for Cisco SIP proxy service

Problem After an IM and Presence Service server upgrade, when all activated feature services and network services are started, a Real-Time Monitoring Tool CoreDumpFileFound alert was generated for the Cisco SIP Proxy service.

Solution You must restart the Cisco SIP Proxy service. In Cisco Unified IM and Presence Serviceability, select **Tools** > **Control Center - Features Services**.

Cannot find upgrade file on remote server

Problem You cannot find the upgrade file on the remote server.

Solution If the upgrade file is located on a Linux or Unix server, you must enter a forward slash at the beginning of the directory path that you want to specify. For example, if the upgrade file is in the patches directory, you must enter **/patches**. If the upgrade file is located on a Windows server, check with your system administrator for the correct directory path.

Upgrade file checksum values do not match

Problem The checksum value of the upgrade file does not match the checksum indicated on Cisco.com.

Solution The two checksum values must match to ensure the authenticity and integrity of the upgrade file. If the checksum values do not match, download a fresh version of the file from Cisco.com and try the upgrade again.

Database replication did not complete

Problem After an upgrade, database replication did not complete and the result of the command **utils dbreplication runtimestate** was not 2.

Solution After a successful upgrade and switch version to the new software, database replication should take place automatically. During this time core services on the subscriber nodes will not start. Database replication in large deployments can take several hours to complete. If, after several hours, the **utils dbreplication runtimestate** command shows that database replication did not complete, you need to reset the database replication. Run the following command on the publisher node: `utils dbreplication reset all`

Version Errors

Version Does Not Match the Active or Inactive Version

Problem During an upgrade on a IM and Presence Service server, you cannot select the software image from the disk or remote directory. The following error is reported: `The version obtained from the name does not match the active or inactive version of the publisher.`

Solution The version matching rules have not been met. The software versions must meet the following requirements:

- The software version of the IM and Presence Service database publisher node (the first IM and Presence Service node that you upgrade) must match the first two numbers of the software version installed on the Unified Communications Manager publisher node. The software version installed on the Unified Communications Manager publisher node may be active or inactive. For example, IM and Presence Service software version 10.0.1.10000-1 is compatible with Unified Communications Manager software version 10.0.1.30000-2. Make sure to follow sequence rules while upgrading Unified Communications Manager and IM and Presence Service nodes.

- The software version of the IM and Presence Service subscriber nodes that you upgrade must match five numbers of the software version installed on the IM and Presence Service database publisher node.

Ensure that the first node that you upgrade is either the Unified Communications Manager publisher node or the IM and Presence Service database publisher node, or select a different image for the software upgrade.

Switch Version on Cisco IM and Presence Node Fails

Problem Switching the version on the Cisco IM and Presence node fails. The following error is reported: `Version mismatch. Please switch versions on the publisher and try again.`

Solution The version matching rules have not been met. The software versions must meet the following requirements:

- The software version of the IM and Presence Service database publisher node (the first IM and Presence Service node that you upgrade) must match the first two numbers of the software version installed on the Unified Communications Manager publisher node. For example, IM and Presence Service Service software version 10.0.1.10000-1 is compatible with Unified Communications Manager software version 10.0.1.30000-2.
- The software version of the IM and Presence Service subscriber nodes that you upgrade must match five numbers of the software version installed on the IM and Presence Service database publisher node.

To correct this error, ensure that the first node that you switch is either theUnified Communications Manager publisher node or the IM and Presence Service database publisher node.

Cancelled or failed upgrade

If you cancel an upgrade at any stage, or if an upgrade fails, you must reboot the IM and Presence Service server before you attempt another upgrade.

Directory Was Located and Searched but No Valid Options or Upgrades Were Available

Problem During an IM and Presence Service upgrade, the IM and Presence Service server generates the following error message, even though the upgrade path and file are valid:

```
The directory was located and searched but no valid options or upgrades
were available. Note, a machine cannot be downgraded so option and upgrade
files for previous releases were ignored.
```

Solution The upgrade manager checks for connectivity between IM and Presence Service and Unified Communications Manager to validate the version during the upgrade. If this fails, the IM and Presence Service server generates the error message even though the upgrade path and file are valid. Use a tool, such as the Cisco Unified CM IM and Presence Administration System Troubleshooter, to check that there is connectivity between IM and Presence Service and Unified Communications Manager before proceeding with the upgrade.

Common Partition Full Upgrade Failure

Problem The upgrade of IM and Presence Service fails with an error stating that the common partition is full.

Solution Download and apply the COP file ciscocm.free_common_cup_space_v<latest_version>.cop.sgn. This COP file cleans up the common partition and allows subsequent upgrades to proceed as normal.

CHAPTER 10

Frequently Asked Questions

Frequently Asked Questions

I am upgrading from a release of Unified Communications Manager or IM and Presence Service that has different requirements for the virtual environment than the new release. What do I need to do?

Verify the requirements for the new release using the information given in the table. After you have verified the requirements for the new release, see Virtual Machine Configuration Tasks, on page 59 for instructions.

Table 14: 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 do not enable required VMware APIs.

Item	Description
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.
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, on page 59 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.

You can find detailed information about the requirements for the virtualized environment by going to .. www.cisco.com go virtualized-collaboration, where you can:

- follow the links for the Unified Communications Manager and IM and Presence Service applications to find the requirements for the release and download OVA files.
- search for the topic "Unified Communications VMware Requirements" to find information about feature support and best practices.

I want to move to a different VM size as part of the upgrade. Can I edit the VM configuration specifications?

Before you edit the VM configuration specifications, review the OVA ReadMe file to find the specific requirements for the release that you are upgrading to. 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. 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 .. www.cisco.com go virtualized-collaboration.

To obtain an OVA file, see Download and Install OVA Templates, on page 61.

I have applications that use an administrative XML (AXL) interface to access and modify Unified Communications Manager information. Will my application continue to work after I upgrade to Unified Communications Manager?

For information about upgrading your AXL applications, see https://developer.cisco.com/site/axl/learn/how-to/upgrade-to-a-new-axl-schema.gsp. To see a list of the AXL operations supported for your release, refer to https://developer.cisco.com/site/axl/documents/operations-by-release/.