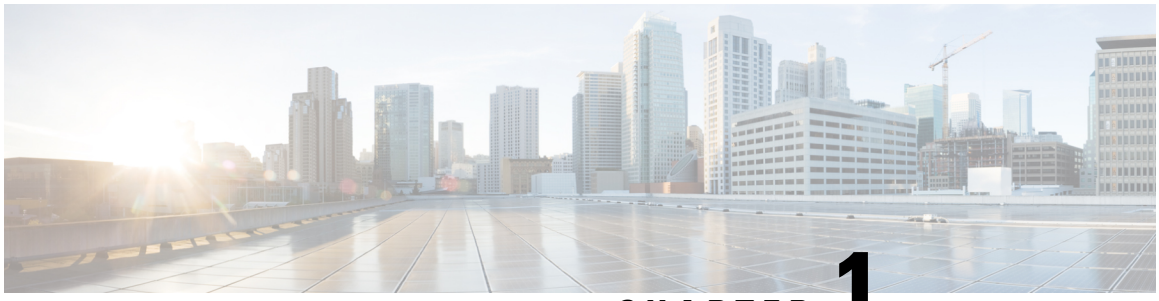
Upgrade and Migration Guide for Cisco Unified Communications Manager and the IM and Presence Service, Release 12.5(1)

First Published: 2019-11-22

Last Modified: 2020-02-12

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

CONTENTS



CHAPTER 1

Upgrade Planning

Upgrade and Migration Overview

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

Use the procedures in this book as a starting point for all upgrades and migration paths.

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
Standard Upgrade (Direct 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. **Example**: Upgrades from 12.5(1) to 12.5(1)SU1. **Note** For standard upgrades where the pre-upgrade release is 12.5(1) or later, you can use the simplified clusterwide upgrade to upgrade your entire cluster.	The following tools can be used to complete standard upgrades: • Unified OS Admin • CLI • PCD Upgrade task

Upgrade Type	Description	Upgrade Tools
Refresh Upgrade (Direct upgrade)	A 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 are upgrading from one major-minor release to another where the OS is different for the two releases. **Example**: Upgrades from 11.5(1) or 12.0(1) to 12.5(1)	The following tools can be used to complete refresh upgrades: • Unified OS Admin • CLI • PCD Upgrade task
Direct migration	A migration involves moving your system from one infrastructure platform to another. It's used in the following cases: • The upgrade requires you to change the infrastructure hardware and platform **Example**: Upgrades from Unified CM 8.5(1) on MCS 7800 HW to 12.5(x) on ESXi involves a mandatory migration due to the HW switch • No direct standard upgrade or direct refresh upgrade path exists 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" use cases, where a direct upgrade path does exist, but PCD Migration is preferred in order to mitigate upgrade path complexity factors such as duration, service impact, and a short outage window.	The following tools can be used to complete migrations: • PCD Migration
Migration from legacy releases	A legacy release is a release that is so old that no direct upgrade or direct migration path exists to the current release. The only option is a direct upgrade to a later release that supports PCD migration followed by a PCD migration to the current release. **Example**: Any upgrade from a pre-6.1(5) Unified CM or a pre-8.5(4) Cisco Unified Presence.	For details, see Upgrading from Legacy Releases, on page 101.

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 Cisco 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 27.

Supported Upgrade and Migration Paths

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

Note Unless indicated otherwise, each release category includes the SU releases within that category. For example, 12.5(x) includes 12.5(1)SU releases. In addition, releases like 10.5(x) and 8.6(5) include any SU releases within those categories as well.

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

Source	Destination	Supported Upgrade Method	Version Switching* (Source to Destination and Vice Versa)
Cisco Unified Communications Manager Upgrade Paths			
Any Unified CM release prior to 6.1(5)	12.5(x)	Legacy upgrade. Direct upgrade and migration is not supported. Do the following: **1.** Upgrade to 6.1(5), 7.1(3) or 7.1(5)—See information on legacy upgrades **2.** PCD Migration** to 12.5(x)	Version switching not supported
Unified CM 6.1(5), 7.1(3), 7.1(5), 8.x, 9.x, 10.0(x)	12.5(x)	PCD Migration**	Version switching not supported
Unified CM 10.5(x), 11.x, 12.0(x)	12.5(x)	Unified OS Admin upgrade (direct refresh) CLI upgrade (direct refresh) PCD Upgrade (direct refresh)** PCD Migration**	Version switching supported for upgrades, but not for migrations

Source	Destination	Supported Upgrade Method	Version Switching* (Source to Destination and Vice Versa)
Unified CM 12.5(x)	12.5(x)	Unified OS Admin upgrade (direct standard) CLI upgrade (direct standard) PCD Upgrade (direct standard)**	Version switching supported for upgrades, but not for migrations
IM and Presence Service Upgrade Paths			
Cisco Unified Presence 8.0(x)	IM and Presence 12.5(x)	Direct upgrade or Migration is not supported. Do the following: **1.** Direct upgrade to 8.5(4)—See information on legacy upgrades **2.** PCD Migration** from 8.5(4) to 12.5(x)	Version switching not supported
Cisco Unified Presence 8.5(4), 8.6(3), 8.6(4), and 8.6(5), IM and Presence 9.x, 10.0(x)	IM and Presence 12.5(x)	PCD Migration**	Version switching not supported
IM and Presence 10.5(x), 11.x or 12.0(x)	12.5(x)	Unified OS Admin upgrade (direct refresh) CLI upgrade (direct refresh) PCD upgrade (direct refresh)** PCD Migration**	Version switching supported for upgrades, but not supported for migrations.
IM and Presence 12.5(x)	12.5(x)	Unified OS Admin upgrade (direct standard) CLI upgrade (direct standard) PCD upgrade (direct standard)**	Version switching supported for upgrades, but not supported for migrations.

* Version switching refers to the ability to install the new version as an inactive version and switch to the new version, and back to the old version, whenever you want. This capability is supported with most direct upgrades, but not with migrations.

** PCD Upgrades and Migrations—Use Cisco Prime Collaboration Deployment Release 12.6 or later for all PCD tasks.

Limitations

The above table does not include direct upgrades and PCD migrations from the following systems. For these systems, we recommend a fresh installation as direct upgrades and PCD migrations are not supported:

- Cisco Business Edition 3000 on MCS 7816-C1
- Cisco Business Edition 5000 on MCS 7828

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, refer to Upgrading from Legacy Releases, on page 101. This is required if you are upgrading from a pre-6.1(5) version of Cisco Unified Communications Manager, or from Cisco Unified Presence 8.0(x).

Table 2: Choose your Upgrade Method

Upgrade Method	Support	When to use this method...	How to complete the Upgrade or Migration
Unified OS Admin or CLI upgrades	Direct upgrades (standard or refresh) via the Cisco Unified OS Administration GUI or CLI.	Consider this tool for: • For simplified clusterwide upgrades • You are only changing the application software and are not updating hardware or VMware. • A direct upgrade path exists. • You are only upgrading Unified CM and IM and Presence Service. There are no other UC applications. • You are upgrading a single Unified CM cluster and a single IM and Presence subcluster. **Note** CLI upgrades provide the same support as Unified OS Admin upgrades, but from a different interface.	Go to Upgrade Tasks, on page 25

Upgrade Method	Support	When to use this method...	How to complete the Upgrade or Migration
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. • 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 33. 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 38 **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.	

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.

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, Cisco strongly recommends that you run the Upgrade Readiness COP file prior to the upgrade in order to maximize upgrade success. Cisco TAC may require that you run this COP file to provide effective technical support.

Table 3: Required COP Files

From	To	COP Files
Cisco Unified Communications Manger Upgrades		
Unified CM 8.6(x), 9.x	12.5(x)	Required COP files: • ciscocm.version3-keys.cop.sgn Optional COP files: • ciscocm.vmware-disk-size-reallocation-<latest_version>.cop.sgn) • ciscocm.free_common_space_v<latest_version>.cop.sgn
Unified CM 10.5(x), 11.0(x)	12.5(x)	Direct Refresh upgrade; no COP file required.
Unified CM 11.5(x)	12.5(x)	Direct Refresh upgrade; COP file is required to increase the disk space. • ciscocm.free_common_space_v<latest_version>.cop.sgn. To download the COP files and the Readme files, go to https://software.cisco.com > click **Software Download** link under **Download & Upgrade** section, and then, navigate to the **Unified Communications** > **Call Control** > **Cisco Unified Communications Manager (CallManager)** > ***<Version>*** > **Unified Communications Manager/CallManager/Cisco Unity Connection Utilities**.
Unified CM 12.0(1)	12.5(x)	PCD Migrations require a COP file: • ciscocm-slm-migration.k3.cop.sgn **Note** This requirement applies only for Prime Collaboration Deployment migrations from Release 12.0(1) of Unified Communications Manager (build 12.0.1.10000-10). If you are migrating from a higher release, such as Unified Communications Manager 12.0(1)SU1, you don't need to install the COP file.
Unified CM 12.5(x)	12.5(x)	Direct Standard upgrade; no COP file required.
IM and Presence Service Upgrades		
CUP 8.5(4) through 8.6(1)	12.5(x)	Required COP files: • `cisco.com.cup.refresh_upgrade_v<latest_version>.cop` • `ciscocm.version3-keys.cop.sgn`
9.1(x)	12.5(x)	Requires following COP File: • `ciscocm.version3-keys.cop.sgn`

From	To	COP Files
10.5(x), 11.x, 12.x	12.5(x)	No COP files required

Requirements and Limitations

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

Hardware Requirements

You can install Unified Communications Manager and Instant Messaging and Presence 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
- Unified Communications (UC) on Cisco Unified Computing System (UCS) Tested Reference Configuration (TRC)
- UC on UCS specifications-based server
- Third-party specifications-based servers

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 Instant Messaging and Presence applications.

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 Instant Messaging and Presence 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.

Item	Description
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.
VMware vCenter	VMware vCenter is optional when you deploy Unified Communications Manager or Instant Messaging and Presence 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 virtual hardware specifications on your VM in order to upgrade to a new release of Unified Communications Manager or Instant Messaging and Presence. For example, verify the requirements for vCPU, vRAM, vNIC adaptor type, and vDisk size, as well as other specifications. Any changes to a VM must align with the OVA configuration. VM changes that result in an unsupported OVA configuration are not allowed. For information about VM requirements, see Readme file with the OVA template that supports your release.

VMware Upgrade Requirements

If the upgrade requires you to update your VMware, go to Virtual Machine Configuration Tasks, on page 43.

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...
• 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 the Field Notice: *Cisco Unified Communications Manager Release 12.0(x) does not support some deprecated phone models* at http://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/rel_notes/12_0_1/deprecated_phones/cucm_b_deprecated-phone-models-for-1201.html.

Upgrades that Involve Deprecated Phones

If you are using any of these phones on an earlier release and you want to upgrade to this release, do the following:

1. Confirm whether the phones in your network will be supported in this release.
2. Identify any non-supported phones.
3. For any non-supported phones, power down the phone and disconnect the phone from the network.
4. Provision a supported phone for the phone user. You can use the 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 Instant Messaging and Presence.

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 Instant Messaging and Presence must either use or not use DNS.
- If your deployment uses DNS—Unified Communications Manager and Instant Messaging and Presence should use the same DNS server. If you use different DNS servers between Instant Messaging and Presence and Unified Communications Manager, it is likely to cause abnormal system behavior.
- If your deployment does not use DNS, 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 Instant Messaging and Presence, see the section regarding multinode deployments in the *Configuration and Administration of IM and Presence on Cisco Unified Communications Manager* for DNS configuration options.

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.

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 Instant Messaging and Presence 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.

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.

Please 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. Refer to your ISO Readme file for details on your specific ISO file. For up to date information on this limitation, see CSCvb14399 at https://bst.cloudapps.cisco.com/bugsearch/bug/CSCvb14399.

Upgrades from 11.5(1)SU2 with Push Notifications Enabled

If you are upgrading from the 11.5(1)SU2 release and you had Push Notifications enabled in the old release, you must disable Push Notifications in the current release and then follow the onboarding process to enable Push Notifications once again. This is required due to API changes in this release that were not a part of the

11.5(1)SU2 release. Your upgraded system will not be able to send troubleshooting logs to the Cisco Cloud unless you disable Push Notifications and then follow the onboarding process for this release.

After you upgrade your system, do the following:

Procedure

Step 1 Disable Push Notifications

Follow these steps:

a. From Cisco Unified CM Administration, choose **Advanced Features** > **Cisco Cloud Onboarding**

b. Uncheck the following check boxes:

- **Enable Push Notifications**
- **Send Troubleshooting information to the Cisco Cloud**
- **Send encrypted PII to the Cisco Cloud for troubleshooting**

c. Click **Save**.

Step 2 Add a Unified Communications Manager product instance into the Smart Licensing system.

See the "Smart Software Licensing" chapter at System Configuration Guide for Cisco Unified Communications Manager.

Step 3 Enable Push Notifications for this release.

For the full onboarding process, See the "Configure Push Notifications for Cisco Jabber on iPhone and iPad" chapter at System Configuration Guide for Cisco Unified Communications Manager.

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"—Refer to 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 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	Task
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.

Migrations from 12.0(1) via Prime Collaboration Deployment

If you are using Cisco Prime Collaboration Deployment to migrate Unified Communications Manager from Release 12.0(1) to any higher release, you must install the below COP file on your 12.0(1) system before you begin the migration. Otherwise, the configuration files related to Smart Licensing will not be migrated.

Table 8: COP Files to Install for Smart Licensing

COP Files
Files: `ciscocm-slm-migration.k3.cop.sgn` You can download the file from: https://software.cisco.com/download/release.html?mdfid=286313357&softwareid=286319173&os=&release=COP-Files&relind=AVAILABLE&rellifecycle=&reltype=latest&i=!pp

Note This requirement applies only for Prime Collaboration Deployment migrations from Release 12.0(1) of Unified Communications Manager (build 12.0.1.10000-10). If you are migrating from a higher release, such as Unified Communications Manager 12.0(1)SU1, you don't need to install the COP file.

Upgrade Considerations for Upgrades from 12.0(1) to 12.5(1)

The following section provide information about the upgrades from 12.0(1) to 12.5(1) that your system must meet, and limitations that apply when you install or upgrade IM and Presence Service.

Note Please select the Reboot Option as “Reboot to upgraded partition” (switch version “Yes”) instead of default Reboot option as "Do not reboot after upgrade" (switch-version as “No”). Hence, the IM and Presence Service 12.5 will be compatible with the Unified Communications Manager 12.5 version.

Refresh upgrade from Unified Communications Manager 12.0.1. to 12.5 or from Unified Communications Manager previous release upgrade to 12.5 release:

Note Before upgrading, run the pre-upgrade Upgrade Readiness COP File. The COP file will run a series of tests to check the pre-upgrade health and connectivity of your system. If the COP file highlights issues that need to be addressed, fix them before proceeding with the upgrade.

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.

  Note If you disable the FIPS mode after installing the COP file, the IPsec configuration page does not appear.

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

FIPS Mode Not Supported in Some 12.x Versions

FIPS mode is supported with 12.5(1)SU1. However, FIPS mode is not supported with Releases 12.0(x) and 12.5(1) of Cisco Unified Communications Manager and the IM and Presence Service. If you are upgrading from an earlier release with FIPS mode, Enhanced Security Mode, or Common Criteria Mode enabled, you must disable them prior to the upgrade to these releases, or upgrade to 12.5(1)SU1 instead. TFTP and other services will not work in 12.0(x) or 12.5(1) with FIPS mode enabled.

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.

Support for Intercluster Peers

The Instant Messaging and Presence supports intercluster peers to clusters that are running different software versions. To find the interdomain federations that are supported, see the "Supported Integrations" chapter 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 12.5(1)SU1 deployment. If required, change VM resources to ensure that your upgraded deployment provides the best performance.

Duplicate ENUMS Break Upgrades and Migrations from 9.1(2)

If you are upgrading or migrating from Release 9.1(2) of Cisco Unified Communications Manager to any 10.x, 11.x or 12.x release, an issue exists with older locale installations that causes upgrade and migration failures. This issue exists if you are using one of the following three locales, and your locale installer is dated prior to August 31, 2017;

- pt-BR (Brazil)
- en-GB (United Kingdom)
- combined_network

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.

Blue Screen Appears for Unified CM Refresh Upgrades

An issue exists with refresh upgrades of Cisco Unified Communications Manager to specific destination releases. After the timezone data populates, you may see a blue transition screen appear for 30 minutes or more.

If you see this blue screen, DO NOT stop the upgrade, or a kernel panic occurs. The upgrade will continue to run even while the blue screen displays. The blue screen will clear itself after approximately 30 minutes

Affected 'To' Versions

This issue affects refresh upgrades of Unified Communications Manager where the destination version falls within the range in the below table. This range includes SU and ES versions that lay within the range. This

issue does not occur for upgrades to older or newer versions that do not fall within the range, or for upgrades of the IM and Presence Service.

Table 9: Affected 'To' Versions for Blue Screen Refresh Upgrade Issue

Release Category	Affected Upgrade Destination Range
10.5(x)	10.5.2.21170-1—10.5.2.22188-1 (includes 10.5(2)SU9)
11.5(x)	11.5.1.16099—11.5.1.17118-1 (includes 11.5(1)SU6)
12.0(x)	12.0.1.23036-1 — 12.0.1.24053-1 (includes 12.0(1)SU3)
12.5(x)	12.5.1.11001-1 — 12.5.1.12018-1 (includes 12.5(1)SU1)

For additional details, see CSCvs28202.

Licensing Requirements

The following sections provide information about the licensing requirements for Unified Communications Manager and the Instant Messaging and Presence

Note As of Unified Communications Manager Release 12.0(1), Smart Licensing replaces Prime License Manager. Smart Licensing requires you to have a Smart Account created and configured before you upgrade or migrate the Unified Communications Manager server.

Several deployment options through which Unified Communications Manager can connect to Cisco Smart Software Manager or Cisco Smart Software Manager satellite are:

- Direct—Unified Communications Manager sends usage information directly over the internet. No additional components are needed.
- Cisco Smart Software Manager satellite—Unified Communications Manager sends usage information to an on-premise Smart Software Manager. Periodically, an exchange of information is performed to keep the databases in synchronization. For more information on installation or configuration of the Smart Software Manager satellite, go to this URL: https://www.cisco.com/c/en/us/buy/smart-accounts/software-manager.html.

  Note Cisco Smart Software Manager satellite is an on-premises collector similar to standalone Prime License Manager.

- Proxy Server—Unified Communications Manager sends usage information over the internet through a proxy server.

Cisco Unified Communications Manager License Requirements

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.

Cisco Smart Software Manager replaces Prime License Manager in Unified Communications Manager Release 12.0(1) and later versions. Cisco Prime License Manager is no longer used as of Release 12.0(1) and no longer appears in the Installed Applications pre-login screen.

If you have enabled the mixed-mode prior to upgrade and have not registered to Cisco Smart Software Manager or Cisco Smart Software Manager satellite then,

- You see the warning message in the Cisco Unified CM Administration page and Cisco Unified OS Administration page as stated below:

Warning The system is currently running Mixed mode. To continue running Mixed mode, please ensure Smart Licensing registration is completed using the Registration Token received from the Smart/Virtual Account that has Allow export-controlled functionality checked.

- An alert named *SmartLicenseExportControlNotAllowed* is sent, when the Unified Communications Manager is not registered with the Registration Token.

For details on how to configure Cisco Smart Software Licensing, see "Smart Software Licensing" chapter, located within the "Configure Initial Parameters for the System" at System Configuration Guide for Cisco Unified Communications Manager.

For more details on Cisco Smart Software Manager satellite, including the *Smart Software Manager satellite Installation Guide*, see http://www.cisco.com/go/smartsatellite.

Migration of PLM Licenses to Smart Entitlement

If you are eligible to upgrade to the Smart Licensing version of the product, then you are able to initiate the migration through the License Registration Portal or Cisco Smart Software Manager. You can self-initiate this process by downloading and installing the Smart Licensing version of the software and registering the device to a Smart Account using a Registration Token. The migration of any entitlements tracked by Cisco automatically migrates to the Customers Smart Account. You will also be able to initiate the migration of unused classic PAKs to Smart Accounts for future consumption by products in Smart Mode. This process is available through the License Registration Portal or Cisco Smart Software Manager.

Unified Communications Manager 9.0x and later version of 12.0(1)

- If you are holding an active Cisco Software Support Service (SWSS) contract, then you can convert the classic licenses to smart entitlements through the Cisco Smart Software Manager at https://software.cisco.com/#SmartLicensing-LicenseConversion.
- Two types of Migration are supported:
  - PAK based—Supported for already fulfilled, partially fulfilled and unfilled PAKs
  - Device based

- Partial Conversion supports mixed environment of older and Unified Communications Manager 12.0(1) clusters.

Upgrade to Smart Entitlement

Unified Communications Manager Pre 9.0x (Device based) to 12.0(1)

You may contact Cisco Global Licensing Operations (GLO) for helping with migrating Device-based licenses to Smart Entitlement.

Customer may establish equivalent user-based licensing required by running License Count Utility (LCU). For more details, see http://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/upgrade/uct/CUCM_BK_UCT_Admin_Guide/CUCM_BK_UCT_Admin_Guide_chapter_01.html.

From the LCU report, Customer may order respective quantity of Upgrade Licenses through Cisco Commerce Workspace. Beyond this, they would have to buy additional new licenses. For more details, see the Ordering Guide at http://www.cisco.com/c/en/us/partners/tools/collaboration-ordering-guides.html.

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 10: 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.

IM and Presence license requirements

The Instant Messaging and Presence Service does not require a server license or software version license. However, you must assign users and enable the Instant Messaging 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 functionality. For more information, see *"Jabber for Everyone Quick Start Guide"*.

You can assign Instant Messaging and Presence on a per user basis, regardless of the number of clients you associate with each user. When you assign Instant Messaging and Presence to a user, this enables the user to send and receive IMs and availability updates. If users are not enabled for Instant Messaging and Presence, they will not be able to log in to the Instant Messaging and Presence 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 Instant Messaging and Presence using any of the following options:

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

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

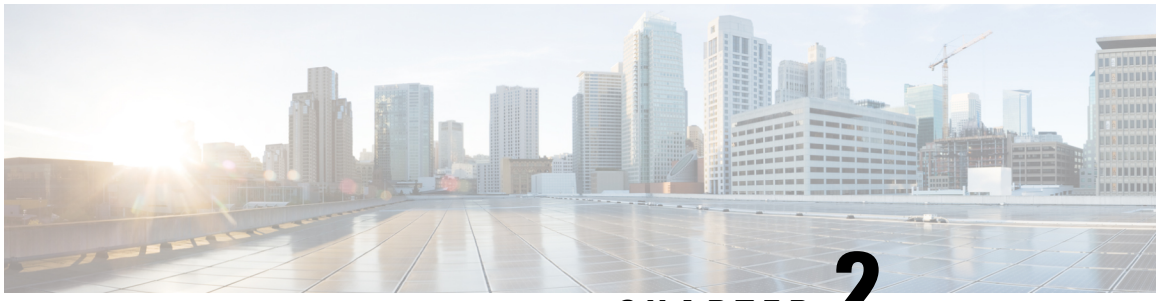
Instant Messaging and Presence capabilities are included within both User Connect Licensing (UCL) and Cisco Unified Workspace Licensing (CUWL). Instant Messaging and Presence capabilities can also be acquired for users that are not Unified Communications Manager IP Telephony users through the Jabber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

Supporting Documentation

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

Task	
Install a Unified Communications (UC) on Cisco Unified Computing System (UCS) Tested Reference Configuration (TRC)	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.

Task	
Install a Cisco Business Edition 6000 or 7000 system	Refer to: • *Install Guide for Cisco Business Edition 6000*—https://www.cisco.com/c/en/us/support/unified-communications/business-edition-6000/tsd-products-support-series-home.html • *Install Guide for Cisco Business Edition 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 Collaboration Sizing Tool at http://tools.cisco.com/cucst



CHAPTER 2

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 Refresh)

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

Before You Begin

Caution Stop all configuration tasks. Do not make any configuration changes during an upgrade. For example, do not change passwords, perform LDAP synchronizations, or run any automated jobs. Do not remove, re-add, or re-install 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 post-upgrade tasks. Any configuration changes that you make during an upgrade will be lost, and some configuration changes can cause the upgrade to fail.

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

- Do not rename or compress the upgrade file as the system will not recognize the file as a valid upgrade file.

- For IM and Presence Service upgrades, check that the contact list size for users has not reached the maximum value. The System Troubleshooter in Cisco Unified CM IM and Presence Administration indicates if there are users who have reached the contact list limit.
- Modify the network adapter to VMXNET3 before the upgrade process. For details, see your OVA readme file.
- If you are upgrading a node in FIPS mode, make sure that your security password has a minimum of 14 characters. For details on how to change security passwords, refer to "Reset the Administartive or Secuirty Password" chapter in the "Getting Started" chapter of the *Administration Guide for Cisco Unified Communications Manager* at https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html.

Note During a refresh upgrade, traffic is no longer processed and several reboots are required, therefore, you must perform a refresh upgrade during a maintenance window.

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 11: 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>.sgn.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>.sgn.iso`.
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`

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).

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 26.

Procedure

	Command or Action	Purpose
Step 1	Run Upgrade Readiness COP File (Pre-upgrade), on page 27	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 29	Specify the reboot sequence beforehand in order to minimize downtime.
Step 3	Upgrade the cluster using either one of these methods: • Complete Clusterwide Upgrade via OS Admin, on page 29 • Complete Clusterwide Upgrade via CLI, on page 30	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 4	Switch Version Manually (Clusterwide), on page 31	Optional. If you chose not to switch versions automatically during the upgrade, switch versions manually.
Step 5	Run Upgrade Readiness COP File (Post-upgrade), on page 38	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)
- 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 Paramters settings
- TFTP Maximum Service Counts
- Active and Inactive versions

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. Some options are available where the pre-upgrade version is 9.x. The COP file does not work where the pre-upgrade version is 8.x or earlier. If the pre-upgrade version is 8.x or earlier, refer to Pre-Upgrade Tasks (Manual Process), on page 59 in the Appendix.

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.

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** > **Reboot 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 29
- Complete Clusterwide Upgrade via CLI, on page 30

Complete Clusterwide Upgrade via OS Admin

Use this procedure to complete a simplified clusterwide upgrade of Cisco 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 clusterwise upgrade by running the `utils system upgrade cluster` CLI command and following the prompts.

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

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

Step 4 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 5 Check the **continue with upgrade after download** 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 6 Check the **switch-version cluster after upgrade (valid only for ISO)** check box if you want to switch over to the upgraded version immediately after upgrade. Otherwise, the upgraded version remains inactive and you will need to switch versions manually later.

Step 7 Click **Next**.

Step 8 Select the upgrade version that you want to install, and click **Next**.
The upgrade commences. The **Istallation Status** page displays information about the upgrade.

Step 9 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 29—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.

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 follow the prompts.

Step 3 When prompted, enter the source where the upgrade file is saved:

- **Remote File system via SFTP or FTP**—you will be prompted to enter the server details and credentials

- **DVD/CD**
- **Local Image**—this option is available only if you initiated an upgrade previously and cancelled the upgrade. The upgrade file is saved locally.

Step 4 Optional. Enter an **SMTP Host** for email notifications that tell you when the upgrade is complete.

Step 5 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 6 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 7 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)

For standard clusterwide upgrades where you chose to save the upgrade to the inactive partition, you can use use this procedure after the upgrade to switch versions manually for the entire cluster.

Note You can use this procedure only for standard upgrades where the pre-upgrade version is 12.5(1) or later.

Note If you prefer to use CLI, you can switch versions with the `utils system switch-version` CLI command, but you must do it on a node-by-node basis. A clusterwide version switch is not available via CLI commands.

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**.

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.

What to do next

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

Upgrade Cluster Nodes (Direct Refresh)

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

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 26.

Procedure

	Command or Action	Purpose
Step 1	Run Upgrade Readiness COP File (Pre-upgrade), on page 27	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	Upgrade cluster nodes using either the GUI or CLI interfaces. • Upgrade Cluster Nodes via OS Admin (Direct Refresh), on page 35 • Upgrade Cluster Nodes via CLI (Direct Refresh), on page 36	Upgrade the cluster nodes in your cluster.
Step 3	Switch Versions Manually, on page 37	Optional. If you did not switch versions automatically during the upgrade, use this procedure to switch versions manually.
Step 4	Run Upgrade Readiness COP File (Post-upgrade), on page 38	After the upgrade, 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)
- 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 Paramters settings
- TFTP Maximum Service Counts
- Active and Inactive versions

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. Some options are available where the pre-upgrade version is 9.x. The COP file does not work where the pre-upgrade version is 8.x or earlier. If the pre-upgrade version is 8.x or earlier, refer to Pre-Upgrade Tasks (Manual Process), on page 59 in the Appendix.

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.

Recommended Sequence (Refresh Upgrades)

The following table displays the recommended node by node upgrade sequence for clusterwide Refresh Upgrades.

Note For additional detailed information on sequencing rules and time requirements for refresh upgrades, including examples, refer to the Appendix Sequencing Rules and Time Requirements, on page 49.

Table 12: Recommended Sequence for Performing Refresh Upgrades

Sequence	Unified Communications Manager Nodes	IM and Presence Service Nodes
1	Upgrade the publisher node to the new software version. The new software is inactive.	—
2	Upgrade the secondary subcriber nodes in parallel. The new software is inactive.	Upgrade the IM and Presence database publisher node in parallel with the Unified Communications Manager subscriber nodes.
3	Upgrade the primary subscriber nodes	Upgrade the subscriber nodes. The new software is inactive.
4	Switch the software version on the publisher node and reboot it. The new software is active.	—
5	Switch the software version on the secondary subscriber nodes in parallel and reboot them.	Switch the software version on the database publisher node and reboot it. The new software is active.
6	Switch the software version on the primary subscriber nodes in parallel and reboot them.	Switch the software version on the subscriber nodes in parallel and reboot them. The new software is active.
7	Ensure that database replication is complete and functioning between the publisher node and all subscriber nodes before proceeding.	Ensure that database replication is complete and functioning between the publisher node and all subscriber nodes.

Upgrade Cluster Nodes via OS Admin (Direct Refresh)

Use this procedure to complete a direct refresh upgrade of Cisco Unified Communications Manager or IM and Presence Service cluster nodes. With refresh upgrades, you must upgrade on a node-by-node basis.

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

Before you begin

Plan the node by node sequence that you will use for the upgrade. For details, see Recommended Sequence (Refresh Upgrades), on page 35.

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

- **DVD/CD**
- **SFTP server**—You must also enter the SFTP server details, including the **Directory**, **Server** address and login credentials.

Step 4 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 5 Check the **continue with upgrade after download** 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 6 Check the **switch-version cluster after upgrade (valid only for ISO)** check box if you want to switch over to the upgraded version immediately after upgrade. Otherwise, the upgraded version remains inactive and you will need to switch versions manually later.

Step 7 Click **Next**.

Step 8 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 9 Click **Finish** when the upgrade completes.
If you chose to switch versions automatically, the node reboots to the upgraded version automatically. Otherwise, the upgrade saves to the inactive partition and you can switch versions manually later.

Step 10 Repeat this procedure for additional cluster nodes.

Upgrade Cluster Nodes via CLI (Direct Refresh)

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

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

Before you begin

Plan the node by node sequence that you will use for the upgrade. For details, see Recommended Sequence (Refresh Upgrades), on page 35.

Procedure

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

Step 2 Run the `utils system upgrade initiate` CLI command and follow the prompts:

Step 3 If you are upgrading a subscriber node, and you have previously upgraded this node, indicate whether you want to use the publisher node credentials for the upgrade (the default is yes).

- **Yes**—The upgrade process checks the publisher node for locally saved upgrade files that you can use as the source file.
- **No**—You are prompted to choose the source (see the following step)

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 completes.

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 locally. 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 31

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.

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 Instant Messaging and Presence 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.

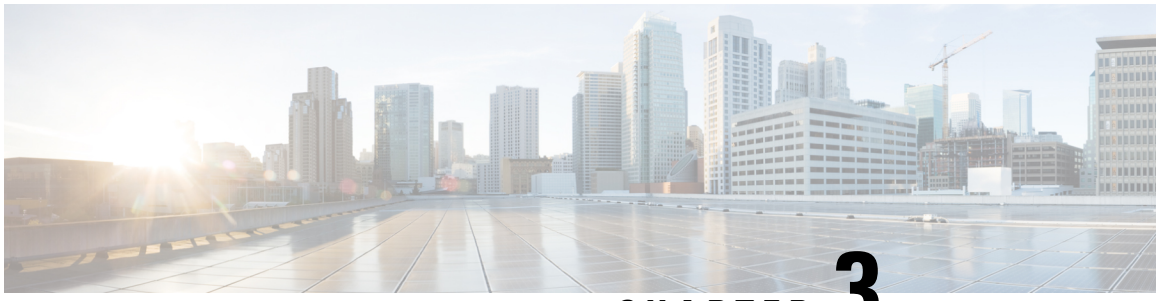
Procedure

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 3

Change the Virtualization Software

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

- Virtual Machine Configuration Tasks, on page 43

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 Instant Messaging and Presence applications.

Procedure

	Command or Action	Purpose
Step 1	Install and Configure VMware vCenter, on page 44	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 Instant Messaging and Presence on UC on UCS tested reference configuration hardware.
Step 2	Upgrade vSphere ESXi, on page 45	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 Instant

	Command or Action	Purpose
		Messaging and Presence; 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 45	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 Instant Messaging and Presence 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 46	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 Instant Messaging and Presence. 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 47	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 Instant Messaging and Presence 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 Instant Messaging and Presence 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 Instant Messaging and Presence, 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 Instant Messaging and Presence.

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
```

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.

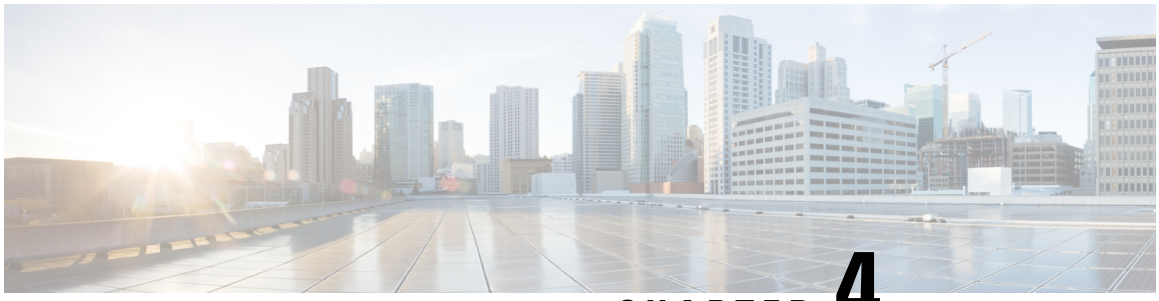
Step 5 Proceed with the upgrade and then power on the virtual machine.

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 46 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 Instant Messaging and Presence 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 4

Sequencing Rules and Time Requirements

Use this information in this appendix only if you need information on sequencing 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—you 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	Reboot to upgraded partition	When you choose this option, the system reboots to the new software version.
	Manual	Do not reboot 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 at a later time.
Refresh upgrade	Manual	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 manually switch to the new software at a later time. When you use this upgrade method, you must switch your publisher node to the new software version before you upgrade your subscriber nodes.
	Automatic	Switch to new version after upgrade	Choose this option to use the new software version immediately following the upgrade.

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.

Recommended Sequence (Refresh Upgrades)

The following table shows the recommended sequence for performing a refresh upgrade. This method provides the least time and impact for the upgrade.

Table 13: Recommended Sequence for Performing Refresh Upgrades

Sequence	Unified Communications Manager Nodes	IM and Presence Service Nodes
1	Upgrade the publisher node to the new software version. The new software is inactive.	—

Sequence	Unified Communications Manager Nodes	IM and Presence Service Nodes
2	Upgrade the secondary subcriber nodes in parallel. The new software is inactive.	Upgrade the IM and Presence database publisher node in parallel with the Unified Communications Manager subscriber nodes.
3	Upgrade the primary subscriber nodes	Upgrade the subscriber nodes. The new software is inactive.
4	Switch the software version on the publisher node and reboot it. The new software is active.	—
5	Switch the software version on the secondary subscriber nodes in parallel and reboot them.	Switch the software version on the database publisher node and reboot it. The new software is active.
6	Switch the software version on the primary subscriber nodes in parallel and reboot them.	Switch the software version on the subscriber nodes in parallel and reboot them. The new software is active.
7	Ensure that database replication is complete and functioning between the publisher node and all subscriber nodes before proceeding.	Ensure that database replication is complete and functioning between the publisher node and all subscriber nodes.

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 Instant Messaging and Presence nodes, you must reboot all IM and Presence nodes after the Unified Communications Manager upgrade is complete.
- If you are upgrading Instant Messaging and Presence nodes in addition to Unified Communications Manager nodes:
    - The Instant Messaging and Presence database publisher node must be the first Instant Messaging and Presence node that you upgrade. The new software is installed as an inactive version.

- You can begin upgrading Instant Messaging and Presence 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 Instant Messaging and Presence database publisher node, or you can choose to upgrade in parallel. If you upgrade in parallel, start upgrading the Instant Messaging and Presence 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 Instant Messaging and Presence nodes.
- You must switch the Instant Messaging and Presence database publisher node to the new software version and reboot it before you switch the software version on any Instant Messaging and Presence subscriber nodes.
- If you upgrade a group of Instant Messaging and Presence 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 Instant Messaging and Presence 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 Instant Messaging and Presence 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 Instant Messaging and Presence 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 Instant Messaging and Presence 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 14: 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 Instant Messaging and Presence virtual machines (VM).
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.

Item	Description
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 Instant Messaging and Presence. Do not oversubscribe CPUs by having VMs share the host resources; use logical cores or resource reservations • Unified Communications Manager and Instant Messaging and Presence 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
Throttling	On Instant Messaging and Presence 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 Instant Messaging and Presence 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

Table 15: 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	—
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

Task	Minimum Time	Service Impact
Upgrade the Instant Messaging and Presence 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 Instant Messaging and Presence 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 Instant Messaging and Presence publisher node to the new software version and reboot	30 minutes	IM and Presence high availability is disabled Jabber is unavailable
Switch the Instant Messaging and Presence subscriber nodes to the new software version and reboot	30 minutes	IM and Presence high availability is disabled Jabber is unavailable
Instant Messaging and Presence 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 52

Example: Time Requirements for a Refresh Upgrade in the Least Time

This example shows an example of how to calculate minimum time requirements if you want to perform a refresh upgrade that takes the least amount of time. This approach will have the greatest service impact on your network.

Table 16: Example: Time Requirements for a Refresh Upgrade in the Least Time

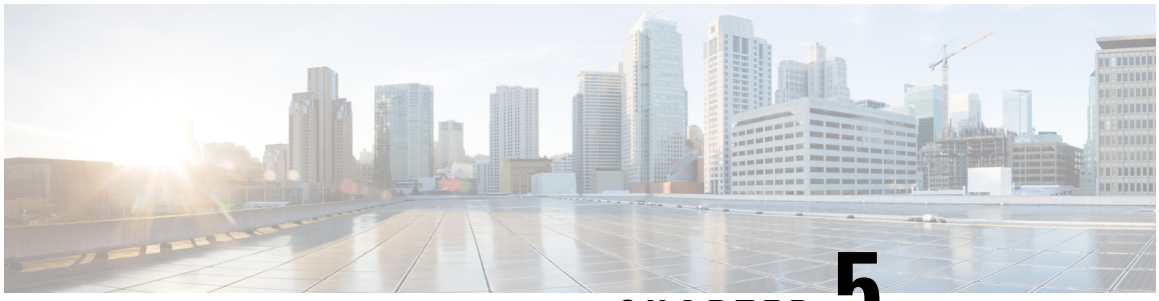
Task		Minimum Estimated Time
1	Upgrade the Unified Communications Manager publisher node to the new software version. The new software is inactive.	4-5 hours
2	Upgrade the Unified Communications Manager subscriber nodes in parallel. The new software is inactive.	1-2 hours
3	Upgrade the Instant Messaging and Presence database publisher node to the new software version. The new software is inactive.	3-4 hours
4	Upgrade the Instant Messaging and Presence subscriber nodes in parallel. The new software is inactive.	1-2 hours
5	Switch the software version on the Unified Communications Manager publisher node and reboot it.	30 minutes
6	Switch the software version on the Unified Communications Manager subscriber nodes in parallel and reboot them.	30 minutes
7	Wait for database replication on the Unified Communications Manager subscriber nodes.	2 hours
8	Switch the software version on the Instant Messaging and Presence database publisher node and reboot it.	30 minutes
9	Switch the software version on the Instant Messaging and Presence subscriber nodes in parallel and reboot them.	1-2 hours
10	Wait for database replication on the Instant Messaging and Presence subscriber nodes.	2 hours
Total		15.5-20.5 hours

Example of Clusterwide upgrade (Direct Standard)

The following example provides an example of the time for a clusterwide upgrade of Cisco Unified Communications Manager and the IM and Presence Service assuming a megacluster deployment. Please note that with the clusterwide upgrade, many of the tasks are completed in parallel and overlap. As a result, the **Time for Task** column is not a linear sum.

Table 17: Example of Clusterwide Upgrade - Megacluster Deployment

	Task	Time for Task
1	Run Upgrade Readiness COP File (pre-upgrade)	0.5 hours
2	Upgrade the cluster	6.5 hours
3	Switch versions and reboot (Maintenance Window required)	1.5 hours
4	Run Upgrade Readiness COP file (post-upgrade)	0.5 hours
	Totals	9.0 hours total (includes 1.5 hour maintenance window)



CHAPTER 5

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.

Note For upgrade paths where the From release is 10.x or later, running the Upgrade Readiness COP file and completing its resolution requests takes the place of these pre-upgrade tasks. The COP file has limited functionality for upgrades from 9.x and does not work for upgrades from releases prior to 9.x.

- Pre-Upgrade Tasks, on page 59

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 27	The Upgrade Readiness COP file checks your system for issues that may interfere with the upgrade. **Note** Cisco strongly recommends that you run the COP file in order to reduce the possibility of an upgrade failure.

	Command or Action	Purpose
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 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 8 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 Requirements, on page 52 and ensure that your system meets the conditions described in that section. • Generate a Database Status Report, on page 64 • Check Database Replication, on page 65 • Check Performance Reports, on page 65 • Run CLI Diagnostics, on page 66	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 66 • Regenerate a Certificate, on page 67 if an identify certificate is expired	For refresh upgrades only. Expired certificates are not imported during refresh upgrades, which can cause errors.
Step 8	Take a Fresh Backup, on page 68	Complete a system backup. **Caution** You may lose data or you may be unable to restore your system if your backup is outdated.

	Command or Action	Purpose
Step 9	Back Up Custom Ringtones and Background Images, on page 69	If you have custom ringtones or background images in the TFTP directory, create a separate backup for these files as they are not included in system backups.
Step 10	Check Network Connectivity, on page 70	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 70	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 71	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 71	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 72	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 72	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 73	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 73	During the upgrade, the Unified Communications Manager enterprise parameter settings may overwrite the IM and Presence Service enteprise parameter settings if the configurations are different.
Step 18	Export User Records, on page 73	Export user records using the Bulk Administration Tool (BAT).

	Command or Action	Purpose
Step 19	Upgrade IP Phone Firmware, on page 74	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.
Step 20	Verify Critical Services, on page 75	Verify that all critical services are activated.
Step 21	Deactivate Cisco Extension Mobility, on page 75	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	Deactivate TFTP services, on page 76	Stop TFTP services on Unified Communications Manager nodes before you begin an upgrade.
Step 23	Stop the IM and Presence Sync Agent, on page 76	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 24	Check the Available Common Partition Space, on page 76	Verify that you have enough common partition space for the upgrade. You can skip this task for migrations.
Step 25	If you do not have enough common partition space, perform one or more of the following procedures: • Adjust High and Low Watermarks, on page 77 • Maximize Usable Disk Space, on page 77	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. **Caution** Performing an upgrade without sufficient disk space can cause the upgrade to fail.
Step 26	Obtain Upgrade Files, on page 78	Download the required upgrade files. For refresh upgrades, you must also download any required COP files. You can skip this task for migrations.
Step 27	Increase the Database Replication Timeout, on page 81	Optional. Unified Communications Manager publisher node only. Use this procedure when you upgrade large clusters. You can skip this task for migrations.

	Command or Action	Purpose
Step 28	Disable High Availability on Presence Redundancy Groups, on page 81	IM and Presence Service only. If High Availability is enabled, disable it prior to the upgrade. You can skip this task for migrations.
Step 29	Add a Serial Port to the Virtual Machine, on page 82	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 30	Configure High Availability for RTMT, on page 82	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.

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)
- 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 Paramters settings
- TFTP Maximum Service Counts
- Active and Inactive versions

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. Some options are available where the pre-upgrade version is 9.x. The COP file does not work where the pre-upgrade version is 8.x or earlier. If the pre-upgrade version is 8.x or earlier, refer to Pre-Upgrade Tasks (Manual Process), on page 59 in the Appendix.

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.

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. Deleting a certificate can break a certificate chain if the certificate is part of an existing chain. You can 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 the certificate that you delete is of the type “CAPF-trust”, “tomcat-trust”, “CallManager-trust”, or “Phone-SAST-trust”, the certificate is deleted across all servers in the cluster.
- 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 During an upgrade, the ITLRecovery certificate is generated per cluster.

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.

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

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

Step 2 Configure the fields on the **Generate New Self-Signed Certificate** window. See the 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 the Related Topics section for more information about the certificate names and their descriptions.

Step 5 Rerun the CTL client (if configured) after you regenerate the CAPF or CallManager certificates.

Note When a Tomcat certificate is regenerated, the TFTP service should be deactivated and later activated. Else, the TFTP will continue to offer the old cached self-signed tomcat certificate.

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 68

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 18: Certificate Names and Descriptions

Name	Description	Related Services
tomcat tomcat-ECDSA	This self-signed root certificate is generated during installation for the HTTPS node.	Tomcat and TFTP
ipsec	This self-signed root certificate is generated during installation for IPsec connections with MGCP and H.323 gateways.	Cisco Disaster Recovery System (DRS) Local and Cisco DRF Master
CallManager	This self-signed root certificate is installed automatically when you install Unified Communications Manager. This certificate provides node identification, including the node name and the global unique identifier (GUID).	CallManager, CAPF, and CTI
CAPF	The system copies this root certificate to your node or to all nodes in the cluster after you complete the Cisco client configuration.	CallManager and CAPF
TVS	This is a self-signed root certificate.	TVS

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 Instant Messaging and Presence cluster nodes must be running the same version of the Instant Messaging and Presence 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 Instant Messaging and Presence 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 Instant Messaging and Presence Service nodes. Some Enterprise Parameters exist on both Unified Communications Manager nodes and Instant Messaging and Presence Service nodes. Where the same parameter exists, the settings that are configured on Unified Communications Manager nodes overwrite the settings configured on Instant Messaging and Presence Service nodes during the upgrade process. Enterprise Parameters that are unique to Instant Messaging and Presence 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 Instant Messaging and Presence 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.

Deactivate TFTP services

Use this procedure to stop TFTP services 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 **Cisco TFTP** services.

Step 4 Click **Stop**.

Step 5 Repeat Steps 2 through 4 for each node that is running **Cisco TFTP** 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 Instant Messaging and Presence upgrade, you must stop the Instant Messaging and Presence 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 Instant Messaging 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 **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.

Note 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 80G single disk 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 Instant Messaging and Presence 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.

Table 19: Required COP Files for Upgrades and Migrations to Unified Communications Manager Release 12.0(1)

From	To	Upgrade Type
8.6(x)	12.x	Refresh upgrade. Required COP files: • ciscocm.version3-keys.cop.sgn Optional COP files: • ciscocm.vmware-disk-size-reallocation-<latest_version>.cop.sgn) • ciscocm.free_common_space_v<latest_version>.cop.sgn
9.1(x)	12.x	Refresh upgrade. Required COP files: • ciscocm.version3-keys.cop.sgn Optional COP files: • ciscocm.vmware-disk-size-reallocation-<latest_version>.cop.sgn) • ciscocm.free_common_space_v<latest_version>.cop.sgn
10.5(x)	12.x	Standard upgrade; no COP file required.
11.0(x)	12.x	Standard upgrade; no COP file required.

From	To	Upgrade Type
11.5(x)	12.x	Standard upgrade; COP file is updated to increase the disk space. • ciscocm.free_common_space_v<latest_version>.cop.sgn. To download the COP files and the Readme files, go to https://software.cisco.com > click **Software Download** link under **Download & Upgrade** section, and then, navigate to the **Unified Communications** > **Call Control** > **Cisco Unified Communications Manager (CallManager)** > ***<Version>*** > **Unified Communications Manager/CallManager/Cisco Unity Connection Utilities**.
12.0(1)	12.0(1)SU1 or higher	PCD Migrations require a COP file: • ciscocm-slm-migration.k3.cop.sgn **Note** This requirement applies only for Prime Collaboration Deployment migrations from Release 12.0(1) of Unified Communications Manager (build 12.0.1.10000-10). If you are migrating from a higher release, such as Unified Communications Manager 12.0(1)SU1, you don't need to install the COP file.

Table 20: Required COP Files for Refresh Upgrades from Cisco Unified Presence Releases

From Cisco Unified Presence Release	To IM and Presence Release	Upgrade Type
8.5(4) through 8.6(1)	12.x	Refresh upgrade. Requires the following COP files: • cisco.com.cup.refresh_upgrade_v<latest_version>.cop • ciscocm.version3-keys.cop.sgn

Table 21: Required COP Files for Refresh Upgrades from IM and Presence Service Releases

From IM and Presence Release	To IM and Presence Release	Upgrade Type
9.1(x)	12.x	Refresh upgrade. Requires the following COP file: • ciscocm.version3-keys.cop.sgn
10.5(x)	12.x	Standard upgrade; no COP file required.
11.0(x)	12.x	Standard upgrade; no COP file required.
11.5(x)	12.x	Standard upgrade; no COP file required.

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 Instant Messaging and Presence Service nodes only. Use it to disable high availability on the Instant Messaging and Presence 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 86. In the event of an upgrade failure, refer to Dump a Log File After an Upgrade Failure, on page 103.

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.

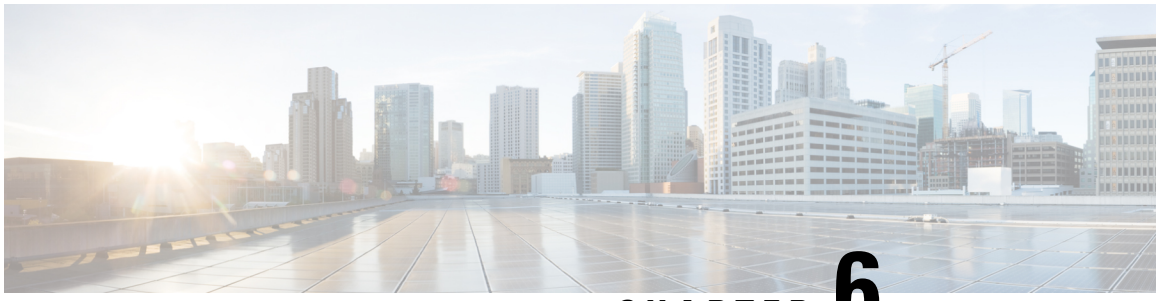
Step 4 From the **Service** drop-down, select **Cisco AMC Service**.

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.



CHAPTER 6

Post-Upgrade Tasks (Manual Process)

The manual post-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 post-upgrade tasks manually.

Note For upgrade paths where the From release is 10.x or later, running the Upgrade Readiness COP file and completing its resolution requests takes the place of these post-upgrade tasks. The COP file has limited functionality for upgrades from 9.x and does not work for upgrades from releases prior to 9.x.

- Post-upgrade Task Flow, on page 83

Post-upgrade Task Flow

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

Procedure

	Command or Action	Purpose
Step 1	Remove the Serial Port, on page 86	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 2	Restart Extension Mobility, on page 86	If you deactivated Cisco extension mobility as part of the pre-upgrade tasks, you can now restart it.
Step 3	Restart TFTP Services, on page 86	Use this procedure to restart TFTP services on Unified CM nodes.
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 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 88	Reset TFTP parameters that are changed during the upgrade process.
Step 6	Restore Enterprise Parameters, on page 88	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 89	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 89	You must update the VMWare Tools after you complete the upgrade. Perform this procedure for all nodes.
Step 9	Install Locales, on page 90	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 91	Use this procedure if you increased the database replication timeout value before you began the upgrade process. Perform this procedure on Unified Communications Manager nodes only.
Step 11	Verify the Registered Device Count, on page 92	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 92	Use this procedure to verify the number of assigned users on Instant Messaging and Presence nodes after the upgrade is complete.

	Command or Action	Purpose
Step 13	Test Functionality, on page 93	Verify phone functions and features are working correctly after the upgrade.
Step 14	Upgrade RTMT, on page 94	If you use Cisco Unified Real Time Monitoring Tool (RTMT), upgrade to the new software version.
Step 15	Manage TFTP Server Files, on page 94	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 95	Optional. For Unified CM nodes only, upload a text file that contains a customized log-on message.
Step 17	Configure IPSec Policies, on page 96	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 97	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 97	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 98	If you disabled High Availability for the Instant Messaging and Presence Service before the upgrade process, use this procedure to turn it back on.
Step 21	Restart the IM and Presence Sync Agent, on page 98	If you stopped the Instant Messaging and Presence Sync Agent service before you began the upgrade process, restart it now.
Step 22	Restart CER Service, on page 99	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.

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**.

Restart TFTP Services

Use this procedure to restart TFTP services on Unified Communications Manager nodes after you complete 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 Select the **Cisco TFTP** 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.

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 Instant Messaging and Presence nodes. Where the same parameter exists, the settings that are configured on Unified Communications Manager nodes overwrite the settings configured on Instant Messaging and Presence nodes during an upgrade. Enterprise Parameters that are unique to Instant Messaging and Presence nodes are retained during an upgrade.

Use this procedure to reconfigure the settings on Instant Messaging and Presence 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. Your system uses one of the following VMware Tools:

- Native VMware Tools (provided by VMware)
- Open VMware Tools (provided by Cisco)

- To upgrade Unified Communications Manager from a version earlier than Release 11.5(x), you must use the native VMware tools option. You can change to open VMware Tools after the upgrade.
- For upgrades from Unified Communications Manager Release 11.5(1) onwards (for example, to a higher SU), you can choose whether your system use Native VMware or Open VMware Tools.
- For fresh installation and PCD migrations from Unified Communications Manager Release 11.5(1) onwards, open VMware tools installed by default.

Procedure

Step 1 Execute a command **utils vmtools status** to ensure that VMware tools are currently running.

Step 2 If necessary, run one of the following commands to switch to the desired VMware tools platform: **utils vmtools switch native** or **utils vmtools switch open**.

Step 3 Follow one of the methods below if you are using *Native VMware Tools*:

- Initiate the automatic tools update with the viClient.

  Note For ESXI 6.5 VM tools update, power off the VM before updating the configuration parameters. Choose the Edit settings > options > Advanced > General > Configuration parameters and then add:

  ```
  tools.hint.imageName=linux.iso
  ```

- Configure the tool to automatically check the version during a VM power-on and upgrade.

For information about how to configure these options, refer to VMware documentation. You can also find more information by searching the topic "VMware Tools" at https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/uc_system/virtualization/virtualization-software-requirements.html#vmtools.

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 orInstant Messaging and Presence node.

You can install locales on Unified Communications Manager or on Instant Messaging and Presence 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 Instant Messaging and Presence 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 Instant Messaging and Presence 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 Instant Messaging and Presence 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 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 Instant Messaging and Presence 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, Cisco recommends that you upgrade RTMT after you complete the Unified Communications Manager 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, Cisco recommends that you uninstall the previous version.

Procedure

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

Step 2 Click **Find**.

Step 3 Perform one of the following actions:

- To install the tool on a computer that is running the Microsoft Windows operating system, click the **Download** link for the Cisco Unified Real-Time Monitoring Tool - Windows.
- To install the tool on a computer that is running the Linux operating system, click the **Download** link for the Cisco Unified Real-Time Monitoring Tool - Linux.

Step 4 Download the installation file to your preferred location.

Step 5 Locate and run the installation file.
The extraction process begins.

Step 6 In the RTMT welcome window, click **Next**.

Step 7 Because you cannot change the installation location for upgrades, click **Next**.
The Setup Status window appears; do not click Cancel.

Step 8 In the **Maintenance Complete** window, click **Finish**.

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.

For information about restarting services, refer to *Cisco Unified Serviceability Administration Guide*.

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 6.1(5). You must recreate your IPSec policies after the PCD migration is complete, because IPSec policies from Release 6.1(5) are not migrated to the new release.

- 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 Instant Messaging and Presence 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 Instant Messaging and Presence 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 Instant Messaging and Presence 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 Instant Messaging and Presence 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 Instant Messaging and Presence 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.

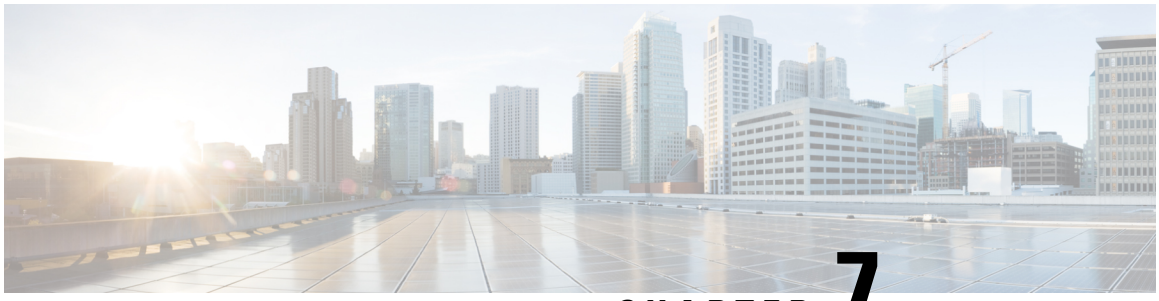
Restart CER Service

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 7

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 Paths To/From Table" at http://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/compat/ccmcompmatr1.html#pgfId-391518.

Table 22: Upgrade to Release 12.0(1) from Legacy Releases

Installed Version	Upgrade to this Version on MCS hardware	Migrate to this Version on a Virtual Machine
Uinified Communications Manager Releases		
4.x	Migrate to 6.1(5), 7.1(3), or 7.1(5) using Uinified Communications Manager Data Migration Assistant (DMA) Check the *Software Compatibility Matrix* for the intermediate release to find the supported upgrade path from your current release, or see the "Supported Upgrade Paths To/From Table" at the link above.	PCD Migration to 12.x

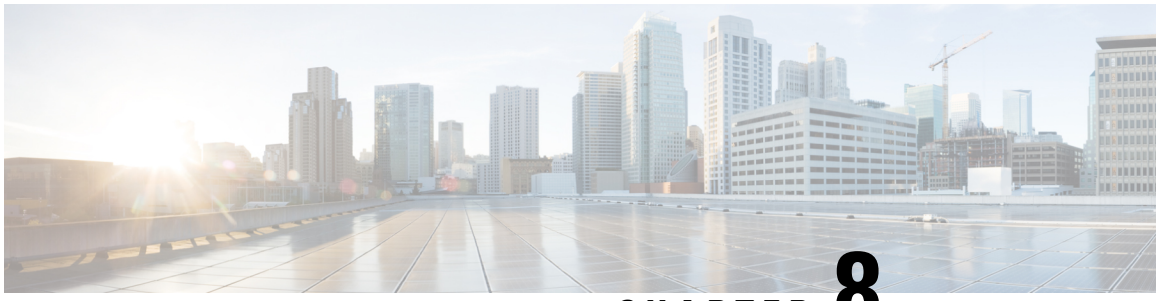
Installed Version	Upgrade to this Version on MCS hardware	Migrate to this Version on a Virtual Machine
5.1(2) 5.1(3) 6.0(x) 6.1(1) 6.1(2) 6.1(3) 6.1(4)	Direct Upgrade to 6.1(5) or 7.1(3)	PCD Migration to 12.x
7.0(1) 7.1(2)	7.1(3), 7.1(5), 8.0(x), 8.5(1), or 8.6(2)	PCD Migration to 12.x
Cisco Unified Presence Releases		
8.0(x)	Direct Upgrade to 8.5(4)	PCD Migration to 12.0(1)
Uinified Communications Manager Business Edition Releases		
Business Edition 3000 (BE3000)	Upgrades and migrations to Unified Communications Manager Release 12.x are not supported for these deployments. We recommend that you perform a fresh installation for upgrades from these products to the current Unified Communications Manager release.	
Business Edition 5000 (BE5000)		

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 Instant Messaging and Presence (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 8

Troubleshooting

This section contains the following information:

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 Instant Messaging and Presence.

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 troubleshootingUnified 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.

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.

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 **Reboot 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 **Reboot 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. Refer to the sections in this Troubleshooting Guide to address your system issues.

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 Instant Messaging and Presence 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 Instant Messaging and Presence 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 Instant Messaging and Presence nodes, and the upgrade of the Instant Messaging and Presence database publisher node fails.

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

- if the upgrade on the Instant Messaging and Presence database publisher node fails before the refresh upgrade causes the node to reboot (that is, if the node failed before switching to the new partition), perform the upgrade again on the Instant Messaging and Presence database publisher node
- If the failure occurred after the Instant Messaging and Presence 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 Instant Messaging and Presence 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 Instant Messaging and Presence 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 Instant Messaging and Presence nodes, and the upgrade of the Instant Messaging and Presence subscriber node fails.

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

- if the upgrade on the Instant Messaging and Presence subscriber node before the refresh upgrade causes the node to reboot (that is, if the node failed before switching to the new partition), perform the upgrade again on the Instant Messaging and Presence subscriber node
- if the upgrade on the Instant Messaging and Presence 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 Instant Messaging and Presence database publisher node back to the earlier software version
  - switch the Instant Messaging and Presence subscriber nodes back to the earlier software version
  - switch the Unified Communications Manager publisher node pub forward to the new software version
  - switch the Instant Messaging and Presence database publisher node forward to the new software version
  - perform the upgrade again on the Instant Messaging and Presence subscriber node

Upgrade From Pre Release 8.6(4) Fails

Problem You are upgrading from a release earlier than Cisco Unified Presence 8.6(4) and the upgrade fails on both the publisher and subscriber nodes.

Solution The Unified Communications Manager hostname is case-sensitive. You must ensure that the entry for the Unified Communications Manager publisher node on the Cisco Unified Presence Administration interface matches exactly the Unified Communications Manager hostname. Complete the following procedure:

1. Log into **Cisco Unified Presence Administration** interface and choose **System** > **CUCM Publisher**.
2. If the **CUCM Publisher Hostname** value does not match the hostname, modify it and click **Save**.
3. Restart the Cluster Manager service with the following CLI command: **utils service restart Cluster Manager**
4. Open the platformConfig.xml file at the following location: `/usr/local/platform/conf/`
5. Verify that the values for *IPSecMasterHost* and *NTPServerHost* match exactly the Cisco Unified Communications Manager hostname.
6. If necessary, modify the value for *IPSecMasterHost* and *NTPServerHost* , save the platformConfig.xml file and restart the Cluster Manager service again.

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

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

Real-Time Monitoring Tool alert for Cisco SIP proxy service

Problem After an Instant Messaging and Presence 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`

Cisco UP Presence Engine database does not restart

Problem After you switch back to Cisco Unified Presence Release 8.6(3) or an earlier software version, the Cisco UP Presence Engine database does not restart.

Solution Ensure that you installed the required COP file, `ciscocm.cup.pe_db_install.cop`, on every node in the cluster after you switched back to Cisco Unified Presence Release 8.6(3), or earlier.

Version Errors

Selected Upgrade Is Disallowed From the Current Version

Problem During a refresh upgrade, the following error is reported: `Error encountered: The selected upgrade is disallowed from the current version.`

Solution You did not install the required COP file on the node. Download the following COP file from Cisco.com: `ciscocm.cup.refresh_upgrade_v<latest_version>.cop`. Restart the server. Install the COP file on every node in the cluster before you attempt the refresh upgrade again.

Version Does Not Match the Active or Inactive Version

Problem During an upgrade on a Instant Messaging and Presence 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 Instant Messaging and Presence database publisher node (the first Instant Messaging and Presence 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, Instant Messaging and Presence 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 Instant Messaging and Presence subscriber nodes that you upgrade must match five numbers of the software version installed on the Instant Messaging and Presence database publisher node.

Ensure that the first node that you upgrade is either the Unified Communications Manager publisher node or the Instant Messaging and Presence 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 Instant Messaging and Presence database publisher node (the first Instant Messaging and Presence node that you upgrade) must match the first two numbers of the software version installed on the Unified Communications Manager publisher node. For example, Instant Messaging and Presence 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 Instant Messaging and Presence subscriber nodes that you upgrade must match five numbers of the software version installed on the Instant Messaging and Presence database publisher node.

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

Failed refresh upgrade

Problem A refresh upgrade failed.

Solution Restart the system, it should reboot to the software version that was running before you attempted the refresh upgrade. If you cannot access the system, you must use the Recovery CD to recover the node.

Cancelled or failed upgrade

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

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

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

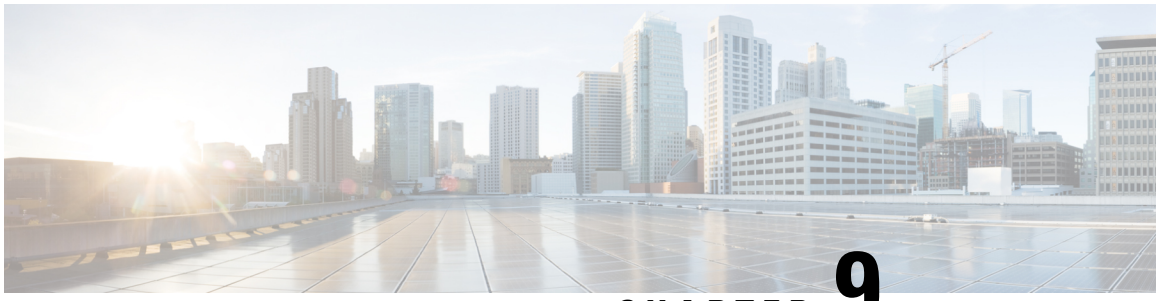
```
The directory was located and searched but no valid options or upgrades
were available. Note, a machine cannot be downgraded so option and upgrade
files for previous releases were ignored.
```

Solution The upgrade manager checks for connectivity between Instant Messaging and Presence and Unified Communications Manager to validate the version during the upgrade. If this fails, the Instant Messaging and Presence 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 Instant Messaging and Presence and Unified Communications Manager before proceeding with the upgrade.

Common Partition Full Upgrade Failure

Problem The upgrade of Instant Messaging and Presence 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 9

Frequently Asked Questions

Frequently Asked Questions

I am upgrading from a release of Unified Communications Manager or Instant Messaging and Presence 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 below. After you have verified the requirements for the new release, see Virtual Machine Configuration Tasks, on page 43for instructions.

Table 23: 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 Instant Messaging and Presence 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 Instant Messaging and Presence 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 virtual hardware specifications on your VM in order to upgrade to a new release of Unified Communications Manager or Instant Messaging and Presence. For example, verify the requirements for vCPU, vRAM, vNIC adaptor type, and vDisk size, as well as other specifications. Any changes to a VM must align with the OVA configuration. VM changes that result in an unsupported OVA configuration are not allowed. For information about VM requirements, see Readme file with the OVA template that supports your release.

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 Instant Messaging and Presence 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 45.

My current Unified Communications Manager andInstant Messaging and Presence Service release is deployed with other Cisco applications, such as Unified Contact Center Express (UCCX), Cisco Unity Connection, or Unified Contact Center Enterprise (UCCE). Do I need to upgrade my other Cisco applications when I upgrade my Unified Communications Manager?

See the Cisco Unified Communications Compatibility Tool at http://tools.cisco.com/ITDIT/vtgsca/VTGServlet for software compatibility information.

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/.