Upgrade Guide for Cisco Unified Communications Manager and IM and Presence Service, Release 10.0(1)

First Published: 2017-03-17

Last Modified: 2021-01-06

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

Text Part Number: OL-29836-01

CONTENTS

Preface

Preface

This document provides information about upgrading software for the 10.x set of releases, including 10.0(1), 10.5(1), and 10.5(2).

Audience

This Upgrade Guide is intended for administrators who are responsible for upgrading the following software:

- Cisco Unified Communications Manager
- IM and Presence Service on Unified Communications Manager

Organization

The following table shows how this guide is organized:

Chapter	Description
Chapter 1	"Getting Started" Provides information about Cisco Unified Communications Manager and the IM and Presence Service, and the relationship between these nodes when they are installed together in a cluster.

Chapter	Description
Chapter 2	"Upgrade Planning" Provides information about system requirements.
Chapter 3	"Upgrade Overview" Provides an overview of the upgrade process, as well as task lists that outline the procedures you must complete for each type of upgrade.
Chapter 4	"Pre-upgrade Tasks" Provides instructions to complete tasks that you must perform before beginning an upgrade.
Chapter 5	"Upgrade Tasks" Provides instructions to upgrade Cisco Unified Communications Manager and the IM and Presence Service.
Chapter 6	"Post-upgrade Tasks" Provides instructions to complete tasks that you must perform after you upgrade Cisco Unified Communications Manager.
Chapter 7	"Troubleshooting" Provides information to help you diagnose problems that may occur during the upgrade process.
Chapter 8	"Reference" Provides information about I/O throttling.

Related Documentation

For additional installation and upgrade information, refer to the following documents:

- *Cisco Prime Collaboration Deployment Administration Guide*

  This document describes how to use the Cisco Prime Collaboration Deployment application, which is designed to assist in the management of Unified Communication applications. You can use this application to perform tasks such as migrate existing clusters to new virtual machines, fresh installs, and upgrades on existing clusters.

- *Administration Guide for Cisco Unified Communications Manager*

  https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html

  This document provides information about upgrading the Unified Communications Manager to a later appliance-based release.

- *Replacing a Single Server or Cluster for Unified Communications Manager*

  http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_installation_guides_list.html

  This document describes how to replace a Unified Communications Manager server or a cluster of servers.

- *Command Line Interface Reference Guide for Cisco Unified Communications Solutions*

  https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html

  This document describes the Command Line Interface for Unified Communications Manager. Some of these commands perform upgrade and installation-related tasks.

For further information about related Cisco IP telephony applications and products, refer to the Unified Communications Manager Documentation Guide for your release at

https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/docguide/11_5_1/cucm_b_documentation-guide-cucm-imp-1151.html

Conventions

This document uses the following conventions:

Convention	Description
boldface font	Commands and keywords are in **boldface**.
italic font	Arguments for which you supply values are in italics.
[ ]	Elements in square brackets are optional.
{ x | y | z }	Alternative keywords are grouped in braces and separated by vertical bars.
[x | y | z]	Optional alternative keywords are grouped in brackets and separated by vertical bars.
string	A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.
`screen` font	Terminal sessions and information the system displays are in **`screen`** font.
`boldface screen` font	Information you must enter is in **`boldface screen`** font.
italic screen font	Arguments for which you supply values are in italic screen font.
^	The symbol ^ represents the key labeled Control—for example, the key combination ^D in a screen display means hold down the Control key while you press the D key.

Convention	Description
< >	Nonprinting characters, such as passwords, are in angle brackets.

Notes use the following conventions:

Note Means reader take note. Notes contain helpful suggestions or references to material not covered in the publication.

Timesavers use the following conventions:

Timesaver Means the described action saves time. You can save time by performing the action described in the paragraph.

Tips use the following conventions:

Tip Means the information contains useful tips.

Cautions use the following conventions:

Caution Means reader be careful. In this situation, you might do something that could result in equipment damage or loss of data.

Warnings use the following conventions:

Warning This warning symbol means danger. You are in a situation that could cause bodily injury. Before you work on any equipment, you must be aware of the hazards involved with electrical circuitry and familiar with standard practices for preventing accidents.

Obtain Documentation and Submit Service Requests

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

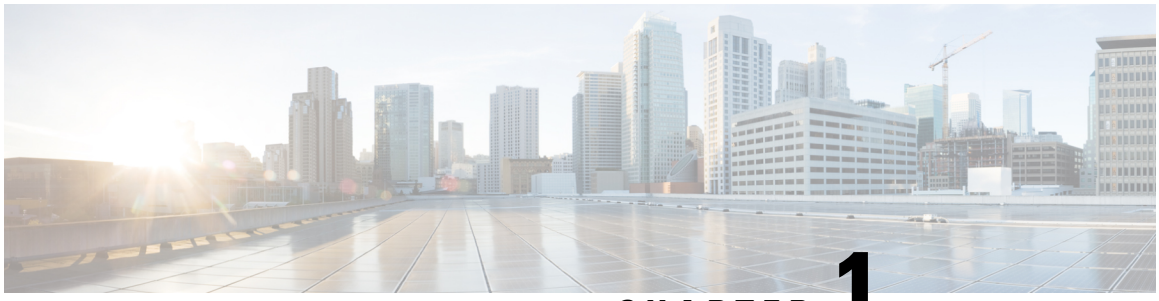
Subscribe to the *What's New in Cisco Product Documentation* as an RSS feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service. Cisco currently supports RSS Version 2.0.

Cisco Product Security Overview

This product contains cryptographic features and is subject to United States and local country laws governing import, export, transfer, and use. Delivery of Cisco cryptographic products does not imply third-party authority to import, export, distribute, or use encryption. Importers, exporters, distributors, and users are responsible for compliance with U.S. and local country laws. By using this product, you agree to comply with applicable laws and regulations. If you are unable to comply with U.S. and local laws, return this product immediately.

Further information regarding U.S. export regulations may be found at

http://www.access.gpo.gov/bis/ear/ear_data.html



CHAPTER 1

Getting Started

The following sections provide information about Cisco Unified Communications Manager and the IM and Presence Service, and the relationship between these nodes when they are installed together in a cluster.

About Cisco Unified Communications Manager

Cisco Unified Communications Manager serves as the software-based call-processing component of the Cisco Unified Communications family of products. A wide range of Cisco Unified Computing System (UCS) servers provides high-availability server platforms for Cisco Unified Communications Manager call processing, services, and applications.

About the IM and Presence Service

IM and Presence, which is a service of Cisco Unified Communications Manager, provides native standards-based dual-protocol enterprise instant messaging (IM) and network-based availability as part of Cisco Unified Communications. This secure, scalable, and easy-to-manage service offers users feature-rich communications capabilities both within and external to the enterprise.

About the System Topology

This section provides an overview of the system topology and describes the relationship between the types of nodes in the topology.

Clusters

Clusters provide a mechanism for distributing call processing and database replication among multiple servers. They provide transparent sharing of resources and features and enable system scalability.

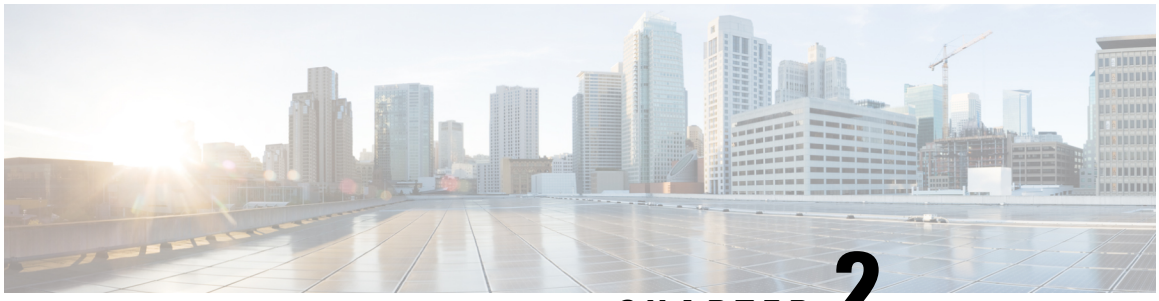
A cluster comprises a set of Cisco Unified Communications Manager (Unified Communications Manager) nodes and IM and Presence nodes that run compatible software versions.

Publisher Nodes and Subscriber Nodes

Within a cluster, there is a database publisher for each type of node that you install.

When you install Unified Communications Manager, the installation wizard prompts you to specify whether the node you are installing is the first node in the cluster. The first Unified Communications Manager node that you install becomes the publisher node, because it publishes the voice and video database to the other Unified Communications Manager nodes in the cluster. All subsequent nodes in the cluster are called subscriber nodes. Each subscriber node must be associated with the publisher node. You must set up all subscriber nodes in the system topology on the publisher node before you install the software on the subscriber nodes.

When you install IM and Presence nodes, the first node that you install functions as the server for the IM and Presence database. Because this node publishes the database for all of the IM and Presence nodes in the cluster, it is referred to as the IM and Presence database publisher; however, you must install this and all other IM and Presence nodes as subscribers of the Unified Communications Manager publisher node. As with other subscriber nodes, you must add these in the system topology before you install the software.



CHAPTER 2

Upgrade Planning

This chapter provides the following information:

Requirements and Limitations

The following sections provide information about the requirements that your system must meet, and limitations that apply when you install or upgrade Unified Communications Manager or IM and Presence Service serivce.

Caution Do not modify any of the IM and Presence Service Service server entries on the Application Server or Server configuration pages of the Cisco Unified CM Administration interface. The IM and Presence Service Service upgrade process automatically updates these entries on the Unified Communications Manager cluster during the final stages (switch version) of the upgrade process.

For upgrades from Release 8.x or 9.x to Release 10.x or later, any manual modification of these entries during the upgrade process will result in data migration failures between IM and Presence Service Service and Unified Communications Manager. If such failures occur, you must restart the entire upgrade process for both Unified Communications Manager and IM and Presence Service Service clusters.

Limitations

This section describes the limitations that apply when you install or upgrade Unified Communications Manager or the IM and Presence Service Service.

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 IM and Presence Service nodes in a cluster is 6.

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

Support for Intercluster Peers

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

Parameter Settings

With the merging of Cisco Unified Communications Manager and IM and Presence Service, enterprise and service parameters are now shared between nodes in a cluster. As such, both types of nodes use the same settings for enterprise and cluster-wide parameters. You need to be aware that not all parameter settings are retained during an upgrade to Release 10.0(1). All enterprise parameters and cluster-wide service parameters that are common to both Cisco Unified Communications Manager and IM and Presence Service retain the value specified on Cisco Unified Communications Manager only, with one exception. The User Assignment Mode parameter is the only enterprise parameter that is retained during upgrade. Service parameters that apply to IM and Presence only are retained after an upgrade.

Cisco recommends that before you begin an upgrade, you make a note of parameter settings and evaluate the best settings for the combined cluster. This will allow you to easily configure those settings after the upgrade is complete.

Network Requirements

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

IP Address Requirements

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

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

DNS requirements

Note the following requirements:

- Mixed-mode DNS deployments not supported—Cisco does not support mixed-mode deployments. Both Unified Communications Manager and IM and Presence Service must either use or not use DNS.

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

SFTP Server Support

Cisco allows you to use any SFTP server product but recommends SFTP products that have been certified with Cisco through the Cisco Solution Partner Program (CSPP). CSPP partners, such as GlobalSCAPE, certify their products with specified versions of Unified Communications Manager. For information on which vendors have certified their products with your version of Unified Communications Manager, go to the following URL and select "Collaboration" from the Technology list in the navigation pane.

https://marketplace.cisco.com/catalog

For information on using GlobalSCAPE with supportedUnified Communications Manager versions, refer to the following URL:

http://www.globalscape.com/gsftps/cisco.aspx

Cisco uses the following servers for internal testing. You may use one of the servers, but you must contact the vendor for support:

- Open SSH (refer tohttp://sshwindows.sourceforge.net/)
- Cygwin (refer to http://www.cygwin.com/)
- Titan (refer to http://www.titanftp.com/)

Cisco does not support using the SFTP product free FTDP. This is because of the 1GB file size limit on this SFTP product.

For issues with third-party products that have not been certified through the CSPP process, contact the third-party vendor for support.

Platform Requirements

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

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

- configure the platform
- install and configure ESXi virtualization software
- deploy the correct OVA template for the release

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

Supported Platforms

Cisco supports virtualized deployments of Unified Communications Manager and the IM and Presence Service on Cisco Unified Computing System servers, or on a Cisco-approved third-party server configuration.

Whether you use a Cisco Unified Computing System server or a Cisco-approved third-party server configuration, you must ensure that the server meets the configuration requirements of the release. The following options are available:

- a tested reference configuration (TRC)
- a specifications-based configuration

For information about the platform configuration specifications, such as CPU, memory, and storage specifications, see UC Virtualization Supported Hardware.

Information about supported platforms is also available in the following documentation:

- *Cisco Unified Communications Manager on Virtualized Servers*
- *Release Notes* for your product release
- *Configuration and Administration of IM and Presence on Cisco Unified Communications Manager*

Related Topics

Change Virtual Machine Configuration Specifications, on page 38

ESXi and VMware Tools

You must install a version of vSphere ESXi hypervisor that meets the requirements of the release, as well as VMWare Tools. VMware Tools are specialized drivers for virtual hardware that is installed in the UC applications when they are running virtualized. It is very important that the VMware tools version be in sync with the version of ESXi being used. For more information, see *Cisco Unified Communications Manager on Virtualized Servers*.

If the server is running VMware EX/ESXi and the motherboard has an ICH10 onboard SATA controller, you must disable the SATA controller in the BIOS. The ICH10 onboard SATA controller is not supported by EX/ESXi.

Related Topics

Upgrade vSphere ESXi, on page 39
Update VMWare Tools, on page 54

OVA Templates

Once ESXi is running on the hardware platform, it is ready to host the virtual machines. The first step is to create the virtual machines on the host. You must use Cisco-generated OVA templates to create the virtual machines to run the Unified Communications Manager application. These OVA templates contain aligned

disk partitions and other specific configurations that are required. See Virtualization for Cisco Unified Communications Manager to download the OVA file for your release.

Power Supply

Ensure that you connect each node to an uninterruptible power supply (UPS) to provide backup power and protect your system. Failure to do so may result in damage to physical media and require a new installation.

If you want the node to automatically monitor UPS signaling and automatically initiate a graceful shutdown upon power loss, Cisco Unified Communications Manager is dependent on the capabilities of the virtualization software or physical server's service processor. Please see documentation for those products for support, if any.

Software Requirements

The following sections provide information about the software requirements that your deployment must meet.

Browser Requirements

Unified Communications Manager and the IM and Presence Service both provide interfaces that you can use to configure and manage the system. You can access the interfaces by using the browsers and operating systems listed in the following table. Cisco does not support or test other browsers.

Table 1: Supported Browsers and Operating Systems

You can access Unified Communications Manager with this browser...	...if you use one of these operating systems
Microsoft Internet Explorer 8	• Microsoft Windows XP SP3 • Microsoft Windows Vista SP2 (or latest service pack available) • Microsoft Windows 7 (32-bit) (with latest service pack available)
Mozilla Firefox 3.x or 4.x (if available)	• Microsoft Windows XP SP3 • Microsoft Windows Vista SP2 (or latest service pack available) • Microsoft Windows 7 (32-bit) (latest service pack available) • Apple Mac OS X (latest service pack available)
Safari 4.x or 5.x (if available)	Apple Mac OS X (or newest OS release available)

Upgrade time requirements

The time required to upgrade the software is variable and depends on a number of factors. For large deployments, installation of the upgrade software may take several hours.

Throttling affects time required to upgrade

To preserve system stability during upgrades, the system throttles the upgrade process, which may increase the time required to complete the upgrade.

If the upgrade process is taking much longer than you would like, you can disable throttling. Although disabling throttling decreases the time it takes to perform the upgrade, it may degrade system performance.

To disable throttling, use the following command in the CLI before you start the upgrade:

```
utils iothrottle disable
```

If you want to restart throttling after you start the upgrade, you must cancel the upgrade, restart throttling, and then restart the upgrade.

System availability after upgrade

For standard upgrades, when you activate the upgraded software, the system restarts and is out of service for up to 30 minutes on the publisher node, depending on the size of the database. The length of the outage on subscriber nodes depends on how long database replication takes to complete.

If you need to revert to an earlier software version, you must restart the system which results in a similar service outage period.

Duplicate ENUMS Break Upgrades and Migrations from 9.1(2)

If you are upgrading or migrating from Release 9.1(2) 10.5(2), or 11.0(1) to any later release, an issue exists with older locale installations that causes upgrade and migration failures. This issue exists if any of the following CUCM combined network locales have been installed:

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

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

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

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

Supported Upgrade Paths

The following sections provide information about the supported upgrade paths for the Cisco Unified Communications Manager and the IM and Presence Service.

Version Requirements

All servers in a cluster must run the same release of Unified Communications Manager. The only exception is during a cluster software upgrade, during which a temporary mismatch is allowed.

If you are installing IM and Presence nodes, the software version of the first IM and Presence node (the IM and Presence database publisher node) must match the first three numbers of the software version installed on the Unified Communications Manager publisher node. For example, IM and Presence Service software version 10.0.1.10000-1 is compatible with Unified Communications Manager software version 10.0.1.30000-2. Refer to the following table for sample Unified Communications Manager versions and IM and Presence Service versions that are compatible. The bolded numbers must match.

Table 2: Examples of Compatible Unified Communications Manager and IM and Presence Service Versions

Sample Unified Communications Manager Version	Example of Compatible IM and Presence Service Version
10.0.1.30000-2	**10.0.1**.10000-1
10.5.1.10000-7	**10.5.1**.10000-9
10.5.2.10000-5	**10.5.2**.10000-9

After you install the first IM and Presence node, the software version of any IM and Presence subscriber nodes that you install must match all five version numbers of the first IM and Presence node. For example, if the IM and Presence database publisher node is at version 10.0.1.10000-1, then all IM and Presence subscriber nodes must also be 10.0.1.10000-1.

Release 11.5(1)SU7

The following versions are supported:

- Cisco Unified Communications Manager 11.5.1.17900-52
- IM and Presence Service 11.5.1.17900-8

This release offers two main deployment options for the IM and Presence Service:

- Standard Deployments (Decentralized)—In this deployment, both Cisco Unified Communications Manager and the IM and Presence Service must be running an 11.5(1)SU7 version for your deployment to be supported. A version mismatch is not supported.
- Centralized Deployments of the IM and Presence Service—Within the IM and Presence central cluster, both the IM and Presence Service and the Cisco Unified Communications Manager instance (this is primarily a database and provisioning instance, and does not handle telephony) must be running an 11.5(1)SU7 version. However, the remote telephony clusters to which the IM and Presence Service connects do not have to be running an 11.5(1)SU7 version.

Release 11.5(1)SU8

The following versions are supported:

- Cisco Unified Communications Manager 11.5.1.18900-97
- IM and Presence Service 11.5.1.18900-15

This release offers two main deployment options for the IM and Presence Service:

- Standard Deployments (Decentralized)—In this deployment, both Cisco Unified Communications Manager and the IM and Presence Service must be running an 11.5(1)SU8 version for your deployment to be supported. A version mismatch is not supported.
- Centralized Deployments of the IM and Presence Service—Within the IM and Presence central cluster, both the IM and Presence Service and the Cisco Unified Communications Manager instance (this is primarily a database and provisioning instance, and does not handle telephony) must be running an 11.5(1)SU8 version. However, the remote telephony clusters to which the IM and Presence Service connects do not have to be running an 11.5(1)SU8 version.

Upgrade Paths For Cisco Unified Communications Manager

The following tables lists the range of upgrade paths that are supported for the Unified Communications Manager 10.x set of releases, including 10.0(1) and 10.5(1), and 10.5(2). For more detailed information about supported upgrade paths, see the *Compatibility Matrix for Cisco Unified Communications Manager and IM and Presence Service*.

Refresh upgrades require you to install Cisco Option Package (COP) files. The following table lists the COP files that you need to download for each upgrade path. You must install the required COP files on all nodes before you begin the upgrade process. Ensure that you review the ReadMe file that supports each COP file before you install it.

Upgrade Paths for Release 10.0(x) of Unified Communications Manager

From	To	Upgrade Type
7.x and older:	10.0(x)	Upgrade to 8.6 first, then refresh upgrade to 10.0(x).
8.0(x) to 8.5(x)	10.0(x)	Refresh upgrade Required COP files: • ciscocm.refresh_upgrade_<latest_version>.cop.sgn • 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
8.6(x) to 9.x	10.0(x)	
10.0(1)x	10.0(1)y	Standard upgrade; no COP files required

Upgrade Paths for Release 10.5(x) of Unified Communications Manager

From	To	Upgrade Type
7.x and older	10.5(x)	Upgrade to 8.6 first, then refresh upgrade to 10.5(x).
8.0(x) to 8.5(x)	10.5(x)	Refresh upgrade Required COP files: • ciscocm.refresh_upgrade_<latest_version>.cop.sgn • 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
8.6(x) to 9.x	10.5(x)	
10.x	10.5(x)	Standard upgrade; no COP files required

Upgrade Paths for IM and Presence Service

The following tables list the range of upgrade paths that are supported for the IM and Presence Service 10.x set of releases, including 10.0(1), 10.5(1) and 10.5(2). For more detailed information about supported upgrade paths, see the *Compatibility Matrix for Cisco Unified Communications Manager and IM and Presence Service*.

Some upgrades require you to install Cisco Option Package (COP) files. The following table lists the COP files that you need to download for each upgrade path. You must install the required COP files on all nodes before you begin the upgrade process. Ensure that you review the ReadMe file that supports each COP file before you install it.

Upgrade Paths for Release 10.0(x) of IM and Presence Service

From Cisco Unified Presence Release	To IM and Presence Release	Upgrade Type
8.5(3) and earlier	10.0(x)	Upgrade to 8.6(5)su5 first, then refresh upgrade to 10.0(x)
8.5(4)	10.0(x)	Refresh upgrade Required COP files: • cisco.com.cup.refresh_upgrade_v<latest_version>.cop • ciscocm.version3-keys.cop.sgn
8.6(3) to 9.x	10.0(x)	Refresh upgrade Required COP file: • ciscocm.version3-keys.cop.sgn

From Cisco Unified Presence Release	To IM and Presence Release	Upgrade Type
10.0.1.x	10.0(x)	Standard upgrade; no COP file required

If you are upgrading from IM and Presence Service 10.0(1) Export Unrestricted to any higher release of IM and Presence Service Export Unrestricted (including Service Updates), you must install the following COP file before you begin the upgrade: `ciscocm.cup.unrst_upgrade_10_0_1_v1.2.cop.sgn`. You can download this file from Cisco.com.

Upgrade Paths for Release 10.5(x) of IM and Presence Service

From Cisco Unified Presence Release	To IM and Presence Release	Upgrade Type
8.5(3) and earlier	10.5(x)	Upgrade to 8.6(5)su5 first, then refresh upgrade to 10.5(x).
8.5(4)	10.5(x)	Refresh upgrade Required COP files: • cisco.com.cup.refresh_upgrade_v<latest_version>.cop • ciscocm.version3-keys.cop.sgn
8.6(3) to 9.x	10.5(x)	Refresh upgrade Required COP file: • ciscocm.version3-keys.cop.sgn
10.x	10.5(x)	Standard upgrade; no COP file required

Upgrade From Cisco Unified Presence Release 8.5(4)

If you upgrade from Cisco Unified Presence Release 8.0(x) or Release 8.5 to the current release, note the following:

- If you have intercluster peers to Cisco Unified Presence Release 8.0(x) or Release 8.5 clusters, you will not have intercluster availability until you upgrade all of these clusters to Release 8.6 or to Release 9.x and later. After the upgrade is complete, the previously configured peers will start working and intercluster availability will be restored.
- If you upgrade a Cisco Unified Presence Release 8.5 cluster that has High Availability (HA) enabled to Release 9.x or later, Cisco recommends that you disable HA on each presence redundancy group before you begin the upgrade. You can reenable HA on each cluster after the switch version is complete, database replication is complete, and all services are back up and running.
- During a software upgrade, the Cisco Replication Watcher service delays feature service startup on the publisher node for up to 20 minutes and on subscriber nodes indefinitely until replication is established.

Note As of IM and Presence Release 10.0(1), the Cisco Replication Watcher service has been renamed to the Cisco IM and Presence Data Monitor service.

Licensing Requirements

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

Cisco Unified Communications Manager License Requirements

Use the Cisco Prime License Manager to allocate and monitor the licenses for Unified Communications Manager, its applications, and endpoints. See the *Cisco Prime License Manager User Guide* for information about generating and installing licenses.

Important Unused PAKs and/or licenses for versions prior to Release 9.0 cannot be installed once your system has been upgraded to Release 9.0 or later. If you have uninstalled PAKs, install all licenses before upgrading.

IM and Presence license requirements

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

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

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

For more information, see the IM and Presence Service chapter in the *Cisco Unified Communications Manager Features and Services Guide*.

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

Export Restricted and Export Unrestricted Software

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

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

Export unrestricted versions differs from restricted versions as follows:

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

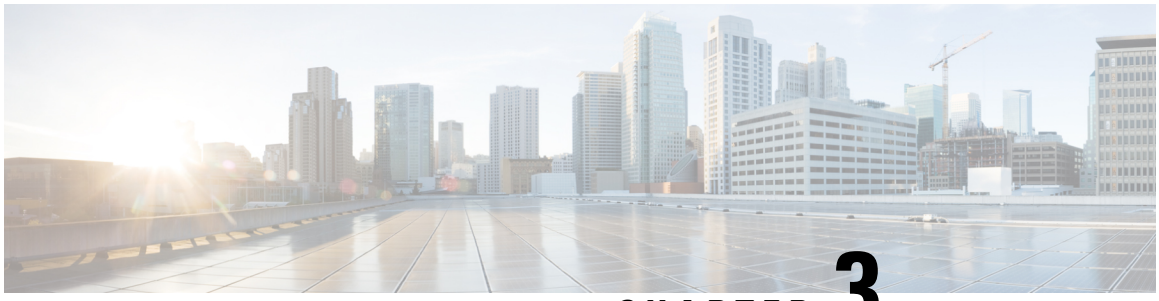
Note Be aware that after you install an unrestricted release, you can never upgrade to a restricted version. You are not allowed to perform a fresh installation of a restricted version on a system that contains an unrestricted version.

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

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

GUI Item	Location	Description
Cisco Unified CM Administration		
VPN Configuration	**Advanced Features** > **VPN**	This menu and its options are not available.
Phone Security Profile Configuration	**System** > **Security** > **Phone Security Profile**	The **Device Security Mode** is set to **Non Secure** and is not configurable.

GUI Item	Location	Description
Cisco Unified CM IM and Presence Administration		
Security Settings	**System** > **Security** > **Settings**	• You cannot check the **Enable XMPP Client to IM/P Service Secure Mode** setting. • You cannot check the **Enable XMPP Router-to-Router Secure Mode** setting. • You cannot check the **Enable Web Client to IM/P Service Secure Mode** setting. • The option to set **SIP intra-cluster Proxy-to-Proxy Transport Protocol** to **TLS** have been removed.
Service Parameter Configuration for Cisco SIP Proxy service	**System** > **Service Parameters** and choose **Cisco SIP Proxy** as the **Service**	• All TLS options have been removed for the **Transport Preferred Order** parameter. • The TLS option have been removed from the **SIP Route Header Transport Type** parameter.
SIP Federated Domains	**Presence** > **Inter-domain Federation** > **SIP Federation**	When you configure interdomain federation to OCS/Lync, you will receive warning popup to indicate that it is only possible to directly federate with another OCS/Lync within the enterprise. Interdomain federation to OCS/Lync outside the enterprise is not supported in unrestricted mode.
XMPP Federation Settings	**Presence** > **Inter-domain Federation** > **XMPP Federation** > **Settings**	You cannot configure the security mode; It is set to **NO TLS**.
Proxy Configuration Settings	**Presence** > **Routing** > **Settings**	You cannot set any TLS or HTTPS listeners as the preferred proxy listener.



CHAPTER 3

Upgrade Overview

This section provides the following information:

Types of upgrades

There are two types of upgrades:

- standard upgrades
- refresh upgrades

The server automatically determines whether you need to perform a standard upgrade or a refresh upgrade.

Standard upgrades

Standard upgrades are upgrades that do not require upgrades to the operating system. You can install upgrade software on your server while the system continues to operate.

For standard upgrades, you install the upgrade software as an inactive version. The system continues to function normally while you are installing the software. When the upgrade is complete, you can choose to automatically reboot the system to the upgraded software or you can manually switch to the new software at a later time. When you reboot to the new software, the old software version remains on the system. This allows you to revert to the old version in the unlikely event of issues with the new software. During an upgrade your configuration information migrates automatically to the upgraded version.

Note You can only make any provisioning changes to the database on the active software. The database for the inactive software is not updated. If you make changes to the database after an upgrade, you must repeat those changes after switching to the new software.

Note See ***Resuming a Failed Upgrade*** section of the ***Troubleshooting*** chapter for more details.

Refresh upgrades

Refresh upgrades are required in situations where incompatibilities exist between the old and new software releases. For example, a refresh upgrade is required when the major version of the embedded operating system changes between the version you are upgrading from and the version that you are upgrading to. Refresh upgrades require multiple reboots during installation to upgrade the underlying operating system, causing a temporary server outage while the software is installed. The duration of this outage will depend on your configuration and the size of the database.

Note You must perform all refresh upgrades during a maintenance window because the system will not be available during the upgrade.

For refresh upgrades, the upgrade wizard allows you to choose whether or not to automatically run the new upgraded software when the upgrade completes. If you select not to run the new software, the system will reboot to the old software version when the upgrade is complete and you can manually switch to the new software at a later time.

If for any reason you decide to revert to the prior software version, you can switch versions to the older version of the software. This switch version requires a reboot. Be aware that any configuration changes that you made after upgrading the software will be lost.

COP Files

When you perform a refresh upgrade, you must install COP files before you begin upgrading from any of the following releases:

- upgrades from Cisco Unified Communications Manager 8.5(x) and older to Cisco Unified Communications Manager 10.0(x)
- upgrades from Cisco Unified Presence 8.5(4) to IM and Presence 10.0(x)

You can download the following COP files from Cisco.com:

COP file	Purpose
ciscocm.refresh_upgrade_v<latest_version>.cop.sgn	Required. Install this file on all Unified Communications Manager nodes to update the operating system so that it supports the new release.
ciscocm.cup.refresh_upgrade_v<latest_version>.cop	Required. Install this file on all IM and Presence Service nodes to update the operating system so that it supports the new release.
ciscocm.vmware-disk-size-reallocation-<latest_version>.cop.sgn	Optional. This COP file expands the vDisk size. Install this COP file on either Unified Communications Manager nodes or IM and Presence Service nodes if you need to increase the vDisk space to meet the space requirements of a refresh upgrade. This option requires a reboot.

COP file	Purpose
ciscocm.free_common_space_<latest_version>.cop.sgn	Optional. This COP file removes the inactive side in the common partition to increase available disk space without requiring a system rebuild. Install this COP file on Unified Communications Manager nodes or IM and Presence Service nodes as required to perform an upgrade. You can use this COP file as an alternative to the COP file listed above, or in conjunction with it. This option does not require a reboot. **Note** You will not be able to switch back to the inactive version after installing this file.

To find COP files on Cisco.com, navigate to **Support > Downloads > Cisco Unified Communications Manager Version 10.0 > Unified Communications Manager/CallManager/Cisco Unity Connection Utilities**.

Caution If you do not install the COP file on all nodes for the required releases, the upgrade will fail.

COP File Installation

The following guidelines apply to installing COP files. If the documentation for a specific COP file contradicts these general guidelines, follow the COP file documentation:

- Install the appropriate COP file on every node in a cluster. Perform this task before you install new software on each node in the cluster and set up the database.
- After you install a COP file, you must restart the node.
- Restart Cisco Unified Communications Manager to ensure that configuration changes that are made during the COP file installation get written into the database.
- Restart the IM and Presence Service to ensure that configuration changes that are made during the COP file installation get written into the database.

Upgrade Process

You can begin an upgrade using either the command line interface or graphical user interface. You can monitor progress of the upgrade using the console until the command line interface and graphical user interface access has been restored. Once these interfaces are restored, you can use the command line interface or graphical user interface to continue to monitor upgrade progress.

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 Cisco 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 Cisco Unified Communications Manager synchronizes the database after an installation or upgrade, which can overwrite phone user settings changes.

Accessing the Upgrade File

The method that you use to access the upgrade file depends on your network environment. The following options are available:

- access the upgrade file on a remote FTP or SFTP server
- access the upgrade file on the physical DVD drive of a VMware ESXi server host
- upgrade from a data store ISO file on the local ESXi host; for this option, you must edit the virtual machine's CD/DVD drive to map to the file
- upgrade from a data store ISO file on a storage area network (SAN) that is connected to the ESXi host;for this option, you must edit the virtual machine's CD/DVD drive to map to the file

Sequence Rules

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

- The Unified Communications Manager publisher node must be the first node that you upgrade. The new software is installed as an inactive version.
- You can begin upgrading Unified Communications Manager subscriber nodes as soon as the publisher node has been upgraded with an inactive version of the new software.
- You must switch the Unified Communications Manager publisher node to the new software version and reboot it before you switch the version on any subscriber nodes. The publisher node must be the first node to switch to the new software version and reboot.
- If you upgrade a group of subscriber nodes, after you switch the software version and reboot, you must wait for database replication to complete on all subscriber nodes before proceeding with any COP file installs or configuration changes.
- If you are upgrading Unified Communications Manager nodes to a Maintenance Release (MR) or an Engineering Special (ES) Release and you are not upgrading IM and Presence Service nodes, you must reboot all IM and Presence nodes after the Unified Communications Manager upgrade is complete.
- If you are upgrading IM and Presence Service nodes in addition to Unified Communications Manager nodes:
    - The IM and Presence Service database publisher node must be the first IM and Presence Service node that you upgrade. The new software is installed as an inactive version.
    - You can begin upgrading IM and Presence Service subscriber nodes as soon as the publisher node has been upgraded with an inactive version of the new software.

- You can wait until all of the Unified Communications Manager nodes are upgraded to an inactive version before you upgrade the IM and Presence Service database publisher node, or you can choose to upgrade in parallel. If you upgrade in parallel, start upgrading the IM and Presence Service database publisher node at the same time that you upgrade the Unified Communications Manager subscriber nodes.
- You must switch to the new software version and reboot all Unified Communications Manager nodes, starting with the publisher node, before you can switch versions on the IM and Presence Service nodes.
- You must switch the IM and Presence Service database publisher node to the new software version and reboot it before you switch the software version on any IM and Presence Service subscriber nodes.
- If you upgrade a group of IM and Presence Service subscriber nodes, after you switch the software version and reboot, you must wait for database replication to complete on all subscriber nodes before proceeding.

- If you are upgrading IM and Presence Service nodes to a Maintenance Release (MR) or an Engineering Special (ES) Release and you are not upgrading Unified Communications Manager nodes, the following additional sequencing rules apply:
  - For upgrades using the Unified CM OS Admin interface, you must upgrade the Unified Communications Manager publisher node and then upgrade the IM and Presence Service nodes to the Maintenance Release (MR) or an Engineering Special (ES) Release.
  - If you are using the Prime Collaboration Deployment migration task, you must select the Unified Communications Manager publisher node in addition to the IM and Presence Service nodes.
  - If you are using the Prime Collaboration Deployment upgrade task, you do not need to select the Unified Communications Manager publisher node as long as the first 3 digits of new version of IM and Presence Service match the first 3 digits of the currently installed version of Unified Communications Manager.

Upgrade Task Lists

The following sections provide a list of the high-level tasks that you must perform for each of the supported upgrade scenarios:

- upgrade the software on both Unified Communications Manager nodes, and IM and Presence nodes
- upgrade the software on Unified Communications Manager nodes only
- upgrade the software on IM and Presence nodes only

Perform the tasks in the order shown in these high-level task lists. For detailed information about how to perform the tasks outlined in these task lists, refer to the Related Topics section included at the end of each task list.

Standard Upgrade of Unified Communications Manager and IM and Presence Nodes

Complete the high-level tasks listed in this section when you want to perform a standard upgrade on both the Unified Communications Manager nodes and the IM and Presence nodes in your network.

Procedure

Step 1 Perform all pre-upgrade tasks that apply to your site.

Step 2 Stop all configuration tasks.

Caution Do not make any configuration changes during an upgrade. For example, do not change passwords, perform LDAP synchronizations, or run any automated jobs until you have completed the upgrade on all nodes and performed the post-upgrade tasks. Any configuration changes that you make during an upgrade may 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 Cisco Unified Communications Manager nodes and all IM and Presence Service nodes.

Do not modify any of the IM and Presence Service server entries on the Application Server or Server configuration pages of the Cisco Unified CM Administration interface. The IM and Presence Service upgrade process automatically updates these entries on the Cisco Unified Communications Manager cluster during the final stages (switch version) of the upgrade process.

Any manual modification of these entries during the upgrade process will result in data migration failures between IM and Presence Service and Cisco Unified Communications Manager. If such failures occur, you must restart the entire upgrade process for both Cisco Unified Communications Manager and IM and Presence Service clusters.

Step 3 Upgrade the Unified Communications Manager publisher node. The Unified Communications Manager publisher node is the first node in the cluster.

Step 4 Upgrade the Unified Communications Manager subscriber nodes.

Step 5 Switch the first node to the upgraded partition.

Step 6 Switch the subscriber nodes to the upgraded partition.

Note You can switch the subscriber nodes to the upgraded partition either all at once or one at a time, depending on your site requirements.

Step 7 Ensure that database replication is functioning between the first node (the Unified Communications Manager publisher node) and the subscriber nodes. You can check database replication status by using one of the following methods:

- In Cisco Unified Reporting, access the Unified Communications Manager Database Status report. Before you proceed, ensure the report indicates that you have a good database replication status with no errors. For more information about using Cisco Unified Reporting, see the *Cisco Unified Reporting Administration Guide*.
- In the Cisco Real Time Monitoring Tool, access the Database Summary service under the CallManager tab to monitor database replication status. The following list indicates the database replication status progress:

- 0 - Initializing; replication setup is in process.
- 1 - Replication setup script running on this node; transitional state.
- 2 - Set-up complete; replication is setup and in a good state.
- 3 - Out of sync; replication is setup, but some data is going out of sync.
- 4 - Failed; replication setup did not succeed.

Before you proceed, ensure that the database replication is setup and in a good state. For more information about using the Real Time Monitoring Tool, see the *Cisco Unified Real Time Monitoring Tool Administration Guide*.

Step 8 Perform post-upgrade tasks for Unified Communications Manager nodes.

Step 9 Upgrade the IM and Presence database publisher node. The IM and Presence database publisher node is the first node in the IM and Presence cluster.

Step 10 Upgrade the IM and Presence subscriber nodes.

Step 11 Switch the software to the new software release on the IM and Presence database publisher node (the first IM and Presence node). Wait until the first node has successfully restarted and is at the sign in prompt before you proceed to the next step.

Step 12 On the IM and Presence subscriber node, switch the software to the new software release. After the IM and Presence subscriber node has restarted and has come back online with the new software release, switch the software release on the next node. Wait until each of the nodes has successfully restarted (is at the sign in prompt) before you proceed with the software switch on the next node. Repeat until the new software release is running on all nodes.

Step 13 Run the following CLI commands:

- run `utils dbreplication status` to check for errors or mismatches in the database tables
- run `utils dbreplication runtimestate` to check if the database replication is active on a node

If database replication is active on all nodes, the output lists all the nodes and the **replication setup** value for each node is **2**.

Note If database replication is not complete (a value other than 2 is returned), core services will not start on the subscriber nodes until replication is complete. Select **Cisco Unified CM IM and Presence Administration** > **System** > **Notifications** to determine whether database replication is complete.

Replication takes 20-30 minutes on average, but it may take longer depending on the size of the database.

Step 14 Perform post-upgrade tasks for the IM and Presence Service.

Related Topics

Perform Pre-Upgrade Tasks, on page 35
Upgrade from a Local Source, on page 42
Upgrade from a Remote Source, on page 44
Switch the Software Version, on page 49
Locale Installation, on page 54
Post-Upgrade Tasks for Cisco Unified Communications Manager Nodes, on page 59
Post-Upgrade Tasks for IM and Presence Nodes, on page 63

Refresh Upgrade of Unified Communications Manager and IM and Presence Nodes

Complete the high-level tasks listed in this section when you want to perform a refresh upgrade on both the Unified Communications Manager nodes and the IM and Presence Service nodes in your network.

Procedure

Step 1 Perform all pre-upgrade tasks that apply to your site.

Step 2 Stop all configuration tasks.

Caution Do not make any configuration changes during an upgrade. For example, do not change passwords, perform LDAP synchronizations, or run any automated jobs until you have completed the upgrade on all nodes and performed the post-upgrade tasks. Any configuration changes that you make during an upgrade may 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 Cisco Unified Communications Manager nodes and all IM and Presence Service nodes.

Do not modify any of the IM and Presence Service server entries on the Application Server or Server configuration pages of the Cisco Unified CM Administration interface. The IM and Presence Service upgrade process automatically updates these entries on the Cisco Unified Communications Manager cluster during the final stages (switch version) of the upgrade process.

Any manual modification of these entries during the upgrade process will result in data migration failures between IM and Presence Service and Cisco Unified Communications Manager. If such failures occur, you must restart the entire upgrade process for both Cisco Unified Communications Manager and IM and Presence Service clusters.

Step 3 If you are performing a refresh upgrade that requires a COP file, install the required COP file.

If you are unsure whether you need to install a COP file, review the information about supported upgrade paths.

Step 4 Upgrade the Unified Communications Manager publisher node. The Unified Communications Manager publisher node is the first node in the cluster.

Step 5 Switch the software to the new software release. To do this, select **Switch to new version after upgrade**. The publisher node must be running the new software before you upgrade each subscriber node.

Step 6 Upgrade each Unified Communications Manager subscriber node.

Step 7 Switch the software on the subscriber nodes to the new software release. To do this, select **Switch to new version after upgrade**.

Note You can switch the subscriber nodes to the upgraded partition either all at once or one at a time, depending on your site requirements.

Step 8 Ensure that database replication is functioning between the first node (the Unified Communications Manager publisher node) and the subscriber nodes. You can check database replication status by using one of the following methods:

- In Cisco Unified Reporting, access the Unified Communications Manager Database Status report. Before you proceed, ensure the report indicates that you have a good database replication status with no errors. For more information about using Cisco Unified Reporting, see the *Cisco Unified Reporting Administration Guide*.
- In the Cisco Real Time Monitoring Tool, access the Database Summary service under the CallManager tab to monitor database replication status. The following list indicates the database replication status progress:
  - 0 - Initializing; replication setup is in process.
  - 1 - Replication setup script running on this node; transitional state.
  - 2 - Set-up complete; replication is setup and in a good state.
  - 3 -Out of sync; replication is setup, but some data is going out of sync.
  - 4 - Failed; replication setup did not succeed.

Before you proceed, ensure that the database replication is setup and in a good state. For more information about using the Real Time Monitoring Tool, see the *Cisco Unified Real Time Monitoring Tool Administration Guide*.

Step 9 Perform post-upgrade tasks for Unified Communications Manager nodes.

Step 10 If you are performing a refresh upgrade that requires a COP file, install the required COP file on every IM and Presence node in the cluster and restart the nodes.

If you are unsure whether you need to install a COP file, review the information about supported upgrade paths. See the Related Topics section below for more information.

Step 11 Upgrade the IM and Presence database publisher node. The IM and Presence database node is the first node in the IM and Presence cluster.

Step 12 Switch the software to the new software release. To do this, select **Switch to new version after upgrade**. The IM and Presence database publisher node must be running the new software before you upgrade the IM and Presence subscriber nodes.

Step 13 Upgrade each IM and Presence subscriber node.

Step 14 Switch the software on the subscriber nodes to the new software release. To do this, select **Switch to new version after upgrade**.

Step 15 Run the following CLI command (on the publisher or subscriber node) to check if the database replication is active on a node:

```
utils dbreplication runtimestate
```

If database replication is active on all nodes, the output lists all the nodes and the **replication setup** value for each node is **2**.

Note If database replication is not complete (a value other than 2 is returned), core services will not start on the subscriber node. Select **Cisco Unified CM IM and Presence Administration** > **System** > **Notifications** to determine whether database replication is complete.

Replication takes 20-30 minutes on average, but it may take longer depending on the size of the database.

Step 16 Perform post-upgrade tasks for the IM and Presence Service.

Related Topics

Perform Pre-Upgrade Tasks, on page 35
COP Files, on page 18
Upgrade from a Local Source, on page 42
Upgrade from a Remote Source, on page 44
Switch the Software Version, on page 49
Locale Installation, on page 54
Post-Upgrade Tasks for Cisco Unified Communications Manager Nodes, on page 59
Post-Upgrade Tasks for IM and Presence Nodes, on page 63

Standard Upgrade of Unified Communications Manager Nodes Only

Complete the high-level tasks listed in this section when you want to perform a standard upgrade of only the Unified Communications Manager nodes in your network. When you upgrade Unified Communications Manager nodes without upgrading IM and Presence nodes, ensure that the installed version of the IM and Presence Service is compatible with the new version of the Unified Communications Manager software.

Note When Cisco Unified Communications Manager 10.0(x) is upgraded as part of a service update or a maintenance release, Cisco Sync Agent sends a notification to Cisco Unified CM IM and Presence Administration that the IM and Presence Service database publisher node and subscriber nodes must be rebooted. You must manually clear this notification after the reboots are complete. A warning message about the upgrade is also raised in the Cisco Unified Communications Manager OS Administration GUI.

Procedure

Step 1 Perform all pre-upgrade tasks that apply to your site.

Step 2 Stop all configuration tasks. Do not perform any configuration tasks during the upgrade.

Caution Do not make any configuration changes during an upgrade. For example, do not change passwords, perform LDAP synchronizations, or run any automated jobs until you have completed the upgrade on all nodes and performed the post-upgrade tasks. Any configuration changes that you make during an upgrade may 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 Cisco Unified Communications Manager nodes.

Step 3 Upgrade the Unified Communications Manager publisher node. The Unified Communications Manager publisher node is the first node in the cluster.

Step 4 Upgrade the Unified Communications Manager subscriber nodes.

Step 5 When you have completed the upgrade of all the subscriber nodes, switch the publisher node to the upgraded software version.

Step 6 When the publisher node is switched to the new version, switch the subscriber nodes to the upgraded software version.

Step 7 Ensure that database replication is functioning between the first node (the Unified Communications Manager publisher node) and the subscriber nodes. You can check database replication status by using one of the following methods:

- In Cisco Unified Reporting, access the Unified Communications Manager Database Status report. Before you proceed, ensure the report indicates that you have a good database replication status with no errors. For more information about using Cisco Unified Reporting, see the *Cisco Unified Reporting Administration Guide*.
- In the Cisco Real Time Monitoring Tool, access the Database Summary service under the CallManager tab to monitor database replication status. The following list indicates the database replication status progress:
  - 0 - Initializing; replication setup is in process.
  - 1 - Replication setup script running on this node; transitional state.
  - 2 - Set-up complete; replication is setup and in a good state.
  - 3 -Out of sync; replication is setup, but some data is going out of sync.
  - 4 - Failed; replication setup did not succeed.

Before you proceed, ensure that the database replication is setup and in a good state. For more information about using the Real Time Monitoring Tool, see the *Cisco Unified Real Time Monitoring Tool Administration Guide*.

Step 8 Perform post-upgrade tasks for Unified Communications Manager nodes.

Step 9 If you upgraded Cisco Unified Communications Manager to a Maintenance Release (MR) or an Engineering Special (ES) Release and you do not upgrade the IM and Presence Service, you must reboot all IM and Presence nodes after the Unified Communications Manager upgrade is complete.

Related Topics

Perform Pre-Upgrade Tasks, on page 35
Upgrade from a Local Source, on page 42
Upgrade from a Remote Source, on page 44
Switch the Software Version, on page 49
Locale Installation, on page 54
Post-Upgrade Tasks for Cisco Unified Communications Manager Nodes, on page 59

Refresh Upgrade Of Unified Communications Manager Nodes Only

Complete the high-level tasks listed in this section when you want to perform a refresh upgrade of only the Unified Communications Manager nodes in your network. When you upgrade Unified Communications Manager nodes without upgrading IM and Presence nodes, ensure that the installed version of the IM and Presence Service is compatible with the new version of the Unified Communications Manager software.

Procedure

Step 1 Perform all pre-upgrade tasks that apply to your site.

Step 2 Stop all configuration tasks.

Caution Do not make any configuration changes during an upgrade. For example, do not change passwords, perform LDAP synchronizations, or run any automated jobs until you have completed the upgrade on all nodes and performed the post-upgrade tasks. Any configuration changes that you make during an upgrade may 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 Cisco Unified Communications Manager nodes.

Step 3 If you are performing a refresh upgrade that requires a COP file, install the required COP file.

If you are unsure whether you need to install a COP file, review the information about supported upgrade paths.

Step 4 Upgrade the Unified Communications Manager publisher node. The Unified Communications Manager publisher node is the first node in the cluster.

Step 5 Switch the software to the new software release. To do this, select **Switch to new version after upgrade**. The publisher node must be running the new software before you upgrade each subscriber node.

Step 6 Upgrade each Unified Communications Manager subscriber node.

Step 7 Switch the software on the subscriber nodes to the new software release. To do this, select **Switch to new version after upgrade**.

Step 8 Ensure that database replication is functioning between the first node (the Unified Communications Manager publisher node) and the subscriber nodes. You can check database replication status by using one of the following methods:

- In Cisco Unified Reporting, access the Unified Communications Manager Database Status report. Before you proceed, ensure the report indicates that you have a good database replication status with no errors. For more information about using Cisco Unified Reporting, see the *Cisco Unified Reporting Administration Guide*.
- In the Cisco Real Time Monitoring Tool, access the Database Summary service under the CallManager tab to monitor database replication status. The following list indicates the database replication status progress:
  - 0 - Initializing; replication setup is in process.
  - 1 - Replication setup script running on this node; transitional state.
  - 2 - Set-up complete; replication is setup and in a good state.
  - 3 -Out of sync; replication is setup, but some data is going out of sync.
  - 4 - Failed; replication setup did not succeed.

Before you proceed, ensure that the database replication is setup and in a good state. For more information about using the Real Time Monitoring Tool, see the *Cisco Unified Real Time Monitoring Tool Administration Guide*.

Step 9 Perform post-upgrade tasks for Unified Communications Manager nodes.

Step 10 If you upgraded Unified Communications Manager to a Maintenance Release (MR) or an Engineering Special (ES) Release and you do not upgrade IM and Presence Service, you must reboot all IM and Presence nodes after the Unified Communications Manager upgrade is complete.

Related Topics

Perform Pre-Upgrade Tasks, on page 35
COP Files, on page 18
Upgrade from a Local Source, on page 42
Upgrade from a Remote Source, on page 44
Switch the Software Version, on page 49
Locale Installation, on page 54
Post-Upgrade Tasks for Cisco Unified Communications Manager Nodes, on page 59

Standard Upgrade of IM and Presence Nodes Only

Complete the high-level tasks listed in this section when you want to perform a standard upgrade the IM and Presence nodes in your network without upgrading Unified Communication Manager subscriber nodes.

When you upgrade IM and Presence nodes without upgrading Unified Communication Manager subscriber nodes, ensure that the installed version of Unified Communication Manager is compatible with the new version of the Unified Communication Manager software. The software version of the first IM and Presence node (the IM and Presence database publisher node) must match the first two numbers of the software version installed on the Unified Communications Manager publisher node. For example, IM and Presence Service software version 10.0.1.10000-1 is compatible with Cisco Unified Communications Manager software version 10.0.1.30000-2.

Procedure

Step 1 Perform all pre-upgrade tasks that apply to your site.

Step 2 Stop all configuration tasks. Do not perform any configuration tasks during the upgrade.

Caution Do not make any configuration changes during an upgrade. For example, do not change passwords, perform LDAP synchronizations, or run any automated jobs until you have completed the upgrade on all nodes and performed the post-upgrade tasks. Any configuration changes that you make during an upgrade may 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 Cisco Unified Communications Manager nodes and all IM and Presence Service nodes.

Do not modify any of the IM and Presence Service server entries on the Application Server or Server configuration pages of the Cisco Unified CM Administration interface. The IM and Presence Service upgrade process automatically updates these entries on the Cisco Unified Communications Manager cluster during the final stages (switch version) of the upgrade process.

Any manual modification of these entries during the upgrade process will result in data migration failures between IM and Presence Service and Cisco Unified Communications Manager. If such failures occur, you must restart the entire upgrade process for both Cisco Unified Communications Manager and IM and Presence Service clusters.

Step 3 Upgrade the Unified Communications Manager publisher node. The Unified Communications Manager publisher node is the first node in the cluster.

Step 4 Upgrade the IM and Presence database publisher node. The IM and Presence database publisher node is the first node in the IM and Presence cluster.

Step 5 Upgrade the IM and Presence subscriber nodes.

Step 6 Switch the software to the new software release. To do this, select **Switch to new version after upgrade**. You must switch the software to the upgraded version in the following order:

- Switch the software on the Unified Communications Manager publisher node.
- Switch the software on the IM and Presence database publisher node.
- Switch the software on the IM and Presence subscriber nodes.

Wait until each of the nodes has successfully restarted and is at the sign in prompt before you proceed with the software switch on the next node. Repeat until the new software release is running on all nodes.

Step 7 Run the following CLI command to check if the database replication is active on a node:

```
utils dbreplication runtimestate
```

If database replication is active on all nodes, the output lists all the nodes and the **replication setup** value for each node is **2**.

Note If database replication is not complete (a value other than 2 is returned), core services will not start on the subscriber nodes. Select **Cisco Unified CM IM and Presence Administration** > **System** > **Notifications** to determine whether database replication is complete.

Replication takes 20-30 minutes on average, but it may take longer depending on the size of the database.

Step 8 Perform post-upgrade tasks for the IM and Presence Service.

In the event of an IM and Presence upgrade failure

If the upgrade of Unified Communications Manager nodes is successful but the upgrade of IM and Presence nodes fails, you must either:

- perform another upgrade of both the Unified Communications Manager nodes and the IM and Presence nodes after you address the issues that caused the failure
- perform a DRS restore on the Unified Communications Manager node where the backup was taken from to restore it to the configuration it had before the attempted upgrade of the IM and Presence nodes

Related Topics

Perform Pre-Upgrade Tasks, on page 35
Upgrade from a Local Source, on page 42
Upgrade from a Remote Source, on page 44
Switch the Software Version, on page 49
Locale Installation, on page 54
Post-Upgrade Tasks for IM and Presence Nodes, on page 63

Refresh Upgrade of IM and Presence Nodes Only

Complete the high-level tasks listed in this section when you want to perform a refresh upgrade the IM and Presence nodes in your network without upgrading Cisco Unified Communication Manager subscriber nodes. When you upgrade IM and Presence nodes without upgrading Unified Communications Manager subscriber nodes, ensure that the installed version of Unified Communications Manager is compatible with the new version of the IM and Presence Service software.

Procedure

Step 1 Perform all pre-upgrade tasks that apply to your site.

Step 2 Stop all configuration tasks. Do not perform any configuration tasks during the upgrade.

Caution Do not make any configuration changes during an upgrade. For example, do not change passwords, perform LDAP synchronizations, or run any automated jobs until you have completed the upgrade on all nodes and performed the post-upgrade tasks. Any configuration changes that you make during an upgrade may 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 Cisco Unified Communications Manager nodes and all IM and Presence Service nodes.

Do not modify any of the IM and Presence Service server entries on the Application Server or Server configuration pages of the Cisco Unified CM Administration interface. The IM and Presence Service upgrade process automatically updates these entries on the Cisco Unified Communications Manager cluster during the final stages (switch version) of the upgrade process.

Any manual modification of these entries during the upgrade process will result in data migration failures between IM and Presence Service and Cisco Unified Communications Manager. If such failures occur, you must restart the entire upgrade process for both Cisco Unified Communications Manager and IM and Presence Service clusters.

Step 3 If you are performing a refresh upgrade that requires a COP file, install the required COP file.

If you are unsure whether you need to install a COP file, review the information about supported upgrade paths. See the Related Topics section below for more information.

Step 4 Upgrade the Unified Communications Manager publisher node. The Unified Communications Manager publisher node is the first node in the cluster.

Step 5 Switch the software to the new software release. To do this, select **Switch to new version after upgrade**. The Unified Communications Manager publisher node must be running the new software before you upgrade each IM and Presence subscriber node.

Step 6 Upgrade the IM and Presence database node. The IM and Presence database node is the first node in the IM and Presence cluster.

Step 7 Switch the software to the new software release. To do this, select **Switch to new version after upgrade**.

Step 8 Upgrade the IM and Presence subscriber nodes.

Step 9 Switch the software on the subscriber nodes to the new software release. To do this, select **Switch to new version after upgrade**.

Wait until each of the nodes has successfully restarted and is at the sign in prompt before you proceed with the software switch on the next node. Repeat until the new software release is running on all nodes.

Step 10 Run the following CLI command to check if the database replication is active on a node:

```
utils dbreplication runtimestate
```

If database replication is active on all nodes, the output lists all the nodes and the **replication setup** value for each node is **2**.

Note If database replication is not complete (a value other than 2 is returned), core services will not start on the subscriber nodes. Select **Cisco Unified CM IM and Presence Administration** > **System** > **Notifications** to determine whether database replication is complete.

Replication takes 20-30 minutes on average, but it may take longer depending on the size of the database.

Step 11 Request that all IM and Presence client users in the local and remote cluster sign out, and sign back in to the application.

Step 12 Perform post-upgrade tasks for the IM and Presence Service.

In the event of an IM and Presence upgrade failure

If the upgrade of Unified Communications Manager nodes is successful but the upgrade of IM and Presence nodes fails, you must either:

- perform another upgrade of both the Unified Communications Manager nodes and the IM and Presence nodes after you address the issues that caused the failure
- perform a DRS restore on the Unified Communications Manager node where the backup was taken from to restore it to the configuration it had before the attempted upgrade of the IM and Presence nodes

Related Topics

Perform Pre-Upgrade Tasks, on page 35
COP Files, on page 18
Upgrade from a Local Source, on page 42
Upgrade from a Remote Source, on page 44
Switch the Software Version, on page 49
Locale Installation, on page 54
Post-Upgrade Tasks for IM and Presence Nodes, on page 63

Parallel Upgrades

Complete the high-level tasks listed in this section when you want to upgrade nodes in a cluster in parallel.

You can begin upgrading subscriber nodes after the publisher node has finished upgrading. If you are performing a refresh upgrade, there will be a temporary server outage until all subscriber nodes get upgraded to the new software version.

Procedure

Step 1 Perform all pre-upgrade tasks that apply to your site.

Step 2 Stop all configuration tasks.

Caution Do not make any configuration changes during an upgrade. For example, do not change passwords, perform LDAP synchronizations, or run any automated jobs until you have completed the upgrade on all nodes and performed the post-upgrade tasks. Any configuration changes that you make during an upgrade may 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 Cisco Unified Communications Manager nodes and all IM and Presence Service nodes.

Do not modify any of the IM and Presence Service server entries on the Application Server or Server configuration pages of the Cisco Unified CM Administration interface. The IM and Presence Service upgrade process automatically updates these entries on the Cisco Unified Communications Manager cluster during the final stages (switch version) of the upgrade process.

Any manual modification of these entries during the upgrade process will result in data migration failures between IM and Presence Service and Cisco Unified Communications Manager. If such failures occur, you must restart the entire upgrade process for both Cisco Unified Communications Manager and IM and Presence Service clusters.

Step 3 Upgrade the Unified Communications Manager publisher node. The Unified Communications Manager publisher node is the first node in the cluster.

Step 4 View the installation log to monitor the status of the upgrade by using the Software Installation/Upgrade window in Cisco Unified Communications Operating System Administration or by using the command line interface (CLI).

- List the install log:

```
file list install install_* date
install_log_2008-10-01.09.41.57.log     install_log_2008-10-08.12.59.29.log
install_log_2008-10-14.09.31.06.log
dir count = 0, file count = 3
```

- Search the most recent install log for the string PRODUCT_VERSION; for example:

```
admin:file search install install_log_2013-01-07.09.39.11.log PRODUCT_VERSION

Searching path: /var/log/install/install_log_2013-01-07.09.39.11.log
Searching file: /var/log/install/install_log_2013-01-07.09.39.11.log
01/07/2013 09:53:54 post_upgrade|PRODUCT_VERSION is 9.1.1.10000-11|<LVL::Info>
01/07/2013 09:53:54 post_upgrade|PRODUCT_VERSION_DISPLAY is
9.1.1.10000-11|<LVL::Info>
Search completed
```

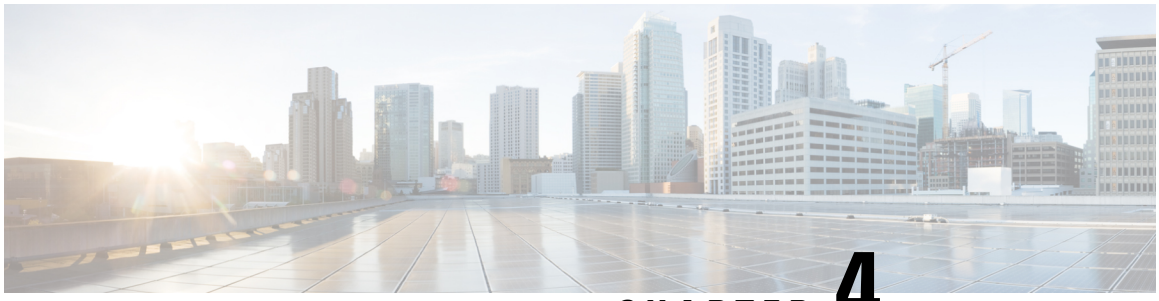
Step 5 When the upgrade on the publisher node is complete, begin the upgrade on the subscriber nodes.

Step 6 Activate the new software on the publisher node.

Step 7 Activate the new software on the subscriber nodes.

Related Topics

Perform Pre-Upgrade Tasks, on page 35
Upgrade from a Local Source, on page 42
Upgrade from a Remote Source, on page 44
Switch the Software Version, on page 49



CHAPTER 4

Pre-Upgrade Tasks

Perform Pre-Upgrade Tasks

Before you begin the upgrade, perform the following tasks:

Procedure

Step 1 Read the release notes for the new release and be sure that you understand the new features and how the upgrade interacts with the other products that are associated with your system.

Step 2 Familiarize yourself with the requirements and limitations listed in this document. Ensure that your system meets all requirements, including network requirements, platform requirements, and software requirements.

Step 3 Run the pre-upgrade COP. It runs a series of tests and detects issues that can cause upgrade failures. Install the pre-upgrade COP file to check the upgrade readiness from the current version to the version you are upgrading to, and if you find any issues in the report, fix them before upgrading. This reduces the chances of an upgrade failure.

Step 4 Ensure that the software version you are upgrading from is running on a virtual machine. If your current deployment is running on MCS hardware, see the *Cisco Prime Collaboration Deployment Administration Guide* for information about how to migrate an existing cluster to a virtualized cluster.

Step 5 Export user records using the Bulk Administration Tool (BAT):

a) From Cisco Unified CM Administration, choose **Bulk Administration** > **Users** > **Export Users**.
b) Click **Find** to display all user records.
c) Click **Next**.
d) Enter a filename in the in the **File Name** text box and choose file format from the **File Format** drop-down list.
e) In the **Job Information** area, enter the Job description.
f) Click **Run Immediately** to export user records immediately
g) Click **Submit**.

h) To download the exported file, choose **Bulk Administration** > **Upload/Download Files**.
i) Enter search criteria for the file that you generated and click **Find**.
j) Select the check box that corresponds to the file that you want to download and click **Download Selected**.
k) In the File Download pop-up window, click **Save**.
l) 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.

Step 6 Use the Real-Time Monitoring Tool (RTMT) to verify that you have enough common partition space for the upgrade. 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. If you do not have enough space, perform one or more of the following steps to create enough space:

- For upgrades from 9.x and earlier, 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.

  Note If you are upgrading from Release 10.0(1) and above, you do not need to install the disk expansion Cisco Options Package (COP) file.

- 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*> > Unified Communications Manager/CallManager/Cisco Unity Connection Utilities**.

Caution Performing an upgrade without sufficient disk space can cause the system to fail.

Step 7 Download any upgrade COP files that are required. COP files are required for refresh upgrades only. To determine which COP files you need, see the information about COP files and supported upgrade paths listed in the Related Topics section below.

Step 8 Ensure that you have the necessary license files for the new release.

Step 9 Ensure that there are no expired certificates on the partition, including any trust certificates in the certificate chain.

Perform this step for refresh upgrades on IM and Presence Service nodes only. Expired certificates are not imported during a refresh upgrade. As a result, a new certificate is generated during upgrade process and can cause errors.

Step 10 Back up your system, ensuring 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.

For more information, see the *Administration Guide for Cisco Unified Communications Manager*

Step 11 If you are upgrading from Release 9.x or earlier, you must disable extension mobility before you begin the upgrade process.

a) From Cisco Unified Serviceability, choose **Tools** > **Service Activation**.
b) From the **Server** list, choose the node on which you want to deactivate services and click **Go**.
c) Deselect the **Cisco Extension Mobility** services.
d) Click **Stop**.
e) Repeat Steps B through D for each node that is running **Cisco Extension Mobility** services.
f) 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.

Note that when you deactivate the Cisco Extension Mobility service, Cisco Extension Mobility users cannot log in and log out of phones that support Cisco Extension Mobility.

Step 12 Perform these additional tasks when you upgrade Cisco Unified Communications Manager:

a) If you have special characters in your Cisco Unified Communications Manager default administrative password, when you upgrade from releases 8.x or 9.x, the connection between IM and Presence Service and Cisco Unified Communications Manager fails. Before you upgrade from an 8.x or 9.x release, you must change your password so that all special characters are removed.
b) Use the **utils dbreplication setrepltimeout** CLI command to increase the database replication timeout value when upgrading large clusters so that more Cisco Unified Communications Manager subscriber nodes have sufficient time to request replication. When the timer expires, the first Cisco Unified Communications Manager subscriber node, plus all other Cisco Unified Communications Manager subscriber nodes that requested replication within that time period, begin a batch data replication with the Cisco Unified Communications Manager database publisher node. The default database replication timeout value is 300 (5 minutes). Restore the timeout to the default value after the entire cluster upgrades and the Cisco Unified Communications Manager subscriber nodes have successfully set up replication. For more information, see the *Command Line Interface Guide for Cisco Unified Communications Solutions*.
c) 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.
d) Ensure that the IP subnet mask of the device is set using the following format:255.255.255.0. You can change the subnet mask by executing the **set network ip eth0 <server_IP_address> 255.255.255.0** command.
e) Before you upgrade a Cisco Unified Communications Manager cluster, execute the **utils network ipv6 ping** CLI command to verify IPv6 networking on the first node (Cisco Unified Communications Manager database publisher node) and Cisco Unified Communications Manager subscriber nodes. If IPv6 is configured incorrectly on the Cisco Unified Communications Manager subscriber nodes, load detection may take 20 minutes.
f) Apply all pre-9.0 licenses to Cisco Unified Communications Manager before you upgrade to Release 9.0 or later software. After you upgrade to Release 9.0 or later software, you cannot apply these licenses to Cisco Unified Communications Manager and you cannot apply them using the Cisco Prime License Manager. Ensure that you install all unused licenses or Product Authorization Keys (PAKs) before you upgrade the system. The Cisco Unified Communications Manager displays a warning to prompt you to install any unused licenses before proceeding.

Step 13 Perform these additional tasks when you upgrade the IM and Presence Service:

a) Disable High Availability on the IM and Presence presence redundancy group. Select **Cisco Unified CM Administration** > **System** > **Presence Redundancy Group.**

   For more information, see the *Deployment Guide for IM and Presence Service on Cisco Unified Communications Manager*.

b) If you need to upgrade Cisco Unified Communications Manager as part of your IM and Presence upgrade, you must stop and restart the IM and Presence Sync Agent service. To restart the Sync Agent service,

navigate to Cisco Unified IM and Presence Serviceability and select **Tools** > **Control Center - Network Services**.

c) Check that the IM and Presence Service node has connectivity with Cisco Unified Communications Manager.

You can use the Cisco Unified CM IM and Presence Administration System Troubleshooter to check node connectivity.

Step 14 Add a serial port to the virtual machine so that you can dump logs in the event of an upgrade failure.

a) Power off the virtual machine.
b) 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.
c) Attach the serial port to a .tmp file.
d) Power on the virtual machine and proceed with the upgrade.

After you successfully upgrade the system, follow the procedure to Remove the Serial Port, on page 53. In the event of an upgrade failure, refer to Dump a Log File After an Upgrade Failure, on page 65.

Related Topics

Requirements and Limitations, on page 3
Supported Upgrade Paths, on page 9
Change Virtual Machine Configuration Specifications, on page 38
Upgrade vSphere ESXi, on page 39
COP Files, on page 18
Obtain Upgrade File, on page 40

Change Virtual Machine Configuration Specifications

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

Caution If you need to change the vNIC, you must change it after the upgrade is complete.

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 http://www.cisco.com/go/uc-virtualized and search on the topic "Implementing Virtualization Deployments." .

Procedure

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

For more information about performing a backup, see the *Cisco Unified Communications Manager Disaster Recovery Administration Guide*.

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 (Red Hat Enterprise Linux 6 (64-bit).

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 disk size using vDisk. 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.

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

Step 5 Upgrade the software to the latest version.

Step 6 Modify the Network Adapter to use the VMXNET 3 Adapter type.

For information about modifying the Network Adapter to meet the requirements of this release, see the Readme file for the OVA template.

Step 7 Power on the virtual machine.

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.

Obtain Upgrade File

Before you begin the upgrade process, you must obtain the appropriate upgrade file from Cisco.com.

For more information, see the *Cisco Unified Communications Manager Release Notes*.

You can access the upgrade file during the installation process from either a local DVD or from a remote FTP or SFTP server. Be aware that directory names and filenames that you enter to access the upgrade file are case-sensitive.

Increase the Virtual Disk Size

Follow this procedure if you require extra temporary disk space in your VM for an upgrade or for disk logging activity. You can perform these steps while your system is running, but you must reboot your system for the increased disk size to take effect.

Note You can only increase your common partition; you cannot decrease it.

Before you begin

Perform a backup of your system.

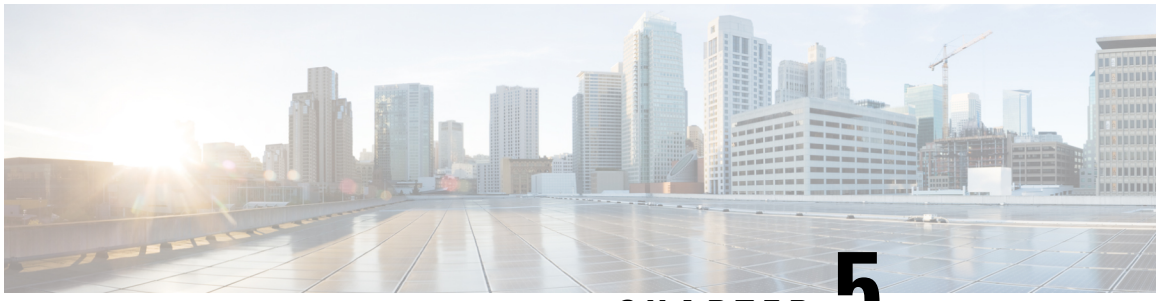
Remove your Virtual Machine (VM) snapshots. Otherwise, the increase disk size option is greyed out. See Working with Snapshots.

Procedure

Step 1 Open the VMware Infrastructure (VI) client and connect to VirtualCenter or the ESX host.

Step 2 Edit the virtual disk settings to increase the storage size. For information about how to configure this setting, see the VMWare documentation.

Step 3 From the CLI, reboot your system with the **utils system restart** command.



CHAPTER 5

Upgrade Tasks

This section contains the procedures for performing an upgrade.

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 reinstall any nodes in the cluster during the upgrade process. You can make configuration changes only when you have completed the upgrade on all nodes and performed the 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 nodes and all IM and Presence Service Service nodes.

Caution 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.

Note If you use RTMT as a monitoring tool and have a mega cluster deployment, Cisco recommends high-availability setup for RTMT to avoid any connectivity loss during Simple Upgrade. Following are the steps to setup high availability for RTMT Monitoring:

1. Login to CM Administration page.
2. Click System → Service Parameter.
3. Select any Unified Communications Manager node from server drop down.
4. Select Cisco AMC Service from Service drop down.
5. Select Primary Collector as any Subscriber node.
6. Select Failover Collector as any Subscriber node other than the node that is selected as Primary collector and then click Save.
7. Connect RTMT to any Subscriber.

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

Note The system checks for any existing phone service URLs during upgrade and automatically appends "**&EMCC=#EMCC#**" if it does not find any phone service URLs. As a result, any phones that do not support EMCC may encounter issues trying to login to Extension Mobility. The appended "**&EMCC=#EMCC#**" can be removed after upgrade if Unified Communications Manager contains any legacy or third-party devices which does not support EMCC

Upgrade the Applications

Related Topics

Upgrade from a Local Source, on page 42
Upgrade from a Remote Source, on page 44

Upgrade from a Local Source

Follow this procedure to upgrade to a new release of Unified Communications Manager or the IM and Presence Service Service from a local source.

Before you begin

Ensure that you have the correct ISO file for the upgrade. Upgrade files use the following naming convention:

- UCSInstall_CUP_<XXXXXXXX>.sgn.iso
- UCSInstall_UCOS_<XXXXXXXX>.sgn.iso
- Export unrestricted software has a XU license SKU.
- Export restricted software has a K9 license SKU.

Procedure

Step 1 Ensure that you can access the upgrade file. Choose one of the following options:

- Insert the CD or DVD into the disc drive on the local server that is to be upgraded.
- Create a data store ISO file on the local ESXi host.
- Create a data store ISO file on a storage area network (SAN) that is connected to the ESXi host.

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

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

Step 3 If you are performing a refresh upgrade that requires a COP file, install the required COP file.

If you are unsure whether you have to install a COP file, review the information about supported upgrade paths. See the Related Topics section for more information.

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

Step 5 Select **DVD/CD** from the **Source** list, or edit the virtual machine to map to the ISO file.

Step 6 In the **Directory** field, enter the path to the location of the patch file. If the file is in the root directory, enter a slash (/).

Step 7 Enter your email address and IP address in the **Email Notification** and **SMTP Server** fields. This option enables you to receive an email notification upon successful completion of the upgrade.

Note These fields are only visible for refresh upgrades.

Step 8 Select **Next** to continue the upgrade process.

Step 9 Select the upgrade version that you want to install and select **Next**.

Step 10 Monitor the progress of the download, which includes the filename and the number of megabytes that are being transferred.

Step 11 When the download completes, verify the checksum value against the checksum for the file that you downloaded from Cisco.com.

Step 12 Perform one of the following actions:

For standard upgrades:

- For a single-node deployment, if you want to install the upgrade and automatically reboot to the upgraded software, select **Reboot to upgraded partition.**

- For a multinode deployment, select **Do not reboot after upgrade**. This option allows you to install the upgrade and later manually reboot to the upgraded software. For more information about how to manually reboot the system and activate the upgrade, see the Related Topics section.

For refresh upgrades:

- Select **Do not switch to new version after upgrade** only if you perform a staged upgrade.
- Select **Switch to new version after upgrade** to remain on the new active software version.

Note For more information about the rules for switching during an upgrade, see *Version Switching during upgrade rules*.

Step 13 Select **Next**.

Step 14 Select **Finish** when the installation completes.

Related Topics

Upgrade Paths For Cisco Unified Communications Manager, on page 10
Upgrade Paths for IM and Presence Service, on page 11
Version Switching, on page 46

Upgrade from a Remote Source

Follow this procedure to upgrade to a new release of Cisco Unified Communications Manager or the IM and Presence Service Service using software from a network drive or remote node. The network drive or remote node must run an SFTP/FTP server that is accessed by each node that you want to upgrade.

Before you begin

Ensure that you have the correct ISO file for the upgrade. Upgrade files use the following naming convention:

- UCSInstall_CUP_<XXXXXXXX>.sgn.iso
- UCSInstall_UCOS_<XXXXXXXX>.sgn.iso
- Export unrestricted software has a XU license SKU.
- Export restricted software has a K9 license SKU.

Procedure

Step 1 Ensure that you can access the FTP/SFTP server where you stored the upgrade file.

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

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

Step 3 If you are performing a refresh upgrade that requires a COP file, install the required COP file.

If you are unsure whether you have to install a COP file, review the information about supported upgrade paths. See the Related Topics section for more information.

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

Step 5 Select **Remote Filesystem** from the **Source** list.

Step 6 In the **Directory** field, enter the path to the patch file on the remote system.

Step 7 In the **Server** field, enter the FTP or SFTP server name.

Step 8 In the **User Name** field, enter the username for the remote node.

Step 9 In the **User Password** field, enter the password for the remote node.

Step 10 Enter your email address and IP address in the **Email Notification** and **SMTP Server** fields. This option enables you to receive an email notification upon successful completion of the upgrade.

Note These fields are only visible for refresh upgrades.

Step 11 From the **Transfer Protocol** field, select the transfer protocol, for example, SFTP.

Step 12 Select **Next** to continue the upgrade process.

Step 13 Select the upgrade version that you want to install and select **Next**.

Step 14 When the download completes, verify the checksum value against the checksum for the file that you downloaded from Cisco.com.

Step 15 Perform one of the following actions:

For standard upgrades:

- If this is a single-node deployment and you want to install the upgrade and automatically reboot to the upgraded software, select **Reboot to upgraded partition.**
- If this is a multinode deployment, select **Do not reboot after upgrade.**This option allows you to install the upgrade and then manually reboot to the upgraded software later. For more information about how to manually reboot the system and activate the upgrade, see the Related Topics section.

For refresh upgrades:

- Select **Do not switch to new version after upgrade** only if you are performing a staged upgrade.
- Select **Switch to new version after upgrade** to remain on the new active software version.

Note See the topic called *Version switching during upgrade rules* for more information about the rules for switching during an upgrade.

Step 16 Select **Next**.

Step 17 Select **Finish** when the installation completes.

Related Topics

Upgrade Paths For Cisco Unified Communications Manager, on page 10
Upgrade Paths for IM and Presence Service, on page 11
Version Switching, on page 46

Version Switching

A number of rules apply when you are manually switching versions and when you switch versions during an upgrade. The table below outlines the version switching rules for activating the release 10.x software version and for switching back to a previous software version.

Note You cannot switch the version of any node if doing so violates the version matching requirements. This rule applies whether you are switching forward to a new software version, or switching back to a previous software version.

Product	Node type	Switch from	Switch to	Switching rule
Activate the new software version				
Unified CM	Publisher	8.x or 9.x	11.x	You must switch the software version on the publisher node before you switch the software version on subscriber nodes.
		10.x	11.x	
Unified CM	Subscriber	8.x or 9.x	11.x	Supported when the publisher node has been switched to the new version. The software version you are switching to must match the version number of the active partition on the Unified Communications Manager publisher node.
		10.x	11.x	
IM and Presence	Database publisher	8.x or 9.x	11.x	Supported when the software version you are switching to matches the major and minor version number of active partition on theUnified Communications Manager publisher node.
		10.x	11.x	
IM and Presence	Subscriber	8.x or 9.x	11.x	Supported when the software version of this node matches the five version numbers of the IM and Presence Service database publisher node.
		10.x	11.x	
Switch back to a previous software version				
Unified CM	Publisher	11.x	8.x or 9.x	Supported. You must switch the software version on the publisher node before you switch the software version on subscriber nodes.
		11.y	10.x	

Product	Node type	Switch from	Switch to	Switching rule
Unified CM	Subscriber	11.x	8.x or 9.x	Supported when the Unified Communications Manager publisher node has been switched to the previous version. The software version you are switching to must match the version number of the active partition on the Unified Communications Manager publisher node. You cannot switch a subscriber node to a previous version when the publisher node is running new version.
		11.y	10.x	
IM and Presence	Database publisher	11.x	8.x or 9.x	Not supported when the Unified Communications Manager publisher node is running a software version that is newer than the one that you are switching back to. Switching the IM and Presence Service database publisher node to a previous release after the Unified Communications Manager has been upgraded to a newer release violates the version matching requirements. Switching back to a previous release is supported only when the software version you are switching to matches the major and minor version number of active partition on the Unified Communications Manager publisher node.
		11.y	10.x	
IM and Presence	Subscriber	11.x	8.x or 9.x	Not supported when the IM and Presence Service database publisher node is running a software version that is newer than the one that you are switching back to. Switching back to a previous release is supported only when the software version of this node matches the five version numbers of the IM and Presence Service database publisher node.
		11.y	10.x	

Product	Node Type	Switch from	Switch to	Switching Rule
Activate the new software version				
Unified CM	Publisher	10.x or 11.x or 12.y	12.x	You must switch the software version on the publisher node before you switch the software version on subscriber nodes.

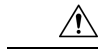
Product	Node Type	Switch from	Switch to	Switching Rule
Unified CM	Subscriber	10.x or 11.x or 12.y	12.x	Supported when the publisher node has been switched to the new version. The software version you are switching to must match the version number of the active partition on the Unified Communications Manager publisher node.
IM and Presence	Database publisher	10.x or 11.x or 12.y	12.x	Supported when the software version you are switching to matches the major and minor version number of active partition on the Unified Communications Manager publisher node.
IM and Presence	Subscriber	10.x or 11.x or 12.y	12.x	Supported when the software version of this node matches the five version numbers of the IM and Presence Service database publisher node.
Switch back to a previous software version				
Unified CM	Publisher	12.x	10.x or 11.x or 12.y	Supported. You must switch the software version on the publisher node before you switch the software version on subscriber nodes.
Unified CM	Subscriber	12.x	10.x or 11.x or 12.y	Supported when the Unified Communications Manager publisher node has been switched to the previous version. The software version you are switching to must match the version number of the active partition on the Unified Communications Manager publisher node. You cannot switch a subscriber node to a previous version when the publisher node is running new version.
IM and Presence	Database publisher	12.x	10.x or 11.x or 12.y	Switching back to a previous release is supported only when the software version you are switching to matches the major and minor version number of active partition on the Unified Communications Manager publisher
IM and Presence	Subscriber	12.x	10.x or 11.x or 12.y	Switching back to a previous release is supported only when the software version of this node matches the five version numbers of the IM and Presence Service database publisher node.node.

Switch the Software Version

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

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

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



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

Before you begin

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

Procedure

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

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

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

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

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

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

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

Switch to Previous Version

If you need to revert to the software version that was running before the upgrade, you can do so by using the Switch Version option to switch the system to the software version on the inactive partition.

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.

Related Topics

Switch the Software Version, on page 49

Switch Node to Previous Version

Procedure

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

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

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

The Version Settings window displays.

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

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

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

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

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

The Version Settings window displays.

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

d) Verify that all activated services are running.

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

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

Reset Database Replication

If you switch back the servers in a cluster to run an older product release, you must manually reset database replication within the cluster. To reset database replication after you revert all the cluster servers to the older product release, enter the CLI command **utils dbreplication reset all** on the publisher server.

When you switch versions by using Cisco Unified Communications Operating System Administration or the CLI, you get a message that reminds you about the requirement to reset database replication if you are reverting to an older product release.

Switch version back to Cisco Unified Presence 8.6(3) or earlier

Cisco Unified Presence releases 8.6(4) and later do not support the Cisco Presence Engine database. If you upgrade from Release 8.6(3) or earlier and you subsequently want to revert to the previous release, you must install a COP file that will reinstall the Cisco Presence Engine database. The COP filename is `ciscocm.cup.pe_db_install.cop` and you can download it from Cisco.com.

Note In a multinode environment, you must install the COP file on every node in the cluster after you switch versions from Cisco Unified Presence Release 8.6(4) or later.

In this release, you cannot downgrade to a version earlier than Release 8.6(3).

Note You must restart the system after you install the COP file.

Before you begin

Switch versions on Unified Communications Manager.

Procedure

Step 1 Download the following COP file from Cisco.com: `ciscocm.cup.pe_db_install.cop`.

Step 2 Sign in to Cisco Unified IM and Presence Operating System Administration.

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

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

Note This procedure only applies if you want to switch from Release 9.0 or later back to a release earlier than 8.6(4).

Step 5 Select **Switch Versions** to switch back to the earlier release and restart the system.

Step 6 After the system has restarted, install the COP file.

Note In a multinode environment, you must install the COP file on every node in the cluster.

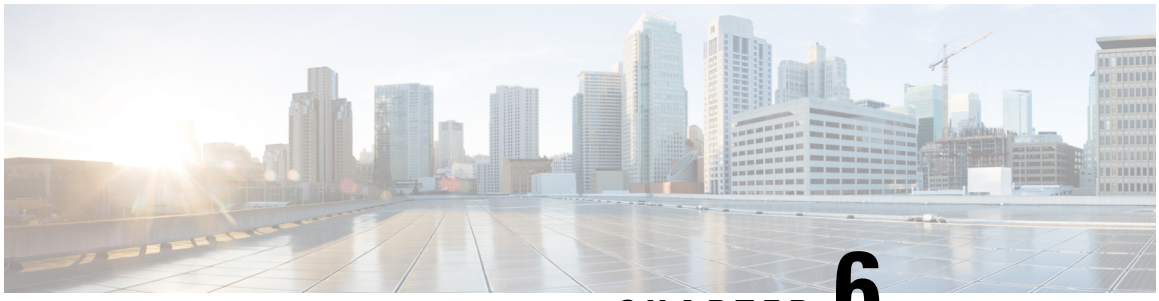
Step 7 After you have installed the COP file, manually restart the system. To do this, select **Settings** > **Version** and select **Restart**.

Step 8 Run the following CLI command (on the publisher or subscriber node) to check if the database replication is active on the node: `utils dbreplication runtimestate`

If database replication is active on all nodes, the output lists all the nodes and the replication setup value for each node is 2. If database replication is not complete (a value other than 2 is returned), core services will not start on the subscriber node until replication is complete.

Step 9 Select **Cisco Unified CM IM and Presence Administration** > **System** > **Notifications** to determine whether database replication is complete.

Step 10 If database replication cannot be established, use the following CLI command on the publisher node to reset replication: `utils dbreplication reset all`



CHAPTER 6

Post-Upgrade Tasks

The following sections provide information about the tasks that you must complete after you upgrade Cisco Unified Communications Manager nodes or IM and Presence nodes.

Post-Upgrade Tasks for All Nodes

This section describes post-upgrade tasks that you must perform for both Unified Communications Manager nodes and IM and Presence Service nodes.

Version Switching

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

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.

Ensure that you power off the VM before you edit the settings to remove the serial port. For information about how to edit the settings, see the VMWare documentation.

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.

Update VMWare Tools

You must update the VMWare Tools after you complete and upgrade. There are two options for updating the VMWare Tools:

- configure the tool to use the Automatic Tools Upgrade option
- configure the tool to automatically check the tools version during a VM power-on and upgrade the tools

For information about how to configure these options, see the VMWare documentation.

Locale Installation

You can configure Cisco Unified Communications Manager and IM and Presence Service to support multiple languages. There is no limit to the number of supported languages you can install.

Cisco provides locale-specific versions of the Cisco Unified Communications Manager Locale Installer and the IM and Presence Service Locale Installer on www.cisco.com. Installed by the system administrator, the locale installer allows the user to view/receive the chosen translated text or tones, if applicable, when a user works with supported interfaces.

After you upgrade Cisco Unified Communications Manager or the IM & Presence Service, you must reinstall all the locales. Install the latest version of the locales that match the major.minor version number of your Cisco Unified Communications Manager node or IM and Presence Service node.

Install locales after you have installed Cisco Unified Communications Manager on every node in the cluster and have set up the database. If you want to install specific locales on IM and Presence Service nodes, you must first install the Cisco Unified Communications Manager locale file for the same country on the Cisco Unified Communications Manager cluster.

Use the information in the following sections to install locales on Cisco Unified Communications Manager nodes and on IM and Presence Service nodes after you complete the software upgrade.

User Locales

User locale files contain language information for a specific language and country. They provide translated text and voice prompts, if available, for phone displays, user applications, and user web pages in the locale that the user chooses. These files use the following naming convention:.

- cm-locale-language-country-version.cop (Cisco Unified Communications Manager)

- ps-locale-language_country-version.cop (IM and Presence Service)

If your system requires user locales only, install them after you have installed the CUCM locale.

Network Locales

Network locale files provide country-specific files 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)

Cisco may combine multiple network locales in a single locale installer.

Note Virtualized deployments of Cisco Unified Communications Manager on Cisco-approved, customer-provided servers can support multiple locales. Installing multiple locale installers ensures that the user can choose from a multitude of locales.

You can install locale files from either a local or a remote source by using the same process for installing software upgrades. You can install more than one locale file on each node in the cluster. Changes do not take effect until you reboot every node in the cluster. Cisco strongly recommends that you do not reboot the nodes until you have installed all locales on all nodes in the cluster. Minimize call-processing interruptions by rebooting the nodes after regular business hours.

Install Locale Installer on Cisco Unified Communications Manager

User locale files provide translated text for user applications and user web pages in the locale that the user chooses. User locales are country-specific. Use the following procedure to install locales on the node. Optionally, you can follow the software upgrade procedure to install locale files from either a local or a remote source.

Before you begin

- Install Cisco Unified Communications Manager on every node in the cluster before you install the Cisco Unified Communications Manager Locale Installer.
- If you want to use a locale other than English, you must install the appropriate language installers on both Cisco Unified Communications Manager and on IM and Presence. Ensure the locale installer is installed on every node in the cluster (install on the Cisco Unified Communications Manager database publisher node before the subscriber nodes).
- User locales should not be set until all appropriate locale installers are loaded on both systems. Users may experience problems if they inadvertently set their user locale after the locale installer is loaded on Cisco Unified Communications Manager but before the locale installer is loaded on IM and Presence. If issues are reported, we recommend that you notify each user to sign into Cisco Unified Communications Manager user options pages and change their locale from the current setting to English and then back again to the appropriate language. You can also use the BAT tool to synchronize user locales to the appropriate language.
- You must restart the nodes for the changes to take effect. After you complete all locale installation procedures, restart each node in the cluster. Updates do not occur in the system until you restart all nodes in the cluster; services restart after the node reboots.

Procedure

Step 1 Download the locale installer from `www.cisco.com`.

Step 2 Click the version of the Cisco Unified Communications Manager Locale Installer.

Step 3 Click **Download** to download the installer file to the node.

Step 4 After downloading the file, save the file to the hard drive and note the location of the saved file.

Step 5 Double-click the file to begin the installation.

Step 6 Perform these actions to complete the installation:

a) Read and accept the license agreement, and then click **Next** to display the **Readme Notes** window.

Note The readme notes contain build-time information such as components and devices that are supported in the released build. The readme may be printed for reference.

b) Examine and accept the readme notes, and then click **Next**. The **Setup Type** window appears.

c) Select a custom setup type in the **Setup Type** window to allow you to select or deselect user locales as required, and then click **Next**. The **Start Copying Files** window appears.

d) Review the setup options, and then click **Next**. The **Ready to Install the Program** window appears.

a) Click **Install** to start the installation of the selected user locales.

Note The speed of installation depends on the performance of the node. It is estimated to take between two to ten minutes to complete the database update. Observe the progress bar and text above it to determine the status of installation.

Step 7 When the installation is complete, a new dialog requests confirmation of a restart. Should you wish to apply another locale installer, repeat this procedure before restarting the node in order to reduce downtime.

Step 8 Click **Finish**. The **Setup** dialog box displays. Do not click any buttons or press any keys.

Step 9 When the **Setup** dialog box automatically closes, you have completed the installation on the node. Install the Cisco Unified Communications Manager Locale Installer on every node in the cluster.

Step 10 After you complete all locale installation procedures, restart each node in the cluster.

Step 11 Verify that your users can select the locale(s) for supported products.

Troubleshooting Tip

Make sure that you install the same components on every node in the cluster.

What to do next

Install Locale Installer on IM and Presence Service, on page 56

Install Locale Installer on IM and Presence Service

Before you begin

- Install the Locale Installer on Cisco Unified Communications Manager. If you want to use a locale other than English, you must install the appropriate language installers on both Cisco Unified Communications Manager and on IM and Presence Service.

- If your IM and Presence Service cluster has more than one node, make sure that the locale installer is installed on every node in the cluster (install on the IM and Presence database publisher node before the subscriber nodes).
- User locales should not be set until all appropriate locale installers are loaded on both systems. Users may experience problems if they inadvertently set their user locale after the locale installer is loaded on Cisco Unified Communications Manager but before the locale installer is loaded on IM and Presence Service. If issues are reported, we recommend that you notify each user to sign into the Cisco Unified Communications Self Care Portal and change their locale from the current setting to English and then back again to the appropriate language. You can also use the BAT tool to synchronize user locales to the appropriate language.
- You must restart the server for the changes to take effect. After you complete all locale installation procedures, restart each server in the cluster. Updates do not occur in the system until you restart all servers in the cluster; services restart after the server reboots.

Procedure

Step 1 Navigate to `cisco.com` and choose the locale installer for your version of IM and Presence Service.

http://software.cisco.com/download/navigator.html?mdfid=285971059

Step 2 Click the version of the IM and Presence Locale Installer that is appropriate for your working environment.

Step 3 After downloading the file, save the file to the hard drive and note the location of the saved file.

Step 4 Copy this file to a server that supports SFTP.

Step 5 Sign into Cisco Unified IM and Presence Operating System Administration using the administrator account and password.

Step 6 Choose **Software Upgrades** > **Install/Upgrade**.

Step 7 Choose Remote File System as the software location source.

Step 8 Enter the file location, for example `/tmp`, in the Directory field.

Step 9 Enter the IM and Presence Service server name in the Server field.

Step 10 Enter your username and password credentials in the User Name and User Password fields.

Step 11 Choose SFTP for the Transfer Protocol.

Step 12 Click **Next**.

Step 13 Choose the IM and Presence Service locale installer from the list of search results.

Step 14 Click **Next** to load the installer file and validate it.

Step 15 After you complete the locale installation, restart each server in the cluster.

Step 16 The default setting for installed locales is "English, United States". While your IM and Presence Service node is restarting, change the language of your browser, if necessary, to match the locale of the installer that you have downloaded.

Step 17 Verify that your users can choose the locales for supported products.

Tip Make sure that you install the same components on every server in the cluster.

Error Messages

See the following table for a description of the messages that can occur during Locale Installer activation. If an error occurs, you can view the messages in the installation log.

Table 3: Locale Installer Error Messages and Descriptions

Message	Description
[LOCALE] File not found: <language>_<country>_user_locale.csv, the user locale has not been added to the database.	This error occurs when the system cannot locate the CSV file, which contains user locale information to add to the database. This indicates an error with the build process.
[LOCALE] File not found: <country>_network_locale.csv, the network locale has not been added to the database.	This error occurs when the system cannot locate the CSV file, which contains network locale information to add to the database. This indicates an error with the build process.
[LOCALE] Communications Manager CSV file installer installdb is not present or not executable.	This error occurs because a Unified Communications Manager application called installdb must be present; it reads information that is contained in a CSV file and applies it correctly to the Unified Communications Manager database. If this application is not found, it either was not installed with Unified Communications Manager (very unlikely), has been deleted (more likely), or the node does not have Unified Communications Manager installed (most likely). Installation of the locale terminates because locales do not work without the correct records that are held in the database.
[LOCALE] Could not create /usr/local/cm/application_locale /cmservices/ipma/com/cisco/ipma /client/locales/maDialogs_<ll>_<CC>.properties.Checksum. [LOCALE] Could not create /usr/local/cm/application_locale/cmservices/ipma/com/cisco/ipma/client/locales/maMessages_<ll>_<CC>.properties.Checksum. [LOCALE] Could not create /usr/local/cm/application_locale/cmservices/ipma/com/cisco/ipma/client/locales/maGlobalUI_<ll>_<CC>.properties.Checksum. [LOCALE] Could not create /usr/local/cm/application_locale/cmservices/ipma/LocaleMasterVersion.txt.Checksum.	These errors could occur when the system fails to create a checksum file; causes can include an absent Java executable, `/usr/local/thirdparty/java/j2sdk/jre/bin/java`, an absent or damaged Java archive file, `/usr/local/cm/jar/cmutil.jar`, or an absent or damaged Java class, com.cisco.ccm.util.Zipper. Even if these errors occur, the locale will continue to work correctly, with the exception of Unified Communications Manager Assistant, which cannot detect a change in localized Unified Communications Manager Assistant files.
[LOCALE] Could not find /usr/local/cm/application_locale/cmservices/ipma/LocaleMasterVersion.txt in order to update Unified CM Assistant locale information.	This error occurs when the file does not get found in the correct location, which is most likely due to an error in the build process.

Message	Description
[LOCALE] Addition of <RPM-file-name> to the Unified Communications Manager database has failed!	This error occurs because of the collective result of any failure that occurs when a locale is being installed; it indicates a terminal condition.

Supported Products

For a list of products that Cisco Unified Communications Manager Locale Installers support, see the Cisco IP Telephony Locale Installer for Cisco Unified Communications Manager, which is available at this URL:

`http://www.cisco.com/cgi-bin/tablebuild.pl/callmgr-locale-51`

Post-Upgrade Tasks for Cisco Unified Communications Manager Nodes

This section describes the post-upgrade tasks that you must perform for Cisco Unified Communication Manager nodes.

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).

Test Functionality

After the upgrade, perform the following tasks:

- Run the post-upgrade COP.

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

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

Dial Plan Installation

You can install dial plan files from either a local or a remote source by using the same process for installing software upgrades. See the *Upgrade Guide for Cisco Unified Communications Manager* for more information about upgrading from a local or remote source.

After you install the dial plan files on the system, log in to Cisco Unified CM Administration and then navigate to **Call Routing** > **Dial Plan Installer** to complete installing the dial plans.

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, 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

If you are upgrading from Unified Communications Manager release 6.1(5) or earlier, you must re-create your IPSec policies after the upgrade is complete. The configuration information for IPSec policies from release 6.1(5) and earlier will not be migrated as part of the upgrade process. For information about how to create IPSec policies, see the *Administration Guide for Cisco Unified Communications Manager*.

Assign New Roles to Deprecated InterCluster Peer-User and Admin-CUMA

The application user group roles InterCluster Peer-User and Admin-CUMA are deprecated from release 10.0(1) onward. Any application users with these roles configured in releases 8.x or 9.x have the roles removed during an upgrade to any 10.x release. After the upgrade the administrator must configure appropriate roles for these users.

Note For intercluster to function correctly, the AXL user defined on the IM and Presence Service user interface (**Presence** > **Inter-Clustering**) must have a Standard AXL API Access role associated with it on the Cisco Unified Communications Manager application user page.

Post-Upgrade Tasks for IM and Presence Nodes

This section describes the post-upgrade tasks for the IM and Presence Service.

Verify IM and Presence Service Data Migration

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

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

Description: Migrated Service Profile Number x

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

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

Procedure

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

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

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

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

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

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

What to do next

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

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

Enable High Availability on Presence Redundancy Groups

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

Procedure

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

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

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

Step 4 Click **Save**.

Step 5 Repeat this procedure in each Presence Redundancy Group.

Restart the IM and Presence Sync Agent

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

Procedure

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

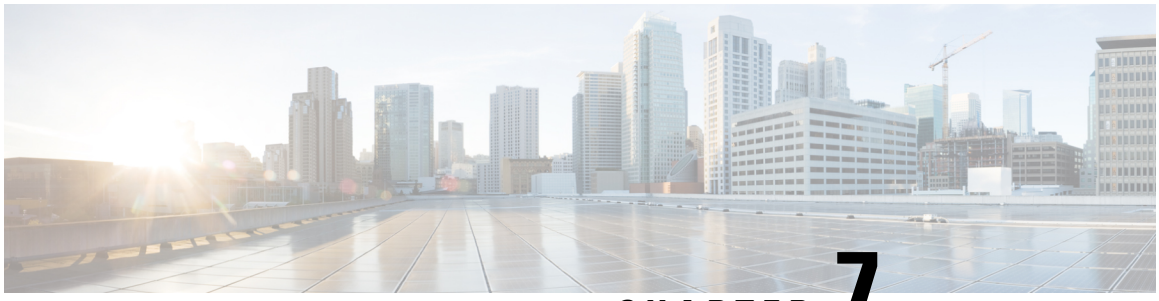
Step 2 Select an IM and Presence Service node from the **Server** drop-down list and click **Go**.

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

Example

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

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



CHAPTER 7

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 IM and Presence Service.

Before you begin

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

Procedure

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

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

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

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

Step 4 Select the datastore where you created the file.

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

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

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

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

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

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

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

Troubleshooting Unified Communications Manager Upgrades

This section provides information about 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.

Reboot include on upgrade Success/Failed/Cancel case

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

Solution: Reboot is required in the following scenarios:

1. Any upgrade (Legacy upgrade/Simple upgrade or Upgrade via PCD) get success or failure:
    - When an L2 upgrade fails, a reboot is required only in case when an upgrade is required again.
    - After a successful L2 upgrade, if you do not wish to switch to the new version and would like to upgrade again, you need to reboot the node first before starting the upgrade.

- When an RU upgrade fails, it automatically switches to old partition and an automatic reboot is performed (if upgrade status is failed, cancel the upgrade and reboot the node).

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

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**.

Download Failure in Cluster-Wide Upgrade

While performing a cluster-wide upgrade that includes both Unified Communications Manager and IM and Presence Service nodes, and download of the image fails in any of the Unified Communications Manager or IM and Presence Service nodes, follow this process:

Procedure

Step 1 Download the build manually on the failed node.

Step 2 Log into Cisco Unified Operating System Administration, choose the **Software Upgrades** > **Install/Upgrade Cluster**.

Step 3 Select the local Filesystem option to get the existing image and proceed further.

Step 4 If you are performing the upgrade at Command Line Interface, run the `utils system upgrade initiate` CLI command and select the `Local Image` option.

You do not need to download the image again.

Reduced Permissions for Access Control Groups

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

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

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

Loss of Phone Settings

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

Post-Upgrade Failure of Unified Communications Manager Publisher Node

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

Solution Do one of the following:

- restore the Unified Communications Manager publisher node use a DRS backup file
- if you do not have a DRS backup file, you must reinstall the entire cluster, including any IM and Presence Service nodes

Post-Upgrade Failure of Unified Communications Manager Subscriber Nodes

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

Solution Do one of the following:

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

Troubleshooting IM and Presence Upgrades

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

Upgrade Failure of IM and Presence Database Publisher Node

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

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

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

Upgrade Failure of IM and Presence Subscriber Node

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

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

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

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

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

Real-Time Monitoring Tool alert for Cisco SIP proxy service

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

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

Cannot find upgrade file on remote server

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

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

Upgrade file checksum values do not match

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

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

Database replication did not complete

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

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

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

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

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

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

Switch Version on Cisco IM and Presence Node Fails

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

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

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

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

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 IM and Presence Service server before you attempt another upgrade.

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

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

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

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

Common Partition Full Upgrade Failure

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

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