Upgrade and Migration Guide for Cisco Unified Communications Manager and IM and Presence Service, Release 11.5(1)

First Published: 2017-01-23

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

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

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

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

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

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

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

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: http://www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

© 2017 Cisco Systems, Inc. All rights reserved.

CONTENTS

Preface — **Preface** xi

Purpose xi

Audience xi

Related Documentation xi

Conventions xii

Obtain Documentation and Submit Service Requests xiii

Cisco Product Security Overview xiv

CHAPTER 1 — **How to Use this Guide** 1

How to Use this Guide 1

PART I — **Understanding Upgrades and Migrations** 3

CHAPTER 2 — **Understanding Upgrades and Migrations** 5

Upgrade and Migration Overview 5

Upgrade Methods 5

Direct Upgrades 5

Standard upgrades 6

Refresh upgrades 6

Migrations 7

Upgrade and Migration Tools 7

Export Restricted and Export Unrestricted Software 7

PART II — **Plan the Upgrade or Migration** 11

CHAPTER 3 — **Determine the Scope of Work** 13

Determine the Scope of the Upgrade or Migration 13

CHAPTER 4 Requirements and Limitations 15

Requirements and Limitations 15
Hardware 15
Network Requirements 16
IP Address Requirements 16
DNS requirements 16
SFTP Server Support 17
Virtual Machine Configuration 17
Browser Requirements 18
Licensing 19
Cisco Unified Communications Manager License Requirements 19
IM and Presence license requirements 19
Limitations 20
Subnet Limitations 20
Cluster Size 20
IP Subnet Mask 20
Support for Intercluster Peers 20
Device Name for Cisco Unified Mobile Communicator 21
Deprecated Phone Models 21
OS Admin Account Required for CLI-Initiated IM and Presence Upgrades 22

CHAPTER 5 Supported Upgrade Paths 23

Version Requirements 23
Supported Upgrade and Migration Paths 23
Applications Installed on Cisco Media Convergence Servers Hardware 24
Applications Installed on Virtual Machines 25

CHAPTER 6 Deployment Types and Recommendations 27

Type of Deployment 27
Business Edition 6000 and Business Edition 7000 Deployments 27
Virtualized Deployments of Cisco Unified Communications Manager and IM and Presence Service 27

CHAPTER 7 Sequencing Rules and Time Requirements 29

Upgrade Sequence and Time Requirements 29
Recommended Sequence for the Least Time 29
Recommended Sequence for the Least Impact 31
Sequence Rules 34
Upgrade time requirements 35
Factors that Affect Upgrade Time Requirements 35
Estimating the Minimum Time Requirements 37
Examples 39
Example: Time Requirements for a Standard Upgrade in the Least Time 39
Example: Time Requirements for a Refresh Upgrade in the Least Time 40
Example: Time Requirements for a Standard Upgrade with the Least Impact 41
Example: Time Requirements for a Refresh Upgrade with the Least Impact 43

CHAPTER 8 Find all Required Upgrade Documentation 45
Upgrade Documentation 45

PART III Change the Virtualization Software 49

CHAPTER 9 Change the Virtualization Software 51
Virtual Machine Configuration Tasks 51
Install and Configure VMware vCenter 52
Upgrade vSphere ESXi 52
Download and Install OVA Templates 53
Change Virtual Machine Configuration Specifications 54
Migrate From Single to Multi-vDisk Virtual Machine 55

PART IV Upgrade the Applications 57

CHAPTER 10 Pre-upgrade Tasks 59
Pre-Upgrade Task Flow 59
Generate a Database Status Report 64
Check Database Replication 64
Check Performance Reports 65
Run CLI Diagnostics 66
Delete a Trust Certificate 66

Regenerate a Certificate 67
Certificate Names and Descriptions 67
Take a Fresh Backup 68
Back Up Custom Ringtones and Background Images 69
Check Network Connectivity 69
Verify IPv6 Networking 70
Check Connectivity between IM and Presence and Cisco Unified Communications Manager 70
Collect Configuration and Login Information 71
Record the Registered Device Count 71
Record the Number of Assigned Users 72
Record TFTP Parameters 72
Record Enterprise Parameters 73
Export User Records 73
Upgrade IP Phone Firmware 74
Verify Critical Services 75
Deactivate Cisco Extension Mobility and TFTP Services 75
Stop the IM and Presence Sync Agent 76
Check the Available Common Partition Space 76
Adjust High and Low Watermarks 76
Create Additional Partition Space 77
Obtain Upgrade Files 78
COP Files Required for Upgrades to Release 11.5(1) 78
Increase the Database Replication Timeout 80
Disable High Availability on Presence Redundancy Groups 80
Add a Serial Port to the Virtual Machine 81

CHAPTER 11 **Upgrade Procedures** 83
Upgrade Overview 83
Publisher Nodes and Subscriber Nodes 83
Understanding Version Switching 84
Before You Begin 86
Upgrade Task Flow 86
Upgrade the Applications 87
Upgrade From a Local Source 87

Upgrade From a Remote Source 89
Version Switching 90
Switch the Software Version 90
Switch to Previous Version 91
Switch Cluster to Previous Version 91
Switch Node to Previous Version 91
Reset Database Replication 92
Switch version back to Cisco Unified Presence 8.6(3) or earlier 92
Verify that Database Replication is Functioning 93
Verify that Database Replication is Complete 94

CHAPTER 12 Post-upgrade Tasks 95
Post-upgrade Task Flow 95
Switch the Software Version 97
Remove the Serial Port 98
Restart Extension Mobility and TFTP Services 98
Reset TFTP Parameters 99
Restore Enterprise Parameters 99
Reset High and Low Watermarks 100
Update VMWare Tools 100
Install Locales 101
Restore the Database Replication Timeout 102
Verify the Registered Device Count 103
Verify Assigned Users 103
Test Functionality 103
Upgrade RTMT 104
Manage TFTP Server Files 105
Set Up a Custom Log-On Message 106
Configure IPSec Policies 107
Assign New Manager Assistant Roles 107
Verify IM and Presence Service Data Migration 108
Enable High Availability on Presence Redundancy Groups 108
Restart the IM and Presence Sync Agent 109

PART V Troubleshooting 111

CHAPTER 13 Troubleshooting 113

Dump a Log File After an Upgrade Failure 113

Troubleshooting Unified Communications Manager Upgrades 114

Upgrade Failure 114

Upgrade Fails with Insufficient Disk Space 114

Reduced Permissions for Access Control Groups 115

Loss of Phone Settings 115

Post-Upgrade Failure of Unified Communications Manager Publisher Node 116

Post-Upgrade Failure of Unified Communications Manager Subscriber Nodes 116

Troubleshooting IM and Presence Upgrades 116

Upgrade Failure of IM and Presence Database Publisher Node 116

Upgrade Failure of IM and Presence Subscriber Node 117

Upgrade From Pre Release 8.6(4) Fails 117

IM and Presence user phone presence problems 118

Presence User Experiences Issues Obtaining Availability 118

Real-Time Monitoring Tool alert for Cisco SIP proxy service 118

Cannot find upgrade file on remote server 118

Upgrade file checksum values do not match 118

Database replication did not complete 119

Cisco UP Presence Engine database does not restart 119

Version Errors 119

Failed refresh upgrade 120

Cancelled or failed upgrade 120

Directory Was Located and Searched but No Valid Options or Upgrades Were Available 120

Common Partition Full Upgrade Failure 121

PART VI Appendix 123

CHAPTER 14 Frequently Asked Questions 125

Frequently Asked Questions 125

CHAPTER 15 Upgrading from Legacy Releases 129

Upgrading and Migrating from Legacy Releases 129

CHAPTER 16 Additional Upgrade Resources 133

Additional Upgrade Resources 133

Preface

- Purpose, page xi
- Audience, page xi
- Related Documentation, page xi
- Conventions, page xii
- Obtain Documentation and Submit Service Requests, page xiii
- Cisco Product Security Overview, page xiv

Purpose

This document provides information about upgrading software.

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 Cisco Unified Communications Manager

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*

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

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

- *Replacing a Single Server or Cluster for Cisco 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 Cisco Unified Communications Manager server or a cluster of servers.

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

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

  This document describes the Command Line Interface for Cisco 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 Cisco Unified Communications Manager Documentation Guide for your release at

http://cisco.com/en/US/products/sw/voicesw/ps556/products_documentation_roadmaps_list.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

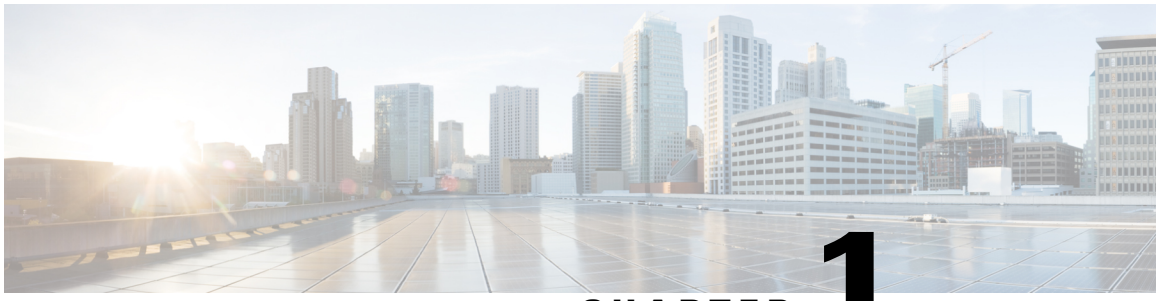
Subscribe to the *What's New in Cisco Product Documentation* as an RSS feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service. Cisco currently supports RSS Version 2.0.

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

How to Use this Guide

- How to Use this Guide, page 1

How to Use this Guide

This guide is the starting point for all upgrades and migrations to a new release of Cisco Unified Communications Manager or IM and Presence Service. The table below outlines how to use this guide to plan and then perform an upgrade or migration.

Procedure

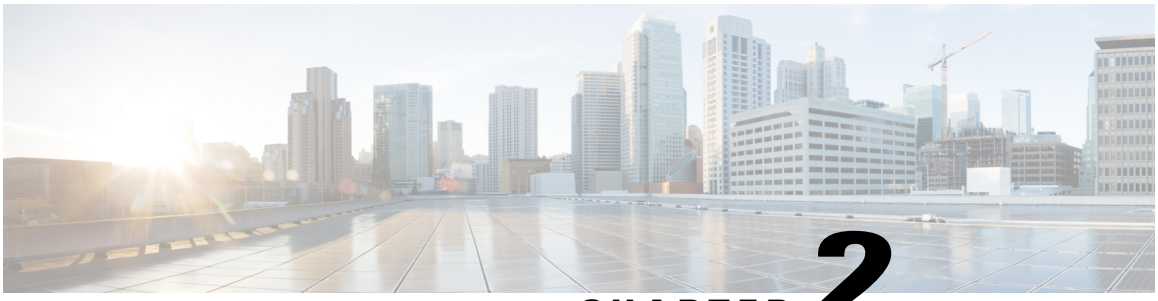
	Command or Action	Purpose
Step 1	Understanding Upgrades and Migrations, on page 3	Use the information in this section to understand: • the differences between an upgrade and a migration • the upgrade methods that are available to you • the differences between export restricted and unrestricted software
Step 2	Plan the Upgrade or Migration, on page 11	Use the information in this section to plan your upgrade or migration: • determine the scope of the upgrade; for example, determine whether you need to upgrade your hardware or your virtual environment to meet the requirements of the new release • understand the system requirements and limitations • verify that your upgrade path is supported • review the deployment types and recommendations to see which upgrade or migration method we recommend for you • if we recommend that you perform a direct upgrade, determine the sequence in which you should perform upgrade procedures in order to balance the time required for the upgrade and the impact on your network

	Command or Action	Purpose
		• gather the documentation that you need to complete the upgrade or migration
Step 3	Change the Virtualization Software, on page 49	Use the information in this section to download and install OVA templates and to upgrade your virtual environment, if needed.
Step 4	Upgrade the Applications, on page 57	Use the information in this section when you are ready to begin to upgrade or migrate the Cisco Unified Communications Manager and the IM and Presence applications. • Complete the pre-upgrade tasks in this section that are identified for the type or upgrade or migration that you are doing. • After you complete the pre-upgrade tasks, perform the upgrade or migration using the method and the documentation that you identified during the planning stage. For example, if you are performing a direct upgrade using the Cisco Unified CM OS Admin interface, follow the procedures in this guide. If you are performing a direct upgrade or a migration using Cisco Prime Collaboration Deployment (PCD), follow the procedures in the PCD documentation. • Complete the post-upgrade tasks in this section for all upgrade and migration methods.
Step 5	Troubleshooting, on page 111	Use the information in this section to troubleshoot problems that occur during the upgrade process.
Step 6	Appendix, on page 123	Use the information in this section to: • review frequently asked questions • find out how to upgrade or migrate from a legacy release • find additional resources to help with the upgrade or migration process

PART I

Understanding Upgrades and Migrations

- Understanding Upgrades and Migrations, page 5



CHAPTER 2

Understanding Upgrades and Migrations

- Upgrade and Migration Overview, page 5
- Upgrade Methods, page 5
- Upgrade and Migration Tools, page 7
- Export Restricted and Export Unrestricted Software, page 7

Upgrade and Migration Overview

Use this section as a starting-point for planning your upgrade to Cisco Unified Communications Manager or IM and Presence Service Release 11.5(1).

This document will guide you through the process of determining what you need to upgrade and where to find the information that you need to complete the upgrade process.

Upgrade Methods

There are two main methods of upgrading Cisco Unified Communications Manager and IM and Presence:

- Direct Upgrades, on page 5
- Migrations, on page 7

Direct Upgrades

A direct upgrade is when the new software will be installed on the same physical server and the same virtual server where the currently installed version is running. Direct upgrades allow you to upgrade from your current release to the latest release without the need to upgrade to an intermediate software version. It is a single upgrade rather than a multi-hop upgrade.

There are two types of direct upgrade:

- standard upgrades
- refresh upgrades

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

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.

The application 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.

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.

Migrations

A migration is an upgrade where the new software will be installed on a different hardware system or virtual machine than the currently installed version. For example, you need to use the migration method in the following situations:

- your currently installed version is running on Cisco 7800 Series Media Convergence Server (MCS 7800) hardware and you are upgrading to release that will run on a virtual machine
- your currently installed version is running on a virtual machine and you need to move to a new virtual machine
- you are upgrading to Cisco Unified Communications Manager from another application, such as Unified Communications 300 (UC300) Series, Unified Communications (UC500) Series, or certain Cisco Business Edition products.

Upgrade and Migration Tools

There are two tools available for upgrading or migrating Cisco Unified Communications Manager and IM and Presence:

- **Unified CM OS Administration:** This interface is part of Cisco Unified Communications Manager and you can use it to perform direct upgrades.
- **Prime Collaboration Deployment (PCD):** This is a management tool for Unified Communications (UC) applications, which supports a range of tasks. You can perform direct upgrades using the PCD Upgrade task, and you can perform migrations using the PCD Migration task.

Export Restricted and Export Unrestricted Software

This release of Cisco 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, Cisco Unified Communications Manager and IM and Presence nodes 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 of IM and Presence.

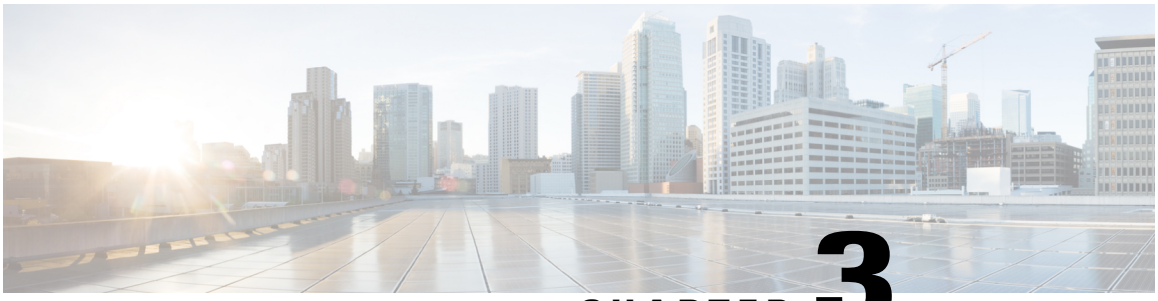
Export unrestricted GUI item location	Description
Cisco Unified Communications Manager Administration	
Advanced Features > **VPN**	This menu and its options are not available.
System > **Security** > **Phone Security Profile**	The **Device Security Mode** is set to **Non Secure** and is not configurable.
Cisco Unified CM IM and Presence Administration	
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 has been removed.
System > **Service Parameters - Cisco SIP Proxy service**	All TLS options have been removed for the Transport Preferred Order parameter.
	The TLS option has been removed from the SIP Route Header Transport Type parameter.

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.
Presence > **Inter-domain Federation** > **XMPP Federation** > **Settings**	You cannot configure the security mode; It is set to "NO TLS".
Presence > **Routing** > **Settings**	You cannot set any TLS or HTTPS listeners as the preferred proxy listener.

PART II

Plan the Upgrade or Migration

- Determine the Scope of Work, page 13
- Requirements and Limitations, page 15
- Supported Upgrade Paths, page 23
- Deployment Types and Recommendations, page 27
- Sequencing Rules and Time Requirements, page 29
- Find all Required Upgrade Documentation, page 45



CHAPTER 3

Determine the Scope of Work

- Determine the Scope of the Upgrade or Migration, page 13

Determine the Scope of the Upgrade or Migration

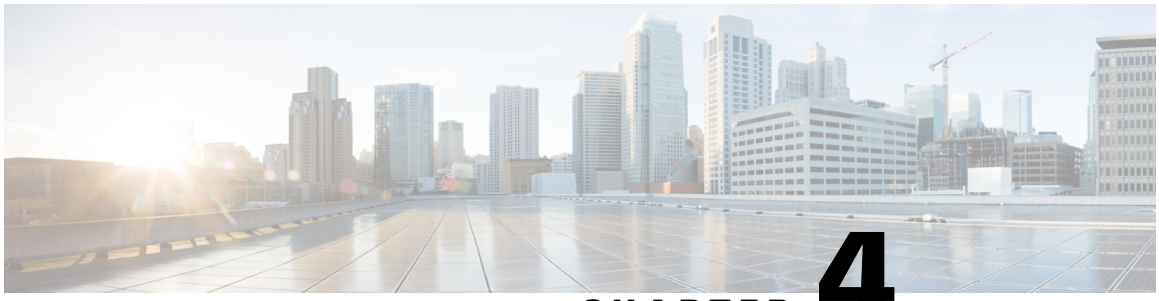
This section will help you determine:

- the scope of your upgrade or migration
- the best upgrade or migration method to use for your deployment
- where to find the information that you need to complete the upgrade or migration process

Procedure

	Command or Action	Purpose
Step 1	Determine whether you need to update the following components: • Hardware, on page 15 • Virtual Machine Configuration, on page 17	Ensure that your system meets the requirements of the new release.
Step 2	Verify the Supported Upgrade and Migration Paths, on page 23.	Use the information in this section to determine whether you can upgrade or migrate directly from your currently installed version, or whether you need to upgrade or migrate to an intermediate version before proceeding.
Step 3	Identify the Type of Deployment, on page 27	Identify the type of deployment you have and use this information to find the upgrade or migration method that Cisco recommends.
Step 4	Determine the Sequencing Rules and Time Requirements, on page 29	Direct upgrades only. The sequence in which you perform upgrade procedures depends on your deployment, and on how you want to balance the level of user impact with the amount

	Command or Action	Purpose
		of time required to complete the upgrade. You must identify the sequence that you will follow before you are ready to perform the upgrade process. The information in this section applies only if you are performing a direct upgrade using either the Unified CM OS Administration interface or the PCD Upgrade task. PCD Migrations do not require this step. If you are performing a PCD migration, proceed to the next task in this list.
Step 5	Find Upgrade Documentation, on page 45.	Find the correct upgrade documentation to use based on the needs of your deployment and the recommended upgrade or migration method.



CHAPTER 4

Requirements and Limitations

- Requirements and Limitations, page 15
- Hardware, page 15
- Network Requirements, page 16
- Virtual Machine Configuration, page 17
- Browser Requirements, page 18
- Licensing, page 19
- Limitations, page 20
- OS Admin Account Required for CLI-Initiated IM and Presence Upgrades, page 22

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 Cisco Unified Communications Manager or IM and Presence Service.

Caution 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.

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 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.

Hardware

You can install Cisco Unified Communications Manager and IM and Presence on a virtual server hosted on the following types of hardware:

- Cisco Business Edition 6000 or 7000
- Unified Communications (UC) on Cisco Unified Computing System (UCS) Tested Reference Configuration (TRC)
- UC on UCS specifications-based server
- third-party specifications-based servers

The requirements and support policies are different for each of these options. Before you begin an upgrade, verify that your current hardware meets the requirements of the new release. You can find detailed information about the requirements by going to http://www.cisco.com/go/uc-virtualized and following the links for the Cisco Unified Communications Manager and IM and Presence applications.

If your current deployment does not use one of the servers listed above, then you must perform a migration to move your deployment to a supported hardware platform.

Network Requirements

This section lists the requirements that your network must meet before you can deploy Cisco 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 Cisco 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

If you are using DNS in your deployment, note the following requirements:

- Mixed-mode DNS deployments not supported—Cisco does not support mixed-mode deployments. Both Cisco Unified Communications Manager (Unified Communications Manager) and IM and Presence must either use or not use DNS.
- If your deployment uses DNS—Unified Communications Manager and IM and Presence should use the same DNS server. If you use different DNS servers between IM and Presence and Unified Communications Manager, it is likely to cause abnormal system behavior.
- If your deployment does not use DNS—You must modify the **Host Name/IP Address** field in the service profile for the Presence and IM UC service. If DNS is not supported, you must change the **Host Name/IP Address** field to the IP address of the IM and Presence publisher node. For more information about configuring services, see *System Configuration Guide for Cisco Unified Communications Manager* .
- Multinode considerations—If you are using the multinode feature in IM and Presence, see the section regarding multinode deployments in the *Configuration and Administration of IM and Presence on Cisco Unified Communications Manager* for DNS configuration options.

SFTP Server Support

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 Cisco Unified Communications Manager. For information on which vendors have certified their products with your version of Cisco 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 supported Cisco Unified Communications 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.

Virtual Machine Configuration

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

Table 1: Virtual Machine Requirements

Item	Description
OVA templates	OVA files provide a set of predefined templates for virtual machine configuration. They cover items such as supported capacity levels and any required OS/VM/SAN alignment. You must use a VM configuration from the OVA file provided for the Cisco Unified Communications Manager and IM and Presence applications. The correct VM configuration to use from the OVA file is based on the size of the deployment. For information about OVA files, search for the topic "Unified Communications Virtualization Sizing Guidelines" at http://www.cisco.com/go/uc-virtualized.

Item	Description
VMware vSphere ESXi	You must install a version of vSphere ESXi hypervisor that meets the compatibility and support requirements the release. If you use Cisco Prime Collaboration Deployment (PCD) to perform an upgrade or migration, you must also ensure that you install vSphere ESXi with the correct license type. PCD is not compatible with all the license types of vSphere ESXi because some of these licenses do not enable required VMware APIs.
VMware vCenter	VMware vCenter is optional when you deploy Cisco Unified Communications Manager or IM and Presence on Business Edition 6000/7000 appliances, or on UC on UCS tested reference configuration hardware. VMware vCenter is mandatory when you deploy on UC on UCS specs-based and third-party server specs-based hardware.
VM configuration virtual hardware specifications	Verify whether you need to change the virtual hardware specifications on your VM in order to upgrade to a new release of Unified Communications Manager or IM and Presence Service. For example, verify the requirements for vCPU, vRAM, vNIC adaptor type, and vDisk size, as well as other specifications. Any changes to a VM must align with the OVA configuration. VM changes that result in an unsupported OVA configuration are not allowed. For information about VM requirements, see the Readme file with the OVA template that supports your release.

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

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

Browser Requirements

Cisco 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 2: Supported Browsers and Operating Systems

You can use this browser...	...with one of these operating systems
Google Chrome (latest browser version)	Microsoft Windows 10 (64 bit)

You can use this browser...	...with one of these operating systems
Microsoft Internet Explorer 11	• Microsoft Windows 10 (64 bit) • Microsoft Windows 8.1 (64 bit) • Microsoft Windows 7 (64 bit)
Microsoft Edge	Microsoft Windows 10 (32 bit/64 bit)
Mozilla Firefox (latest browser version)	Microsoft Windows 10 (64 bit)
Safari	Apple Mac OS 10.x (or newest OS release available)

Licensing

The following sections provide information about the licensing requirements for Cisco 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 Cisco 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 does not require a server license or software version license. However, you must assign users and enable the IM and Presence Service for each assigned user.

Note With the Jabber for Everyone Offer, no end user licenses are required to enable IM and Presence functionality. See the *Jabber for Everyone Quick Start Guide* for more information.

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

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

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

Refer to the*System Configuration Guide for Cisco Unified Communications Manager* for more information.

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

Limitations

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

Subnet Limitations

Do not install Cisco Unified Communications Manager in a large Class A or Class B subnet that contains a large number of devices.

Cluster Size

The number of Cisco 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 Cisco Unified Communications Manager publisher node, TFTP server, and media servers, cannot exceed 21.

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

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

IP Subnet Mask

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

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

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* for your

release, at http://www.cisco.com/c/en/us/support/unified-communications/unified-presence/products-device-support-tables-list.html.

Device Name for Cisco Unified Mobile Communicator

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

Deprecated Phone Models

As of Cisco Unified Communications Manager Release 11.5, the following phones are no longer supported. If you use any of these phone models on an older release of Cisco Unified Communications Manager and you upgrade to Release 11.5, the phone will not work after the upgrade completes.

- Cisco IP Phone 12 S
- Cisco IP Phone 12 SP
- Cisco IP Phone 12 SP+
- Cisco IP Phone 30 SP+
- Cisco IP Phone 30 VIP
- Cisco Unified IP Phone 7902G
- Cisco Unified IP Phone 7905G
- Cisco Unified IP Phone 7910
- Cisco Unified IP Phone 7910G
- Cisco Unified IP Phone 7910+SW
- Cisco Unified IP Phone 7910G+SW
- Cisco Unified IP Phone 7912G
- Cisco Unified Wireless IP Phone 7920
- Cisco Unified IP Conference Station 7935

Upgrades that Involve Deprecated Phones

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

1. Confirm whether the phones in your network will be supported in Release 11.5.
2. Identify any non-supported phones.
3. For any non-supported phones, power down the phone and disconnect the phone from the network.
4. Provision a supported phone for the phone user. You can use the Migration FX tool to migrate from older model to newer model phones. For details, go to: http://refreshcollab.cisco.com/webportal/46/CUCM%20Readiness%20Assessment#endpoint_refresh_tool.
5. Once all the phones in your network are supported by Release 11.5, upgrade your system.

Note Deprecated phones can also be removed after the upgrade. When the administrator logs in to Cisco Unified Communications Manager after completing the upgrade, the system displays a warning message notifying the administrator of the deprecated phones.

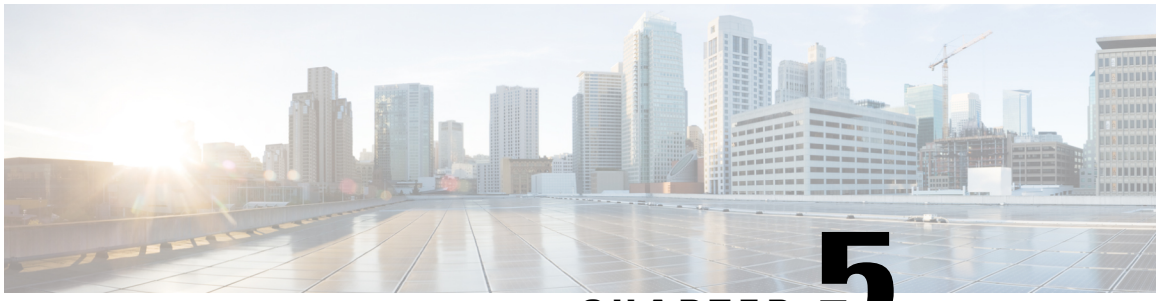
Licensing

You do not need to purchase a new device license to replace a deprecated phone with a supported phone. The device license becomes available for a new phone when you either remove the deprecated phone from the system, or when you switch to the new Cisco Unified Communications Manager version, and the deprecated phone fails to register.

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

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

Please note that this limitation exists for CLI-initiated upgrades of IM and Presence Service only and does not apply to Cisco Unified Communications Manager. Also note that this limitation may be fixed for newer ISO files. Refer to your ISO Readme file for details on your specific ISO file. For up to date information on this limitation, see CSCvb14399 at https://bst.cloudapps.cisco.com/bugsearch/bug/CSCvb14399.



CHAPTER 5

Supported Upgrade Paths

- Version Requirements, page 23
- Supported Upgrade and Migration Paths, page 23

Version Requirements

All servers in a cluster must run the same release of Cisco 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 two numbers of the software version installed on the Unified Communications Manager publisher node. For example, IM and Presence Service software version 11.0.1.10000-1 is compatible with Cisco Unified Communications Manager software version 11.0.1.30000-2.

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 11.5.1.10000-1, then all IM and Presence subscriber nodes must also be 11.5.1.10000-1.

Supported Upgrade and Migration Paths

Use the tables below to determine whether you can upgrade or migrate from your currently installed version, and which of the supported upgrade methods are available to you:

- direct upgrades using either the Cisco Unified CM OS Admin interface or the Cisco Prime Collaboration Deployment (PCD) Upgrade task
- migrations using the PCD Migration task

If an upgrade or migration from your current release is not supported, see the instructions in the section Upgrading from Legacy Releases, on page 129.

Applications Installed on Cisco Media Convergence Servers Hardware

Applications Installed on Cisco Media Convergence Server (MCS) 7800 Series Hardware

You cannot install or run Cisco Unified Communications Manager and the IM and Presence Service directly on server hardware; you must run these applications on virtual machines. The tables below list the supported migration paths for deployments that are currently running on MCS 7800 hardware. All of the supported migration paths listed below are physical-to-virtual (P2V) migrations.

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

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

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

Table 3: Cisco Unified Communications Manager Releases Installed on MCS 7800 Series Hardware

From	To	Supported Method
6.1(5)	11.5(1)	PCD Migration
7.1(3) and 7.1(5)	11.5(1)	PCD Migration
8.x	11.5(1)	PCD Migration
9.x	11.5(1)	PCD Migration

Table 4: Cisco Unified Presence and IM and Presence Releases Installed on MCS 7800 Series Hardware

From	To	Supported Method
CUP 8.5(4)	11.5(1)	PCD Migration
CUP 8.6(3), 8.6(4), and 8.6(5)	11.5(1)	PCD Migration
IM and Presence 9.x	11.5(1)	PCD Migration

Applications Installed on Virtual Machines

Applications Installed on Virtual Machines

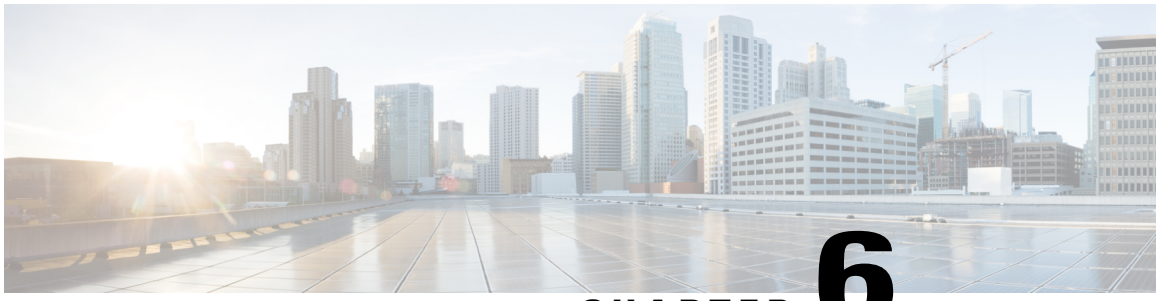
The tables below list the supported upgrade and migration paths for deployments that are currently running on virtual machines. All of the supported upgrade and migration paths listed below are virtual-to-virtual (V2V).

Table 5: Cisco Unified Communications Manager Releases Installed on Virtual Machines

From	To	Supported Method
8.6(x)	11.5(1)	Cisco Unified OS Admin PCD Migration or PCD Upgrade
9.x	11.5(1)	PCD Migration or PCD Upgrade
9.1(x)	11.5(1)	Cisco Unified OS Admin
10.x	11.5(1)	PCD Migration or PCD Upgrade
10.5(x)	11.5(1)	Cisco Unified OS Admin
11.0(1)	11.5(1)	Cisco Unified OS Admin PCD Migration or PCD Upgrade

Table 6: Cisco Unified Presence and IM and Presence Releases Installed on Virtual Machines

From	To	Supported Method
CUP 8.5(4)	11.5(1)	PCD Migration
CUP 8.6(3), 8.6(4), and 8.6(5)	11.5(1)	PCD Migration or PCD Upgrade
CUP 8.6(x)	11.5	Cisco Unified OS Admin
IM and Presence 9.x	11.5(1)	PCD Migration or PCD Upgrade
IM and Presence 9.1(x)	11.5(1)	Cisco Unified OS Admin
IM and Presence 10.x	11.5(1)	PCD Migration or PCD Upgrade
IM and Presence 10.5(x)	11.5(1)	Cisco Unified OS Admin
IM and Presence 11.0(1)	11.5(1)	Cisco Unified OS Admin PCD Migration or PCD Upgrade



CHAPTER 6

Deployment Types and Recommendations

- Type of Deployment, page 27

Type of Deployment

Use the information in this section after you have reviewed the tables in the Supported Upgrade and Migration Paths, on page 23 section. If those tables indicate that you have a choice of which upgrade method to use, refer to the recommendations in the following sections to help you choose the best option for your deployment.

Business Edition 6000 and Business Edition 7000 Deployments

If your hardware and VMware are current and do not need any changes to meet the compatibility and support requirements of the release, use Unified CM OS Admin to perform the upgrade.

If you are running several applications in addition to Cisco Unified Communications Manager and IM and Presence Service, such as Cisco Unity Connection and/or Cisco Unified Contact Center Express, you can use the PCD upgrade task to automate the process.

Virtualized Deployments of Cisco Unified Communications Manager and IM and Presence Service

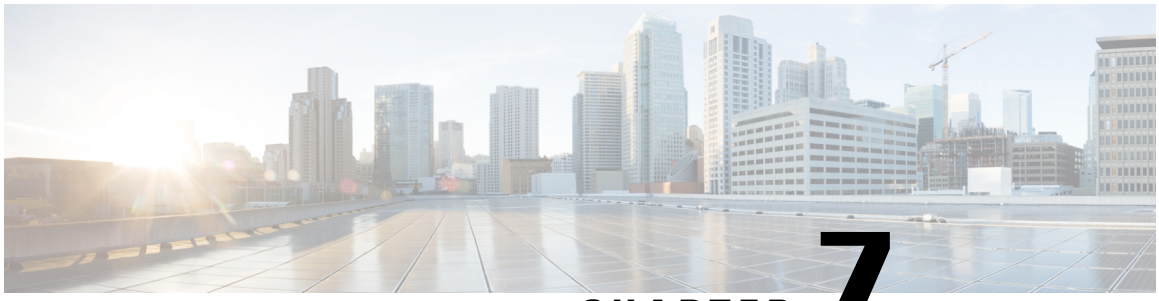
If your current version is running in a virtualized environment, your upgrade path may allow you to choose your upgrade method. Use the information in this section to help you choose your upgrade method.

Consider performing a PCD migration when:

- you need old and new systems up in parallel
- you want to change virtual machine configurations in Release 11.5(1) but the change forces a reinstall

Consider performing a PCD upgrade when:

- you have large number of virtual machines and a complex upgrade sequence or a need to forward-schedule
- you need to upgrade other applications, such as Cisco Unity Connection or Cisco Unified Contact Center Express



CHAPTER 7

Sequencing Rules and Time Requirements

- Upgrade Sequence and Time Requirements, page 29
- Upgrade time requirements, page 35

Upgrade Sequence and Time Requirements

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

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

We recommend that you follow the sequences that are outlined in this section when you plan your upgrade. Choose one of the following options, based on your business needs:

- Recommended Sequence for the Least Time , on page 29
- Recommended Sequence for the Least Impact, on page 31

If you do not follow one of the recommended sequences, you must ensure that your upgrade plan meets the requirements listed in Sequence Rules, on page 34

Recommended Sequence for the Least Time

Use the information in this section if you want to perform a direct upgrade that takes the least amount of time. This approach will have the greatest service impact on your network.

To perform an upgrade in the least amount of time, you can upgrade all Cisco Unified Communications Manager subscriber nodes in parallel; with this option, all phones will be out of service for the duration of the upgrade. You can reduce the impact on phone service by organizing the subscriber nodes into subgroups. Upgrade the subscriber nodes within each subgroup in parallel, but upgrade each subgroup sequentially. This will reduce the impact to your phone service but will add time to the upgrade process.

The tables below list the sequence to follow for direct refresh upgrades and direct standard upgrades. Plan to perform the tasks in the order shown in the appropriate table below. You must always begin an upgrade with the Cisco Unified Communications Manager nodes. You can perform upgrade procedures on the IM and

Presence nodes in parallel with Cisco Unified Communications Manager nodes only as indicated in the table below. Any tasks that are listed on the same row in the table are ones that you can perform in parallel.

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.

Refresh Upgrades

Use the table below to plan a refresh upgrade when your priority is to perform the upgrade in the least amount of time. If you are unsure whether you need to perform a refresh upgrade or a standard upgrade, review the information in Direct Upgrades, on page 5.

Table 7: Recommended Sequence for Performing Refresh Upgrades in the Least Amount of Time

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

Standard Upgrades

Use the table below to plan a standard upgrade when your priority is to perform the upgrade in the least amount of time.

Table 8: Recommended Sequence for Performing Standard Upgrades in the Least Amount of Time

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

Recommended Sequence for the Least Impact

Use the information in this section if you want to perform a direct upgrade that has the least impact on your network and you can accept the completion of the upgrade over a longer period.

The tables below list the sequence to follow for direct refresh upgrades and direct standard upgrades. Plan to perform the tasks in the order shown in the appropriate table below. You must always begin an upgrade with the Cisco Unified Communications Manager nodes. You can perform upgrade procedures on the IM and Presence nodes in parallel with Cisco Unified Communications Manager nodes. Any tasks that are listed on the same row in the table are ones that you can perform in parallel.

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.

Note In addition to following the recommended sequence, you must also verify that your phones and devices are configured for redundancy through the use of Cisco Unified CM Groups (CMGs) with primary subscriber nodes and backup subscriber nodes. As part of your upgrade planning, ensure that you have assigned nodes and devices to CMGs so that when one of the nodes in the CMG is unavailable, the remaining nodes within the CMG can support all of the devices that are assigned to the CMG. This configuration allows you to ensure availability throughout the upgrade. For more information about CMGs, see the chapter "Configure Core Settings for Device Pools" in the *System Configuration Guide for Cisco Unified Communications Manager* at http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.html.

Refresh Upgrades

Use the table below to plan a refresh upgrade when your priority is to perform the upgrade with the least impact on phone services.

Table 9: Recommended Sequence for Performing Refresh Upgrades with the Least Impact

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

Sequence	Cisco Unified Communications Manager Nodes	IM and Presence Service Nodes
8	Ensure that database replication is complete and functioning between the publisher node and all primary subscriber nodes.	—
9	—	Switch the software version on the database publisher node and reboot it. The new software is active.
10	—	Switch the software version on the subscriber nodes in parallel and reboot them. The new software is active.
11	—	Ensure that database replication is complete and functioning between the publisher node and all subscriber nodes.

Standard Upgrades

Use the table below to plan a standard upgrade when your priority is to perform the upgrade with the least impact on phone services.

Table 10: Recommended Sequence for Performing Standard Upgrades with the Least Impact

Sequence	Cisco Unified Communications Manager Nodes	IM and Presence Service Nodes
1	Upgrade the publisher node to the new software version. The new software is inactive.	—
2	Upgrade the primary and secondary subscriber nodes. The new software is inactive.	Upgrade the IM and Presence database publisher node in parallel with the Cisco Unified Communications Manager subscriber nodes. The new software is inactive.
3	—	Upgrade the subscriber nodes. The new software is inactive.
4	Switch the software version on the publisher node and reboot it.	—
5	Verify that phones are registered to primary subscriber nodes in CMGs. Switch the software version on the secondary subscriber nodes in parallel and reboot them. The new software is active.	Switch the software version on the database publisher node and reboot it.

Sequence	Cisco Unified Communications Manager Nodes	IM and Presence Service Nodes
6	Ensure that database replication is complete and functioning between the publisher node and all secondary subscriber nodes.	Switch the software version on the subscriber nodes in parallel and reboot them. The new software is active.
7	Verify that phones are registered to secondary subscriber nodes in CMGs. Switch the software version on the primary subscriber nodes in parallel and reboot them.	Ensure that database replication is complete and functioning between the publisher node and all subscriber nodes.
8	Ensure that database replication is complete and functioning between the publisher node and all primary subscriber nodes. Verify that phones are registered to primary subscriber nodes in CMGs.	—

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 Cisco 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 Cisco 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 Cisco 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.
- 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 nodes in addition to Cisco Unified Communications Manager nodes:
    - The IM and Presence database publisher node must be the first IM and Presence node that you upgrade. The new software is installed as an inactive version.
    - You can begin upgrading IM and Presence subscriber nodes as soon as the publisher node has been upgraded with an inactive version of the new software.
    - You can wait until all of the Cisco Unified Communications Manager nodes are upgraded to an inactive version before you upgrade the IM and Presence database publisher node, or you can choose to upgrade in parallel. If you upgrade in parallel, start upgrading the IM and Presence database publisher node at the same time that you upgrade the Cisco Unified Communications Manager subscriber nodes.

- You must switch to the new software version and reboot all Cisco Unified Communications Manager nodes, starting with the publisher node, before you can switch versions on the IM and Presence nodes.
- You must switch the IM and Presence database publisher node to the new software version and reboot it before you switch the software version on any IM and Presence subscriber nodes.
- If you upgrade a group of IM and Presence subscriber nodes, after you switch the software version and reboot, you must wait for database replication to complete on all subscriber nodes before proceeding.

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

Upgrade time requirements

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

Factors that Affect Upgrade Time Requirements

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

Table 11: Factors that Affect Time Requirements

Item	Description
External Services and Tools	Time requirements are reduced when external services and tools, such as NTP servers, DNS servers, LDAP directories, and other network services are reachable with response times as short as possible with no dropped packets. We recommend that you configure the ESXi server and the Cisco Unified Communications Manager publisher node to point to the same NTP server.

Item	Description
Accessibility of upgrade images	Save time by ensuring that ISO images are on DVD, or are already downloaded and staged on the same LAN as the Cisco Unified Communications Manager and IM and Presence Service virtual machines (VM).
System health	The virtual machine configuration impacts the time requirement for an upgrade. Use the virtual machine specifications that are correct for your deployment size. If your database exceeds the virtual machine's configuration limits, the upgrade process will take longer to complete or fail. For example, having too many devices for the VM configuration will impact the upgrade.
	Low memory or memory leaks will impact the upgrade.
	Round Trip Times (RTT) between nodes will extend the time required.
	Ensure that there are no OutOfSynch (OOS) tables in the database.
	Ensure that there are no SD link out-of -service events on the Cisco Unified Communications Manager node. These events typically indicate a network problem, which you must address before you begin the upgrade process.
	System errors can impact upgrade time. In the Real Time Monitoring Tool (RTMT) interface, double-click Alert Central in the left navigation pane and ensure that there are no errors.

Item	Description
Physical and virtual hardware infrastructure	Upgrade time is reduced when your infrastructure is configured for high-capacity and low-latency, and when there is low contention from other traffic. For example, you can optimize the upgrade process by ensuring that: • There are no infrastructure bottlenecks from VMs sharing same ESXi host, the same Direct Attached Storage (DAS) volume, the same Logical Unit Number (LUN), or the same congested network link. • Storage latencies meet the requirements specified at http://www.cisco.com/go/uc-virtualized. • The physical CPU cores and the virtualization design comply with virtualization requirements of Cisco Unified Communications Manager and IM and Presence Service. Do not oversubscribe CPUs by having VMs share the host resources; use logical cores or resource reservations • Cisco Unified Communications Manager and IM and Presence Service virtual machines are on same hosts, or on hosts wtih 1GbE LAN between them with low contention from other traffic. • If the cluster is over a WAN, ensure that you follow all bandwidth and latency rules listed in the *Cisco Collaboration Systems Solution Reference Network Designs (SRND)* for at http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-system/products-implementation-design-guides-list.html.
System capacity	Reduce the upgrade time by purging unnecessary files, such as: • Call Detail Recording (CDR) records • Outdated files, such as TFTP files, firmware, and log files
Throttling	On IM and Presence Service nodes, the system throttles the upgrade process to preserve system stability during upgrades. Throttling may increase the time required to complete the upgrade. Although you can disable throttling to decrease the time it takes to perform the upgrade, doing so may degrade system performance.

Estimating the Minimum Time Requirements

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

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

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

Table 12: Minimum Time Required for Upgrade Tasks

Task	Minimum Time	Service Impact
Upgrade the Cisco Unified Communications Manager publisher node to an inactive version	2 to 4 hours Add 1 hour if a refresh upgrade	Refresh upgrades: no access to the UI
Upgrade the Cisco Unified Communications Manager subscriber nodes to an inactive version	1 to 2 hours	Refresh upgrades: phones are unavailable if no backup subscribers are configured
Switch the Cisco Unified Communications Manager publisher node to the new software version and reboot	30 minutes	—
Switch the Cisco Unified Communications Manager subscriber nodes to the new software version and reboot	30 minutes	Standard upgrades: phones are unavailable if no backup subscribers are configured
Cisco Unified Communications Manager database replication	30 minutes for deployments with small clusters or small databases 2 hours for megaclusters or large databases **Note** WAN latency of 80ms or more can significantly lengthen these times	Phones are available with dial tone but end-user features are unavailable until upgrade is complete

Task	Minimum Time	Service Impact
Upgrade the IM and Presence database publisher node to an inactive version	2 to 4 hours Add 1 hour if a refresh upgrade	IM and Presence high availability is disabled Jabber is unavailable
Upgrade the IM and Presence subscriber nodes to an inactive version	1 to 2 hours	IM and Presence high availability is disabled Jabber is unavailable
Switch the IM and Presence publisher node to the new software version and reboot	30 minutes	IM and Presence high availability is disabled Jabber is unavailable
Switch the IM and Presence subscriber nodes to the new software version and reboot	30 minutes	IM and Presence high availability is disabled Jabber is unavailable
IM and Presence database replication	30 minutes for deployments with small clusters or small databases 2 hours for megaclusters or large databases **Note** WAN latency of 80ms or more can significantly lengthen these times	IM and Presence high availability is disabled Jabber is unavailable

Examples

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

- a megacluster that includes Cisco Unified Communications Manager nodes as well as IM and Presence nodes
- 75,000 users
- a system that is healthy and that has been optimized for the upgrade, as described in Factors that Affect Upgrade Time Requirements, on page 35

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

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

your network. The tasks in this example are performed in parallel wherever possible to help reduce the time required for the upgrade.

Table 13: Example: Time Requirements for a Standard Upgrade in the Least Time

Task		Minimum Estimated Time
1	Upgrade the Cisco Unified Communications Manager publisher node to the new software version. The new software is inactive.	2-4 hours
2	In parallel: • Upgrade the Cisco Unified Communications Manager subscriber nodes. The new software is inactive. • Upgrade the IM and Presence database publisher node.	2-3 hours
3	Upgrade the IM and Presence subscriber nodes. The new software is inactive.	1-2 hours
4	Switch the software version on the Cisco Unified Communications Manager publisher node and reboot it.	30 minutes
5	In parallel: • Switch the software version on the Cisco Unified Communications Manager subscriber nodes and reboot them. • Switch the software version on the IM and Presence database publisher node and reboot it.	30 minutes
6	In parallel: • Wait for database replication on the Cisco Unified Communications Manager subscriber nodes. • Switch the software version on the IM and Presence subscriber nodes and reboot them.	2 hours
7	Wait for database replication on the IM and Presence subscriber nodes.	2 hours
Total		10 to 14 hours

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

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

Table 14: Example: Time Requirements for a Refresh Upgrade in the Least Time

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

Example: Time Requirements for a Standard Upgrade with the Least Impact

This example shows an example of how to calculate minimum time requirements if you want to perform a standard upgrade that has the least impact on your phone service. The tasks in this example are performed in parallel wherever possible to reduce the length of the service outage.

Table 15: Example: Time Requirements for a Standard Upgrade in the Least Impact

Task		Minimum Estimated Time
1	Upgrade the Cisco Unified Communications Manager publisher node to the new software version. The new software is inactive.	2-3 hours

Task		Minimum Estimated Time
2	In parallel: • Upgrade all of the Cisco Unified Communications Manager subscriber nodes. The new software is inactive. • Upgrade the IM and Presence database publisher node.	2-3 hours
3	Upgrade the IM and Presence subscriber nodes in parallel. The new software is inactive.	1-2 hours
4	Switch the software version on the Cisco Unified Communications Manager publisher node and reboot it.	30 minutes
5	In parallel: • Switch the software version on the Cisco Unified Communications Manager secondary subscriber nodes and reboot them. • Switch the software version on the IM and Presence database publisher node and reboot it.	30 minutes
6	In parallel: • Wait for database replication on the Cisco Unified Communications Manager secondary subscriber nodes. • Switch the software version on the IM and Presence subscriber nodes in parallel and reboot them.	2 hours
7	In parallel: • Wait for database replication on the IM and Presence subscriber nodes. Switch the software version on the Cisco Unified Communications Manager primary subscriber nodes and reboot them.	2 hours
8	Wait for database replication on the Cisco Unified Communications Manager primary subscriber nodes.	2 hours
Total		12-15 hours

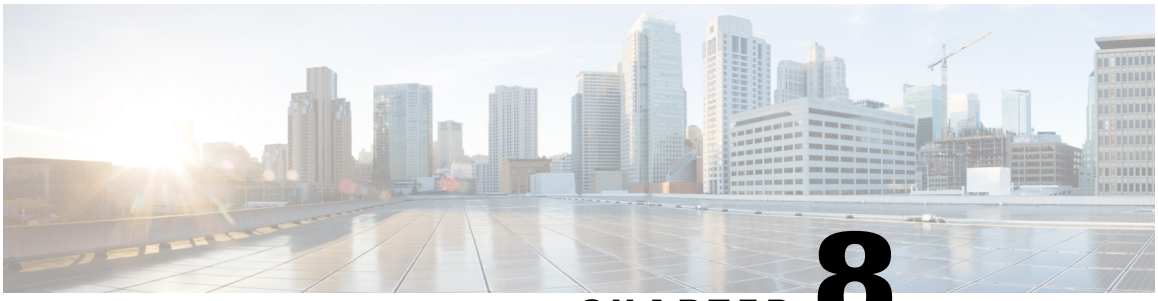
Example: Time Requirements for a Refresh Upgrade with the Least Impact

This example shows an example of how to calculate minimum time requirements if you want to perform a refresh upgrade that has the least impact on your phone service. The tasks in this example are performed in parallel wherever possible to reduce the length of the service outage.

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

Task		Minimum Estimated Time
1	Upgrade the Cisco Unified Communications Manager publisher node to the new software version. The new software is inactive.	3-4 hours
2	In parallel: • Upgrade the Cisco Unified Communications Manager secondary subscriber nodes in parallel. The new software is inactive. • Upgrade the IM and Presence database publisher node.	3-4 hours
3	In parallel: • Upgrade the Cisco Unified Communications Manager primary subscriber nodes in parallel. The new software is inactive. • Upgrade the IM and Presence subscriber nodes in parallel. The new software is inactive.	1-2 hours
4	Switch the software version on the Cisco Unified Communications Manager publisher node and reboot it.	30 minutes
5	Switch the software version on the Cisco Unified Communications Manager secondary subscriber nodes and reboot them.	30 minutes
6	Wait for database replication on the Cisco Unified Communications Manager secondary subscriber nodes.	2 hours
7	Switch the software version on the Cisco Unified Communications Manager primary subscriber nodes and reboot them.	30 minutes
8	Wait for database replication on the Cisco Unified Communications Manager primary subscriber nodes.	2 hours
9	Switch the software version on the IM and Presence database publisher node and reboot it.	30 minutes
10	Switch the software version on the IM and Presence subscriber nodes in parallel and reboot them.	1-2 hours
11	Wait for database replication on the IM and Presence subscriber nodes.	2 hours

Task	Minimum Estimated Time
Total	16-20 hours



CHAPTER 8

Find all Required Upgrade Documentation

- Upgrade Documentation, page 45

Upgrade Documentation

Find the correct upgrade documentation to use based on the scope of your upgrade and the recommended upgrade method.

Task	See . . .
Prepare the hardware platform	
Install a Unified Communications (UC) on Cisco Unified Computing System (UCS) Tested Reference Configuration (TRC)	*Cisco Collaboration on Virtual Servers* at http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-guides-list.html
Install a Business Edition 6000 (BE 6000) appliance	Installation guides for your version of BE 6000 at http://www.cisco.com/c/en/us/support/unified-communications/business-edition-6000/products-installation-guides-list.html
Install a Business Edition 7000 (BE 7000) appliance	*Cisco Business Edition 7000 Installation Guide* at http://www.cisco.com/c/en/us/support/unified-communications/business-edition-7000/products-installation-guides-list.html
Install new virtualized 3rd-party specs-based server or Cisco UCS specs-based server	See the documentation from the server vendor and from VMware. See application support information at http://www.cisco.com/go/uc-virtualized Information about specs-based support is available by searching on the topic "UC Virtualization Supported Hardware" at http://www.cisco.com/go/uc-virtualized

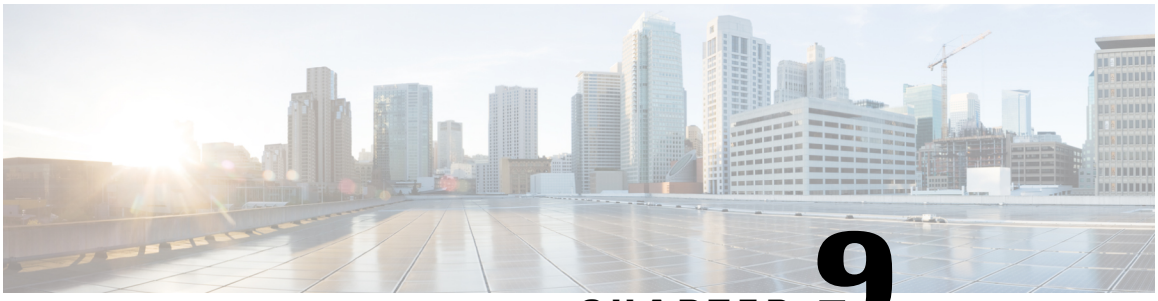
Task	See . . .
Replace existing hardware and preserve the server configuration	*Replacing a Single Server or Cluster for Cisco Unified Communications Manager* at http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-guides-list.html
Change the IP address or hostname	**To automate the changes:** • Perform a PCD Upgrade or PCD Migration with network migration to change the application version and the IP address at the same time. • Use the PCD Re-address task after the upgrade is complete. This task changes the IP addresses only. See *Cisco Prime Collaboration Deployment Administration Guide* at http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html
	To make the changes manually: See *Changing IP Address and Hostname for Cisco Unified Communications Manager or IM and Presence Service* at http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html
Prepare the virtual platform	
Review requirements and best practices	Cisco Unified Communications Manager and IM and Presence Service information at http://www.cisco.com/go/uc-virtualized
Download the Cisco OVA file	Follow the procedures contained in this document.See Download and Install OVA Templates, on page 53
Edit the virtual machine configuration	Vendor documentation at http://www.VMware.com Follow the procedures contained in this document.See Change the Virtualization Software, on page 51
Upgrade to a new release of Cisco Unified Communications Manager and IM and Presence Service	
Upgrade and install new licenses	*Cisco Prime License Manager User Guide* at http://www.cisco.com/c/en/us/support/cloud-systems-management/prime-license-manager/products-user-guide-list.html
Migrate from one hardware platform to another as part of the upgrade process	*Cisco Prime Collaboration Deployment Administration Guide* at http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html

Task	See . . .
Upgrade on the same hardware platform using Prime Collaboration Deployment	*Cisco Prime Collaboration Deployment Administration Guide* at http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html
Upgrade on the same hardware platform using Unified CM OS Administration	Follow the procedures contained in this document.
Read the Release Notes for the new software version	*Release Notes for Cisco Unified Communications Manager and IM and Presence Service* at http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-release-notes-list.html

PART III

Change the Virtualization Software

- Change the Virtualization Software, page 51



CHAPTER 9

Change the Virtualization Software

- Virtual Machine Configuration Tasks, page 51

Virtual Machine Configuration Tasks

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

Before You Begin

Verify whether you need to upgrade your virtual machine to meet the requirements of the new release. You can find the requirements by going to http://www.cisco.com/go/uc-virtualized and following the links for the Cisco Unified Communications Manager and IM and Presence applications.

Procedure

	Command or Action	Purpose
Step 1	Install and Configure VMware vCenter, on page 52	VMware vCenter is required only when you are migrating from Cisco Business Edition or Tested Reference Configuration (TRC) hardware to UC on UCS specs-based or third-party server specs-based hardware. If you require VMware vCenter, install and configure it first. Using VMware vCenter is optional when you deploy Cisco Unified Communications Manager or IM and Presence on UC on UCS tested reference configuration hardware.
Step 2	Upgrade vSphere ESXi, on page 52	You must install a version of vSphere ESXi hypervisor that meets the requirements of the release. We recommend that you upgrade the ESXi hypervisor before you begin an upgrade of Cisco Unified Communications Manager or IM and Presence Service; however, if your currently installed version of these applications is not compatible with the ESXi version required for the new release, you can upgrade the ESXi version after you upgrade the Cisco applications.

	Command or Action	Purpose
Step 3	Download and Install OVA Templates, on page 53	OVA files provide a set of predefined templates for virtual machine configuration. They cover items such as supported capacity levels and any required OS/VM/SAN alignment. This procedure is optional. If you are already running Cisco Unified Communications Manager or IM and Presence on a virtual machine, and your deployment size has not changed, you do not need to download and install a new OVA template. If you are changing the size of your system, download and install an OVA template for the new release that is sized for your deployment.
Step 4	Change Virtual Machine Configuration Specifications, on page 54	Use this procedure when you need to change the vCPU, vRAM, vDisk size, or vNIC type on your virtual machine (VM) in order to upgrade to a new release of Unified Communications Manager or IM and Presence Service. Do this step for only for direct upgrades, which use either the Unified CM OS Admin interface or the PCD Upgrade task to perform the upgrade.
Step 5	Migrate From Single to Multi-vDisk Virtual Machine, on page 55	Use this procedure if you are migrating to a larger virtual machine (VM) deployment that requires multiple vDisks.

Install and Configure VMware vCenter

Using VMware vCenter is optional when you deploy Cisco Unified Communications Manager or IM and Presence on UC on UCS tested reference configuration hardware. VMware vCenter is mandatory when you deploy on UC on UCS specs-based and third-party server specs-based hardware.

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

Procedure

Step 1 Install VMware vCenter.

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

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

Upgrade vSphere ESXi

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

Procedure

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

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

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

Step 3 Verify that the vSphere ESXi upgraded successfully.

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

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

Download and Install OVA Templates

OVA files provide a set of predefined templates for virtual machine configuration. They cover items such as supported capacity levels and any required OS/VM/SAN alignment. For information about OVA files, search for the topic "Unified Communications Virtualization Sizing Guidelines" at http://www.cisco.com/go/uc-virtualized.

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

Procedure

Step 1 Locate the OVA template for your release:

- For Cisco Unified Communications Manager, go to http://www.cisco.com/go/uc-virtualized and search for the topic "Virtualization for Cisco Unified Communications Manager."

- For IM and Presence Service, go to http://www.cisco.com/go/uc-virtualized and search for the topic "Virtualization for Unified CM IM and Presence."

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

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

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

Step 5 Click on one of the following links:

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

A new browser window appears.

Step 6 Save the file:

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

Change Virtual Machine Configuration Specifications

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

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

Before You Begin

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

Procedure

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

Step 2 (Optional) For an upgrade from 9.x or earlier, if you need to increase the vDisk space to meet the space requirements of a refresh upgrade, install the following COP file:
`ciscocm.vmware-disk-size-reallocation-<latest_version>.cop.sgn`

Step 3 Shut down the virtual machine.

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

a) Change the Guest OS version to match the requirements of the new release.

b) To change the vCPU, make the change in vSphere Client. Ensure that you change the reservation value to match the specifications of the new release.
c) To change the vRAM, make the change in vSphere Client. Ensure that you change the reservation value to match the specifications of the new release.
d) To increase the vDisk space, edit the storage size using vSphere Client. If the virtual machine has two disks, expand the second one.
The new space is automatically added to the common partition when you restart the virtual machine.

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

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

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

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

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

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

Migrate From Single to Multi-vDisk Virtual Machine

If you are migrating to a larger virtual machine (VM) deployment that requires multiple vDisks, perform the following procedure. After you complete this procedure, you must Change Virtual Machine Configuration Specifications, on page 54 to ensure that the specifications match the requirements of the release.

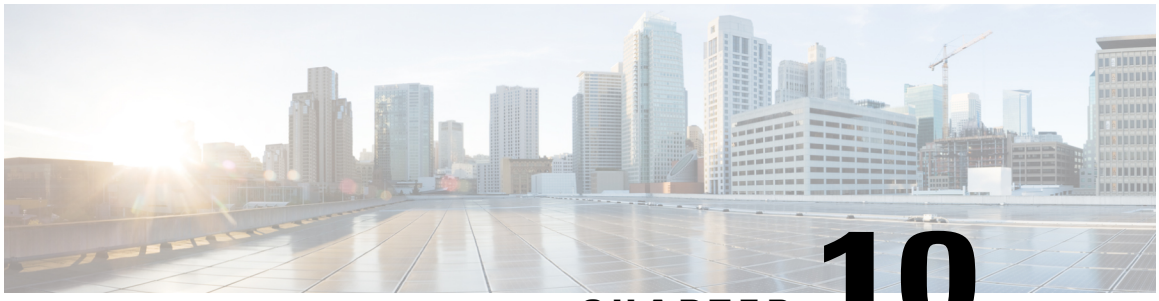
Procedure

Step 1 Use the Disaster Recovery System (DRS) to perform a backup of the existing virtual machine (VM).
Step 2 Power off the existing VM and remove it from the network.
Step 3 Deploy a new VM at the correct user count using the appropriate OVA template.
Step 4 Perform a fresh installation of the same software release of IM and Presence or Cisco Unified Communications Manager on the new VM using the same hostname and IP address.
Step 5 Perform a DRS restore on the new VM.

PART IV

Upgrade the Applications

- Pre-upgrade Tasks, page 59
- Upgrade Procedures, page 83
- Post-upgrade Tasks , page 95



CHAPTER 10

Pre-upgrade Tasks

- Pre-Upgrade Task Flow, page 59

Pre-Upgrade Task Flow

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

Procedure

	Command or Action	Purpose
Step 1	Read the release notes for the new release: http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-release-notes-list.html	Ensure that you understand the new features and how the upgrade interacts with the other products that are associated with your system. Do this step for all upgrade and migration methods.
Step 2	Check 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* at http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html for information about how to migrate an existing cluster to a virtualized cluster.	You cannot install or run Cisco Unified Communications Manager and the IM and Presence Service directly on server hardware; you must run these applications on virtual machines. Do this step for all upgrade and migration methods.
Step 3	Familiarize yourself with the requirements and limitations of this release: Requirements and Limitations, on page 15	Ensure that your system meets all requirements, including network requirements, platform requirements, and software requirements. Do this step for all upgrade and migration methods.

	Command or Action	Purpose
Step 4	Check the health of your network: • Read Factors that Affect Upgrade Time Requirements, on page 35 and ensure that your system meets the conditions described in that section. • Generate a Database Status Report, on page 64 • Check Database Replication, on page 64 • Check Performance Reports, on page 65 • Run CLI Diagnostics, on page 66	The health of your system affects the amount of time that an upgrade requires. You can reduce the amount of time needed for an upgrade by ensuring that your system meets the conditions described in these sections. Do this step for all upgrade and migration methods.
Step 5	Ensure that there are no expired certificates on the partition, including any trust certificates in the certificate chain. If there are expired certificates, perform one or more of the following procedures: • Delete a Trust Certificate, on page 66 • Regenerate a Certificate, on page 67 if an identify certificate is expired	Perform this step for refresh upgrades on Cisco Unified Communications Manager and 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 6	Take a Fresh Backup, on page 68	You must create a fresh backup file in case you need to restore your existing system. Do this step for all upgrade and migration methods. **Caution** You may lose data or you may be unable to restore your system if your backup is outdated.
Step 7	Back Up Custom Ringtones and Background Images, on page 69	If you have custom ringtones or background images in the TFTP directory, you need to create a separate backup for these files. They are not included in the Disaster Recovery System (DRS) backup file.
Step 8	Check Network Connectivity, on page 69	Use this procedure to verify connectivity between Cisco Unified Communications Manager nodes and services in your network, such as NTP, SMTP, and DNS.
Step 9	Verify IPv6 Networking, on page 70	This procedure applies to Cisco Unified Communications Manager nodes only. 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

	Command or Action	Purpose
		subscriber nodes, load detection may take 20 minutes. Do this step for all upgrade and migration methods.
Step 10	Check Connectivity between IM and Presence and Cisco Unified Communications Manager, on page 70	Verify that the IM and Presence Service node has connectivity with Cisco Unified Communications Manager. Do this step for only for direct upgrades, which use either the Unified CM OS Admin interface or the PCD Upgrade task to perform the upgrade.
Step 11	Collect Configuration and Login Information, on page 71	Record the current configuration and login information for your Unified Communications Manager nodes in case any issues are encountered during the upgrade process.
Step 12	Record the Registered Device Count, on page 71	Use the Real Time Monitoring Tool (RTMT) to capture the device count so that you can verify your endpoints and resources after the upgrade is complete. You can also use this information to verify that you have not exceeded the capacity of the virtual machine (VM) that you are deploying. Do this step for all upgrade and migration methods.
Step 13	Record the Number of Assigned Users, on page 72	Record the number of assigned users on IM and Presence Service nodes so that you can verify this information after the upgrade is complete. Do this step for all upgrade and migration methods.
Step 14	Record TFTP Parameters, on page 72	The upgrade process changes a TFTP parameter. Record the current setting so that you can reset the parameter after the upgrade is complete.
Step 15	Record Enterprise Parameters, on page 73	Record the settings for Enterprise Parameters on both Unified Communications Manager nodes and IM and Presence Service nodes. Some Enterprise Parameters exist on both types of nodes and the settings that are configured on Unified Communications Manager nodes may overwrite the settings configured on IM and Presence Service nodes during an upgrade. Record the settings so that you can restore them as needed after the upgrade is complete. Do this step for all upgrade and migration methods.
Step 16	Export User Records, on page 73	Export user records using the Bulk Administration Tool (BAT). Do this step for all upgrade and migration methods.

	Command or Action	Purpose
Step 17	Upgrade IP Phone Firmware, on page 74	You can upgrade your IP phones to the firmware that corresponds to the new release as a pre-upgrade task. Although IP phones automatically download their new firmware after an upgrade, you can choose to apply new firmware files to the endpoints in a controlled manner prior to the upgrade in order to minimize phone downtime after an upgrade. Do this step for only for direct upgrades, which use either the Unified CM OS Admin interface or the PCD Upgrade task to perform the upgrade.
Step 18	Verify Critical Services, on page 75	Verify that all critical services are activated.
Step 19	Deactivate Cisco Extension Mobility and TFTP Services, on page 75	Stop Cisco extension mobility and TFTP services on Cisco Unified Communications Manager nodes before you begin an upgrade. Do this step for only for direct upgrades, which use either the Unified CM OS Admin interface or the PCD Upgrade task to perform the upgrade.
Step 20	Stop the IM and Presence Sync Agent, on page 76	If you need to upgrade Cisco Unified Communications Manager as part of your IM and Presence upgrade, you must stop the IM and Presence Sync Agent service before you begin the upgrade process. Do this step for only for direct upgrades, which use either the Unified CM OS Admin interface or the PCD Upgrade task to perform the upgrade.
Step 21	Check the Available Common Partition Space, on page 76	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. Do this step for only for direct upgrades, which use either the Unified CM OS Admin interface or the PCD Upgrade task to perform the upgrade.
Step 22	If you do not have enough common partition space, perform one or more of the following procedures: • Adjust High and Low Watermarks, on page 76 • Create Additional Partition Space, on page 77	Do this step for only for direct upgrades, which use either the Unified CM OS Admin interface or the PCD Upgrade task to perform the upgrade. **Caution** Performing an upgrade without sufficient disk space can cause the upgrade to fail.

	Command or Action	Purpose
Step 23	Obtain Upgrade Files, on page 78	Download the upgrade files for the Cisco Unified Communications Manager and the IM and Presence Service. For refresh upgrades, you must also download the upgrade COP files. Do this step for only for direct upgrades, which use either the Unified CM OS Admin interface or the PCD Upgrade task to perform the upgrade.
Step 24	Ensure that you have the necessary license files for the new release.	Use the Cisco Prime License Manager to allocate and monitor the licenses for Cisco Unified Communications Manager, its applications and endpoints. See the *Cisco Prime License Manager User Guide* at http://www.cisco.com/c/en/us/support/cloud-systems-management/prime-license-manager/products-user-guide-list.html for information about generating and installing licenses. Do this step for all upgrade and migration methods. **Note** 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 25	Increase the Database Replication Timeout, on page 80	Optional. This procedure applies to the Cisco Unified Communications Manager publisher node only. Use this procedure when you upgrade large clusters. If you increase the database replication timeout, you must 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. Do this step for only for direct upgrades, which use either the Unified CM OS Admin interface or the PCD Upgrade task to perform the upgrade.
Step 26	Disable High Availability on Presence Redundancy Groups, on page 80	This procedure applies to IM and Presence Service nodes only. If you have configured presence redundancy groups for high availability, you must disable it during the upgrade process.

	Command or Action	Purpose
		Do this step for only for direct upgrades, which use either the Unified CM OS Admin interface or the PCD Upgrade task to perform the upgrade.
Step 27	Add a Serial Port to the Virtual Machine, on page 81	Add a serial port to the virtual machine so that you can dump logs in the event of an upgrade failure. Perform this procedure for all nodes. Do this step for all upgrade and migration methods.

Generate a Database Status Report

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

Procedure

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

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

Step 2 Select **System Reports**.

Step 3 Select the report for the node:

- To check database replication on a Unified Communications Manager node, select **Unified CM Database Status**.
- To check database replication on an IM and Presence Service node, select **IM and Presence Database Status**.

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

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

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

Check Database Replication

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

Procedure

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

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

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

Step 3 Execute the **utils dbreplication runtimestate** command to check if the database replication is active on the node.
The output lists all the nodes and if database replication is set up and in a good state, the **replication setup** value for each node is **2**.

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

Check Performance Reports

Procedure

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

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

Step 3 Click the **CallActivitiesRep** to open the Call Activities Report in a new tab and verify that the number of **Calls Attempted** is not too high for the capacity of the virtual machine. You can determine the threshold for the number of **Calls Attempted** by checking the recommendations for your system in the *Cisco Collaboration Systems Solution Reference Network Designs (SRND)* at http://www.cisco.com/goucsrnd.

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

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

- *Cisco Collaboration Systems Solution Reference Network Designs (SRND)* at http://www.cisco.com/goucsrnd.
- Collaboration Sizing Tool at http://tools.cisco.com/cucst. Partners can use this tool to evaluate a customer's configuration.

Run CLI Diagnostics

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

Procedure

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

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

Step 2 Execute the **utils diagnose test** command.
This command runs all diagnostic commands but does not attempt to fix problems. You can view a list of all the diagnostic commands by executing the **utils diagnose list** command.

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

Delete a Trust Certificate

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

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

Procedure

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

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

Step 3 Choose the filename of the certificate.

Step 4 Click **Delete**.

Step 5 Click **OK**.

Note If the certificate that you delete is of the type “tomcat-trust”, “CallManager-trust” or “Phone-SAST-trust”, the certificate is deleted across all servers in the cluster.

Regenerate a Certificate

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

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

Procedure

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

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

Step 3 Click **Generate**.

Step 4 Restart all services that are affected by the regenerated certificate. See the Related Topics section for more information about the certificate names and their descriptions.

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

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

What to Do Next

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

Related Topics

Certificate Names and Descriptions, on page 67

Certificate Names and Descriptions

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

Table 17: Certificate Names and Descriptions

Name	Description	Related Services
tomcat tomcat-ECDSA	This self-signed root certificate is generated during installation for the HTTPS node.	Tomcat and TFTP

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

Take a Fresh Backup

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

Perform this procedure for all upgrade and migration methods.

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

Before You Begin

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

  For each application, the entire version string must match. For example, if the IM and Presence database publisher node is at version 11.5.1.10000-1, then all IM and Presence subscriber nodes must be 11.5.1.10000-1, and you must create a backup file for version 11.5.1.10000-1.
- The backup process can fail due to non availability of space on a remote server or due to interruptions in the network connectivity. You need to start a fresh backup after addressing the issues that caused the backup to fail.

- Make sure that you have a record of the cluster security password. If the cluster security password changes after you complete this backup, you will need to know the password or you will not be able to use the backup file to restore your system.

Procedure

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

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

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

Step 4 Click **Start Backup.**

Back Up Custom Ringtones and Background Images

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

Procedure

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

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

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

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

Check Network Connectivity

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

Procedure

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

- From a remote system, use SSH to connect securely to the Cisco Unified Operating System. In your SSH client, enter your ssh *adminname@hostname* and enter your password.

- From a direct connection to the serial port, enter your credentials at the prompt that displays automatically.

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

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

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

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

Step 6 Check that DNS name resolution is working correctly:

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

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

Verify IPv6 Networking

This procedure applies to Cisco Unified Communications Manager nodes only.

Verify that 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.

Procedure

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

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

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

- *destination* is a valid IPv6 address or host name that you want to ping
- *count* is the number of times to ping the external server. The default is 4.

Check Connectivity between IM and Presence and Cisco Unified Communications Manager

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

Procedure

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

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

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

Collect Configuration and Login Information

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

Procedure

Step 1 Record the following information about your network configuration:

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

Step 2 Record the following login and password information:

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

Record the Registered Device Count

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

Procedure

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

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

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

Record the Number of Assigned Users

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

Procedure

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

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

Record TFTP Parameters

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

Procedure

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

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

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

Step 4 Click **Advanced**.

Step 5 Click **Save**.

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

Record Enterprise Parameters

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

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

Procedure

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

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

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

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

Export User Records

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

Procedure

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

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

Step 3 Click **Next**.

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

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

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

Step 7 Click **Submit**.

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

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

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

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

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

Upgrade IP Phone Firmware

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

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

Before You Begin

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

Procedure

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

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

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

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

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

Step 6 Check that you received a success message.

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

Step 7 Stop and restart the TFTP server.

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

Step 9 From Cisco Unified CM Administration, choose **Device** > **Device Settings** > **Device Defaults** and manually change the name of the load file (for specific devices) to the new load.

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

Verify Critical Services

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

Procedure

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

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

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

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

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

Deactivate Cisco Extension Mobility and TFTP Services

Use this procedure to stop Cisco extension mobility and TFTP services on Cisco Unified Communications Manager nodes before you begin an upgrade.

Procedure

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

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

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

Step 4 Click **Stop**.

Step 5 Repeat Steps 2 and 3 for each node that is running **Cisco Extension Mobility** or **Cisco TFTP** services.

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

Stop the IM and Presence Sync Agent

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

Procedure

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

Step 2 Select an 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 **Stop**.

Check the Available Common Partition Space

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

Procedure

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

Step 2 View the tables on the bottom of the page and compare the **Total Space** to the **Used Space** for the common partition. You need a minimum 25G of available common partition space before you begin an upgrade.

Adjust High and Low Watermarks

Use this procedure to adjust the low and high watermarks to reduce the traces and remove unnecessary log files. After the upgrade, you must restore the high and low watermarks to their original values in order to

avoid premature purging of traces. The default value for the high watermark is 85. The default value for the low watermark is 80.

Procedure

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

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

Step 3 Select **Next**.

Step 4 Adjust the slider value to 30.

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

Step 6 Select **Next**.

Step 7 Adjust the slider value to 40.

Create Additional Partition Space

To create additional space in the common partition, you can perform one or more of the steps in this procedure. To download the COP files and the Readme files listed in this procedure, go to https://software.cisco.com and navigate to **Unified Communications** > **Call Control** > **Cisco Unified Communications Manager (CallManager)** > **<*Version*>** > **Unified Communications Manager/CallManager/Cisco Unity Connection Utilities**.

Procedure

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

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

Step 2 If you are upgrading from release 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.

Step 3 Perform this step only if the previous steps did not create enough disk space for the upgrade. Use the Free Common Space COP file (ciscocm.free_common_space_v<latest_version>.cop.sgn).
This COP file removes the inactive side in the common partition to increase available disk space without requiring a system rebuild. Ensure that you review the Readme file that supports this COP file before you proceed.

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

Obtain Upgrade Files

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

Procedure

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

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

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

Step 3 Go to https://software.cisco.com and navigate to **Unified Communications** > **Call Control** > **Cisco Unified Communications Manager (CallManager)** > **<*Version*>** > **Unified Communications Manager/CallManager/Cisco Unity Connection Utilities** to download COP files for Cisco Unified Communications Manager.

Step 4 Go to https://software.cisco.com and navigate to **Unified Communications** > **Unified Communications Applications** > **Presence Software** > **Unified Communications Manager IM and Presence Service** > **<*Version*>** > **Unified Presence Service (CUP) Updates** and select **UTILS** to download COP files for IM and Presence Service.

COP Files Required for Upgrades to Release 11.5(1)

The tables below lists the upgrade paths that require COP files. You must install COP files on each node before you begin an upgrade using the Cisco Unified OS Admin interface, or before you begin an upgrade or migration using the Prime Collaboration Deployment (PCD) tool. If you are using PCD, you can perform a bulk installation of the COP files before you begin the upgrade.

Table 18: Required COP Files for Upgrades and Migrations to Cisco Unified Communications Manager Release 11.5(1)

From	To	Upgrade Type
Releases prior to and including 8.5(x)	11.5(1)	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)	11.5(1)	Refresh upgrade. Required COP files: • ciscocm.version3-keys.cop.sgn Optional COP files: • ciscocm.vmware-disk-size-reallocation-<latest_version>.cop.sgn) • ciscocm.free_common_space_v<latest_version>.cop.sgn
9.1(x)	11.5(1)	Refresh upgrade. Required COP files: • ciscocm.version3-keys.cop.sgn Optional COP files: • ciscocm.vmware-disk-size-reallocation-<latest_version>.cop.sgn) • ciscocm.free_common_space_v<latest_version>.cop.sgn
10.5(x)	11.5(1)	Standard upgrade; no COP file required.
11.0(x)	11.5(1)	Standard upgrade; no COP file required.
11.5(1)	11.5(x)	Standard upgrade; no COP file required.

Table 19: Required COP Files for Refresh Upgrades from Cisco Unified Presence Releases

From Cisco Unified Presence Release	To IM and Presence Release	Upgrade Type
8.5(4) through 8.6(1)	11.5(1)	Refresh upgrade. Requires the following COP files: • cisco.com.cup.refresh_upgrade_v<latest_version>.cop • ciscocm.version3-keys.cop.sgn

Table 20: Required COP Files for Refresh Upgrades from IM and Presence Service Releases

From IM and Presence Release	To IM and Presence Release	Upgrade Type
9.1(x)	11.5(1)	Refresh upgrade. Requires the following COP file: • ciscocm.version3-keys.cop.sgn
10.5(x)	11.5(1)	Standard upgrade; no COP file required.
11.0(x)	11.5(1)	Standard upgrade; no COP file required.
11.5(1)	11.5(x)	Standard upgrade; no COP file required.

Increase the Database Replication Timeout

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

Increase the database replication timeout value when you upgrade 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.

Procedure

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

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

Step 2 Execute the **utils dbreplication setrepltimeout** *timeout* command, where *timeout* is database replication timeout, in seconds. Ensure that the value is between 300 and 3600.
The default database replication timeout value is 300 (5 minutes).

Disable High Availability on Presence Redundancy Groups

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

Procedure

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

Step 2 Enter the presence redundancy group search parameters and then click **Find**.

Step 3 From the search results, select the presence redundancy group that you want to disable.

Step 4 On the Presence Redundancy Group Configuration window, uncheck the **Enable High Availability** check box.

Step 5 Click **Save**.

Add a Serial Port to the Virtual Machine

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

Procedure

Step 1 Power off the virtual machine.

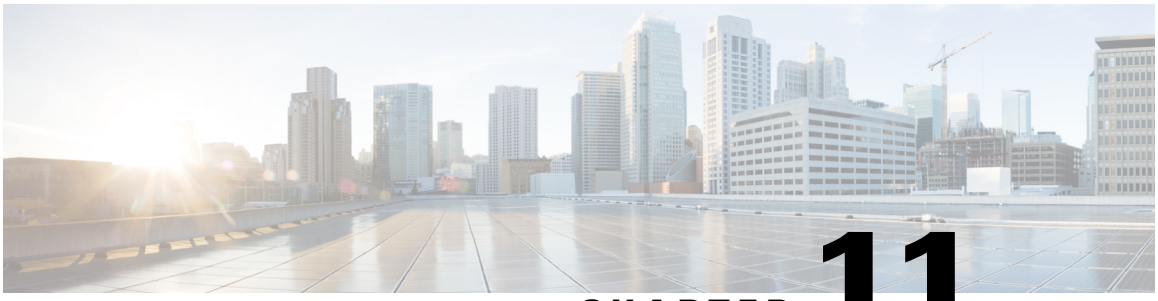
Step 2 Edit the settings to add a serial port. For more information about making configuration changes using vSphere Client, refer to the user manual for the product.

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

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

What to Do Next

After you successfully upgrade the system, follow the procedure to Remove the Serial Port, on page 98. In the event of an upgrade failure, refer to Dump a Log File After an Upgrade Failure, on page 113.



CHAPTER 11

Upgrade Procedures

- Upgrade Overview, page 83
- Before You Begin, page 86
- Upgrade Task Flow, page 86
- Upgrade the Applications, page 87
- Version Switching, page 90
- Switch to Previous Version, page 91
- Verify that Database Replication is Functioning, page 93
- Verify that Database Replication is Complete, page 94

Upgrade Overview

Use the procedures in this chapter to perform an upgrade using the Unified CM OS Administration interface.

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.

Understanding Version Switching

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

- automatic switching—the system switches the version automatically as part of the upgrade process
- manual switching—you switch the version using the OS Administration interface after the upgrade process is complete

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

Upgrade type	Switching type	When prompted, choose . . .	Result
Standard upgrade	Automatic	Reboot to upgraded partition	When you choose this option, the system reboots to the new software version.
	Manual	Do not reboot after upgrade	When you choose this option, the system continues to run the old software version when the upgrade is complete. You can manually switch to the new software at a later time.

Upgrade type	Switching type	When prompted, choose . . .	Result
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 use this upgrade method, you must switch your publisher node to the new software version before you upgrade your subscriber nodes.

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.

Before You Begin

Caution Stop all configuration tasks. Do not make any configuration changes during an upgrade. For example, do not change passwords, perform LDAP synchronizations, or run any automated jobs. Do not remove, re-add, or re-install any nodes in the cluster during the upgrade process. You can make configuration changes only when you have completed the upgrade on all nodes and 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 Cisco Unified Communications Manager nodes and all IM and Presence Service nodes.

- Review the pre-installation tasks and ensure that you have performed all the steps.
- Do not rename the upgrade file before you install it because the system will not recognize it as a valid file.
- Do not decompress the file. If you do, the system may not be able to read the upgrade file.
- For upgrades to the IM and Presence Service software, check that the contact list size for users has not reached the maximum value. The System Troubleshooter in Cisco Unified CM IM and Presence Administration indicates if there are users who have reached the contact list limit.

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.

Upgrade Task Flow

Procedure

	Command or Action	Purpose
Step 1	Upgrade the application using one of the following procedures: • Upgrade From a Local Source, on page 87 • Upgrade From a Remote Source, on page 89	Use these procedures when you upgrade Cisco Unified Communications Manager or the IM and Presence Service using the Unified CM OS Administration interface.
Step 2	Switch the Software Version, on page 90	Use this procedure to activate the new software.

	Command or Action	Purpose
Step 3	Switch to Previous Version, on page 91	Use the procedures in this section if you need to revert to the software version that was running before the upgrade.
Step 4	Verify that Database Replication is Functioning, on page 93	
Step 5	Verify that Database Replication is Complete, on page 94	

Upgrade the Applications

You can access the upgrade file during the installation process from either a local CD or 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.

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

Upgrade From a Local Source

Follow this procedure to upgrade to a new release of Unified Communications Manager or the IM and Presence 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
- Export unrestricted software has a XU license SKU.
- Export restricted software has a K9 licence 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 node, log in to Cisco Unified IM and Presence Operating System Administration.
- If you are upgrading a Cisco 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 need to install a COP file, review the information about supported upgrade paths. See the Related Topics section below 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 will enable 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:

- 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 allows you to install the upgrade and then manually reboot to the upgraded software at a later time. For more information about how to manually reboot the system and activate the upgrade, see the Related Topics section below.

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 the Related Topics section below for more information about the rules for switching during an upgrade.

Step 13 Select **Next** and select **Finish** when the installation completes.

Upgrade From a Remote Source

Follow this procedure to upgrade to a new release of Cisco Cisco Unified Communications Manager or the IM and Presence Service using software from a network drive or remote node. The network drive or remote node must be running an SFTP/FTP server that can be 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
- Export unrestricted software has a XU license SKU.
- Export restricted software has a K9 licence 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 node, log in to Cisco Unified IM and Presence Operating System Administration.
- If you are upgrading a Cisco 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 need to install a COP file, review the information about supported upgrade paths. See the Related Topics section below 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 user name 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 will enable 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 Monitor the progress of the download, which includes the filename and the number of megabytes that are being transferred.

Step 15 When the download completes, verify the checksum value against the checksum for the file that you downloaded from Cisco.com.

Step 16 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 allows you to install the upgrade and then manually reboot to the upgraded software at a later time. For more information about how to manually reboot the system and activate the upgrade, see the Related Topics section below.

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 17 Select **Next** and select **Finish** when the installation completes.

Version Switching

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.

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 Cisco Unified Communications Manager and IM and Presence nodes must match according to the manual switching rules. Therefore, you must switch Unified Communications Manager before you switch IM and Presence.

Review the information in Understanding Version Switching, on page 84

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 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.

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

Verify that Database Replication is Functioning

Use Cisco Unified Reporting to generate Database Status reports for Cisco Unified Communications Manager and IM and Presence Service nodes. You can use the reports to confirm that you have a database replication with no errors.

Before You Begin

Ensure that the Cisco Tomcat service is running.

Procedure

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

- For Unified Communications Manager nodes, log in to the Cisco Unified Reporting interface.

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

Step 2 Select **System Reports**.

Step 3 Select the report for the node:

- To check database replication on a Unified Communications Manager node, select **Unified CM Database Status**.
- To check database replication on an IM and Presence Service node, select **IM and Presence Database Status**.

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

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

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

Verify that Database Replication is Complete

Use this procedure to verify that the database replication has completed successfully. Replication takes 30 minutes on average, but it may take longer depending on the size of the database.

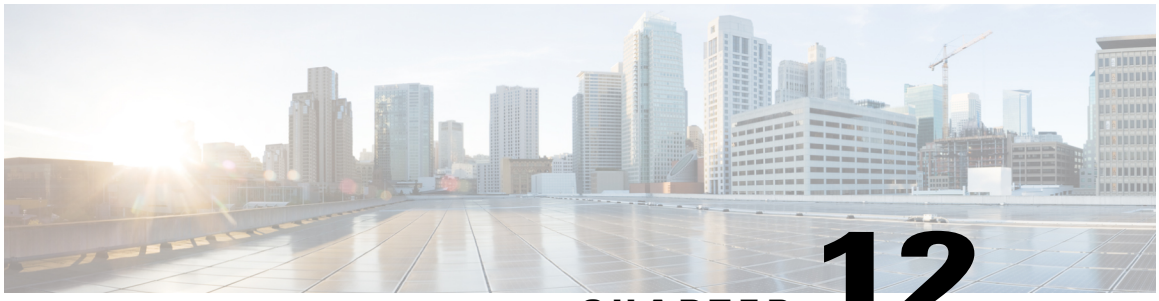
Procedure

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 runtimestate** command to monitor whether the database replication is active on the node and to view the progress of the database setup.
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 nodes until replication is complete.



CHAPTER 12

Post-upgrade Tasks

- Post-upgrade Task Flow, page 95

Post-upgrade Task Flow

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

Procedure

	Command or Action	Purpose
Step 1	Switch the Software Version, on page 97	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. Perform this procedure for all nodes.
Step 2	Remove the Serial Port, on page 98	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. Perform this procedure for all nodes.
Step 3	Restart Extension Mobility and TFTP Services, on page 98	Use this procedure to restart Cisco extension mobility and TFTP services on Cisco Unified Communications Manager nodes after you complete an upgrade.
Step 4	Reset TFTP Parameters, on page 99	Reset TFTP parameters that are changed during the upgrade process.
Step 5	Restore Enterprise Parameters, on page 99	Use this procedure to restore Enterprise Parameters on IM and Presence Service nodes that may have been overwritten during the upgrade process.
Step 6	Reset High and Low Watermarks, on page 100	Use this procedure to restore the high and low watermarks to their original values in order to avoid premature purging of traces.

	Command or Action	Purpose
		Do this step for only for direct upgrades, which use either the Unified CM OS Admin interface or the PCD Upgrade task to perform the upgrade.
Step 7	Update VMWare Tools, on page 100	You must update the VMWare Tools after you complete the upgrade. Perform this procedure for all nodes.
Step 8	Install Locales, on page 101	Use this procedure to install locales. After an upgrade, you must reinstall any locales that you are using, with the exception of US-English, which is installed by default. Perform this procedure for all nodes.
Step 9	Restore the Database Replication Timeout, on page 102	Use this procedure if you increased the database replication timeout value before you began the upgrade process. Perform this procedure on Cisco Unified Communications Manager nodes only.
Step 10	Verify the Registered Device Count, on page 103	Use this procedure to verify your endpoints and resources on Cisco Unified Communications Manager nodes after the upgrade is complete.
Step 11	Verify Assigned Users, on page 103	Use this procedure to verify the number of assigned users on IM and Presence Service nodes after the upgrade is complete.
Step 12	Test Functionality, on page 103	Verify phone functions and features are working correctly after the upgrade.
Step 13	Upgrade RTMT, on page 104	If you use Cisco Unified Real Time Monitoring Tool (RTMT), upgrade to the new software version.
Step 14	Manage TFTP Server Files, on page 105	Optional. Use this procedure to upload phone rings, callback tones, and backgrounds to a TFTP server so that they are available to Cisco Unified Communications Manager nodes.
Step 15	Set Up a Custom Log-On Message, on page 106	Optional. Upload a text file that contains a customized log-on message that appears in Cisco Unified Communications Operating System Administration, Cisco Unified CM Administration, Cisco Unified Serviceability, Disaster Recovery System Administration, Cisco Prime License Manager, and the command line interface. Perform this procedure on Cisco Unified Communications Manager nodes only.
Step 16	Configure IPSec Policies, on page 107	Use this procedure only if you are performing a PCD migration from Release 6.1(5). You must recreate your IPSec policies after the PCD migration is complete, because IPSec policies from Release 6.1(5) are not migrated to the new release.
Step 17	Assign New Manager Assistant Roles, on page 107	Perform this procedure only if your previous release was configured to use the Cisco Unified Communications Manager

	Command or Action	Purpose
		Assistant feature, and you assigned application users to use either the InterCluster Peer-User or the Admin-CUMA roles. The InterCluster Peer-User and Admin-CUMA roles are deprecated and are removed during the upgrade process. You must assign new roles for those users. Perform this procedure on Cisco Unified Communications Manager nodes only.
Step 18	Verify IM and Presence Service Data Migration, on page 108	Use this procedure only if you performed an upgrade or migration from Cisco Unified Presence Release 8.x to an IM and Presence Service release.
Step 19	Enable High Availability on Presence Redundancy Groups, on page 108	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.
Step 20	Restart the IM and Presence Sync Agent, on page 109	If you stopped the IM and Presence Sync Agent service before you began the upgrade process, restart it now.

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 Cisco Unified Communications Manager and IM and Presence nodes must match according to the manual switching rules. Therefore, you must switch Unified Communications Manager before you switch IM and Presence.

Review the information in Understanding Version Switching, on page 84

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 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.

Remove the Serial Port

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

Procedure

Step 1 Power off the virtual machine.

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

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

Restart Extension Mobility and TFTP Services

Use this procedure to restart Cisco extension mobility and TFTP services on Cisco Unified Communications Manager nodes after you complete an upgrade.

Procedure

	Command or Action	Purpose
Step 1	From Cisco Unified Serviceability, choose **Tools** > **Service Activation**.	
Step 2	From the **Server** list, choose the node on which you want to deactivate services and click **Go**.	

	Command or Action	Purpose
Step 3	Select the **Cisco Extension Mobility** and **Cisco TFTP** services.	
Step 4	Click **Restart**.	

Reset TFTP Parameters

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

Procedure

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

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

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

Step 4 Click **Advanced**.

Step 5 Click **Save**.

Step 6 Set the **Maximum Serving Count** to the same value that you used prior to the upgrade, or to the value that is recommended for your configuration.
The default value is 500. We recommend that you use the default value if you run the TFTP service with other Cisco CallManager services on the same server. For a dedicated TFTP server, use the following values:

- 1500 for a single-processor system
- 3000 for a dual-processor system
- 3500 for dedicated TFTP servers with higher CPU configurations

Restore Enterprise Parameters

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

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

Before You Begin

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

Procedure

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

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

Step 3 Click **Save**.

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

Reset High and Low Watermarks

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

Procedure

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

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

Step 3 Select **Next**.

Step 4 Adjust the slider value to 80.

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

Step 6 Select **Next**.

Step 7 Adjust the slider value to 85.

Update VMWare Tools

You must update the VMWare Tools after you complete the upgrade.

Procedure

Choose one of the following options:

- initiate the automatic tools update through the viClient
- 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. You can also find more information by searching on the topic "VMWare Tools" at http://www.cisco.com/go/uc-virtualized.

Install Locales

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

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

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

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

Procedure

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

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

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

- User Locale files—These files contain language information for a specific language and country and use the following convention:
  - `cm-locale-language-country-version.cop` (Cisco Unified Communications Manager)
  - `ps-locale-language_country-version.cop` (IM and Presence Service)
- Combined Network Locale file—Contains country-specific files for all countries for various network items, including phone tones, annunciators, and gateway tones. The combined network locale file uses the following naming convention:
  - `cm- locale-combinednetworklocale-version.cop` (Cisco Unified Communications Manager)

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

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

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

- For the **Source**, choose **Remote file System**.

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

Step 6 Click **Next**.

Step 7 Download and install the locale on the server.

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

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

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

Restore the Database Replication Timeout

This procedure applies to Cisco 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 Cisco Unified Communications Manager subscriber nodes have successfully set up replication.

Procedure

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

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

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

Verify the Registered Device Count

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

Procedure

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

Step 2 Record the number of registered devices:

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

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

Verify Assigned Users

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

Procedure

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

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

Test Functionality

After the upgrade, perform the following tasks:

- Verify phone functions by making the following types of calls:
  - Voice mail
  - Interoffice
  - Mobile phone

- Local
- National
- International
- Shared line

- Test the following phone features:
  - Conference
  - Barge
  - Transfer
  - C-Barge
  - Ring on shared lines
  - Do Not Disturb
  - Privacy
  - Presence
  - CTI call control
  - Busy Lamp Field

- Test IM and Presence Service functions:
  - Basic presence states, such as available, unavailable, and busy
  - Send and receive files
  - Advanced features, such as persistent chat, federated users, and message archiving

Upgrade RTMT

Tip To ensure compatibility, Cisco recommends that you upgrade RTMT after you complete the Cisco Unified Communications Manager upgrade on all servers in the cluster.

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

Before You Begin

Before you upgrade to a newer version of RTMT, Cisco recommends that you uninstall the previous version.

Procedure

Step 1 From Cisco Unified CM Administration, choose **Application** > **Plugins**.

Step 2 Click **Find**.

Step 3 Perform one of the following actions:

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

Step 4 Download the installation file to your preferred location.

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

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

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

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

Manage TFTP Server Files

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

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

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

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

Procedure

Step 1 From the Cisco Unified Communications Operating System Administration window, navigate to **Software Upgrades** > **TFTP** > **File Management**.
The TFTP File Management window displays and shows a listing of the current uploaded files. You can filter the file list by using the Find controls.

Step 2 To upload a file, follow this procedure:

a) Click **Upload File**.
The Upload File dialog box opens.

b) To upload a file, click **Browse** and then choose the file that you want to upload.

c) To upload the file to a subdirectory of the tftp directory, enter the subdirectory in the **Directory** field.

d) To start the upload, click **Upload File**.
The Status area indicates when the file uploads successfully.

e) After the file uploads, restart the Cisco TFTP service.
Note If you plan to upload several files, restart the Cisco TFTP service only once, after you have uploaded all the files.
For information about restarting services, refer to *Cisco Unified Serviceability Administration Guide*.

Step 3 To delete files, follow this procedure:

a) Check the check boxes next to the files that you want to delete.
You can also click **Select All** to select all of the files, or **Clear All** to clear all selection.

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

Set Up a Custom Log-On Message

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

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

Procedure

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

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

Step 3 Click **Upload File**.
Note You cannot upload a file that is larger than 10kB.
The system displays the customized log-on message.

Step 4 To revert to the default log-on message, click **Delete**.
Your customized log-on message gets deleted, and the system displays the default log-on message.

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

Configure IPSec Policies

Use this procedure only if you are performing a PCD migration from Release 6.1(5). You must recreate your IPSec policies after the PCD migration is complete, because IPSec policies from Release 6.1(5) are not migrated to the new release.

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

Procedure

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

Step 2 Click **Add New**.

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

Step 4 Click **Save**.

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

Assign New Manager Assistant Roles

Perform this procedure only if your previous release was configured to use the Cisco Unified Communications Manager Assistant feature, and you assigned application users to use either the InterCluster Peer-User or the Admin-CUMA roles. The InterCluster Peer-User and Admin-CUMA roles are deprecated from release 10.0(1) onward and are removed during the upgrade process. You must assign new roles for those users.

Procedure

Step 1 To configure roles and users, see the chapter "Manage Users" in the *Administration Guide for Cisco Unified Communications Manager and IM and Presence Service* at http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html.

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

Verify IM and Presence Service Data Migration

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

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 Enter the presence redundancy group search parameters and then click **Find**.

Step 3 From the search results, select the presence redundancy group that you want to enable.

Step 4 On the Presence Redundancy Group Configuration window, select the **Enable High Availability** check box.

Step 5 Click **Save**.

Restart the IM and Presence Sync Agent

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

Procedure

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

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

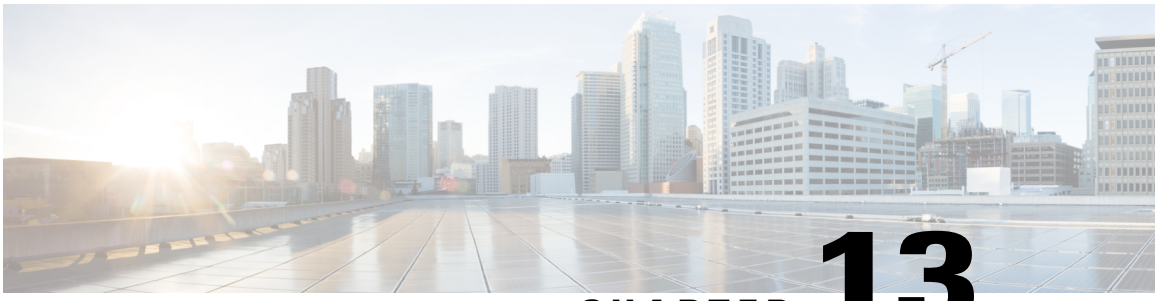
Step 3 In the **IM and Presence Services** section, select the **Cisco Sync Agent** and click **Restart**.

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

PART V

Troubleshooting

- Troubleshooting, page 113



CHAPTER 13

Troubleshooting

This section contains the following information:

- Dump a Log File After an Upgrade Failure, page 113
- Troubleshooting Unified Communications Manager Upgrades, page 114
- Troubleshooting IM and Presence Upgrades, page 116

Dump a Log File After an Upgrade Failure

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

Before You Begin

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

Procedure

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

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

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

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

Step 4 Select the datastore where you created the file.

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

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

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

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

- If the file size is 0, proceed to the next step.

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

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

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

Troubleshooting Unified Communications Manager Upgrades

This section provides information about troubleshooting Unified Communications Manager upgrades.

Upgrade Failure

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

Solution Do one of the following:

- Correct the errors that caused the upgrade failure on the subscriber node. You may want to check the network connectivity of the nodes in your cluster, reboot the subscriber node, and ensure that the server memory and CPU usage on the subscriber node is not too high. Upgrade the subscriber node again.
- Make sure that the active partition of the Unified Communications Manager publisher node runs the newest version of software installed on the server. Perform a fresh installation on the subscriber node using the same software version as that running on the active partition of the publisher node. If you are reinstalling the subscriber node, you should delete the server from Cisco Unified CM Administration and add the server again as described in the *Administration Guide for Cisco Unified Communications Manager*.

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**.

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 Cisco 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 Cisco 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 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 nodes, and the upgrade of the IM and Presence database publisher node fails.

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

- if the upgrade on the IM and Presence database publisher node fails before the refresh upgrade causes the node to reboot (that is, if the node failed before switching to the new partition), perform the upgrade again on the IM and Presence database publisher node
- If the failure occurred after the IM and Presence database publisher node switched to the new software version, you must switch back all the nodes and perform the upgrade again. Complete the following tasks in the order listed:
    - switch back the Unified Communications Manager publisher node
    - switch back the Unified Communications Manager subscriber nodes
    - switch back the IM and Presence database publisher node
    - upgrade the Unified Communications Manager publisher node again

- switch the Unified Communications Manager publisher node forward to the new software version
- upgrade the Unified Communications Manager subscriber nodes again
- switch the Unified Communications Manager subscriber nodes forward to the new software version
- upgrade the IM and Presence database publisher node again

Upgrade Failure of IM and Presence Subscriber Node

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

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

- if the upgrade on the IM and Presence subscriber node before the refresh upgrade causes the node to reboot (that is, if the node failed before switching to the new partition), perform the upgrade again on the IM and Presence subscriber node
- if the upgrade on the IM and Presence subscriber node fails after the node switched to the new version, you must complete the following tasks in the order listed:
  - switch the Unified Communications Manager publisher node back to the earlier software version
  - switch the Unified Communications Manager subscriber node back to the earlier software version
  - switch the IM and Presence database publisher node back to the earlier software version
  - switch the IM and Presence subscriber nodes back to the earlier software version
  - switch the Unified Communications Manager publisher node pub forward to the new software version
  - switch the IM and Presence database publisher node forward to the new software version
  - perform the upgrade again on the IM and Presence subscriber node

Upgrade From Pre Release 8.6(4) Fails

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

Solution The Cisco Unified Communications Manager hostname is case-sensitive. You must ensure that the entry for the Cisco Unified Communications Manager publisher node on the Cisco Unified Presence Administration interface matches exactly the Cisco 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 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 Cisco IM and Presence server, you cannot select the software image from the disk or remote directory. The following error is reported: `The version obtained from the name does not match the active or inactive version of the publisher.`

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

- The software version of the IM and Presence database publisher node (the first IM and Presence node that you upgrade) must match the first two numbers of the software version installed on the Unified Communications Manager publisher node. The software version installed on the Unified Communications Manager publisher node may be active or inactive. For example, 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.

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

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

Switch Version on Cisco IM and Presence Node Fails

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

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

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

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

Failed refresh upgrade

Problem A refresh upgrade failed.

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

Cancelled or failed upgrade

If you cancel an upgrade at any stage, or if an upgrade fails, you must reboot the IM and Presence 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 Cisco 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 Cisco Unified Communications Manager before proceeding with the upgrade.

Common Partition Full Upgrade Failure

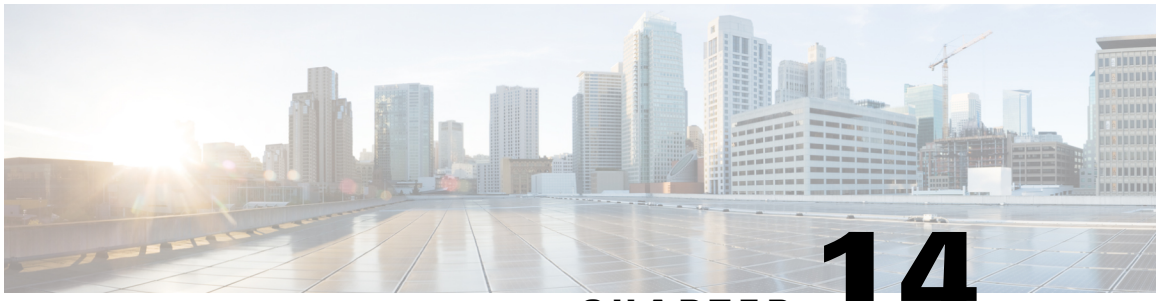
Problem The upgrade of IM and Presence Service fails with an error stating that the common partition is full.

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.

PART VI

Appendix

- Frequently Asked Questions, page 125
- Upgrading from Legacy Releases, page 129
- Additional Upgrade Resources, page 133



CHAPTER 14

Frequently Asked Questions

- Frequently Asked Questions, page 125

Frequently Asked Questions

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

Verify the requirements for the new release using the information below. After you have verified the requirements for the new release, see Change the Virtualization Software, on page 49 for instructions.

Table 21: Virtual Machine Requirements

Item	Description
OVA templates	OVA files provide a set of predefined templates for virtual machine configuration. They cover items such as supported capacity levels and any required OS/VM/SAN alignment. You must use a VM configuration from the OVA file provided for the Cisco Unified Communications Manager and IM and Presence applications. The correct VM configuration to use from the OVA file is based on the size of the deployment. For information about OVA files, search for the topic "Unified Communications Virtualization Sizing Guidelines" at http://www.cisco.com/go/uc-virtualized.
VMware vSphere ESXi	You must install a version of vSphere ESXi hypervisor that meets the compatibility and support requirements the release. If you use Cisco Prime Collaboration Deployment (PCD) to perform an upgrade or migration, you must also ensure that you install vSphere ESXi with the correct license type. PCD is not compatible with all the license types of vSphere ESXi because some of these licenses do not enable required VMware APIs.

Item	Description
VMware vCenter	VMware vCenter is optional when you deploy Cisco Unified Communications Manager or IM and Presence on Business Edition 6000/7000 appliances, or on UC on UCS tested reference configuration hardware. VMware vCenter is mandatory when you deploy on UC on UCS specs-based and third-party server specs-based hardware.
VM configuration virtual hardware specifications	Verify whether you need to change the virtual hardware specifications on your VM in order to upgrade to a new release of Unified Communications Manager or IM and Presence Service. For example, verify the requirements for vCPU, vRAM, vNIC adaptor type, and vDisk size, as well as other specifications. Any changes to a VM must align with the OVA configuration. VM changes that result in an unsupported OVA configuration are not allowed. For information about VM requirements, see the Readme file with the OVA template that supports your release.

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

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

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

Before you edit the VM configuration specifications, review the OVA ReadMe file to find the specific requirements for the release that you are upgrading to. OVA files provide a set of predefined templates for virtual machine configuration. They cover items such as supported capacity levels and any required OS/VM/SAN alignment. The correct VM configuration to use from the OVA file is based on the size of the deployment.

For information about OVA files, search for the topic "Unified Communications Virtualization Sizing Guidelines" at http://www.cisco.com/go/uc-virtualized.

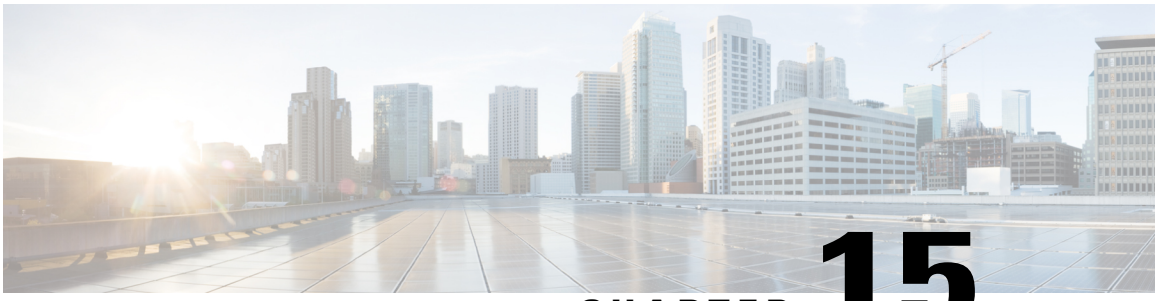
To obtain an OVA file, see Download and Install OVA Templates, on page 53.

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

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

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

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



CHAPTER 15

Upgrading from Legacy Releases

- Upgrading and Migrating from Legacy Releases, page 129

Upgrading and Migrating from Legacy Releases

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

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

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

If your starting release is not listed, it may require an upgrade to more than one intermediate release. See the "Supported Upgrade Paths To/From Table" at http://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/compat/ccmcompmatr1.html#pgfId-391518.

Table 22: Upgrade Paths for Legacy Releases

Installed Version	Upgrade to this Version on MCS hardware	Migrate to this Version on a Virtual Machine
Cisco Unified Communications Manager Releases		
4.x	Direct upgrade to 6.1(5), 7.1(3), or 7.1(5) using Cisco Unified Communications Manager Data Migration Assistant (DMA) Check the *Software Compatibility Matrix* for the intermediate release to find the supported upgrade path from your current release, or see the "Supported Upgrade Paths To/From Table" at the link above.	PCD Migration to 11.5(1)

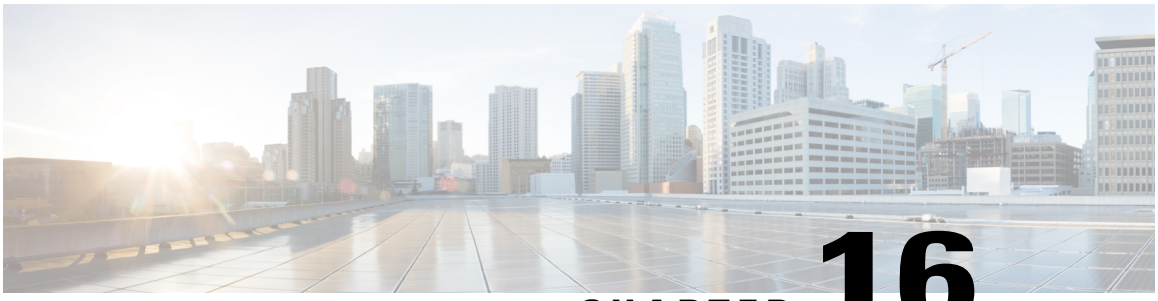
Installed Version	Upgrade to this Version on MCS hardware	Migrate to this Version on a Virtual Machine
5.1(2) 5.1(3) 6.0(x) 6.1(1) 6.1(2) 6.1(3) 6.1(4)	Direct Upgrade to 6.1(5) or 7.1(3)	PCD Migration to 11.5(1)
7.0(1) 7.1(2)	7.1(3), 7.1(5), 8.x, or 9.x	PCD Migration to 11.5(1)
Cisco Unified Presence Releases		
8.0(x)	Direct Upgrade to 8.5(4)	PCD Migration to 11.5(1)
Cisco Unified Communications Manager Business Edition Releases		
Business Edition 3000 (BE3000)	Upgrades and migrations are not supported for these deployments. We recommend that you perform a fresh installation for upgrades from these products to the current Cisco Unified Communications Manager release.	
Business Edition 5000 (BE5000)		

Procedure

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

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

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



CHAPTER 16

Additional Upgrade Resources

- Additional Upgrade Resources, page 133

Additional Upgrade Resources

Cisco Collaboration Systems Solution Reference Network Designs (SRND) for at http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-system/products-implementation-design-guides-list.html

Cisco Preferred Architecture guides and *Cisco Validated Design* guides at http://www.cisco.com/c/en/us/solutions/enterprise/design-zone-collaboration/index.html

Collaboration Virtual Machine Replacement Tool at http://ucs.cloudapps.cisco.com/

Cisco Collaboration Sizing Tool at http://tools.cisco.com/cucst