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 of data arising out of the use or inability to use this manual, even if Cisco or its suppliers have been advised of the possibility of such damages.

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

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

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

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: 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. (1721R)

© 2019 Cisco Systems, Inc. All rights reserved.
CONTENTS

PREFACE
Preface 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 5

CHAPTER 2
Understanding Upgrades and Migrations 7
Upgrade and Migration Overview 7
Upgrade Methods 7
Direct Upgrades 7
Standard upgrades 8
Refresh upgrades 8
Migrations 9
Upgrade and Migration Tools 9
Export Restricted and Export Unrestricted Software 9

PART II
Plan the Upgrade or Migration 13

CHAPTER 3
Determine the Scope of Work 15
CHAPTER 6  Deployment Types and Recommendations 33
  Type of Deployment 33
  Business Edition 6000 and Business Edition 7000 Deployments 33
  Virtualized Deployments of Cisco Unified Communications Manager and IM and Presence Service 33

CHAPTER 7  Sequencing Rules and Time Requirements 35
  Upgrade Sequence and Time Requirements 35
    Recommended Sequence for the Least Time 35
    Recommended Sequence for the Least Impact 37
  Sequence Rules 40
  Upgrade time requirements 41
    Factors that Affect Upgrade Time Requirements 41
  Estimating the Minimum Time Requirements 43
  Examples 45
    Example: Time Requirements for a Standard Upgrade in the Least Time 45
    Example: Time Requirements for a Refresh Upgrade in the Least Time 46
    Example: Time Requirements for a Standard Upgrade with the Least Impact 47
    Example: Time Requirements for a Refresh Upgrade with the Least Impact 48

CHAPTER 8  Find all Required Upgrade Documentation 49
  Additional Upgrade Documentation 49

PART III  Change the Virtualization Software 53

CHAPTER 9  Change the Virtualization Software 55
  Virtual Machine Configuration Tasks 55
    Install and Configure VMware vCenter 56
    Upgrade vSphere ESXi 57
  Download and Install OVA Templates 57
  Change Virtual Machine Configuration Specifications 58
  Migrate From Single to Multi-vDisk Virtual Machine 59
PART IV
Upgrade the Applications  61

CHAPTER 10
Pre-upgrade Tasks  63

Pre-Upgrade Task Flow  63
Generate a Database Status Report  69
Check Database Replication  69
Check Performance Reports  70
Run CLI Diagnostics  70
Delete a Trust Certificate  71
Regenerate a Certificate  71
Certificate Names and Descriptions  72
Take a Fresh Backup  73
Back Up Custom Ringtones and Background Images  74
Check Network Connectivity  74
Verify IPv6 Networking  75
Check Connectivity between IM and Presence and Cisco Unified Communications Manager  75
Collect Configuration and Login Information  75
Record the Registered Device Count  76
Record the Number of Assigned Users  77
Record TFTP Parameters  77
Record Enterprise Parameters  77
Export User Records  78
Upgrade IP Phone Firmware  78
Verify Critical Services  79
Deactivate Cisco Extension Mobility  80
Deactivate TFTP services  80
Stop the IM and Presence Sync Agent  80
Check the Available Common Partition Space  81
Adjust High and Low Watermarks  81
Maximize Usable Disk Space  81
Obtain Upgrade Files  83
COP Files Required for Upgrades to Release 11.5  84
Increase the Database Replication Timeout  85

Contents
CHAPTER 11

Upgrade Procedures 87

Upgrade Overview 87

Publisher Nodes and Subscriber Nodes 87

Understanding Version Switching 88

Before You Begin 89

Upgrade Task Flow 89

Upgrade the Applications 90

Upgrade from a Local Source 90

Upgrade from a Remote Source 91

Version Switching 93

Switch the Software Version 96

Switch to Previous Version 97

Switch Cluster to Previous Version 97

Switch Node to Previous Version 97

Reset Database Replication 98

Switch version back to Cisco Unified Presence 8.6(3) or earlier 98

Verify that Database Replication is Functioning 99

Verify that Database Replication is Complete 100

CHAPTER 12

Post-upgrade Tasks 101

Post-upgrade Task Flow 101

Switch the Software Version 103

Remove the Serial Port 104

Restart Extension Mobility 104

Restart TFTP Services 105

Reset TFTP Parameters 105

Restore Enterprise Parameters 105

Reset High and Low Watermarks 106

Updating VMware Tools 106

Install Locales 107

Restore the Database Replication Timeout 109
Verify the Registered Device Count 109
Verify Assigned Users 110
Test Functionality 110
Upgrade RTMT 111
Manage TFTP Server Files 112
Set Up a Custom Log-On Message 113
Configure IPSec Policies 113
Assign New Manager Assistant Roles 114
Verify IM and Presence Service Data Migration 114
Enable High Availability on Presence Redundancy Groups 115
Restart the IM and Presence Sync Agent 116

PART V
Troubleshooting 117

CHAPTER 13
Troubleshooting 119
Dump a Log File After an Upgrade Failure 119
Troubleshooting Unified Communications Manager Upgrades 120
Upgrade Failure 120
Upgrade Fails with Insufficient Disk Space 120
Download Failure in Cluster-Wide Upgrade 121
Reduced Permissions for Access Control Groups 121
Loss of Phone Settings 122
Post-Upgrade Failure of Unified Communications Manager Publisher Node 122
Post-Upgrade Failure of Unified Communications Manager Subscriber Nodes 122
Troubleshooting IM and Presence Upgrades 122
Upgrade Failure of IM and Presence Database Publisher Node 122
Upgrade Failure of IM and Presence Subscriber Node 123
Upgrade From Pre Release 8.6(4) Fails 124
IM and Presence user phone presence problems 124
Presence User Experiences Issues Obtaining Availability 124
Real-Time Monitoring Tool alert for Cisco SIP proxy service 124
Cannot find upgrade file on remote server 125
Upgrade file checksum values do not match 125
Database replication did not complete 125
Cisco UP Presence Engine database does not restart 125
Version Errors 125
Failed refresh upgrade 126
Cancelled or failed upgrade 127
Directory Was Located and Searched but No Valid Options or Upgrades Were Available 127
Common Partition Full Upgrade Failure 127
Preface

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

Audience

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

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

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

• Replacing a Single Server or Cluster for Unified Communications Manager
  This document describes how to replace a Unified Communications Manager server or a cluster of servers.

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

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

## Conventions

This document uses the following conventions:

<table>
<thead>
<tr>
<th>Convention</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>boldface</strong> font</td>
<td>Commands and keywords are in <strong>boldface</strong>.</td>
</tr>
<tr>
<td>italic font</td>
<td>Arguments for which you supply values are in italics.</td>
</tr>
<tr>
<td>[ ]</td>
<td>Elements in square brackets are optional.</td>
</tr>
<tr>
<td>{ x</td>
<td>y</td>
</tr>
<tr>
<td>[x</td>
<td>y</td>
</tr>
<tr>
<td>string</td>
<td>A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.</td>
</tr>
<tr>
<td><strong>screen</strong> font</td>
<td>Terminal sessions and information the system displays are in <strong>screen</strong> font.</td>
</tr>
<tr>
<td><strong>boldface</strong> screen</td>
<td>Information you must enter is in <strong>boldface</strong> <strong>screen</strong> font.</td>
</tr>
<tr>
<td>italic screen font</td>
<td>Arguments for which you supply values are in italic screen font.</td>
</tr>
<tr>
<td>Convention</td>
<td>Description</td>
</tr>
<tr>
<td>------------</td>
<td>-------------</td>
</tr>
<tr>
<td>^</td>
<td>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.</td>
</tr>
<tr>
<td>&lt; &gt;</td>
<td>Nonprinting characters, such as passwords, are in angle brackets.</td>
</tr>
</tbody>
</table>

Notes use the following conventions:

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

- **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:

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
How to Use this Guide

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

### Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Understanding Upgrades and Migrations, on page 5</td>
<td>Use the information in this section to understand:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• the differences between an upgrade and a migration</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• the upgrade methods that are available to you</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• the differences between export restricted and unrestricted software</td>
</tr>
<tr>
<td>Step 2</td>
<td>Plan the Upgrade or Migration, on page 13</td>
<td>Use the information in this section to plan your upgrade or migration:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 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.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• understand the system requirements and limitations.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• verify that your upgrade path is supported.</td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
<td></td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
<td></td>
</tr>
<tr>
<td>• review the deployment types and recommendations to see which upgrade or migration method we recommend for you.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• 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.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• gather the documentation that you need to complete the upgrade or migration.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Step 3**  
Change the Virtualization Software, on page 53  
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 61  
Use the information in this section when you are ready to begin to upgrade or migrate the Unified Communications Manager and the Instant Messaging 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 117  
Use the information in this section to troubleshoot problems that occur during the upgrade process.

**Step 6**  
Appendix, on page 129  
Use the information in this section to:

• review frequently asked questions.
<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• find out how to upgrade or migrate from a legacy release.</td>
</tr>
<tr>
<td></td>
<td>• find additional resources to help with the upgrade or migration process.</td>
</tr>
</tbody>
</table>
PART I

Understanding Upgrades and Migrations

• Understanding Upgrades and Migrations, on page 7
CHAPTER 2

Understanding Upgrades and Migrations

• Upgrade and Migration Overview, on page 7
• Upgrade Methods, on page 7
• Upgrade and Migration Tools, on page 9
• Export Restricted and Export Unrestricted Software, on page 9

Upgrade and Migration Overview

Use this section as a starting-point for planning your Unified Communications Manager or Instant Messaging and Presence upgrade.

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 Unified Communications Manager and Instant Messaging and Presence:

• Direct Upgrades, on page 7
• Migrations, on page 9

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.

**Note**

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

**Refresh upgrades**

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

**Note**

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

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

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

Following are tools available for upgrading or migrating Unified Communications Manager and Instant Messaging and Presence:

- **Unified CM OS Administration:** This interface is part of 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 Unified Communications Manager and Instant Messaging and Presence supports an export unrestricted (XU) version, in addition to the export restricted (K9) version.

---

**Note**

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

Export unrestricted versions differs from restricted versions as follows:

- Encryption of user payload (information exchange) is not supported.

- External SIP interdomain federation with Microsoft OCS/Lync or AOL is not supported.

- After you install an unrestricted release, you can never upgrade to a restricted version. A fresh install of a restricted version on a system that contains an unrestricted version is also not supported.

- All nodes within a single cluster must be in the same mode. For example, Unified Communications Manager and Instant Messaging and Presence 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 Instant Messaging and Presence.

<table>
<thead>
<tr>
<th>GUI Item</th>
<th>Location</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco Unified CM Administration</td>
<td></td>
<td></td>
</tr>
<tr>
<td>VPN Configuration</td>
<td>Advanced Features &gt; VPN</td>
<td>This menu and its options are not available.</td>
</tr>
<tr>
<td>Phone Security Profile Configuration</td>
<td>System &gt; Security &gt; Phone Security Profile</td>
<td>The Device Security Mode is set to Non Secure and is not configurable.</td>
</tr>
<tr>
<td>Cisco Unified CM IM and Presence Administration</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Security Settings</td>
<td>System &gt; Security &gt; Settings</td>
<td>• You cannot check the Enable XMPP Client to IM/P Service Secure Mode setting.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• You cannot check the Enable XMPP Router-to-Router Secure Mode setting.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• You cannot check the Enable Web Client to IM/P Service Secure Mode setting.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• The option to set SIP intra-cluster Proxy-to-Proxy Transport Protocol to TLS have been removed.</td>
</tr>
<tr>
<td>Service Parameter Configuration for Cisco SIP Proxy service</td>
<td>System &gt; Service Parameters and choose Cisco SIP Proxy as the Service</td>
<td>• All TLS options have been removed for the Transport Preferred Order parameter.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• The TLS option have been removed from the SIP Route Header Transport Type parameter.</td>
</tr>
<tr>
<td>GUI Item</td>
<td>Location</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>-----------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>SIP Federated Domains</td>
<td>Presence &gt; Inter-domain Federation &gt; SIP Federation</td>
<td>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.</td>
</tr>
<tr>
<td>XMPP Federation Settings</td>
<td>Presence &gt; Inter-domain Federation &gt; XMPP Federation &gt; Settings</td>
<td>You cannot configure the security mode; It is set to NO TLS.</td>
</tr>
<tr>
<td>Proxy Configuration Settings</td>
<td>Presence &gt; Routing &gt; Settings</td>
<td>You cannot set any TLS or HTTPS listeners as the preferred proxy listener.</td>
</tr>
</tbody>
</table>
PART II

Plan the Upgrade or Migration

• Determine the Scope of Work, on page 15
• Requirements and Limitations, on page 17
• Supported Upgrade and Migration Paths, on page 27
• Deployment Types and Recommendations, on page 33
• Sequencing Rules and Time Requirements, on page 35
• Find all Required Upgrade Documentation, on page 49
Determine the Scope of Work

- Determine the Scope of the Upgrade or Migration, on page 15

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

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1** | Determine whether you need to update the following components:  
- Hardware Requirements, on page 18  
- Virtual Machine Configuration, on page 19 | Ensure that your system meets the requirements of the new release. |
| **Step 2** | Verify the Supported Upgrade and Migration Paths, on page 27. | Use the information in this chapter 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 33 | 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 35 | 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 of time required to complete the upgrade. You |
### Command or Action

<table>
<thead>
<tr>
<th>Step 5</th>
<th>Find Additional Upgrade Documentation, on page 49.</th>
</tr>
</thead>
</table>

**Purpose**

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.

Find the correct upgrade documentation to use based on the needs of your deployment and the recommended upgrade or migration method.
Requirements and Limitations

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

⚠️ Caution

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

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

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

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

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

Network Requirements

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

IP Address Requirements

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

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

DNS requirements

Note the following requirements:

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

• If your deployment uses DNS—Unified Communications Manager and Instant Messaging and Presence should use the same DNS server. If you use different DNS servers between Instant Messaging and Presence and Unified Communications Manager, it is likely to cause abnormal system behavior.

• If your deployment does not use DNS, will need to edit the following Host Name/IP Address fields:
• Server—In the Cisco Unified CM Administration Server Configuration window, set IP addresses for your cluster nodes.

• IM and Presence UC Service—In the Cisco Unified CM Administration UC Service Configuration window, create an IM and Presence UC service that points to the IP address of the IM and Presence database publisher node.

• CCMCIP Profiles—In the Cisco Unified CM IM and Presence Administration CCMCIP Profile Configuration window, point any CCMCIP profiles to the IP address of the host.

• Multinode considerations—If you are using the multinode feature in Instant Messaging and Presence, see the section regarding multinode deployments in the Configuration and Administration of IM and Presence on Cisco Unified Communications Manager for DNS configuration options.

SFTP Server Support

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


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

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

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

• Open SSH (refer to http://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

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>OVA templates</td>
<td>OVA files provide a set of predefined templates for virtual machine configuration. They cover items such as supported capacity levels and any required OS/VM/SAN alignment. You must use a VM configuration from the OVA file provided for the Unified Communications Manager and Instant Messaging and Presence applications. The correct VM configuration to use from the OVA file is based on the size of the deployment. For information about OVA files, search for the topic &quot;Unified Communications Virtualization Sizing Guidelines&quot; at <a href="https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/uc_system/virtualization/collaboration-virtualization-sizing.html">https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/uc_system/virtualization/collaboration-virtualization-sizing.html</a>.</td>
</tr>
<tr>
<td>VMware vSphere ESXi</td>
<td>You must install a version of vSphere ESXi hypervisor that meets the compatibility and support requirements for the release. If you use Cisco Prime Collaboration Deployment (PCD) to perform an upgrade or migration, you must also ensure that you install vSphere ESXi with the correct license type. PCD is not compatible with all the license types of vSphere ESXi because some of these licenses do not enable required VMware APIs.</td>
</tr>
<tr>
<td>VMware vCenter</td>
<td>VMware vCenter is optional when you deploy Unified Communications Manager or Instant Messaging and Presence on Business Edition 6000/7000 appliances, or on UC on UCS tested reference configuration hardware. VMware vCenter is mandatory when you deploy on UC on UCS specs-based and third-party server specs-based hardware.</td>
</tr>
<tr>
<td>VM configuration virtual</td>
<td>Verify whether you need to change the virtual hardware specifications on your VM in order to upgrade to a new release of Unified Communications Manager or Instant Messaging and Presence. For example, verify the requirements for vCPU, vRAM, vNIC adaptor type, and vDisk size, as well as other specifications. Any changes to a VM must align with the OVA configuration. VM changes that result in an unsupported OVA configuration are not allowed. For information about VM requirements, see Readme file with the OVA template that supports your release.</td>
</tr>
<tr>
<td>hardware specifications</td>
<td></td>
</tr>
</tbody>
</table>

### VMware Upgrade Requirements

If the upgrade requires you to update your VMware, go to [Virtual Machine Configuration Tasks, on page 55](#).

### Browser Requirements

Unified Communications Manager and the Instant Messaging and Presence 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.
### Licensing Requirements

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

#### Cisco Unified Communications Manager License Requirements

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

**Important**

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

#### IM and Presence license requirements

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

**Note**

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

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

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

• The **End User Configuration** window in Unified Communications Manager. For more information, see Administration Guide for Cisco Unified Communications Manager.

• The Bulk Administration Tool (BAT)

• Assign Instant Messaging and Presence to a feature group template which you can reference from the **Quick User/Phone Add** window in Unified Communications Manager.

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

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

**Limitations**

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

**Subnet Limitations**

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

**Cluster Size**

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

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

For more information, see “Cisco Collaboration Solutions Design Guidance” at http://www.cisco.com/go/ucsrd

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

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

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 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.

Upgrade Requirements with Standalone Prime License Manager

Cisco Unified Communications Manager Release 11.5(1)SU3, SU4, SU5, and SU6 are compatible with Cisco Prime License Manager Release 11.5(1)SU2 or higher. If you are deploying a standalone Cisco Prime License Manager, make sure that your Prime License Manager version is a minimum release of 11.5(1)SU2. Otherwise, Cisco Unified Communications Manager cannot synchronize its license usage with the standalone Prime License Manager.

If you are upgrading to one of these Cisco Unified Communications Manager releases and you are running a standalone version of Prime License Manager, upgrade your Prime License Manager instance to 11.5(1)SU2 or higher before you upgrade Cisco Unified Communications Manager.

---

**Note**

With co-resident Prime License Manager deployments, Cisco Unified Communications Manager and Cisco Prime License Manager are compatible automatically.

---

Upgrades from 11.5(1)SU2 with Push Notifications Enabled

If you are upgrading from the 11.5(1)SU2 release and you had Push Notifications enabled in the old release, you must disable Push Notifications in the current release and then follow the onboarding process to enable Push Notifications once again. This is required due to API changes in this release that were not a part of the 11.5(1)SU2 release. Your upgraded system will not be able to send troubleshooting logs to the Cisco Cloud unless you disable Push Notifications and then follow the onboarding process for this release.

After you upgrade your system, do the following:

**Procedure**

---

**Step 1**

Disable Push Notifications

Follow these steps:
1. From Cisco Unified CM Administration, choose Advanced Features > Cisco Cloud Onboarding
2. Uncheck the following checkboxes:
   • Enable Push Notifications
   • Send Troubleshooting information to the Cisco Cloud
   • Send encrypted PII to the Cisco Cloud for troubleshooting
3. Click Save.

Step 2
Enable Push Notifications for this release.


Upgrade Requirements with Standalone Prime License Manager
Cisco Unified Communications Manager Release 11.5(1)SU3, SU4, SU5, and SU6 are compatible with Cisco Prime License Manager Release 11.5(1)SU2 or higher. If you are deploying a standalone Cisco Prime License Manager, make sure that your Prime License Manager version is a minimum release of 11.5(1)SU2. Otherwise, Cisco Unified Communications Manager cannot synchronize its license usage with the standalone Prime License Manager.

If you are upgrading to one of these Cisco Unified Communications Manager releases and you are running a standalone version of Prime License Manager, upgrade your Prime License Manager instance to 11.5(1)SU2 or higher before you upgrade Cisco Unified Communications Manager.

Note
With co-resident Prime License Manager deployments, Cisco Unified Communications Manager and Cisco Prime License Manager are compatible automatically.

Duplicate ENUMS Break Upgrades and Migrations from 9.1(2)
If you are upgrading or migrating from Release 9.1(2) of Cisco Unified Communications Manager to any 10.x, 11.x or 12.x release, an issue exists with older locale installations that causes upgrade and migration failures. This issue exists if you are using one of the following three locales, and your locale installer is dated prior to August 31, 2017;
   • pt-BR (Brazil)
   • en-GB (United Kingdom)
   • combined_network
To ensure that your upgrade does not fail, update your Unified Communications Manager and phone locale installation to use a locale that is dated after August 31, 2017 as this issue does not exist for any locale file issued after that date. After you update your locale installation, you can begin the upgrade or migration.
CHAPTER 5

Supported Upgrade and Migration Paths

- Version Requirements, on page 27
- Supported Upgrade and Migration Paths, on page 29

Version Requirements

For 11.x Versions up to 11.5(1)SU1

If you are installing IM and Presence nodes, the software version of the first IM and Presence node (the IM and Presence database publisher node) must match the first three numbers of the software version installed on the Unified Communications Manager publisher node. For example, IM and Presence Service software version 11.0.1.10000-1 is compatible with Unified Communications Manager software version 11.0.1.30000-2. Refer to the following table for sample Unified Communications Manager versions and IM and Presence Service versions that are compatible. The bolded numbers must match.

<table>
<thead>
<tr>
<th>Sample Unified Communications Manager Version</th>
<th>Example of Compatible IM and Presence Service Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.0.1.30000-2</td>
<td>11.0.1.10000-1</td>
</tr>
<tr>
<td>11.5.1.10000-6</td>
<td>11.5.1.10000-4</td>
</tr>
</tbody>
</table>

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.

Release 11.5(1)SU2

For Release 11.5(1)SU2, both Unified Communications Manager and IM and Presence Service must be running official 11.5(1)SU2 versions. Running an 11.5(1)SU2 version of Unified Communications Manager with an earlier version of IM and Presence Service is not supported. Similarly, running an 11.5(1)SU2 version of IM and Presence Service with an earlier version of Unified Communications Manager is not supported.

The following software versions are supported with Release 11.5(1)SU2:

- Unified Communications Manager 11.5.1.12900-21
• IM and Presence Service 11.5.1.12900-25

Release 11.5(1)SU3

For Release 11.5(1)SU3, both Unified Communications Manager and IM and Presence Service must be running official 11.5(1)SU3 versions. Running an 11.5(1)SU3 version of Unified Communications Manager with an earlier version of IM and Presence Service is not supported. Similarly, running an 11.5(1)SU3 version of IM and Presence Service with an earlier version of Unified Communications Manager is not supported.

The following software versions are supported with Release 11.5(1)SU3:

• Unified Communications Manager 11.5.1.13900-52
• Unified Communications Manager 11.5.1.13901-3
• Unified Communications Manager 11.5.1.13902-2
• IM and Presence Service 11.5.1.13900-57
• IM and Presence Service 11.5.1.13901-1

Release 11.5(1)SU4

The following versions are supported:

• Cisco Unified Communications Manager 11.5.1.14900-11
• IM and Presence Service 11.5.1.14900-32

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

• Standard Deployments (Decentralized)—In this deployment, both Cisco Unified Communications Manager and the IM and Presence Service must be running an 11.5(1)SU4 version for your deployment to be supported. A version mismatch is not supported.

• Centralized Deployments of the IM and Presence Service—Within the IM and Presence central cluster, both the IM and Presence Service and the Cisco Unified Communications Manager instance (this is primarily a database and provisioning instance, and does not handle telephony) must be running an 11.5(1)SU4 version. However, the remote telephony clusters to which the IM and Presence Service connects do not have to be running an 11.5(1)SU4 version.

Release 11.5(1)SU5

The following versions are supported:

• Cisco Unified Communications Manager 11.5.1.15900-18
• IM and Presence Service 11.5.1.15900-33

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

• Standard Deployments (Decentralized)—In this deployment, both Cisco Unified Communications Manager and the IM and Presence Service must be running an 11.5(1)SU5 version for your deployment to be supported. A version mismatch is not supported.

• Centralized Deployments of the IM and Presence Service—Within the IM and Presence central cluster, both the IM and Presence Service and the Cisco Unified Communications Manager instance (this is primarily a database and provisioning instance, and does not handle telephony) must be running an 11.5(1)SU5 version. However, the remote telephony clusters to which the IM and Presence Service connects do not have to be running an 11.5(1)SU5 version.
primarily a database and provisioning instance, and does not handle telephony) must be running an 11.5(1)SU5 version. However, the remote telephony clusters to which the IM and Presence Service connects do not have to be running an 11.5(1)SU5 version.

**Release 11.5(1)SU6**

The following versions are supported:

- Cisco Unified Communications Manager 11.5.1.16900-16
- IM and Presence Service 11.5.1.16910-12

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

- Standard Deployments (Decentralized)—In this deployment, both Cisco Unified Communications Manager and the IM and Presence Service must be running an 11.5(1)SU6 version for your deployment to be supported. A version mismatch is not supported.

- Centralized Deployments of the IM and Presence Service—Within the IM and Presence central cluster, both the IM and Presence Service and the Cisco Unified Communications Manager instance (this is primarily a database and provisioning instance, and does not handle telephony) must be running an 11.5(1)SU6 version. However, the remote telephony clusters to which the IM and Presence Service connects do not have to be running an 11.5(1)SU6 version.

### Supported Upgrade and Migration Paths

Use the following tables 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 "Upgrading from Legacy Releases" chapter of the Upgrade and Migration Guide for Cisco Unified Communications Manager and IM and Presence Service.

### Deployments on Cisco Media Convergence Servers 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 Cisco 7800 Series Media Convergence Server (MCS 7800) hardware. All of the supported migration paths listed below are physical-to-virtual (P2V) migrations.
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 4: Unified Communications Manager Releases Installed on MCS 7800 Series Hardware

<table>
<thead>
<tr>
<th>From</th>
<th>To</th>
<th>Supported Method</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1(5)</td>
<td>11.5(x)</td>
<td>PCD Migration</td>
</tr>
<tr>
<td>7.1(3) and 7.1(5)</td>
<td>11.5(x)</td>
<td>PCD Migration</td>
</tr>
<tr>
<td>8.x</td>
<td>11.5(x)</td>
<td>PCD Migration</td>
</tr>
<tr>
<td>9.x</td>
<td>11.5(x)</td>
<td>PCD Migration</td>
</tr>
</tbody>
</table>

### Table 5: Cisco Unified Presence and IM and Presence Releases Installed on MCS 7800 Series Hardware

<table>
<thead>
<tr>
<th>From</th>
<th>To</th>
<th>Supported Method</th>
</tr>
</thead>
<tbody>
<tr>
<td>CUP 8.5(4)</td>
<td>11.5(x)</td>
<td>PCD Migration</td>
</tr>
<tr>
<td>CUP 8.6(3), 8.6(4), and 8.6(5)</td>
<td>11.5(x)</td>
<td>PCD Migration</td>
</tr>
<tr>
<td>IM and Presence 9.x</td>
<td>11.5(x)</td>
<td>PCD Migration</td>
</tr>
</tbody>
</table>

## Deployments on Virtual Machines

The tables below list the supported upgrade and migration paths for Cisco Unified Communications Manager and IM and Presence Service deployments that are currently running on virtual machines. All of the supported upgrade and migration paths listed below are virtual-to-virtual (V2V). Service Updates (SU) within each path are supported, unless otherwise indicated.

### Table 6: Unified Communications Manager Releases Installed on Virtual Machines

<table>
<thead>
<tr>
<th>From</th>
<th>To</th>
<th>Supported Method</th>
</tr>
</thead>
</table>
| 8.6(x) | 11.5(x) | Cisco Unified OS Admin (Direct Refresh)  
PCD Migration  
PCD Upgrade (Direct Refresh) |
| 9.0(x) | 11.5(x) | PCD Migration  
PCD Upgrade (Direct Refresh) |
<table>
<thead>
<tr>
<th>From</th>
<th>To</th>
<th>Supported Method</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.1(x)</td>
<td>11.5(x)</td>
<td>PCD Migration</td>
</tr>
<tr>
<td></td>
<td></td>
<td>PCD Upgrade (Direct Refresh)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Cisco Unified OS Admin (Direct Refresh)</td>
</tr>
<tr>
<td>10.0(x)</td>
<td>11.5(x)</td>
<td>PCD Migration</td>
</tr>
<tr>
<td></td>
<td></td>
<td>PCD Upgrade (Direct Standard)</td>
</tr>
<tr>
<td>10.5(x)</td>
<td>11.5(x)</td>
<td>PCD Migration</td>
</tr>
<tr>
<td></td>
<td></td>
<td>PCD Upgrade (Direct Standard)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Cisco Unified OS Admin (Direct Standard)</td>
</tr>
<tr>
<td>11.0(1)</td>
<td>11.5(x)</td>
<td>Cisco Unified OS Admin (Direct Standard)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>PCD Migration</td>
</tr>
<tr>
<td></td>
<td></td>
<td>PCD Upgrade (Direct Standard)</td>
</tr>
<tr>
<td>11.5(x)</td>
<td>11.5(y)</td>
<td>Cisco Unified OS Admin (Direct Standard)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>PCD Migration</td>
</tr>
<tr>
<td></td>
<td></td>
<td>PCD Upgrade (Direct Standard)</td>
</tr>
</tbody>
</table>

Table 7: Cisco Unified Presence and IM and Presence Releases Installed on Virtual Machines

<table>
<thead>
<tr>
<th>From</th>
<th>To</th>
<th>Supported Method</th>
</tr>
</thead>
<tbody>
<tr>
<td>CUP 8.5(4)</td>
<td>11.5(x)</td>
<td>PCD Migration</td>
</tr>
<tr>
<td>CUP 8.6(3), 8.6(4), and 8.6(5)</td>
<td>11.5(x)</td>
<td>PCD Migration</td>
</tr>
<tr>
<td></td>
<td></td>
<td>PCD Upgrade (Direct Refresh)</td>
</tr>
<tr>
<td>CUP 8.6(x)</td>
<td>11.5(x)</td>
<td>Cisco Unified OS Admin (Direct Refresh)</td>
</tr>
<tr>
<td>IM and Presence 9.0(x)</td>
<td>11.5(x)</td>
<td>PCD Migration</td>
</tr>
<tr>
<td></td>
<td></td>
<td>PCD Upgrade (Direct Refresh)</td>
</tr>
<tr>
<td>IM and Presence 9.1(x)</td>
<td>11.5(x)</td>
<td>PCD Migration</td>
</tr>
<tr>
<td></td>
<td></td>
<td>PCD Upgrade (Direct Refresh)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Cisco Unified OS Admin (Direct Refresh)</td>
</tr>
<tr>
<td>IM and Presence 10.0(x)</td>
<td>11.5(x)</td>
<td>PCD Migration</td>
</tr>
<tr>
<td></td>
<td></td>
<td>PCD Upgrade (Direct Standard)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>PCD Upgrade (Direct Standard)</td>
</tr>
</tbody>
</table>
Upgrade Path Restrictions for Release 11.5(x)

Upgrade and migration paths generally support the Service Updates (SU) within each path; however, there are some exceptions for specific SU releases. The table below lists the exceptions for upgrades and migrations to Cisco Unified Communications Manager Release 11.5(x).

Table 8: Restrictions to Supported Upgrade and Migration Paths, Cisco Unified Communications Manager Release 11.5(x)

<table>
<thead>
<tr>
<th>From</th>
<th>To</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IM and Presence 10.5(x)</td>
<td>11.5(x)</td>
<td>Path is unsupported. For these releases, upgrade to 11.5(1)SU2 instead.</td>
</tr>
<tr>
<td>IM and Presence 11.0(1)</td>
<td>11.5(x)</td>
<td>Cisco Unified OS Admin (Direct Standard)</td>
</tr>
<tr>
<td>IM and Presence 11.5(x)</td>
<td>11.5(y)</td>
<td>Cisco Unified OS Admin (Direct Standard)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>From</th>
<th>To</th>
<th>Supported Method</th>
</tr>
</thead>
<tbody>
<tr>
<td>IM and Presence 10.5(x)</td>
<td>11.5(x)</td>
<td>PCD Migration</td>
</tr>
<tr>
<td>IM and Presence 11.0(1)</td>
<td>11.5(x)</td>
<td>PCD Upgrade (Direct Standard)</td>
</tr>
<tr>
<td>IM and Presence 11.5(x)</td>
<td>11.5(y)</td>
<td>PCD Migration (Direct Standard)</td>
</tr>
</tbody>
</table>

Upgrade Path Restrictions for Release 11.5(x)

Upgrade and migration paths generally support the Service Updates (SU) within each path; however, there are some exceptions for specific SU releases. The table below lists the exceptions for upgrades and migrations to Cisco Unified Communications Manager Release 11.5(x).

Table 8: Restrictions to Supported Upgrade and Migration Paths, Cisco Unified Communications Manager Release 11.5(x)

<table>
<thead>
<tr>
<th>From</th>
<th>To</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.5(2)SU5</td>
<td>11.5(1.10000-6) through 11.5(1.120xx)</td>
<td>Path is unsupported. For these releases, upgrade to 11.5(1)SU2 instead.</td>
</tr>
</tbody>
</table>
Deployment Types and Recommendations

Type of Deployment

Use the information in this section after you have reviewed the tables in the Supported Upgrade and Migration Paths, on page 27 chapter. 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 Unified Communications Manager and Instant Messaging and Presence, 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, on page 35
- Upgrade time requirements, on page 41

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 35
- Recommended Sequence for the Least Impact, on page 37

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 40

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 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 Unified Communications Manager nodes. You can perform upgrade procedures on the Instant Messaging and Presence nodes in parallel with 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 Instant Messaging and Presence nodes, you must reboot all Instant Messaging 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 7.

**Table 9: Recommended Sequence for Performing Refresh Upgrades in the Least Amount of Time**

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

**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 10: Recommended Sequence for Performing Standard Upgrades in the Least Amount of Time

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

**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 Unified Communications Manager nodes. You can perform upgrade procedures on the Instant Messaging and Presence nodes in parallel with 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 Instant Messaging and Presence nodes, you must reboot all IM and Presence nodes after the Unified Communications Manager upgrade is complete.
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" at System Configuration Guide for Cisco Unified Communications Manager.

**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 11: Recommended Sequence for Performing Refresh Upgrades with the Least Impact*

<table>
<thead>
<tr>
<th>Sequence</th>
<th>Unified Communications Manager Nodes</th>
<th>IM and Presence Service Nodes</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Upgrade the publisher node to the new software version. The new software is inactive.</td>
<td>—</td>
</tr>
<tr>
<td>2</td>
<td>Verify that phones are registered to primary subscriber nodes in CMGs. Upgrade the secondary subscriber nodes. The new software is inactive.</td>
<td>Upgrade the Instant Messaging and Presence database publisher node in parallel with the Unified Communications Manager subscriber nodes.</td>
</tr>
<tr>
<td>3</td>
<td>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.</td>
<td>Upgrade the subscriber nodes. The new software is inactive.</td>
</tr>
<tr>
<td>4</td>
<td>Switch the software version on the publisher node and reboot it. The new software is active.</td>
<td>—</td>
</tr>
<tr>
<td>5</td>
<td>Switch the software version on the secondary subscriber nodes in parallel and reboot them. The new software is active.</td>
<td>—</td>
</tr>
<tr>
<td>6</td>
<td>Ensure that database replication is complete and functioning between the publisher node and all secondary subscriber nodes.</td>
<td>—</td>
</tr>
<tr>
<td>7</td>
<td>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.</td>
<td>—</td>
</tr>
<tr>
<td>8</td>
<td>Ensure that database replication is complete and functioning between the publisher node and all primary subscriber nodes.</td>
<td>—</td>
</tr>
<tr>
<td>Sequence</td>
<td>Unified Communications Manager Nodes</td>
<td>IM and Presence Service Nodes</td>
</tr>
<tr>
<td>----------</td>
<td>-------------------------------------</td>
<td>------------------------------</td>
</tr>
<tr>
<td>9</td>
<td>—</td>
<td>Switch the software version on the database publisher node and reboot it. The new software is active.</td>
</tr>
<tr>
<td>10</td>
<td>—</td>
<td>Switch the software version on the subscriber nodes in parallel and reboot them. The new software is active.</td>
</tr>
<tr>
<td>11</td>
<td>—</td>
<td>Ensure that database replication is complete and functioning between the publisher node and all subscriber nodes.</td>
</tr>
</tbody>
</table>

**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 12: Recommended Sequence for Performing Standard Upgrades with the Least Impact**

<table>
<thead>
<tr>
<th>Sequence</th>
<th>Unified Communications Manager Nodes</th>
<th>IM and Presence Service Nodes</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Upgrade the publisher node to the new software version. The new software is inactive.</td>
<td>—</td>
</tr>
<tr>
<td>2</td>
<td>Upgrade the primary and secondary subscriber nodes. The new software is inactive.</td>
<td>Upgrade the Instant Messaging and Presence database publisher node in parallel with the Unified Communications Manager subscriber nodes. The new software is inactive.</td>
</tr>
<tr>
<td>3</td>
<td>—</td>
<td>Upgrade the subscriber nodes. The new software is inactive.</td>
</tr>
<tr>
<td>4</td>
<td>Switch the software version on the publisher node and reboot it.</td>
<td>—</td>
</tr>
<tr>
<td>5</td>
<td>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.</td>
<td>Switch the software version on the database publisher node and reboot it.</td>
</tr>
<tr>
<td>6</td>
<td>Ensure that database replication is complete and functioning between the publisher node and all secondary subscriber nodes.</td>
<td>Switch the software version on the subscriber nodes in parallel and reboot them. The new software is active.</td>
</tr>
<tr>
<td>7</td>
<td>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.</td>
<td>Ensure that database replication is complete and functioning between the publisher node and all subscriber nodes.</td>
</tr>
</tbody>
</table>
### Sequence Rules

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

- The Unified Communications Manager publisher node must be the first node that you upgrade. The new software is installed as an inactive version.

- You can begin upgrading Unified Communications Manager subscriber nodes as soon as the publisher node has been upgraded with an inactive version of the new software.

- You must switch the Unified Communications Manager publisher node to the new software version and reboot it before you switch the version on any subscriber nodes. The publisher node must be the first node to switch to the new software version and reboot.

- If you upgrade a group of subscriber nodes, after you switch the software version and reboot, you must wait for database replication to complete on all subscriber nodes before proceeding with any COP file installs or configuration changes.

- If you are upgrading Unified Communications Manager nodes to a Maintenance Release (MR) or an Engineering Special (ES) Release and you are not upgrading Instant Messaging and Presence nodes, you must reboot all IM and Presence nodes after the Unified Communications Manager upgrade is complete.

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

  - You can begin upgrading Instant Messaging and Presence subscriber nodes as soon as the publisher node has been upgraded with an inactive version of the new software.

  - You can wait until all of the Unified Communications Manager nodes are upgraded to an inactive version before you upgrade the Instant Messaging and Presence database publisher node, or you can choose to upgrade in parallel. If you upgrade in parallel, start upgrading the Instant Messaging and Presence database publisher node at the same time that you upgrade the Unified Communications Manager subscriber nodes.

  - You must switch to the new software version and reboot all Unified Communications Manager nodes, starting with the publisher node, before you can switch versions on the Instant Messaging and Presence nodes.

  - You must switch the Instant Messaging and Presence database publisher node to the new software version and reboot it before you switch the software version on any Instant Messaging and Presence subscriber nodes.
• If you upgrade a group of Instant Messaging and Presence subscriber nodes, after you switch the software version and reboot, you must wait for database replication to complete on all subscriber nodes before proceeding.

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

Upgrade time requirements

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

Factors that Affect Upgrade Time Requirements

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

Table 13: Factors that Affect Time Requirements

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
</table>
| External Services and Tools | Time requirements are reduced when external services and tools, such as NTP servers, DNS servers, LDAP directories, and other network services are reachable with response times as short as possible with no dropped packets.  
  We recommend that you configure the ESXi server and the Unified Communications Manager publisher node to point to the same NTP server. |
| Accessibility of upgrade images | Save time by ensuring that ISO images are on DVD, or are already downloaded and staged on the same LAN as the Unified Communications Manager and Instant Messaging and Presence virtual machines (VM). |
### Factors that Affect Upgrade Time Requirements

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>System health</strong></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>Low memory or memory leaks will impact the upgrade.</td>
</tr>
<tr>
<td></td>
<td>Round Trip Times (RTT) between nodes will extend the time required.</td>
</tr>
<tr>
<td></td>
<td>Ensure that there are no OutOfSynch (OOS) tables in the database.</td>
</tr>
<tr>
<td></td>
<td>Ensure that there are no SD link out-of-service events on the Unified Communications Manager node. These events typically indicate a network problem, which you must address before you begin the upgrade process.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Physical and virtual hardware infrastructure</strong></td>
<td>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:</td>
</tr>
<tr>
<td></td>
<td>• 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.</td>
</tr>
<tr>
<td></td>
<td>• Storage latencies meet the requirements specified at [<a href="http://www.cisco.com/go">www.cisco.com/go</a> virtualized-collaboration](<a href="http://www.cisco.com/go">http://www.cisco.com/go</a> virtualized-collaboration).</td>
</tr>
<tr>
<td></td>
<td>• The physical CPU cores and the virtualization design comply with virtualization requirements of Unified Communications Manager and Instant Messaging and Presence. Do not oversubscribe CPUs by having VMs share the host resources; use logical cores or resource reservations</td>
</tr>
<tr>
<td></td>
<td>• Unified Communications Manager and Instant Messaging and Presence virtual machines are on same hosts, or on hosts with 1GbE LAN between them with low contention from other traffic.</td>
</tr>
<tr>
<td><strong>System capacity</strong></td>
<td>Reduce the upgrade time by purging unnecessary files, such as:</td>
</tr>
<tr>
<td></td>
<td>• Call Detail Recording (CDR) records</td>
</tr>
<tr>
<td></td>
<td>• Outdated files, such as TFTP files, firmware, and log files</td>
</tr>
</tbody>
</table>
Throttling

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

### Estimating the Minimum Time Requirements

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

#### Note

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

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

#### Table 14: Minimum Time Required for Upgrade Tasks

<table>
<thead>
<tr>
<th>Task</th>
<th>Minimum Time</th>
<th>Service Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>Upgrade the Unified Communications Manager publisher node to an inactive version</td>
<td>2 to 4 hours Add 1 hour if a refresh upgrade</td>
<td>Refresh upgrades: no access to the UI</td>
</tr>
<tr>
<td>Upgrade the Unified Communications Manager subscriber nodes to an inactive version</td>
<td>1 to 2 hours</td>
<td>Refresh upgrades: phones are unavailable if no backup subscribers are configured</td>
</tr>
<tr>
<td>Switch the Unified Communications Manager publisher node to the new software version and reboot</td>
<td>30 minutes</td>
<td>—</td>
</tr>
<tr>
<td>Switch the Unified Communications Manager subscriber nodes to the new software version and reboot</td>
<td>30 minutes</td>
<td>Standard upgrades: phones are unavailable if no backup subscribers are configured</td>
</tr>
</tbody>
</table>
### Estimating the Minimum Time Requirements

<table>
<thead>
<tr>
<th>Task</th>
<th>Minimum Time</th>
<th>Service Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unified Communications Manager database replication</td>
<td>30 minutes for deployments with small clusters or small databases, 2 hours for megaclusters or large databases</td>
<td>Phones are available with dial tone but end-user features are unavailable until upgrade is complete</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td><strong>WAN latency of 80ms or more can significantly lengthen these times</strong></td>
<td></td>
</tr>
<tr>
<td>Upgrade the Instant Messaging and Presence database publisher node to an inactive version</td>
<td>2 to 4 hours, Add 1 hour if a refresh upgrade</td>
<td>At the time of L2 upgrade neither phone services nor IM and Presence should be impacted</td>
</tr>
<tr>
<td></td>
<td></td>
<td>IM and Presence should be impacted only in the case of Refresh Upgrade</td>
</tr>
<tr>
<td>Upgrade the Instant Messaging and Presence subscriber nodes to an inactive version</td>
<td>1 to 2 hours</td>
<td>During the switch version, irrespective of L2 or Refresh Upgrade phone services should continue to work while IM and Presence is impacted</td>
</tr>
<tr>
<td>Switch the Instant Messaging and Presence publisher node to the new software version and reboot</td>
<td>30 minutes</td>
<td>IM and Presence high availability is disabled, Jabber is unavailable</td>
</tr>
<tr>
<td>Switch the Instant Messaging and Presence subscriber nodes to the new software version and reboot</td>
<td>30 minutes</td>
<td>IM and Presence high availability is disabled, Jabber is unavailable</td>
</tr>
<tr>
<td>Instant Messaging and Presence database replication</td>
<td>30 minutes for deployments with small clusters or small databases, 2 hours for megaclusters or large databases</td>
<td>IM and Presence high availability is disabled, Jabber is unavailable</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td><strong>WAN latency of 80ms or more can significantly lengthen these times</strong></td>
<td></td>
</tr>
</tbody>
</table>
Examples

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

- a megacluster that includes Unified Communications Manager nodes as well as Instant Messaging and Presence nodes
- 75,000 users
- a system that is healthy and that has been optimized for the upgrade, as described in Factors that Affect Upgrade Time Requirements, on page 41

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

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
<th>Minimum Estimated Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Upgrade the Unified Communications Manager publisher node to the new software version. The new software is inactive.</td>
<td>2-4 hours</td>
</tr>
</tbody>
</table>
| 2    | In parallel:  
  - Upgrade the Unified Communications Manager subscriber nodes. The new software is inactive.  
  - Upgrade the Instant Messaging and Presence database publisher node. | 2-3 hours |
| 3    | Upgrade the Instant Messaging and Presence subscriber nodes. The new software is inactive. | 1-2 hours |
| 4    | Switch the software version on the Unified Communications Manager publisher node and reboot it. | 30 minutes |
| 5    | In parallel:  
  - Switch the software version on the Unified Communications Manager subscriber nodes and reboot them.  
  - Switch the software version on the Instant Messaging and Presence database publisher node and reboot it. | 30 minutes |
| 6    | In parallel:  
  - Wait for database replication on the Unified Communications Manager subscriber nodes.  
  - Switch the software version on the Instant Messaging and Presence subscriber nodes and reboot them. | 2 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 16: Example: Time Requirements for a Refresh Upgrade in the Least Time**

<table>
<thead>
<tr>
<th>Task</th>
<th>Minimum Estimated Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Upgrade the Unified Communications Manager publisher node to the new software version. The new software is inactive.</td>
</tr>
<tr>
<td>2</td>
<td>Upgrade the Unified Communications Manager subscriber nodes in parallel. The new software is inactive.</td>
</tr>
<tr>
<td>3</td>
<td>Upgrade the Instant Messaging and Presence database publisher node to the new software version. The new software is inactive.</td>
</tr>
<tr>
<td>4</td>
<td>Upgrade the Instant Messaging and Presence subscriber nodes in parallel. The new software is inactive.</td>
</tr>
<tr>
<td>5</td>
<td>Switch the software version on the Unified Communications Manager publisher node and reboot it.</td>
</tr>
<tr>
<td>6</td>
<td>Switch the software version on the Unified Communications Manager subscriber nodes in parallel and reboot them.</td>
</tr>
<tr>
<td>7</td>
<td>Wait for database replication on the Unified Communications Manager subscriber nodes.</td>
</tr>
<tr>
<td>8</td>
<td>Switch the software version on the Instant Messaging and Presence database publisher node and reboot it.</td>
</tr>
<tr>
<td>9</td>
<td>Switch the software version on the Instant Messaging and Presence subscriber nodes in parallel and reboot them.</td>
</tr>
<tr>
<td>10</td>
<td>Wait for database replication on the Instant Messaging and Presence subscriber nodes.</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td>15.5-20.5 hours</td>
</tr>
</tbody>
</table>
### 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 17: Example: Time Requirements for a Standard Upgrade in the Least Impact

<table>
<thead>
<tr>
<th>Task</th>
<th>Minimum Estimated Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Upgrade the Unified Communications Manager publisher node to the new software version. The new software is inactive.</td>
</tr>
</tbody>
</table>
| 2    | In parallel:  
  • Upgrade all of the Unified Communications Manager subscriber nodes. The new software is inactive.  
  • Upgrade the Instant Messaging and Presence database publisher node. | 2-3 hours |
| 3    | Upgrade the Instant Messaging and Presence subscriber nodes in parallel. The new software is inactive. | 1-2 hours |
| 4    | Switch the software version on the Unified Communications Manager publisher node and reboot it. | 30 minutes |
| 5    | In parallel:  
  • Switch the software version on the Unified Communications Manager secondary subscriber nodes and reboot them.  
  • Switch the software version on the Instant Messaging and Presence database publisher node and reboot it. | 30 minutes |
| 6    | In parallel:  
  • Wait for database replication on the Unified Communications Manager secondary subscriber nodes.  
  • Switch the software version on the Instant Messaging and Presence subscriber nodes in parallel and reboot them. | 2 hours |
| 7    | In parallel:  
  • Wait for database replication on the Instant Messaging and Presence subscriber nodes.  
  Switch the software version on the Unified Communications Manager primary subscriber nodes and reboot them. | 2 hours |
| 8    | Wait for database replication on the 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 18: Example: Time Requirements for a Refresh Upgrade with the Least Impact

<table>
<thead>
<tr>
<th>Task</th>
<th>Minimum Estimated Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Upgrade the Unified Communications Manager publisher node to the new software version. The new software is inactive.</td>
<td>3-4 hours</td>
</tr>
</tbody>
</table>
| 2 In parallel:  
  • Upgrade the Unified Communications Manager secondary subscriber nodes in parallel. The new software is inactive.  
  • Upgrade the Instant Messaging and Presence database publisher node. | 3-4 hours |
| 3 In parallel:  
  • Upgrade the Unified Communications Manager primary subscriber nodes in parallel. The new software is inactive.  
  • Upgrade the Instant Messaging and Presence subscriber nodes in parallel. The new software is inactive. | 1-2 hours |
| 4 Switch the software version on the Unified Communications Manager publisher node and reboot it. | 30 minutes |
| 5 Switch the software version on the Unified Communications Manager secondary subscriber nodes and reboot them. | 30 minutes |
| 6 Wait for database replication on the Unified Communications Manager secondary subscriber nodes. | 2 hours |
| 7 Switch the software version on the Unified Communications Manager primary subscriber nodes and reboot them. | 30 minutes |
| 8 Wait for database replication on the Unified Communications Manager primary subscriber nodes. | 2 hours |
| 9 Switch the software version on the Instant Messaging and Presence database publisher node and reboot it. | 30 minutes |
| 10 Switch the software version on the Instant Messaging and Presence subscriber nodes in parallel and reboot them. | 1-2 hours |
| 11 Wait for database replication on the Instant Messaging and Presence subscriber nodes. | 2 hours |
| Total | 16-20 hours |
Find all Required Upgrade Documentation

Additional Upgrade Documentation

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

<table>
<thead>
<tr>
<th>Task</th>
<th>See . . .</th>
</tr>
</thead>
<tbody>
<tr>
<td>Prepare the hardware platform</td>
<td></td>
</tr>
</tbody>
</table>
| 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 [www.cisco.com/go virtualized-collaboration](http://www.cisco.com/go virtualized-collaboration)  
Information about specs-based support is available by searching on the topic "UC Virtualization Supported Hardware" at [www.cisco.com/go virtualized-collaboration](http://www.cisco.com/go virtualized-collaboration) |
<table>
<thead>
<tr>
<th>Task</th>
<th>See . . .</th>
</tr>
</thead>
</table>
| 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.  
  
  

### Prepare the virtual platform

<table>
<thead>
<tr>
<th>Task</th>
<th>See . . .</th>
</tr>
</thead>
<tbody>
<tr>
<td>Download the Cisco OVA file</td>
<td>Follow the procedures contained in this document. See <em>Download and Install OVA Templates</em>, on page 57</td>
</tr>
</tbody>
</table>
| Edit the virtual machine configuration | *Vendor documentation at [http://www_VMware.com](http://www_VMware.com)*  
  
  Follow the procedures contained in this document. See *Change the Virtualization Software*, on page 55 |

### Upgrade to a new release of Unified Communications Manager and IM and Presence Service

<table>
<thead>
<tr>
<th>Task</th>
<th>See . . .</th>
</tr>
</thead>
<tbody>
<tr>
<td>Upgrade on the same hardware platform using Unified CM OS Administration</td>
<td>Follow the procedures contained in this document.</td>
</tr>
<tr>
<td>Task</td>
<td>See...</td>
</tr>
<tr>
<td>------</td>
<td>--------</td>
</tr>
</tbody>
</table>
PART III

Change the Virtualization Software

• Change the Virtualization Software, on page 55
CHAPTER 9

Change the Virtualization Software

- Virtual Machine Configuration Tasks, on page 55

Virtual Machine Configuration Tasks

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

Before you begin

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

Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Install and Configure VMware vCenter, on page 56</td>
<td>VMware vCenter is required only when you are migrating from Cisco Business Edition or Tested Reference Configuration (TRC) hardware to UC on UCS specs-based or third-party server specs-based hardware. If you require VMware vCenter, install and configure it first. Using VMware vCenter is optional when you deploy Unified Communications Manager or Instant Messaging and Presence on UC on UCS tested reference configuration hardware.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Upgrade vSphere ESXi, on page 57</td>
<td>You must install a version of vSphere ESXi hypervisor that meets the requirements of the release. We recommend that you upgrade the ESXi hypervisor before you begin an upgrade of Unified Communications Manager or Instant Messaging and Presence; however, if your</td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
<td></td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
<td></td>
</tr>
<tr>
<td>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.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> Download and Install OVA Templates, on page 57</td>
<td>OVA files provide a set of predefined templates for virtual machine configuration. They cover items such as supported capacity levels and any required OS/VM/SAN alignment. This procedure is optional. If you are already running Unified Communications Manager or Instant Messaging and Presence on a virtual machine, and your deployment size has not changed, you do not need to download and install a new OVA template. If you are changing the size of your system, download and install an OVA template for the new release that is sized for your deployment.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> Change Virtual Machine Configuration Specifications, on page 58</td>
<td>Use this procedure when you need to change the vCPU, vRAM, vDisk size, or vNIC type on your virtual machine (VM) in order to upgrade to a new release of Unified Communications Manager or Instant Messaging and Presence. Do this step for only for direct upgrades, which use either the Unified CM OS Admin interface or the PCD Upgrade task to perform the upgrade.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> Migrate From Single to Multi-vDisk Virtual Machine, on page 59</td>
<td>Use this procedure if you are migrating to a larger virtual machine (VM) deployment that requires multiple vDisks.</td>
<td></td>
</tr>
</tbody>
</table>

### Install and Configure VMware vCenter

Using VMware vCenter is optional when you deploy Unified Communications Manager or Instant Messaging and Presence on UC on UCS tested reference configuration hardware. VMware vCenter is mandatory when you deploy on UC on UCS specs-based and third-party server specs-based hardware. VMware vCenter allows you to collect performance data. For information about how to install and configure the application, see the VMWare documentation.

**Procedure**

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

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

---

### Upgrade vSphere ESXi

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

**Procedure**

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

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

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

**Step 3**  Verify that the vSphere ESXi upgraded successfully.

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

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

---

### Download and Install OVA Templates

OVA files provide a set of predefined templates for virtual machine configuration. They cover items such as supported capacity levels and any required OS/VM/SAN alignment. For information about OVA files, search for the topic "Unified Communications Virtualization Sizing Guidelines" at https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/uc_system/virtualization/cisco-collaboration-virtualization.html.

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

**Procedure**

**Step 1**  Locate the OVA template for your release:
**Change Virtual Machine Configuration Specifications**

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

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

**Before you begin**

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

**Procedure**

1. **Step 1** Perform a Disaster Recovery System (DRS) backup.
2. **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

3. **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 58 to ensure that the specifications match the requirements of the release.

Procedure

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

Upgrade the Applications

• Pre-upgrade Tasks, on page 63
• Upgrade Procedures, on page 87
• Post-upgrade Tasks, on page 101
Pre-upgrade Tasks

• Pre-Upgrade Task Flow, on page 63

Pre-Upgrade Task Flow

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

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 2</strong></td>
<td>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 <a href="http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html">http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html</a> for information about how to migrate an existing cluster to a virtualized cluster.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Familiarize yourself with the requirements and limitations of this release: <a href="#">Requirements and Limitations, on page 17</a></td>
</tr>
<tr>
<td><strong>Command or Action</strong></td>
<td><strong>Purpose</strong></td>
</tr>
<tr>
<td>----------------------</td>
<td>-------------</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>Check the health of your network:</td>
</tr>
<tr>
<td>• Read Factors that Affect Upgrade Time Requirements, on page 41 and ensure that your system meets the conditions described in that section.</td>
<td>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.</td>
</tr>
<tr>
<td>• Generate a Database Status Report, on page 69</td>
<td></td>
</tr>
<tr>
<td>• Check Database Replication, on page 69</td>
<td></td>
</tr>
<tr>
<td>• Check Performance Reports, on page 70</td>
<td></td>
</tr>
<tr>
<td>• Run CLI Diagnostics, on page 70</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>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:</td>
</tr>
<tr>
<td>• Delete a Trust Certificate, on page 71</td>
<td>Perform this step for refresh upgrades on 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.</td>
</tr>
<tr>
<td>• Regenerate a Certificate, on page 71 if an identify certificate is expired</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>Take a Fresh Backup, on page 73</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Caution</strong></td>
<td>You may lose data or you may be unable to restore your system if your backup is outdated.</td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td>Back Up Custom Ringtones and Background Images, on page 74</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Step 8</strong></td>
<td>Check Network Connectivity, on page 74</td>
</tr>
<tr>
<td></td>
<td>Use this procedure to verify connectivity between Unified Communications Manager nodes and services in your network, such as NTP, SMTP, and DNS.</td>
</tr>
<tr>
<td><strong>Step 9</strong></td>
<td>Verify IPv6 Networking, on page 75</td>
</tr>
<tr>
<td></td>
<td>This procedure applies to Unified Communications Manager nodes only. Verify IPv6 networking on the first node (Unified Communications Manager database publisher node) and Unified Communications Manager subscriber nodes. If IPv6 is configured incorrectly on the Unified Communications...</td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>------------------</td>
<td>---------</td>
</tr>
<tr>
<td></td>
<td>Manager subscriber nodes, load detection may take 20 minutes. Do this step for all upgrade and migration methods.</td>
</tr>
<tr>
<td><strong>Step 10</strong></td>
<td>Check Connectivity between IM and Presence and Cisco Unified Communications Manager, on page 75</td>
</tr>
<tr>
<td><strong>Step 11</strong></td>
<td>Collect Configuration and Login Information, on page 75</td>
</tr>
<tr>
<td><strong>Step 12</strong></td>
<td>Record the Registered Device Count, on page 76</td>
</tr>
<tr>
<td><strong>Step 13</strong></td>
<td>Record the Number of Assigned Users, on page 77</td>
</tr>
<tr>
<td><strong>Step 14</strong></td>
<td>Record TFTP Parameters, on page 77</td>
</tr>
<tr>
<td><strong>Step 15</strong></td>
<td>Record Enterprise Parameters, on page 77</td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>--------------------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>you can restore them as needed after the upgrade is complete. Do this step for all upgrade and migration methods.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 16</strong> Export User Records, on page 78</td>
<td>Export user records using the Bulk Administration Tool (BAT). Do this step for all upgrade and migration methods.</td>
</tr>
<tr>
<td><strong>Step 17</strong> Upgrade IP Phone Firmware, on page 78</td>
<td>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 before the upgrade in order to minimize phone downtime after an upgrade. If you need to upgrade Unified Communications Manager as part of your IM and Presence upgrade, you must stop the IM and Presence Sync Agent service before you 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.</td>
</tr>
<tr>
<td><strong>Step 18</strong> Verify Critical Services, on page 79</td>
<td>Verify that all critical services are activated.</td>
</tr>
<tr>
<td><strong>Step 19</strong> Deactivate Cisco Extension Mobility, on page 80</td>
<td>Perform this procedure only if you are upgrading from Release 9.x or earlier. For upgrades from Release 9.x or earlier, you must stop Cisco extension mobility services on 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.</td>
</tr>
<tr>
<td><strong>Step 20</strong> Deactivate TFTP services, on page 80</td>
<td>Stop TFTP services on Unified Communications Manager nodes before you begin an upgrade.</td>
</tr>
<tr>
<td><strong>Step 21</strong> Stop the IM and Presence Sync Agent, on page 80</td>
<td>If you need to upgrade Unified Communications Manager as part of your IM and Presence upgrade, you must stop the IM and Presence Sync Agent service before you begin the upgrade process. Do this step for only for direct upgrades, which use either the Unified CM OS Admin interface</td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
</tr>
<tr>
<td><strong>Step 22</strong> Check the Available Common Partition Space, on page 81</td>
<td>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.</td>
</tr>
</tbody>
</table>
| **Step 23** If you do not have enough common partition space, perform one or more of the following procedures:  
  • Adjust High and Low Watermarks, on page 81  
  • Maximize Usable Disk Space, on page 81 | Do this step for only for direct upgrades, which use either the Unified CM OS Admin interface or the PCD Upgrade task to perform the upgrade.  
  **Caution** Performing an upgrade without sufficient disk space can cause the upgrade to fail. |
| **Step 24** Obtain Upgrade Files, on page 83 | Download the upgrade files for the 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. |
Do this step for all upgrade and migration methods. |
<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Note</strong></td>
<td>Apply all pre-9.0 licenses to 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 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 Unified Communications Manager displays a warning to prompt you to install any unused licenses before proceeding.</td>
</tr>
</tbody>
</table>

**Step 26** Increase the Database Replication Timeout, on page 85  
Optional. This procedure applies to the 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 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 27** Disable High Availability on Presence Redundancy Groups, on page 85  
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.  
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 28** Add a Serial Port to the Virtual Machine, on page 86  
Add a serial port to the virtual machine so that you can dump logs if an upgrade fails. 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 CM nodes, log in to the Cisco Unified Reporting interface.
- For IM and Presence nodes, log in to the Cisco Unified IM and Presence Reporting interface.

**Step 2** Select **System Reports**.

**Step 3** Check database replication on the node:
- For Unified CM, select **Unified CM Database Status**.
- For IM and Presence, select **IM and Presence Database Status**.

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

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

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

---

**Check Database Replication**

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

**Procedure**

**Step 1** Start a CLI session using one of the following methods:
- From a remote system, use SSH to connect securely to the Cisco Unified Operating System. In your SSH client, enter your `ssh adminname@hostname` and enter your password.
- From a direct connection to the serial port, enter your credentials at the prompt that displays automatically.

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

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

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

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

Procedure

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

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

**Step 3** Click the **CallActivitiesRep** to open the Call Activities Report in a new tab and verify that the number of **Calls Attempted** is not too high for the capacity of the virtual machine. You can determine the threshold for the number of **Calls Attempted** by checking the recommendations for your system in the *Cisco Collaboration Systems Solution Reference Network Designs (SRND)* at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/srnd/collab11/collab11.html.

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

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

For information about deployment sizing, see:

- 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.

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

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

To regenerate a self-signed certificate with a new key length of 3072 or 4096, Click Generate Self-Signed Certificate.
Step 2 Configure the fields on the **Generate New Self-Signed Certificate** window. See the online help for more information about the fields and their configuration options.

Step 3 Click **Generate**.

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

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

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

---

**What to do next**

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

**Related Topics**

Certificate Names and Descriptions, on page 72

**Certificate Names and Descriptions**


*Table 19: Certificate Names and Descriptions*

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Related Services</th>
</tr>
</thead>
<tbody>
<tr>
<td>tomcat</td>
<td>This self-signed root certificate is generated during installation for the HTTPS node.</td>
<td>Tomcat and TFTP</td>
</tr>
<tr>
<td>tomcat-ECDSA</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ipsec</td>
<td>This self-signed root certificate is generated during installation for IPSec connections with MGCP and H.323 gateways.</td>
<td>Cisco Disaster Recovery System (DRS) Local and Cisco DRF Master</td>
</tr>
<tr>
<td>CallManager</td>
<td>This self-signed root certificate is installed automatically when you install Unified Communications Manager. This certificate provides node identification, including the node name and the global unique identifier (GUID).</td>
<td>CallManager, CAPF, and CTI</td>
</tr>
</tbody>
</table>
**Take a Fresh Backup**

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

Perform this procedure for all upgrade and migration methods.

**Caution**

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

**Before you begin**

- Ensure that you use a network device as the storage location for the backup files. Virtualized deployments of Unified Communications Manager do not support the use of tape drives to store backup files.

- Ensure that your system meets the version requirements:
  - All Unified Communications Manager cluster nodes must be running the same version of the Unified Communications Manager application.
  - All Instant Messaging and Presence cluster nodes must be running the same version of the Instant Messaging and Presence application.

For each application, the entire version string must match. For example, if the IM and Presence database publisher node is at version 11.5.1.10000-1, then all IM and Presence subscriber nodes must be 11.5.1.10000-1, and you must create a backup file for version 11.5.1.10000-1.

- The backup process can fail due to non availability of space on a remote server or due to interruptions in the network connectivity. You need to start a fresh backup after addressing the issues that caused the backup to fail.

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

**Procedure**

**Step 1**

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

**Step 2**

In the **Manual Backup** window, select a backup device from the **Backup Device Name** area.
Step 3 Choose a feature from the Select Features area.
Step 4 Click Start Backup.

Back Up Custom Ringtones and Background Images

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

Procedure

Step 1 Use a web browser or TFTP client to access the directories where the ringtones and background images are stored.
Step 2 Backup the following files: Ringlist.xml and List.xml.
Step 3 Back up the custom ringtones. These are located in the TFTP directory.
Step 4 Back up the background images. These are located in the folder /Desktops (and its subfolders) in the TFTP directory.

Check Network Connectivity

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

Procedure

Step 1 Start a CLI session using one of the following methods:
   • From a remote system, use SSH to connect securely to the Cisco Unified Operating System. In your SSH client, enter your ssh adminname@hostname and enter your password.
   • From a direct connection to the serial port, enter your credentials at the prompt that displays automatically.
Step 2 Execute the show network cluster command on each node in your network to verify communication between Unified Communications Manager servers in the cluster.
Step 3 If you have an NTP server, execute the utils ntp status command to verify connectivity to the NTP server.
Step 4 If you have an SMTP server, ping the server to verify connectivity.
Step 5 If you are using DNS, execute the show network eth0 command on each node in your network to verify that the DNS and domain are configured.
Step 6 Check that DNS name resolution is working correctly:
   a) Ping the FQDN of each Unified Communications Manager node to ensure that it resolves to the IP address.
   b) Ping the IP address of each Unified Communications Manager to ensure that it resolves to the FQDN.
**Verify IPv6 Networking**

This procedure applies to Unified Communications Manager nodes only.

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

**Procedure**

**Step 1**
Start a CLI session using one of the following methods:
- From a remote system, use SSH to connect securely to the Cisco Unified Operating System. In your SSH client, enter your `ssh adminname@hostname` and enter your password.
- From a direct connection to the serial port, enter your credentials at the prompt that displays automatically.

**Step 2**
Execute the following command: `utils network ipv6 ping destination [count]`
- `destination` is a valid IPv6 address or host name that you want to ping
- `count` is the number of times to ping the external server. The default is 4.

**Check Connectivity between IM and Presence and Cisco Unified Communications Manager**

Verify that the Instant Messaging and Presence service node has connectivity with Unified Communications Manager.

**Procedure**

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

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

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

**Collect Configuration and Login Information**

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

Step 1
Record the following login and password information:
- all application users credentials, such as DRS, AXL, and accounts for other third-party integrations
- administrator, cluster security, and Certificate Trust List (CTL) security token passwords

Step 2
Record the following information about your network configuration:
- IP addresses, hostnames, gateways, domain names, DNS servers, NTP servers, the Call Detail Recording (CDR) server, and SMTP information
- server versions and time zones
- services running on each server and the associated activation status
- LDAP information and access details
- SNMP information

Record the Registered Device Count

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

Procedure

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

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

<table>
<thead>
<tr>
<th>Item</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>Registered Phones</td>
<td></td>
</tr>
<tr>
<td>FSX</td>
<td></td>
</tr>
<tr>
<td>FSO</td>
<td></td>
</tr>
<tr>
<td>T1 CAS</td>
<td></td>
</tr>
<tr>
<td>PRI</td>
<td></td>
</tr>
<tr>
<td>MOH</td>
<td></td>
</tr>
<tr>
<td>MTP</td>
<td></td>
</tr>
<tr>
<td>CFB</td>
<td></td>
</tr>
</tbody>
</table>
Record the Number of Assigned Users

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

Procedure

Step 1  From the Cisco Unified CM IM and Presence Administration interface, select **System > Cluster Topology**. The Cluster Topology Details page displays information about nodes and subclusters.
Step 2  Record the number of users that are assigned to each node and cluster.

Record TFTP Parameters

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

Procedure

Step 1  From the Cisco Unified CM Administration interface, choose **System > Service Parameters**.
Step 2  From the **Server** drop-down list, select the node that is running the TFTP service.
Step 3  From the **Service** drop-down list, select **Cisco TFTP service**.
Step 4  Click **Advanced**.
Step 5  Click **Save**.
Step 6  Record the value that is configured for the **Maximum Serving Count**.

Record Enterprise Parameters

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

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

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

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Instruction</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>From Cisco Unified CM Administration, choose <strong>Bulk Administration &gt; Users &gt; Export Users</strong>.</td>
</tr>
<tr>
<td>2</td>
<td>Click <strong>Find</strong> to display all user records.</td>
</tr>
<tr>
<td>3</td>
<td>Click <strong>Next</strong>.</td>
</tr>
<tr>
<td>4</td>
<td>Enter a filename in the <strong>File Name</strong> text box and choose file format from the <strong>File Format</strong> drop-down list.</td>
</tr>
<tr>
<td>5</td>
<td>In the <strong>Job Information</strong> area, enter the <strong>Job description</strong>.</td>
</tr>
<tr>
<td>6</td>
<td>Click <strong>Run Immediately</strong> to export user records immediately</td>
</tr>
<tr>
<td>7</td>
<td>Click <strong>Submit</strong>.</td>
</tr>
<tr>
<td>8</td>
<td>To download the exported file, choose <strong>Bulk Administration &gt; Upload/Download Files</strong>.</td>
</tr>
<tr>
<td>9</td>
<td>Enter search criteria for the file that you generated and click <strong>Find</strong>.</td>
</tr>
<tr>
<td>10</td>
<td>Select the check box that corresponds to the file that you want to download and click <strong>Download Selected</strong>.</td>
</tr>
<tr>
<td>11</td>
<td>In the File Download pop-up window, click <strong>Save</strong>.</td>
</tr>
<tr>
<td>12</td>
<td>In the Save As pop-up window, choose the location where you want to save the file and click <strong>Save</strong>. Ensure that you copy the file off of the server and save it to a remote PC or device.</td>
</tr>
</tbody>
</table>

**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**

<table>
<thead>
<tr>
<th>Step 1</th>
<th>From Cisco Unified OS Administration, choose <strong>Software Upgrades &gt; Install/Upgrade.</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>Fill in the applicable values in the Software Location section and click <strong>Next.</strong></td>
</tr>
<tr>
<td>Step 3</td>
<td>In the <strong>Available Software</strong> drop-down list, select the device package file and click <strong>Next.</strong></td>
</tr>
<tr>
<td>Step 4</td>
<td>Verify that the MD5 value is correct, and then click <strong>Next.</strong></td>
</tr>
<tr>
<td>Step 5</td>
<td>In the warning box, verify that you selected the correct firmware, and then click <strong>Install.</strong></td>
</tr>
<tr>
<td>Step 6</td>
<td>Check that you received a success message.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>Skip to Step 8 if you are rebooting the cluster.</td>
</tr>
</tbody>
</table>

| Step 7   | Stop and restart the TFTP server.                                                     |
| Step 8   | Reset the affected devices to upgrade the devices to the new load.                    |
| Step 9   | From Cisco Unified CM Administration, choose **Device > Device Settings > Device Defaults** and manually change the name of the "Load Information" and "Inactive Load Information" for the specific Device Type fields for the new load on the TFTP server. |
| Step 10  | Click **Save**, and then reset the devices.                                             |

**Verify Critical Services**

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

**Procedure**

<table>
<thead>
<tr>
<th>Step 1</th>
<th>From the Unified RTMT interface, select <strong>System &gt; Server &gt; Critical Services.</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>To display system critical services, click the <strong>System</strong> tab.</td>
</tr>
<tr>
<td>Step 3</td>
<td>To display Unified Communications Manager critical services, select a Unified Communications Manager node from the drop-down list and click the <strong>Voice/Video</strong> tab.</td>
</tr>
<tr>
<td>Step 4</td>
<td>To display IM and Presence Service critical services, click the <strong>IM and Presence</strong> tab and select an Instant Messaging and Presence Service node from the drop-down list.</td>
</tr>
<tr>
<td>Step 5</td>
<td>If the status indicates that any critical services are stopped, reactivate them before beginning the upgrade.</td>
</tr>
</tbody>
</table>
Deactivate Cisco Extension Mobility

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

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>From Cisco Unified Serviceability, choose <strong>Tools &gt; Service Activation</strong>.</td>
</tr>
<tr>
<td>2</td>
<td>From the <strong>Server</strong> list, choose the node on which you want to deactivate services and click <strong>Go</strong>.</td>
</tr>
<tr>
<td>3</td>
<td>Deselect the <strong>Cisco Extension Mobility</strong> services.</td>
</tr>
<tr>
<td>4</td>
<td>Click <strong>Stop</strong>.</td>
</tr>
<tr>
<td>5</td>
<td>Repeat Steps 2 through 4 for each node that is running <strong>Cisco Extension Mobility</strong> services.</td>
</tr>
<tr>
<td>6</td>
<td>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.</td>
</tr>
</tbody>
</table>

Deactivate TFTP services

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

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>From Cisco Unified Serviceability, choose <strong>Tools &gt; Service Activation</strong>.</td>
</tr>
<tr>
<td>2</td>
<td>From the <strong>Server</strong> list, choose the node on which you want to deactivate services and click <strong>Go</strong>.</td>
</tr>
<tr>
<td>3</td>
<td>Deselect <strong>Cisco TFTP</strong> services.</td>
</tr>
<tr>
<td>4</td>
<td>Click <strong>Stop</strong>.</td>
</tr>
<tr>
<td>5</td>
<td>Repeat Steps 2 through 4 for each node that is running <strong>Cisco TFTP</strong> services.</td>
</tr>
<tr>
<td>6</td>
<td>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.</td>
</tr>
</tbody>
</table>

Stop the IM and Presence Sync Agent

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

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>From the Cisco Unified Serviceability interface, select <strong>Tools &gt; Control Center - Network Services</strong>.</td>
</tr>
</tbody>
</table>
**Step 2** Select an Instant Messaging and Presence Service node from the Server drop-down list and click Go.

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

---

**Check the Available Common Partition Space**

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

**Procedure**

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

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

---

**Adjust High and Low Watermarks**

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

**Procedure**

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

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

**Step 3** Select Next.

**Step 4** Adjust the slider value to 30.

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

**Step 6** Select Next.

**Step 7** Adjust the slider value to 40.

---

**Maximize Usable Disk Space**

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 that are listed in this procedure, go to https://software.cisco.com and then, navigate to Unified Communications > Call Control > Cisco Unified Communications Manager (CallManager) > <Version> > Unified Communications Manager/CallManager/Cisco Unity Connection Utilities.
If your current version has previously used a serial connection to upgrade from a pre-11.5(x) version then it's likely that have an older OS partitioning scheme and virtual disk layout. This will amplify "out of disk space" issues, thereby limiting the effectiveness of adding additional virtual disk space. The upgrade readiness COP file checks for these issues, and provides guidance on how to resolve them.

**Procedure**

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

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

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

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

**Step 2** 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_<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.
For 110G or 80G single disk or two 80G disk deployments, available space for upgrade should be at least twice the active partition disk space. For example, in a two 80G disk deployment, active partition should not be more than 25G, and available space should be at least 50G. Following are commands to check the disk usage.

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

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

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

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

---

**Obtain Upgrade Files**

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

**Procedure**

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

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

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

- To download the Instant Messaging and Presence Service upgrade file, go to https://software.cisco.com and then, navigate to Unified Communications > Unified Communications Applications > Presence Software > Unified Communications Manager IM and Presence Service > <Version> > Unified Presence Service (CUP) Updates.

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

**Step 4**
Go to https://software.cisco.com and then, navigate to Unified Communications > Unified Communications Applications > Presence Software > Unified Communications Manager IM and Presence Service > <Version> > Unified Presence Service (CUP) Updates and select UTILS to download COP files for IM and Presence Service.
COP Files Required for Upgrades to Release 11.5

The tables below list 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 20: Required COP Files for Upgrades and Migrations to Cisco Unified Communications Manager Release 11.5(x)

<table>
<thead>
<tr>
<th>From</th>
<th>To</th>
<th>Upgrade Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.6(x)</td>
<td>11.5(x)</td>
<td>Refresh upgrade. Required COP files:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• ciscocm.version3-keys.cop.sgn</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Optional COP files:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• ciscocm.vmware-disk-size-reallocation-&lt;latest_version&gt;.cop.sgn</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• ciscocm.free_common_space_v&lt;latest_version&gt;.cop.sgn</td>
</tr>
<tr>
<td>9.1(x)</td>
<td>11.5(x)</td>
<td>Refresh upgrade. Required COP files:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• ciscocm.version3-keys.cop.sgn</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Optional COP files:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• ciscocm.vmware-disk-size-reallocation-&lt;latest_version&gt;.cop.sgn</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• ciscocm.free_common_space_v&lt;latest_version&gt;.cop.sgn</td>
</tr>
<tr>
<td>10.5(x)</td>
<td>11.5(x)</td>
<td>Standard upgrade; no COP file required.</td>
</tr>
<tr>
<td>11.0(x)</td>
<td>11.5(x)</td>
<td>Standard upgrade; no COP file required.</td>
</tr>
<tr>
<td>11.5(x)</td>
<td>11.5((y)</td>
<td>Standard upgrade; no COP file required.</td>
</tr>
</tbody>
</table>

### Table 21: Required COP Files for Refresh Upgrades from Cisco Unified Presence Releases

<table>
<thead>
<tr>
<th>From Cisco Unified Presence Release</th>
<th>To IM and Presence Release</th>
<th>Upgrade Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.5(4) through 8.6(1)</td>
<td>11.5(x)</td>
<td>Refresh upgrade. Requires the following COP files:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• cisco.com.cup.refresh_upgrade_v&lt;latest_version&gt;.cop</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• ciscocm.version3-keys.cop.sgn</td>
</tr>
</tbody>
</table>

### Table 22: Required COP Files for Refresh Upgrades from IM and Presence Service Releases

<table>
<thead>
<tr>
<th>From IM and Presence Release</th>
<th>To IM and Presence Release</th>
<th>Upgrade Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.1(x)</td>
<td>11.5(x)</td>
<td>Refresh upgrade. Requires the following COP file:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• ciscocm.version3-keys.cop.sgn</td>
</tr>
</tbody>
</table>
### Increase the Database Replication Timeout

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

**Procedure**

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

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

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

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

### Disable High Availability on Presence Redundancy Groups

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

**Before you begin**

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

**Procedure**

**Step 1**
From the Cisco Unified CM Administration user interface, choose System > Presence Redundancy Groups.
**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 104. In the event of an upgrade failure, refer to Dump aLogFile After an Upgrade Failure, on page 119.

---

**Add a Serial Port to the Virtual Machine**

Step 2 Click Find and select the group.

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

Step 4 Click Save.

Step 5 Repeat this procedure for each Presence Redundancy Group.

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

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

Note

If you want to use Cisco Prime Collaboration Deployment to complete an upgrade or migration, refer to the Cisco Prime Collaboration Deployment Administration Guide to set up an upgrade task or migration task.

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 Instant Messaging and Presence nodes, the first node that you install functions as the server for the Instant Messaging and Presence database. Because this node publishes the database for all of the Instant Messaging and Presence nodes in the cluster, it is referred to as the Instant Messaging 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.

<table>
<thead>
<tr>
<th>Upgrade type</th>
<th>Switching type</th>
<th>When prompted, choose . . .</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>Standard upgrade</td>
<td>Automatic</td>
<td>Reboot to upgraded partition</td>
<td>When you choose this option, the system reboots to the new software version.</td>
</tr>
<tr>
<td></td>
<td>Manual</td>
<td>Do not reboot after upgrade</td>
<td>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.</td>
</tr>
<tr>
<td>Refresh upgrade</td>
<td>Manual</td>
<td>Do not switch to new version after upgrade</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>Automatic</td>
<td>Switch to new version after upgrade</td>
<td>Choose this option to use the new software version immediately following the upgrade.</td>
</tr>
</tbody>
</table>

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

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

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

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 Unified Communications Manager nodes and all Instant Messaging and Presence Service nodes.

Caution

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

Caution

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

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

Upgrade Task Flow

Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 Upgrade the application using one of the following procedures:</td>
<td>Use these procedures when you upgrade Unified Communications Manager or the Instant</td>
</tr>
<tr>
<td>• Upgrade from a Local Source, on page 90</td>
<td>Messaging and Presence using the Unified CM OS Administration interface.</td>
</tr>
</tbody>
</table>
### Purpose

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Upgrade from a Remote Source, on page 91</td>
<td></td>
</tr>
</tbody>
</table>

### Step 2

**Switch the Software Version, on page 96**

Use this procedure to activate the new software.

### Step 3

**Switch to Previous Version, on page 97**

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 99**

### Step 5

**Verify that Database Replication is Complete, on page 100**

---

## Upgrade the Applications

### Upgrade from a Local Source

Follow this procedure to upgrade to a new release of Unified Communications Manager or the Instant Messaging 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
- UCSInstall_UCOS_<XXXXXXXX>.sgn.iso
- Export unrestricted software has a XU license SKU.
- Export restricted software has a K9 license SKU.

### Procedure

#### Step 1

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

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

#### Step 2

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

- If you are upgrading an Instant Messaging and Presence node, log in to Cisco Unified IM and Presence Operating System Administration.
- If you are upgrading a Unified Communications Manager node, log in to Cisco Unified Communications Operating System Administration.
Step 3  If you are performing a refresh upgrade that requires a COP file, install the required COP file. If you are unsure whether you have to install a COP file, review the information about supported upgrade paths. See the Related Topics section for more information.

Step 4  Select Software Upgrades > Install/Upgrade.

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

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

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

Note  These fields are only visible for refresh upgrades.

Step 8  Select Next to continue the upgrade process.

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

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

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

Step 12  Perform one of the following actions:

For standard upgrades:

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

For refresh upgrades:

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

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

Step 13  Select Next.

Step 14  Select Finish when the installation completes.

Upgrade from a Remote Source

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

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

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

Procedure

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

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

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

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

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

Step 4
Select Software Upgrades > Install/Upgrade.

Step 5
Select Remote Filesystem from the Source list.

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

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

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

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

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

Note These fields are only visible for refresh upgrades.

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

Step 12
Select Next to continue the upgrade process.

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

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

Step 15
Perform one of the following actions:

For standard upgrades:

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

**For refresh upgrades:**

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

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

**Step 16** Select Next.

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

---

## Version Switching

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

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

<table>
<thead>
<tr>
<th>Product</th>
<th>Node type</th>
<th>Switch from</th>
<th>Switch to</th>
<th>Switching rule</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Activate the new software version</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Unified CM</td>
<td>Publisher</td>
<td>8.x or 9.x</td>
<td>11.x</td>
<td>You must switch the software version on the publisher node before you switch the software version on subscriber nodes.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>10.x</td>
<td>11.x</td>
<td></td>
</tr>
<tr>
<td>Unified CM</td>
<td>Subscriber</td>
<td>8.x or 9.x</td>
<td>11.x</td>
<td>Supported when the publisher node has been switched to the new version. The software version you are switching to must match the version number of the active partition on the Unified Communications Manager publisher node.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>10.x</td>
<td>11.x</td>
<td></td>
</tr>
<tr>
<td>IM and Presence</td>
<td>Database</td>
<td>8.x or 9.x</td>
<td>11.x</td>
<td>Supported when the software version you are switching to matches the major and minor version number of active partition on the Unified Communications Manager publisher node.</td>
</tr>
<tr>
<td></td>
<td>publisher</td>
<td>10.x</td>
<td>11.x</td>
<td></td>
</tr>
</tbody>
</table>
### Product

<table>
<thead>
<tr>
<th>Node type</th>
<th>Switch from</th>
<th>Switch to</th>
<th>Switching rule</th>
</tr>
</thead>
<tbody>
<tr>
<td>IM and Presence</td>
<td>Subscriber</td>
<td>8.x or 9.x</td>
<td>11.x</td>
</tr>
<tr>
<td></td>
<td>10.x</td>
<td>11.x</td>
<td></td>
</tr>
</tbody>
</table>

### Switch back to a previous software version

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

<table>
<thead>
<tr>
<th>Product</th>
<th>Node Type</th>
<th>Switch from</th>
<th>Switch to</th>
<th>Switching Rule</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unified CM</td>
<td>Publisher</td>
<td>10.x or 11.x or 12.y</td>
<td>12.x</td>
<td>You must switch the software version on the publisher node before you switch the software version on subscriber nodes.</td>
</tr>
<tr>
<td>Unified CM</td>
<td>Subscriber</td>
<td>10.x or 11.x or 12.y</td>
<td>12.x</td>
<td>Supported when the publisher node has been switched to the new version. The software version you are switching to must match the version number of the active partition on the Unified Communications Manager publisher node.</td>
</tr>
<tr>
<td>IM and Presence</td>
<td>Database publisher</td>
<td>10.x or 11.x or 12.y</td>
<td>12.x</td>
<td>Supported when the software version you are switching to matches the major and minor version number of active partition on the Unified Communications Manager publisher node.</td>
</tr>
<tr>
<td>IM and Presence</td>
<td>Subscriber</td>
<td>10.x or 11.x or 12.y</td>
<td>12.x</td>
<td>Supported when the software version of this node matches the five version numbers of the Instant Messaging and Presence database publisher node.</td>
</tr>
</tbody>
</table>

### Switch back to a previous software version

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

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

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

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

⚠️ Caution

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

Before you begin

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

Review the information in Understanding Version Switching, on page 88

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

Step 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

<table>
<thead>
<tr>
<th>Step</th>
<th>Task</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Switch back the publisher node.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Switch back all backup subscriber nodes.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Switch back all primary subscriber nodes.</td>
</tr>
<tr>
<td>Step 4</td>
<td>If you are reverting to an older product release, reset database replication within the cluster.</td>
</tr>
</tbody>
</table>

Switch Node to Previous Version

Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Task</th>
</tr>
</thead>
</table>
| Step 1 | Log in to the management software for the node that you are upgrading:  
  • If you are upgrading an Instant Messaging and Presence node, log in to Cisco Unified IM and Presence Operating System Administration.  
  • If you are upgrading a Unified Communications Manager node, log in to Cisco Unified Communications Operating System Administration. |
| Step 2 | Choose **Settings > Version.**  
  The Version Settings window displays. |
| Step 3 | Click the **Switch Versions** button.  
  After you verify that you want to restart the system, the system restarts, which might take up to 15 minutes. |
| Step 4 | To verify that the version switch was successful, follow these steps:  
  a) Log in again to the management software for the node that you are upgrading.  
  b) Choose **Settings > Version.**  
  The Version Settings window displays.  
  c) Verify that the correct product version is now running on the active partition.  
  d) Verify that all activated services are running.  
  e) For the publisher node, log in to Cisco Unified CM Administration. |
f) Verify that you can log in and that your configuration data exists.

---

**Reset Database Replication**

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

---

<table>
<thead>
<tr>
<th>Note</th>
</tr>
</thead>
<tbody>
<tr>
<td>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.</td>
</tr>
</tbody>
</table>

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

---

<table>
<thead>
<tr>
<th>Note</th>
</tr>
</thead>
<tbody>
<tr>
<td>You must restart the system after you install the COP file.</td>
</tr>
</tbody>
</table>

Before you begin

Switch versions on Unified Communications Manager.

**Procedure**

- **Step 1** Download the following COP file from Cisco.com: `ciscocm.cup.pe_db_install.cop`.
- **Step 2** Sign in to Cisco Unified IM and Presence Operating System Administration.
- **Step 3** Select **Settings > Version**.
- **Step 4** Verify the version of the active and inactive software.
  - **Note** This procedure only applies if you want to switch from Release 9.0 or later back to a release earlier than 8.6(4).
- **Step 5** Select **Switch Versions** to switch back to the earlier release and restart the system.
- **Step 6** After the system has restarted, install the COP file.
  - **Note** In a multinode environment, you must install the COP file on every node in the cluster.
Verify that Database Replication is Functioning

Use Cisco Unified Reporting to generate Database Status reports for Unified Communications Manager and Instant Messaging and Presence 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 CM nodes, log in to the Cisco Unified Reporting interface.
- For IM and Presence nodes, log in to the Cisco Unified IM and Presence Reporting interface.

Step 2 Select System Reports.

Step 3 Check database replication on the node:
- For Unified CM, select Unified CM Database Status.
- For IM and Presence, select IM and Presence Database Status.

Step 4 Click the Generate Report (bar chart) icon in the Reports window.
Step 5 Click the View Details link to expose details for a section that does not automatically appear.
Step 6 If the report indicates that there are errors, select the Report Descriptions report and review the troubleshooting information with possible remedies.

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 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.
Post-upgrade Tasks

- Post-upgrade Task Flow, on page 101

Post-upgrade Task Flow

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

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td><strong>Switch the Software Version, on page 103</strong></td>
<td>If you did not switch versions immediately after completing the upgrade, do so now in order to complete the upgrade. Do not perform a backup until you have switched to the new software version. Perform this procedure for all nodes.</td>
</tr>
<tr>
<td>Step 2</td>
<td><strong>Remove the Serial Port, on page 104</strong></td>
<td>Remove the serial port that you added during the pre-upgrade tasks so that it does not impact VM performance. Perform this procedure for all nodes.</td>
</tr>
<tr>
<td>Step 3</td>
<td><strong>Restart Extension Mobility, on page 104</strong></td>
<td>If you deactivated Cisco extension mobility as part of the pre-upgrade tasks, you can now restart it.</td>
</tr>
<tr>
<td>Step 4</td>
<td><strong>Restart TFTP Services, on page 105</strong></td>
<td>Use this procedure to restart TFTP services on Unified CM nodes.</td>
</tr>
<tr>
<td>Step 5</td>
<td><strong>Reset TFTP Parameters, on page 105</strong></td>
<td>Reset TFTP parameters that are changed during the upgrade process.</td>
</tr>
<tr>
<td>Step 6</td>
<td><strong>Restore Enterprise Parameters, on page 105</strong></td>
<td>Restore any Enterprise Parameter settings on IM and Presence Service nodes that may have been overwritten during the upgrade process.</td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
<td></td>
</tr>
<tr>
<td>-------------------------------------------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------</td>
<td></td>
</tr>
</tbody>
</table>
| **Step 7** Reset High and Low Watermarks, on page 106 | Use this procedure to restore the high and low watermarks to their original values in order to avoid premature purging of traces.  
You can skip this task for PCD migrations.                     |
| **Step 8** Updating VMWare Tools, on page 106         | You must update the VMWare Tools after you complete the upgrade.  
Perform this procedure for all nodes.                                      |
| **Step 9** Install Locales, on page 107               | After an upgrade, you must reinstall any locales that you are using, with the exception of US-English, which is installed by default.  
Perform this procedure for all nodes.                                |
| **Step 10** Restore the Database Replication Timeout, on page 109 | Use this procedure if you increased the database replication timeout value before you began the upgrade process.  
Perform this procedure on Unified Communications Manager nodes only. |
| **Step 11** Verify the Registered Device Count, on page 109 | Use this procedure to verify your endpoints and resources on Unified CM nodes after the upgrade is complete.            |
| **Step 12** Verify Assigned Users, on page 110        | Use this procedure to verify the number of assigned users on Instant Messaging and Presence nodes after the upgrade is complete. |
| **Step 13** Test Functionality, on page 110           | Verify phone functions and features are working correctly after the upgrade.                                                           |
| **Step 14** Upgrade RTMT, on page 111                 | If you use Cisco Unified Real Time Monitoring Tool (RTMT), upgrade to the new software version.                                        |
| **Step 15** Manage TFTP Server Files, on page 112     | Optional. Use this procedure to upload phone rings, callback tones, and backgrounds to a TFTP server so that they are available to Unified CM nodes. |
| **Step 16** Set Up a Custom Log-On Message, on page 113 | Optional. For Unified CM nodes only, upload a text file that contains a customized log-on message.                                 |
| **Step 17** Configure IPSec Policies, on page 113     | If you are completing a PCD migration from Release 6.1(5), you must recreate your IPSec policies as they are not migrated to the new release. |
### Purpose

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 18</strong> Assign New Manager Assistant Roles, on page 114</td>
<td>If you had Manager Assistant deployed before the upgrade and users were assigned to the InterCluster Peer-User or Admin-CUMA roles, you must reassign users to roles, as these roles do not exist in the current release.</td>
</tr>
<tr>
<td><strong>Step 19</strong> Verify IM and Presence Service Data Migration, on page 114</td>
<td>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.</td>
</tr>
<tr>
<td><strong>Step 20</strong> Enable High Availability on Presence Redundancy Groups, on page 115</td>
<td>If you disabled High Availability for the Instant Messaging and Presence Service before the upgrade process, use this procedure to turn it back on.</td>
</tr>
<tr>
<td><strong>Step 21</strong> Restart the IM and Presence Sync Agent, on page 116</td>
<td>If you stopped the Instant Messaging and Presence Sync Agent service before you began the upgrade process, restart it now.</td>
</tr>
</tbody>
</table>

### Switch the Software Version

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

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

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

⚠️ **Caution**

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

### Before you begin

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

Review the information in **Understanding Version Switching, on page 88**

### Procedure

1. **Step 1** If you switch versions in a multinode deployment, you must switch the publisher node first.
2. **Step 2** Log in to the management software for the node that you are upgrading:
• If you are upgrading an Instant Messaging and Presence node, log in to Cisco Unified IM and Presence Operating System Administration.
• If you are upgrading a Unified Communications Manager node, log in to Cisco Unified Communications Operating System Administration.

**Step 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

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

**Procedure**

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

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

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

**Step 4** Click **Restart**.
Restart TFTP Services

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

**Procedure**

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

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

**Step 3**  
Select the **Cisco TFTP** services.

**Step 4**  
Click **Restart**.

Reset TFTP Parameters

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

**Procedure**

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

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

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

**Step 4**  
Click **Advanced**.

**Step 5**  
Click **Save**.

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

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

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

Restore Enterprise Parameters

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

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

**Before you begin**

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

**Procedure**

1. From the Cisco Unified CM IM and Presence Administration interface, choose System > Enterprise Parameters.
2. Compare the current settings to the settings that existed prior to the upgrade and update the Enterprise Parameters as needed.
3. Click **Save**.
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**

1. In the Real Time Monitoring Tool (RTMT) interface, double-click Alert Central in the left navigation pane.
2. On the System tab, right-click LogPartitionLowWaterMarkExceeded and select Set Alert/Properties.
3. Select Next.
4. Adjust the slider value to 80.
5. On the System tab, right-click LogPartitionHighWaterMarkExceeded and select Set Alert/Properties.
6. Select Next.
7. Adjust the slider value to 85.

**Updating VMware Tools**

VMware Tools are a set of utilities for management and performance optimization. Your system uses one of the following VMware Tools:

- Native VMware Tools (provided by VMware)
- Open VMware Tools (provided by Cisco)
• To upgrade Unified Communications Manager from a version earlier than Release 11.5(x), you must use the native VMware tools option. You can change to open VMware Tools after the upgrade.

• For upgrades from Unified Communications Manager Release 11.5(1) onwards (for example, to a higher SU), you can choose whether your system use Native VMware or Open VMware Tools.

• For fresh installation and PCD migrations from Unified Communications Manager Release 11.5(1) onwards, open VMware tools installed by default.

Procedure

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

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

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

- Initiate the automatic tools update with the viClient.

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

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

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

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

**Install Locales**

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

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

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

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

Step 1  Find the locale installer for your release on cisco.com:
   • For Cisco Unified Communications Manager, go to https://software.cisco.com/download/navigator.html?mdfid=268439621&i=rm
   • For IM and Presence Service, go to https://software.cisco.com/download/navigator.html?mdfid=280448682&i=rm

Step 2  Download your release's locale installer to a server that supports SFTP. You need the following files:
   • User Locale files—These files contain language information for a specific language and country and use the following convention:
     • cm-locale-language-country-version.cop (Cisco Unified Communications Manager)
     • ps-locale-language_country-version.cop (IM and Presence Service)
   • Combined Network Locale file—Contains country-specific files for all countries for various network items, including phone tones, annunciators, and gateway tones. The combined network locale file uses the following naming convention:
     • cm-locale-combinednetworklocale-version.cop (Cisco Unified Communications Manager)

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

Step 4  Choose Software Upgrades > Install/Upgrade.

Step 5  Complete the following fields in the Software Installation/Upgrade window:
   • For the Source, choose Remote file System.
   • From the Directory, enter the path to the directory where you saved the locale installer.
   • From the Server field, enter the server name for the remote file system.
   • Enter the credentials for the remote file system.
   • From the Transfer Protocol drop-down list, choose SFTP. You must use SFTP for the transfer protocol.

Step 6  Click Next.

Step 7  Download and install the locale on the server.

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

Step 9  Repeat this procedure on all Unified Communications Manager and Instant Messaging and Presence cluster nodes in the prescribed order.
Do not reset user locales for your end users until the new locale is installed on all cluster nodes. If you are installing the locale for both Unified Communications Manager and Instant Messaging and Presence Service, you must install the locale for both products before you reset user locales. If you run into any issues, such as could occur if an end user resets a phone language before the locale installation is complete for Instant Messaging and Presence Service, have your users reset their phone language in the Self-Care Portal to English. After the locale installation is complete, users can reset their phone language, or you use Bulk Administration to synchronize locales to the appropriate language by bulk.

**Note**

**Restore the Database Replication Timeout**

This procedure applies to Unified Communications Manager nodes only.

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

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

**Procedure**

**Step 1**

Start a CLI session using one of the following methods:

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

**Step 2**

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

**Verify the Registered Device Count**

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

**Procedure**

**Step 1**

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

**Step 2**

Record the number of registered devices:

<table>
<thead>
<tr>
<th>Item</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>Registered Phones</td>
<td></td>
</tr>
<tr>
<td>Registered Gateways</td>
<td></td>
</tr>
</tbody>
</table>
Verify Assigned Users

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

Procedure

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

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

Test Functionality

After the upgrade, perform the following tasks:

- 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
Upgrade RTMT

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

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

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

Procedure

Step 1 From Unified Communications Manager Administration, choose Application > Plugins.
Step 2 Click Find.
Step 3 Perform one of the following actions:
   • To install the tool on a computer that is running the Microsoft Windows operating system, click the Download link for the Cisco Unified Real-Time Monitoring Tool - Windows.
   • To install the tool on a computer that is running the Linux operating system, click the Download link for the Cisco Unified Real-Time Monitoring Tool - Linux.
Step 4 Download the installation file to your preferred location.
Step 5 Locate and run the installation file.
The extraction process begins.
Step 6 In the RTMT welcome window, click Next.
Step 7 Because you cannot change the installation location for upgrades, click Next.
The Setup Status window appears; do not click Cancel.
Step 8  In the **Maintenance Complete** window, click **Finish**.

---

**Manage TFTP Server Files**

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

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

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

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

**Procedure**

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

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

**Step 2**  To upload a file, follow this procedure:

a) Click **Upload File**.

   The Upload File dialog box opens.

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

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

d) To start the upload, click **Upload File**.

   The Status area indicates when the file uploads successfully.

c) 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**.
Set Up a Custom Log-On Message

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

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

**Procedure**

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

The Customized Logon Message window displays.

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

**Step 3**
Click **Upload File**.

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

The system displays the customized log-on message.

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

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

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

Configure IPSec Policies

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

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

• IPsec, especially with encryption, affects the performance of your system.

Procedure

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

Step 2
Click Add New.

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

Step 4
Click Save.

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

Assign New Manager Assistant Roles

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

Procedure

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

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

Verify IM and Presence Service Data Migration

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

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

Description: Migrated Service Profile Number x

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

Profiles that are created but that are not assigned to users are not migrated to Unified Communications Manager.
Enable High Availability on Presence Redundancy Groups

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

Before you begin

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

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

Procedure

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

Step 2 Click Find and select the Presence Redundancy Group.

Step 3 Check the Enable High Availability check box.

Step 4 Click Save.

Step 5 Repeat this procedure in each Presence Redundancy Group.
Restart the IM and Presence Sync Agent

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

Procedure

| Step 1 | From the Cisco Unified Serviceability interface, select Tools > Control Center - Network Services. |
|Step 2 | Select an Instant Messaging and Presence node from the Server drop-down list and click Go. |
|Step 3 | In the IM and Presence Services section, select the Cisco Sync Agent and click Restart. |

Example

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

Troubleshooting

• Troubleshooting, on page 119
Troubleshooting

This section contains the following information:

- Dump a Log File After an Upgrade Failure, on page 119
- Troubleshooting Unified Communications Manager Upgrades, on page 120
- Troubleshooting IM and Presence Upgrades, on page 122

Dump a Log File After an Upgrade Failure

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

Before you begin

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

Procedure

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

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

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

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

Step 4  Select the datastore where you created the file.

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

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

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

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

Step 8  If the file size is zero, complete the following steps:
a) Power off the virtual machine.
b) Create a new file for log output.
c) Unmap the installation disk.
d) On the Options tab, select Boot Options and enable Force BIOS Setup.
e) Power on the virtual machine and wait for it to boot to the BIOS.
f) In the BIOS, select the hard drive as the first boot device and save and exit.
   The system will boot to the hard drive and go back to the point where the upgrade failed. A failure notification displays.
g) Input yes to dump the contents of the log to a file.
h) Navigate to the file and open it using 7-Zip.

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

**Troubleshooting Unified Communications Manager Upgrades**

This section provides information about 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_y<latest_version>.cop.sgn). This
COP file removes the inactive side in the common partition to increase available disk space without
requiring a system rebuild. Ensure that you review the Readme file that supports this COP file before
you proceed.

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

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

Download Failure in Cluster-Wide Upgrade

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

Procedure

Step 1 Download the build manually on the failed node.
Step 2 Log into Cisco Unified Operating System Administration, choose the Software Upgrades > Install/Upgrade
Cluster.
Step 3 Select the local Filesystem option to get the existing image and proceed further.
Step 4 If you are performing the upgrade at Command Line Interface, run the utils system upgrade initiate
CLI command and select the Local Image option.

You do not need to download the image again.

Reduced Permissions for Access Control Groups

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

Solution Users can belong to multiple access control groups. When you add a new access control group to
existing users, the current level of privileges for some pre-existing access control groups may be reduced if
the new access control group has the “Effective Access Privileges for Overlapping User Groups and Roles”
Enterprise parameter set to minimum.
Access privilege reduction can occur inadvertently, for example, during an upgrade of Cisco Unified CM Administration. If the upgrade version supports the Standard RealTimeAndTrace Collection user group, which has the “Effective Access Privileges for Overlapping User Groups and Roles” Enterprise parameter set to minimum, all users are automatically added to that user group during the upgrade. To resolve the permissions issue in this example, you can remove users from the Standard RealTimeAndTrace Collection user group.

Loss of Phone Settings

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

Post-Upgrade Failure of Unified Communications Manager Publisher Node

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

**Solution** Do one of the following:

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

Post-Upgrade Failure of Unified Communications Manager Subscriber Nodes

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

**Solution** Do one of the following:

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

Troubleshooting IM and Presence Upgrades

This section provides information about troubleshooting Instant Messaging and Presence Service upgrades.

Upgrade Failure of IM and Presence Database Publisher Node

**Problem** You are upgrading a multinode cluster that includes both Unified Communications Manager and Instant Messaging and Presence nodes, and the upgrade of the Instant Messaging and Presence database publisher node fails.
Solution The action that you take depends on the point at which the failure occurred:

• if the upgrade on the Instant Messaging and Presence database publisher node fails before the refresh upgrade causes the node to reboot (that is, if the node failed before switching to the new partition), perform the upgrade again on the Instant Messaging and Presence database publisher node

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

Upgrade Failure of IM and Presence Subscriber Node

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

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

• if the upgrade on the Instant Messaging and Presence subscriber node before the refresh upgrade causes the node to reboot (that is, if the node failed before switching to the new partition), perform the upgrade again on the Instant Messaging and Presence subscriber node

• if the upgrade on the Instant Messaging and Presence subscriber node fails after the node switched to the new version, you must complete the following tasks in the order listed:
  • switch the Unified Communications Manager publisher node back to the earlier software version
  • switch the Unified Communications Manager subscriber node back to the earlier software version
  • switch the Instant Messaging and Presence database publisher node back to the earlier software version
  • switch the Instant Messaging and Presence subscriber nodes back to the earlier software version
  • switch the Unified Communications Manager publisher node pub forward to the new software version
  • switch the Instant Messaging and Presence database publisher node forward to the new software version
  • perform the upgrade again on the Instant Messaging and Presence subscriber node
Upgrade From Pre Release 8.6(4) Fails

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

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

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

IM and Presence user phone presence problems

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

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

Presence User Experiences Issues Obtaining Availability

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

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

Real-Time Monitoring Tool alert for Cisco SIP proxy service

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

Solution You must restart the Cisco SIP Proxy service. In Cisco Unified IM and Presence Serviceability, select Tools > Control Center - Features Services.
Cannot find upgrade file on remote server

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

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

Upgrade file checksum values do not match

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

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

Database replication did not complete

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

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

Cisco UP Presence Engine database does not restart

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

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

Version Errors

**Selected Upgrade Is Disallowed From the Current Version**

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

**Solution** You did not install the required COP file on the node. Download the following COP file from Cisco.com: `ciscocm.cup.refresh_upgrade_<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 an Instant Messaging and Presence server, you cannot select the software image from the disk or remote directory. The following error is reported: The version obtained from the name does not match the active or inactive version of the publisher.

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

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

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

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

Switch Version on Cisco IM and Presence Node Fails

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

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

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

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

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

Failed refresh upgrade

**Problem** A refresh upgrade failed.

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

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

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

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

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

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

Common Partition Full Upgrade Failure

**Problem** The upgrade of Instant Messaging and Presence fails with an error stating that the common partition is full.

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

Appendix

• Frequently Asked Questions, on page 131
• Upgrading from Legacy Releases, on page 135
• Additional Upgrade Resources, on page 137
Frequently Asked Questions

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

Verify the requirements for the new release using the information below. After you have verified the requirements for the new release, see Virtual Machine Configuration Tasks, on page 55 for instructions.

Table 23: Virtual Machine Requirements

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

Verify whether you need to change the virtual hardware specifications on your VM in order to upgrade to a new release of Unified Communications Manager or Instant Messaging and Presence. For example, verify the requirements for vCPU, vRAM, vNIC adaptor type, and vDisk size, as well as other specifications.

Any changes to a VM must align with the OVA configuration. VM changes that result in an unsupported OVA configuration are not allowed. For information about VM requirements, see Readme file with the OVA template that supports your release.

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

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

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

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


To obtain an OVA file, see Download and Install OVA Templates, on page 57.

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

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/.
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](http://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/compat/ccmcompmatr1.html#pgfId-391518).

Table 24: Upgrade Paths for Legacy Releases

<table>
<thead>
<tr>
<th>Installed Version</th>
<th>Upgrade to this Version on MCS hardware</th>
<th>Migrate to this Version on a Virtual Machine</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco Unified Communications Manager Releases</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4.x</td>
<td>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 &quot;Supported Upgrade Paths To/From Table&quot; at the link above.</td>
<td>PCD Migration to 11.5(1)</td>
</tr>
</tbody>
</table>
### Installed Version

<table>
<thead>
<tr>
<th>Installed Version</th>
<th>Upgrade to this Version on MCS hardware</th>
<th>Migrate to this Version on a Virtual Machine</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.1(2)</td>
<td>Direct Upgrade to 6.1(5) or 7.1(3)</td>
<td>PCD Migration to 11.5(1)</td>
</tr>
<tr>
<td>5.1(3)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6.0(x)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6.1(1)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6.1(2)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6.1(3)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6.1(4)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>7.0(1)</td>
<td>7.1(3), 7.1(5), 8.x, or 9.x</td>
<td>PCD Migration to 11.5(1)</td>
</tr>
<tr>
<td>7.1(2)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Cisco Unified Presence Releases

<table>
<thead>
<tr>
<th>Installed Version</th>
<th>Upgrade to this Version on MCS hardware</th>
<th>Migrate to this Version on a Virtual Machine</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.0(x)</td>
<td>Direct Upgrade to 8.5(4)</td>
<td>PCD Migration to 11.5(1)</td>
</tr>
</tbody>
</table>

### Cisco Unified Communications Manager Business Edition Releases

<table>
<thead>
<tr>
<th>Installed Version</th>
<th>Upgrade to this Version on MCS hardware</th>
<th>Migrate to this Version on a Virtual Machine</th>
</tr>
</thead>
<tbody>
<tr>
<td>Business Edition 3000 (BE3000)</td>
<td>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.</td>
<td></td>
</tr>
<tr>
<td>Business Edition 5000 (BE5000)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Procedure

**Step 1**

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


**Step 2**

Additional Upgrade Resources

- Additional Upgrade Resources, on page 137

Additional Upgrade Resources


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